Proceedings of the

INTERNATIONAL ATOMIC ENERGY AGENCY
SPECIALISTS' MEETING ON

HUMAN-MACHINE INTERFACE FOR OFF NORMAL AND EMERGENCY SITUATIONS IN NUCLEAR POWER PLANTS

Taejon, Korea
1999 October 26 - 28

**Organized by the
International Atomic Energy Agency
in co-operation with
Korea Atomic Energy Research Institute and
Korea Power Engineering Company, Inc.**

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Submission Statement

TO: The president of KAERI

This technical report is submitted as the report for the proceedings of the IAEA specialists' meeting on "Human-Machine Interface for Off normal and Emergency Situations in Nuclear Power Plants"

January 10, 2000

Prepared by

Kee-Choon Kwon (MMIS Team)

PREFACE

The International Atomic Energy Agency (IAEA) Specialists' Meeting on "Human-Machine Interface for Off Normal and Emergency Situations in Nuclear Power Plants" was co-organized by the Korea Atomic Energy Research Institute (KAERI) and the Korea Power Engineering Company, INC (KOPEC), and took place in Taejon, Republic of Korea, 1999 October 26-28.

Fifty eight participants, representing nine member countries reviewed recent developments and discussed directions for future efforts in the Human-Machine Interface for Off Normal and Emergency Situations in NPPs. Twenty papers were presented, covering a wide spectrum of technical and scientific subjects including recent experience and benefits from Operational Experience with HMI, Development of HMI System, Licensing Issues for HMI and Future Development and Trends.

The conference banquet was held at Lotte Hotel on Tuesday evening hosted by Dr. Ki-In Han, vice president of KOPEC.

The meeting concluded on Wednesday afternoon with a tour of KAERI/ITF and Hanaro Research Reactor. A technical visit to Yonggwang NPP was arranged by the Korea Electric Power Company (KEPCO) on Thursday, 28th October. A visit to the beautiful Korean temple Sunwoon-Sa also followed in a shiny and warm weather.

CONTENTS

Session 0:
Opening Address and Meeting Schedule

Session 1:
Operational Experience with HMI
Chairmen:Suk-Joon Park and Andrei Kossilov

Session 2:
Development of HMI System for Off Normal and Emergency
Chairmen: Poong Hyun Seong and Gerhard Schildt

Session 3:
Licensing Issues for HMI
Chairmen: Won Young Yun and Brian Smith

Session 4:
Further Development and Trends
Chairmen: Kee-Choon Kwon and S. Kono

Session 5 :
General Discussions, Conclusions and Recommendations
Chairmen: Hyun-Kook Shin and Richard Coe

SESSION 0

OPENING ADDRESS
AND
MEETING SCHEDULE

WELCOMING REMARKS

Suk-Joon Park
Meeting Chairman
Korea Power Engineering Company

Ladies and Gentlemen,

It is my pleasure to welcome you to this Specialists' Meeting on "Human-Machine Interface for Off Normal and Emergency Situations in Nuclear Power Plants". Welcome to Taejon, the center of scientific research in Korean Republic.

In the past two decades, constantly evolving technologies in the human-machine interface and computer applications contributed to the enhancement of control room environment in nuclear power plants. When operating nuclear power plants, it is of crucial importance to train and provide adequate amount of carefully orchestrated real-time information to the operating personnel and the engineering staff.

Especially in emergency and off-normal situations, it is important not to confuse or overload the crew with too much information or misleading information presented on the monitoring and control panel devices.

History shows that many severe accidents or events practically resulted from human errors along with incorrect interpretation given by poorly configured human-machine systems. Since Three Mile Island accident, much effort and attention have been drawn into developing better display and annunciation systems following human factors engineering research.

While there are various human-machine interface systems in nuclear power plants, issues about improving the control room panels and training the operating personnel on the ever-evolving control room environment are receiving more attention. Digital technology has been increasingly recognized as an invaluable means for the support and enhancement of human-machine interfaces in nuclear power plants in all aspects. Areas other than control room panel also deserve more attention and research.

Those are; maintenance, shutdown operations, disturbance and emergency operations, process control and safety engineering.

With technological and philosophical development of control room concepts and other engineering concerns, heavy effort has been put in integrating the best hardware and software in order to provide secure operating environment. This naturally resulted in developers having to spend more time and budget on verification and validation of the systems undergoing development and staging.

During the last several years, the IAEA has been addressing the importance of these issues, and recognizing the growing importance of the human-machine interface to safety and economics of nuclear energy production, and considering that new solutions are being developed, the IAEA decide to convene this specialist meeting on HMI in nuclear power plants, focused on off-normal and emergency situations. It will provide an opportunity to exchange experiences on HMI from a variety of positions and solutions developed in different countries and utilities under differing circumstances.

Economic concerns regarding more cost-effective tools and evaluation methods to support decisions on HMI for emergency situations in nuclear power plants, will be discussed along with experience by entities from related industries.

Main topics of this meeting are the following;

Sharing operational experience with HMI
Development of HMI system for off normal and emergency situation
Licensing issues for HMI
Further developments and trends in HMI

I would like to thank Drs. Kee-Choon Kwon of Korea Atomic Energy Research Institute and Hyun-Kook Shin of Korea Power Engineering Company for coordinating and organizing this meeting, and especially thank Messrs. Milorad Dusic and Andrei Kossilov of IAEA for assuming the role of scientific secretaries and helping in developing the program and sessions with their technical experience and knowledge.

To the participants from member countries and institutions, I thank you all again and wish you to have a productive and successful meeting.

IAEA SPECIALISTS' MEETING ON HUMAN-MACHINE INTERFACE FOR OFF NORMAL AND EMERGENCY SITUATION IN NPPs

Taejon, Rep. Of Korea
1999 26-28 October

MONDAY, 25 OCTOBER 1999	
Afternoon	Organizing Group(IAEA, KAERI, KOPEC) Pre-meeting for final schedule adjustment

TUESDAY, 26 OCTOBER 1999	
8:30 - 09:00	Registration at KAERI, bus leaves from the Lotte hotel at 8:10
09:00 - 9:30	**Opening Session** Welcoming Remarks – Meeting Chairman
9:30 - 10:30	**Session 1: <u>Operational Experience with HMI</u>** **Chair:** Suk-Joon Park and Andrei Kossilov
	Paper 1: Seung Han, J.B.Han, S.M.Baek, K.C.Son, Robert Fuld; "Experiences on HFE Verification and Validation of Critical Function Monitoring System for Yonggwang Units 5and 6"
	Paper 2: S. Kono, M. Kotoku, M. Katsuta, Y. Hosaka; "Retrofit Application of Digital Power Range Monitor to BWR"
10:30-11:00	COFFEE BREAK AND REGISTRATION
11:00-12:30	**Session 1:** (Continuation)
	Paper 11: T. Tahir; "Computerized Operator Information System at KANUPP"
	Paper 4: R. Coe; "Real World Simulator Training for NPP Operators and Management - when Off-Normal becomes Normal"
	Paper 5: Daihwan Min,Yun-Hyung Chung,Borkryeul Kim ; "Distributed GOMS: An Application to Emergency Operation of NPP"
12.30-13.30	LUNCH BREAK
13:30-15:00	**Session 2: <u>Development of HMI System for Off Normal and Emergency</u>** **Chair:** Poong Hyun Seong and Gerhard Schildt
	Paper 6: Yong-Hee Lee, Wan. C Yoon; "Human Factor Evaluation of a Safety Parameter Display System in Nuclear Power Plants using a Cognitive Task Analysis Method"
	Paper 7: R. Brice; "Creating Effective Control Room Layouts"
	Paper 8: Jin-Koo Kim, Moon-Jae Choi, Il-Nam Choe; "Design Approach and Development of Prototype for Soft Control Systems in KNGR MMIS"
15:00-15:30	COFFEE BREAK
15:30-17:30	**Session 2:** (Continuation)
	Paper 9: M. P. Feher; "The Design of CANDU Control Centres in Support of Off-Normal and Emergency Situations"
	Paper 10: Eung Se Oh,Yeong-Cheol Shin; "KNGR Information Display Designs "
	Paper 3: Joong Nam Kim; "The Role of Computerized Procedure System in Facilitating Operator Performance during Off-Normal and Emergency"
	Paper 20: A. Puzanov, I. Puzanova, A. Bazin: "Vibration Diagnostic System: Analysis of Emergency Situation in Power Plant"

WEDNESDAY, 27 OCTOBER 1999	
9:00 - 10:30	**Session 3:** Licensing Issues for HMI **Chair:** Won Young Yun and Brian Smith
	Paper 12: Hyun Gook Kang, Poong Hyun Seong; "A Methodology for Evaluating Alarm-processing System using Information Entropy Based Measure and the Analytic Hierarchy Process"
	Paper 13: Jong Hyun Kim, Poong Hyun Seong; "A Methodology for Quantitative Evaluation of Dynamic Aspects of NPP Fault Diagnostic Systems"
	Paper 14: Seung-Min Baek, J.B.Han, K.S.Sung, S.Han, Y.H.Lee; "Application of Human Factor Engineering Program for Safety Parameter Display and Evaluation system (SPADES) Design"
10:30 - 11:00	**COFFEE BREAK**
11:00 - 12:30	**Session 4:** Further Development and Trends **Chair:** Kee-Choon Kwon and S. Kono
	Paper 15: In-Koo Hwang, Jung-Taek Kim; "Development of Alarm-Diagnosis Integrated Operator Support System"
	Paper 16: G. Schildt; "Safety Critical Process Visualization for NPPs"
	Paper 17: Soon-Ja Song, I.K. Hwang, D.Y. Lee, W. M. Park, K. H. Cha; "A Display System Design for Remote User Using Relational Data Base"
12:30 - 13:30	**LUNCH BREAK**
13:30 - 14:30	**Session 4:** (Continuation)
	Paper 18: M. Lechleuthner, C. Hessler; Information and Diagnostic Systems
	Paper 19: Cheol-Kwon Lee, "Development of Safety Console Layout for the design of SMART MCR"
14:30 - 15:00	**COFFEE BREAK**
15:00 - 16:00	**Session 5** : General Discussions **Chair**: Hyun-Kook Shin and Richard Coe Conclusions and Recommendations
16:00 - 18:00	Tour on KAERI ITF and HANARO Research Reactor

THURSDAY, 28 OCTOBER 1999	
	Technical Visit to Yonggwang NPP
8:30 - 11:00	Bus Trip to SunWoon-sa Temple
11:00 - 12:00	Tour of SunWoon-sa Temple
12:00-13:00	**LUNCH BREAK**
13:00 - 14:00	Bus Trip to Yonggwang NPP
14:00 - 16:00	Site Tour
16:00 - 19:00	Bus Trip to Taejon

SESSION 1

OPERATIONAL EXPERIENCE WITH HMI

Experiences on HFE Verification and Validation of Critical Function Monitoring System for Yonggwang Units 5 and 6

Seung Han, Seung-Min Baek, Ki-Chang Son, Jai-Bok Han
Korea Power Engineering Company, Inc.
Duk-jin Dong 150, Yu-song Gu, Taejon, 305-353, Republic of Korea
E-mail: hanlee@ns.kopec.co.kr

Robert B. Fuld
ABB-CE
2000 Day Hill Rd. Windsor, CT. 06095 U.S.A.
E-mail: robert.b.fuld@us.abb.com

ABSTRACT

The Critical Function Monitoring System(CFMS), which is a part of Plant Monitoring System for Yonggwang Units 5 and 6(YGN 5 and 6), provides operator with concise and integrated information to evaluate plant status. CFMS satisfies post-TMI regulatory requirements for a Safety Parameter Display System(SPDS). According to human factors requirements for SPDS in related codes and standards, CFMS must be confirmed to be usable and effective for this task based on Human Factors Engineering Verification and Validation(HFE V&V) activities. Following the HFE V&V Plan for YGN 5 and 6, Availability verification and Suitability verification for CFMS were performed using appropriate reviews, analyses, and checklists. Several findings that were determined to be Human Engineering Discrepancies(HEDs) were evaluated and results were formalized for resolution. At a later time, as-installed inspections and final validation activities will be conducted.

1. INTRODUCTION

The Critical Function Monitoring System(CFMS) for YGN 5 and 6 is designed to meet the Safety Parameter Display System(SPDS) criteria set forth as part of the post-TMI Action Plans in NUREG-0696[1] and Supplement 1 to NUREG-0737[2]. CFMS continuously displays information from which the safety status of the plant can be readily assessed by control room operators who are responsible for protecting the plant. CFMS is designed to incorporate accepted human factors principles so that the displayed information can be readily perceived and comprehended by operating crew.

The guidelines for the implementation of SPDS requirements described in NUREG-0737 supplement 1[2] are presented in SRP 18.2[7], and human factors acceptance criteria and supporting information are described in NUREG-0700[3]. In SRP 18.2 and Appendix A, review guidelines that are related to human factors engineering are presented. The scope of the staff's review is to evaluate that SPDS can support control room personnel during abnormal and emergency conditions in determining the safety status of the plant and to assess whether abnormal conditions can be corrected by operators to avoid a degraded core. The review is bounded by the minimal set of plant variables, hardware, software processing algorithms and operator training to achieve the principal SPDS functions. In NUREG-0700, general guidelines for visual display, process computer and CRT display are described. Also, it emphasizes human factors engineering principles for SPDS CRT display. According to the specific requirements for the SPDS described above, it is required that CFMS need to be verified based on human factors principles in HFE V&V Plan[11].

HFE V&V Plan addresses HFE V&V team organization, responsibility of V&V team, detail HFE V&V plan and methodologies for each HFE V&V activities. With the schedule described in HFE V&V plan, the HFE review staff analyzes CFMS display design concept, verifies its acceptability and provides evaluation results and proposed resolution to solve the problem that is found during V&V process.

2. GENERAL METHOD OF HFE V&V

The general method of Human Factors Engineering Verification & Validation (HFE V&V) for YGN 5 and 6 CFMS followed the classic approach defined in NUREG-0700[3]. This consists of three main components:

- Verification of Availability (AV),
- Verification of Suitability (SV),
- Validation (V).

This general approach to HFE V&V is consistent with V&V for post-TMI control room design reviews, YGN 3 and 4[17] and UCN 3 and 4[14] CFMS, the Nuplex 80+ Advanced Control Complex[12] and KNGR Man-Machine Interface System[13]. In addition, HFE V&V offers sufficient flexibility and it can be effectively combined with portions of Software V&V guidelines provided by NSAC-39[5]. Finally, HFE V&V is shown to be compatible with and acceptable in terms of applicable human factors engineering program criteria presented in NUREG-0711[6].

2.1 Verification of Availability

The Availability checklist for YGN 5 and 6 CFMS V&V was prepared based on a list of applicable human factors requirements. The source of such requirements is as follows:

- Regulatory/licensing requirements
- Design requirements for display and alarm
- Emergency procedures/guidelines
- Resolved commitments from Operating Experience Review(OER)

The Availability verification of CFMS was planned in two phases. A preliminary Availability verification (analysis) was performed on the final CFMS implemented list(List-I). The requirement-based list as criteria was applied to verify acceptable contents of List-I. Copies of the lists were annotated by the reviewers as a record of the review activity. After the preliminary Availability verification, Human Engineering Discrepancies (HEDs) were identified and explained in a formal report, including a proposed resolution. The Availability verification report was reviewed and the resolutions approved by an interdisciplinary team including representatives from system design and plant operation. Based on the approved resolutions, the List-I will be revised. After revising List-I, the Availability analyst will confirm the revisions as proper implementation. The revised and confirmed List-I will be served as the checklist for the final Availability verification (inspection) of the as-built and installed displays.

2.2 Verification of Suitability

The Suitability checklist for YGN 5 and 6 CFMS V&V was prepared based on the guidelines for YGN 3 and 4 and UCN 3 and 4 V&V. YGN 3 and 4 CFMS V&V utilized the guidelines from NUREG-0700(Sections 6.5 & 6.7)[3], NUREG-0737 (Supplement 1)[2], NUREG-0835 (Section 4)[8], Generic Letter 89-06[4], and HF-010 for YGN 3 and 4 (Section IX)[18]. UCN 3 and 4 CFMS V&V utilized an innovative 'keyword search' technique extracted from applicable regulatory requirements, standards, and guideline documents. The combined set of guidelines and references was updated for YGN 5 and 6, while incorporating the strengths and lessons learned from both approaches. With minimal effort, the best CFMS Suitability checklist was produced. In addition to the use of the checklist, reviewers specifically assessed the navigation scheme of CFMS. These two types of review were performed in parallel at UCN 3 and 4 CFMS V&V, and were related to top-down/bottom-up distinction used by Nuplex 80+ and KNGR in their mockup Suitability verification activities.

The Usability of display format is the primary issue in the verification of Suitability. Therefore, it is required that the system displays or some relatively accurate representation of the system displays should be available for review activity. Suitability review was performed by a human factors specialist, and results of the review were documented on the checklist. Then, HEDs recorded on the checklist were explained in a formal report. The Suitability verification report will be reviewed and the HEDs will be resolved by an interdisciplinary team including representatives from system design and plant operation.

2.3 Validation

Validation of the usability of YGN 5 and 6 CFMS is to confirm that necessary tasks for CFMS can be performed in a reliable and convenient way. Typical CFMS tasks include verification of plant conditions using Safety Function Status Checks. Ideally, these tests would be performed in a control room simulator environment, where plant upset conditions could be replicated. Since subjective measures are most practical and cost-effective, validation data should be prepared based on the performance of trained users of the system along with both their comments and the comments from knowledgeable observers.

3. HFE V&V METHODOLOGIES AND ACTIVITIES

3.1 Availability Verification of CFMS

Availability verification is the process of confirming that required information content (displays, alarms) is actually provided to operators by the system. The required content is compiled and compared with actual content for Availability verification. The first consideration is that all necessary information is provided. The second consideration is that unnecessary information is removed, but this is less of an issue particularly for flexible(e.g., CRT-based) display systems.

1) Methodology

CFMS HFE V&V was planned in two phases. A preliminary Availability verification (*analysis*) is performed on the final CFMS implemented list, and a final Availability verification (*inspection*) is performed on the as-built and installed displays. In fact, the final inspection can be performed in a minimum technical scope for licensing, the preliminary analysis allows findings to be corrected earlier in the design process and reduces the number and impact of errors expected in the final inspection. The verified list from the result of the analysis also provides a basis for the final inspection checklist.

2) Preliminary Availability Verification(Analysis):

For YGN 5 and 6 CFMS AV, Availability criteria and checklists were prepared based on applicable human factors requirements from the following sources:

- Regulatory/licensing requirements – NUREG-1342 Table 2[9] and PSAR Table 18.2-1[19] (List-Reg)
- Design requirements for display and alarm – Design Requirements for CFMS for YGN 5 and 6[16](List-D & List-A)
- Emergency procedure guideline – UCN 3 and 4 EPG Safety Function Status Checks[20] (List-P)
- Resolved commitments from OER – YGN 3 and 4 resolutions & operator experiences (List-O)

The criteria were applied in checklist form. The implemented CFMS list(represented by List-I) was compared with the requirement-based checklists described above. Each checklist item was checked by Point ID(PID) for assuring appropriate data variables from List-I. Analysis utilized the separate checklists identified above. Some overlap was expected among the checklists, providing diversity and increasing confidence in the results. Because of an unnecessary effort and possibility of increasing omission errors in the criteria, reducing the criteria as a single list was not considered.

3) Data Recording

Copies of the criteria and List-I were annotated by the reviewers and formally retained as a record of review activities. The primary verification result, confirming that all necessary information was provided, was tested as follows. The analyst verified that each required checklist item was actually available on List-I, recording the display page number and the PID for each item on the checklist. Any checklist item not listed in List-I PIDs was treated as a finding. Findings were investigated by the analyst, who did "follow-up" on each finding until he had basis to resolve the issue. Some findings were screened out by this process, and the rest were incorporated in HEDs. Thus, actual CFMS deficiencies were a subset of HEDs, and HEDs were a subset of findings. The secondary verification result, that unnecessary information was minimized, was tested as follows. The analyst check-marked each List-I item when it was required by a checklist criterion. Though items should be checked repeatedly, as applicable, it was generally not important either checklist was the source of the requirement or how many times the item was check-marked. All items on List-I without having a check-mark (and are thus not yet shown to be required) were findings. It was required to confirm that they had some reasonable basis for being in CFMS. Otherwise, the finding became an HED. For the purpose of identifying items without check-mark, it was more reliable and efficient to annotate a single copy of List-I than to annotate separate copies and combine the results.

In the case of List-P, the analyst prepared the checklist identifying what data variables in the procedure required to be read by the operator when using the system. This assessment was annotated as well so that the variables can be referred to unambiguously in the other analysis. Finally, all HEDs were recorded in unambiguous detail to be reliably traced and understood. HEDs were documented using forms similar to that of UCN 3 and 4 CFMS V&V, but a traceable numbering scheme was added to the UCN 3 and 4 form. In particular, findings should be combined into a single HED when they are redundant, or when they are highly similar and related.

4) HED Resolution and Results Reporting

After Analysis, HEDs identified were presented in a formal report, including an explanation and a proposed resolution. The draft Availability report was subject to formal review and comment by an interdisciplinary team including representatives from system design and plant operation. Resolutions were made based on their comments and a report was issued. Finally, List-I (or CFMS displays) will be revised. In both cases of analysis and inspection, the revisions will be confirmed by the analyst for proper implementation.

5) Final Availability Inspection

The main difference between inspection and analysis is that inspection is performed on the as-built and installed displays. The revised and confirmed List-I will be served as the checklist for the final Availability inspection. List-I will be used to record the primary finding of necessary information, i.e. the correctness of actual PIDs available from the system displays for specified objects on the screens. Also, the secondary finding of unnecessary information will be considered more carefully for the inspection of specific screens with particular purposes. Printed images of the screen displays can provide a useful form for recording these secondary findings.

3.2 Suitability Verification of CFMS

Suitability Verification (SV) is the process of confirming that the format of information in a system is acceptable for human use. To verify Suitability of the YGN 5 and 6 CFMS, the system displays and navigation features were evaluated in terms of applicable human factors design guidelines. This evaluation was performed by persons who had extensive knowledge of human factors and YGN 5 and 6 CFMS.

1) Methodology

The SV methodology in this section provides details for the general approach to SV described previously. This includes the following activities:

- Checklist Development
- Checklist Application
- Navigation Assessment
- Treatment of Findings
- In-situ Inspection

2) Checklist Development

The SV checklists for YGN 5 and 6 CFMS V&V were prepared based on the guidelines from the previous YGN 3 and 4 and UCN 3 and 4 V&V. These sources were reviewed and a comprehensive subsets were selected as follows:

- NUREG-0700, Chapter 6.5 (Visual Displays)[3]
- NUREG-0700, Chapter 6.7 (Process Computers)[3]
- NUREG-0800, Chapter 18.2 Appendix A [7]
- Generic Letter 89-06[4]
- HF-010 for YGN 5 and 6, Section 9 (Computer Displays)[10]

Since the references in the original sources did not conflict with one another, they were retained in the checklists and used for traceability. The checklist items were generic and they were pre-processed to improve their efficiency. Specifically, the following issues were addressed as much as possible before applying the checklist to the actual design:

- Guidelines inapplicable to CFMS are marked in N/A
- Guidelines depending on as-installed conditions are marked for "in-situ" inspection
- Redundant or conflicting guidelines are cross-referenced to a single effective item

The number of guidelines to be applied to the design prior to in-situ inspection was reduced by half. Since the issues were better focussed and the number of issues to be processed was significantly reduced, the main benefit of this pre-processing was to be shown in the downstream review and resolution of findings.

3) Checklist Application

The checklist was applied in a once-through way. Each guideline was evaluated for the entire system. The verifier was responsible for ensuring that the important aspects of the system were addressed by the relevant guidelines. Guidelines evaluated as 'N/A' or 'No' required further comment to be provided on the checklist. Guidelines that are 'N/A' based on other guidelines had cross-reference(e.g. "see HF-10 9.3.1"). The annotated checklists were formally retained as a record of verification activities. Any checklist item that was checked "No" was a finding.

4) Navigation Assessment

Besides the use of checklists, the Suitability of CFMS navigation scheme was verified as follows:

- Navigation Keys/Buttons (ESC, PREV, NEXT, PAGE, SECTOR, TREND, MAIN, CAL, CFM) were exercised and their behavior evaluated.
- Menu and Directory features were exercised and their behavior evaluated.
- UCN 3 and 4 CFMS V&V navigation findings (inconvenient navigation; inconsistent navigation, and inconsistent ESC function) were reviewed in terms of the YGN 5 and 6 CFMS design.

Issues such as consistency, compatibility, number of steps, memory support, and error proneness were considered. Evaluation results included findings and recommendations to ensure that the YGN 5 and 6 CFMS navigation scheme is suitable and acceptable.

5) Treatment of Findings

Findings recorded on the SV checklist were explained in a formal report. Individual findings were combined into integrated issues where they were similar or closely related. Traceable references in individual guidelines were retained in each finding. The evaluator followed each finding until he could propose acceptable resolution to the issue. These draft resolutions will be reviewed by an interdisciplinary team including representatives from system design and plant operation. Resolutions will be made based on their comments, and a report will be issued. Changes required for CFMS design are being documented using HEDs forms similar to that of UCN 3 and 4 CFMS V&V. The HED form will include a traceable numbering scheme. The HEDs will be closed when their implementation (i.e. as resolved) is confirmed in the actual CFMS.

6) Final (In-Situ) Inspection

The Suitability verification of CFMS was planned in two phases. A preliminary SV (analysis) was performed on the site deliverable system, and a final SV (inspection) will be performed on the as-built and installed displays. In fact, the final inspection can be performed in a minimum technical scope for licensing, the preliminary analysis allows findings to be corrected earlier in the design process and reduces the number and impact of errors expected in the final inspection. The same checklists will be used for both activities and emphasis in inspection can be placed on:

- guidelines identified for "in-situ" evaluation (i.e. in-situation, or as-installed)
- display features that were modified following the present SV Analysis

4. HFE V&V RESULTS

4.1 Findings from Availability Verification

There are several items that need to be checked by operator for "Maintenance of Vital Auxiliaries" in List-P from emergency procedure guideline. "Status of Vital 120 volt AC instrument channel" is one of those items to be checked, but current CFMS display does not contain this information in any of display pages. So, this information should be added for operator's convenient checking.

4.2 Findings from Suitability Verification

1) Navigation Assessment

a. Inconvenient/Inconsistent Navigation – These issues are easily mitigated by adding a dedicated DIR (directory) function key. A dedicated DIR button will reduce page navigation action by 2 steps.

b. ESC Key Issues – The basic problem is that ESC is designed to function two ways: 1) Hierarchical Exit, and 2) Rotating Buffer between current and last page. Hierarchical exit is fairly standard and the function should be retained. The rotating page buffer is a simple "last page" feature and it should be a separate function key. This relates to the PRIOR/NEXT Key functions discussed below.

c. PRIOR/NEXT Key Issues - PRIOR/NEXT functions are holdovers from keyboard navigation. The use of the directory and the mouse can minimize the value of this navigation method. It is recommended that the existing PRIOR/NEXT function should be eliminated, and a more general "last page" key should be provided.

d. Function Key Highlighting – Function keys on the CRT should be highlighted in a standard manner to show whether they are available or not for use. Otherwise, users may have unnecessary memory burden, frequent errors, and definite annoyance. Such highlights are standard conventions in commercial software programs. Highlights would make clear whether invalid functions are available or not.

e. Function Key Grouping and Order – The function keys should be grouped in a meaningful and visible way. Groups should not exceed 4 items in size without visible parsing. Also, the order of function keys on the screen and on the keyboard should be the same.

2) General Conventions and Behavior

a. Pointer and Touch Feedback – The current response of dynamic objects from pointer touch is not consistent with each type (e.g., parameters, components, directories, buttons, sector numbers, etc.). Instead, a general approach using reverse video to give touch feedback is recommended as conventional, effective, and compatible with other coding conventions (e.g., color, blink) in the system.

b. Use of White(Dynamic)/Grey(Static) Code – This subtle but important distinction is not consistently applied. For example, the Directory uses white to highlight current touch. In general, parameters are presented with white colored units even though these are static.

c. Blink Rate and Duty Cycle – The readability of blinking labels and messages would be significantly improved if the bright flash were showed up in longer cycle of the two half-cycles (presently it does not).

d. Invisible Variables – Certain dynamic status variables (e.g. acoustic leak sensors and sector numbers) are presented in an invisible default state. These are, in effect, spatially dedicated messages whose natural status is "inactive." This seems reasonable as messages, but variables should be visible as a positive indication in all states. Considering previous systems, operator experience, and avoidance of screen crowding, no change in the current approach is recommended.

e. Digital Value Alignment – Several cases were found that similar decimal values in a column were not justified by their decimal points. This makes values more difficult to be read and compared directly.

f. Digital Value Format – Some cases were found that numbers require unnecessary translation into the usual format. This was the result of using exponential notation for percentages and temperatures with four or fewer significant digits.

g. Digital Value Precision – Most CFMS screens have digital values with excess precision for their expected use with visual and cognitive load. The four significant digit rule is a useful generic guideline. In the case of not meeting the rule, eliminate decimal places or use exponential notation as necessary to maintain four significant digit displays.

h. Trend Axes - The trend axes have relatively small numeric label. In particular, the readout of time and value that are driven by the position of the cursor should be the same size as other dynamic data values.

i. Pump Symbol Labeling Convention – There are inconsistencies in the label of pump symbols. Generally, a single pump should be labeled below the symbol. A component group (three or more) should be labeled above the group, and the label should be underlined.

5. CONCLUSION

The HFE verification and validation activities of YGN 5 and 6 CFMS are being performed based on HFE V&V Plan. Well-defined HFE V&V process and methodology for CRT based system such as CFMS were constructed, and actual V&V activities were performed. The Availability verification and Suitability verification were performed using checklists extracted from applicable design requirements and human factor guidelines. The findings from Availability verification and Suitability verification were evaluated to provide proposed resolution, and the results will be added in HED for formal reporting. Validation will be performed in a control room environment according to validation plan. From the results of verification, it is recommended that information display system like CFMS shall be designed based on human factors engineering principles during development period.

REFERENCES

[1] NUREG-0696, Functional Criteria for Emergency Response Facilities, USNRC, 1981

[2] NUREG-0737 (Supplement 1). Requirements for Emergency Response Capability, USNRC, 1982.

[3] NUREG-0700, Rev.00, Guidelines for Control Room Design Review, USNRC, 1981.

[4] Generic Letter 89-06, Task Action Plan Item 1.D.2 – Safety Parameter Display System – 10 CFR 50.34(f), USNRC, 1989.

[5] NSAC-39, Verification and Validation of Safety Parameter Display Systems, NSAC, 1981.

[6] NUREG-0711, Human Factors Engineering Program Review Model, USNRC, 1994.

[7] NUREG-0800, Standard Review Plan, Chapter 18.2, USNRC, 1984.

[8] NUREG-0835, Human Factors Acceptance Criteria for the Safety Parameter Display System: Draft Report for Comment, USNRC, 1981.

[9] NUREG-1342, A Status Report Regarding Industry Implementation of Safety Parameter Display Systems, USNRC, 1989.

[10] HF-010, YGN 5 and 6 Human Factors Engineering Guideline, KOPEC, 1999.

[11] HFE-IC-710-VP, Human Factors Engineering V&V Implementation Plan for YGN 5 and 6 CFMS, KOPEC, 1999.

[12] NPX80-IC-VP790-03, HFE Verification and Validation Plan for Nuplex 80+, ABB-CE, 1995.

[13] HFE Verification and Validation Plan for KNGR Man-Machine Interface, KEPRI, 1997.

[14] Y. H. Lee, et al., KAERI/CR-024/96, Human Factors Reviews of CFMS Displays for UCN Nuclear Power Units 3 and 4, KAERI, 1996.

[15] N0594-IC-DS710, Design Specification for Plant Computer System for YGN 5 and 6, KOPEC, 1997.

[16] N0594-FS-DR210X, Design Requirements for CFMS for YGN 5 and 6, KOPEC, 1998.

[17] NU/HS-940420L. Letter delivering final YGN 3 and 4 CFMS Verification and Validation Report, KEPCO, 1994.

[18] HF-010, YGN 3 and 4 Human Factors Engineering Guideline Document, KOPEC, 1990.

[19] Preliminary Safety Analysis Report for Yonggwang Units 5 and 6, KEPCO, 1995.

[20] Ulchin Units 3 and 4 Emergency Procedure Guidelines, KAERI, 1996

Retrofit Application of Digital Power Range Neutron Monitor to BWR

S.Kono, M.Kotoku, M.Katsuta, Y.Hosaka
Toshiba Corporation Power System & Services Company, Japan

Introduction

Digital Power Range Neutron Monitor (D-PRNM) has been installed for the first time in Japan in Kashiwazaki-Kariwa Unit No6 (K-6), the first ABWR plant and have been gaining good evaluation. Based on the technology and experience of D-PRNM for ABWR, the authors have developed and installed the D-PRNM to FUKUSHIMA 2nd No.1 (2F-1) as the first retrofit application to existing BWRS in JAPAN.

The primary components of Retrofit D-PRNM are same as those for ABWR, whose reliability have already been proven in ABWR operation. However, the system configuration has been rearranged due to the difference in system requirements between ABWR and BWR. The retrofit D-PRNM have the same maintenance and operation support function as those for ABWR D-PRNM. They covers graphical man-machine interface, self-test, calibration, record and trace of trips and operations, voltage monitor of power supply and so on, which gives the convenient RAS capability as good as ABWR D-PRNM.

1. General function

PRNM system is one of in-core neutron monitoring systems that measure the neutron flux inside reactor core, and is used in power operation range where the neutron flux is from 10^{12}nv to 10^{14}nv and electric power generator is working.

The general functions of PRNM System are to input and process the output signals from plural in-core neutron detectors, monitor these processed results, calculate the average power of the nuclear reactor via averaging neutron flux in the core, monitor this average, and to induce emergency scrum signal to Reactor Protection System (RPS) which shut down the reactor when predefined limits are exceeded as one of the safety protection function. Because of this function, the system has multiply redundancy. Also, PRNM inputs re-circulation flow signals, converts them to core flow rates, and calculates the trip set points of nuclear reactor power based on the core flow rates.

Furthermore, PRNM system has RBM (Rod Block Monitor) function to restrict thermal stress of the fuel rod accompanied by the increase in the local neutron flux of the circumference of the control rod that is selected to withdraw. RBM averages the neutron-detector signals surrounding the withdrawal control rod, monitors the local average power, and outputs Rod Block signal to stop withdrawing in abnormal condition.

2. Difference with ABWR

The generation power of ABWR (K-6) is 1,350 MWe, it is 1,100 MWe for BWR (in the case of 2 F-1). The difference of reactor core size makes the number of in-core neutron detectors different. There is difference in the number of power supply system. ABWR has independent 4 systems, BWR has 2. The actuate logic of the nuclear reactor protection circuit is ' 2/4 logic' in ABWR, it is ' 1/2 twice logic' in BWR. Because of these differences, the system constitution of PRNM is also different. When the operation of reactor penetrated into the range where the core flow is low and thermal power is high, the possibility of unstableness of in-core neutron flux distribution becomes high. To prevent this condition and to secure the stability of the reactor power, the SRI function was installed to BWR that generates the signal to insert the previously selected control rods into the core when the above condition occurs. Since the internal pump (RIP) is adopted in ABWR, one Core Flow signal is calculated from one core plate differential pressure signal in each power supply division. In BWR, two Re-circulation Loop Flow signals are averaged into one Core Flow signal. In BWR-5 of a 1,100 MWe class, two Core Flow signals are calculated from 2 sets (4 pieces) of Re-circulation Loop Flow signals, and the lower value selection is performed in each power supply system. Furthermore, in comparison the FMCRD (Fine Motion Control Rod Drive) of ABWR with the water pressure drive of BWR, the longer drive stroke of BWR requests shorter response time for the rod block signal processing in RBM than ABWR, which is demanded less than 100ms for BWR, though it is 250ms for ABWR.

The difference of the plant condition of ABWR and BWR, which are related to the specification of the PRNM are shown in Table 1.

In ABWR, 208 neutron detectors are installed, and every 52 output signals are assigned to each of four independent power supply divisions (-). In each power supply division, 4 sets of units are installed respectively. 1 set is made as APRM unit that performs the monitor of a reactor average power. The other 3 sets are made as LPRM units that perform only 13 detector-signals processing. The results by 3 LPRM units are inputted to the APRM unit using the data transmission, thus APRM computes the average of the 52 detector signals. On the other hand, in 1,100 MWe classes BWR, there are 2 power-supply system (A system and B system), the number of neutron detectors is 172 pieces, 84 pieces of them are assigning to A system and rest of 84 pieces are assigning to B system. And there are 3 APRM divisions and 1 LPRM division in each power supply system. In ABWR, the signals between PRNM and process computer is a data transmission, and 1 data interface unit (DCF) is installed in every division. In existing BWR, the form of the signal is analog like voltage, current or point-of-contact.

The difference in ABWR and BWR of the D-PRNM are shown in Table 2.

Table 1. The difference of ABWR and BWR plant condition relating PRNM

	ABWR	BWR (1100 MWe)
Number of power supply system	4 systems.	2 systems.
Actuate logic circuit of RPS	out of	out of twice
Number of neutron detectors for PRNM	208 detectors	172 detectors
Core cooling water compulsion circulation method.	Pressure vessel internal pump	Circulation pump Jet pump.
Core Flow measurement instrument	Core plate differential pressure	Circulation loop flow
Number of flow signal transmitter	4 sets	8 sets
SRI function	N/A	exist
Output to Regional Exclusion system	N/A	exist
Simultaneous Rod Withdrawal number in Power Range	8 rods	1 rod
Control Rod Drive system	Fine Motion CRD (FMCRD)	Locking Piston CRD
Minimum Withdrawal number of control rod	1 step (1/4 notches)	1 notch
Response time of Rod Block signal processing (Required by safety analysis)	less than 250ms	less than 100ms

Table 2, The difference of D-PRNM system in ABWR and BWR

	ABWR	BWR (1100 MWe)
Number of neutron detectors in 1 division	52 detectors	21 or 22 detectors
Number of computation units in 1 division	4 units	1 units
Number of neutron detectors in 1 unit	13 detectors	21 or 22 detectors
Data transmission between the units inside the same division.	exist	N/A
Number of PC-boards installed in 1 unit	8 boards	19 boards
Separated Power Supply modules from computation unit	N/A	exist
Number of HVPS for 1 computation unit	2 units	4 units
Interface to process computer	Data transmission	Analog signal
Independent FLOW unit	N/A	exist (4 units / system)
Total panel width	10 m (2 m X 5 panels,including SRNM and safety PrRM)	4 m (0.8 m X 5bays)

* Even data transmission is possibility, in the case that a process computer side is corresponding.

3. Adjustment and difference with analog system

Because the retrofit replacement of the existing analog system is the main usage, the compatibility with the analog system is necessary. In full panel replacement, total size of new panels must be equal to the existing analog panels. The electric interface with external system must retain compatibility with the existing analog system too, to use the existing cables as it is even after the replacement. And the panel arrangement is also retained to prevent the operator who got used to the conventional operation of the existing analog system doing wrong operation.

The electrical isolation and physical isolation at PRNM system have already been implemented in the existing analog system. The concept of functional isolation was clarified furthermore at the D-PRNM. It means that a functional failure in a division does not affect to any other division, and it can be possible by functional independence between divisions of the redundant system. To put it concretely, the functional connection between APRM divisions via the loop connection of the core flow signals such as conventional analog system having are deleted by adoption of the independent processing of re-circulation flow signals in APRM. In the analog PRNM system, the processing results of re-circulation flow signals in each APRM divisions are exchanged with another division, so a failure in a APRM division affects another division through the low value selection and comparison abnormal determination of the core flow signals. The digital PRNM can process it respectively. Also, the comparison abnormal determination of the core flow signals is performed in RBM unit.

Although the general function of PRNM stated in Chapter 1 does not change, the details like unit functions were changed with digitization. Although the following functions were adopted in K-6, they are improving noise reduction ability, operability, and maintainability in BWR too.

- The application of the digital filter to detector signal input
- Self-diagnostic function
- Record and trend display of trip and operation
- The screen (user interface) input of calibration signal values
- The screen (user interface) input of set point values

The difference of the analog system and the digital system of the PRNM are shown in Table 3.

Table 3, The difference in digital PRNM and analog one.

	Analog	Digital
Neutron detector signal input filter	Analog filter (CR circuit	Digital filter Finite Impulse Response
Gain adjustment method of neutron detector	Selection by range switch and adjustment by variable resister	Numerical calculation by software (data transmission or key input)
Signal operation	Analog operation circuit	Numerical calculation by software
Trip judgment	Analog comparator	Numerical calculation by software
FLOW signal selection	Low value gate of self division's results and other's	Low value gate inside self unit results
SRI performed by	External equipment	APRM unit (external equipment available)
Output to Regional Exclusion	from External equipment	from RBM unit (external equipment available)
Flow signal comparison by	Flow signal rotation between APRM divisions	comparison of maximum and minimum signal in RBM unit
Display of a signal level	Analog pointer meter	Bar graph and numerical value display on flat screen
Mode selection by	Rotary switch	cursor on the screen and function key switch
Alternation of setting value	adjustment by Variable Resister	numerical value input by key operation
Self-diagnostic function	N/A	exist
Record display function of diagnosis results / Trip and alarm occurrence / Operation	N/A	exist

4. Equipment design

In the equipment design, it made a principle to follow the design at K-6 in both of hardware and software. Especially, the digital filter to the detector signal input was adopted as it is, which was developed in the joint study with Japanese BWR utilities and constructors including U.S. GE (General Electric company of the United States). However, the combination of modules inside the equipment was restructured to suit with BWR specification. In the examination of the combination of the modules, it made the improvement of reliability the highest priority .

The APRM unit block diagrams of ABWR and BWR are shown in Figure 1.

In the APRM equipment, the modules are grouped into the number that is calculated by dividing the total detectors number of a unit by the maximum number of bypass allowable detectors. The bypass allowable detector means that is permitted to be in-operative condition with keeping APRM function. And it made a fundamental idea to maintain the APRM monitoring function even if all the detectors assigned to the same group are bypassed at once when abnormality occurred in a group.

In the case of 2F-1, at least 14 detectors of 21 or 22 detectors that are allocated to one APRM unit should operate normally to maintain APRM function; therefore the maximum number of bypass allowable detectors is 7 or 8. So the modules relating to detector signal processing are grouped into 3 groups, and 7 or 8 detector signals were allocated to 1 group. Each group consisted of two detector signal conversion modules, one digital filter module, one high voltage power supply module, and one power-supply control module. The APRM unit can maintain the function even if the 2 detector signal conversion modules malfunctioned simultaneously, because 1 detector signal conversion module inputs 3 or 4 detector signals.

One more high voltage power supply module is installed in each APRM, which is used to measure detector plateau characteristic. This high voltage power supply module has enough capacity that can supply current to all the detector that are assigned to one APRM, it can be used as the backups of the other 3 high voltage power supply modules which are usually using in the same APRM when it is not used for plateau measurement. In order to receive all detector signals assigned to one division by one unit, the total of 4 high voltage power supply modules and 2 low voltage modules are taken out of APRM unit and compose another unit named ICPS.

The failure rate of unit is sharply reduced by deleting movable parts, such as variable resistor and rotary switch that were used by the analog system. The function of these parts were replaced by software adjusting.

Merit of digital equipment in comparison with analog is that it are able to materialize the various processing that treat the same input signals easily with only to make software logic, without increasing hardware. The analog PRNM system installed some additional equipment for SRI function and for the signal output to the external instability monitoring system. The D-PRNM is able to include these functions, so the equipment that added later in analog system becomes useless. However, in the 2F-1 plant, this equipment is using as it is, because of short use years and cost to remove this equipment.

5. Panel Design

The schematic diagram of the PRNM panel of 2F-1 is shown in Fig. 2.

The physical separation was not adopted to 2F-1 PRNM panel at the construction time, which requests to separate the system into 2 panels keeping physical distance. So the new PRNM panel for 2F-1 is 5 bays continuation to 1 face same as the existing analog panels. This panels have the isolation walls inside it to isolate each bays. Although the other arrangement was examined, in which the safety system separated from usual use system by gathering RBM units and DCF units to 1 bay like Figure 3.

This design was not adopted based on the judgment that to maintain the existing arrangement is more desirable by the viewpoint of incorrect operation prevention and to use existing cables as it is.

Compared with ABWR the width of the panel for BWR is narrower and the number of devices that are assigned to 1 bay of panel is larger in BWR than in ABWR, therefore the details of the install position of the devices inside the panel for BWR were decided after the temperature evaluation. The heat-analysis simulation evaluated the temperature within a panel. One example of the heat analysis is shown in Figure 4. The heat analysis estimated influence of a unit distance and a separation board, and influence of a back door of panel.

And the effort to reduce the number of units was done in adoption for 2F-1. The highly integrated Analog Output circuit was developed to reduce the number of DCF units. Using this circuit, the DCF unit was enabled to output all signals to the process computer by one unit. But considering in the case of one DCF unit failure, not to loss all signal to the computer, one more DCF was set. These tow DCF units can backup each other. Thus the number of the DCF units was reduced from initially 5 to finally 2. It decreases the total number of units in the system and expanded the mounting interval of units, and the temperature rise in a panel was reduced.

The optimal value in the unit interval was decided in consideration of the following. The isolation distance between units shall match to the demand value of the separation guideline. Keep the heat radiation route corresponding to the heating generation value of each unit. The operability of the user interface shall be fine. And display of unit screen shall be easy to see. This reduced the temperature rise in a panel and the failure rate of unit, and improved the reliability of the system.

6. Software Design

The APRM unit monitors the reactor average power, and RBM unit monitors of the control-rod drawing out considering. Both units have important functions that are safety or safety related. The software of these are treated as the standard parts of PRNM, and not change as much as possible. This improves reliability of the D-PRNM system. On the other hand, the DCF unit performs signal interface with external system, and its software is treaded as the flexibility part. This makes the system easy to adopt various interface specification that are different in each plant.

Although the fundamental structure of software is same with ABWR and BWR, the difference in the number of detectors and modules changes the repetition number of the same software loops. As shown in Chapter 2 the core flow signal processing in BWR is different from ABWR. Each APRM calculates 2 core flow signals from 4 re-circulation flow signals respectively in BWR. One APRM unit can process all detector signals in a division, so there is no data handshake between units in BWR. This simple constitution makes the software structure also simple and removes the possibility that software suspends for data reception waiting . No possibility of influence to the software action by outside condition and the simple structure of software increases the system reliability.

7.V & V

The V&V (Verification and Validation) based on JEAG4609 that are similar to ANS 7-4.3.2-1982 are not required to PRNM, because in-core neutron monitor system is positioned not as control system but sensor. As for recent the economization of V&V works is proposed. Therefore, it is in the trend that the work is carried out targeting only the modified part from a precedence system if it is. And V&V of D-PRNM had already been carried out at K-6. Without concerning with these situations, V&V were done over again completely in the application to 2F-1, although it was an independence work of a manufacturer's own free will.

The V&V carried out on the software of DPRNM for 2F-1 were guided by JEAG 4609.

The V&V team by the designers who are not regarding to the renewal design of 2 F-1 was composed, they reviewed the adjustment between the specifications of each software manufacture stages and the validity of the written contents were verified at each step of Ver.1 to Ver.5, and fitness in integrating hardware and software at Validation test. The results of V&V in 2F-1 will be able to use as the established sample at the time of application of the D-PRNM to other BWR plant, and it will contribute to the increase in efficiency of V&V works in the future.

8. Human-Machine Interface

The Human-Machine Interface of APRM unit and RBM unit are based on the same hardware that furnished a graphic display, 8 alterable function keys and 2 fixed function keys on its front panel. An operator can use these to select display and to change parameters. In usually, parameter changing is protected by key-lock switch and password doubly. When turn on the key-lock switch to changeable position and input correct password, the operator become to be able to change unit mode, setting parameters.

Usually the display turn off except the time to check the processing results and unit status. The processing results includes APRM value, TPM value, Core Flow values, LPRM values, and trips and alarms condition regarding these values. And unit status means self-test results, power supply monitors, trend list of self-test results and trip and operation, and parameter settings. In severance test, displays of trip test mode are useful. In these displays, the trip actions are checked using dummy signals inputted from the user interface. The sensitivity of neutron detector change as exposure, so gain adjustment needs every month. In the display of calibration, sensor gain adjustment factors are inputted from user interface manually or from data transmission automatically.

9. Consideration of Off Normal and Emergency Situations

As same as analog system, PRNM does not use any equipment like preamplifier in the reactor building. The detector signal connects to APRM unit through the sensor cable directly, so it is possible to check the detector from the main control room without going to the reactor building even in the accident where people cannot access to the reactor building. However, because the detector of PRNM is tended to measure the neutron in Power generating Range, it will be out of the sensitivity of the detector after the reactor shut down. If neutron flux is keeping enough high to be detected by PRNM, the system constitution of PRNM becomes convenient.

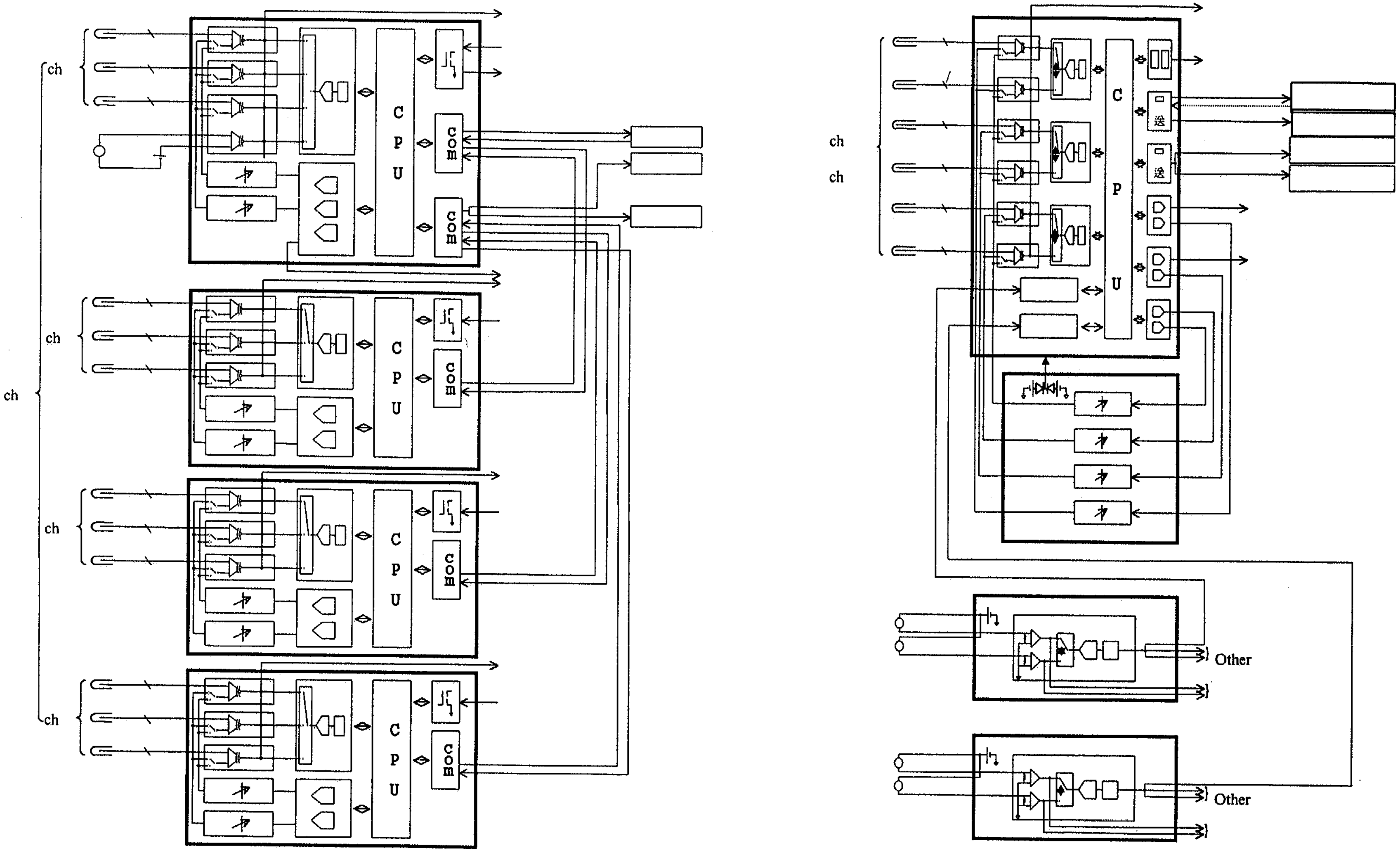
The digital PRNM can display the detector output signal in both current and percent. In the case of over flow in percent, the detector can be monitored in current if the neutron flux is inside the detector sensitivity range. The detector raw signal only converted from current to voltage is output to the external diagnostic system. This signal dose not through the processing by CPU module in APRM unit, so this signal shows the correct value even in the case of CPU failure. This constitution is one of actual diversity system.

Followings are the consideration in the display of PRNM for emergency situations.

- Operability without sense of incongruity in comparison with existing analog system
- Display contents that understand like intuition
- Unification of the bar graph scale in all display
- Constantly display of trip, rod block, unit mode, number of detector in operate, serious malfunction, and slight malfunction in fixed position
- Same function display in the same position
- Trace possibility of the cause using chronological order list of trips and alarms

10. Conclusion

D-PRNM equipment suitable for BWR was developed, employing K-6 actual results efficiently. Moreover, perfection of electric isolation characteristic to digital technology was pursued with the composition of the PRNM for BWR, and the design that esteemed reliability most was performed. Especially, functional isolation was also established, even adjusting with the existing analog system. The replace construction and site examination in 2 F-1 were completed with a margin even though the 13th periodical inspection was very short term, and everything is working well at present.



DCFData Communication Function

ICPSIon Chamber Power Supply

FLOWFLOW signal conversion

Figure 1, APRM unit block figure shoeing the comparison of ABWR and BWR

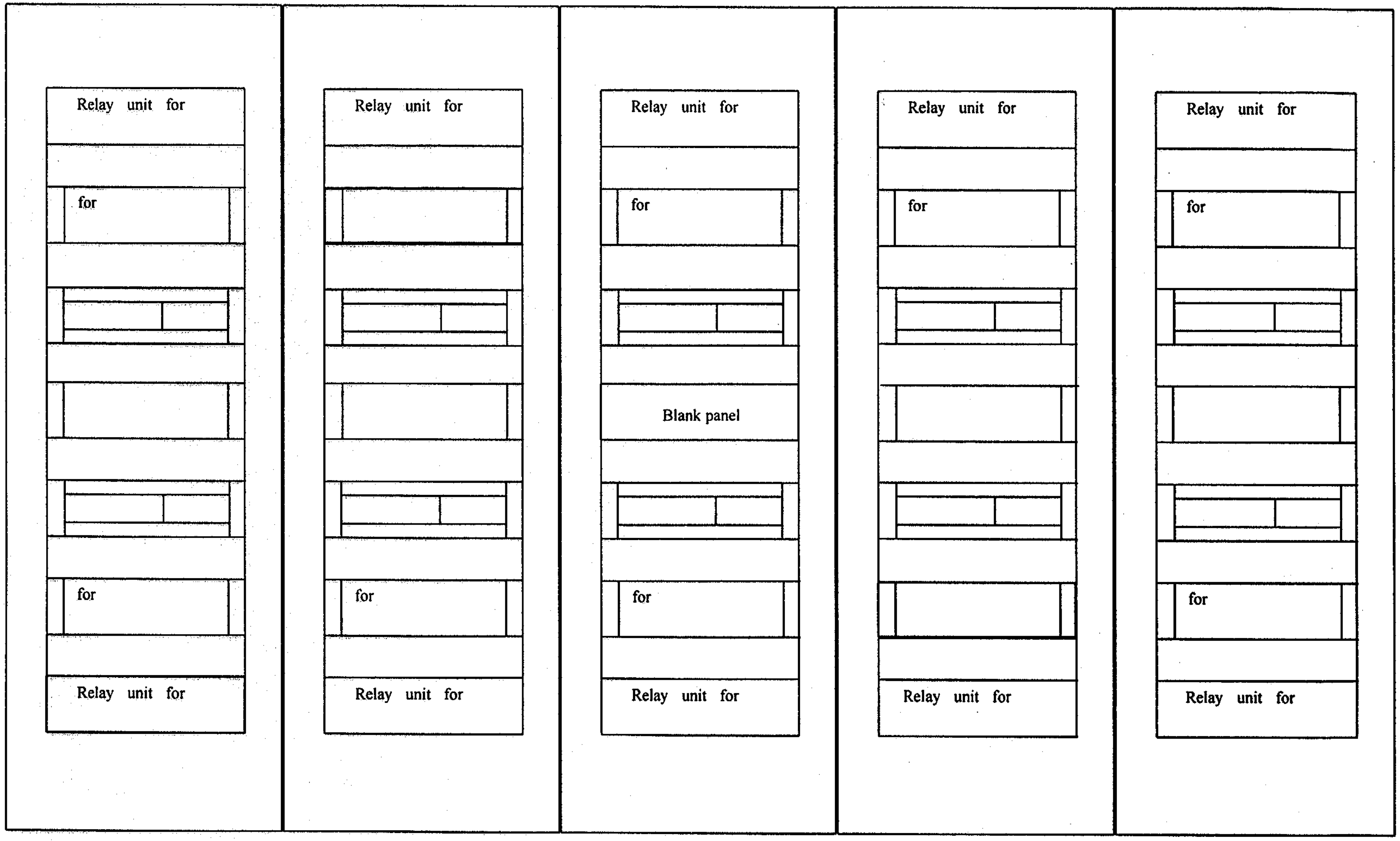
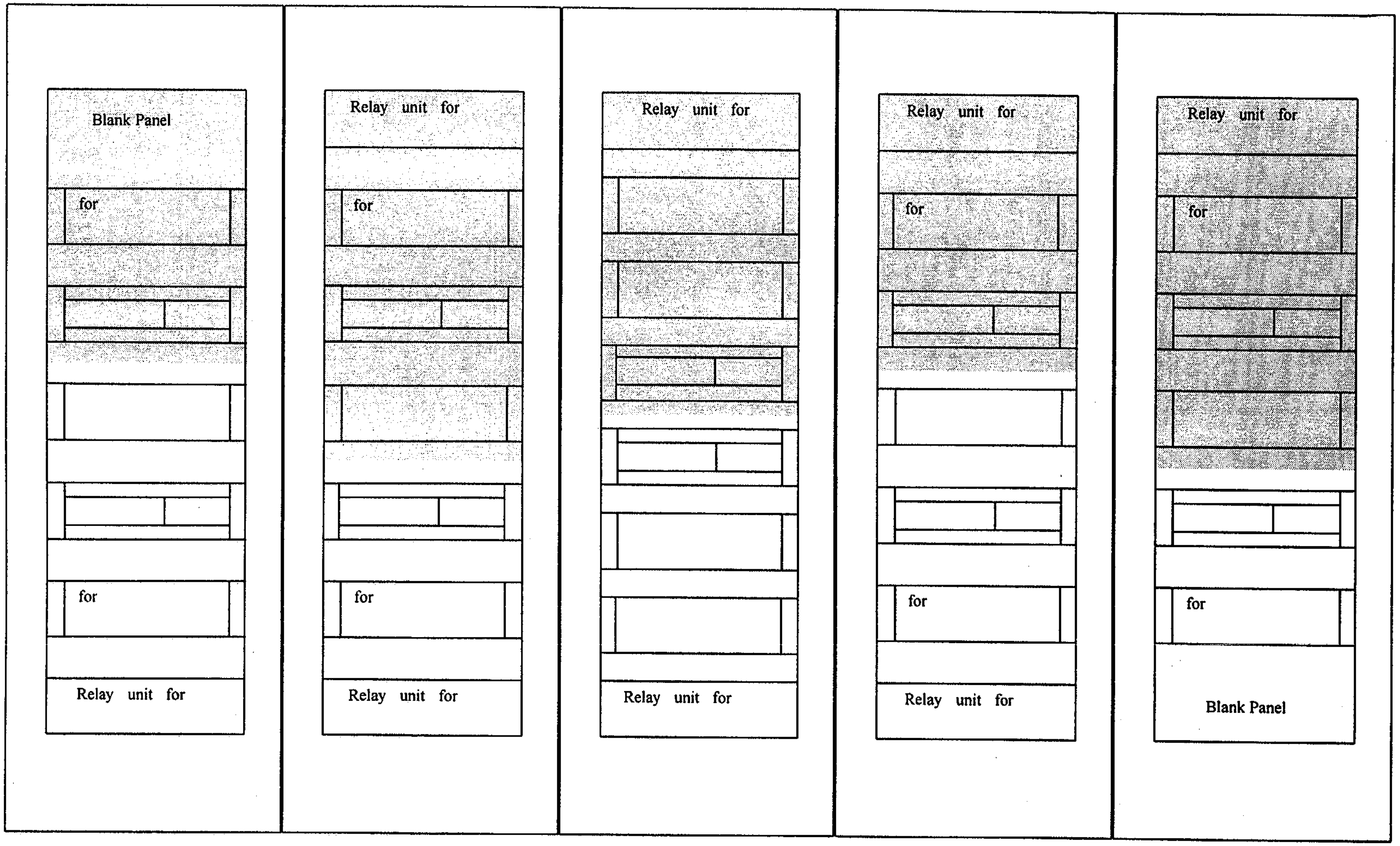


Figure 2, The appearance figure of the actual PRNM panel of 2F-1.



▨ Power Supply System A

□ Power Supply System B

Figure 3, The other appearance figure of the PRNM panel of 2F-1(as an idea only).

OPERATIONAL INFORMATION SYSTEMS AT KANUPP

TARIQ B. TAHIR
Karachi Nuclear Power Plant
P.O. Box 3183
Karachi-75400
Pakistan

Abstract

This paper describes the Operational Information (OI) Systems that are being installed at KANUPP. The main purpose of the OI Systems will be to improve the general man-machine interface, reduce the generation and handling of paper and automate many tasks currently performed manually. It is expected that this would result in a better awareness of the operators towards the state of the plant, reduce human errors and thereby increase the safety and availability of the plant. This paper describes one of the sub-systems of the OI Systems, the Process Information (PI) System which includes the Critical Function Monitoring.

1. INTRODUCTION

Karachi Nuclear Power Plant (KANUPP) is a 137 MWe CANDU PHWR. It is located at Paradise Point on the Arabian Sea coast 25 Km west of Karachi. The reactor has been generating power since October 1971. Till the end of 1998 the plant has produced over 9.2 billion units of electricity. The plant faced many challenges during its 28 years of operation mainly due to withdrawal of vendor support, but through indigenous efforts the plant continues to be operational till now.

The plant Control and Instrumentation is based on technology and design concepts of the mid 60's which have changed dramatically since then. The equipment is now obsolete and very difficult to maintain, so a major backfitting of the Computers and C&I equipment is being undertaken. With this backfitting it is proposed to incorporate an improved Information System. This system called the Operational Information (OI) Systems will be added to the original design to improve the man-machine interface in the Control Room and will also provide process information in other areas of the plant.

2. OPERATIONAL INFORMATION SYSTEMS

The OI Systems consists of 3 sub-systems: The Process Information (PI) System, the Equipment Information (EI) System and the Documentation Information (DI) System.

- Process Information (PI) System

  The PI System shall improve the man-machine interface by presenting to the operator the current process information in concentrated, relevant, simple and unambiguous form through colour visual displays.

- Documentation Information (DI) System

  The DI System shall make available to the operator all the operational documents that may be required for operating the plant. These documents consist of all technical reports, logs, test results, flowsheets and drawings related to plant operation.

- Equipment Information (EI) System

  The EI System shall help in managing the maintenance status of the plant equipment. It shall control the preparation, generation and issuance of the Work Authorizations and Work & Test Authorizations. The System shall generate the Isolation Tags and help the operator in the preparation of Orders-to-Operate (OTOs).

3. PRINCIPLES AND POLICIES OF THE OI SYSTEMS

The OI Systems shall be designed to follow these underlying principles:

- The OI Systems shall be not essential to the operation of the plant. Their failure during plant operation or their unavailability during shutdown shall not be a constraint to the plant operational program.

- The OI Systems will be very useful and convenient to the plant operational personnel and it is expected that in time they will become fairly dependent on them. Therefore they shall be designed to have a high reliability and availability factors so that they are operational most of the time.

- Certain functions of the existing centralized Process Computer System will be implemented in the PI System. However these functions are such that their unavailability for a certain time can be tolerated.

- The OI Systems shall not send any direct information or command to affect the plant process or control systems neither by itself nor under human command. But they can influence the plant by affecting the decisions made by the human operators, based on the information presented.

- The OI Systems shall generally ease the operation of the plant. They shall not introduce complex or lengthy operations nor in any way restrict or hinder normal plant operation.

- The OI Systems do not replace any existing process information equipment in the Control Room.

- The OI Systems should generally result in a reduction of paper and paper work. However all paper documents and manual procedures will still exist or remain possible, though less conveniently.

- Generally no new basic skill shall be required from the plant operators except typing skills. The introduction of colour VDUs will require an ability to discriminate between different colours.

- No extra work load shall be generated for the plant operators by the introduction of the OI Systems. Only the work methods may change. Over all the work load for the operator should decrease.

- The KANUPP environment will be considered non-hostile in context of the OI Systems. Whereas security techniques shall be incorporated they will be primarily to reduce data corruption and operator errors. Passwords and restrictory procedures shall be used only to prevent un-authorized access.

- The OI Systems shall be inherently designed to be easily modifiable.

- A consistent Man Machine Interface methodology with other Computerized Systems within KANUPP should be observed.

4. PROCESS INFORMATION (PI) SYSTEM

The PI System is a new addition to the original design of KANUPP. Its main purpose is to improve the plant availability by:

- increasing the probability of timely operator responses, by computerized analysis, concentrated and fast presentation of all relevant information at convenient locations.

- reducing the probability of human error or oversight in operator actions, by presenting the plant status in context of simplified logical views of systems relevant to the situation, as well as procedure guidance at convenient locations. The System also provides much expanded facilities to verify the validity of information.

- recording all significant events of the plant and thereby allowing the operator to retrieve and analyze the plant history readily and accurately in a concise and correlated form.

The Process Information System receives information about the plant, and presents it to the human beings, but it does not send any information or command back to affect the plant process or control systems directly. Similarly it has no role in communicating human decisions back to affect the plant processes.

The information about the plant collected and presented, and the locations and modes of presentation, are selected to suit the following broad classes of personnel and situations:

- Personnel in the Control Room directly responsible for operating the plant in normal and abnormal conditions.

- Personnel in the Technical Support Center, responsible for providing expert guidance to Control Room personnel in handling abnormal or emergency conditions.

- Personnel in the Technical Support Center responsible for long-term planning of operational policy and philosophy, requiring analysis of operational history also.

- Personnel in the Maintenance Engineers' Offices responsible for planning maintenance tasks.

5. CRITICAL FUNCTIONS

Nine important functions related to plant safety are declared as Critical Functions in KANUPP. These functions are:

- Primary Heat Transport System Integrity
- Primary System Heavy Water Inventory
- Moderator Inventory
- Reactor Core Cooling
- Booster Rod Cooling
- Reactor Power & Criticality
- Secondary Cooling
- Containment Integrity
- Radiological Emission

The Critical Functions can have normal, degraded or not computed states. At any time each Critical Function will be in one of the following possible states:

Normal State

In this state all the safety conditions of the function will be satisfied and the plant systems are operating normally.

Degraded State - I

In this state the operating parameters deviate from the normal range and safety action has been called or safety action has been actuated.

Degraded State – II

This state is reached when due to malfunction or otherwise, the automatic safety action have not actuated although the safety parameters have crossed their set points. This leads to a potentially unsafe condition. The operator must initiate emergency procedures to lessen the potential damage that may result due to this incident.

Not Computed

If for any reason a Critical Function cannot be computed it is declared to be in the Not Computed state.

The state of each of these Critical Functions are determined by a fixed set of complex algorithms based on a number of digital and analog parameters acquired from the process by the PI System. These algorithms are developed specially for KANUPP. The computation of these algorithms is performed continuously by the PI System Computers.

5. Conclusion

The OI Systems will be a significant change in the man-machine interface of the KANUPP Control Room. It is expected that after their implementation the operators will have more precise and relevant process information in a concise and concentrated form which will help them to make correct operational decisions.

Real World Simulator Training for NPP Operators and Management – When Off-Normal Becomes Normal

Dr. Richard P. Coe
School of Business Studies
The Richard Stockton College of New Jersey

Abstract

For nearly two decades since the accident at Three Mile Island Unit 2, full scope plant referenced simulators have become the primary vehicle to train, license, examine and test US NPP Operators and their Management on normal, off-normal and emergency conditions. It has also become common practice to install, test and train operators, engineers and maintenance technicians on plant modifications prior to their installation in the NPP. Simulators have become so technically sophisticated that instructors, operators and their management can conduct "What if" scenarios that can take them through catastrophic conditions that go far beyond plant design basis. Although licensed individually control room crews and their licensed management are trained and examined as a team. Crew members and other licensed personnel are often trained and in multiple positions where each team member is evaluated in the shift crew position that is required for their specific license. Senior Reactor Operators(SRO) are evaluated as both the Control Room SRO and the Shift Supervisor(SS). Reactor Operator(RO) are normally evaluated in a Balance of Plant(BOP) position as well as the RO position. The US Nuclear Regulatory Commission(NRC) has provided industry wide guidance through NUREG 1021, Operator Licensing Examination Standards for Power Reactors. In the sections dealing with licensed operator requalification the control room crew is evaluated as a team. A member can receive an individual failure but the emphasis is on overall team performance. If the team should fail then the team is removed from license duties until the unsatisfactory performance is remediated and the team can once again demonstrate satisfactory performance. Equally as important as technical capability is the ability of the team to communicate effectively among themselves and with groups outside the control room during plant normal, off-normal and emergency conditions. Licensed personnel are also trained and evaluated on communications, problem solving, stress management and teamwork. One week in every six week cycle is dedicated for crew training. Management is also brought into training to upgrade their technical and management skills. Crews and their management and instructors work closely together on the simulator in a variety of plant conditions. As their skills increase handling off-normal plant scenarios become normal. These skills transfer to their responsibilities in the plant. US NPPs are now recognized for their long, uninterrupted fuel cycle runs. These runs are also marked with minimal unplanned shutdowns and short duration refueling outages. As an example, Three Mile Island Unit I just shut down for a refueling outage after 618 days of continuous operation. This was TMIs' 3rd world record.

Introduction:

Full scope simulators have now become the primary method for training in many industries and organizations. Commercial and military aviation has long used simulation and/or simulators to train pilots both in normal, off-normal, and emergency conditions. They continue to be used in required refresher training as well as upgrade and promotional training. The US Nuclear Navy trains numerous submarine personnel on prototype trainers and has developed sophisticated simulation for advanced weapons and equipment. Other industries such as marine shipping, commercial transportation, energy transmission and private aviation use simulation in varying forms to train and qualify personnel. For nearly two decades since the accident at Three Mile Island Unit 2, full scope plant referenced simulators have become the primary vehicle to train, license, examine and test US NPP Operators and their Management in normal, off-normal and emergency conditions.

It has also become common practice to install, test and train operators, engineers, technicians and management on plant modification installed first on the simulator prior to their installation in the NPP. This process helps debug and fine tune a modification helping assure a smoother and more efficient installation in the plant. Many refueling outages have been shorter in duration due to this process. Crews who have experienced difficulty handling an off-normal or emergency condition can receive additional training until their proficiency becomes acceptable. If the condition warrants all of the crews in the NPP can receive additional "lessons learned" training to assure that a potential reoccurrence is handled effectively on any shift cycle. The US Commercial Nuclear Industry commonly shares "Industry Events" where plants of similar design can analyze and train accordingly. Simulators have become so technically sophisticated that instructors, operators and their management can conduct "what if" scenarios that can take them through catastrophic conditions that go far beyond plant design basis.

Technical Training:

The US Nuclear Regulatory Commission (NRC) have provided industry wide guidance through NUREG 1021, Operator Licensing Examination Standards for Power Reactors. The document provides the guidance for initial licensing activities as well as the requalification of licensed personnel. Each utility then develops, around the NRC guidance, local programs for training operators that often goes beyond regulatory requirement. GPU Nuclear, operator of the Oyster Creek NPP, has developed demanding licensed training programs that makes extensive use of it's plant referenced simulator.

<u>Control Room Operator (CRO)</u> **(Exhibit 1)**

Initial Training: This program provides the trainee with the knowledge and skills to enable him/her to assume the duties and responsibilities of a licensed Control Room Operator. The classroom phase consists of Boiling Water Reactor (BWR) Plant Fundamentals, Systems, and Procedures.

The BWR fundamentals portion of the program covers the following topics and lasts up to 15 weeks:

- Instrumentation and Control
- Electrical Fundamentals
- Mechanical Fundamentals
- Radiation Protection
- Chemistry
- Plant Materials
- Reactor Theory
- Thermodynamics, Heat Transfer, Fluid Flow
- BWR Operating Characteristics
- Mitigating Core Damage

The Oyster Creek Plant Systems lessons make up an additional 10 weeks of classroom training. The site-specific simulator is used throughout the systems courses to enhance training. A review of the following procedures, documents and skills provide the remaining 5 weeks.

- Administrative Procedures
- General Plant Operating Procedures
- Plant Systems Procedures
- Abnormal Event Operating Procedures
- System Diagnostic and Restoration Procedures
- Symptom Based Emergency Operating Procedures
- Maintenance and Surveillance Procedures
- Emergency Plan Procedures
- Operating License and Technical specifications
- Black Start Plan
- Spill Prevention Controls and Countermeasures
- Team Skills
- Work Practices
- Applicable SOERS

The on-the-job training phase requires a minimum of 13 weeks on shift as a Reactor Operator trainee during which time the Control Room Operator Qualification Standards are to be completed. Oral exams are administered towards the completion of the OJT phase and Job Performance Measures (JPMs) are administered during the systems phase of training.

Prior to participation in the site-specific Simulator Training phase, the trainee attends a Team Skills Communication Course. Approximately eight weeks are dedicated to training on the site-specific simulator. Simulator training includes the following plant evolutions:

- Cold Startup to Full Power
- Hot Startup to POAH with Heatup Rate Established
- Feed Pump Startup
- Turbine Roll and Generator Synchronization
- Plant Shutdown to Cold Condition
- Plant Shutdown to Hot Standby
- Startup Certification
- 2000-ABN-3200 Abnormal Procedures

- 2000-OPS-3024 System Diagnostic and Restoration
- Emergency Operating Procedures – Introduction
- Emergency Operating Procedures – Proficiency Training
- Casualty Drills

The Oyster Creek Fundamentals Final Examination must be successfully passed prior to sitting for the NRC-administered Generic Fundamentals Examination Section (GFES).

Continuing Training: The continuing training program consists of classroom instruction, in-plant training, and task performance evaluations (JPMs). It is based on a two-year training and requalification cycle. The biennial re-qualification process involves a comprehensive written exam and the annual operating exam consisting of simulator and JPMs. Classroom instruction includes topics determined by the job-specific task analysis as well as the following:

- Training Requests
- Plant Modifications
- Plant and Industry Operating Experiences
- Regulatory Changes
- Plant Procedure Changes
- Management Discussion Periods
- Program Content Committee
- Safety Training Needs
- Fire Brigade Training Requirements
- Emergency Plan Training Requirements

Continuing training may also use or repeat initial training lessons and OJT items. In-plant training provides hands-on training to maintain proficiency on important tasks and/or infrequently operated systems and equipment. Continuing training in-plant evolutions are based on the individual needs of operating shifts, planned evolutions, identified operating deficiencies, availability of plant systems, equipment and personnel, or other criteria determined by the Plant Operations Director.

Senior Reactor Operator (SRO) Exhibit 2

Initial Training: The classroom portion consists of approximately 184 hours of BWR plant fundamentals, 250 hours of systems and 112 hours of procedures training.
Fundamentals Training includes:

- Reactor Theory
- Thermodynamics, Heat Transfer, Fluid Flow
- Transient and Accident Analysis
- Radiation Protection
- BWR Chemistry/Materials
- Mitigating Core Damage

Unless successfully completed earlier, SRO license candidates must pass the NRC administered generic fundamentals examination. Personnel without a reactor operator's license at Oyster Creek participate in a 250-hour course on plant systems. Personnel with a reactor operator's license at

Oyster Creek are given a minimum of 100 hours of instructor guided study time and three to four exams covering all the plant systems in lieu of a formal course. Procedure Training includes:

- Administrative Procedures
- General Plant Operating Procedures
- Plant Systems Procedures
- Abnormal Event Operating Procedures
- System Diagnostic and Restoration Procedures
- Symptom Based Emergency Operating Procedures
- Emergency Plan Implementing Procedures
- Operating License and Technical Specifications
- New Jersey Pollution Discharge Elimination System (NJPDES)

The on-the-job portion of the training program requires:

- A minimum of 520 hours on shift as a senior reactor operator trainee.
- The completion of Control Room Operator Practical Factors (imbedded in the Group Operating Supervisor Qualification Standard).
- The completion of the Group Operating Supervisor Qualification Standard.
- The performance of five reactivity manipulations at Oyster Creek in accordance with NUREG 1021.

Simulator training is conducted on the Oyster Creek site-specific simulator in three phases lasting six weeks. Phase I consists of approximately 100 hours of training on the following plant evolutions:

- Cold Startup to Full Power
- Establishing Plant Heat up
- Feed Pump Startup
- Turbine Roll and Generator Synchronization
- Plant Shutdown to Cold Condition
- Plant Shutdown to Hot Standby
- Startup Certification

Phase II consists of approximately 60 hours of training to include as a minimum the following:

- Abnormal Procedures
- Systems Diagnostic and Restoration Procedures

Continuing Training: The continuing training program consists of classroom instruction, in-plant training and task performance evaluations (JPMs). It is based on a two-year training and re-qualification cycle. The biennial re-qualification process involves a comprehensive written exam and the annual operating exam consisting of simulator and JPMs. Classroom instruction includes topics determined by the job specific task analysis as well as the following:

- Training Requests
- Plant Modifications
- Plant and Industry Operating Experiences

- Regulator Changes
- Plant Procedure Changes
- Management Discussion Periods
- Program Content Committee
- Safety Training Needs
- Fire Brigade Training Requirements
- Emergency Plan Training Requirements

Continuing training may also use or repeat initial training lessons and OJT items. In-plant training provides hands-on training to maintain proficiency on important tasks and/or infrequently operated systems and equipment. Continuing training in-plant evolutions are based on the individual needs of operating shifts, planned evolutions, identified operating deficiencies, availability of plant systems, equipment and personnel or other criteria determined by the Plant Operations Director.

Shift Supervisor (SS) – Shift Manager (SM) Exhibit 3

Initial Training: This program consists of the following elements:

- Completion of the Oyster Creek Licensed SRO Training Program
- Formal Classroom Training on a variety of management topics
- Shift Supervisor On-the-Job Training
- Plant/Department Interviews
- Shift Supervisor Candidate Simulator Evaluations

The initial training program is to be completed prior to independent assignment to the position of shift manager. Shift Supervisors promoted to the position are required to attend the INPO Professional Development Seminar within the first year of assignment to the position.

The Licensed SRO training program provides candidates with many specific knowledge and performance skills required as a Shift Manager. Classroom training requires satisfactory completion of the following courses:

- Industrial Safety
- Observation Techniques
- Safety Review Process Training
- Human Resources – GPU System Fitness-for-Duty Training
- Management Development – Teamwork and Leadership
- Management Development – Supervisory Development
- Human Performance Enhancement System Evaluator Training

On-the-job training consists of the following:

- Interdepartmental Evolutions
- Personnel Performance Evaluation
- Modification Package Review
- Event Documentation and Reporting
- Eighty hours of shift time as a SS Trainee

- Licensed Operator Requalification Simulator Evaluation as SS

The interviews consist of face-to-face discussions with management or subject matter experts covering a variety of subject areas and situations. The purpose of the interviews is to enhance the candidate's understanding of specific operating evolutions, operating philosophy and procedural requirements.

Plant Operations, Training Management and Instructors conduct simulator evaluations during the candidate's annual SRO simulator exam. This evaluation is done with the candidate in the role of SS.

Continuing Training: The continuing training for Shift Supervisors consists of attendance with their crew to the Licensed Operator Re-qualification training program and any other applicable required training (e.g., GET, E-Plan, Fire Brigade). Also included in continuing training are assignments for the enhancement of management and leadership skills, generic professional development modules and any additional technical training deemed appropriate by operations management.

Professional Development Programs: Additional programs are made available to strengthen supervisors' leadership, analytical and teamwork skills. The following are examples of developmental activities:

- Day-to-day Coaching by Operations Management
- Attendance at INPO Shift Managers Seminar
- The Management Tour Program
- Attendance at specific management development courses
- Assignments as INPO Peer Evaluators
- Off-site Seminars and College Courses
- Visits to other NPP's
- Adjunct Instructor and other rotational assignments

Further personnel development on how to improve human performance has been an integral part of the following training development modules:

- Vision Training for handling the deregulated utility environment
- Responsible Decision-Making (RDM) Training
- Interaction Management Skills (IMS) Program
- Managing Multiple Projects
- INPO Shift Managers Course
- Positive Reinforcement Skills Course
- Quality, Validation and Verification Training
- Steps Towards Excellence Management Meetings
- Event Free Operation Program

<u>Shift Technical Advisor (STA)</u> Exhibit 4

Initial Training: The initial program establishes the candidate's understanding of the concepts of safe and efficient plant operation. The classroom portion includes fundamentals, systems, procedures, and integrated plant operations.

It is based on the STA job analysis and meets the requirements of INPO 90-003, Guidelines for the Training and Qualification of Shift Technical Advisors. The initial program takes twelve months to complete and consists of classroom, self-study, simulator and on-the-job training.

The fundamentals training not only builds a strong foundation for understanding nuclear power plant operation but also complements the candidate's engineering background by presenting challenging applications of course material that is normally not emphasized during college education.
The following areas are covered:

- Reactor Physics
- Reactor Design
- Heat Transfer, Fluid Flow, and Thermodynamics
- Instrumentation and Control
- Electrical/Electronic Theory and Power Distribution
- Chemistry, Corrosion, and Materials
- Radiation Control
- Technical Specifications and other selected licensing basis documents

The integrated plant operations training section combines theory and systems training with the duties and responsibilities of the STA during normal and off-normal operating conditions. The following topics are covered during this phase of training:

- Oyster Creek Safety Analysis
- Plant Operations – BWR Operating Characteristics
- Plant performance monitoring and evaluation
- Critical functions approach to plant monitoring
- Transient Analysis
- Problem Analysis and Decision Making (diagnostics)
- STA Duties and Responsibilities
- Team Skills
- Emergency Plan

The on-the-job training portion of the program consists of pre-selected exercises, watch standing and system checkouts that involve observation and participation by the candidate in job-related activities. The STA Qualification Standard is completed during this phase of training.

Simulator training provides the STA trainee with real time plant transient experience and a final operational evaluation. Specifically, the STA will be evaluated on the ability to apply a "Critical Safety Functions" approach to power plant control during various NPP operating modes as follows:

- Reactor and Plant Startup and Shut Down
- Power Operations
- Transient Response

- Hot Shutdown
- Plant Cool Down

At the end of the initial program, there are approximately two weeks designated for instructor-guided self-study. The written comprehensive exam and the final oral board are normally administered during this time period.

Continuing Training: The Shift Technical Advisor (STA) Re-qualification Training Program presents a range of material necessary for the STA to maintain and improve the knowledge and technical skills required to perform the STA function in an on-shift environment. In addition to attendance in the Licensed Operator Re-qualification Program, the STA's training is augmented with selected topics, such as:

- Industry Events
- Critical Safety Functions
- Transient/Accident Analysis
- Integrated Plant Response
- STA Duties and Responsibilities
- Diagnostic Skills
- Engineering Codes and Standards
- STA Administration Requirements
- Advanced Fundamentals
- Basic Safety Principles
- Codes and Standards
- Administrative Responsibilities
- Personal Computer Topics

The annual operating examination is developed from the tasks derived from systematic analysis of reactor operator or senior reactor operator duties performed at Oyster Creek. The test is administered in two parts:

- An individual plant walk-through exam using Job performance Measures (JPMs).
- A site-specific simulator exam (individual and crew).

An accelerated re-qualification program is designed for students who demonstrate deficiencies in examinations or performance or who are temporarily withdrawn from the re-qualification program.

Crew and Shift Team Training:

It has become evident to many organizations that the new workplace needs and values change and adaptation. Pressures abound for organizations to search for new ways of operating for higher productivity, total quality and service, customer satisfaction and better quality of working life. Recent developments have shown the importance of aggressively exploring the full potential of group synergy as a crucial organizational resource. Highly motivated groups effectively supported and managed properly can be the best strategy any organization has in adapting to and achieving long term success in a challenging environment. Groups and their management are training in:

- Group Development and Effectiveness
- Group Dynamics, Membership and Leadership
- Group Diversity and Interactions
- Group Decision Making and Commitment
- Problem Solving in a group
- Group Communication and Stress
- Empowerment

Managing a highly effective workgroup presents a leadership challenge to traditional management. Leaders need to use more of their interpersonal aspects of managing as opposed to formal autocratic authority. Managers in the training of their groups also learn and develop skills to:

- Achieve positive influence on group behavior
- Effectively manage conflict
- Effectively negotiate agreement and commitment by groups
- Effectively manage stress both workplace and individual as it affects the groups

Managers must also develop skills in dealing with outsiders, peers, superiors and other higher level personnel. Unique training is also provided on the empowerment of groups and individuals. This skill is crucial to organizational productivity and effectiveness since empowered groups tend to be more willing to make decisions, take more conservative risks and actions to get their jobs done. Managers must also learn that as groups become more powerful it does not mean that the manager becomes less powerful or responsible.

Management Training:

Many researchers and organizations agree that the most frequently used skills of effective manages are:

- Verbal communication (including listening)
- Managing time and stress
- Managing individual decisions
- Recognizing, defining and solving problems
- Motivating and influencing others
- Delegating
- Setting goals and articulating a vision
- Self-awareness
- Team building
- Managing conflict

Key to any organizational success is effective leadership. The skills needed to manage successfully in a dynamic changing environment are as equally important as the technical skills needed to run an NPP safely and efficiently. Most NPPs are providing management specific training to supervisors, managers and potential managers. Control room supervisors and shift managers are routinely trained in:

- Leadership
- Managing Change and Innovation
- Motivation
- Communication
- Interpersonal Skills
- Problem Solving
- Team Building – Group Effectiveness
- Managing Stress
- Ethics and Professionalism

Manages are given assessments to determine their individual management style(s). The results determine if the manager is task-oriented, people-oriented or team-oriented.

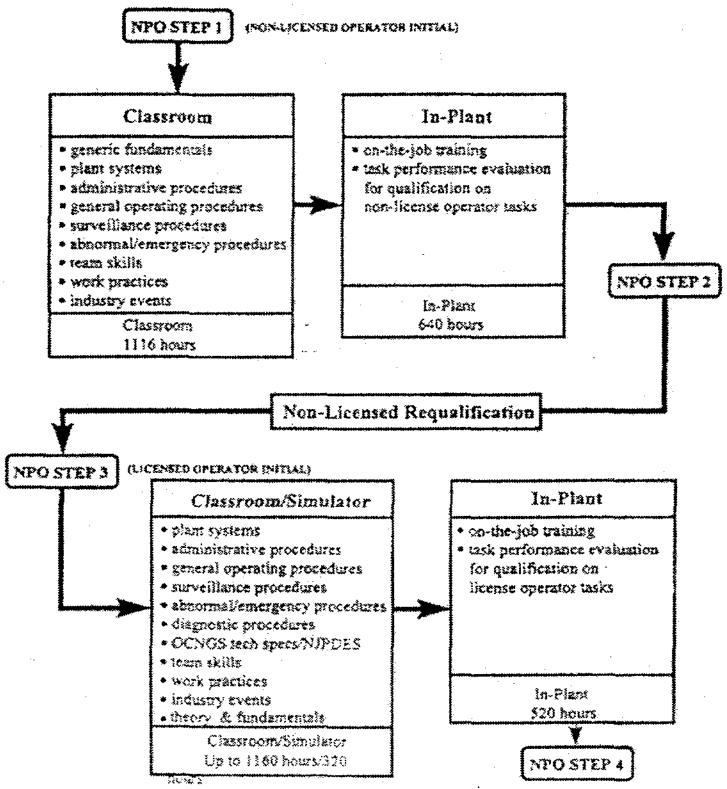
Training is given in gaining skills in the strengths and uses of each of these styles. Training is also given in situational leadership and how it applies to the maturity and readiness of the group to be empowered. Communication skills and active listening are taught along with interpersonal skills and styles. Effective and creative problem solving is given both to managers and groups together. Various models are used to foster innovative and rational problem solutions in a rapid yet effective way. Managers are also given an in-depth exposure to managing groups effectively. Group dynamics, decision making and effectiveness are part of a core program. This includes managing change and stress effectively. Finally since leaders and managers are expected to be models of ethical behavior and professionalism, training is given on this process and how it relates to working in a legal and regulated environment.

Summary and Conclusions:

Simulators have made the difference in the upgrade of skills in operators of US NPP's. Control room crews and their management and instructors work closely together on the simulator in a variety of plant conditions. As their skills increase, handling off-normal plant scenarios becomes normal. As these skills transfer to their responsibilities in the plant we are seeing less human mistakes and a greater increase in error free human performance. US NPPs are now recognized for their long uninterrupted fuel cycle runs. These runs are also marked with minimal unplanned power reductions and shutdowns as well as short duration refueling outages. Other performance indicators such as lower person-rem exposures, lower lost time accident rates, reduced radwaste generation and contaminated areas are and continue to be showing positive trends. Proper training along with advanced technology training equipment such as simulators are making the difference. As we move into the new millenium NPP operators and their managers will become the best-trained professionals in the world. Working on even more sophisticated full scope and part task simulators plant personnel will be handling off-normal and emergency situations as if they were **routine and normal.**

NUCLEAR PLANT OPERATOR (NPO) TRAINING PROGRAM

Flowchart of Training and Qualification Sequence


NPO STEP 1
(NON-LICENSED OPERATOR INITIAL)
Classroom
• generic fundamentals
• plant systems
• administrative procedures
• general operating procedures
• surveillance procedures
• abnormal/emergency procedures
• team skills
• work practices
• industry events
Classroom
1116 hours
In-Plant
• on-the-job training
• task performance evaluation for qualification on non-license operator tasks
In-Plant
640 hours
NPO STEP 2
Non-Licensed Requalification
NPO STEP 3
(LICENSED OPERATOR INITIAL)
Classroom/Simulator
• plant systems
• administrative procedures
• general operating procedures
• surveillance procedures
• abnormal/emergency procedures
• diagnostic procedures
• OCNGS tech specs/NJPDES
• team skills
• work practices
• industry events
• theory & fundamentals
Classroom/Simulator
Up to 1160 hours/320
In-Plant
• on-the-job training
• task performance evaluation for qualification on license operator tasks
In-Plant
520 hours
NPO STEP 4

Note: Step 4 attained after ~ 1 year in the LCRO position.

Exhibit 1

SENIOR REACTOR OPERATOR INITIAL TRAINING PROGRAM

Flowchart of Training and Qualification Sequence

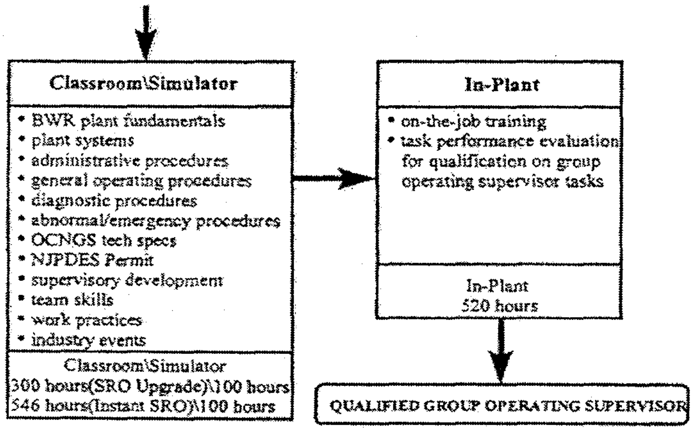

Classroom\Simulator
• BWR plant fundamentals
• plant systems
• administrative procedures
• general operating procedures
• diagnostic procedures
• abnormal/emergency procedures
• OCNGS tech specs
• NJPDES Permit
• supervisory development
• team skills
• work practices
• industry events
Classroom\Simulator
300 hours(SRO Upgrade)\100 hours
546 hours(Instant SRO)\100 hours
In-Plant
• on-the-job training
• task performance evaluation for qualification on group operating supervisor tasks
In-Plant
520 hours
QUALIFIED GROUP OPERATING SUPERVISOR

Exhibit 2

SHIFT SUPERVISOR TRAINING PROGRAM

Flowchart of Training and Qualification Sequence

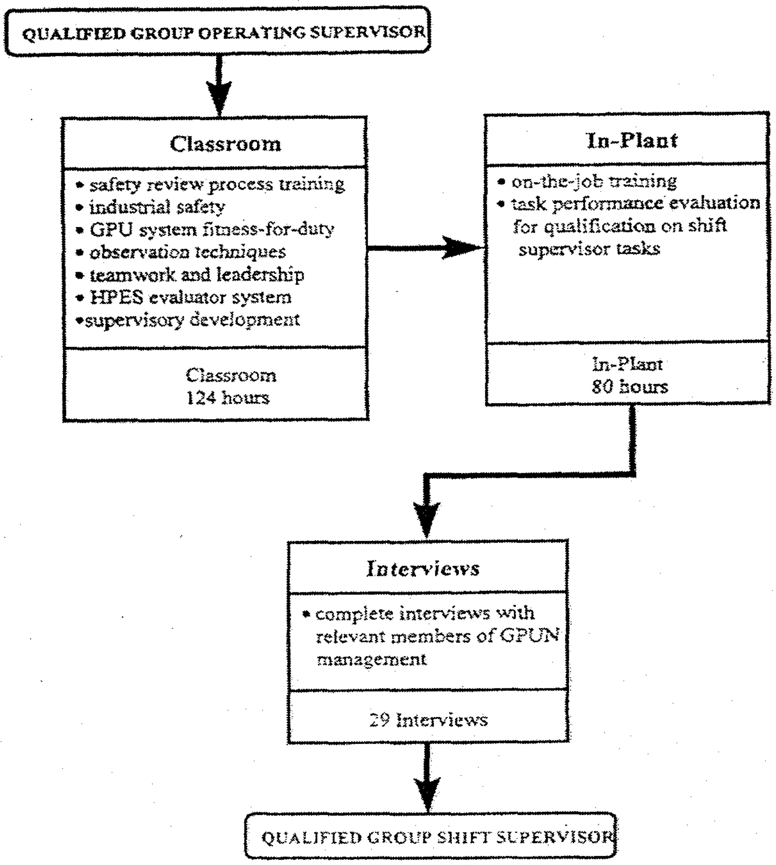

QUALIFIED GROUP OPERATING SUPERVISOR
Classroom
• safety review process training
• industrial safety
• GPU system fitness-for-duty
• observation techniques
• teamwork and leadership
• HPES evaluator system
•supervisory development
Classroom
124 hours
In-Plant
• on-the-job training
• task performance evaluation for qualification on shift supervisor tasks
In-Plant
80 hours
Interviews
• complete interviews with relevant members of GPUN management
29 Interviews
QUALIFIED GROUP SHIFT SUPERVISOR

Exhibit 3

SHIFT TECHNICAL ADVISOR INITIAL TRAINING PROGRAM

Flowchart of Training and Qualification Sequence

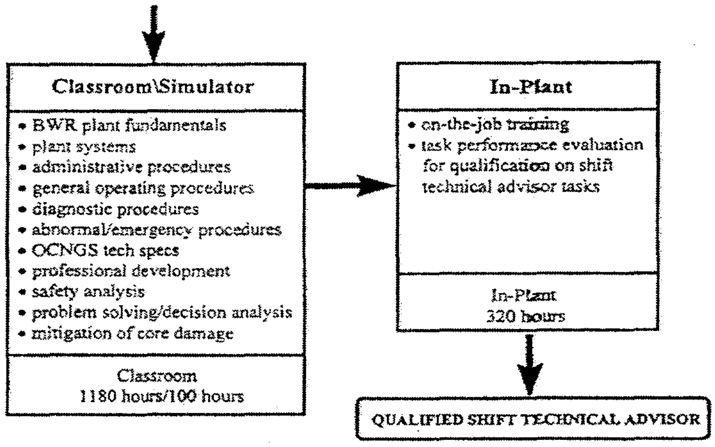

Classroom\Simulator
• BWR plant fundamentals
• plant systems
• administrative procedures
• general operating procedures
• diagnostic procedures
• abnormal/emergency procedures
• OCNGS tech specs
• professional development
• safety analysis
• problem solving/decision analysis
• mitigation of core damage
Classroom
1180 hours/100 hours
In-Plant
• on-the-job training
• task performance evaluation for qualification on shift technical advisor tasks
In-Plant
320 hours
QUALIFIED SHIFT TECHNICAL ADVISOR

Exhibit 4

Distributed GOMS: An Application of GOMS to EOP

Daihwan Min[1], Sanghoe Koo[2], Yun-Hyung Chung[3], & Bokryeul Kim[4]
[1], [2] Dept. of MIS, Korea University,
Jochiwon-Eup, Choongnam, 339-700, South Korea
[1] mismdh@tiger.korea.ac.kr
[2] shkoo@tiger.korea.ac.kr
[3], [4] Korea Institute of Nuclear Safety
19 Guseong-Dong Yuseong-Gu, Taejon, 305-338, South Korea
[3] k078cyh@kins.re.kr
[4] k060kbr@ kins.re.kr

ABSTRACT

This study presents an evaluation technique named DGOMS that is an extension from GOMS. Also, the study shows a sample case that is an application of DGOMS to a specific task at the control room of a nuclear power plant. The use of DGOMS enables (1) to model not only individual user's interface with technical subsystems but also their communications collectively, (2) to analyze group performance as well as individual performance in terms of execution time, and (3) to compare mental workloads among multiple users.

1. INTRODUCTION

In cases of large-scale complex systems such as Nuclear Power Plant(NPP), it takes many years to learn how to control such complicated systems. Even after many years of experiences they make mistakes, which may result in critical situations. Especially, the interface between humans and technical subsystems has a great impact on the reliability and safety. The purpose of this study is to develop a technique for evaluating HMI(Human-Machine Interface) in main control rooms of NPPs in Korea.

From the past literature, we can find two kinds of HMI evaluation techniques, i.e., analytical and experimental. Analytical techniques do not involve actual human users during evaluation. Instead, it builds models of human-machine interfaces and analyzes the models to predict various aspects such as execution time or cognitive workloads. On the other hand, experimental techniques involve actual human users to measure performances such as execution time or manipulation errors. Thus, experimental techniques cost a lot more time and efforts than analytical techniques.

As an analytic technique, GOMS (Goals, Operators, Methods and Selection rules) has been widely used in the past in order to analyze an individual's interface to a technical subsystem. More specifically, GOMS models a task as a hierarchical tree consisting of a sequence of primitive operators[6]. The tree model is used to predict the time to learn the procedural knowledge required in order to operate a given technical subsystem and to predict the execution time from the estimates of primitive operators. The model is also used to analyze mental workloads required to perform a specific task.

A few GOMS techniques have been suggested and applied to various areas including NPPs. Endestad and Meyer[3] have shown the usefulness of GOMS by evaluating two technical systems: ISACS-I(Integrated Surveillance And Control System-I) and COPMA-II(Computerized OPerational MAnual-II). As a result, they have shortened the hours for performing tasks in a main control room and reduced engineers' mental workload.

However, one outstanding limitation of past GOMS techniques is that they are applicable only to analyzing individuals, but not appropriate for analyzing group's interaction with multiple technical systems. They do not consider the allocation of sub-tasks and the communications among humans that are important in complex systems.

In real NPP control rooms, tasks are performed by a group of engineers including SRO(shift supervisor), RO(reactor operator), TO(turbine operator), and EO(electric operator). They work collaboratively to accomplish common goals. While a group task is performed, there exist inter-dependencies between operations by individual engineers. For examples, EO's operation sequence may vary according to the information given by TO. An SRO usually monitors overall situations and makes appropriate decisions while he observes every engineers' works to estimate current progress and to determine the following operation sequences.

For such systems, we need a way to evaluate the interface between the human group and the technical sub-systems by considering the inter-dependencies among engineers as well as the relations between sub-tasks within an individual engineer [4].

With the consideration of task allocation and communications among a group of engineers, we have developed a new procedure called DGOMS (Distributed GOMS) which is an extension from GOMS [8].

This paper presents the procedure of the DGOMS technique, compares the previous GOMS techniques with DGOMS, and applies DGOMS to an EOP (Emergency Operation Procedure) task at a NPP control room.

2. DGOMS PROCEDURE

The DGOMS procedure is as follows:

[Step 1] Build a hierarchical tree model for the whole task: At this step, we utilize the NGOMSL (Natural GOMS Language) technique, on the assumption that the whole task is performed by an individual even though the whole task demands much more cognitive capacities than an individual's. We need to decompose the task into subtasks until all the subtasks at leaf nodes can be assigned to an individual.

[Step 2] Allocate each subtask to an individual in the group: If the Step 1 has been done correctly, it would be evident to allocate the subtasks at the leaf nodes. For the other subtasks at the intermediate nodes and the root node, we need to consider who is in charge of that subtask covering all its decomposed subtasks.

[Step 3] Collect subtasks assigned for each individual: Considering sequential relations among subtasks within each individual, we arrange all the subtasks for each individual.

[Step 4] Build a PERT chart for the whole task: Now we need to connect subtasks among individuals by adding communication operators. There are various situations when communications are necessary. A typical situation is when a subtask X is performed by one person and the subsequent subtask Y performed by another person.

[Step 5] For each subtask at the leaf nodes in Step 1, build a model by applying either NGOMSL or CPM-GOMS (Cognitive-Perceptual-Motor GOMS) technique according to the characteristics of the subtask: If the subtask allows parallel execution of primitive operators, we can apply CPM-GOMS. Otherwise, we use NGOMSL.

[Step 6] Perform an analysis for each GOMS model built in Step 5 at the individual level: We utilize again either NGOMSL or CPM-GOMS for analyzing learning time, execution time, and mental workload.

[Step 7] Perform an analysis for the whole task at the group level: For analyzing execution time, fine the critical path from the PERT chart built in Step 4. For analyzing learning time and mental workload, combine the results from Step 6.

3. COMPARISON OF DGOMS WITH GOMS

DGOMS have different characteristics from previous GOMS techniques such as CMN-GOMS[1], NGOMSL, and CPM-GOMS, as shown in Table 1.

First, the level of analysis by all the previous GOMS is at the individual level. Although those techniques are adequate for analyzing individual's cognitive process while using a technical subsystem, they are not applicable to situations where a group works together for a common goal by controlling a large-scale technical system. In contrast, DGOMS analyzes the group task by combining communications among individuals with models resulting from the application of previous GOMS techniques. Steps 1-4 and 7 are for the analysis at the group level, and Steps 5-6 are for the analysis at the individual level.

Table 1: Comparison of DGOMS with previous GOMS

	Previous GOMS techniques			DGOMS
	CMN-GOMS[2]	NGOMSL [6]	CPM-GOMS [5]	
level of analysis	individual	individual	individual	group
model structure	tree (sequential)	tree (sequential)	PERT, (parallel)	tree, PERT, (parallel)
primitive operators	external operators, internal operators	external operators, internal operators	external operators, internal operators	external operators, internal operators, communication operators
performance variables	execution time	execution time, learning time, consistency, mental workload	execution time	execution time, learning time, cognitive load, distribution of execution time, balance in workload balance in mental workload

Second, in terms of model structure both CMN-GOMS and NGOMSL build a tree model to represent sequential relations among operators, while CPM-GOMS and DGOMS build a PERT model to show parallel relations among operators. However, there is a difference between CPM-GOMS and DGOMS. CPM-GOMS recognizes parallelism among cognitive,

[1] This represents the first GOMS technique presented by Card, Moran, and Newell [2].

perceptual, and motor operators within an individual. In contrast, DGOMS admits socially distributed cognition among individuals as well as parallelism within an individual. DGOMS also build a tree model in Step 1.

Third, previous GOMS have two types of operators, i.e., external operators and internal operators. External operators are composed of perceptual operators and motor operators, and internal operators consist of control operators, memory operators, and analyst-defined operators. DGOMS has another additional type of operators called communication operators as well as external and internal operators. Communication operators are necessary when two persons exchange information to perform parts of the given group task.

Fourth, CMN-GOMS and CPM-GOMS evaluate execution time of an individual as a performance variable, and NGOMSL measures learning time, consistency among methods, and mental workload including execution time. DGOMS measures execution time, mental workload, learning time, and distribution of execution time between CPM operators and communication operators at the individual level. At the group level DGOMS calculates execution time after finding the critical path, and checks the balances in workload and in mental workload among individuals.

4. DGOMS APPLICATION

Table 2: Task allocation to engineers

Engineer	Action description	Task Id.
SRO	Detect an emergency situation	A1
SRO	AGO Verify reactor trip	A2
SRO	Decide: If <reactor trip> then AGO Carry out immediate actions	A3
SRO	RGA	A4
	Section Rules for AGO Verify reactor trip	S(A2)
RO	Decide: if <rod bottom light - lit> then RGA	A21
RO	Decide: if <reactor trip and bypass breakers - open> then RGA	A22
RO	Decide: if <rod position indicators – at zero> then RGA	A23
RO	Decide: if <neutron flux - decreasing> then RGA	A24
	Method to AGO Carry out immediate actions	M(A3)
SRO	AGO Check response to power generation	A31
EO	Verify power to AC emergency buses	A32
RO	Check RCS inventory	A33
RO	Check RCS pressure	A34
RO	Verify SI flow	A35
SRO	AGO Verify RCS temperature - cooled	A36
EO	Verify containment radiation - normal	A37
EO	Verify containment pressure - normal	A38
	RGA	A39
	M to AGO Check response to power generation	M(A31)
RO & TO	Manually trip reactor	A311
RO	Check if reactor output - decreasing	A312
RO	Check if every rod is at the bottom	A313
	RGA	A314

In order to examine the applicability of DGOMS, we have selected an EOP task called 'EOP-01' from a NPP at YoungKwang in Korea and applied the DGOMS procedure. This task should be carried out right away when there is any symptom of reactor trip.

[Step 1 & Step 2] The original description for 'EOP-01' task explains step by step actions for the whole group without specifying who is doing which action. First, we have rearranged this description without further decomposition. Then, we have identified who is in charge for each subtask of 'EOP-01'. The result of the first two steps is shown in Table 2.

The first column shows the person in charge of the corresponding task the third column shows task identification number in order to use in the following steps. If one action is done by RO, TO, or EO alone, we need not decompose the task any further at this point. However, if one action is carried out by two engineers or SRO is in charge of an action, the evaluator needs to judge whether that action needs further decomposition or not. For example, we do not decompose A311 since it is carried out by RO & TO together simultaneously. In contrast, we need to decompose A36, because this action is to done more than two engineers. Table 3 shows the decomposition of A36.

Table 3: Decomposition of A36

Engineer	Action description	Task Id.
	M to AGO Verify RCS temperature - cooled	M(A36)
TO	Keep SG levels	A361
RO	Keep RCS T_{avg} at 292~299°C	A362
TO	Keep RCS pressure in the range of 77~86kg/cm^{2}A	A363
	RGA	A364

[Step 3] This step is straightforward. We just regroup actions for each engineer considering precedence. If one engineer is in charge of an action and performs its subtasks, we separate the action into the beginning part and the ending part. For example, SRO is in charge of A3 and two subtasks A31 and A36. So, A3 has its beginning and ending part. Table 4 shows the actions for each engineer.

Table 4: Action sequence for each engineer

Engineer	Action description
SRO	A1-A2-A3(begin)-A31-A36-A3(end)-A4
RO	A21-A22-A23-A24-A33-A34-A35-A311-A312-A313-A362
TO	A311-A361-A363
EO	A32-A37-A38

[Step 4] Now, we need to add communication operators. The first situation for adding a communication operator is between

SRO and RO. SRO who is in charge of A2 directs RO to do A2. After performing A21, A22, A23, and/or A24, RO reports back to SRO. If two consecutive actions are performed by different engineers, a communication operator is necessary for each engineer.

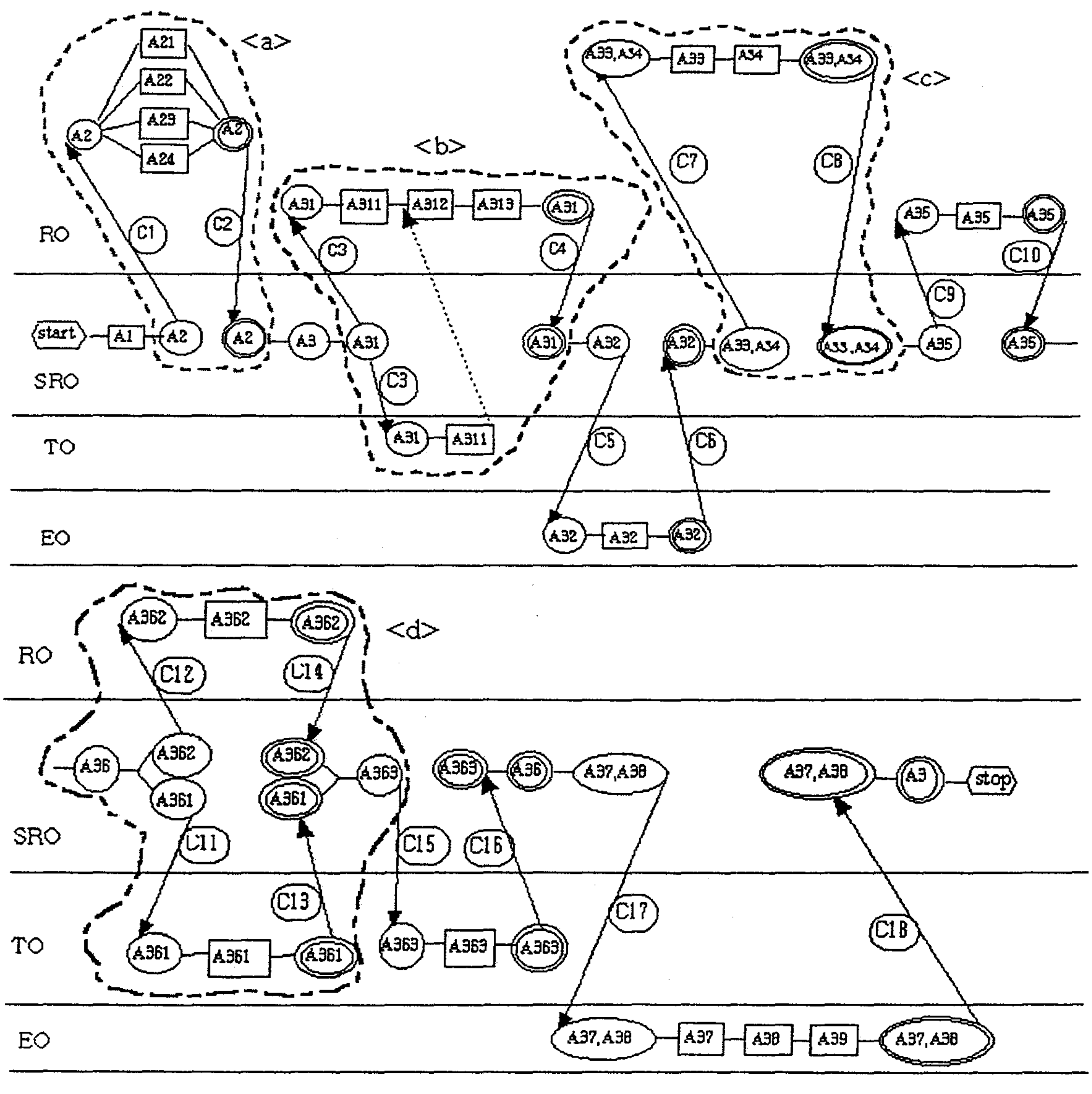
Table 5: Action sequences after adding communication operators

Engineer	Action description
SRO	A1-A2-C1-C2-A3(begin)-A31-C3-C4-C5-C6-C7-C8-C9-C10-A36-C11-C12-C13-C14-C15-C16-C17-C18-A3(end)-A4
RO	C1-A21-A22-A23-A24-C2-C3-A311-A312-A313-C4-C7-A33-A34-C8-C9-A35-C10-C12-A362-C14
TO	C3-A311-C11-A361-C13-C15-A363-C16
EO	C5-A32-C6-C17-A37-A38-C18

Even if one person carries out two consecutive actions, the evaluator may add a communication operator if necessary. After adding communication operators, Table 5 shows the action sequence for each engineer.

A PERT chart for Table 5 is shown in Figure 1. Rectangles represent methods or operators including internal and external operators, while circles connected by arrows represent communication operators. The area <a> shows that more than one operator among A21~A24 are carried out; The area <b> represents that the operator A311 should be performed by both RO and TO together simultaneously and that RO continues to do A312 after A311 is completed; The area <c> shows that SRO directs RO to perform A33 and A34, but SRO does not care about the order of the two actions; The area <d> represents that SRO directs RO to do A361 and directs TO to do A362. RO and TO can carry out each action in parallel. A363 can start after both A361 and A362 terminate.

Figure 1: PERT model



[Step 5] For each action at the leaf node, either NGOMSL or CPM-GOMS is applied depending on whether primitive operators are carried out in parallel. As an example, Table 6 shows primitive operators of A311.

Table 6: Decomposition of A311

Engineer	Action description	Task Id.
	M to AGO Manually trip reactor	M(A311)
RO & TO	Retrieve the location of trip switch from LTM	A3111
RO & TO	Go to the trip switch	A3112
RO & TO	Move a hand onto the trip switch	A3113
RO & TO	Count 3 to synchronize	A3114
RO & TO	Press the trip switch	A3115
	RGA	A3116

[Step 6] Quantitative analysis suggested by NGOMSL includes learning time, execution time, and mental workload. If there is any estimate for a primitive operator, we have used them.

Table 7: Estimates for A311

Task Id.	Statement Time (sec)	Execution time(sec)	Operator type	Mental workload
M(A311)	0.6(0.1x6)			
A3111	0.1	1.2	Memory	M(A311)
A3112	0.1	3	External	M(A311)
A3113	0.1	0.4	External	M(A311)
A3114	0.1	3	External	M(A311)
A3115	0.1	0.2	Internal	M(A311)
A3116	0.1		Control	M(A311)

Otherwise, estimates are derived from informal observations. For more realistic estimates, further experimental studies would be required. As an example, estimates for A311 are shown in Table 7.

Execution time for retrieval from long-term memory (A3111) is estimated at 1.2 and the time for moving to the location of trip switch (A3112) is estimated at 3 from an informal observation. The time for moving a hand onto the switch (A3113) and the time for pressing the switch (A3115) are estimated from Kieras[6]. Three seconds are assumed for A3114, because they actually count three to synchronize their actions.

[Step 7] After the quantitative analysis for all actions, we can extend the analysis for the group. We need to make some adjustments for Figure 1, because it represents the action sequence on the assumption that every action by RO, TO, or EO can start after SRO gives an order. However, when they are experienced, in some cases they do not wait until SRO gives them an order. They expect the next order and carry out before an order if that is not prohibited. With this consideration, we have revised Figure 1.

After simplifying Figure 1, we need to add communication time. Estimates from an informal observation are used for communication time. Figure 2 shows a revised PERT.

For A2, we assume that only one of four actions is carried out and add the communication time to the mean time of A21, A22, A23, and A23. After we have calculated execution times in this way, we have found the critical path in Figure 2. The summation of the execution time on the critical path is the total execution time for the whole group. We also measure individual engineer's execution time which is composed of action time and communication time. Then, we can compare the execution time among engineers. For mental workload, we use the same concept that Kieras suggested [6]. Only maximum load is included in this study. Table 8 summarizes execution time, communication time, and maximum mental workload.

Figure 2: A Revised PERT

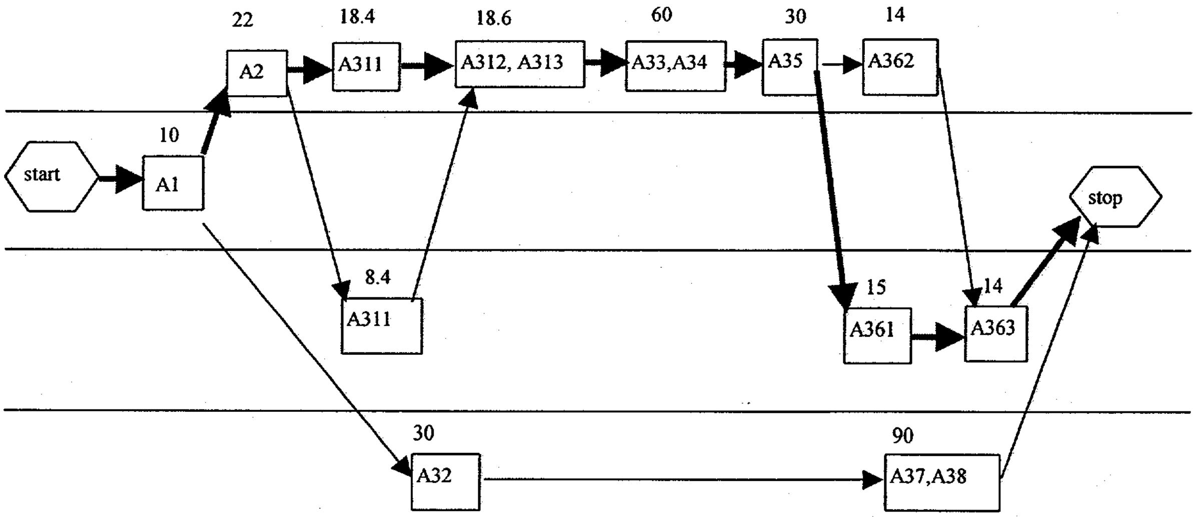


Table 8: Task distribution

Engineer	Execution time	Communication time	Maximum Mental workload
SRO	103.6	93.6	3
RO	167	78.6	4
TO	36.4	14	2
EO	120	25	3

5. CONCLUSION

This paper has presented DGOMS technique that has been developed in order to evaluate the interface between human group and technical subsystems. Then, the paper has compared DGOMS with previous GOMS. After choosing one emergency operation task, the paper has shown an application of DGOMS to a task.

The result from the tentative application can be summarized in three aspects. First, the DGOMS procedure has been applied without much difficulty. We have identified a few types of communication operators as well as primitive operators suggested by the previous GOMS. Second, DGOMS is an extension from GOMS which does not consider social distribution of cognition. DGOMS evaluates whether the cognitive load is balanced among individual engineers of a group and whether the task allocation among the human members of a group is balanced. Third, the selected task for evaluation is not very complex in comparison with other NPP operation tasks. The cognitive load for each engineer is acceptable in terms of safety since the cognitive load is below the critical level causing human error.

The limitation of this research is summarized as follows. First, the NPP operations manual is not described at the primitive operator level, but at a higher level. So, subjective judgment of evaluators plays a large role in the process of decomposing tasks into primitive operators. Second, the time estimates lack the precision because of insufficient empirical data with details in the domain of NPP. In order to alleviate this problem, we have made informal observations and videotaped the training process at a training center. We need to refine estimates for quantitative analysis. Third, mental workload of communication operators might differ depending on the communication content. Yet, there is no theoretical basis for estimating mental workload during communications. This again invites evaluator's judgment. Fourth, DGOMS does not provide a way to combine results from two evaluations.

In the future, we are going to improve DGOMS by applying it to various tasks at NPP control rooms. The accumulation of evaluation results would set up a basis for HMI standards and contribute to the safety at NPPs.

6. REFERENCES

[1] Card, S. K., Moran, T. P., and Newell, A., The Keystroke-Level Model for User Performance Time with Interactive Systems. Communications of the ACM, 23(7), 1980, pp. 396-410.

[2] Card, S. K., Moran, T. P., and Newell, A., The Psychology of Human -Computer Interaction. Hillsdale, NJ: Lawrence Erlbaum Associates, 1983.

[3] Endestad, T. and Meyer, P., GOMS Analysis as an Evaluation Tool in Process Control: An Evaluation of the ISACS-1 Prototype and the COPMA System, Technical Report HWR-349, OECD Halden Reactor Project, Halden, Norway, 1993,

[4] Hutchins, E., Cognition in the Wild, MIT Press, Cambridge, Massachusetts, 1995.

[5] John, B. E. and Kieras, D. E., The GOMS Family of Analysis Technique: Tools for Design and Evaluation, working paper CMU-CS-94-181, Department of Computer Science, Carnegie-Mellon University, 1994.

[6] Kieras, D. E., Towards a Practical GOMS Model Methodology for User Interface Design, Handbook of Human Computer Interaction. M. Helander, (ed.). Elsevier, 1988.

[7] Kieras, D. E. and Polson, P. G., An Approach to the Formal Analysis of User Complexity, International Journal of Man-Machine Studies, vol. 22, 1985, pp. 365-394

[8] Min, D., Koo, S. H., Ahn, J., and Yoo, Y., An Evaluation Technique for Human-Machine Interface(II), Project Report, KINS, 1998

SESSION 2

DEVELOPMENT OF HMI SYSTEM FOR OFF NORMAL AND EMERGENCY

IAEA Specialists' Meeting on HMI for Off-Normal and Emergency Situations in NPP,
26-28, Oct.1999 Taejon, Rep. of Korea

Human Factor Evaluation of a Safety Parameter Display System in Nuclear Power Plants using a Cognitive Task Analysis Method

Yong H. Lee

Man-Machine Interface System Team, Korea Atomic Energy Research Institute(KAERI)

Phone: +82-42-868-294, Fax:+82-42-868-8357, E-mail:Yhlee1@nanum.kaeri.re.kr

Wan C. Yoon

Intelligent System Lab., Korea Advanced Institute of Science and Technology(KAIST)

Abstract

Safety Parameter Display System (SPDS) is a typical implementation function to monitor the safety status of nuclear power plants and support operators in off-normal and emergency situations. Critical Function Monitoring System (CFMS) has been adopted to Korean NPPs as a basic SPDS function. A human factors verification and validation (V&V) on SPDS in a more formal and intensive manner is a mandatory process requested by the licensing authority. Availability and suitability are included within the major topics of the human factors V&V. Licensing requirements tell so much on the necessity of the availability and suitability test, but there are very few technical words on the method and no detail in practice. Since CFMS is an information system to operators, the information aspects of availability and suitability must be the center of the test. To verify the human factor aspects of CFMS, there should be a prescribed requirement of the information design as a reference in the verification. Task analysis has been generally expected to reveal the set of requirement items and their structures from the early stage of design. However, since the information requirements of CFMS can not be explicit and observable, an information- oriented method is articulated for cognitive task analysis. The method the information flows along the task procedures that might be utilized in emergency situations in NPPs. It reveals *cognitive spans* of information items, and *cognitive envelopes* and *Working Memory Relief Points* of task procedures as the cognitive requirements of SPDS. We performed a cognitive task analysis of operating procedures and others to define the requirements of CFMS, and tested the information availability and suitability of the current CFMS design. The result reveals the potential Human Engineering Discrepancies (HEDs). Their resolutions update the CFMS design.

1. Introduction

After TMI#2 incident, human factors evaluation on the systems for emergency operations such as SPDS have been mandatory in the design process. In Korea, there have been several HFE (Human Factors Engineering) V&V (Verification and Validation) projects on the SPDSs, which were mainly established with Critical Function Monitoring Concept. Independent evaluations are conducted through a series of pre-planned review activities. Evaluations mainly focused on the assessment of availability, suitability and, finally, total effectiveness of the system and its interfaces. Various methods have been applied during the evaluations. The cognitive aspect on interfaces and information system is assessed based on the requirements that are extracted through cognitive task analysis of operating procedures. The suitability test mainly utilizes a structured checklist, which is based on a minimal set of human factors evaluation items. Many design issues including HEDs (Human Engineering Deficiencies) are accumulated for tracking in the licensing review, and evaluated by their importance scores for design decision-makings. A computer support system named DIMS (Design Issue Management System) was developed and is now imported on the Web.

In Korean, we adopt Critical Function Monitoring System (CFMS) which satisfies the licensing requirement of SDPS. Human factors of CFMS for Ulchin 3&4 and Yeonggwang 3&4 nuclear power units have been assessed to support the licensing, according to SPDS requirements, which has been one of major licensing issues for human factors engineering of nuclear power plants in Korea. The conceptual goal of human factors requirement itself was clear, however, the methods and the practice have not been so clear to promote a progressive improvement. Although almost all NPPs have been equipped with SPDSs or other equivalant systems, SPDS might be notorious to be such a typical license-wise upgraded feature all over the world including Korea. The operators' acceptance and the operational benefit have not yet been reported positively in Korea as well as in U.S. and others.

In Korea, SPDS, which is mainly developed by ABB-CE and established with critical function concept, is adopted to Korean Standard Nuclear Power Plant (KS-NPP). Two independent evaluation projects have been conducted succeedingly. Evaluations are mainly based on the domestic licensing requirement definition, which is not much different from the US-NRC's SRP section 18 and other NUREG documents. A few additional works and implemented processes are identified during the projects. Recently, a more practical method is defined based on the experiences on HFE V&V of SPDSs, and the framework procedures and a support system are now on the way of development not only for licensing but for design improvement. This paper describes a part of the experiences of independent evaluations on human factors of an SPDS as a part of HFE V&V projects in Korea.

2. Approach for HFE V&V on SPDS

At first, independent evaluations are conducted through a series of pre-planned activities. By reviewing issues regarding the design process of present CFMS, two generic plans such as human factors engineering program plan and HFE V&V plan for CFMS were proposed to satisfy the procedural exhaustiveness of human factor engineering work. These plans are established separately from the main HFEPP and software engineering plan, but the activities are defined in incoperative manner with software design. Although CFMS is not a safety system, regulation requires a through review on human factors such as ; the function, the interface compatibility, the satisfaction to the requirements and current principles as well as the design process. However, Korea donot have a clear evidence to the operators satisfaction, nor the background for the human factor requirements because CFMS had been originally based on and just imported from ABB-CE's concept. The human factor concernings such as the cognitive compatibility to the operators must be verified whether CFMS would properly support operators to satisfying the safety goal during the tasks in assumed situations in NPPs.

Secondly, the evaluation is focused to the assessment of availability, suitability and effectiveness of the system and its interfaces according to IEEE std-845 and EPRI NP-3701 vol. 2. The availability and suitability were assessed according to human factor criteria and requirements on the CFMS display design, and overall effectiveness was also evaluated by experiments and in parts by introducing an operator performance model. A cognitive task analysis (CTA) method was applied to the definition of information requirements for CFMS. CTA method helps to identify the information requirements of tasks which operators supposed to perform during the emergency situation. It emphasizes upon the information organization of a task that is supposed to be the cognitive workload rather than the behavioral workload to the operators. Discrepancies between the requirement information and the information provided in the design are evaluated by studying how those requirements and discrepancies affect the operator's cognitive work during performing the procedural tasks. The result shows that the task support-ness of CFMS would be enhanced and verified in information aspects.

For the HFE V&V of a design, regulatory documents utilize a new word of the task supportness, which means that the design is enough and not excessive to support all tasks operator intended to do during the use of the design. We break down the task supportness requirement into two succeeding requirements with an emphasis on the cognitive aspect of task supportness. They are the availability and the suitability of information items provided to the operator. In other words, we tested what and how the information items are provided by CFMS. Several deficiencies in the information availability and the suitability of CFMS displays including the interaction and navigation aspects were identified. Almost of these deficiencies could be solved easily by introducing human factors engineering principles. Some deficiencies, however, which are not the problems violating directly the regulatory requirements, are still issued to design decision for the better quality of future design and the maintenance of CFMS.

Finally, a support system named by DIMS (design issue management system), was developed to support the review process by maintaining the requirements, the design issues and their treatments in form of a database. Several review worksheets were also developed from the requirement database of DIMS through holding out the HFE requirements and being specified to CFMS. Recommendations were made to each human factor problem identified in accordance with its estimated importance, and an implementation plan was suggested for the resolution of problems. A multi-criteria and multi-participant decision process is also proposed to support the consistent design decisions on the problems identified by evaluating their relative importance in technical, engineering and managerial aspect.

In the review, most of the methods mentioned in IEEE-std-845 available for man-machine system evaluation had been utilized such as ; documentation review, review by standards, review based on the development facility (a dynamic mockup of CFMS), review by interviewing the operators who are the prospective users or the experienced personnel, review by experiments, review by individual experts and a team of multi-disciplinary experts including licensing staff, and others.

Table 1. Methods for human factors design review

Review Methods	Availability	Suitability	Efficiency
Document - Analysis	◎	△	△
Specialist Opinion - Checklist	△	◎	△
Experiment Review - Simulator	△	0	◎
Operator Opinion - Interview, WT/TT	0	0	0
Facility Review - PMS-DF	△	△	△

◎ : Main Review , 0 : Supporting Review, △ : Assistant Review

3. An Approach to Cognitive Task Analysis

3.1 Methods and Approaches for Task Analysis

As a fundamental element of various human factor studies, task analysis (TA) in general attempts to describe and analyze how a human in a system interacts with both the system and other personnel in the system. The primary aim of TA is to describe the details of human involvement in a system in terms of behavioral and/or cognitive processes, but it can also provide the bases for analyzing the adequacy and/or degree of the involvement. The outcome of TA provides useful bases for various human-related designs and engineering decisions.

The operation of nuclear power plants, in both normal and emergency situations, is mostly guided by prescribed procedures. Following operational procedures involves more than merely reading instruction lines and acting as specified. The operator must assess the situation, confirm the consequences of operations, and check the conditions for the next steps in the procedure. These activities frequently deal with an abstract understanding of the system and the tasks, rather than the raw data as specified in the procedure. Thus, assessing and minimizing the cognitive workload in conducting prescribed procedures is important for a better design of the human-machine interface and/or the procedures. When a task procedure is given, it may provide a context for figuring out the practical significance of the cognitive requirements as well as behavioral ones. Therefore, it is desirable that a TA identifies such requirements and assesses them in the light of the underlying organization of tasks in the given procedure itself. With most TA methods, tasks are usually broken down into sub-tasks and further into elementary actions to enumerate all possible requirements for their specific purposes. This decomposition approach is fairly effective in analyzing the physical aspects of tasks (i.e., actions) and their requirements. Analysis of the cognitive aspects of tasks, however, is not as straightforward. Analysts performing TAs seem to face confusion because the decisions related to the decomposition of tasks are often made heavily dependent upon the context of the tasks. Perhaps the most fundamental reason for this is that the task steps are not organized only through the order or control flows in physical activities but also through the task information. The flows and usage of task information can not be easily described in a sequence only. Instead, the information in tasks may often be integrated or abstracted by the operator(i.e., the task performer) and only partially ordered in time.

In this paper, we propose a TA method that identifies information requirements of tasks and analyzes how those requirements affect the operator's cognitive work during performing the task procedures. An emphasis is put upon the cognitive organization of a task that is imposed by its information requirements rather than the functional or behavioral organization. The method was also designed to preserve as much simplicity of the analysis procedure as possible for practical applications.

3.2 task analysis methods

In general TA methods are performed in three stages : identification, description, and evaluation of tasks. The details of these stages vary depending on different purposes of the analysis. Task description, being affected by the viewpoint of a TA, is particularly important to accomplish the purpose. Now, we discuss some TA methods in terms of their description approaches.

3.2.1 Application of Taxonomy

Applying a taxonomy to classify human performance has been a common method to obtain task requirements, since a suitable taxonomy can facilitate good interpretation and a plausible prediction of human performance. Performance taxonomy has worked as an effective method especially for human error studies. When the taxonomy of describing tasks is adopted or derived from an action-based approach rather than function-based one, TA methods based on the taxonomy can better describe physical aspects of tasks than their underlying cognitive processes. However, a few recent works on human error studies are still trying to utilize the merit of using taxonomy, and show progress of developing new cognitive classification taxonomy derived by the human models and the interpretations of real error-cases.

3.2.2 Decomposition schemes

Task description usually takes the schemes of sequence, link, hierarchy, network, and others. The most frequent description scheme is hierarchy which HTA (Hierarchical Task Analysis) utilizes to express the structure of tasks. Hierarchy, in general, fits the goal structure. Since aggregation of several steps in tasks are closely related with abstraction or meaning of those steps, reconstructing the procedures in a hierarchy can describe the goal structure of a task. Hierarchy seems to be almost indispensable for a TA that starts with task procedures. However, the hierarchical scheme alone is not very capable of handling the multiple relations that appear in cognitive processes of the operators when performing procedures in a complex technical system. Over the hierarchical scheme of task goal and its operations HTA itemizes *plans*, which describe the control relations (such as the order, condition, and iterations) among operations under their goal. GMTA (Goals-Means Task Analysis) identifies pre-conditions for tasks and sub-tasks and sets them as sub-goals in a recursive manner. The goal-means structure in GMTA is emphasized for the assessment of the cognitive aspects of tasks, and enhances the capability of handling multiple relations among task steps in a complex technical system.

3.2.3 Direction of Description

TA usually decomposes a task into sub-tasks or elementary task units until it can clarify the task requirements. According to this *decomposition paradigm*, the most TA methods adopt top-down decomposition approach with a few exceptions such as TAKD (Task Analysis for Knowledge Description) and its variations. TAKD is notable for its bottom-up approach and the *generification* by mappings between *specific actions/objects* and *generic actions/objects* , which may be used to account for possible abstraction of task requirements for cognitive task analysis (CTA).

Within the NPP domain, the crew task analysis was conducted in a large scale by U.S. NRC in the early eighties. Although the data base contains a vast amount of detailed task requirements, good implication especially for computerized features in NPPs can hardly be found on cognitive aspects of the tasks. It was partly due to the decomposition approach and the use of the task taxonomy which was based on typical behavioral terms.

Many of recent TA methods emphasize cognitive aspects and employ some features to capture them. Most prevailing features are frameworks such as abstraction hierarchy or model-based schemes. The models, especially human information processing models, help to describe the cognitive aspects of human performance. A typical use of a simplified human decision making model to a retrospective analysis can be seen in Lee & Yoon's recent work that has a model-based description scheme for analyzing events occurred in NPPs. Keeping a rigorous account on the human activities based on a human model, however, may be a burden to task analysts in practice unless the model is simple and clear to them. Moreover, since the models cannot predict the actual path and all possible paths of human cognitive process, the application of model-based methods should be carefully adopted to a prospective type of analysis rather than retrospective one. A good use of human model to a prospective type of analysis can be seen in Hollnagel's recent human error study. Recent works for the enhancement of task descriptions to meet the TA goal show the integration of two or more methods such as model-based methods and the classification taxonomy.

3.3 view and overview of the CTA method proposed

3.3.1 An information-oriented method

A task is defined as a unit of actions required by the system and allocated to human operators. Cognitive tasks are more than overt actions. Cognitive tasks are rather described in terms of information processing steps including input, output of information, decision making, storage and retrieval of memory, etc. Cognitive requirements of a task can be assessed by the *information items required to the successful performance of the task*. We focus to the characteristics of operator's working memory such as the limit of capacity and the internal management of information items, because these are critical aspects of task performance in sense of information processing.

The operator's tasks in NPPs are extensively documented for most situations in the forms of prescribed operating procedures. It is reasonable to develop a specific method for CTA that utilizes those written procedures, which would carry well-composed details, as the primary information about the tasks. Cognitive aspects are still crucial, since the operator, even when undertaking an instructed procedure, is stressed mentally by the need to understand the situations and follow the tasks in abstract terms. Such underlying cognitive demands are usually not evident in the procedure description itself, and hence subject to TA investigation. Although some data is required from the domain experts, the CTA based on procedures is analytic in nature rather than empirical. It has three main phases: task description, cognitive requirement assessment, and application evaluation. Figure 1 shows the steps of the first two phases in the CTA method proposed.

TA has been performed from diverse viewpoints depending on their applications. In NPPs, operating procedures are conceptually subordinate to human-machine system functions that are hierarchically enlisted in the basic design of NPP dynamics. Thus, a functional view of operation should be embraced by task analysis in NPPs. It is our contention that the physical aspects (i.e., actions) of tasks fit part-whole organization better and the functional aspects can better be organized in abstraction hierarchy. Actions are temporally sequenced on a single line (i.e., totally-ordered) both in their actual occurrences and in the prescribed procedures, while functions are logically interconnected and form a network. Where functions involve cognitive activities, the logical interconnections are pre-dominantly determined by information flows. The information is also integrated and/or abstracted by the operator to relate it to the abstract understanding of the functions. It is reasonable to say that precise and thorough identification of the information requirements, flows, and abstraction is the primary key to effective analysis of cognitive tasks in NPPs. The proposed CTA method is in line with this information-oriented view.

4. Cognitive Assessment of CFMS

4.1 Assessing the Information Availability of CFMS

CFMS is to support operators during the emergency situation by providing the safety status information as an SPDS in nuclear power plants. CFMS must provide the safety information required by NUREG-0737, Supplement 1, categorizing into 9 critical safety functions (CSFs). Each CSF has its own logic of alerting the operator the challenge to the safety of the plants through basically one CRT page in form of a summary matrix. Several CRT pages can be accessed by a special function key-board and a dedicated CRT in case that operator want to know the details of the CSFs' challenge and their changes according to recovery actions. Since the main indications in main control room are mostly hard-wired conventional, CFMS is assumed to be utilized by Safety Engineer who is responsible to the maintenance of the plant safety, rather than Senior Reactor Operator who is responsible to the management of transients and overall operating process. CFMS is assumed to be utilized in accordance to the emergency operating procedures (EOPs). There is a dedicated set of tasks, named First-02, which consists of not more than 10 steps. However, all of steps must be conducted by Safety Engineer in parallel with every step of EOPs in order to mitigate the transients and maintain the safe state of the plant during emergency operation. Although there is only one explicit procedure for CFMS, the procedure itself does not covers every detail tasks for utilizing CFMS. The procedure involves more than the line and the instructions, because operator sometimes needs to identify the specific causes and understand the context of CFS challenge in order to decide whether related prioritized procedures (FRG: functional recovery guideline) should be conducted or not. In order to attain the task goal of procedure by utilizing CFMS, operators should follow the details of alarm logic and information items through the information legs in each CSF, the trends of critical parameters through their temporal plots, and the overall state of the related system through P&ID (pipe and instrumentation diagram) mimic. The information requirements for CFMS can be defined by analyzing the task procedure, including the implicit steps as well as explicit description. Following types of requirement sources are considered for this review such as ; Alarm logic of CFSs, procedures related, and operating experience.

The information availability is assessed based on the requirements that are extracted through cognitive task analysis (CTA) of operating procedures. Procedures are usually not finalized for the HFE V&V during NPP design, however, the information requirement items is well defined in, for example, ERGs (Emergency Response Guidelines). CTA is proposed for enumerating the operators' interface requirement items based on the operating procedures. Requirement list (LIST-R) is defined from the analysis of procedures (LIST-P), operating experiences (LIST-O), alarming logics in SPDS (LIST-A), and the thermo-hydraulic analysis of safety functions (LIST-T). Each list adds up and results to a set of requirements for the availability. Another list is defined from the design itself. The inventory list (LIST-I) information items found in the implemented design is extracted for assessing the availability by comparing the two lists. For each information item, the comparisons show whether the partial or complete fulfillment of requirements for SPDS.

4.2 Requirement extraction through Cognitive Task Analysis

The operation in both normal and emergency conditions, are prescribed and mostly guided by operating procedures. Conducting tasks for operation requires more than merely following operating procedures, reading instruction lines and acting as specified. The operator must frequently abstract for understanding the status of the systems and the goal of tasks, rather than read the indications and raw data as specified in the procedure. Thus, assessing the cognitive processes in conducting the prescribed tasks with a given design is important for a better SPDS that is more compatible to the operators' cognitive process and acceptable to the operators. Therefore, it is desirable that a task analysis identifies such design requirements and assesses them in the light of the underlying organization of tasks with a given design. Task analysis provides data for the human factors design requirements of Human System Interface such as main control room, and other facilities and equipments in NPPs.

It is hard to define the requirements to the cognitive aspect of tasks, however, which become more important in recent NPP designs. An enhanced method for cognitive task analysis proposed by Lee & Yoon based on an information-oriented view on tasks was applied. The method identifies cognitive requirements of operators' tasks by capturing the cognitive aspects of tasks that are supposed to be conducted by operators in emergency situation in nuclear power plants. The method proposed focused to the implicit as well as explicit information for task performance. It identifies the information requirement items for each step of task performance, and then traces their flows in task profiles. Like most TA methods, tasks are decomposed into sub-tasks and further into elementary actions to enumerate all possible requirements for their specific purposes. The information items should be provided by the CFMS when the tasks are intended to utilize the design. Availability means a question of whether the all information items required are provided by the design or not.

Analysis of the cognitive requirements of tasks, however, is not enough until the requirement items can provide a higher level contextual requirement of the tasks. Task steps are usually organized only through the temporal order or the control flows in physical activities. The flows and usage of task information that will form a kind of cognitive load to the operator can not be easily described in a sequence or aggregating the lower level requirement items. The information items in tasks may often be integrated or abstracted by the operator depending on the condition of his working memory and other cognitive resources as well as task goals. The information flow reveals the cognitive organization of a task, especially given in form of procedure. We introduce some new concepts such as: *cognitive spans* of task information, *working memory relief points*, and *cognitive envelopes* of task procedures. Some of the cognitive characteristics of tasks with a given design of CFMS can be identified in terms of these additional terms that can be obtained by the proposed cognitive task analysis. The congruence of CFMS to the tasks that are required to utilize CMFS can then be assessed.

5. Conclusion and Discussions for future works

In this paper, our experiences of HFE V&V on SPDSs in NPPs are described briefly based on a proposed cognitive task analysis method. Additional information items and a few more functions such as SFSC (safety function status check) were recommended for enhancing the availability, suitability and effectiveness of current CFMS design as an SPDS for NPPs. The experiences show the applicability and the usefulness of CTA for extracting opearator's cognitive requirements from task procedures and others. Efficiency and effectiveness of the human factors review process could be enhanced significantly with a full-scaled task analysis including CTA. Although the benefits have been found in the evaluation of the CFMS, more researches and works are still required when it is extended to the evaluation and/or design of a computer-based I&C system. For more efficient evaluation, support functions for CTA should be developed and incooperated into the overall design process of CFMS.

References

1. NRC, *Human Factors Engineering Program Review Model, NUREG-0711*, 1994.
2. NRC, *Guidelines for Control Room Design Reviews, NUREG-0700*, 1981.
3. NRC, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, NUREG-0800*, 1984.
4. Saaty, T.L., *Analytic Hierarchy Process*, McGraw-Hill, 1980.
5. IEEE, IEEE Guide to the Evaluation of Man-Machine Performance in Nuclear Power Generating Station Comtrol Room and other Peripheries, IEEE-STD 845,1988.
6. Lee, Y.H., et al., Development of a Systematic Checklist for the Ergonomic Evaluation of the Critical Function Monitoring System of a Nuclear Power Plant, *Proceedings of IEA'97 Conference*, 1997.
7. Lee, Y.H., et al., *Human Factors Review of CFMS Displays for Ulchin Nuclear Power Unit 3 & 4 (In Korean), KAERI/CR-027/96*, KAERI, Taejon, Korea, 1996.
8. Lee, Y. H. and Yoon, W. C., A Cognitive Task Analysis Method for Procedure-Based Tasks in Nuclear Power Plants, *Proceedings of Cognitive Systems Engineering in Process Control (CSEPC'96)*, Kyoto, Japan, November 12-15, 1996, pp. 261-267.
9. Korea Atomic Energy Research Institute (KAERI), Design Requirements for the Critical Functions Monitoring System for UCN 3 & 4. N0291-FS-DR210-X, KAERI, Taejon, Korea, 1995.
10. Yun, M.H. et al. Development of a Systematic Checklist for the Human Factors Evaluation of the Operator Aiding System in a Nuclear Power Plant, Int. J. of Industrial Ergonomics (accepted), 1999.

Creating Effective Control Room Layouts

Richard Brice, OAO Technology Solutions, Inc.
Atlanta, Georgia USA 30340

Introduction

In past years, it has been clearly established that digital technology and documented procedures are beneficial to supporting off-normal and emergency situations in nuclear power plants (NPP). Although most practitioners recognize the human machine interface (HMI) issues for the creation and organization of operational information on digitally driven screens, fewer understand that there are also HMI issues associated with the location and adaptation of hardware items for effective use by the human operators. During off-normal and emergency operations, more than at any other time, the interactions of traffic, placement of equipment, sightlines, and access to documents become extremely important. The operator's smooth and practiced response to off-normal and emergency situations can either be aided or hindered by the control room layout.

There are numerous anthropometic, ergonomic and other standards for the placement of equipment in control rooms, and graphical user interface guidelines for operator interface design. However, static application of these rules may not address the diverse dynamics involved in handling off-normal and emergency situations. The challenge for the designer is to discover the most effective control room design with competing requirements, particularly true in retrofit projects where the existing space is limited. The key to addressing this challenge is the creation of a realistic set of site specific design criteria, which can only be achieved by understanding the control room from the perspective of the operators themselves.

This paper presents a methodology for resolving demands of competing requirements while still developing a coherent design criteria for improving an existing control room for off-normal and emergency conditions. The paper discusses the methodology in terms of collecting information, developing the criteria, and creating the final design for the control room upgrade. The methodology is particularly useful in its demonstrated ability to draw out from the operators, a clear description of how their particular control room should function. The methodology facilitates a highly participatory design and development process, with the operators becoming the designer and the designer becoming a facilitator.

Background and Philosophy

In September of 1981 the United States nuclear industry made commitments to address ergonomic issues using NUREG 0700, a guideline published by the US Nuclear Regulatory Commission (NRC). The Detailed Control Room Design Review (DCRDR) process specified in NUREG 0700 defined procedures for discovering human engineering discrepancies (HEDs) within their control rooms. In the area of workspace and workstation design, these guidelines represent a good first step. Since 1981, however, tremendous progress has been made in the study of advanced human machine interface (HMI) technologies. The latest guidelines for nuclear plant control rooms published by the NRC in July 1994 in BNL-NUREG-5233, *Advanced Human System Interface Design Review Guideline,* makes many references to these advances. However, other than noting the static guidelines for computer display viewing angles, distance, glare and ambient lighting, BNL-NUREG-5233 provide no guidance to the workspace dynamics of control room configurations. The guidelines published by the NRC and other agencies are all good starting points and provide checklists of the basic requirements. Without these guidelines, many poor anthropomorphic conditions would still exist in the work areas of nuclear plant control rooms.

In fact, a study cited in BNL-NUREG-5233 shows that 15% of all HEDs discovered at 25 Nuclear Plant Control Rooms were workspace related. However, the discovery of HEDs using checklists provided in guidelines is a single-threaded diagnostic process and cannot be used as a means to design for the dynamic processes unique to each control room, especially during off-normal and emergency situations. Control rooms that are designed using only these guidelines without addressing the dynamic issues result in a room without any identified HEDs but may be still poorly laid out. This paradoxical result arises because each of the static issues are interrelated. For example, if traffic areas are widened to ideal dimensions, this tends to reduce the available workspace for laying out emergency procedures or emergency logic charts. In a second example, if the operator is seated ideally for paperwork while monitoring the control panels, the workstation will probably be an obstacle to accessing the control panels. The major factor that must be addressed is the dynamics in a nuclear plant control room. Depending on the plant's status during off-normal and emergency conditions, the dynamic actions required in the control room can change radically. The layout of the work area should function well under off-normal and emergency conditions as well as during normal, outage and start-up conditions.

As more and more computer equipment is installed in nuclear plant control rooms to support off-normal and emergency conditions, usually the plant installs this equipment in standard off-the-shelf furniture. Alternatively, the computer equipment is sometimes placed on existing workstations creating sightline problems and leaving little room for laying out emergency procedures.

With the introduction of computer equipment to aid in data evaluation, the control room at a nuclear plant becomes a hybrid of both digital and analog equipment. In the hybrid control room, the operator must view a monitor, yet still rely on readings from analog indicators some distance from his viewing position. The static guidelines for operator ergonomics produce competing requirements in such areas as sightlines, ambient lighting, workspace utilization and physical access. These competing requirements can be resolved with a unique layout developed specifically for that control room.

The challenge in designing a layout for hybrid control rooms is discovering the best practical design. The key to meeting this challenge is to create a realistic and practical set of site specific design criteria (SSDC). This can only be done by understanding the functions of the control room from the operators view point. The best way to understand the operator's perspective is to ask them. This empirical approach for data collection is by far the quickest way to understanding the facts, needs and problems of the operators. The following sections describe how the basic information can be collected, integrated with other real constraints such as budgets and schedules, and used to create a useful set of design criteria. These design criteria can then be used by a design team to create the control room layout for all the dynamic conditions.

Importance of Sequence

Once it is fully understood, every problem can be solved easily. One of the major pitfalls of any problem solving effort is to predetermine a solution before all the facts are known. Another pitfall is that a linear sequential problem solving approach creates a dilemma because solving one problem often creates another problem. The solution to the dilemma is to take all the information and first create the most efficient and ergonomically sound layout. In other words, create the most efficient arrangement for the staff, equipment, space and the known dynamic interaction in the ideal control room. This ideal control room can be designed first for normal conditions, then outage, off normal, start-up and emergency, in that order. This sequence also gives the design team, especially management, a chance to create a layout that enhances specific operations policy, plant requirements and operational efficiency.

Only after the ideal design has been completed, should the practical considerations of budgets and schedules be introduced. Compromising the design before the most ideal arrangement has been developed will lead to only a partial solution set and invariably leave some problems unsolved.

The design issues, therefore, must be addressed in a specific sequence. Figure 1 shows these design issues in three major groups, which are defined in a specific order, using the methodology.

Figure 1: List of relevant design issues.

DESIGN ISSUES		
DEFINING the BEST ORGANIZATION	1	**Operational Goals** Operational Management should include information on operational philosophy and participate in resolving issues of competing requirements during the design effort.
	2	**Personnel Relationships** Broad relationships between personnel, equipment, furnishings, procedures and control room environment should be defined in great detail through on-site interviews.
DEFINING the SPACE	3	**Equipment** The equipment to be used in the design consists of existing equipment used at the beginning of the design, as well as known future equipment additions, deletions or other changes
	4	**Anthropometries** Limitations of space required to perform tasks desired and anthropometric standards for the comfortable efficient Interface of man, machine and environment. Some of the anthropometric standards can be found in J. Panero and M. Zelnick, 1979. Human Dimensions and Interior Space. New York: Watson - Guptil Publications, NUREG 0700, Guidelines for Control Room Design Reviews, USNRC (1981) and Human Factors Society, Inc. 1969. Human Factors in Quality Assurance. New York: John Wiley & Sons.
DEFINING what is PRACTICAL	5	**Budget** The design process should include the development of a budget for fabrication and installation.
	6	**Schedule** The design process should also consider schedule constraints caused by delivery and retrofitting of new equipment, outage windows for installation, and previous commitments.

Methodology

The design methodology addresses interior and environmental design in the control room. This design problem should be addressed by a multi-disciplined design team made up of Operation Managers, Operators, Human Factor Specialists, Plant Engineers, Training Personnel, and Project Managers. The effort should be facilitated from beginning to end by an experienced design specialist familiar with nuclear control room logistics. The design methodology provides insights into the type of questions and methods that should be employed to assemble the information.

The first step of the methodology is to collect the static information. An inventory of all equipment and procedures should be gathered as well as basic job descriptions of the operating team members. With this information as background, the design specialist is ready to conduct personal interviews with the various operations personnel. It is important to interview most, if not all of the operating crews. During this step, it is important for the design specialist to maintain informality in these interviews, carefully remaining focused on gathering information. The interviewer should be cautious not to allow his personal past experience to stifle or affect the interview process. The information learned during these interviews should be organized into an outline which will become the Design Criteria Document (DCD).

Well-formed criteria are synonymous with a good design. Theoretically, for every set of criteria, there is a single best design but empirical considerations require compromises, often expressed as one or more design proposals. The design criteria is based on the information that was collected during the interviews and is the link between the operators to the creative design process. The Design Criteria Document is the most important piece of information in the process because at all times it represents the operators view of the requirements. The DCD is a living document that is updated as more information becomes available to the designer. This information should be validated by a cross section of the operator personnel to assure the data is relevant

At the next step in the methodology, the design specialist creates a control room layout using the DCD as a guide. Actually, several layouts are created to reflect optional solutions and different views of competing requirements which can be interpreted from the DCD. These designs should then be presented to the design team to obtain specific feedback on the optimum arrangement. It is during this step of the methodology that the best information is collected because people find it easier to comment on the concrete concepts presented rather than in an open-ended interview.

The comments on these layouts are used to refine the DCD, which in turn is used to revise the layouts. The iterative refinement of the DCD creates an important record of the decisions that led to the design. The careful documentation of design decisions prevents the solution of one problem from creating another problem. This iterative process within this step of the methodology helps the operators to refine their requirements which ultimately lead to the final design.

The final layout design should include floor plans, elevations, sightline sections and three dimensional color renderings. After the final validation of these drawings by the operators, the design represents the optimal layout. It is only after the optimal layout is achieved that the costs and schedule should be evaluated. If the optimal design cannot be built within the cost and schedule constraints then compromises must be made to the design. Doing the cost and schedule evaluation after the optimal design has been created enables the design team to evaluate the cost-benefit of given design features. It also provides the design team with a clear record of which features were compromised and why.

Although not always done, the construction of a full-scale mockup of the final design is highly recommended. The mock-up will allow the operators to evaluate the layout with practice scenarios for off-normal and emergency conditions, as well as for normal, outage, and start-up conditions. In the past, many plants were reluctant to pay for the construction of a mock-up. However, managers have realized that the built-in workstations in the final layout will probably last the life of the plant. Considering the longevity of the layout, most plants elect to build a mock-up. Operator evaluations of the mock-up do result in changes to the final design, but often a 10% refinement in the design adds 40% to the usefulness of the layout and the workstations.

Significance

The most significant element of this methodology is the attention given to operator feedback. Every step of the methodology is aimed at creating an operator-designed control room. The design team functions as a resource of industry standards, and creative designs with the design specialist serving as a catalyst.

The insights of the operators, those people dealing daily with the routines in the control room, are the best guiding forces to achieving an efficient layout. The integration of the operator driven ideas with managerial direction make acceptance of the new design by the operators relatively easy. Dr. Fritz Steel, a renowned organizational consultant, states in his book *Workplace by Design*, "without this involvement [*the users, ed.*] there will be no buy in, and it is likely that the data collected will be challenged as irrelevant or biased".

Results

The design methodology can identify specific problems with solutions that produce tangible improvements. Some examples are:

- Sightlines and Hierarchy Recognition – Each operator's position in the control room can be rearranged and physically elevated to improve sightlines to specific areas. This allows for easy recognition of the control room command hierarchy.

- Traffic Flow – Controlled access can be enhanced by adding barriers within easy eyesight of the approving operator's position. Other improvements can be made such as redesigning the desk layouts to offer better operator access to the control boards.

- Area Definition – Color-coded carpeting can be used to direct general traffic away from vital areas or to define the watch area.

- Noise Abatement – Where possible, sound dampening material can be used throughout the control room to reduce reverberation thus aiding clear voice communication.

- Work Areas – Operator workspace area can be increased with appropriate placement for files, procedures, spare parts, drawing files, layout areas, and other paperwork areas.

- Shift Manning Enhancement – The space nearest the control boards can be reorganized to allow for closer placement of the operating team to the control panels. The arrangement can also be designed to improve voice communications during off-normal and emergencies and to enhance the alternate command hierarchy during a transient event.

A very dramatic example of the difference in control room designs based on static guidelines versus the methodology described in this paper is shown in Figures 2 and 3. Figure 2 shows the design of an actual nuclear power plant control room which was developed using the static guidelines with very little operator involvement in the design process. This design was predicated on off-the-shelf furniture and uses standard office cubical furniture, overhead bins and cabinets. The layout shows an office niche type of arrangement that isolates the Shift Supervisor and Senior Operator from the at-the-controls area. This design also isolates the team members from one another, making voice communication between the operators difficult. During off-normal or emergency scenarios this layout would result in congestion at the control boards

The design in Figure 3 shows the same control room, based on the operator-centric methodology described in this paper. The design incorporates custom workstations, in a layout specifically crafted to enhance the off-normal and emergency profiles. The layout design is totally open with all team members facing the control boards. During off-normal or emergency conditions, the reactor operator (RO) and the balance-of-plant (BOP) operator can easily move to the control boards. The Senior Operator is in a central position to direct the operators' response to the event with adequate space for laying out his procedures.

Figure 4 shows another example of an actual control room. In this case, the control room was overburdened with digital equipment placed on existing workstations. The major problem with this layout is the lack of room for the emergency logic charts which can be as large as 36" x 48". In some areas, the monitors placed on the desk tops block the operator's view of the control boards from a seated position. The introduction of digital equipment creates a cluttered workspace, leaving the operator with little area to perform his normal paperwork duties

Figure 5 shows this same control room, designed using the operator-centric methodology. This design incorporates customized areas to accommodate the emergency logic charts. It also allows for easy viewing of the digital monitors which aid the operators' response to the event. A key feature of this design is partially sinking all digital monitors into the desk surface so that the operators can easily view all the control boards from a seated position.

Conclusion

These examples clearly demonstrate that the operators' intense and active involvement in the design results in a more organic layout for the control room. This organic quality evolves naturally from the operator-centric process because humans all operate in a dynamic organic fashion. The goal of ergonomic design in nuclear plant control rooms is to blend the access to the digital and analog equipment in such a way to enhance the human operator in his duties of controlling the plant, especially during off-normal and emergency conditions.

The methodology described in this paper has been successfully used in over half of the nuclear plant control rooms in the United States and in Europe. Some of these plants have been using these workstations for over twenty years with excellent results. The proof of the methodology's success has been clearly demonstrated by these enthusiastic end users – the operators themselves.

References

Fritz Steele, 1995: by Jossey-Bass, Inc. San Francisco, CA. USA

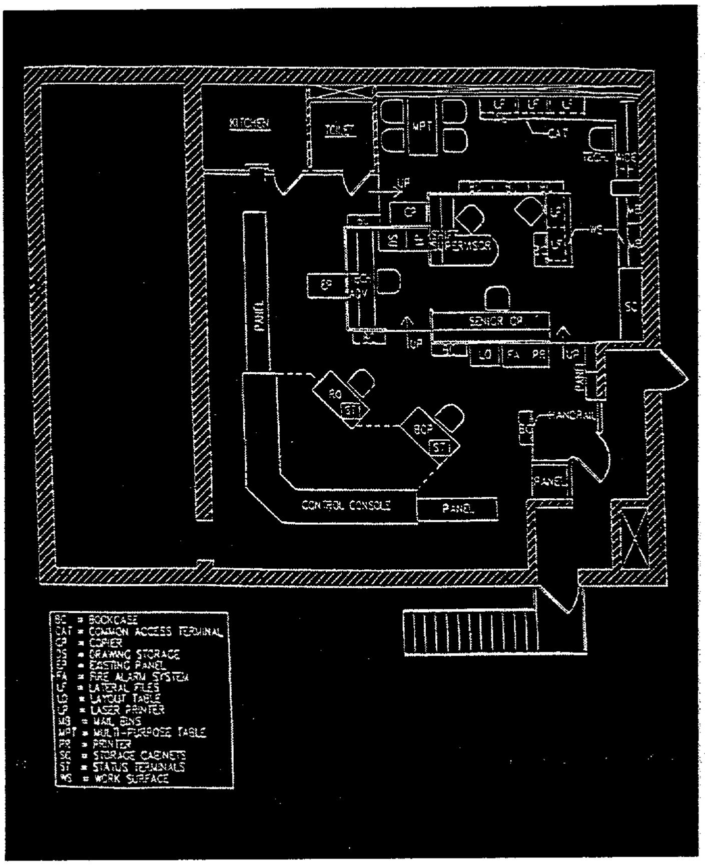


Figure 2: Control Room "X" Designed using Static Guidelines and Off-The Shelf Furniture

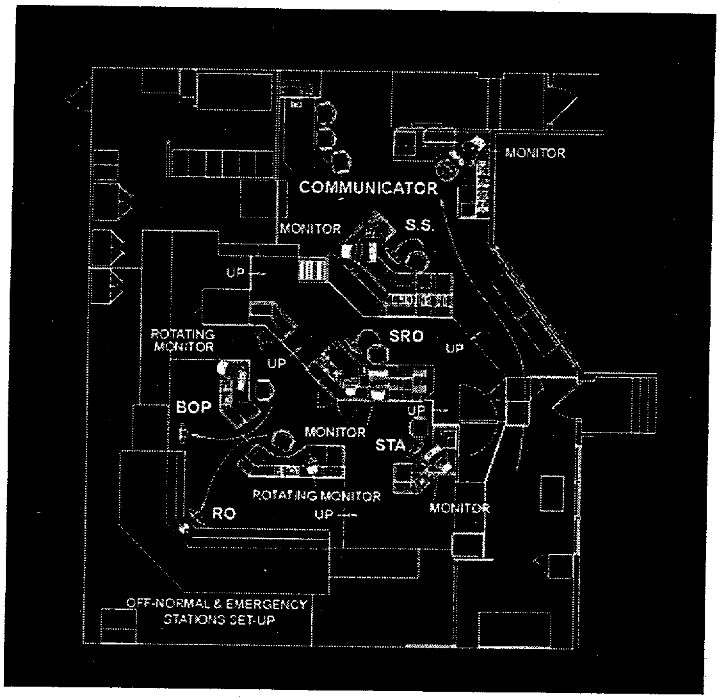


Figure 3: Control Room "X" Designed With Extensive Input and Custom Furniture

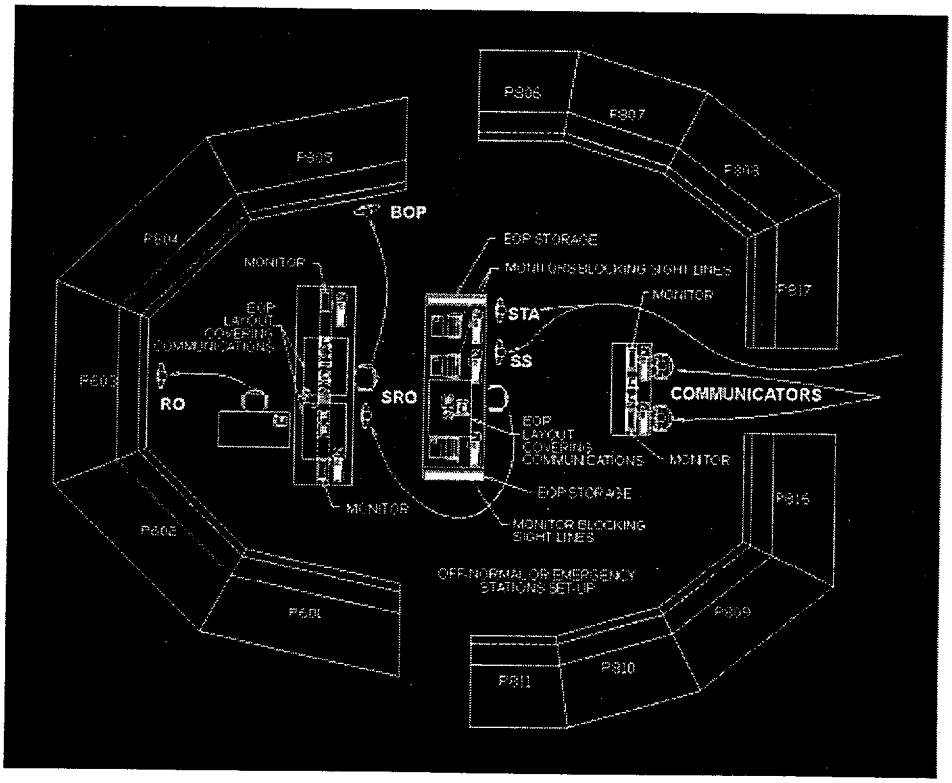

P806
P807
P805
P808
BOP
P804
EOP STORAGE
MONITORS BLOCKING SIGHT LINES
MONITOR
MONITOR
P817
EOP LAYOUT COVERING COMMUNICATIONS
STA
SS
P803
RO
SRO
COMMUNICATORS
EOP LAYOUT COVERING COMMUNICATIONS
MONITOR
EOP STORAGE
MONITOR
P816
P802
MONITOR BLOCKING SIGHT LINES
OFF-NORMAL OR EMERGENCY STATIONS SET-UP
P801
P809
P810
P811

Figure 4: Control Room "Y" Designed using Existing Workstations

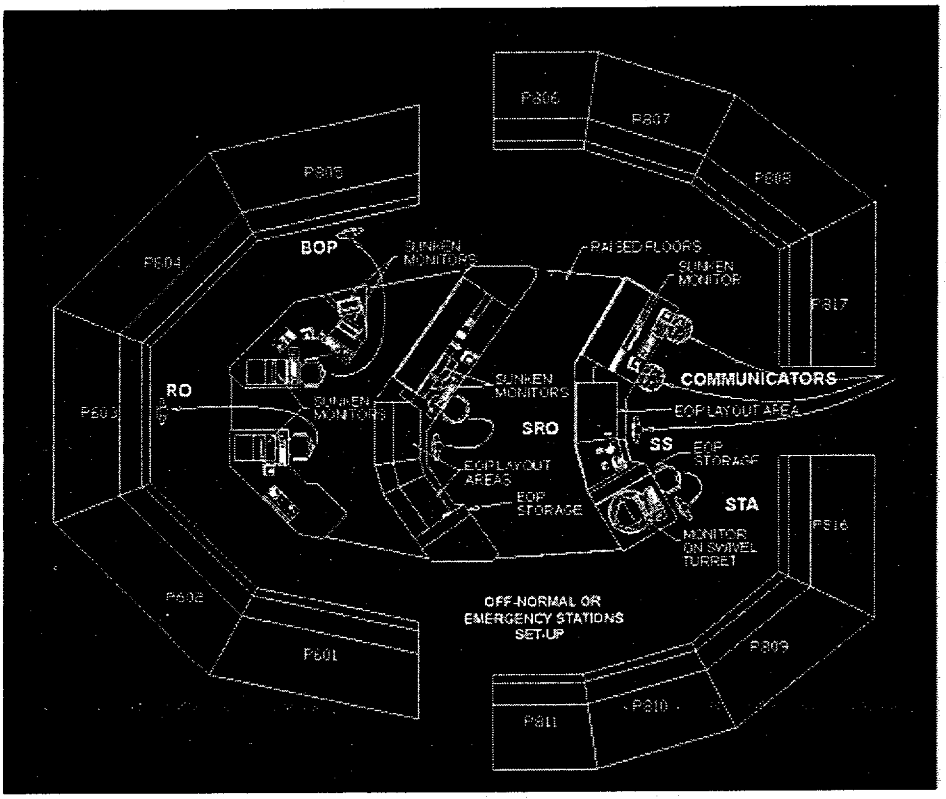


Figure 5: Control Room "Y" Designed With Extensive Operator Input and Custom Furniture

Design Approach of Soft Control System for KNGR MMIS

Jin-Koo Kim, Moon-Jae Choi, and Il-Nam Choe
Korea Power Engineering Co., Inc.

ABSTRACT

Among several advanced design features adopted in the Korean Next Generation Reactor (KNGR) design, the Man-Machine Interface System (MMIS) is one of the most distinguishing areas, since the technologies and design methodologies being implemented are completely new and notably different from those used in the conventional control room and control system design.

To overcome the inherent inflexibility of spatially dedicated MMI in conventional control rooms, computer based MMI technologies, along with compact workstation concepts, are adopted in the KNGR control room design. In order to achieve the compact workstation design, a large number of spatially dedicated control switches and manual/auto stations in a traditional control room have to be replaced by a few common multi-function devices. These control devices, so called Soft Control System, consist of a PC based Flat Panel Display (FPD) device with a touch sensitive screen which provides control MMI for the component selected among a number of plant components.

This paper describes the design features, operation and display design of the Soft Control System. The evaluation results of Soft Control System prototype is also presented in this paper.

1. Introduction

The KNGR Main Control Room (MCR) design is being developed by implementing advanced digital technologies. The Compact workstation-type operator consoles that can provide a convenient working environment to the control room operators facilitate operator's plant status information perception such that the operability and reliability can be enhanced and the human error rate can be diminished in great scale.

The KNGR MCR comprises the following operating facilities to support the operating staff in their goal of maintaining efficient and safe plant operation.

1) Three identical compact workstations
2) A Large Display Panel (LDP) to provide for overall plant operational and safety assessment
3) A safety console which provides control of all class 1E, safety-related components independently of the operator workstations.

Each compact workstation allows access to all information and controls necessary for one operator to monitor and control all processes associated with nuclear plant operation and safety. This includes both safety and non-safety systems. Each workstation contains one dedicated alarm CRT, three information CRT's to support process monitoring or computerized procedures, and three touch sensitive FPD's used as Soft Controllers for process and component control.

The Control MMI of KNGR consists of the Soft Control System, Operators Modules and fixed position switches. The Soft Control Systems are MMI devices to provide plant control capability for the control room operators. These devices replace conventional dedicated pushbuttons, indicators and M/A stations. The Operator Modules for each Control System channel provide diverse and independent backup to the Soft Control System. The fixed position switches provides the manual actuation or control capability to the operator during emergency conditions, and these switches further provide adequate diversity necessary for digital I&C system applications. (see Figure 1)

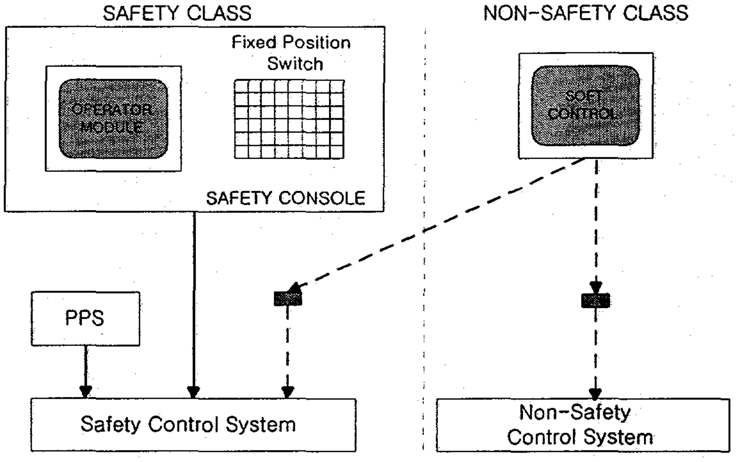


Figure 1. KNGR Control MMI Overview

This paper describes the design approaches and methodologies of the Soft Control System, and also explains the implemented results of soft control system prototype to verify the functional performance and design requirements of the Soft Control System.

2. Soft Control System Design Description

2.1 Soft Control System Overview

The Soft Control Systems are MMI device to provide plant control capability to control room operators and replaces the conventional dedicated pushbuttons, indicators and M/A stations. The Soft Control System provides the ability to manipulate continuous and discrete control devices which are supported by Control System from single control device. The operator can control both safety and non-safety components by the Soft Control System. To insure that the operator has all information necessary for optimal process control, continuous display of all controlled parameters is provided on Soft Control display.

The Soft Control System utilizes multi-function, touch sensitive FPDs to emulate the various physical switches and analog control devices which populate conventional plant control panels. The operator interfaces with the FPD via the touch sensitive screen.

Three (3) Soft Controllers are provided on each operator workstation (RO, TO, CRS) in the MCR and on the Remote Shutdown Console (RSC). Each of the three (3) Soft Controllers interface with information CRTs which are used for plant monitoring or computerized procedures on the control workstation. Typically, one (1) of those information CRTs can be used for a Computerized Procedures while the other two (2) CRTs can be used for plant monitoring. Also, one (1) Soft Controller is provided on safety console to support the operator task of Assistant Reactor Operator (ARO) in post trip conditions as a means for controlling non-safety related equipment.

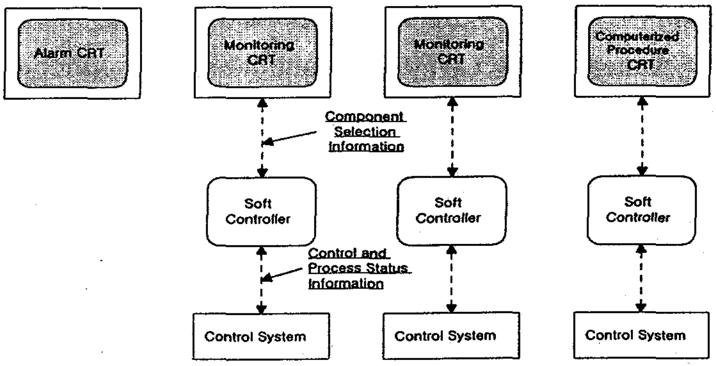


Figure 2. Configuration for One (1) Operator Workstation

2.2 Basic Requirements

No credible failure on the safety side of an isolation device shall prevent any portion of the safety system from meeting its minimum performance requirement during and following any design basis event requiring that safety function.

2.3 Soft Control System Components

The Soft Control System consists of five components as follows (see Figure 3); Soft Controller, Channel Selector, Control Gateway, Channel Confirm Switch and Fiber Optic Modem.

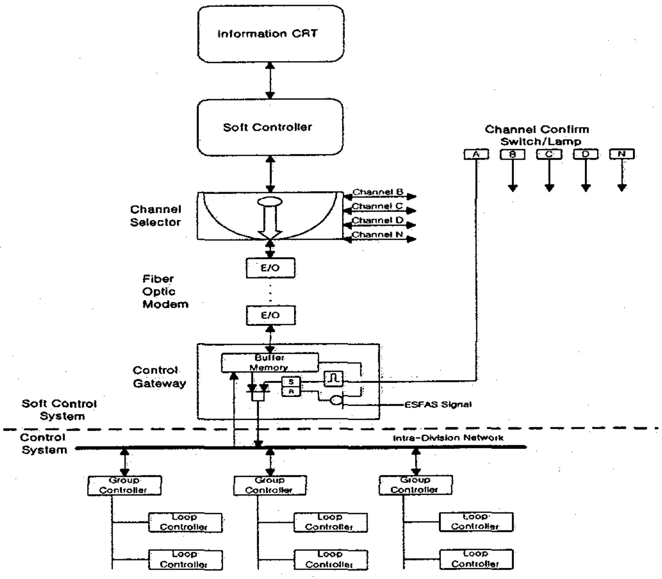


Figure 3. System Configuration of Soft Control System

Soft Controller - The Soft Controller consists of a FPD and supporting computer(s). It works in conjunction with a CRT-based control workstation for component selection. After the Soft Controller receives a component ID from the Information CRT it compares the ID to an internal lookup table. The Soft Controller provides the corresponding control template on Soft Controller. Through this display template, the operator gives control commands (i.e., on-off, increase, decrease, etc.) and receives feedback. The Soft Controller outputs to the Channel Selector are a channel select code, a component ID, and a control action command.

Channel Selector - The Channel Selector consists of hardware-based switching device (i.e., no microprocessors) connecting one component channel at a time using AND, OR, or other comparable passive logic components. The Channel Selector decodes this addressing signal and makes a connection to the related channel.

Channel Confirm Switch – Channel Confirm Switches are class 1E qualified push-buttons or comparable switches which are separated and independent from the Soft Controller. Five Channel Confirm Switches are provided for each Soft Controller, one per each safety channel and one for the non-safety channel. The Channel Confirm Switch provides clear definition of channel separation and independence. The activation of the correct channel confirm switch permits sending the control enable signal to the intra-division network where the control component is connected.

Control Gateway – The Control Gateway receives Soft Controller output from the Channel Selector, confirmation output from the Channel Confirm Switch and ESF signals. When Control Gateway receives the component ID signal from the Soft Controller it returns the related component data to the Soft Controller. Once the Control Gateway receives the controller's command signal, it is then necessary for the operator to confirm the command. Once confirmed, the Control Gateway will pass the command signal to the intra-division network of Control System. The command signal from Soft Controller is automatically overridden if an Engineered Safety Feature Actuation signal is received from Plant Protection System (PPS) or if Control Gateway detects physical break error or logical break error in Soft Control System.

Fiber Optic Modem - A Fiber Optic Modem passes the Soft Controller commands and component identification from the Channel Selector to the Control Gateway. A fiber optic modem provides the function of electrical isolation between Channel Selector and Control Gateway.

3. Significant Feature of Soft Control System Design

Common Mode Failure (CMF) of the Soft Control System software : The non-1E Soft Control System provides control signals to both the safety equipment and the non-safety equipment. Since the Soft Control System provides a common interface for all non-safety control signals, it is necessary to evaluate the potential impact of a common mode failure of software used in the Soft Control System. As a coping method for a common mode failure of software, the Soft Control System shall provide other solutions which do not compromise the basic CMF protection which provided by the diverse between safety and non-safety systems. CMF switches based on SECY 93-087 Position 4 provides protection against common mode failure including the failure of Soft Control System software. These switches perform system level controls for safety functions in order to provide sufficient means to bring the plant to a safe shutdown condition.

Failure of Soft Control System : The safety console contains class 1E controls for all safety related components independent of the Soft Control System and provides the capabilities of safe shutdown. The KNGR Control is designed in order that any failure does not impact the automatic protection system actuation or manual safety control through class 1E MMI. Thus, if a failure of Soft Control System occurs, class 1E components are controlled by Operator Module and Fixed Position Control on safety console.

Limiting Impact of a Malfunction to the Safety System : *Logical Break-Before-Make Function (Class 1E)*: The signal from a Soft Controller is allowed to take effect on only one channel of the Control System at a time by using divisional enable by Channel Confirm Switch and disable by break detection logic in Control Gateway.

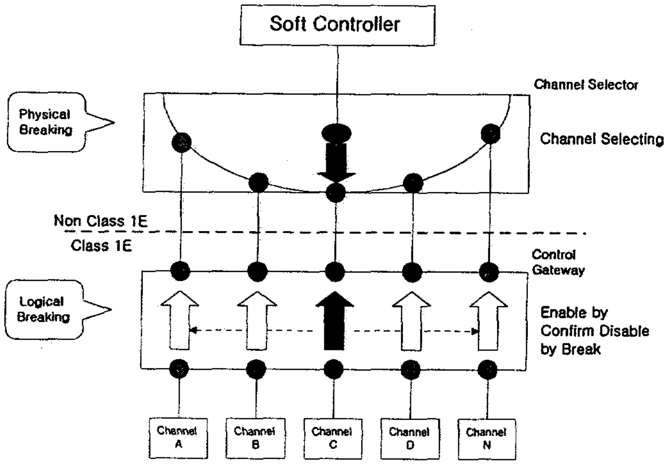


Figure 4. The concept of logical break and physical break

Physical Break-Before-Make Function: The signal from a Soft Controller is connected to only one channel of the Control System. The Channel Selector connects the communication lines between the Soft Controller to only one channel of Control System using an addressing signal from the Soft Controller.

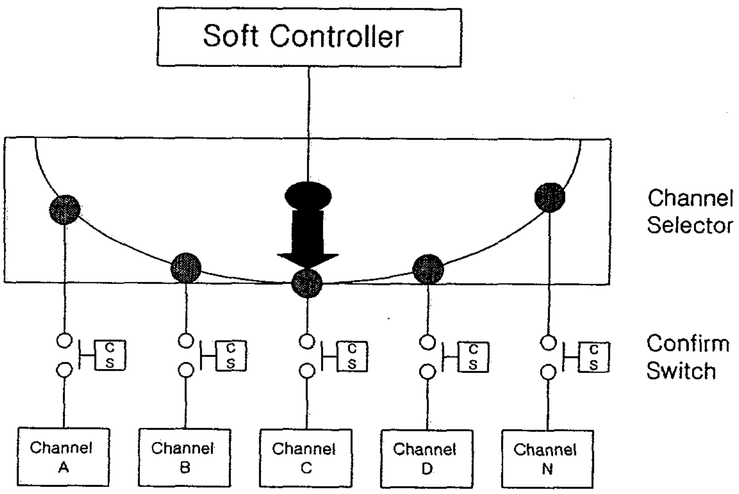


Figure 5. Connection between Channel Selector and Channel Confirm Switch

<u>Safety Function Performance Unaffected (Priority Interlock)</u> : The safety computer (Safety Control System) must be able to override the non-safety computer (Soft Controller) when the safety system is performing its safety function. Priority interlock is used to block any effect on ESFAS component control (system level) from the Soft

Controller during safety function performance. ESFAS signals from the PPS can override Soft Controller signals at any time. The actuation signal from class 1E fixed position controls can also override the component actuation from Soft Controller. Control signals from Soft Controller has the lowest priority.

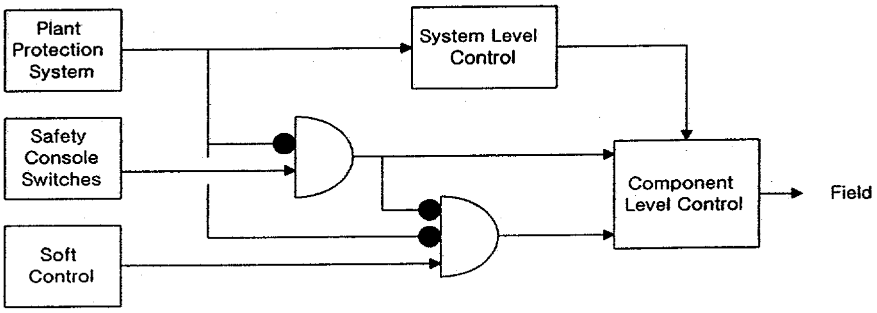


Figure 6. Priority Interlock

__Communication Isolation Between Soft Controller and Control System__ : The Control Gateway provides buffering circuits used to allow the handshaking between Soft Controller and one channel of safety Control System. This gateway is used to assure integrity of safety function by detecting and blocking 1) connection of Soft Controller to unintended channel of safety Control System, 2) communication malfunctions of Soft Controller impacting the safety computer.

__Isolation Between Soft Controller and Confirm Circuit__ : Independence of functional, physical, electrical interfaces between Soft Control System devices and the confirm circuit will be maintained. A 1E confirm circuit safeguards Soft Control System malfunction.

__Qualification:__ The Soft Controller and Channel Selector is qualified seismically and environmentally, and the software for the Soft Control System will be qualified important to safety. The confirmation circuit, Control Gateway and fiber optic modems shall be designed as safety.

4. Soft Control Display Configuration

Soft Control displays are dynamic, interactive graphics display devices used by plant operators to monitor and manipulate process control functions. Each Soft Control display has an interface to the Information CRT that is used by the operator to call up a control by selecting a component on the display. The Soft Control display graphic of a specific component comes out when the operator selects the symbol on the Inf*ormation* CRT by using a trackball. The Soft Control displays are provided on the Soft Controller to give the operator the ability to control plant process control loops. Each Soft Control display is designed for its specific application in accordance with standardized graphic templates to provide design and operational consistency. This design approach minimizes potential for operator-induced process control errors.

Soft Control displays are designed to be user friendly in accordance with Human Factor Engineering (HFE) principles delineated in NUREG-0711, -5908, and –0700 Rev. 1.

The Soft Control display facilitates the control and monitoring of process control functions. The standardized display is divided into two standard sections; A Display Window that provides process information display and component selection, and Control Window that provides component control template. (See Figure 7).

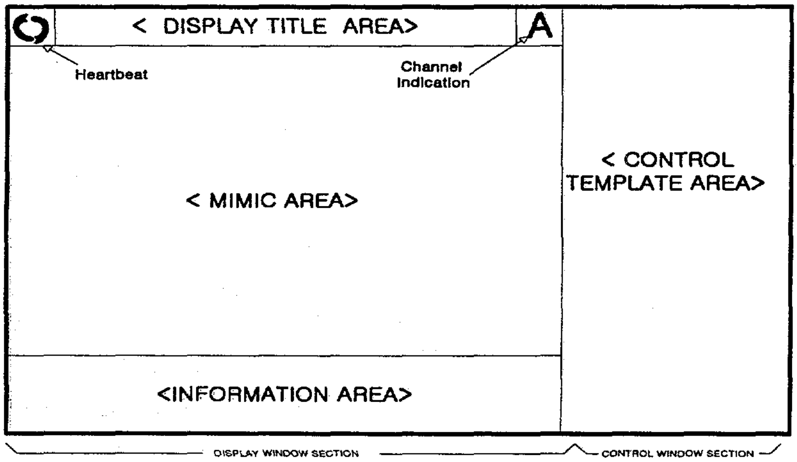


Figure 7. Soft Control Display Basic Format

Display window : A display window provides process mimic, component control target, process status/condition for component groups, data associated with the process represented, and helpful information for understanding the process. The Display Window consists of title area, mimic area and information area.

In the Display Window the top line is its title line. The title of the display page is centered. “Title” is the name of the current display page and the title name is determined based on process system or function. The Mimic area is a graphical representation of flow process or control loop signal line that the user operates and monitors. In this area the operator can see the component status to be controlled or monitor desired process data. In addition to these display-related functions, it is also possible for the operator to execute such functions that open the control window for the component control using touch targets. The major process information for the selected component group, e.g., main steam flow, steam generator level, feedwater flow etc., are dynamically provided in information area.

<u>Control Window</u> : The Control Window is changed upon operator demand based on touch target selection from the Display Window. The Control Window displays the control templates for modulating and discrete control. The Control Window for modulation control provides loop operating mode (i.e., AUTO, MANUAL), remote/local, setpoint, demand output, process value, increase/ decrease button and bargraph. The Control switch provides open/start button, close/stop button, auto/man selection switch, inoperable indicating lamp and exercise button, etc, necessary for the control of discrete devices. Some touch targets such as start (open)/stop (close) on the Control Window has a feedback indication for control demand and basically the feedback on the virtual switches and modulation controllers are the same as for a physical switch and modulation controller.

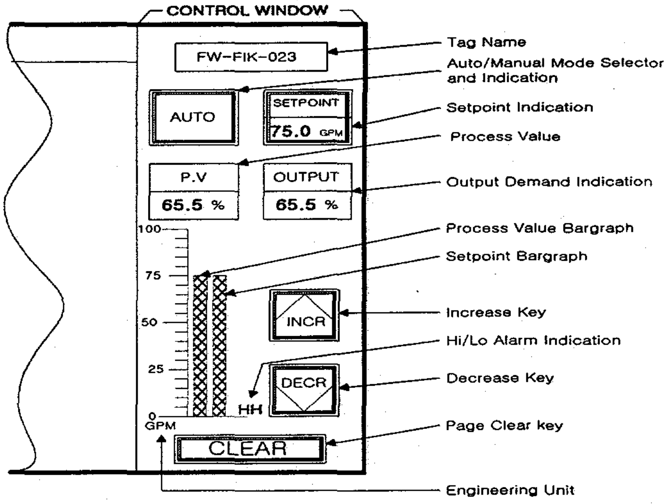


Figure 8. Typical Modulation Controller on Control Window

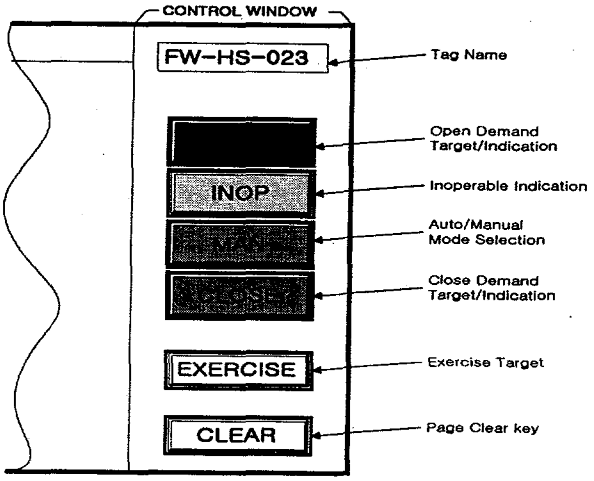


Figure 9. Typical Control Switch for On-off Valve

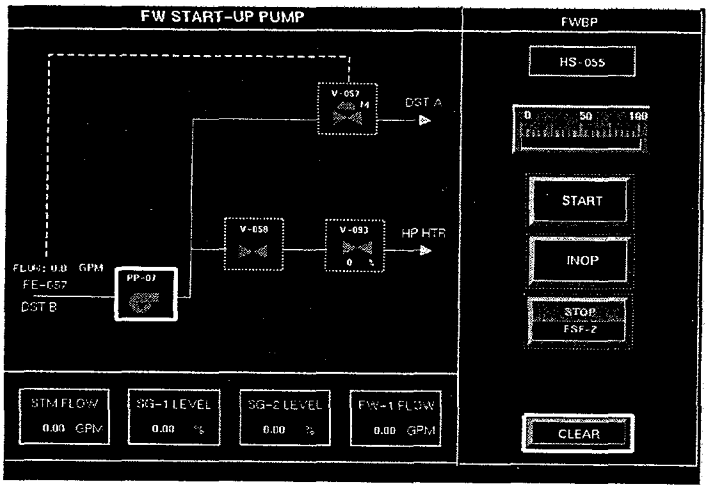


Figure 10. Typical Soft Control Display

5. Soft Control System Operation

When the operator selects the symbol of a component on the plant Information CRT by the trackball, a control display associated with the selected plant component appears on Soft Controller.

The Soft Controller sends the related channel address (A, B, C, D and N) to the Channel Selector. The Channel Selector decodes this addressing signal and makes connection to the related channel.

When the channel connection is obtained, the Soft Controller requests the component related information (current status, output, set point, etc.) from the Control Gateway.

On the Soft Controller display screen, related component information is displayed dynamically (on-line).

The operator confirms that the correct control template is selected on a Soft Controller using the Channel Confirm Switch.

The Control Gateway receives this confirmation signal and after a check of signal validity, it links the Soft Controller with the related sub-controller of the Control System.

The operator selects the control action type at the Soft Controller screen. (on-off, raise-lower, increases-decrease, auto-manual, etc.).

The selected component control command is transmitted to the component control circuit in the sub-controller of Control System.

The related component in the field is actuated and the feedback information is sent back to the Soft Controller through the Control Gateway.

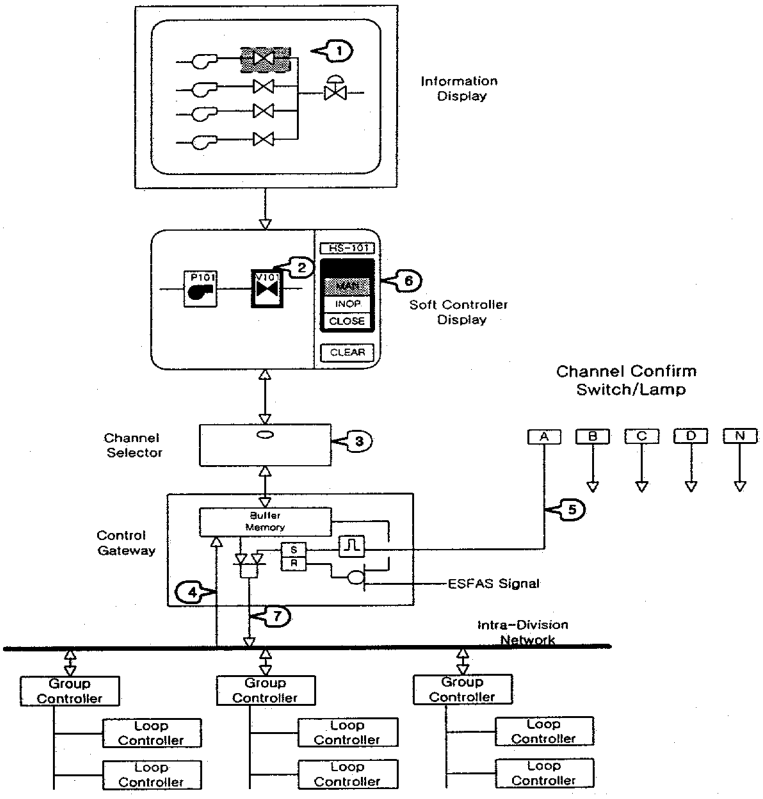


Figure 11. Operation Procedure of Soft Control System

6. Soft Control System Prototype

Based on the design features of the Soft Control System, a prototype of Soft Control System has been implemented to verify the functional performance and design integrity of the system.

The prototype of the Soft Control System consists of workstation-based Information CRT, Soft Controller, Channel Selector, Control Gateway, Channel Confirm Switch and Fiber Optic Modem. The system configuration diagram for the prototype is shown in Figure 12. In the actual design the Soft Controller shall interface with five channels (A, B, C, D, and N) of a Control System through separated Control Gateways. Two channels of safety Control System (A, B) and one channel of non-safety system (N) have been implemented for the prototype for the functional validation between Soft Controller and Control System.

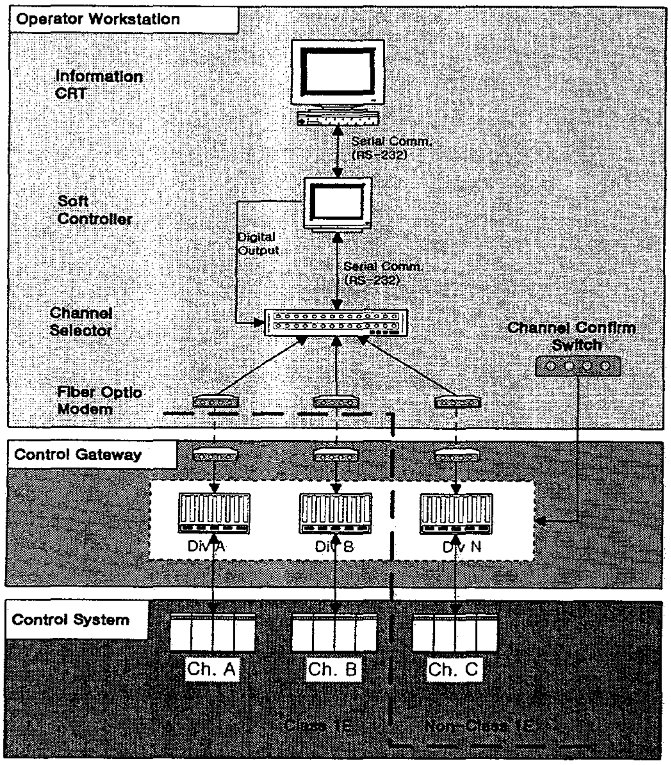


Figure 12. Configuration Diagram of Soft Control System Prototype

The Information CRT is implemented by a Hewlett-Packard workstation, and the Soft Controller is implemented by a Pentium II class computer with FPD. The Channel Selector consists of the passive switching devices, and the Channel Confirm Switches are implemented by a push-button with lamp. ABB AC-110 PLC is used for safety Control Gateway and Control System, and Modicon Quantum PLC is used for non-safety Control Gateway and Control System.

This prototype assures that the Soft Control System can be successfully operated in accordance with the design features and assures that the available implementation technology is adequate. Additionally, a Failure Mode Effective Analysis (FMEA) as described in IEEE-352 (Reference 3) has been performed for the Soft Control System prototype. The goal of FMEA for the Soft Control System prototype is to determine whether credible failures could adversely affect more than one safety channel within the safety Control System. Through performing of the FMEA, the design approach of Soft Control System has shown that there are no credible failures which could prevent performing the safety function of Control System.

The quantitative reliability analysis is also performed by system modeling using the reliability block diagram methodology. The total MTBF of the Soft Control System prototype is calculated as 28,029 hours (1,167 days).

7. Conclusion

The design approach of the KNGR Soft Control System provides the advantage of allowing operators to access all plant controls from a single workstation (since the Soft Control display are re-configurable) and also simplifies hardware configuration and maintenance. It is, however, necessary for the operator to perform the several operation steps to control the component through the Information CRT and Soft Control System. Thus, the design upgrade for Soft Control System is being reviewed by KNGR MMI team to find a solution to the reduction of the operating steps.

Through the prototype testing, the design features of the Soft Control System can were fully evaluated to verify their functional performance and to determine the interfacing features between the Soft Control System and Control System. However, the evaluation results show that the several Control Gateways were required. So, the design improvement should be considered for economical efficiency (i.e., reduction of Control Gateway quantity etc,) in order that the Soft Control System can be applied in the actual plant.

References;

1. URD Chapter 10 - Man Machine Interface System.
2. System Description for Component Control System for Nuplex 80^+ NPX 80-IC-SD640 Rev 0.0
3. Design Bases for KNGR MMIS Rev.0
4. Letter from the USNRC to GE Nuclear Energy, Subject: -staff position on Minimum Inventory of Fixed Position Controls, Display and Alarms for the Advanced Boiling Water Reactor (ABWR) Docket No. 52-001, date May 13, 1993.
5. SECY-93-087, "Policy, Technical, and Licensing Issues Preparing to Evolutionary and ALWR Designs"
6. IEEE-379, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety 1E Systems"
7. IEEE-384, "Standard Criteria for Independence of Class 1E Equipment and Circuits
8. IEEE-603, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations"
9. IEEE 7-4.3.2 "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"
10. Jin-Koo Kim, Moon-Jae Choi, and Il-Nam Choe, Design methodology for software design to implement advanced MMI, KOPEC Journal, Summer, 1999.

IAEA Specialists' Meeting on Human-Machine Interface for Off-Normal and Emergency Situations in NPP, Taejon, Republic of Korea, 26-28 October, 1999.

The Design of CANDU Control Centres in Support of Off-Normal and Emergency Situations

M.P. Feher
Atomic Energy of Canada Ltd. (AECL)
2251 Speakman Dr., Mississauga,
Ontario, Canada, L5K 1B2.
(905) 823-9040

Introduction

AECL has a program of evolving our CANDU design through the CANDU 6, CANDU 9 and Advanced CANDU development programs. All of these programs share a common set of design principles in the areas of control centre design and human factors.

The importance of the human's role in supervising and controlling complex systems like nuclear power plants and aircraft has been recognised internationally[1,2,3]. Based on observations and discussions with operations staff at PLGS and other CANDU plants, the human involvement in supervising and controlling CANDU plant operations can be characterised by five high-level statements:

- ***Plant operation is fundamentally goal-based.*** Nuclear power plants are designed to produce electrical energy in a safe and cost-effective manner. The plant control centres play the principal role in providing the information and controls necessary for the operating staff to achieve these two fundamental goals. If challenged, the safety goals of employee safety and protecting the public and the environment from danger due to plant operation shall over-ride the power production goal.
- ***Plant functions to support Operations must be performed by a combination of automated systems and humans.*** The two primary goals of maintaining safety and producing electricity cost-effectively are effected by a large number of inter-related lower-level functions. These functions are accomplished by the actions of both humans and automated systems. In practice, the performance of a specific function is accomplished via a shared division of responsibility between human operators and automated equipment rather than being allocated exclusively to one or the other. The control centres play the principal role of:
  - providing operators with information regarding the state of automated and shared plant functions,
  - alerting operators to changes in the state of plant functions, and
  - providing a direct means for operators to intervene in the plant process where and when required.
- ***Plant operation is supervised by human operators from control centres.*** Human operators are assigned the prime responsibility for all aspects of plant operation (i.e., achievement of safety and production goals). Operators supervise the status of plant goals and effect operational changes from control centres based on approved procedures. Operator communication with plant equipment and processes is effected through interfaces located in these control centres.
- ***Four principal strategies form the basis of operation of the plant processes: normal operation, abnormal operation, upset operation, and emergency operation.*** Each strategy outlines the sets of tasks and functions available for use by operators and the priorities that apply when using them.
- ***Combinations of four secondary strategies (maintenance, testing, fuelling, and commissioning) support each of the principal strategies.*** Each secondary strategy outlines the set of tasks/activities and functions available for use by operators and the priorities that apply when using them. The critical issues involved are the rules for initiating, terminating, completing or suspending each activity (e.g., during an emergency, maintenance activities are terminated) appropriate for each principal strategy and operating region combination.

[1] Sheridan, T.B.. 1987. 'Task Allocation and Supervisory Control'. In M. Helander (Ed.), Handbook of Human-Computer Interaction (pp. 159-173). New York, New York: Elsevier Science Publishers.

[2] Moray, N.P. 1988. 'Monitoring Behavior and Supervisory Control'. In K.R. Boff, L. Kaufman, and J.P. Thomas (Eds.), Handbook of Perception and Human Performance (volume 2) (pp. 40.1-40.51). Toronto, Ontario: John Wiley & Sons.

[3] Billings, C.E.. (1991). 'Human-Centered Aircraft Automation: A Concept and Guidelines'. National Aeronautics and Space Administration technical memorandum 103885, Ames Research Center, Moffet Field, California.

These principles have been used to support the evolution of the design of control centres through the identification of design improvements and enhancements. These improvements and enhancements are developed through co-operation with existing CANDU stations with many of them implemented/proved in full or part in Canadian CANDU stations or their simulators or in AECL's CANDU Control Centre evaluation facility to confirm effectiveness. This approach has resulted in design evolution of the CANDU 6 for Qinshan, China and have been further extended for the CANDU 9. Further extension of the proven design features as well as development of more novel design enhancements continue as part of future development of the CANDU product.

This process and the resulting design features were reviewed by the Canadian regulator, the Atomic Energy Control Board (AECB) in a pre-licensing review. During this time, the AECB concluded that "the human factors effort which has been applied to the CANDU 9 project to date has been acceptable according to standard human factors practice", and "the Human Factors Engineering approach taken in the design phase for CANDU 9 results in a better overall plant design."

The following sections of the paper will provide background to the definition of off-normal and emergency situations, and provide a framework for establishing requirements in support of operations. It will then describe some of the features that resulted from the application of this process.

Background on Off-Normal and Emergency Situations

At all times during the operation of a CANDU station, the operating staff uses one of a limited number of strategies to establish the operational priorities and the set of possible activities to perform. The four principal operating strategies (Normal, Abnormal, Upset, Emergency) and four sub-strategies (Maintenance, Testing, Fueling, and Commissioning) are represented in Figure 1. A description of each strategy follows.

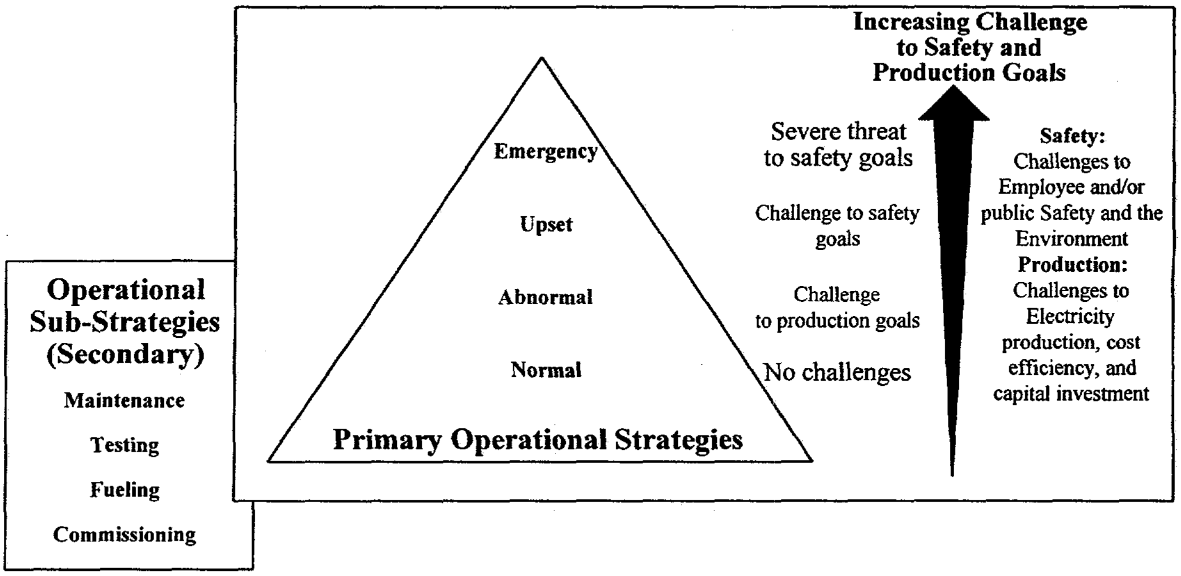

Increasing Challenge to Safety and Production Goals
Emergency
Upset
Abnormal
Normal
Primary Operational Strategies
Severe threat to safety goals
Challenge to safety goals
Challenge to production goals
No challenges
Safety:
Challenges to Employee and/or public Safety and the Environment
Production:
Challenges to Electricity production, cost efficiency, and capital investment
Operational Sub-Strategies (Secondary)
Maintenance
Testing
Fueling
Commissioning

Figure 1: CANDU Operating Strategies.

The conditions and boundaries for operating the plant are defined in specific station documents. Operating Policies and Practices (OP&Ps) establish the conditions and boundaries for safe plant operation based on an interpretation of the plant safety analyses. OP&P limits are proposed by the utility with designer input and approved by the regulator. Operating Manuals (OMs) provide a more conservative and restrictive definition of the station operating envelope. OMs also specify the manner in which reliability tests are to be conducted to confirm that poised systems are available to perform their function if demanded to do so.

The following are descriptions of each of these operational situations:

- Normal operation represents activities directed at maintaining the power production goals and safety margins of the plant and includes all phases of operations from shutdown, normal plant start-up, power production, planned plant shutdown and outage management. Operators supervise overall plant operation and automation controls process parameters to setpoints. Operators run the plant by executing actions in written procedures supplemented by training and experience. Approved procedures are organised in Operating Manuals (OMs).
- Abnormal operation represents the strategic response to challenges to production goals, typically on a single system/function/component basis (e.g., deaerator level control valve failure). Operators continue to supervise overall plant operation and automation continues to control most process parameters to setpoints. Operators respond to the disturbance by executing actions in written procedures supplemented by training and experience. Approved procedures and alarm responses are organised in OMs.
- Upset or Emergency - Canadian CANDU utilities have formalised the strategies to be used by operations personnel in responding to plant upsets and emergencies. The difference between the upset and emergency response is primarily the degree to which safety goals are challenged. For these strategies, the severity of the threat to the safety goals is characterised by the use of Critical Safety Parameters (CSPs). These parameters assess the reactor power level, the adequacy of fuel cooling, and the integrity of the heat transport system and containment.
  - The upset response strategy is normally used as a result of an unplanned but postulated event such as a total or partial failure of a single process, special safety or a safety support system. Operators would usually stop execution of normal/abnormal operating procedures in favour of an Emergency Operating Procedure (EOP). The CSPs are not challenged but may be trending towards unacceptable values. Event-based EOPs are typically used to restore the plant to a point where an Abnormal or Normal operating strategy can be applied.
  - Emergency response is used as a result of an unplanned and perhaps unpostulated event that leads to an increased uncertainty as to the plant safety state (Myles, 1992):
    - some CSPs become unacceptable, implying a severe threat to the safety goals, and
    - execution of an event-based EOP is not effective to restore the plant to a point where an Abnormal or Normal strategy can be used, due to the failure of more than one function or system.

    Operators would normally be required to stop the execution of event-based EOPs, or any other procedure, and address safety goals from a first principles basis (i.e., symptom-based approach). A symptom-based EOP serves this role and is supplemented by specific procedures for restoration of CSP values to acceptable safe ranges.

Framework for Discussing Support for Operations

AECL has established a design program that integrates Human Factors Engineering processes with the standard engineering design process. The approach entails the creation of Human Factors Program Plans to guide the Human Machine Interface design aspects of CANDU projects. The programs support the overall mission of enhancing the operational effectiveness of CANDU designs to meet evolving customer needs. As part of this program, AECL has increased up-front integration of the Off-Normal and Emergency Response requirements into the design process.

To discuss the concept of design for operation in off-normal and emergency situations we need to first present a brief discussion of the framework for designing for operation. A good model to be used is presented in Figure 2[4].

Brief descriptions of key points associated with some of the elements relevant to the focus of this paper are:

- Underlying Operating Philosophy
  - AECL, as with most nuclear plant designers, use a fundamental concept of Defence in Depth. This philosophy provides for design features that result in redundancy and/or diversity of critical or key systems or components related to safety or protection of high capital cost items. The result is the ability to provide functional replacement for failed systems or components to retain the barrier or to provide a new barrier should one fail. Other design philosophies included 2 of 3 voting logic to protect

[4] Howlett II, H.C. 1995. The Industrial Operator's Handbook: A Systematic Approach to Industrial Operations.

against spurious signals and grouping and separation of components to eliminate common cause failures that lead to safety challenges.

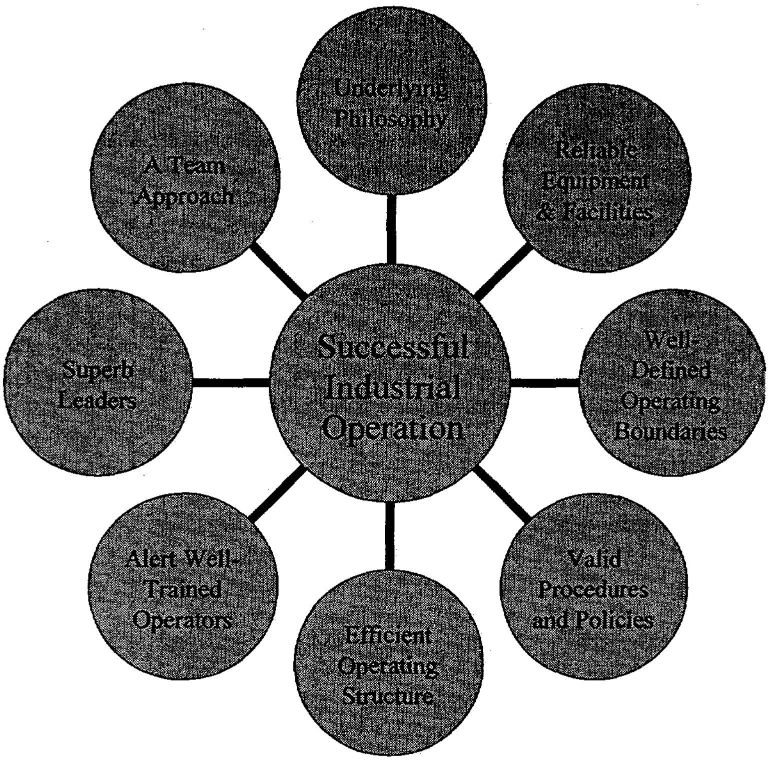

Underlying Philosophy
A Team Approach
Reliable Equipment & Facilities
Superb Leaders
Successful Industrial Operation
Well-Defined Operating Boundaries
Alert Well-Trained Operators
Efficient Operating Structure
Valid Procedures and Policies

Figure 2: Elements of a successful operating strategy[4].

- Well-defined Operating Boundaries/Valid Procedures and Policies
  - Operating Canadian CANDUs have licensed Operating Policies and Procedures that define the limits and bounds of operation. These boundaries clearly define the bounds and the rules that apply should these boundaries be exceeded for any reason.
- Efficient Operating Structure
  - "No operating strategy can succeed without a functional operating structure. Efficient group interaction, successful problem-solving, and more importantly, effective problem prevention are acutely dependent upon developing the right team structure to manage the organisation's mission"[4]. AECL has chosen to build on successful operating experience of one of its Canadian CANDU 6 stations as well as incorporating good practice from other Canadian CANDU stations.
- A Team Approach
  - "There are at least three major reasons for creating a team. Teams can accomplish more than individuals acting alone, teams can usually solve problems better than individuals, and teams offer mutual encouragement to their members"[4]. Although many of the elements of teamwork are non-design related, the ability of teams to work effectively and efficiently can be enhanced by a well-designed environment.

Each of these basic factors that influence design contribute to the success of operating under uncertain or complex situations typical to off-normal and emergency conditions.

Design Features in Support of Off-Normal and Emergency Situations

Support for off-normal and emergency situations involves many aspects of the CANDU design. The human-machine interface (HMI) is one very important aspect of the design to support the operators' role as ultimate authority and responsibility for the operation of the station.

Since the design of a nuclear station precedes its operation, AECL has predefined an operating structure based on successful organisational structures in existing CANDUs. This structure is explained in the Operational Basis and is used to support definition of requirements and features that directly support the Operating Structure to achieve the operational goals. This results in requirements for several aspects of the HMI including:

- facilities (e.g., rooms),
- equipment (e.g., controls, displays, consoles, communication devices),
- procedures,
- appropriate information content, and
- organisation, location and layout of all of the above.

In the specific context of the control room layout for both the CANDU 9 and the CANDU 6 in Qinshan, the design had to consider the change in crew structure and response from Normal and Abnormal operating situations to Upset and Emergency situations. Figure 3 and Figure 4 present the two typical crew structures that need to be support under these two different situations.

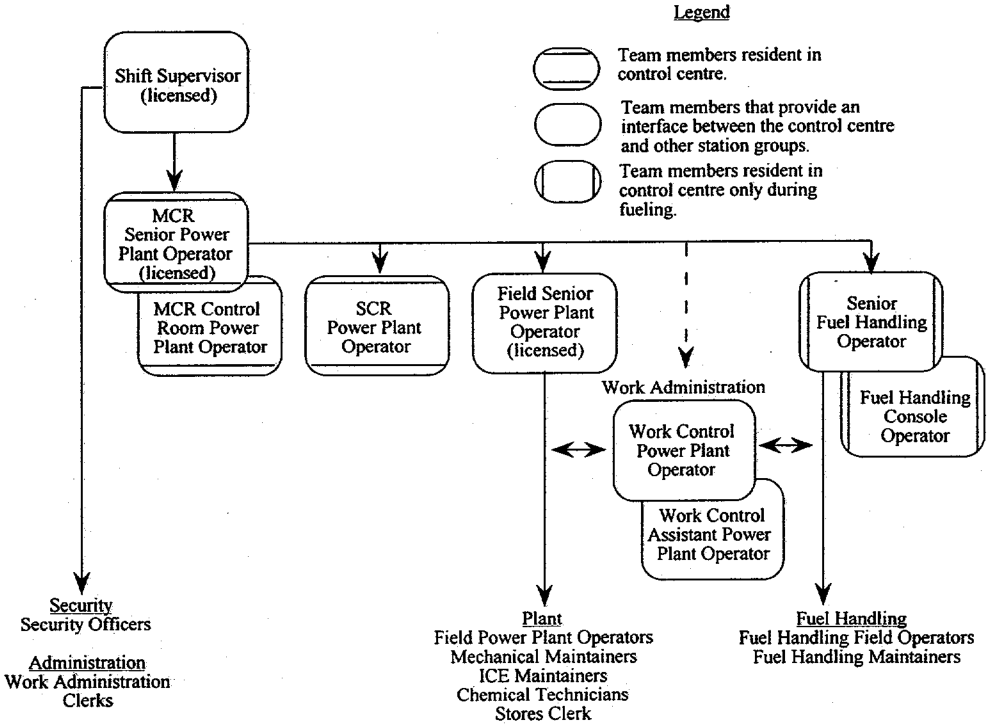

Legend
Team members resident in control centre.
Team members that provide an interface between the control centre and other station groups.
Team members resident in control centre only during fueling.
Shift Supervisor (licensed)
MCR Senior Power Plant Operator (licensed)
MCR Control Room Power Plant Operator
SCR Power Plant Operator
Field Senior Power Plant Operator (licensed)
Senior Fuel Handling Operator
Fuel Handling Console Operator
Work Administration
Work Control Power Plant Operator
Work Control Assistant Power Plant Operator
Security
Security Officers
Administration
Work Administration Clerks
Plant
Field Power Plant Operators
Mechanical Maintainers
ICE Maintainers
Chemical Technicians
Stores Clerk
Fuel Handling
Fuel Handling Field Operators
Fuel Handling Maintainers

Figure 3: Lines of authority for Normal and Abnormal operating strategies.

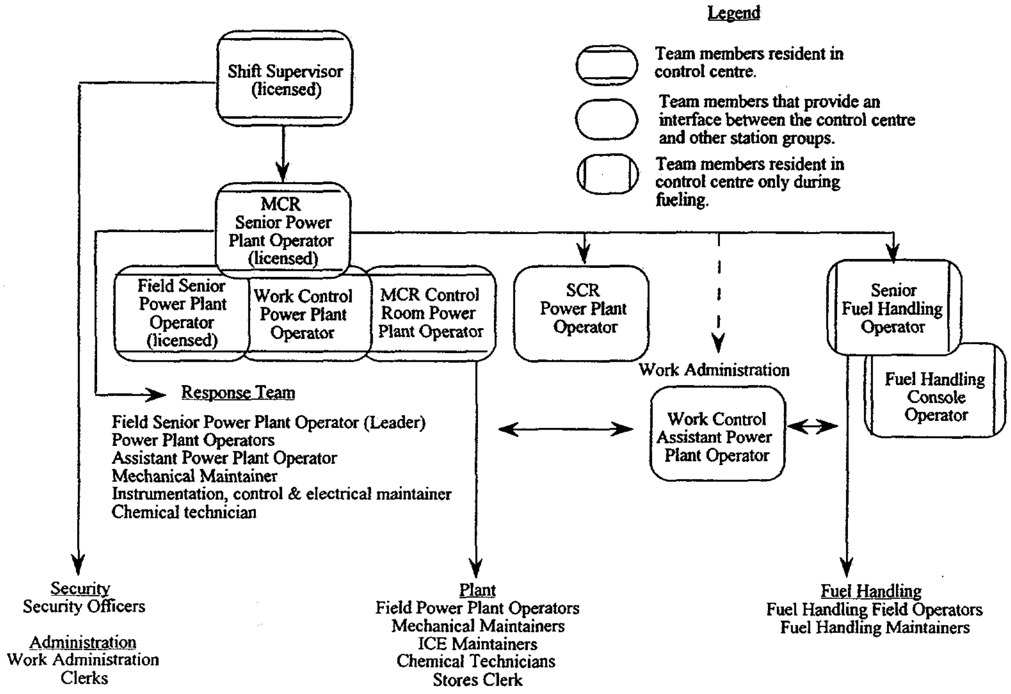

Legend
Team members resident in control centre.
Team members that provide an interface between the control centre and other station groups.
Team members resident in control centre only during fueling.
Shift Supervisor (licensed)
MCR Senior Power Plant Operator (licensed)
Field Senior Power Plant Operator (licensed)
Work Control Power Plant Operator
MCR Control Room Power Plant Operator
SCR Power Plant Operator
Senior Fuel Handling Operator
Fuel Handling Console Operator
Work Administration
Work Control Assistant Power Plant Operator
Response Team
Field Senior Power Plant Operator (Leader)
Power Plant Operators
Assistant Power Plant Operator
Mechanical Maintainer
Instrumentation, control & electrical maintainer
Chemical technician
Security
Security Officers
Administration
Work Administration Clerks
Plant
Field Power Plant Operators
Mechanical Maintainers
ICE Maintainers
Chemical Technicians
Stores Clerk
Fuel Handling
Fuel Handling Field Operators
Fuel Handling Maintainers

Figure 4: Lines of authority for Upset and Emergency operating strategies.

Support for these two different structures and the extended emergency response teams result in the need for and requirements imposed on the design of several facilities including the:

- Main control room,
- Work control area,
- Technical support centre
- Emergency operations centre, and
- the Emergency response centre.
- Secondary Control Area

The requirements include provisions for:

- adequate space,
- communications devices,
- procedures, drawings and other significant reference material,
- plant process information,
- team response and communication features (e.g., central room focus, common information sources)

Further, the Operational Basis includes the descriptions of the roles and responsibilities for each of these staff in different situations, including off-normal and emergency. These roles and responsibilities and the resulting tasks round out the source of requirements to be imposed on the design.

The following sub-sections describe specific design features that resulted from this process and are related to support for off-normal and emergency situations.

Control Room Layout

Some special design features of note related to the layout of the control room and related facilities include:

- Direct support for the Team Approach by providing
  - Large screen displays, centrally located in the control room to promote team monitoring and error-

catching and provide a common frame of reference for team communications (implemented in CANDU 6 China and included in CANDU 9).

- Capability to provide the entire suite of control room plant display system displays in real-time to the technical support centre and in near real-time to a remote Emergency Response Centre (~2 km away from the site). This provides a common frame of reference between the control room, the technical support centre and the emergency response centre in support of communication and decision making (implemented in CANDU 6 China and available for CANDU 9).

- Support for changing operating structure and associated responsibilities from Normal to Emergency Operation
  - Design of the Main Operators' Console to provide for both normal operations (plant monitoring and control and safety system testing) as well as upset and emergency operation (primary upset and emergency response and independent safety state monitoring) from the same furniture and display suites and layout for emergencies where the PDS is expected to be operational (non-seismic). (implemented in CANDU 6 China and extended support for CANDU 9).
  - Provision for dedicated technical support centre and emergency operations centre (implemented in CANDU 6 China and extended capability available for CANDU 9).

Plant Display System

Some special design features of note related to the layout of the control room and related facilities include:

- Providing information that relates the plant processes and performance to Underlying Operating Philosophy and the Operating Boundaries to the past, current and possible future plant state. In very complex systems, such as during emergencies and off-normal situations, this is known to be key to high performance of the system as a whole (people, processes and automation).
  - AECLs advance display suite is designed to support these concepts by providing a hierarchy of displays that starts at the top by representing larger plant goals and objectives with displays that integrate multiple systems and components designed to achieve particular goals. Further, the displays are designed to provide for integration of operating limits and boundaries and to integrate the alarm and health status of both systems and components as well as higher order functions into the displays. (A set of high level displays has been implemented for CANDU 6 Qinshan and have been extended to the whole display suite for CANDU 9). An example of such a display is the typical Critical Safety Parameter monitoring display (Figure 5).

    This display in Figure 5 is designed to provide a functional representation of the status of control, cool, and contain, the primary safety functions for the specific heat sinks of Steam Generators with or without Emergency Core Cooling. The display of the various parameters include alarm limits and visual alerts to parameters that have exceeded limits. These alarms are driven from the same source as the primary central alarm system and have the same characteristics (e.g., colour). Trends are used for key indicators to provide both past and current value as well as to provide for interpolation by the operator to predict possible future state. In addition to the primary indications, health indications are also provided where possible. For example, the state of source inventory for cooling is provided to support prediction of possible future challenge to the primary functions. (The CSP monitor display was developed in co-operation with Canadian CANDU stations and implemented in Pickering A and Pickering B CANDU stations. The design was extended and implemented for CANDU 6 Qinshan and CANDU 9 as part of the integrated display suite).

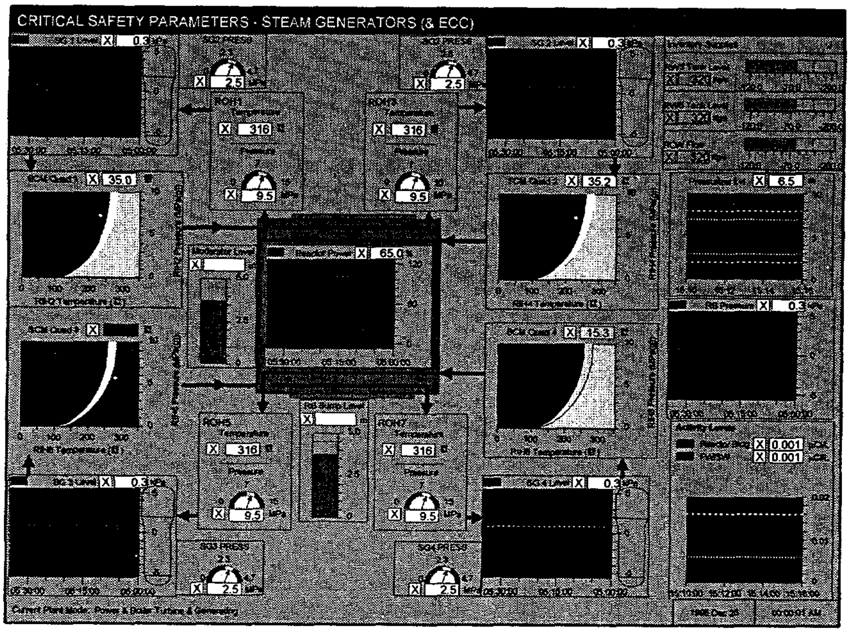
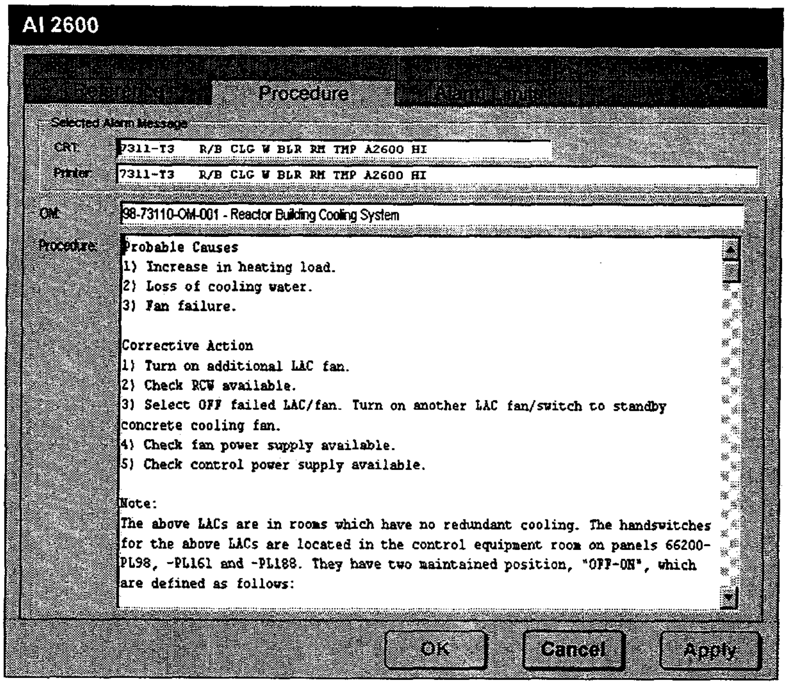


Figure 5: Typical Critical Safety Parameter Display.

- In addition to the primary display, objects on the screen are selectable for further interrogation or, where available, to provide for control of the component. Example object interrogation dialogues are provided in Figure 6 and Figure 7.



Selected Alarm Message

CRT: 7311-T3 R/B CLG W BLR RM THP A2600 HI

Printer: 7311-T3 R/B CLG W BLR RM THP A2600 HI

OM: 98-73110-OM-001 - Reactor Building Cooling System

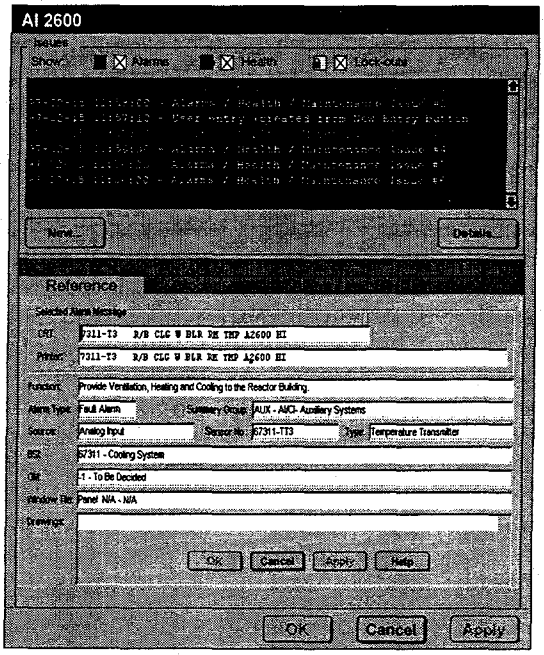
Procedure:

```
Probable Causes
1) Increase in heating load.
2) Loss of cooling water.
3) Fan failure.

Corrective Action
1) Turn on additional LAC fan.
2) Check RCW available.
3) Select OFF failed LAC/fan. Turn on another LAC fan/switch to standby
concrete cooling fan.
4) Check fan power supply available.
5) Check control power supply available.

Note:
The above LACs are in rooms which have no redundant cooling. The handswitches
for the above LACs are located in the control equipment room on panels 66200-
PL98, -PL161 and -PL188. They have two maintained position, "OFF-ON", which
are defined as follows:
```

Figure 6: Example CANDU 6 Qinshan object interrogation dialogue–Reference Information.



AI 2600

Issues

Show: ☒ Alarms ☒ Health ☒ Lock-outs

```
[illegible] - Alarms / Health / Maintenance Issue #1
[illegible] 11:57:10 - User entry (created from New Entry button)
[illegible] - Alarms / Health / Maintenance Issue #4
[illegible] - Alarms / Health / Maintenance Issue #[illegible]
[illegible] - Alarms / Health / Maintenance Issue #[illegible]
```

Reference

Selected Alarm Message

CRT: 7311-T3 R/B CLG W BLR RM TMP A2600 HI

Printer: 7311-T3 R/B CLG W BLR RM TMP A2600 HI

Function: Provide Ventilation, Heating and Cooling to the Reactor Building.

Alarm Type: Fault Alarm Summary Group: AUX - AI/CI- Auxiliary Systems

Source: Analog Input Sensor No: 67311-TT3 Type: Temperature Transmitter

BSI: 67311 - Cooling System

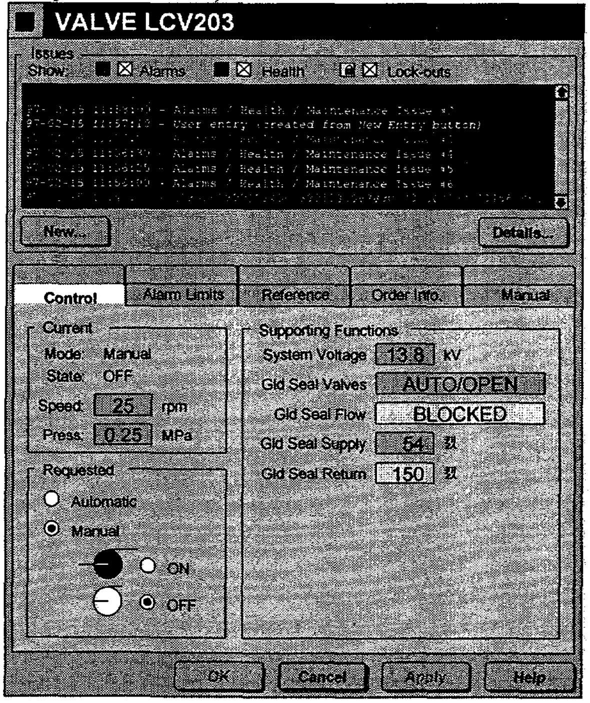
OM: -1 - To Be Decided

Window File: Panel N/A - N/A

Drawings:

Figure 7: Example CANDU 9 object interrogation dialogue – Reference Information.

The information provided in these dialogues support association of operating alarms and limits, reference drawings and procedures, and current and past alarm, health and maintenance state of the component, system, or function being interrogated. An example of a component/system control dialogue is provide in Figure 8. (This capability is partially implemented in CANDU 6 Qinshan and is extended in capability for CANDU 9).



VALVE LCV203

Issues

Show: ☒ Alarms ☒ Health ☒ Lock-outs

```
97-[illegible]-15 11:5[illegible] - Alarms / Health / Maintenance Issue #[illegible]
97-02-15 11:57:10 - User entry (created from New Entry button)
[illegible]
97-02-15 11:56:30 - Alarms / Health / Maintenance Issue #4
97-02-15 11:56:25 - Alarms / Health / Maintenance Issue #5
97-02-15 11:56:00 - Alarms / Health / Maintenance Issue #6
```

Control | Alarm Limits | Reference | Order Info. | Manual

Current

Mode: Manual

State: OFF

Speed: 25 rpm

Press: 0.25 MPa

Requested

○ Automatic

◉ Manual

○ ON

◉ OFF

Supporting Functions

System Voltage 13.8 kV

Gld Seal Valves AUTO/OPEN

Gld Seal Flow BLOCKED

Gld Seal Supply 54 [illegible]

Gld Seal Return 150 [illegible]

Figure 8: Example CANDU 9 object interrogation dialogue – Component Control.

The control dialogue is explicitly designed to support operators ensuring the objective of control will be achieved. This is done by providing not only the current and requested state of the component but also the related alarm, health and maintenance history and the state of variables key (support indications) to the ability of the device or system being controlled to meet its intended purpose. In this way, the operators are provided with everything that they need to know about a device or system before they perform the control action including the ability to monitor successful operation following the control action. (This feature is part of the extended capability for CANDU 9).

- Provide alarm information in a manner that supports operators tasks while providing the ability to process and manage large volumes of alarm information expected during off-normal and emergency situations.
  - AECLs advanced alarms system CAMLS (Computerised Alarm Message List System) provides for the presentation and manipulation of alarms to support operators effectively with this task[5]. A particular feature of interest is the creation of what are known as function-based alarms. These alarms represent higher order information for operators in support of understanding the state of the plant and planning response strategies. An example of a function-based alarm is LOSS OF CLASS IV POWER that indicates that conventional site power has been lost and battery back-up and then diesel generators are required to support primary process control and safe shutdown operation. This alarm is the logical and deterministic result of as many as 60 lower level alarms that individually have limited implications, but as a group have a much more significant impact on plant safety and performance. (CAMLS was implemented and validated in two Canadian CANDU plant simulators[6], is implemented in CANDU 6 China and is extended for CANDU 9).

The display and alarm systems are integrated into the overall operator information system that includes hardwired panels and indications, safety credited instrumentation, and control system displays and interfaces. Each of these systems work together to provide graceful transfer from one system to the next depending on the state of the plant and the ability of operators to restore the plant to a safe and stable state during emergencies.

Future Development

To further extend the capability of the CANDU product in the future, AECL is developing additional features either as further extensions to the existing capability in several key areas including:

- Operating Policies and Procedures (operating envelope) monitoring system integrated into the on-line display suite to provide both monitoring and indication of the required configuration that is sensitive to the operating state of the plant and the desired operational mission.
- Extension of the alarm system to provide for the monitoring of Emergency Procedure Entry Conditions as well as provision for continuos monitoring steps within the procedures. As procedures get more complex to address more and more postulated and uncertain situations, operators will need increased support for monitoring and detecting special conditions and prioritising selection of response procedures.

Such features will be considered for introduction to the CANDU 6 or CANDU 9 products when a sufficient level of confidence/proveness has been established.

Beyond Design Basis Accident Support

AECL is currently working towards specifying the approach to monitoring and control of the plant for beyond design basis accidents. The approach will draw heavily on the functional approach that is used to establish the content of various levels of the display hierarchy described earlier and apply it to the entire information system for emergency respose including beyond design basis accidents. A functional model provides for monitoring and control of the

[5] Davey, E.C. and Feher, M.P. 1995. 'An Improved Annunciation Strategy for Plants', Paper presented at the American Nuclear Society embedded topical meeting on 'Computer-based Human Support Systems: Technology, Methods, and Future', Philadelphia, Pennsylvania, 1995.

[6] Feher, M.P., Davey, E.C. and Lupton. L.R. 1996. 'Validation of the Computerized Annunciation Message List System', Paper presented at the IAEA topical meeting on 'Experience and Improvements in Advanced Alarm Annunciation Systems in Nuclear Power Plants', 1996 September 17-19, Chalk River, Ontario, Canada.

plant state independent of the actual event or situation. This relies heavily on understanding the functions available to control the plant and rules for move the plant to a stable state from any possible configuration. Detailed postulations of availability of systems and equipment to monitor and control the plant under previously undefined configurations or states are in progress to complete the translation to detailed design requirements and features.

Conclusions

AECLs CANDU Control Centres design has established a process that integrates human factors into the design early in the design. Support for off-normal and emergency situations is addressed as an integral part of the design and the resultant design features rather than add-on tools that are rarely used.

Our approach relies heavily on proven concepts and methods matched with direct support for the operating mission, staff roles and responsibilities, and operator tasks.

The features developed for both the CANDU 6 in China and the CANDU 9 are based on proven installations in operating Canadian CANDU facilities. The evolutionary model provides for continued extension of proven concepts to better support operational needs based on experience feedback from previous installations.

The process used for CANDU 9 was reviewed by our Canadian nuclear regulator and considered a step forward for the Canadian nuclear industry.

Operators of new CANDUs will benefit from significant enhancement in their abilities to remain up to date on the state of the plant and be able to respond more effectively during off-normal and emergency situations. Operators of existing CANDUs can benefit from upgrades to their designs using many of the same features while achieving similar benefits.

KNGR Display Design for Off-normal and Emergency Operation

Eung-Se Oh, Yeong-Cheol Shin
Korea Electric Power Research Institute (KEPRI)
103-16, Munji, Yusoung, Taejon
Republic of Korea

Robert B. Fuld
ABB-CE
Windsor, CT
USA

October 26, 1999

Abstract

The Korean Next Generation Reactor (KNGR) employs a state-of-the-art man-machine interface to support the operator and to mitigate problems in conventional control rooms. This paper provides a summary of KNGR display design features that are relevant to off-normal and emergency operations.

Introduction

The focus of Man-Machine Interface (MMI) design on off-normal and emergency conditions reflects the importance of the MMI to Nuclear Power Plant (NPP) safety. Besides responsibilities for operating efficiency and for protecting equipment investments, the human operator provides an indispensable level of the "defense-in-depth" that assures health and safety of the public. Although many efforts have been made to assure safety with minimal reliance on operator actions, there is also major continuing effort to improve the MMI (particularly for off-normal conditions) and thus to improve the operator's capability to safeguard the plant.

KNGR provides a state-of-the-art MMI based on digital technology. It has been developed via systematic, top-down design methods to mitigate problems of conventional control rooms using new MMI technology and proven design innovations. In the remainder of this paper, a summary is provided of KNGR display design features having particular relevance to off-normal and emergency operations.

Large Display Panel

A key concern in computer-based control rooms is the loss of a broad view of plant data on spatially-dedicated displays, and its replacement by narrow, inefficient serially-accessed views into a plant database. In KNGR, this issue is addressed by the alarm and display capabilities of the Large Display Panel (LDP). More than a continuous overview, the (length 27 feet x width 7 feet) LDP provides graphic representation of the major heat transport systems and systems that are required to support the major heat transport systems. These systems include those that require availability monitoring per Regulatory Guide 1.47, and all major success paths that support the plant critical functions. System information presented on LDP includes system operational status, change in operational status (i.e. active to inactive or inactive to active) and the existence of alarms associated with the system. Process variables required to assess the critical functions are also presented on LDP. It supports control room staff awareness of dynamic situations with a shared "big picture" of the plant.

The LDP exceeds NUREG-0737 Supplement 1 requirements for continuous safety parameter display, allowing direct assessment of the status of critical safety functions and the performance of associated success paths.

Alarm Display Features

When conditions depart from normal, alarms provide main alerting function to support rapid detection of anomaly. Alarm information in KNGR MMI is presented through 1) LDP, 2) dedicated Alarm CRT at each workstation, and 3) Alarm indications on IPS computer display pages. These redundant and diverse displays ensure that alarm information can be viewed in a manner (e.g. time-sequential, functionally grouped, systems-related, etc.) that suits the operator's understanding of or approach to a given situation.

General principles of KNGR display include that raw data should be processed as far as possible into useful information, and that non-informative indications should be minimized. Both are principles that pertain to standard criticisms of NPP alarm systems, e.g. that there are too many alarm indications during events (many of which are unimportant) so that it is difficult to identify and respond to the most important problems. In response, KNGR alarm processing employs prioritization, dependency logic, and grouping techniques to organize and support the operator's assessment of the situation.

Computerized Procedure System

Although KNGR should be licensed based on demonstrating successful operation with hardcopy procedures, a key advantage of computer-based control rooms is expected to be that operating procedures can be presented as integral dynamic displays. KNGR enters this era of electronic operating procedures with the Computerized Procedure System (CPS). The basic advantage of the CPS display for off-normal conditions is that probability of human error in procedure execution is reduced. Advantages of the CPS include 1) presentation of dynamic plant data in the 'pages' of the procedure, 2) computer monitoring of continuously applicable procedure steps, 3) computer shadowing/confirmation of operator decisions, 4) computer call of selected component controls and 5) links to the page of supplemental information for the procedure execution. The increased support and constraint provided to the operator by the CPS ensures increased reliability of procedure execution under stressful, off-normal conditions.

Other Computer-based Displays

A variety of computer-based display features are provided to support operator performance in both normal and off-normal conditions. The displayed data is provided by the Information Processing System (IPS) and a diverse Qualified Information and Alarm System (QIAS). Efficient navigation among displays is provided by flat hierarchies of display resources (directories) which are supplemented by hyperlinks between individual display objects. Typical access to any resource requires no more than two touches.

In most cases, displays are unconditionally applicable in all modes and conditions covered by the plant design basis. These displays include system mimic displays, critical function and success path monitoring displays, display directories (which also provide directing function during alarm conditions), and alarm response procedure displays. In some cases displays are supplemented by condition-specific information or logic. For example, all alarm indications benefit from algorithmic processing to reduce non-informative nuisance alarms; this may include the change of setpoints or the suppression of alarms based on plant mode or conditions.

Safety Console Displays

The Safety Console provides a set of spatially dedicated displays and controls that:

- meet Reg. Guide 1.97 requirements for post-accident monitoring,
- meet NRC diversity Position 4 (SECY-93-097) requirements for common-mode failure,
- are sufficient to execute emergency procedures.

In addition, channelized flat panel devices (operator modules) permit control of all remotely operable components of plant protection system, and a CRT display support is also provided.

Conclusion

The KNGR information displays can be characterized as an integrated display system. The high level plant functions are continuously monitored using LDP and detail level plant information is available at each CRT information display. All display design is performed per pre-defined HFE standards and iterative design process. Improved alarm presentation method and computerized procedure with soft control reduce operator's error likelihood at off normal plant situation. Each display design features are thoroughly evaluated for usability using full scope dynamic simulation. All these make KNGR significant advancements over conventional control room.

References

[1] Korean Next Generation Reactor Standard Safety Analysis Report Vol. 18, Rev 0, 1998.

[2] Korean Next Generation Reactor Standard Safety Analysis Report Vol. 7, Rev 0, 1998.

The Role of Computerized Procedure System in Facilitating Operator Performance during Off-Normal and Emergency

Joong Nam Kim, Yeong Cheol Shin, and Chan Ho Sung
Korea Electric Power Research Institute (KEPRI)
(jnkim@kepri.re.kr, ycshin@kepri.re.kr, and chsung@kepri.re.kr)

ABSTRACT

Changes of a plant state from normal to abnormal/emergency in nuclear power plants often provide opportunities of human performance degradation resulting from stress, workload, nervousness, as well as insufficient information synthesis and analysis. This type of performance deterioration may result in undesirable consequences and ultimately affect plant safety.

Computerized procedure is a type of man-machine interface (MMI) resource introduced in an advanced control room to facilitate operator tasks in situations where the use of operating procedures is needed. Among many types of computerized procedures, a special emphasis lies in abnormal operating procedures (AOP) and emergency operating procedures (EOPs) primarily due to the criticality of the situation—off-normal and emergency.

In KNGR (Korean Next Generation Reactor), the operator uses an electronic procedure called computerized procedure system (CPS) instead of paper procedure conventionally used. The KNGR CPS is more than a presentation of procedures on a VDU; it provides operator aiding functions such as automatic place keeping of procedure execution and automatic plant status monitoring.

This paper describes the key features of the KNGR CPS, which support main control room operator tasks during off-normal and emergency situations. The progress of the interface features that has been made during the development of the CPS is also described, and the new features are compared with the previous COPMA-like features. Strengths and potential weaknesses of those different features are also discussed.

INTRODUCTION

In nuclear power plant operations, procedures have been used as operating instructions and memory aids for operators. In general, operating procedures can be categorized into the following three—normal, abnormal, and emergency procedures. Among these three, abnormal and emergency procedures play an especially important role in safe operation of nuclear power plants.

Paper-based procedures have been used in a conventional control room for a long time, and the operator task of utilizing paper-based procedures are cognitively separated from the operator task of utilizing control room man-machine interfaces for plant monitoring and controlling. Although paper-based procedures have such advantages as simplicity and readability, they have many limitations in flexibility, place keeping, memory aids, and integration with monitoring and control tasks of operators.

As digital technology has been developed and computer-based systems have been introduced in nuclear power plant control rooms. Despite of many efforts to cope with the limitations of the paper-based procedures, there still have been many concerns about the use of computer-based procedures. According to studies about the comparison of reading performance on computer vs. typical hardcopy formats, "reading is generally slower and more fatiguing when performed using a VDU presentation" resulting from difficulties in "maintaining a sense of location (knowing where you are in a document), navigation (moving from one place in a document to another), and fatigue" (O'Hara, 1996).

KNGR (Korean Next Generation Reactor) is an effort to develop an advanced light water nuclear power plant with a significant safety improvement and cost reduction. For KNGR, the concept of an advanced control station is applied to the design of main control room (MCR). Computer-based man-machine interfaces for KNGR include: large display panel (LDP), operator workstations, soft controller, and computerized procedure system (CPS) (Figure 1).

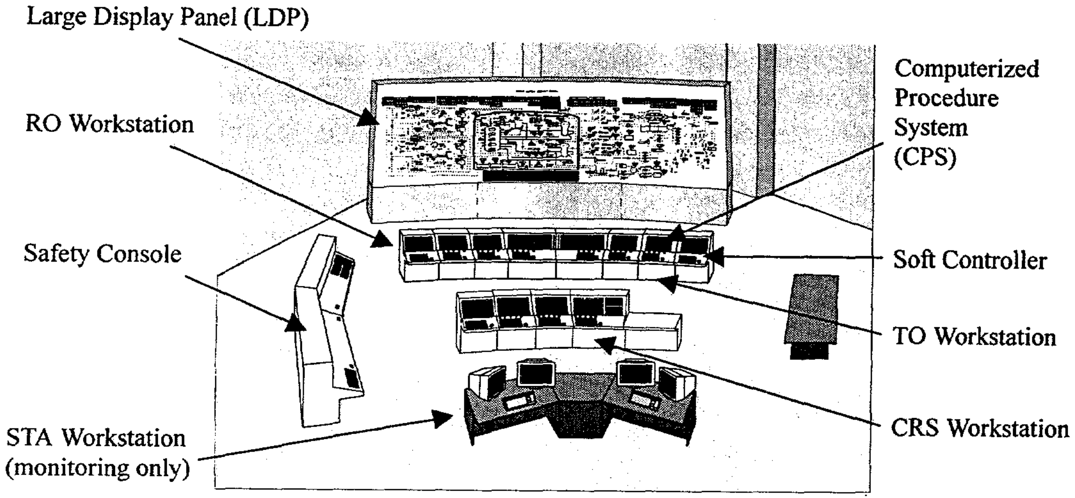

Large Display Panel (LDP)
RO Workstation
Safety Console
STA Workstation (monitoring only)
Computerized Procedure System (CPS)
Soft Controller
TO Workstation
CRS Workstation

Figure 1. Overview of MMIs in the KNGR MCR

DEVELOPMENT OF KNGR CPS

CPS (Computerized Procedure System) is a computerized procedure to be imbedded into the computerized workstations of the KNGR MCR. The location of the CPS display is the second right CRT in each of the operator workstations. However, it is technically possible to bring up the CPS display on any workstation CRT. In KNGR, the operator uses an electronic procedure called computerized procedure system (CPS) instead of paper procedures conventionally used, although the paper procedures are available in the control room as a backup in case the CPS fails.

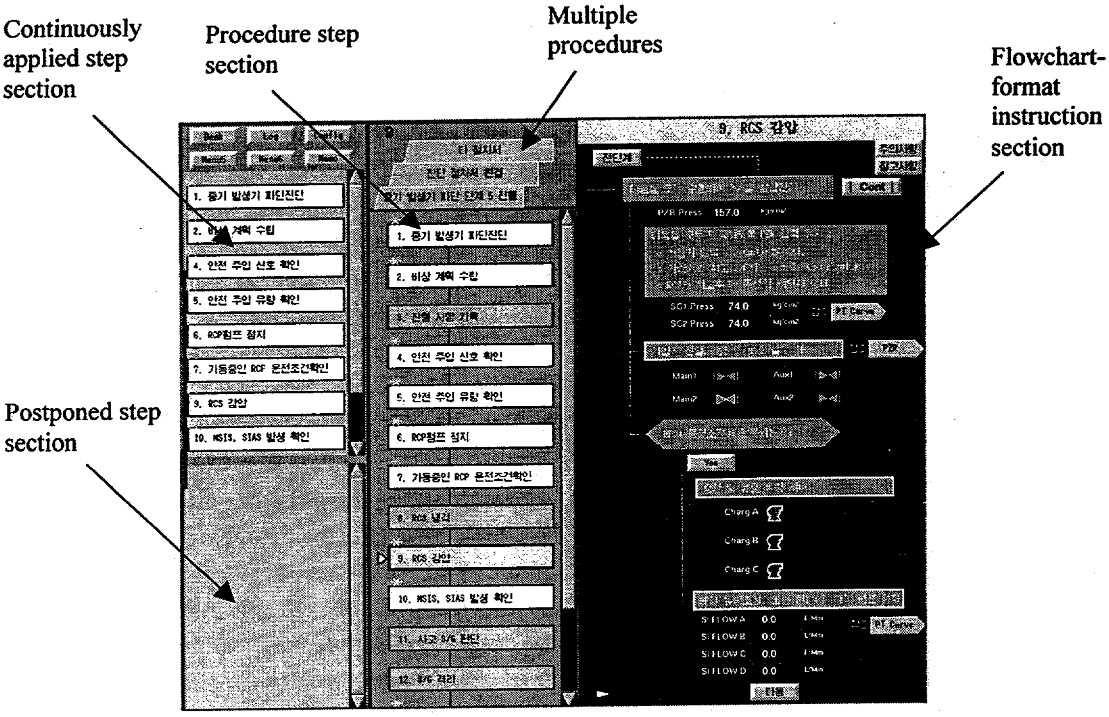


Figure 2. A Snapshot of CPS Display

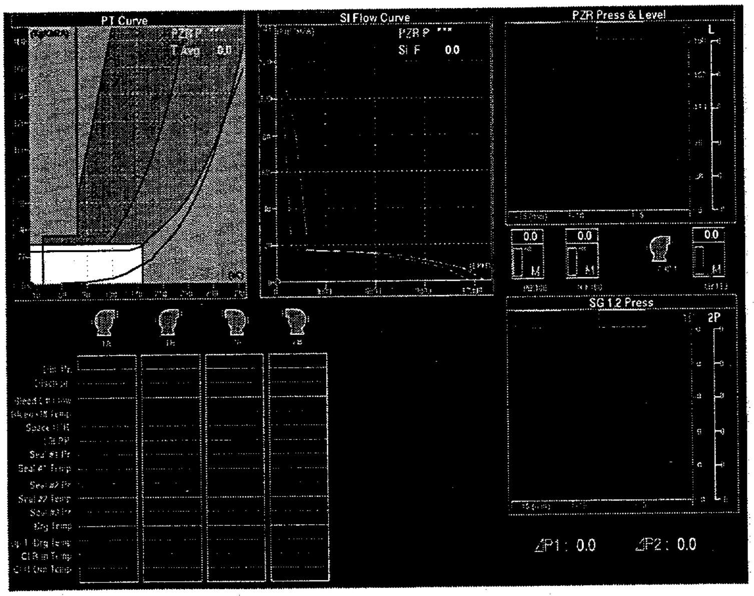


Figure 3. A Snapshot of CPS Supporting Display

The key design characteristics of the KNGR CPS to support the functions include the following (Figure 3):

- flowchart-format instruction for each procedure step description (Figure 2)
- real-time component status and plant parameter display by automatic detection and monitoring
- component symbol display through which control action can be executed
- integration of procedure instruction and control functions
- dedicated display section for continuously applied steps
- dedicated display section for postponed steps
- simultaneous handling of multiple procedure
- auxiliary support display (i.e., CPS Supporting Display) in a separate CRT
- procedure editing (i.e., procedure writing, installation into CPS framework, and modification).

ROLES OF CPS DURING OFF-NORMAL AND EMERGENCY

The characteristics of operator tasks change when the plant states changes from normal to off-normal or emergency. The operators become required for quick response to changes of plant states and become busier resulting in high workload, the operators' situation awareness become degraded and the possibility of losing big picture about the overall plant state increases, and the chance of various operator errors in information processing and control actions also increases. Since the time of off-normal and emergency situation is when the MCR operators need to rely on the use of operating procedures, the CPS plays an important role in the safe operation of plant in this critical situation. This section describes how the CPS provides operator aids during off-normal and emergency situation.

Support for Detection and Monitoring Task

Comparing to normal situation, off-normal or emergency situation requires much more amount of detection and monitoring of plant parameters in quicker time. Since plant indications are incorporated into the KNGR CPS and it has a capability of providing the operator with context-sensitive plant state information only, the KNGR CPS is able to play a role of facilitating the operator for quicker detection and monitoring of plant states. The automatic monitoring function of CPS on continuously applied steps and postponed steps also reduces the burden of detection and monitoring tasks.

Besides the information displayed in the CPS, which is the primary information to perform a procedure step, subsidiary information is displayed in the adjacent CRT—i.e., right side of the CPS CRT (Figure 3). This information in the CPS Supporting Display also helps the operator detecting and monitoring plant parameters.

Support for Planning and Decision Making

In an MCR of an advanced nuclear power plant, the operator plays a supervisory role, i.e., the responsibility of the operator include such supervisory activities as planning and decision making. Such smart features of the KNGR CPS as automatic detection and monitoring relieves the MCR operators from many moment-to-moment equipment control, and this helps the operators more focus on planning and decision making. Context-sensitive procedure guidance and action recommendation provided by the KNGR CPS would also facilitate the MCR operators to perform supervisory activities including planning and decision making.

When following operating procedures during off-normal or emergency situations, the MCR operators often lose awareness of where they are and what they are doing resulting in operational error. Dedicated and context-sensitive display about the current goal and salient coding for the current procedure step would facilitate the operators to maintain high awareness of operational goal awareness.

According to the results of a study on computer-based procedures, computer-based EOPs "appear to be helpful in assisting operators in coping with multiple failure scenarios, where a loss of situation awareness can lead operators to focus on one concern while failing to react to changes caused by other failures" (Spurgin and et al., 1993).

Support for Control Action

While some computer-based procedure provide an automatic procedure execution capability that executes procedure steps without step-by-step intervention from the operator; the KNGR CPS requires explicit operator action to "execute" a procedure step. However, the current version of KNGR CPS facilitates the operators' control actions by providing recommended action automatically generated based on the current plant condition. The KNGR CPS also facilitates operator by displaying component symbols in the CPS Display (Figure 2) as well as in the CPS Supporting Display (Figure 3) so that the operators can bring up necessary control page at soft controller (Figure 1) using the symbols. Context-sensitive, real-time plant condition displays resulting from automatic detecting and monitoring function of the KNGR CPS, as well as automatic recommendation for action control would also support for MCR operators' control actions.

CONCLUSION

An electronic procedure or computerized procedure system (CPS) is being developed for KNGR operation. Like other computerized procedures, the KNGR CPS has many advantages that could not be possible in conventionally used paper-based procedures. Such advantages include flexibility in procedure presentation format, automatic detection and monitoring of plant condition, and automatic guidance for component control actions.

It is expected that CPS would drastically decrease the navigation workload and reduce time for procedure manipulation and execution while increasing the operation convenience by providing context-sensitive task information with less operator's efforts. Since the KNGR CPS is still under development, however, more studies should be done to make an improvement in usability.

DISCUSSION

Despite many potential advantages, there also are challenges in designing an effective computer-based procedure system such as decrease of operator competence for operation by exercising knowledge and the decrease of operator vigilance during operation using a computerized procedure. Results of the studies on computer-based procedures show many types of usability concerns. For example, the compatibility problem between computer-based procedure displays and paper-based backup procedures is one typical issue to resolve.

A study on computer-based procedures internationally used found out that differences in philosophy regarding the purpose of EOPs and the role of the operator resulted in important differences in a computer-based EOP design. For example, while the computer-based EOPs developed in EdF provides instruction, which the operator is expected to follow for all but special exceptions (O'Hara, 1996), the KNGR CPS is designed merely to provide information and make recommendation that can always be overruled by the operators.

Integration with other computerized systems in the KNGR MCR, coordination among operators in use of CPS's, appropriate level of automation in CPS design are some of the important issues to resolve in the design of the KNGR CPS. Also, it cannot be overemphasized that the design of such a complex and critical system as CPS should be carefully made considering necessary and sufficient human factors principles. More discussions and research results about the development efforts of the KNGR CPS would be available in the future.

REFERENCES

Barns, V., P. Desmond, and C. Moore (1996), Preliminary Review Criteria for Evaluating Computer-Based Procedures (BNL Technical Report E2090-T4-2-9/96), Brookhaven National Laboratory.

O'Hara, John M., William F. Stubler, and James C. Higgins (1996), Hybrid Human-System Interfaces: Human Factors Considerations (BNL Report J6012-T1-4/96), Brookhaven National Laboratory.

Spurgin, A., J. Wachtel, and P. Moieni (1993), The State of Practice of Computerized Operating Procedures in the Commercial Nuclear Power Industry, Proceddings of the Human Factors and Ergonomics Society 37th Annual Meeting, Santa Monica, CA, Human Factors and Ergonomics Society.

IAEA SPECIALISTS' MEETING
on
"Human-Machine Interface for Off-Normal and Emergency Situations in NPPs"
Oct. 26-28, 1999, Taejon, Korea

Analysis of vibration diagnostic and protection system (VDS) operation at nuclear and fossil PPs.

Emergency situation at PP.

A.I. Puzanov, I.N. Puzanova, A.A. Bazin.

1. Introduction

The offered Vibration Monitoring, Measurements and analysis system carries out by means of computers in automatic regime the estimation of vibration state of the unit on the base of currant and preliminary measurements analysis, both property vibration values (bearings, shaft vibration) and parameters, characterizing unit operational regime (shaft power, rotor current of the generator, etc), and also its operational conditions (lubricant and bearing babbitt temperatures, temperature of metal, live steam pressure). The automatical diagnostics allows to find out in proper time the causes of changes of vibration condition and unit operational parameters of turboset. It provides the possibility to take proper technical measures to prevent possible defect (trouble) to shut-down with the aim to prevent emergency conditions occurring or that is also most important function of diagnostic system - to avoid false shut-down or unit off-loading.

The system of monitoring, measurement, and analysis of vibrations is designed to increase the operating reliability of the existing turbosets manufactured by "Leningradsky Metallichesky Zavod" Joint Stock Company (AO "LMZ"). The system of monitoring, measurement, and analysis offered is based on the vibration diagnostics approach worked out by AO LMZ and Scientific-Production Enterprise "Turbotest" Joint Stock Company (AO NPP "Turbotest") to provide for:

- continuous monitoring of vibration-related condition of the turboset,
- generation of signal upon vibration rates of bearing supports and rotor journal relative movement swing exceeding the specifide levels in two settings (Warning and emergency alarm),
- supplying the attending personnel with information on changes in vibration parameters of the turboset, in real time,
- timely warning the attending personnel on the most probable causes of changes in vibration-related condition of the turboset to prevent an emergency from arising at the power-generating unit,
- issue of recommendation on elimination of the faults found and timely response to the defects in operation of the equipment,
- possibility of spatial location of the fault found,
- formation of an archives of the faults found (a repair request form) to be used in scheduled maintenance works, to cover the troubles found to a maximum,
- formation of a database to record the changes in vibration and and thermomechnical parameters characterizing the turboset condition, and also the cases of these parameters going beyond the specified values.

2. Vibration Diagnostic Algorithm

Vibration Diagnostic Algorithm is a variety of expert system, represented in the form of a table (matrix) whose main elements are as follows:

◊ **list of parameters to be measured and computed, analysis of those parameters being a base of diagnostic;**

◊ **list of defects to be determined;**

◊ **numerical values which fill in the matrix field and characterise "contribution" of each parameter in the determination of a defect.**

Matrix-like nature of the diagnostic algorithm provides simultaneous and continuous determination of all possible defects and their causes which allows to analyse mechanical state of the turboset with the entire interconnection and interinfluence of various defects, failures and operating departures in dynamics of their development and growth of danger rate.

List of defects to be diagnosed is:

1. Rotor technological disbalance.
2. Radial error ("bending") in rotor connection.
3. Angular error in rotor connection.
4. Abrupt disbalance.
5. Rubbing in the streampath in bearing oil sealings.
6. Crack in rotor.
7. Low frequency vibration (oil whip).
8. Destruction of bearing babbit.
9. Severe misalignment of supports.
10. Lack of oil clearances in bearings.
11. Shot circuit in generator rotor windings.
12. Cooling system disbalance in generator rotor.

3. Metrologic Support of Vibration Diagnostics System (MS VDS)

One of the most important features of VDS is validity of its decisions which depends of vibration velocity values and other controlled parameters, but also on the validity which the numerical values of the parameters in question are determined with.

In case of low validity of determination of parameter values the errors in estimation of critical values of the characteristics which determine the decision, whether to stop the turboset or to continue its operation, may result in grave consequences of two types. In the first case due to a vast zone of unsertainty, the turboset will be stopped though, objectively, it isn't necessary. In the second case, a heavier one, the turboset will go on to operate though it should have been stopped to avoid mechanical damage.

As appears from the above the problems of accuracy and validity of measurements which influence significantly the validity of decisions made on their bases, are of primary importance for the operating personnel of thermal and nuclear power stations. That is why much attention is given to MS VDS at all stages of VDS development, manufacture, tests by Disigner, mounting work at the Customer's place and during operation.

4. Predesign Examination of the Object for VDS Introduction

At the stage of predesign examination (after technical requirements for VDS and its components have been agreed upon with Customer) it is necessary to evaluate the level of technical equipment of the object, its availability for VDS integrating into the power unit control system.

This most labour consuming stage covers:

- ◊ **study of technical characteristics of standard measuring channels required for VDS functioning with the aim of finding out the possibility of VDS connection, either directly or through appropriate transition units;**

- ◊ **study of mounting conditions and layout of VDS equipment at the power unit;**

- ◊ **analysis of additional requirements of Customer for Customer functional interaction of VDS with other systems operating at the power unit namely: with the information computer system; exit into local computer network; integration of VDS of several power units of thermal and nuclear power stations into one information network; programming subsystem of connection with modular control board operator (user interface) is agreed upon in general;**

- ◊ **study of operating modes of the power station or particular power unit (peak, base power load) which is the determining factor when planning the term of VDS introduction into trial-commercial operation. Along with this it should found out whether all the works connected with VDS introduction are to match in time with overhauls or medium repairs of the power unit equipment or it is possible for mounting and system debugging of VDS, to make use of scheduled shutdowns of the power unit (in the case of the power unit operation under peak load).**

5. Promotion of VDS.

5.1 Design Work on VDS Introduction

At the stage of design work on VDS introduction at a particular power unit on the basis of the result of the preceding stage, three design documents are worked out and agreed upon with Customer.

- ◊ **technical assignment for VDS of a particular turboset;**

- ◊ **detail design of VDS for a particular turboset;**

- ◊ **technical assignment to Chief Designer of the power unit to carry out the contractor design of adjusting VDS (to be agreed upon separately with Chief Designer of the power unit).**

5.2 Delivery of VDS Components to Customer

5.3 Mounting and Starting-and-Adjustment Work on VDS Introsuction; Putting the system into Trial-and-Commercial Operation

6. Location of VDS.

VDS's practically are installed on all types of turbounits manufactured by Joint Stock Co. LMZ.

Vibration diagnostic system has been certified by State Standard Authorities of Russia.

Turbounit type	Quantity of turbounits equipped with VDS's	Quantity of turbounits on which VDS's are being mounted	Operation, (years)
K-100-90-6	1	-	2
T-180/210	2	-	3
ПТ-60/130	1	-	2
K-1200-240	1	-	6
K-300-240	6	4	4
K-200-130	1	-	1.5
ПТ-80/100	1	1	6
ПТ-135/165	-	1	-
T-100/120	-	1	-
K-1000/1500	-	1	-

7. Analysis of emergency situation in power plant.

Vibration diagnostic system developed for turbounits consists of the following instruments:

- control and measuring of bearings vibration;
- vibrodisplacement of shaft;
- termomechanical measurements;
- spectrum analyser;
- PC.

The function of VDS operation can be broken down into the phases:

- start up;
- coast down;
- diagnostic.

In 1993 VDS was installed at the K-1200-240 PP with 14 supports. After planned maintenance works performed within three days was carried out a start up of the turbine.

At the stage of gaining revolutions from 0 to 1000 rpm and from 1000 to 3000 rpm detailed analysis of database information showed that the main parameters of turbounit condition are tolerable:

- vibrovelocity (root-mean-square) of 14 bearings in axial, horizontal and vertical directions;
- amplitudes and phases of six vibrovelocity harmonics in three directions;
- vibrodisplacement (peak-to-peak) of rotors in vertical and horizontal directions;
- termomechanical parameters;
- special measurements (axial shift; HP, IP and LP cylinder displacement, relative displacements of rotors).

The turbine generator was idling, vibrovelocity did not exceed 2.5 mm/s at 1-10 bearings and 3.3 mm/s at 11-14 bearings.

The unique deduction of the gaining s period is that all turbounit parameters were within tolerance.

During the phase of trip strikers testing when shaft rotation is 10-12 % greater than operating frequency was noted an abrupt increase of vibration at all bearings.

"Danger" level of vibrovelosity (11.2 mm/s) was exceeded at :

- 3 and 5 bearings (vertical component);
- 6 and 7 bearings (horizontal component);
- 4, 5, 6 and 7 bearings (axial component).

"Danger" level of vibrodisplacement (150 mcm) was exceeded at all rotors exept 12 in vertical and axial directions.

Database noted discrete signals:

- danger vibration;
- alert vibration;
- protection (when vibrovelosity exceeds danger level at two adjacent bearings).

The largest increase of alert level of vibrovelosity and was noted at bearings:

- 4 - 7 - axial component ;
- 1 - 7 - horizontal component;
- 2 - 7 - vertical component.

3 and 6 bearings had the largest increase of vibrovelosity and vibrodisplacement of rotors. It allows to assume that the sources of critical event were intermediate power cylinder or low power cylinder #1.

Protection system came into action 17 seconds later once the stop valves were closed at the beginning of coast down process. This demonstrates the abrupt disbalance of HPS-1 rotor (abstraction of blade or shroud parts caused by increase of steam and particularly centrifugal forces on blades suggests developing of concealed defects on one of blades).

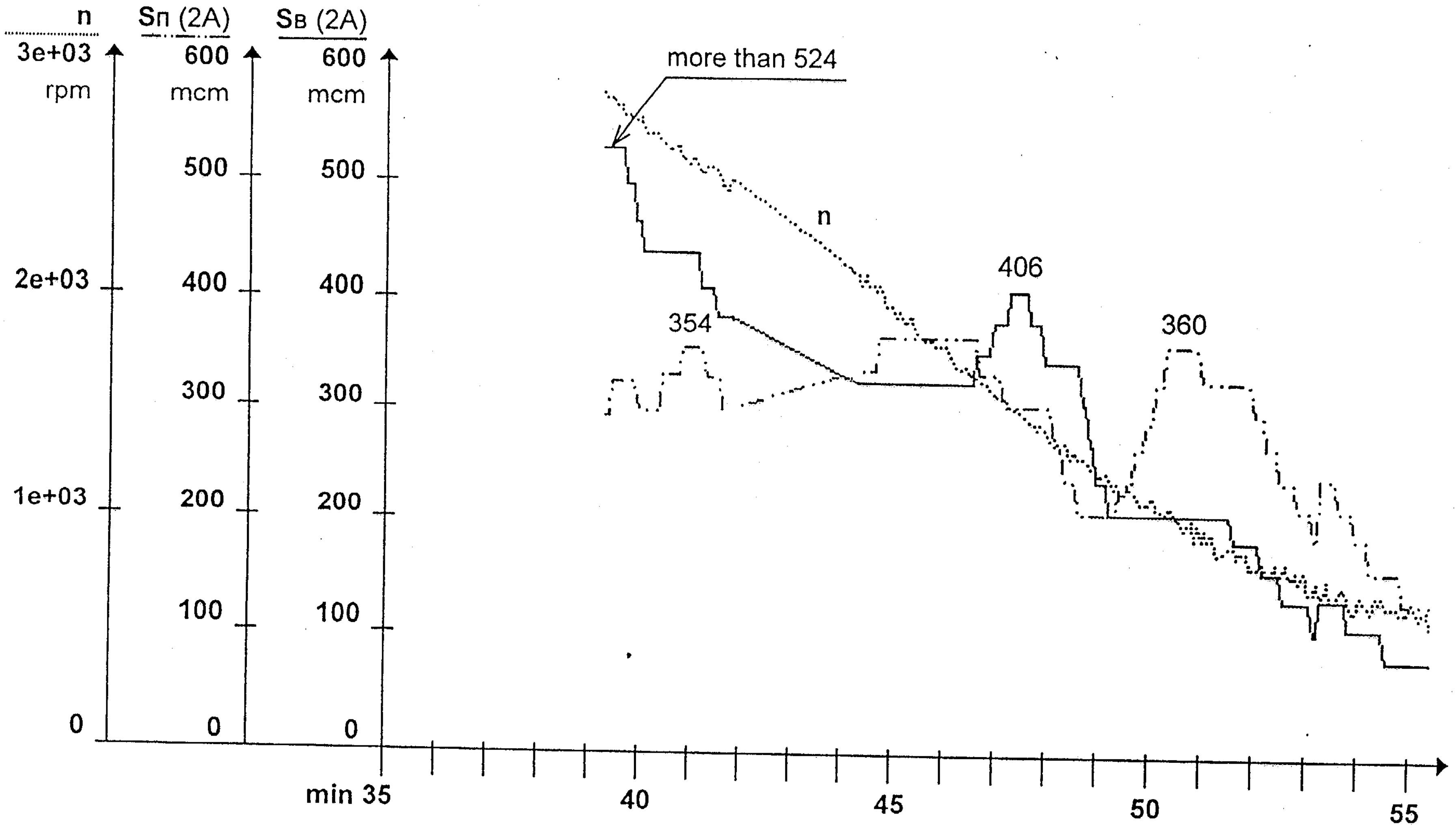
The process of blade disintegration happened without essential change of its length.

Abstraction of shroud or blade happened instantaneously. Under the action of centrifugal force torn loose part struck the shroud and caused radial rubbings of other blades and their destruction. Taking into consideration great mass of the shaft it is believed that the disruption of other blades happened during one revolution of the shaft. Sudden disbalance of LPC-1 rotor caused drastic deterioration of the whole shaft and lead to turbine vibration protection system functioning.

Analysis of VDS database demonstrated that the system performed its functions in the "sudden failure" mode of operation.

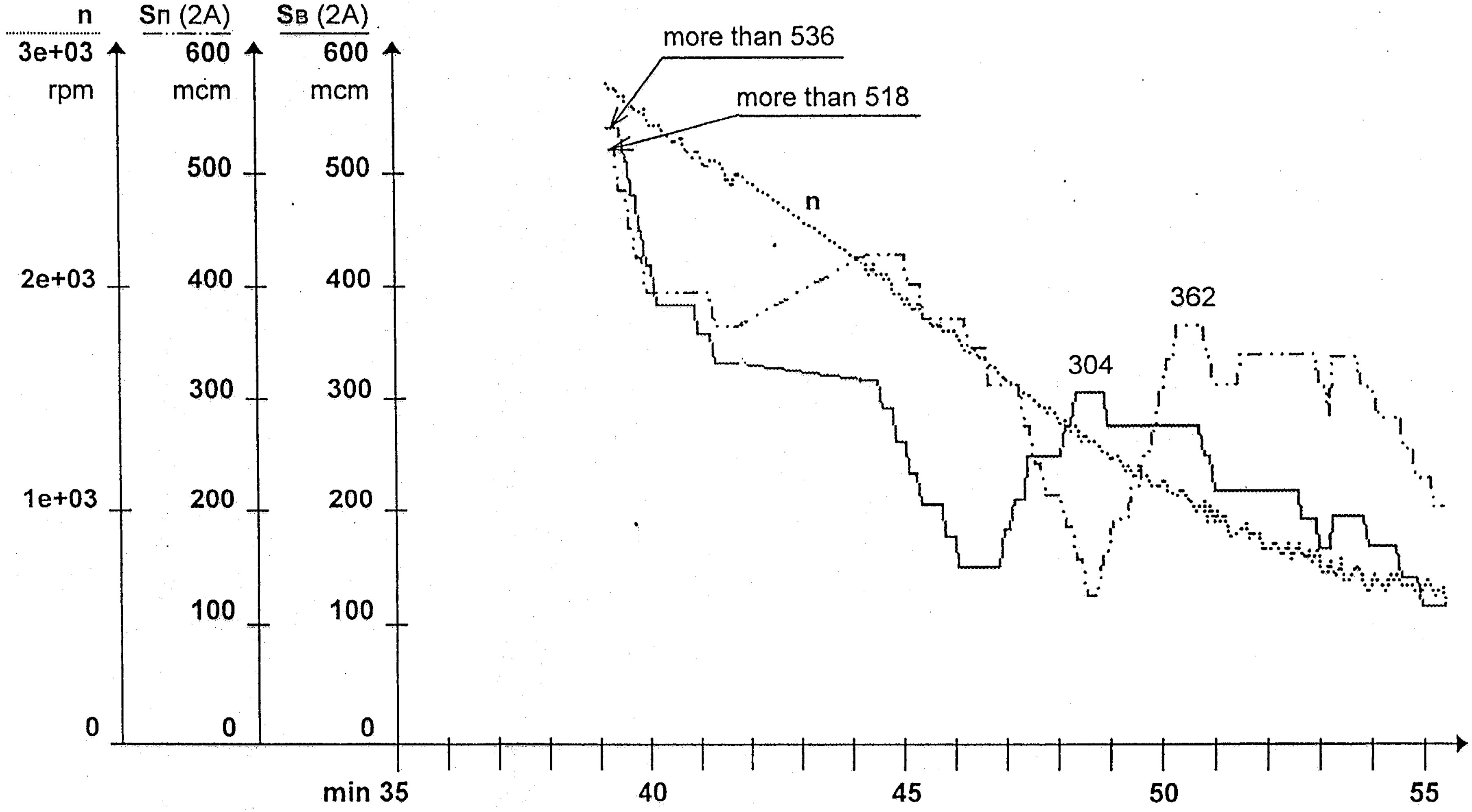
On pictures 1- 4 are presented the levels of vibrovelocity and vibrodisplacement on bearings 5,6 at coast down mode of operation.

Operating experience of VDS manufactured by JSC "Turbotest" allows to conclude that though the expenditures on installation and maintenance of VDS are rather high they can be justified within 2-3 years.



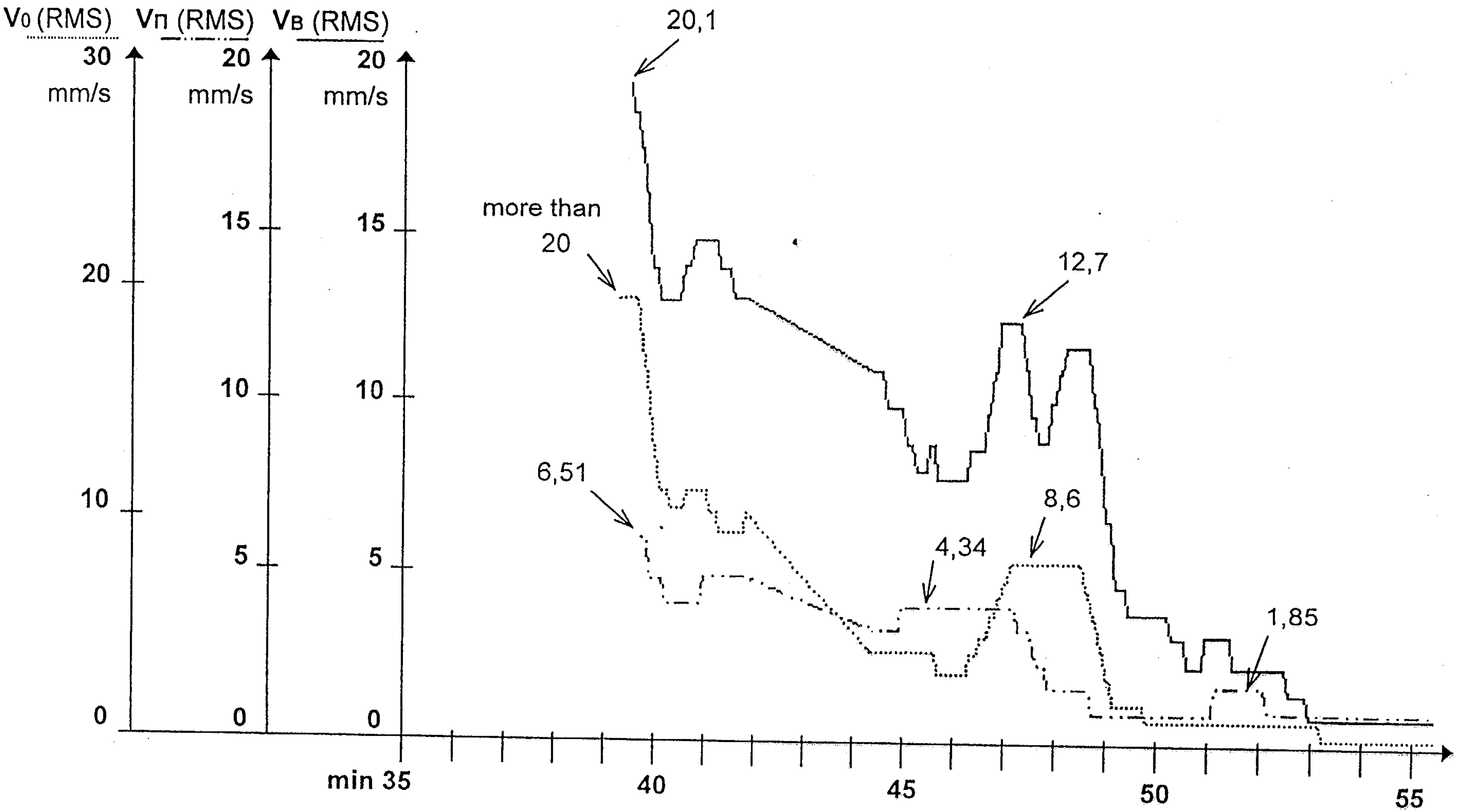
03.11.1995 14:35:00 03.11.1995 14:55:24

Fig. 1 Vibrodisplacement of rotor, bearing № 5:
vertical component Sв (2A); horizontal component Sп (2A).



03.11.1995 14:35:00 03.11.1995 14:55:24

Fig. 2 Vibrodisplacement of rotor, bearing № 6:
vertical component Sв (2A); horizontal component Sп (2A).



03.11.1995 14:35:00

03.11.1995 14:55:24

Fig. 3 RMS vibrovelocity of bearing № 5:
vertical component ($V_{\text{в}}$); horizontal component ($V_{\text{п}}$); axial component (V_0).

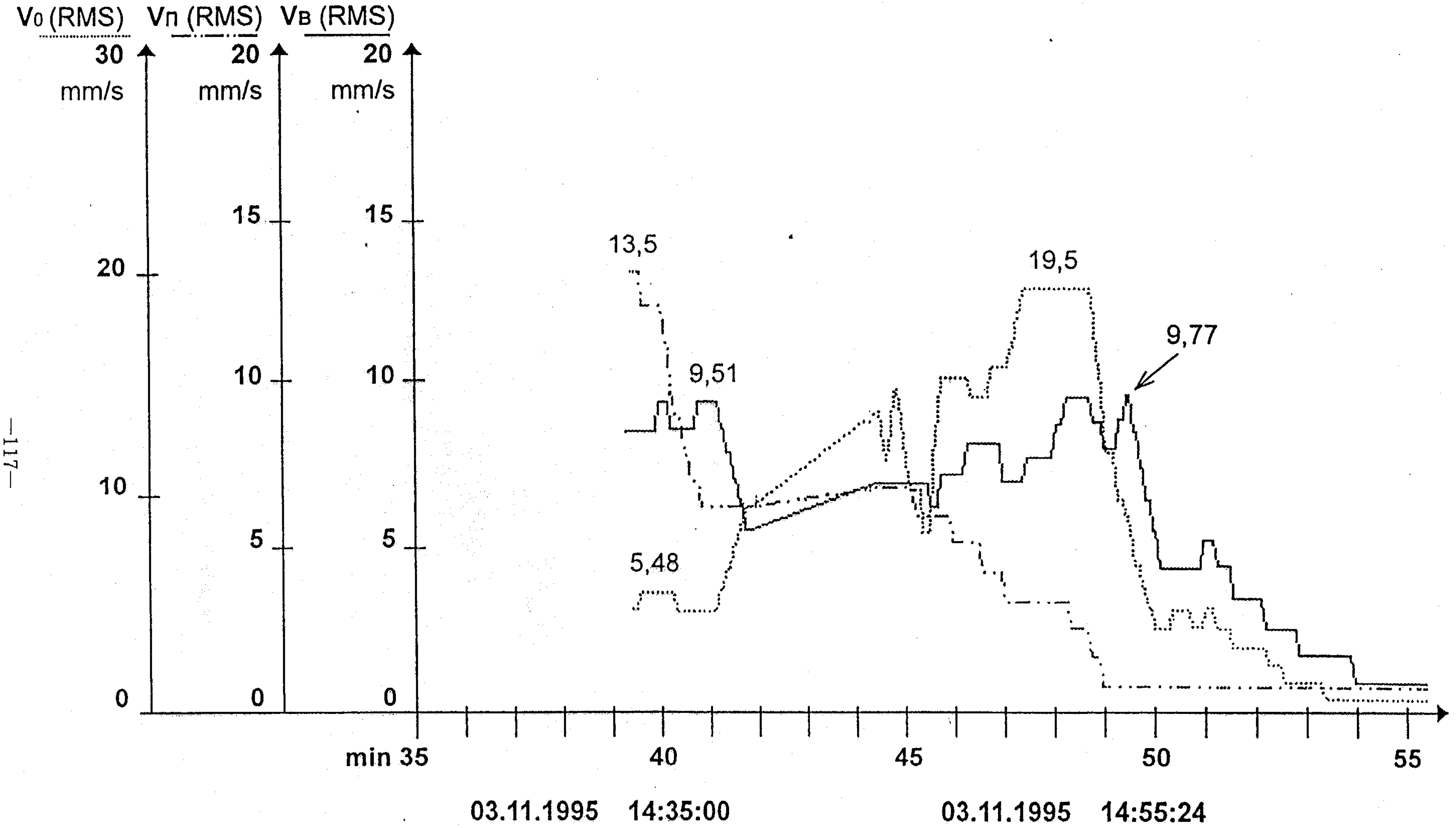


Fig. 4 RMS vibrovelocity of bearing № 6:
vertical component ($V_В$); horizontal component ($V_п$); axial component (V_0).

SESSION 3

LICENSING ISSUES FOR HMI

A Methodology for Evaluating Alarm-processing Systems using Informational Entropy Based Measure and the Analytic Hierarchy Process

Hyun G. Kang
Korea Atomic Energy Research Institute
Dukjin-dong, Yusong-gu, Taejon 305-353, Korea

Poong H. Seong
Korea Advanced Institute of Science and Technology
Kusong-dong, Yusong-gu, Taejon 305-701, Korea

Abstract

We propose a new measure based on the informational entropy concept. It is designed to reflect the cognitive complexity, which users perceive when they work with alarm-processing systems. An experimental verification for the proposed measure is performed. The result shows that the proposed measure is superior to the other measures. We also propose a procedure for evaluating alarm-processing systems based on the analytic hierarchy process (AHP) with regard to integrating a series of deviations that must be considered. This procedure aims to perform effective simulator-based evaluations of alarm systems' design. An exemplary application is shown in this paper.

1. Introduction

Many researchers, even those who recognize the advantage of conventional hard-wired annunciator systems, have pointed out the need for improvement of alarm systems through the use of advanced computer technologies [1], [2], [3]. This is why the alarm systems of the next generation nuclear power plants are being designed to be computerized and conventional ones are being scheduled to be improved by computerized systems.

In order to verify its usefulness, system designers should evaluate a newly developed alarm system in many aspects that can affect the performance of operators. Conventionally, the most common evaluation method is an experiment that is based on the expertise of the operators. It is time-consuming and its results tend to depend on the participants' experience. The predictive/theoretical evaluation method is more attractive. These predictive/theoretical methods enable system designers to anticipate the performance of a developed alarm system without experiments. These methods require only repeated calculations with alarm lists which are recorded or simulated.

Hogg et al. [4] proposed a situation awareness measure, named SACRI, in the Halden Project. They selected A' measure as an indication of how accurately an operator had assessed the current situation and nature of its effects throughout the process. The measure of A' is based on the signal detection theory. Park [2] also proposed a theory-based measure, *E*, using the concept of A'. *E* provides an estimate for the performance of an alarm-processing method. It consists of an informativeness measure (A') and a reduction rate (simple ratio of the reduced alarms to the activated alarms).

A basic role of alarm systems is the provision of alerts for process deviations. Well-designed alarm systems could provide informative cues that are useful for the identification of process deviation. An alarm system is a system that is designed to collaborate with a human operator. Even with computerized alarm systems, the task of diagnosing the cause of process failures still falls to the operator [5]. Therefore, the measure for an alarm-processing system's usefulness should be a user-oriented one. Evaluation by *E* is a system-oriented approach because both the informativeness and the reduction rate contain the term related to the number of 'correctly rejected alarms'. Only a system designer is concerned with this 'correct rejection'. An operator of a nuclear power plant, the intended user of the alarm-processing system, has no reason to be concerned with the 'correct rejection'. He/she is not even able to recognize the existence of rejected alarms.

On the other hand, in the early design phase, the absence of a well-established performance evaluation procedure is another significant problem. The experimental evaluation is deviation-specific and we cannot transfer the experimental evaluation result for a deviation (e.g., a loss of coolant accident) to that of another (e.g., a steam generator tube rupture). Both the measure that are proposed in this paper and E proposed by Park provide deviation-specific results. The deviation specific results should be integrated for evaluating the usefulness of the overall system.

2. A Usefulness Measure for Alarm-processing Systems

A. Characteristics and evaluation philosophy of alarm systems

An alarm system in a nuclear power plant control room must be designed to optimize the ability of operators to acquire the necessary information and to process that information in order to identify plant status and take corrective actions [3]. It should alert operators if a system or process deviation occurs but should not increase their workload.

First, we should define the circumstance in which human operators acquire 'adequate information in effective manner' in order to evaluate the usefulness of an alarm-processing system. As mentioned in the previous section, an alarm system is a system that is designed to be collaborating with a human operator. Therefore, the better alarm system requires the lower cognitive workload and it also leads human-operators to make more accurate diagnosis. The user-oriented approach of this study forms a contrast with that of Park's E [2].

The information provided to the operator can be categorized into two groups: content and shape. The content information has strong relation to the alarm-processing method (i.e., what alarms are so important that the operator should recognize them?). The shape has strong relation to the display design (i.e., how should alarms be presented?). This study focuses on the evaluation of the effects of the content information.

We can assume that the operator recognizes the process deviation based on the similarity matching. Early studies [2], [6] show that this assumption is reasonable. Park [2] pointed out that operators could identify the deviation more easily with which they were very familiar. The operator's familiarity for a specific deviation is mainly dependent on the training program. Their experience in operating also affects this familiarity. Based on this assumption, we can obtain the key alarm set which characterizes each deviation by investigating some documents or by interviewing some operators.

B. Informational entropy

Entropy has been widely used as a quantitative measure of uncertainty in many areas including thermodynamics, information theory, biology, decision theory, and sociology [7]. Shannon [8], who largely originated information theory, suggested the most important information quantity, entropy, which played a central role in information theory as a measure of information, choice and uncertainty. Hick and Hyman applied the informational entropy to quantify the uncertainty of stimulus events. Both investigators found that choice response time increased by a constant amount each time the information in the stimulus was increased by one *bit* [9].

Early experimental results of numerous investigators show that human being could be represented as an information channel and the informational entropy is a more appropriate measure than the number of alternatives. Miller found that the number of categories to which stimuli could readily be assigned was consistently near seven for a wide variety of tasks. That is, a human being can be represented as an information channel and also has some vigilance limits on performing cognitive tasks [10]. The informational entropy, therefore, could measure the difficulty perceived by operator. This difficulty is due to the complexity of recognizing alarms which are presented via an alarm system and the complexity of bringing back key alarms from the memory.

According to the information theory, the amount of information, *bits*, is simply equal to the base 2 logarithm of the inverse of probability, i.e.,

$$H_i = \log_2 \frac{1}{p_i} \qquad (1)$$

where H_i is the amount of information and p_i is the probability of occurrence of event i. The average information conveyed by a series of events with different probability is computed as

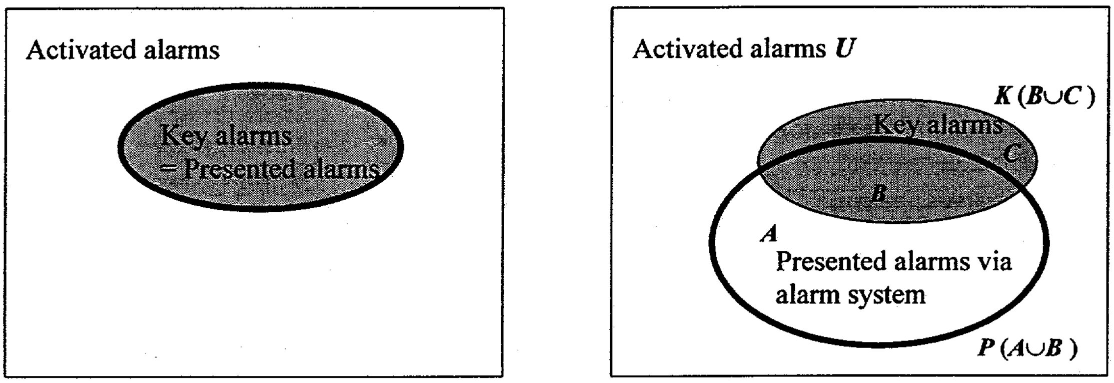
$$H = \sum_{i=1}^{n} p_i \log_2 \frac{1}{p_i} \qquad (2)$$

where $\sum_{i=1}^{n} p_i = 1$,

p_i: probability of occurrence of event i, and

n : total number of possible events.

An important characteristic of Equation (2) is that the value of H for not equally probable events will always be less than that for equally probable events.



(a)

(b)

Figure 1. Venn diagrams for an ideal alarm system (a), and an actual alarm system (b), where K is the set of key alarms and P is the set of presented alarms

C. A measure of alarm system usefulness, R (K, P)

In order to evaluate the usefulness of alarm-processing systems with regard to the human performance of identifying process deviations, a new measure is proposed based on the informational entropy concept. Using Venn diagram, Figure 1 represents the situations of which the operator identifies the process deviation. Figure 1 (a) shows the situation with an ideal alarm system. It suppresses every nuisance alarm and presents every key alarm for the given deviation. Figure 1 (b) shows the situation with an actual alarm system, which presents some of key alarms and some of nuisance alarms. K represents the key alarm set, which can be obtained from operators' training. Therefore, $U - K$ represents the set of nuisance alarms. P represents the presented alarm set, which is processed by an alarm system. It should be noted that the more key alarms and the less nuisance alarms it presents, the more easily operators identify the deviation.

In Figure 1 (b), when an alarm system presents processed alarms of P, the alarms in B help operators to correctly identify the deviation but those in A lead to misidentification. The alarms in C also obstruct the correct identification. The number of alarms helpful to identification is the number of alarms in B, $n(B)$, and those harmful to identification is $n(A \cup C)$. We call the alarms in B 'hit alarms', those in A 'false alarms', and those in C 'missed alarms'.

On the other hand, the absolute size of $P \cup K$ also affects on the decision of operators. The bigger $n(P \cup K)$ implies that the more alarms operators must consider. It will increase the workload of operators and may mislead them. Based on these concepts, we can define three effects on the identification correctness of process deviations as follows:

Effect 1: an increase in n(B)/n(A) or in n(B)/n(C) will increase the correctness,

Effect 2: an increase in n(A) will decrease the correctness, and

Effect 3: an increase in n(C) will decrease the correctness.

In order to represent the three effects, we develop a measure, R (K, P) which is named relation entropy, because it is well known that entropy is more proper for measuring human performance than the number of alternatives [11]. *R* (*K*, *P*) is a modification of 'amount of transmitted information [9], [10]', *T* (*K*, *P*). By modifying the relation matrix (*K*×*P*) of the 'amount of transmitted information', we can define the relation entropy as follows:

$$R\,(K,P) = H\,(K) + H\,(P) - H\,(K,P). \tag{3}$$

By substitution of Equation (2) to Equation (3),

$$\begin{aligned} R(K,P) = &\sum_{i=1}^{n(K)} p(K)_i\, h(K)_i + \sum_{j=1}^{n(P)} p(P)_j\, h(P)_j \\ &- \sum_{i=1}^{n(K)} \sum_{j=1}^{n(P)} p(K,P)_{ij}\, h(K,P)_{ij} \end{aligned} \tag{4}$$

where

$$\sum_{i=1}^{n(K)} p(K)_i = \sum_{j=1}^{n(P)} p(P)_j = \sum_{i=1}^{n(K)} \sum_{j=1}^{n(P)} p(K,P)_{ij} = 1,$$

$p(K)_i$, $p(P)_j$: the probability of occurrence of alarm *i*, alarm *j*, respectively, and

$p(K, P)_{ij}$: the probability which is determined by relation of an alarm in *P* and an alarm in *K*.

The amount of information associated with the key alarm *i*, $h(K)_i$, is

$$h(K)_i = \log_2 \frac{1}{p(K)_i}. \tag{5.a}$$

The amount of information associated with the presented alarm *j*, $h(P)_j$, is

$$h(P)_j = \log_2 \frac{1}{p(P)_j}. \tag{5.b}$$

As mentioned in the previous section, we assumed that an operator recognizes a deviation based on the similarity matching. Therefore, the relation between the key alarm and the presented alarm can be considered as the comparison between them. If an operator finds an expected key alarm among presented alarms ($K \cap P$), the comparison between them will not carry out any information. So the amount of information associated with the comparison between the key alarm *i* and presented alarm *j*, $h(K, P)_{ij}$, can be defined as follows:

$$h(K,P)_{ij} = \begin{bmatrix} \log_2 \dfrac{1}{p(K,P)_{ij}} & (\textit{if alarm}_i \neq \textit{alarm}_j) \\ 0 & (\textit{if alarm}_i = \textit{alarm}_j) \end{bmatrix}$$

Table 1 shows an example for illustrating the concept of $h(K, P)_{ij}$.

Table 1. The example of an contingency matrix

p(*K*, *P*)			Key alarms		
			alarm$_1$	alarm$_3$	alarm$_5$
			0.5	0.3	0.2
Pre-sented Alarms	alarm$_1$	0.125	0.125	0.075	0.05
	alarm$_2$	0.125	0.125	0.075	0.05
	alarm$_3$	0.125	0.125	0.075	0.05
	alarm$_6$	0.125	0.125	0.075	0.05

h(*K*, *P*)			Key alarms		
			alarm$_1$	alarm$_3$	alarm$_5$
			1.000	1.737	2.322
Pre-sented Alarms	alarm$_1$	2.000	0	3.737	4.322
	alarm$_2$	2.000	3.000	3.737	4.322
	alarm$_3$	2.000	3.000	0	4.322
	alarm$_6$	2.000	3.000	3.737	4.322

3. Validation Test for *R (K, P)*

In order to show that the suggested the informational entropy measure provides proper indication of alarm-processing systems' usefulness in identifying process deviations of nuclear power plants, we performed an experiment. This subjective experiment uses the dynamic alarm console (DAC), which was developed for effective alarm reduction in Korea Advanced Institute of Science and Technology (KAIST) [12], [2]. This experiment provides deviation identification rates for 12 cases by varying the deviation scenario, the key alarm set and the alarm reduction criterion. In each case, the result of experiment and that of measure calculation are compared with each other. That is, we examined the correlation between the proposed measure and the actual human performance index of correct identification rate.

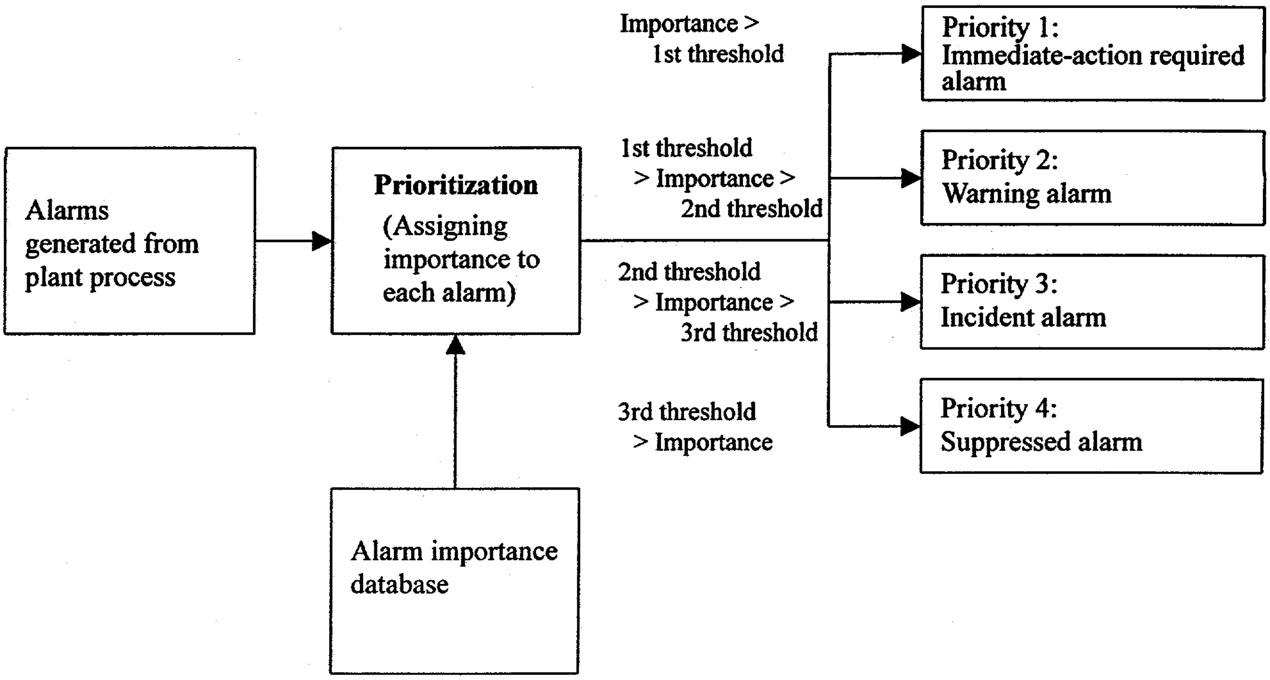

Alarms generated from plant process
Prioritization
(Assigning importance to each alarm)
Alarm importance database
Importance > 1st threshold
1st threshold > Importance > 2nd threshold
2nd threshold > Importance > 3rd threshold
3rd threshold > Importance
Priority 1: Immediate-action required alarm
Priority 2: Warning alarm
Priority 3: Incident alarm
Priority 4: Suppressed alarm

Figure 2. Schematic diagram of alarm-processing in DAC

A. DAC

DAC is a part of an advanced human-machine interface, which Chang et al. [12] developed for application to Korean Next Generation Reactor (KNGR). The roles of DAC are the processing and presentation of multiple activated alarms, the offer of alarm-related information, and the record of time history of alarms. DAC reduces the number of alarms by prioritization. The priority in the DAC is assigned by two methodologies. The one is the system-oriented prioritization which evaluates individual alarms considering urgency of recovery actions and severity of their impacts. The other is the mode-oriented prioritization which considers plant operational modes.

DAC eliminates unnecessary alarms for status identification, and suppresses less important alarms among activated ones. All process deviation scenarios used in this experiment are departures from nominal-power operation mode. Therefore, in this experiment, the mode-oriented prioritization could be excluded. By the system-oriented prioritization, a specific priority score is assigned to each alarm. The range of this score is 1 to 27. Figure 2 illustrates the alarm-processing scheme in DAC. The operators in Yonggwang Nuclear Unit 3 and 4 established the database for alarm prioritization of DAC.

B. Participants

The operators in actual plants could be suitable subjects because of their expert knowledge. However, if the operators were the subjects of this experiment, we could not examine the effect caused by the change of key alarm sets because the operators had their own key alarm sets in their memory. For addressing this effect, the qualified graduate students who have enough basic knowledge for nuclear power plants are more adequate participants. Therefore, 20 volunteers (19 men and 1 woman) were selected for subjects of this experiment. They were specialized in nuclear engineering. They went through several courses in nuclear power plant system engineering. The volunteers were ranged in ages from 21 to 30 years and had normal or corrected-to-normal vision. All the subjects had enough computer experience and mouse device manipulating skill. They were informed that the correctness of identifications would be used as a human performance parameter. Randomly, we allocated 10 of participants to group 1 and the others to group 2.

Table 2. Evaluation results for the usefulness of DAC

Key Alarm set	Criterion	Deviation	Processed results			Identification rate	R (K, P)
			Hit	False	Miss		
Set 1	α	LOCA	6	48	2	0.5	0.122
		LOFA	5	19	1	1.0	0.249
		SGTR	5	15	4	0.3	0.208
	β	LOCA	6	51	2	0.4	0.116
		LOFA	5	23	1	0.6	0.220
		SGTR	5	18	4	0.4	0.186
Set 2	α	LOCA	5	50	1	0.4	0.127
		LOFA	4	20	1	0.8	0.230
		SGTR	3	20	1	0.5	0.213
	β	LOCA	5	53	1	0.3	0.121
		LOFA	4	24	1	0.8	0.204
		SGTR	3	23	1	0.4	0.193

C. Experimental design

Using the full scope simulator for Yonggwang Nuclear Unit 3 and 4, we obtained the alarm lists for three process deviations, loss of coolant accident (LOCA), loss of feedwater accident (LOFA) and steam generator tube rupture (SGTR). We recorded the alarms every 5 seconds. Supervisory reactor operators (SRO) of Yonggwang Nuclear Unit 3 and 4 determined the key alarms for identifying each deviation. In consideration of experimental participants' knowledge, we excluded some alarms (e.g., the alarms related to control element driving mechanism control system (CEDMCS)) from this key alarm list in order to avoid confusing participants. This key alarm lists are called 'standard key alarm sets (set 1)'. The effect of the knowledge of operators (training program or operation experience) can be addressed by using different key alarm sets. In order to address this effect, we made another key alarm sets, called 'shortened key alarm sets (set 2)', in which we intentionally hide some alarms of set 1.

We parted participants into two groups (one for set 1 and the other for set 2) and provided them with a brief description of deviations (LOCA, LOFA and SGTR). For each deviation, it also contained the names and explanations of the alarms of each key alarm set. An assistant gave the participants short instruction about this experiment. The assistant requested the participants to memorize key alarm sets and their descriptions. Then, he initiated DAC and showed the first priority alarm screen to the participants. The alarms presented in the first priority alarm screen are determined by the 1st threshold value (see Figure 2). In order to examine the effect caused by the level of reduction, we applied two 1st threshold values (α and β). The 1st threshold value, α was higher value, so it leads to the smaller number of alarms in the first priority alarm screen than β did.

The assistant requested participants to identify the deviation before each deviation scenario finished. The order of displayed problems (deviation scenarios) is random and unknown to the participants. Each participant solved six problems (3 deviations × 2 criteria). Totally, we had 12 variations in experimental results (3 deviations × 2 criteria × 2 sets of key alarm).

D. Results and discussion

Table 2 represents the evaluation results. It shows the results of alarm processing by DAC (the number of hit alarms, false alarms and missed alarms). It also shows the experimental results (correct identification rate) and *R* (*K*, *P*) values. The *R* (*K*, *P*) values are calculated using Equation (7) for each case. The Pearson correlation coefficient (the point estimate of correlation coefficient) between the identification rate and *R* (*K*, *P*), 0. 644, is obtained by using a data analysis software package, SAS. The result also shows that the hypothesis, 'there is no relationship between the identification rate and R (K, P)' would be rejected (p<0.03). For the comparison, E [2] and A' [4] are calculated for this experiment. The Pearson correlation coefficient between the identification rate and the E is 0.00733 and that between the identification rate and A' is 0.53602. These results show that R (K, P) is superior to E and A'.

One may think that they ought to be recognized easily even by conventional alarm systems because LOCA, LOFA and SGTR are very severe transients. However, without alarm reduction mechanisms, even skillful experts tend to be confused when hundreds of alarms are presented (179 alarms are activated in the case of LOCA within 20 minutes, 104 alarm in LOFA, and 175 alarms in SGTR). In Park's experiment [2], less than 30% of experts identified the LOCA deviation. In consideration of the participants of this experiment, graduate students, the correct identification rates are not that bad. The Pearson correlation coefficient of 0.644 implies moderate relationship [13]. We believe that detailed consideration of the personal characteristics (such as prior knowledge of nuclear power plant systems and alarm systems) will provide higher correlation coefficient.

In this paper, we cannot compare the DAC with other alarm processing systems because there is the difficulty of other system's availability. However, 12 variations in this experiment show the validity of R (K, P) and the possibility of comparisons to other systems using R (K, P).

One can easily find the way to improve the usefulness of this alarm-processing system. The performance bottleneck of this system is located on LOCA deviation. When SROs assigned the priority of each alarm, they considered various possible deviations. So they assigned priorities higher than generally expected. With this type of prioritization database, we cannot reduce the number of alarms effectively – especially for the case of LOCA which is the most severe and sudden deviation of nuclear power plants. The modification of the prioritization database for the LOCA deviation is a fairly complicated problem. We can lower the priorities of some alarms. It might reduce the number of nuisance alarms in the LOCA but it may also reduce the number of hit alarms in other deviations. We should apply some different alarm reduction algorithms to solve this problem.

On the other hand, the operator training-materials' modification that will adjust the key alarm set is also one of the best ways to improve the human performance.

4. A Procedure for Evaluation in an Integrated Manner

As mentioned in the Introduction section, the evaluation result for a specific deviation, no matter whether it is experimental or theoretical, cannot represent that for the others. In this study, in order to develop an effective evaluation procedure in an integrated manner, we propose a procedure based on the AHP.

A. The AHP

Satty [14] originally proposed the AHP that aimed at facilitating decision-making in problems which involved multiple criteria. It is used to elicit weighing information from decision-makers through verbal, numerical or graphical means. Traditional AHP is known as the eigenvector method because it produces a corresponding weight matrix and eigenvector. In this paper, we will make a short introduction about the AHP, because its procedure is that well established.

The followings are the steps for the completion of the AHP [15], [16]:

(1) Define the problem and reduce it to a number of factors or elements.

(2) Group the elements at different levels, forming a chain or hierarchy.

(3) Construct a pairwise comparison matrix of the relevant contribution or impact of each element on each governing element in the preceding higher level. In the AHP, weights are determined using pairwise comparison between each pair of criteria. Each comparison is then transformed to a numerical value. The numerical value of each comparison should not greater than 9. The result is a positive reciprocal matrix A= $\{a_{jk}\}$ with $a_{kj} = 1/a_{jk}$, where a_{jk} is the numerical equivalent of the comparison between criteria j and k.

(4) Determine the consistency within these matri-

ces using the vector of priorities. In order to compute the priorities of the elements in each matrix, the eigenvalues of each matrix are calculated. The priorities (normalized weight vector), w = (w_1, ..., w_N), is obtained by solving the equation $Aw = \lambda_{MAX} w$, where λ_{MAX} is the largest eigenvalue and w is normalized eigenvector associated with A and λ_{MAX}.

(5) Test for inconsistency using matrix theory. The consistency index (CI) is the deviation of the maximum eigenvalue (λ_{MAX}) from the number of criteria (n) used in the comparison process. That is, $CI = (\lambda_{MAX} - n) / (n - 1)$.

(6) Determine the consistency Ratio (CR), which is the ratio of CI and the corresponding random average consistency index (RI). At Oak Ridge National Laboratory, colleagues generated an average RI for a matrix of size n (See page 21 of [14]).

(7) Repeat steps 3, 4, 5 and 6 for all levels in the hierarchy.

(8) Determine the consistency of the entire hierarchy by summing the products of each CI and the priority of the corresponding criterion.

B. The problem definition and structure

Basically, one of the primary roles of alarm systems, both conventional and advanced ones, is the provision of cues or alerts that are useful for the identification of process deviation [2]. Therefore, the usefulness in the activity of identifying process deviations that must be considered is the most important factor in an alarm system's evaluation. Figure 3 shows an example of the problem structure of the alarm-processing system evaluation. Higher level factors are the severity of a deviation and the frequency of a deviation.

In this study, the validity of generalization is not an issue. It is principles and methodologies that are being examined. In order to apply the result of *R* (*K*, *P*) which is proposed and examined through above sections, the exemplary problem structure represented in Figure 3 is constructed. If one intends to get more generality, he/she should consider more number of deviations including accidents, non-accident transients and anticipated operational occurrences (AOOs). Also he/she should break down the severity of deviations into several parts (e.g., radiation leakage, system damage, etc.).

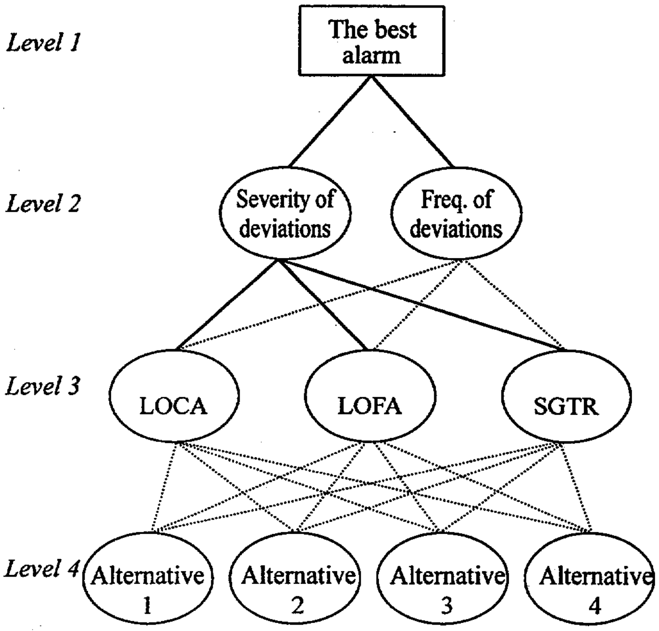


Figure 3. Hierarchical problem structure of this study This structure is aimed at examining principles and methodologies (not at generalizing the results).

C. Procedure

The hierarchical structure represented in Figure 3 implies that the problem requires six comparison matrices. One matrix is for the level 1 comparison (priority between the severity and the frequency), two for level 2 and three for level 3. It is noticeable that we can utilize the measure proposed in this paper for evaluating alarm systems for a specific process deviation. That is, we could make the comparison matrices for level 3 without subjective evaluation. In addition, the matrix for the frequency (level 2) comparison could be established without subjective evaluation. The Safety Analysis Report of Yonggwang Nuclear Unit presents the design-based calculation for the frequency of each deviation. Using these frequencies, we could establish the comparison matrix for deviation frequency.

The matrices remained for subjective evaluations are indicated with solid lines in Figure 3. The matrices for level 1 and level 2 are not operation-affairs but design-affairs. Therefore, in order to establish these two comparison matrices (one for the best system and the other for the severity of deviations), we made interview with safety analysists and system design engineers of Korea Power Engineering Company.

D. Results and discussion

The analysis begins with pairwise comparisons and development of a normalized matrix. Table 3 shows the established matrices for the best alarm system and the severity of deviation, respectively. In this study, we made five surveys for each matrix. Therefore, the data are the geometric mean of five matrices.

The Safety Analysis Report of Yonggwang Nuclear Unit 3 and 4 shows that the anticipating frequency of LOCA, LOFA and SGTR is 3.4×10^2 [#/10^6 years], 4.5×10^3 [#/10^6 years] and 5.75×10^5 [#/10^6 years], respectively. It is well known that a human being estimates quantities in logarithmic scale [9]. Therefore, $a_{ij} = \log(freq_i) / \log(freq_j)$. Table 3 shows the pairwise comparison matrix for the frequency of deviations and the normalized eigenvector.

As stated in section C, we could calculate a_{ij} by $R(K, P)_i / R(K, P)_j$. It is not logarithmic scale because $R(K, P)$ is originally designed based on logarithmic function. In fact, we already showed that $R(K, P)$ is in proportion to human performance.

Table 3. Pairwise comparisons

Best system	Severity	Frequency	Eigenvector
Severity	1	1.380	0.579
Frequency	0.725	1	0.421

Severity	LOCA	LOFA	SGTR	Eigenvector
LOCA	1	6.434	5.909	0.737
LOFA	0.155	1	0.272	0.076
SGTR	0.169	3.680	1	0.187

Frequency	LOCA	LOFA	SGTR	Eigenvector
LOCA	1	0.693	0.440	0.212
LOFA	1.443	1	0.634	0.306
SGTR	2.275	1.577	1	0.482

LOCA	S1 + α	S1 + β	S2 + α	S2 + β	Eigenvector
S1 + α	1	1.056	0.916	0.966	0.245
S1 + β	0.947	1	0.868	0.915	0.233
S2 + α	1.092	1.153	1	1.055	0.268
S2 + β	1.035	1.093	0.948	1	0.254

LOFA	S1 + α	S1 + β	S2 + α	S2 + β	Eigenvector
S1 + α	1	1.170	1.042	1.219	0.245
S1 + β	0.855	1	0.891	1.042	0.233
S2 + α	0.959	1.122	1	1.170	0.268
S2 + β	0.820	0.959	0.855	1	0.254

SGTR	S1 + α	S1 + β	S2 + α	S2 + β	Eigenvector
S1 + α	1	1.152	0.850	0.962	0.245
S1 + β	0.868	1	0.738	0.835	0.233
S2 + α	1.177	1.356	1	1.133	0.268
S2 + β	1.039	1.197	0.883	1	0.254

Next step is the calculation of consistency indices. Among these six matrices, the matrix for severity is the only one which requires consistency check. From the matrix for the best alarm system, we always get the best consistency index (CI = 0) because it has only two columns and rows. From the other 5 matrices, we also always get CI = 0 because they are established by numerical calculations. CR should never exceed 20% and generally CR should be 10% or less to be acceptable [15]. Followings are the procedure for calculating consistency indices for the severity matrix.

$n = 3.$

$\lambda_{MAX} = 3.166.$

$RI(n = 3) = 0.58.$

$CI = (\lambda_{MAX} - n) / (n - 1) = (3.166 - 3) / (3 - 1)$
$= 0.083.$

$\therefore\ CR = CI / RI = 0.083 / 0.58 = 0.143.$

Then, using eigenvectors in Tables 3, the overall vector of priorities is calculated by following matrix operation and can be presented as in Table 4.

$$\left\{\begin{bmatrix} 0.245 & 0.275 & 0.245 \\ 0.233 & 0.235 & 0.213 \\ 0.268 & 0.264 & 0.288 \\ 0.254 & 0.256 & 0.254 \end{bmatrix}\begin{bmatrix} 0.737 & 0.212 \\ 0.076 & 0.306 \\ 0.187 & 0.482 \end{bmatrix}\right\}\begin{bmatrix} 0.579 \\ 0.421 \end{bmatrix} = \begin{bmatrix} 0.250 \\ 0.227 \\ 0.274 \\ 0.254 \end{bmatrix}$$

Table 4. Overall vector of priorities

Alternative	Priority
Set 1 + Cr. α	0.250
Set 1 + Cr. β	0.227
Set 2 + Cr. α	0.274
Set 2 + Cr. β	0.254

Composed CI for overall matrix is calculated as fol-
lows:

$$\text{Composed CI} = 0 + \begin{bmatrix} 0.083 & 0 \end{bmatrix} \begin{bmatrix} 0.579 \\ 0.421 \end{bmatrix} + 0 = 0.048 \cdot$$

The priority values obtained in this analysis can be used to support a decision made in regard to the selection of one of the alternatives in the hierarchy. The result implies that the third (Set 2 + Cr. α) is the best alternative, and the second (Set 1 + Cr. β) is the worst. As shown in Table 3, the severity is more important than the frequency. The LOCA deviation has the largest priority for the severity. The third alternative scores the best in the LOCA deviation. The SGTR has the largest priority for the frequency. The third alternative also scores the best in the SGTR deviation.

The result might also be interpreted as follows:

(1) With the effectively established alarm set (key alarm set 2), the smaller number of alarms (criterion α) are enough to identify the deviation.

(2) Even with the rich alarm set (key alarm set 1), the presented alarms by criterion β are too much.

We should remind that the training (key alarm set) and the alarm-processing method (criterion) make a pair and that they cannot be considered in a separate manner. For example, by the result in Table 4, we cannot conclude that the key alarm set 2 is better than the key alarm set 1. It depends on the alarm-processing method. Generally, the use of the AHP in this example produced a simple and exact solution to the problem. It successfully integrates a series of evaluation results for deviations.

5. Conclusions

In this work, we propose *R* (*K*, *P*), a measure for an alarm-processing system's usefulness. It is designed to perform user-oriented evaluation based on the informational entropy concept. It is expected to effectively quantify the cognitive complexity, which users perceive when they work with alarm-processing systems. It will be especially useful in early design phase because we could estimate the usefulness of an alarm system by the short calculations instead of the consumptive operator-based tests.

Based on the AHP, we also propose a procedure for evaluating alarm-processing systems with regard to integrating a series of deviations. It aims to perform effective simulator-based evaluations of an alarm system's design. It provides a relative rank among alternative alarm systems by integrating the evaluation results of the usefulness on identifying deviations. The conventional AHP determines weights using the subjective pairwise comparison between each pair of criteria. In this paper, we reduce the number of pairwise comparisons by introducing the measure, *R* (*K*, *P*).

The result of the experiments for the proposed measure shows that as the problem contains larger *R* (*K*, *P*), the correctness of identifying process deviations becomes higher. The larger *R* (*K*, *P*) implies better match between the operator training program and the processed alarms. That is, the experimental result shows that both the operator training program and the alarm processing method should be considered concurrently when evaluating alarm systems. It also shows that the *R* (*K*, *P*) is superior to the other measures in predicting the correctness of deviation identifications.

In order to show the validity of the integrating procedure which is proposed in this paper, we present an exemplary application. Generally, this AHP based evaluation procedure successfully integrates a series of evaluation results for deviations and clearly shows relative ranks. More investigation including the enlargement on various deviations will provide a valuable guideline for the alarm system evaluation.

Subjective evaluations for the newly developed alarm system might be still required in validation phase, but we expect that the proposed measure and procedure will effectively reduce the number and peits readiness for use, and so on; and (2) investigation into the assumptions and limitations of the model, its appropriate uses, and the reason why it produces the results [1]. The objective for FDS evaluation is twofold. The first is to integrate evaluation into development process. Evaluation is needed as feedback at each step of development. Due to the iterative and incremental nature, it is of primary importance that evaluation is performed after each step so that the work done is assessed and wrong construction steps are corrected [2]. Moreover, evaluation is an implicit activity in each development step of the blueprint; it is required to deal with the various types of judgments and decisions, by users and developers alike, that are inherent in the development process. The second is to compare alternatives. When different FDSs are the alternatives that are proposed to be implemented for the same problem, it is necessary to compare and rank them based on appropriate criteria.

We first define the dynamic aspects of FDS in this work. Dynamic aspects are concerned with the way FDS responds to the input. Dynamic aspects include what FDS provides and how FDS operates. On the contrary, static aspect is concerned with the hardware and the software of the system. Since static aspects depend on which program language is used and which maker's hardware system or what kind of system is used, only dynamic aspects of FDS are chosen for the evaluation targets in this work. We present the hierarchical structure of the evaluation criteria for dynamic aspects of FDS. For quantitative evaluation, we calculate the relative weights of the criteria. The method used to gain and aggregate the priority of the components in this work is AHP. The criteria at the lowest level are quantified by simple numerical expressions and questionnaires developed in this work that are considered to well describe the characteristics of the criteria. A main focus of our work is to evaluate a single system quantitatively by proposing the index to quantify the criteria of the lowest level. In the previous researches using the AHP, because of comparing alternatives for each criterion, they could not evaluate a single system. In order to evaluate a new developed system, these methods have the weak point that they need equivalent systems implemented for the same purpose to compare. Finally, in order to demonstrate the feasibility of our proposition, we performed one case study for the fault diagnosis module of OASYS^{TM} (On-Line Operator Aid SYStem for Nuclear Power Plant), which is an operator support system developed at Korea Advanced Institute of Science and Technology (KAIST) [3].

II. Definition of the criteria for evaluating a FDS' dynamic aspect

Defining evaluation criteria is necessary to carry out evaluation. We characterize dynamic aspects as the way a FDS responds to the input. Dynamic aspects include what a FDS provides and how a FDS operates. We define the former as *content* and the latter as *behavior*. After having reviewed the features of FDSs, we have selected the primitives considered as important factors in nuclear power plant operation. Content and behavior have two and six elements in the lower hierarchies, respectively. The content is a criterion for evaluating the integrity of a FDS, the problem type which a FDS deals with, and the level of information. The behavior is for evaluating robustness, understandability, timeliness, transparency, effectiveness, and communicativeness of FDSs. The criteria include the evaluation of knowledge base, inference engine, and user interface that are the major components of an expert system.

II.1 Content

Content is related with what a FDS provides. "For a given problem, if FDS provides correct answers", or "For a given fault, if a FDS can generate the diagnostic results" corresponds to *content. Content* can be evaluated in terms of *coverage* and *integrity.*

A. *Coverage*

Coverage represents the set of domain concepts and the types of problems a FDS can deal with [2]. It can be further decomposed into two components as follows:

· *Extent - Extent* represents the set of entities, properties, and relations a FDS deals with. Extent is concerned with the faults and the systems the FDS diagnoses. Extent is a criterion which evaluates whether a FDS can generate diagnostic results for the faults or the systems it is expected to diagnose when it is implemented in the NPP.

· *Depth - Depth* represents the level of the information a FDS provides. A FDS not only diagnoses the faults after analyzing the obtained values of plant parameters but also notifies operators to be in abnormal situation and suggests the corrective actions [4]. The depth evaluates the level of depth of information.

B. *Integrity*

Integrity means the ability of a FDS to generate correct solutions for a given problem within its actual coverage. For example, the fact that a FDS provides LOCA for the symptom of steam line break as the result of diagnosis, concerns *integrity.* The soundness of knowledge base and the accuracy of inference engine have effects on *integrity.*

II.2 Behavior

Behavior concerns how a FDS provides operators with information and how it behaves during operation, i.e., the way and the form its problem solving activity is actually carried out and displayed to operators. *Behavior* contains usability, user satisfaction, ease of use, and so on. *Behavior* is categorized into six aspects as follows:

A. *Robustness*

Robustness represents the ability of a FDS to behave in an acceptable and consistent way when at out of its extent. For example, for a FDS diagnosing turbine generator faults, when secondary loop pressure drops due to the fault of other facilities, the fact that the FDS provides the result of "Turbine generator is normally operating. Pressure drop may be caused by the fault of another facility." concerns *robustness.* In safety critical systems such as nuclear power plants, the situation that a FDS does not give any result to operators when faults occur can lead to a serious problem.

B. *Understandability*

Understandability means the ability of a FDS to behave in a way operators understand its operation easily. "How much coincident the operator's internal model of NPP is with the FDS's representation" is related with *understandability*. Accordance of a FDS's representation with the operator-training model is an influential factor on *understandability*. Using the language easy to understand is also an important factor.

C. *Transparency*

Transparency represents the ability of a FDS to provide the information which operators want to know so as to have a deeper understanding of the situation, for example, alarm data and values of plant parameters. The information which operators can query during the operation are also inference processes, values or trends of plant parameters and help menu.

D. *Effectiveness*

Effectiveness represents the ability of a FDS to provide results effectively. The number of wrong hypotheses resulting from diagnosing the symptoms of plant before arriving right solutions concerns *effectiveness*. Generally, FDSs do not provide only one diagnostic result, but display several potential faults with each probability or confidence level generated in inference process. The system that gives reliable hit results and fewer wrong results can be called a good system in effectiveness.

E. *Communicativeness*

Communicativeness represents the ability of a FDS to provide the effective and easy-to-use man-machine communication or interaction. The I/O device and environmental equipment which are familiar to operators and easy to use, concern *communicativeness*.

F. *Timeliness*

Timeliness represents the ability of a FDS to provide appropriately the diagnosis results in time. For example, the fact that the diagnosis results which are provided after the due time when operators must take response actions to faults is meaningless concerns *timeliness*. Timeliness is important in nuclear power plant when operator's fast reaction to abnormal situations is necessary.

III. Prioritizing the evaluation criteria for dynamic aspect of NPP FDS

In this study, we use AHP to prioritize the evaluation criteria defined in previous section. Satty [5] originally proposed AHP that aimed at facilitating decision-making on problems which involved multiple criteria. It is used to elicit weighing information from decision-makers through verbal, numerical or graphical means. Traditional AHP is known as the eigenvector method because it produces a corresponding weight matrix or an eigenvector.

In order to prioritize the criteria defined in the previous section, seven experienced researchers of directorial caliber working at the department of computer system design in KOrea Power Engineering Company (KOPEC) were asked to answer the questionnaire to inquire personal preference about the criteria. The reason of choosing the system designers is that it is thought that they have more knowledge about system requirements and system evaluation than operators. The designers have bestowed higher priority on *content* than *behavior*. For behavior, it is reasonable that the attributes related with safety, such as *robustness* and *timeliness*, are regarded as more important factors. Figure 1 shows the hierarchy of the criteria and their normalized priorities obtained from the questionnaire to the designers.

<Figure 1 The hierarchy of the criteria and normalized priorities >

IV. Quantitative evaluation for dynamic aspects of NPP FDS

The method used for quantitative evaluation in this work is to sum weighted measures. Weighting factors follow the priorities calculated in the previous section. For the criteria at the lowest level of the hierarchy, the measures are proposed in this work. The measures are given with the value between 0 and 1 by means of expressions or methods that are developed in this work. This method makes not only the comparative evaluation but also the absolute evaluation possible. As the conventional approaches using the AHP have performed the evaluation by comparing alternatives for the lowest criteria and computing the preference for each criterion in the same way as in obtaining the priorities, they can not be applied to the absolute evaluation.

The overall evaluation value of a FDS is calculated as follows.

$$E_{overall} = \sum_{i=1}^{k} W_i E_i = W_{content}\ E_{content} + W_{behavior}\ E_{behavior} = 0.555\ E_{content} + 0.445\ E_{behavior}$$

When the weights $W_{content}$ and $W_{behavior}$ follow the priorities calculated in the previous section, $E_{content}$ and $E_{behavior}$ are the scores to evaluate the content and the behavior, respectively and they are obtained as in the followings.

IV.1 Evaluation of the content

$E_{content}$ is obtained according to the following formula:

$$E_{content} = W_{coverage} E_{coverage} + W_{integrity} E_{integrity} = 0.484028 E_{coverage} + 0.515972 E_{integrity}$$

$E_{coverage}$ is also computed as follows.

$$E_{coverage} = W_{extent} D_{extent} + W_{depth} D_{depth} = 0.591668 D_{extent} + 0.408332 D_{depth}$$

D_{extent} and D_{depth} of the lowest level are quantification indices for the extent and the depth, respectively, and are quantified by the following measures:

· *The extent index,* D_{extent}

$$D_{extent} = \frac{\textit{the number of the systems or faults a FDS is able to diagnose}}{\textit{the number of the systems or faults a FDS is expected to diagnose}}$$

· *The depth index,* D_{depth} The quantification index for depth is as shown in Table 1. According to the level of depth of Table 1 that a FDS provides, D_{depth} is determined.

< Table 1 The depth index>

$E_{integrity}$ is given as follows:

The integrity is twofold: the accuracy of knowledge base and the accuracy of inference engine. The integrity is quantified by the following expression. The expression $E_{integrity}$ means the probability that knowledge base is accurate and given that the knowledge base is accurate, inference process is accurate.

$$E_{integrity} = D_{knowledge} \times D_{inference}$$

$D_{knowledge}$ *and* $D_{inference}$ are the indices representing the accuracy of the knowledge base and the inference engine, respectively and are calculated as follows:

- *The probability index that the knowledge base is accurate,* $D_{knowledge}$

$$D_{knowledge} = \frac{the\ number\ \ of\ correct\ rules}{the\ number\ \ of\ total\ rules}$$

- *The accuracy index of inference engine,* $D_{inference}$

$$D_{inference} = \frac{\sum H_i \times R_i}{The\ Number\ of\ Scenarios}$$

H_i = 0 (not hit) or 1 (hit)

R_i = Confidence level or Probability of i th Scenario's hit

IV.2 Evaluation of the behavior

Behavior is divided into six elements. $E_{behavior}$ is calculated according to the following formula:

$$\begin{aligned} E_{behavior} &= W_{robustness}D_{robustness} + W_{understandability}D_{understandability} + W_{transparency}D_{transparency} + \\ &\quad W_{effectiveness}D_{effectiveness} + W_{communicativeness}D_{communicativeness} + W_{timeliness}D_{timeliness} \\ &= 0.297056D_{robustmess} + 0.092223D_{understandability} + 0.152133D_{transparency} + \\ &\quad 0.121553D_{effectiveness} + 0.099785D_{communicativeness} + 0.23725D_{timeliness} \end{aligned}$$

Six criteria of behaviors are quantified by the following measures:

- *The robustness index,* $D_{robustness}$,

$$D_{robustmess} = \frac{the\ number\ of\ a\ FDS\ to\ provide\ some\ appropriate\ warnings,\ or\ explanations}{the\ number\ of\ cases\ out\ of\ extent}$$

- *The understandability index,* $D_{understandability}$ The understandability is evaluated through subjective method using a questionnaire to ask operators' opinion. The questions are developed using a five point Likert-type scale: 1 = "very poor"; 2 = "poor"; 3 = "neither poor nor good"; 4 = "good"; and 5 = "very good". Table 2 shows the questionnaire.

< Table 2 The questionnaire for evaluating the understandability>

- *The transparency index,* $D_{transparency}$

$$D_{transparency} = \frac{1}{4}\sum_{k=1}^{4} T_k$$

where,

T_k = 0 (not provided), 0.33 (poorly provided), 0.67(fairly provided), 1 (excellently provided)

k : 1 = inference or internal process
2 = alarm data
3 = values or trends of plant parameters
4 = help menu

· *The effectiveness index, $D_{effectiveness}$*

$$D_{effectiven\,ess} = \frac{\begin{array}{c}\textit{sum of the probabilit ies or levels of confidence of right hypotheses}\\ \textit{provided by a FDS}\end{array}}{\begin{array}{c}\textit{sum of the probabilit ies or levels of confidence of all hypotheses}\\ \textit{provided by a FDS}\end{array}}$$

· *The communicativeness index, $D_{communicativeness}$,* The communication index is following the rating scale values shown in Table 3 for three elements: ease of use and familiarity of input devices, output devices, and the rest of operation equipment. The sum of the elements is normalized to 1.

< Table 3 Rating scale values for *communicativeness*>

· *The timeliness index, $D_{timeliness}$*

$$D_{timeliness} = 1 - \frac{t_d}{t_o}$$

t_o : the time interval from fault occurrence to due time when operator's action is essentially required

t_d : the time interval from fault occurrence to time when the right diagnostic results are provided

V. A case study – OASYS^{TM}

In this section, we introduce a sample FDS, OASYS^{TM} [3], in order to demonstrate feasibility of the evaluation method presented in this work. The OASYS^{TM} is a FDS which is designed to support emergency actions and to diagnose the failure according to the plant's states. The main functions of the OASYS^{TM} are as follows:

1) On-line signal processing
2) Display of major parameters
3) Prediction of major parameters
4) Monitoring the Critical Safety Functions (CSFs)
5) Graphical display of RCS Pressure-Temperature (PT) curve
6) Temporal trend display of major parameters

7) Early judgment of a plant state
8) Display and printing of logging sheets
9) Providing alarm guidance for each alarm
10) Processing multiple alarms
11) Failure diagnosis in case of multiple alarm actuation
12) Automatic processing of the emergency response procedures (ERGs)
13) Graphical display of ERG flow charts
14) Long-term storage data in its memory

The OASYS^{TM} got the score of 0.8090 = 0.555×0.8946+0.445×0.7023 as a result of the evaluation by the method proposed in this work. Figure 2 show the points the OASYS^{TM} scored. Since it has been already implemented in 1994, it was difficult to define the extent, that is, the faults and systems the OASYS^{TM} is expected to diagnose. In addition, the OASYS^{TM} can diagnose almost all of the accidents and the faults in general, abnormal, and emergency operating procedures of NPP. Thus, we gave 1 to the extent. The OASYS^{TM} scored 1 on the depth, for it provides all of the occurrence of faults, the diagnostic results, and the corrective actions. Though the OASYS^{TM} has a sound knowledge base, it gives hit results with some deviations from the maximum confidence level of 1. Therefore, it scored 0.7958 on the integrity. In order to evaluate understandability, twelve operators of Yonggwang NPP's unit 3 and 4 in Korea were asked to answer the questionnaire. The result was 0.6806 and the variance of the result was 0.00484. For the transparency, it does not provide its inference process. However, other factors of the transparency are excellent. The result was 0.6875. The reason why its effectiveness is so low (0.4336) is that the wrong results generated by OASYS^{TM} have high confidence levels, compared with those of the hit results. Since the OASYS^{TM} uses easy-to-use interfaces such as the window-based display, Unix system, mouse and so on, we gave the high score, 0.8333, to communicativeness. In this case study, we set the time interval, t_o, as the time interval from fault occurrence to reactor trip. It scored 0.4299 on the timeliness as the evaluation result.

When we analyze the evaluation results of the OASYS^{TM}, the OASYS^{TM} had a soundness of the knowledge base, a good user-interface, and an excellent ability to provide the various kinds of information as shown in Figure 2. However, it scored low points on effectiveness, timeliness, and integrity and that means its inference engine does not work in an elegant way.

< Figure 2 The result of the evaluation for the OASYS^{TM}>

VI. Conclusion

In this study, we defined the dynamic aspects of a NPP FDS and the evaluation criteria. In addition, a quantitative evaluation method of the criteria was proposed. The functional components of FDS's dynamic aspects were modeled in a hierarchical structure. Then, we used the AHP's scoring method to find the relative weights of the components. One of our contributions in this work is the suggestion of measures for the absolute evaluation of a FDS. Previous researches have used AHP mostly to compare alternatives. Another of our contributions is to use the quantitative measures with relatively simple expressions. Proposing the approach that uses appropriately subjective, empirical, and technical methods Adelman classified [6], we tried to make the evaluation process simple and easy.

A FDS can be regarded as a compensator in control theory. It should help operators to make quick and correct decisions. Whereas the evaluation issue was on the problem of accuracy in the early days of the development of FDSs, it is changing to the problem of user friendliness and operator-supporting ability, namely, the function of compensator. The method proposed in this work focused on these new evaluation criteria as well as the accuracy of a FDS.

In our proposed method, evaluators play an important role in evaluation. The evaluators should have unbiased and objective insights into FDSs. Therefore it is desirable for the evaluators to be excluded in the development team. Since more FDSs are considered to be implemented in order to reduce the operator's workload and to support their decisions, the proposed criteria can be a guideline and a requirement for FDS developments. Furthermore, it is thought that it can be extended to other man-machine systems in NPP with some modifications.

VII. References

[1] Denis Borenstein, "Towards a practical method to validate decision support systems," Decision Support Systems, Vol.23, 227-239, 1998

[2] Giovanni Guida, Giancarlo Mauri, "Evaluating Performance and Quality of Knowledge-Based Systems: Foundation and Methodology", IEEE Trans. on Knowledge and Data Engineering, Vol.5, No. 2, 204-224, 1993

[3] Soon Heung Chang, "A Study on the Construction of Failure diagnosis and Emergency Response Supporting System for Nuclear Power Plants," Korea Electric Power Research Institute, Report No. KRC-91N-JO2, September 1994

[4] John A. Bernard, Takashi Washio, "Expert systems applications within the nuclear industry," American Nuclear Society, 1989

[5] Thomas L. Saaty, "Analytic Hierarchy Process", McGraw-Hill, 1980

[6] Leonard Adelman, " Evaluating decision support and expert systems," John Wiley & Sons, 1992

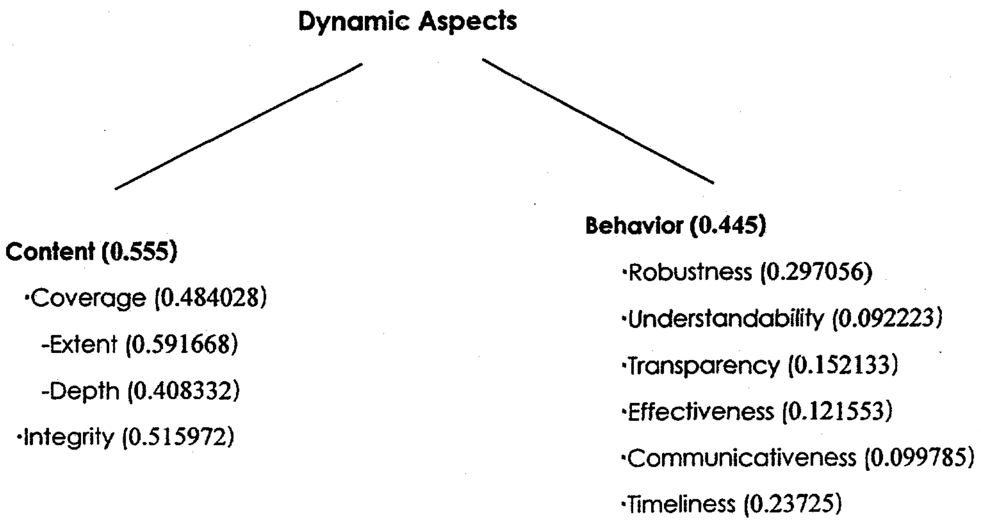


Figure 1 The hierarchy of the criteria and normalized priorities

Level of depth that a FDS provides	Quantification index
Nothing	0
Occurrence of faults	0.33
Diagnosis results	0.67
Operator's corrective action	1

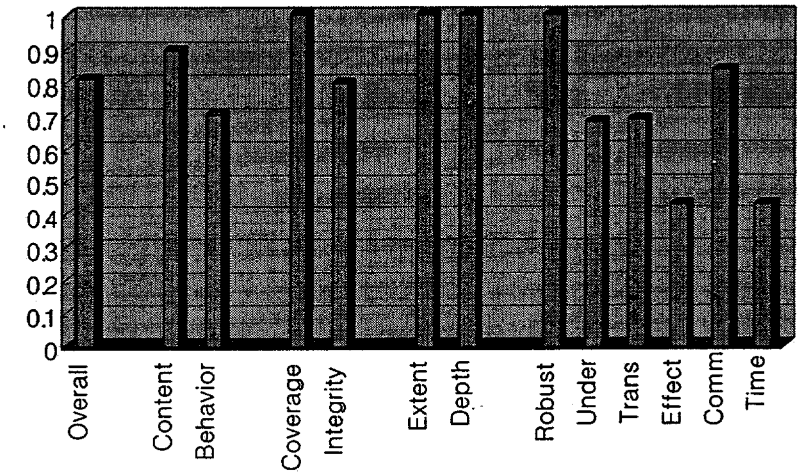
Table 1 The depth index

1. Do you think the output is presented in a useful format?
2. Is the information clear?
3. Are you happy with the layout of the output?
4. Is the output easy to understand?
5. Is the system user friendly?
6. Is the system easy to use?
7. Are the graphical modeling, graph, and table easy to understand?
8. Does the system match with personnel training & technical background?
9. Is the text and language used easy to understand?

Table 2 The questionnaire for evaluating the understandability

0	Very difficult, requires specialized mathematical or programming skills and then specialized training
0.25	Quite difficult, but required skill level and training is somewhat less
0.5	Requires concentrated training, but most people can acquire the method without difficulty
0.75	Requires only a little training, almost everyone can acquire the skill
1	Requires virtually no training, anybody can pick it up while using it after a few minutes

Table 3 Rating scale values for *communicativeness*



$E_{overall}$	Overall evaluation result	0.8090
$E_{content}$	Content	0.8946
$E_{behavior}$	Behavior	0.7023
$E_{coverage}$	Coverage	1
$E_{integrity}$	Integrity	0.7958
D_{extent}	Extent	1
D_{depth}	Depth	1
$D_{robustness}$	Robustness	1
$D_{understandability}$	Understandability	0.6806
$D_{transparency}$	Transparency	0.6875
$D_{effectiveness}$	Effectiveness	0.4336
$D_{communicativeness}$	Communicativeness	0.8333
$D_{timeliness}$	Timeliness	0.4299

Figure 2 The result of the evaluation for the OASYS^{TM}

Application of Human Factor Engineering Program For Safety Parameter Display and Evaluation System (SPADES) Design

Seung-Min Baek, Seung Han, Kang-Sik Sung, Jai-Bok Han
Korea Power Engineering Company, Inc.
150 Dukjin-dong, Yusong-gu, Taejon, 305-353, Republic of Korea
E-mail: smbaek@ns.kopec.co.kr

Yong-Hee Lee
Korea Atomic Energy Research Institute
150 Dukjin-dong, Yusong-gu, Taejon, 305-353, Republic of Korea
E-mail: yhlee1@nanum.kaeri.re.kr

ABSTRACT

The Safety Parameter Display and Evaluation System (SPADES) for the Korean Standard Nuclear Power Plants has been developed according to the safety parameter display requirements by applying the Human Factor Engineering (HFE) design concept in order to warrant high reliability and effectiveness. During the SPADES design process, a well-defined HFE design and implementation plan was established based on the HFE Program Review Model and applied to the entire design process from the planning to the evaluation stages. Therefore, it is believed that the SPADES can achieve a high system reliability and availability by reducing the human errors as well as the system errors. Furthermore, the HFE design concept developed for the SPADES design is applicable to the design of other computerized operator support systems for a nuclear power plant.

1. INTRODUCTION

Critical Function Monitoring System (CFMS), originally developed by ABB-CE in early 1980's, has been incorporated in Korean Standard Nuclear Power Plants to meet the Safety Parameter Display System (SPDS) requirements specified in NUREG-0696 [1] and NUREG-0737 supplement 1 [2]. The CFMS provides on-line monitoring and display functions for the critical safety functions and has been operated in Yonggwang nuclear units 3 and 4 (YGN 3&4) since 1995 and in Ulchin nuclear units 3 and 4(UCN 3&4) since 1998. However, it has been pointed out that the CFMS may not be useful under the emergency situation mainly because of the inconsistency with the Emergency Operating Procedure (EOP). Therefore, the Safety

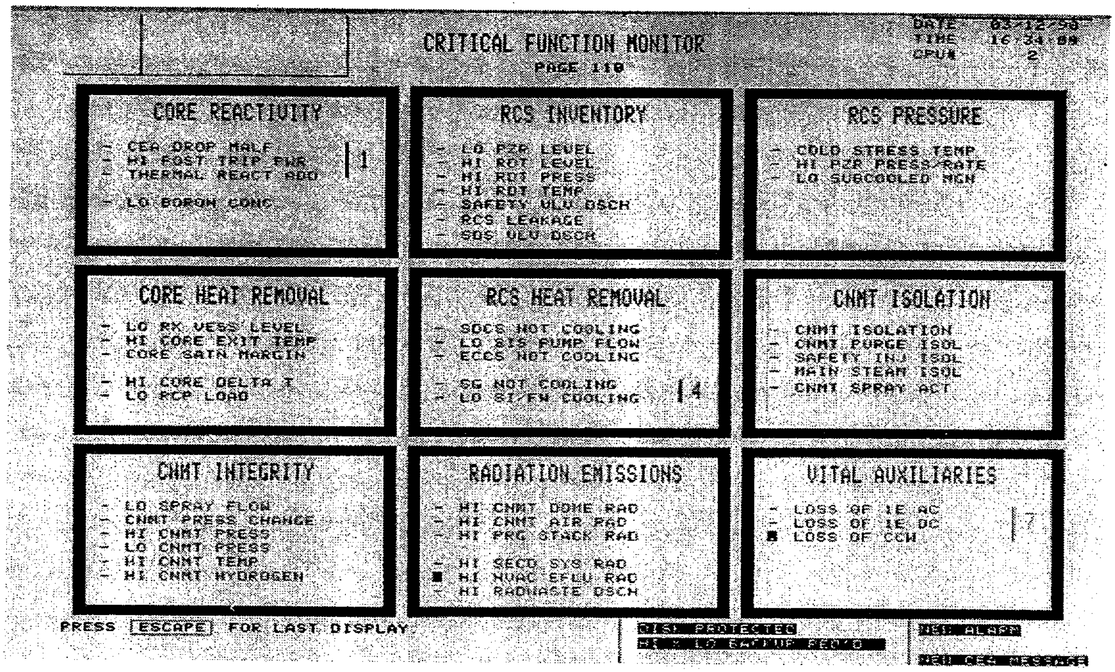
Parameter Display and Evaluation System (SPADES) has been developed to generate the consistent information with EOP so that it can support control room operators in determining the safety status of plant in a reliable and timely manner when the EOP needs to be implemented.

To meet the SPDS requirements, the SPADES is designed to provide operators with the Critical Safety Function (CSF) status information of the plant during all modes of operation. The information is provided in a concise, understandable and integrated format to assist operator or technical staff for a timely assessment of the plant safety status. Also, the SPADES was developed based on the human factor engineered design process to achieve a high reliability and to enhance human performance as compared to the CFMS. The process incorporated the human factor principles and guidelines so that the information can be readily perceived and comprehended by operators. The benefits of applying a systematic Human Factor Engineering (HFE) approach in the design process would be the improvement of interactions between systems and operators, the reduction of human errors by enhancing operator's working conditions, and the increased reliability and availability of the system.

At the initial stage of the SPADES design and development, a Human Factors Engineering Program Plan (HFEPP) was prepared to apply the HFE principles in such a way that the design activities could be defined clearly and performed among the well-organized HFE and design teams. The HFE program in the HFEPP includes HFE program management, operating experience review, functional requirements analysis, system requirements analysis, interface design, procedure development and HFE verification and validation. In this paper, the HFE program developed for the SPADES design process is presented in detail along with brief comparison of the CFMS and the SPADES.

2. DESIGN COMPARISON

The level 1 display of the current CFMS is illustrated in Fig. 1. As shown in this figure, the CFMS level 1 display consists of 9 safety functions which are inconsistent with the EOP in the aspect of priority and acceptance criteria of the CSFs. Also, the same CSFs are applied for all modes of plant operation regardless of the event characteristics under emergency conditions. Therefore, it has been pointed out that the operating personnel may not get appropriate plant status information from the current CFMS in performing the tasks described in the EOP. The SPADES level 1 display, illustrated in Fig. 2, was developed based on the EOP concept which emphasizes priority level of operator actions during a specific accident or recovery from



CRITICAL FUNCTION MONITOR
PAGE 110

DATE 03/12/98
TIME 16:34:09
CPU# 2

CORE REACTIVITY
- CEA DROP MALF
- HI FOST TRIP PWR
- THERMAL REACT ADD
- LO BORON CONC

RCS INVENTORY
- LO PZR LEVEL
- HI RDT LEVEL
- HI RDT PRESS
- HI RDT TEMP
- SAFETY VLV DSCH
- RCS LEAKAGE
- SDS VLV DSCH

RCS PRESSURE
- COLD STRESS TEMP
- HI PZR PRESS/RATE
- LO SUBCOOLED MGN

CORE HEAT REMOVAL
- LO RX VESS LEVEL
- HI CORE EXIT TEMP
- CORE SATN MARGIN
- HI CORE DELTA T
- LO RCP LOAD

RCS HEAT REMOVAL
- SDCS NOT COOLING
- LO SIS PUMP FLOW
- ECCS NOT COOLING
- SG NOT COOLING
- LO SI/FW COOLING

CNMT ISOLATION
- CNMT ISOLATION
- CNMT PURGE ISOL
- SAFETY INJ ISOL
- MAIN STEAM ISOL
- CNMT SPRAY ACT

CNMT INTEGRITY
- LO SPRAY FLOW
- CNMT PRESS CHANGE
- HI CNMT PRESS
- LO CNMT PRESS
- HI CNMT TEMP
- HI CNMT HYDROGEN

RADIATION EMISSIONS
- HI CNMT DOME RAD
- HI CNMT AIR RAD
- HI PRG STACK RAD
- HI SECD SYS RAD
■ HI HVAC EFLU RAD
- HI RADWASTE DSCH

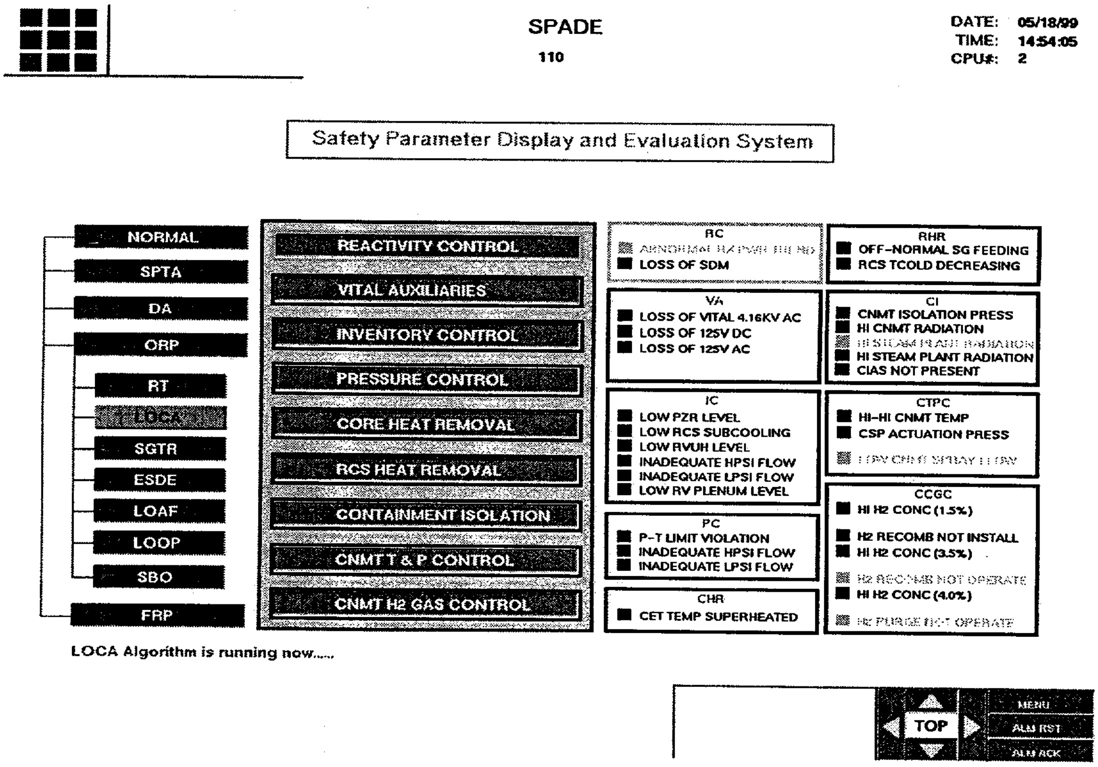
VITAL AUXILIARIES
- LOSS OF 1E AC
- LOSS OF 1E DC
■ LOSS OF CCW

PRESS ESCAPE FOR LAST DISPLAY

DISK PROTECTED
HI & LO BACKUP REQ'D

NEW ALARM
NEW CEA MESSAGE

Figure 1. Current CFMS Level 1 Display



SPADE
110

DATE: 05/18/99
TIME: 14:54:05
CPU#: 2

Safety Parameter Display and Evaluation System

RC
▨ ABNORMAL RX PWR TREND
■ LOSS OF SDM

RHR
■ OFF-NORMAL SG FEEDING
■ RCS TCOLD DECREASING

VA
■ LOSS OF VITAL 4.16KV AC
■ LOSS OF 125V DC
■ LOSS OF 125V AC

CI
■ CNMT ISOLATION PRESS
■ HI CNMT RADIATION
▨ HI STEAM PLANT RADIATION
■ HI STEAM PLANT RADIATION
■ CIAS NOT PRESENT

IC
■ LOW PZR LEVEL
■ LOW RCS SUBCOOLING
■ LOW RVUH LEVEL
■ INADEQUATE HPSI FLOW
■ INADEQUATE LPSI FLOW
■ LOW RV PLENUM LEVEL

CTPC
■ HI-HI CNMT TEMP
■ CSP ACTUATION PRESS
▨ LOW CNMT SPRAY FLOW

PC
■ P-T LIMIT VIOLATION
■ INADEQUATE HPSI FLOW
■ INADEQUATE LPSI FLOW

CCGC
■ HI H2 CONC (1.5%)
■ H2 RECOMB NOT INSTALL
■ HI H2 CONC (3.5%)
▨ H2 RECOMB NOT OPERATE
■ HI H2 CONC (4.0%)
▨ H2 PURGE NOT OPERATE

CHR
■ CET TEMP SUPERHEATED

LOCA Algorithm is running now.....

Figure 2. Developed SPADES Level 1 Display

accident. This display reflects task-oriented requirements extracted from the operator's task applied to the emergency operation.

The level 2 displays of CFMS and SPADES are very different because the SPADES provides alarm causes directly using alarm logic diagram display, while the CFMS only presents P&I diagram display for the major systems. Therefore, it is very difficult for operators to find out alarm causes when a CFMS alarm occurs. In addition to the alarm logic diagram display in the SPADES, the Resource Assessment Tree (RAT), which provides the systems or components status information for the success path to be implemented, is provided as a supplementary information in case of the Functional Recovery Procedure deployment. In spite of the fact that the RAT is the essential information in recovering the jeopardized safety function, the CFMS does not provide RAT display.

The CFMS has a system based display hierarchy so that it can provide sub-system and component displays in the level 3 display to support the level 2 displays. The level 3 display of the SPADES also consists of systems and components, but they are linked directly to the function based level 2 display. The level 3 displays can be used for evaluating the success path in emergency operation and provide the operators with the useful information for normal operation as well.

3. DEVELOPMENT OF HFE PROGRAM

A design and implementation process should include the required HFE program elements to develop an acceptable detailed design and the HFE evaluations to ensure that the final design reflects good HFE principles and that operator performance and reliability are appropriately supported for the protection of the public health and safety. Since the HFE acceptability focused on the detailed control room design reviews in the past as provided in NUREG-0700, rev 00 [3], the review on the design process was not emphasized. Thus, the US NRC staff evaluation criteria in Chapter 18 of NUREG-0800 [4] and in NUREG-0700, Rev.00 provide little information to support this type of evaluation. To support the advanced reactor design reviews, NUREG-0711 [5], "HFE Program Review Model", was developed by US NRC providing criteria for the evaluation of a design process and the final design implementation itself as well. Also, NUREG-0700, Rev. 01[6] describes HFE criteria for the evaluation of a design process.

NURGE-0711 requires that the system have following characteristics to ensure an acceptable design:

- The system to be developed by a qualified HFE design team, using an acceptable HFE program plan.
- The system to be resulted from appropriate HFE studies and analyses that provide accurate and complete input to the design process and the V&V assessment criteria.
- The system to be designed using proven technology based on the human performance and task requirements incorporating HFE standards and guidelines.
- The system to be evaluated in accordance with a thorough V&V test program.

HFE program for the SPADES design has been developed based on the HFE Program Review Model (PRM) so that the Human System Interface (HSI) could be designed and evaluated according to the HFE principles.

4. HFE DESIGN APPROACH FOR SPADES

To apply an acceptable HFE program to the SPADES design, the HFEPP for SPADES was developed at the early stage of design process. The HFEPP specifies the scope of design and the division of responsibility for design process, the purpose of applying HFE program on design process, the technical program to accomplish design goal, the organization of HFE and design teams, and the interface management between the teams. The HFE program decomposes the SPADES design process into eight elements as follows:

- HFE Program Management
- Operating Experience Review
- Functional Requirements Analysis
- System Requirements Analysis
- Interface Design
- Procedure Development
- Training Program Development
- Human Factors Verification and Validation

4.1 Overall Description of HFE Program

The purpose of HFE program is that the SPADES should be developed and evaluated using acceptable HFE principles based on the current HFE practices. The HFE program consists of the aforementioned eight elements of review process reflecting the four stages of design and implementation: planning, analysis, design and evaluation. The HFE program for SPADES design process is illustrated in Fig. 3.

At the planning stage, the plan for the SPADES design has been developed including goals and scope, review team, management process and procedures, and technical program.

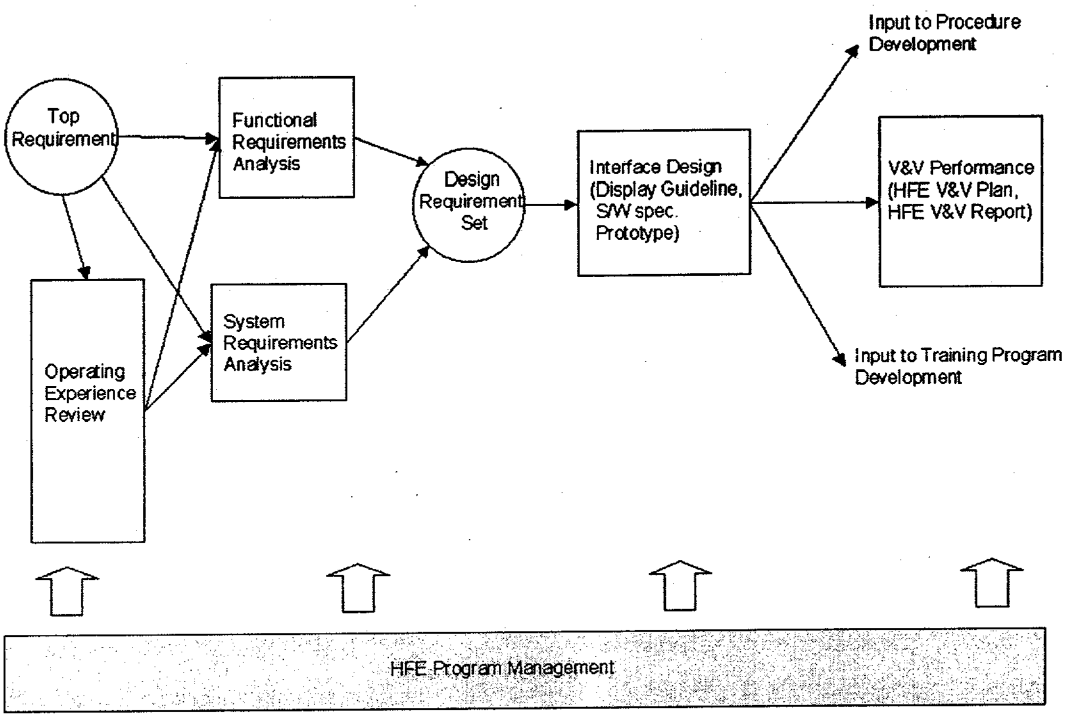

Top Requirement
Functional Requirements Analysis
Design Requirement Set
Interface Design (Display Guideline, S/W spec. Prototype)
V&V Performance (HFE V&V Plan, HFE V&V Report)
Input to Procedure Development
Input to Training Program Development
System Requirements Analysis
Operating Experience Review
HFE Program Management

Figure 3. HFE Program Model for SPADES Design Process

The activities performed at the analysis stage are as follows:

- Operating Experience Review(OER) including interview with operating crew
- Study on SPDS usability for the operating plants including YGN 3&4 and UCN 3&4
- Review of SPADES design requirements against regulatory requirements for the SPDS
- Survey on the major drawbacks in the current CFMS from the viewpoint of usability and on the HFE consideration learned from functional analysis, system requirements analysis in order to clarify the functional requirements and performance criteria of the SPADES

In the design stage, the SPADES design team performed system interface design and software design according to procedures established during the planning and analysis stages. The HFE team review on the HSI design was performed to ensure that the SPADES has been appropriately designed and implemented reflecting proper design process defined in the planning stage, and proper requirements, criteria and HFE principles identified in the analysis stage.

In the evaluation stage, the HFE verification and validation was performed to ensure that the SPADES has been designed and implemented to account for human capabilities and limitations. The Human Engineering Discrepancies (HEDs) were identified and documented in case that the SPADES design or implementation of HSI was inconsistent with HFE guidelines. The HEDs have been reviewed and evaluated for further improvement.

4.2 HFE Activities during SPADES Design Process

4.2.1 Planning Stage

The overall purpose of HFE program is to ensure that the HFE has been integrated into development, design and evaluation in order to design the system in a safe, efficient and reliable manner. The HFE team was guided by the HFEPP to ensure the proper development, execution, management and documentation of the HFE program. The HFEPP describes technical program elements ensuring that all aspects of HSI are developed, designed and evaluated on the basis of a structured top-down system analysis using accepted HFE principles. The HFEPP contains general HFE program goals and scope, HFE team organization, HFE process and procedures, HFE issue tracking and technical program to be performed during design process. The technical program in the HFEPP includes the description on the general development of implementation plans, analyses and evaluation for the SPADES.

4.2.2 Analysis Stage

1) Operating Experience Review

The operating experience review (OER) related to HSI issues was performed through the documentation review and the interview with operating crews as follows:

- ■ Documentation Review
    - HEDs from YGN 3&4 and UCN 3&4 CFMS HFE Verification and Validation
    - HEDs resolution for YGN 3&4 and UCN 3&4
    - HFE Review of UCN 3& 4 CFMS Display
    - Modified Items for Operating in Design Specification

- Interview with Operating Crew including Supervisory Reactor Operator(SRO), Reactor Operator(RO) and Technician in YGN 3&4 and UCN 3&4

After completion of the documentation review and the interview with operating crews, the effects of identified HFE issues on human performance and human error were evaluated and documented in the form of Table 1 for HFE issue tracking and management. In the Table 1, problems identified during review process are described in "ISSUE" column, and the design team review and their opinion for corresponding issue is explained in "REVIEW" column. Suggestions for resolution and implementation method are described in "DESIGN RESOLUTION" column.

NO.	ISSUE	REVIEW	DESIGN RESOLUTION	REF	DATE	DESIGN TEAM	REVIEWER

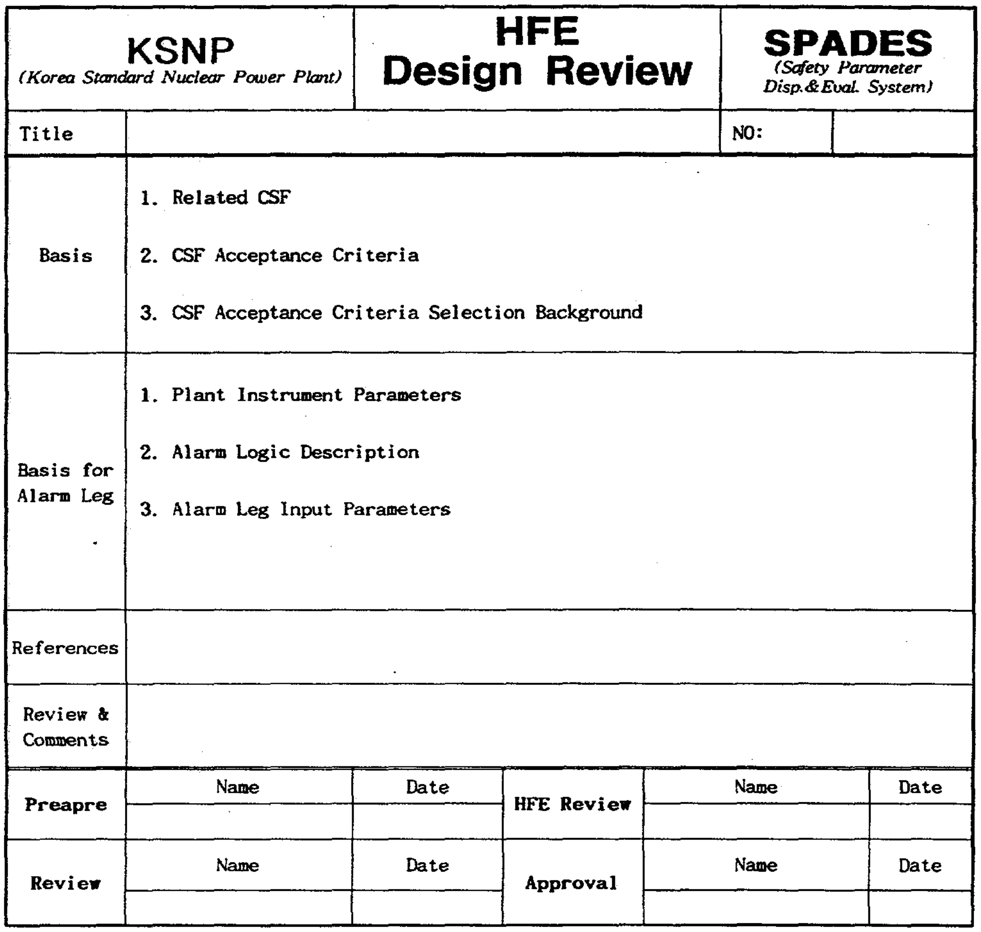
Table 1. Operating Experience Review Form

2) Functional Requirement Analysis

The purpose of Functional Requirements Analysis (FRA) is the identification of those functions that must be performed to satisfy plant safety objectives, that is, to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. The FRA is performed to determine the objectives, performance requirements and constraints of the design and also to define the functions that must be accomplished. The design team developed the functions based on the Functional Requirement Analysis and those functions were used as input in determining the SPADES configuration and hierarchical display structure and basis for the detail task analysis. FRA activities were performed by the design team and reviewed by HFE staff as follows:

- Analysis on current CFMS functions: To analyze acceptability of YGN 3&4 and UCN 3&4 CFMS and identify strength and weakness, and propose items to be improved.
- Emergency Operating Procedure Analysis
  - Analysis for appropriate Critical Safety Function (CSF) selection: To select valid CSF for normal and abnormal operations and analyze acceptability of selected CSF (Fig. 4).
  - Analysis for proper input parameter selection: To provide selection criteria of input parameters to implement alarm legs corresponding to each CSF (Fig. 4).

- Alarm Algorithm Generation for each CSF based on the EOP analysis results



KSNP *(Korea Standard Nuclear Power Plant)*		HFE Design Review		SPADES *(Safety Parameter Disp.&Eval. System)*	
Title				NO:	
Basis	1. Related CSF 2. CSF Acceptance Criteria 3. CSF Acceptance Criteria Selection Background				
Basis for Alarm Leg	1. Plant Instrument Parameters 2. Alarm Logic Description 3. Alarm Leg Input Parameters				
References					
Review & Comments					
Preapre	Name	Date	**HFE Review**	Name	Date
Review	Name	Date	**Approval**	Name	Date

Figure 4. HFE Design Review Form

3) System Requirements Analysis

The Software and hardware requirements for the SPADES were proposed and the bases for those requirements was provided by the design team. The HFE staff reviewed the proposed system requirements in such a way that the functional requirements could be satisfied with the identified system requirements. The activities to identify system requirements are as follows:

- System Information Requirements: To analyze all information and display parameters and provide proper reason for selection.
- Software Requirements: To describe software configuration and environment to support function and identify appropriate requirements.
- Hardware Requirements: To describe hardware configuration to support function and identify appropriate requirements.

4.2.3 Design Stage

1) Interface Design

The design team performed system design including system interface and software design according to the procedures and consideration established during the planning and analysis stages. The HFE staff reviewed to ensure that the design team has appropriately translated functional and system requirements to the detailed HSI design through the systematic application of HFE principles and criteria. Following activities were performed during the interface design period:

- Display Guideline Preparation: To provide specific guideline for the SPADES display elements such as symbol, terminology, menu, color, information presentation and information allocation considering acceptable HFE principles.
- Development Environment Evaluation: Design team to set up the development environment and HFE staff to evaluate if the development environment is appropriate to meet HSI design principles.
- Prototype Design: To define minimal set of SPADES function and to perform rapid prototyping to resolve HFE problem in early stage of design and to incorporate these solutions into the system design.
- Software Design: To implement the system and functional requirements of the SPADES defined in the analysis stage.
- Integration: To integrate the software and hardware to provide complete set of SPADES and to provide the environment for the validation. The evaluation to be conducted to ensure that the HSI includes all information and actions required to perform operator tasks and that the extraneous actions and displays not required for the accomplishment of any tasks are excluded.
- Documentation: To document all the requirements, the guidance, technical basis for the requirements and the evaluation results.

2) Procedure Development

It is recommended that the operating procedure be developed for operator to use the SPADES effectively. However, a plant specific operation guideline or an operating procedure has not been prepared in this phase. They will be prepared in coordination with utility when the SPADES is to be installed at site for actual use in operation.

3) Training Development

It is recommended that the personnel training program be set up for operating crew to use SPADES effectively. The training program should incorporate human factor principles and practices. However, a specific training program has not been developed in this phase. When SPADES is installed in plant site, an appropriate training program will be developed in coordination with utility.

4.2.4 Evaluation Stage: HFE Verification and Validation (HFE V&V)

The Verification and Validation evaluation comprehensively determines that the SPADES design conforms to the HFE design principles. The HFE V&V was performed based on the following documents and methodologies.

- HFE V&V Plan: HFE V&V Plan describes V&V organization and Division of Responsibility (DOR), V&V procedure, V&V activities and methodologies including availability verification, suitability verification and validation.
- V&V Activities:
  - Availability Verification

    Availability verification is the process of confirming that the required information content (displays, alarms) is actually provided to the operators. The required content is compiled and compared with the actual implementation.
  - Suitability Verification

    Suitability Verification is the process of confirming that the format of information in a system is acceptable for operator use. To verify suitability, the system displays and navigation features are evaluated in terms of applicable human factors design guidelines.
  - Validation

    Validation of the SPADES usability should confirm that necessary tasks could be performed in reliable and convenient fashion when it is expected to be used. Ideally, this would be performed in the simulator environment where plant upset conditions could be replicated.
- HED Evaluation: All the HEDs are evaluated to determine the need for the correction, to identify design solutions, to address significant HEDs and to verify the implementation of the design solutions resolving HEDs.

5. CONCLUSIONS

The well-defined HFE design and implementation plan was set up based on the HFE Program Review Model to reflect good HFE principles during the SPADES design process. The HFE program was formalized to be used in developing the system and configuring development method practically applicable from the planning to the evaluation stages. It is believed that the enhancement in system reliability and availability can be achieved by reducing human errors as well as system errors according to the application of well-defined HFE design program during the whole design process of the SPADES. Furthermore, the HFE design concept developed for the SPADES design is applicable to the design of other computerized operator support systems for nuclear power plant so that a more reliable and effective operator support system may be constructed.

6. REFERENCES

[1] NUREG-0696, Functional Criteria for Emergency Response Facilities, USNRC, 1981.

[2] NUREG-0737 (Supplement 1), Requirements for Emergency Response Capability, USNRC, 1982.

[3] NUREG-0711, Human Factors Engineering Program Review Model, USNRC, 1994.

[4] NUREG-0700, Rev. 00, Guidelines for Control Room Design Review, USNRC, 1981.

[5] NUREG-0700, Rev. 01, Human-System Interface Design Review Guideline, USNRC, 1996

[6] NUREG-0800, Standard Review Plan, Chapter 18.2, USNRC, 1984.

[7] Y. H. Lee, et al., KAERI/CR-024/96, Human Factors Reviews of CFMS Displays for UCN Nuclear Power Units 3 and 4, KAERI, 1996.

[8] KINS/AR-167, Standard Review Plan for SPDS of SAR, KINS, 1993

SESSION 4

FURTHER DEVELOPMENT AND TRENDS

IAEA Specialists' Meeting on
Human-Machine Interface for Off-normal
and Emergency Situations in NPP, 26 - 28 October 1999
Taejon, Rep. of Korea

Development of Alarm and Diagnosis-Integrated Operator Support System

In-koo Hwang, Jung-taek. Kim, Dong-young Lee, Hyun-chul Lee, Kee-choon Kwon
Korea Atomic Energy Research Institute
P.O. Box 105, Yusong, Taejon 305-353, Republic of Korea
(Fax : 82-42-868-8357, e-mail : ikhwang@nanum.kaeri.re.kr)

ABSTRACT

A computer-based alarm processing system for nuclear power plants, called Alarm and Diagnosis-Integrated Operator Support System(ADIOS), was developed using the 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 to another color in accordance with the priority 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 was constructed by analyses of the plant process as well as discussion with operators and nuclear plant experts. An evaluation on ADIOS was performed in two steps : (1)First, preliminary tests were conducted to refine the knowledge base and inference structure of ADIOS in a dynamic environment, and to evaluate the appropriateness of alarm-processing algorithms. (2)Secondly, A cognitive performance evaluation was performed using the Simulation Analyzer with the KAERI's Integrated Test Facility (ITF).

1. INTRODUCTION

Improvement in alarm processing and presentation in nuclear power plants has been a great concern for many years. 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, may lead the control room operators to be confused with avalanching alarms during plant transients. The advances in computer software and hardware technology, and also in information processing provide a good opportunity to improve the annunciator systems of nuclear power plants or other similar process plants. As a result, considerable works are underway worldwide to improve the alarm annunciator systems.[1-3]

Korea Atomic Energy Research Institute(KAERI) is developing an Alarm and Diagnosis - Integrated Operator Support system(ADIOS) for intelligent process monitoring, alarming, and diagnosis.[4,5] It was implemented by using G2 real-time expert system shell. The alarm system is aimed at presenting an optimal set of alarm information which will conform to the operator's mental model and facilitate their tasks of information gathering, interpretation, and decision making. In addition, the special features of sensor validation and diagnosis will be added to the alarm system to implement ADIOS.

ADIOS is connected to a Functional Test Facility(FTF)[6] model via a network to demonstrate an effective management of alarm annunciation in a more practical environment. Therefore, ADIOS has been tested in a simulated environment of various scenarios such as the TMI-2 accident, turbine trip, and so on. ADIOS then was evaluated for cognitive performance using the KAERI's Integrated Test Facility(ITF)[7]. The test result shows that the important benefits of this alarm system are the reduction of the number of activated alarms and dynamic prioritization of the alarm information to help the operation staff understand the plant's situation and cope with the occurring disturbances more rapidly and accurately.

2. ALARM CLASSIFICATION AND PROCESSING

2.1 Classification of Alarms

The alarm management in ADIOS is based on an alarm classification scheme which clearly distinguishes the types of alarms based on their inherent characteristics. The alarms are classified into three major categories: 1) process alarms, 2) status alarms, and 3) plant alarms.

The process alarms are either main or auxiliary process alarms, depending on whether they belong to the main process(i.e., reactor coolant system, steam generators, condensate and feedwater systems, and main steam system) or to auxiliary systems (e.g., component cooling water system, nuclear service cooling water system, circulating water system, or turbine plant cross cooling water system). The status alarms are divided into equipment-related alarms, equipment-status alarms, equipment-status information, system-status information, and system-trouble alarms.

An equipment-related alarm indicates an abnormality in the support function of equipment, for example, *pump bearing temperature high.* And, an equipment-status alarm is an indication that the equipment is at a state that it is not supposed to be in. *Pressure relief valve not opening* is an example of equipment-status alarm. For equipment-status alarms, a clear distinction was made between status information and status alarms. The equipment/system-status information is operating information of equipment or system such as a *Valve Open*, a *System Actuation*, etc. The status information and status alarms are presented to the operator separately, as opposed to the conventional alarm systems where they are intermingled. System trouble alarms include most of *Trouble/Disable* alarms which are being used in current conventional power plants. Important alarms at plant level, such as containment pressure, are classified to the plant alarms.

2.2 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. For example, 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, 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[8]. 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.

2.3 Processing and Prioritization of Alarms

ADIOS uses various alarm processing techniques such as equipment-state dependency, plant-mode dependency, alarm generation, cause-consequence relationship, and multi-setpoint relationship. In addition, other methods including categorization of alarms into the process alarms (e.g., temperature or pressure alarms of the main process) and 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 are key features of ADIOS. Figure 1 illustrates 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. 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.

2.4 Alarm Display

The presentation of alarms should conform to the operators' mental model of the process as much as practical. The alarm presentation in ADIOS aims at the operator's fast recognition of the overall plant or alarm situation, and also an easy access to any detailed alarm information. For this purpose, the prioritized alarms are displayed on the process overview mimic shown in figure 2, and also the chronological list of alarms is presented on another dedicated video display unit(VDU), with those alarms categorized by systems shown on the third VDU as a spatially dedicated soft alarm panel. Priority 1, 2, or 3 alarms are shown 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.

Intimately correlated process alarms are represented on the process overview mimic after being coalesced into groups. The group alarms, such as *"T_{avg}", "ΔT", "Flux", and "SGL"*, represent several related alarms. For instance, the *"SGL"* group alarm indicates that it represents a deviation in the steam generator (SG) level, high-high, high, low, and low-low SG level alarms. The group alarms take the highest priority among the associated subsidiary alarms that have been activated. For instance, if both *"high-high"* and *"high SG Level"* alarms are active and their priorities are 1 and 2, respectively, then the priority of the *SGL* alarm is set to 1.

Contrary to the above case, some alarm information is combined into one window unit in a conventional alarm systems. 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 a 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 resolves those kind of combined alarms and presents more detailed messages.

Status alarms (e.g., PORV not closed) are not directly shown on the overview mimic if no such alarms are active. However, for example, when the power operated relief valve(PORV) is open while it should be closed, the status alarm of PORV is indicated by changing the body color of the valve to red; the red color will blink until the operator acknowledges the alarm by clicking on the valve. The PORV status alarm is activated when the valve should have been closed because the pressurizer pressure decreased below its setpoint, but has not been closed, or vice versa.

When an equipment-related alarm, such as a lubrication alarm, is activated, the alarm is shown on the process overview mimic by changing the boundary color of the equipment to red, yellow or white. When the operator wishes to look at the specific alarms activated, he or she can click on the equipment icon after first acknowledging the alarmed condition. Then, the specific alarms are shown on a subsidiary window.

Alarm lists are provided on a dedicated screen in time sequence. The operator can choose only a certain priority of alarms that are of interest to him in a given situation, either single priority or multiple priorities. A soft alarm panel, namely, a computer-based panel of alarm tiles arranged in the similar way as in conventional alarm systems, is also provided to take advantage of the spatial dedication of alarm information. These alarms are arranged in systems, after some grouping and sorting of the conventional alarms.

3. ADIOS CONFIGURATION

Figure 3 shows the system configuration of the ADIOS prototype. I&C Functional Test Facility simulates the process of Kori unit 4 nuclear power plant, or the KAERI's ITF can send the simulation data of the process of Koran Standard Nuclear Plants to the Alarm processing Unit. Alarm Processing Unit is the host processor in ADIOS where the G2 real-time expert system shell runs and the alarms are processed. This host computer obtains process data of the plant from the FTF or ITF at a regular scan interval, and displays processed alarms on the process overview mimic and time-sequential lists on another dedicated CRT. Also, ADIOS presents the processed alarms as tiles on a small alarm panel, as in conventional alarm systems, to allow the operator's investigation of the alarms arranged in systems.

4. PRELIMINARY TEST AND DEMONSTRATION

Preliminary tests were conducted to refine the knowledge base and inference structure of ADIOS and to evaluate the appropriateness of alarm-processing algorithms in a dynamic environment as shown in figure 3.

The TMI-2 accident scenario, manual turbine trip, etc. were simulated to test the alarm processing methodology discussed above, and to demonstrate the feasibility of the alarm system. Figure 4 is a snapshot of the plant state when the pressure of the primary system has been lowered below the set-point of the PORV at the TMI-2 scenario. ADIOS shows the activated status alarm of the PORV by a red flashing of the valve body, because the PORV should have been closed, but is open.

5. EVALUATION OF HUMAN PERFORMANCE

5.1 Evaluation Environment

The cognitive performance of ADIOS to human-machine interactions was tested and evaluated using the ITF. ITF is an environment for human factor experiments. It has a PWR-type nuclear power plant simulator, main and support test rooms with VDU-based HMIs(Human-Machine Interfaces), an experiment control room, human factors measurements as well as built-in alarm systems. HMIs of ITF include flat-panel displays for safety function monitoring, VDTs(Video Display Terminals) for hierarchical plant mimic screens and trend graphs, a large scale overview display, and soft control devices (mouse, trackball, and touch-screen). The ITF alarm system consists of VDT-based alarm list, alarm tile windows, and hardwired annunciator panels. However, it does not include advanced alarm processing features such as alarm reduction or prioritization.

The most important features of ITF is to secure the flexibility and expandability of HMI design to change easily the environment of experiments to accomplish the experiment's objects.

5.2 An Evaluation of Human Performance

5.2.1 Evaluation Method

Two display monitors were added to ITF for evaluation of human performance of ADIOS. One VDT provided the alarm lists combined with the hardwired alarm panels of ITF. The other VDT displays alarms on plant mimic diagrams. To compare the two display methods, a human factor experiment was performed in the ITF for three event scenarios. During the experiment, physiological measurements, system and operator action log, and audio/video recordings were collected. Operators' subjective opinions were also collected after the experiment, because their feelings are another factor to evaluate an alarm system.

5.2.2 Experiment

- *Scenarios*

On the basis of event surveys and challenges to plant safety, three scenarios were selected for this study: a feed-water pump trip together with RCP sealing line leakage, a steam generator tube rupture, and a loss of feed-water together with main steam isolation valve fail-close. Time windows for each scenario were defined before the actual experiment.

- *Subjects*

Two operation crews (4 men) from a commercial NPP participated in this experiment. Performance differences between subjects were ignored because they work at the same plant and have enough operating experience. Before the actual experiment, they were trained on the ITF with and without the ADIOS prototype.

- ***Experiment Design***

The randomized block design was chosen so that the number of scenarios were considered as the number of repetitions. Pairwised T-tests were performed to determine statistical significance. Time, error rate, and situation awareness were chosen as major evaluation criteria for operator performance.

- ***Experimentation***

There were two breaks for situation awareness data acquisition in each scenario. Video/audio recordings, physiological data, alarm events and operator action logs were automatically collected during the experiment for each scenario. After the experiment, interviews with the operators were performed to obtain subjective opinions. In general, one scenario took 40-50 minutes to complete.

- ***Data Analysis***

The ITF includes the Data Analysis and Experiment Evaluation Supporting System (DAEXESS) which enables analysts to analyze experimental data quickly and easily. In particular, DAEXESS provides functions for qualitative analysis that requires many types of data, such as video recordings, system and operator events, and workload data[9] . DAEXESS was used in this study for statistical (quantitative) and observational (qualitative) analysis of experimental data. Time and error rate were calculated on the basis of predetermined time windows for each scenario. Operator workload was determined by physiological signal processing. Data from the post-experiment interviews were summarized to find human factors discrepancies and items to be improved.

- ***Analysis Results***

Statistical analysis of the time and error rate resulted in no statistical significance. Although workload analysis was not performed because data from one experimental run was contaminated, the other data showed insignificant differences. Regarding situation awareness, we performed two statistical comparison tests: ADIOS vs. ITF alarm system and RO vs. TO, but the results were not significant in both tests.

5.2.3 Evaluation Results

Although it has failed to find significant performance differences, important information on operators' preference to ADIOS and ITF alarm systems was identified through the interviews. Their opinions were confirmed by a video recording review. The lessons learned from the evaluations are :

- The color coding scheme of ADIOS is very useful to identify the cause of alarms. Priority-based and mode-dependent color coding was preferred by operators.

- Operators have difficulties in moving from an ADIOS display to ITF HMI screens. They recommended the integration of ITF HMI with ADIOS features.
- Operators tend to look at ADIOS overview displays to identify which systems have problems and then refer to the ADIOS alarm list display to determine which alarm is the key-alarm.
- During the initial phase of events, operators try to identify the key-alarm for the events.
- Operators refer to the trend graphs of plant parameters to confirm their decision on plant status after the key-alarm is identified.
- Operators don't pay attention to any alarms other than the key-alarm when their immediate response is not required.
- Operators refer to an alarm list display on the course of mitigating plant events.

It seems to be necessary to integrate the ADIOS alarm system with ITF HMI screens and trend graphs. Contrary to our expectation that operators refer frequently to overview displays, an alarm list plays an important role in identifying the key-alarm during plant disturbances.

6. CONCLUSION

This paper has described the overall techniques for processing alarm signals and evaluation of human cognitive performance for ADIOS. ADIOS is an object-oriented system developed in a G2 expert system software tool. 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, icon color, and so on. ADIOS was evaluated using ITF to verify its usability and performance for operators. Although no statistical significance was found in the result of the evaluation, several findings were identified through the analysis of subjective opinion.

ACKNOWLEDGEMENT

This paper was prepared as an account of work sponsored by the Ministry of Science and Technology of Korea.

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. I.S. Kim, et. al., "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. In-Koo Hwang, et. al., "An Object-Oriented implementation to improve Annunciation," *IAEA Specialists' Meeting (IWG-NPPCI) on Experience and Improvements in Advanced Alarm Annunciation Systems in Nuclear Power Plants*, September 17-20, 1996,Chalk River, Ontario, Canada.

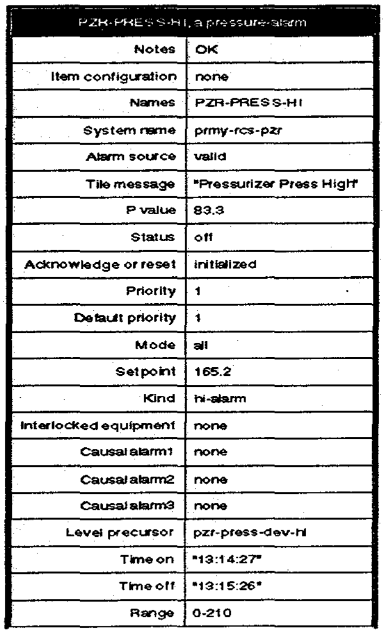
6 Kee-Choon Kwon, et.al., "The Real-Time Functional Test Facility for Advanced Instrumentation and Control in Nuclear Power Plants," *IEEE Transaction on Nuclear Science*, Vol. 46, No. 2, April 1999.

7 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.

8. Gensym Corporation, *G2 Reference Manual,* Version 4.0, Sep. 1995.

9. H.C. Lee, et. al., Development of Data Analysis and Experiment Evaluation Supporting System, *Journal of the Ergonomics Society of Korea, Vol. 16,* No.1, 1997

Table 1. Attribute Table of an Alarm Object



PZR-PRESS-HI, a pressure-alarm	
Notes	OK
Item configuration	none
Names	PZR-PRES S-HI
System name	prmy-rcs-pzr
Alarm source	valid
Tile message	"Pressurizer Press High"
P value	83.3
Status	off
Acknowledge or reset	initialized
Priority	1
Default priority	1
Mode	all
Setpoint	165.2
Kind	hi-alarm
Interlocked equipment	none
Causal alarm1	none
Causal alarm2	none
Causal alarm3	none
Level precursor	pzr-press-dev-hi
Time on	"13:14:27"
Time off	"13:15:26"
Range	0-210

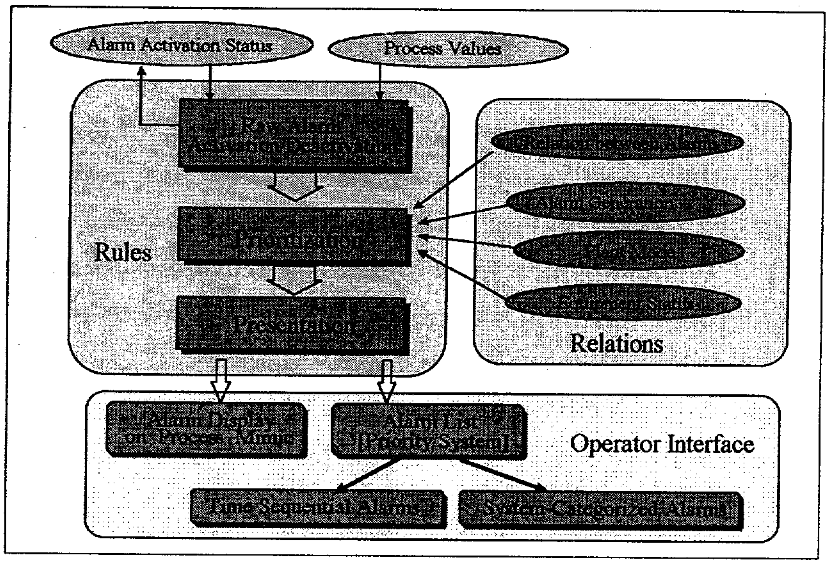


Figure 1. Alarm Processing Flow in ADIOS

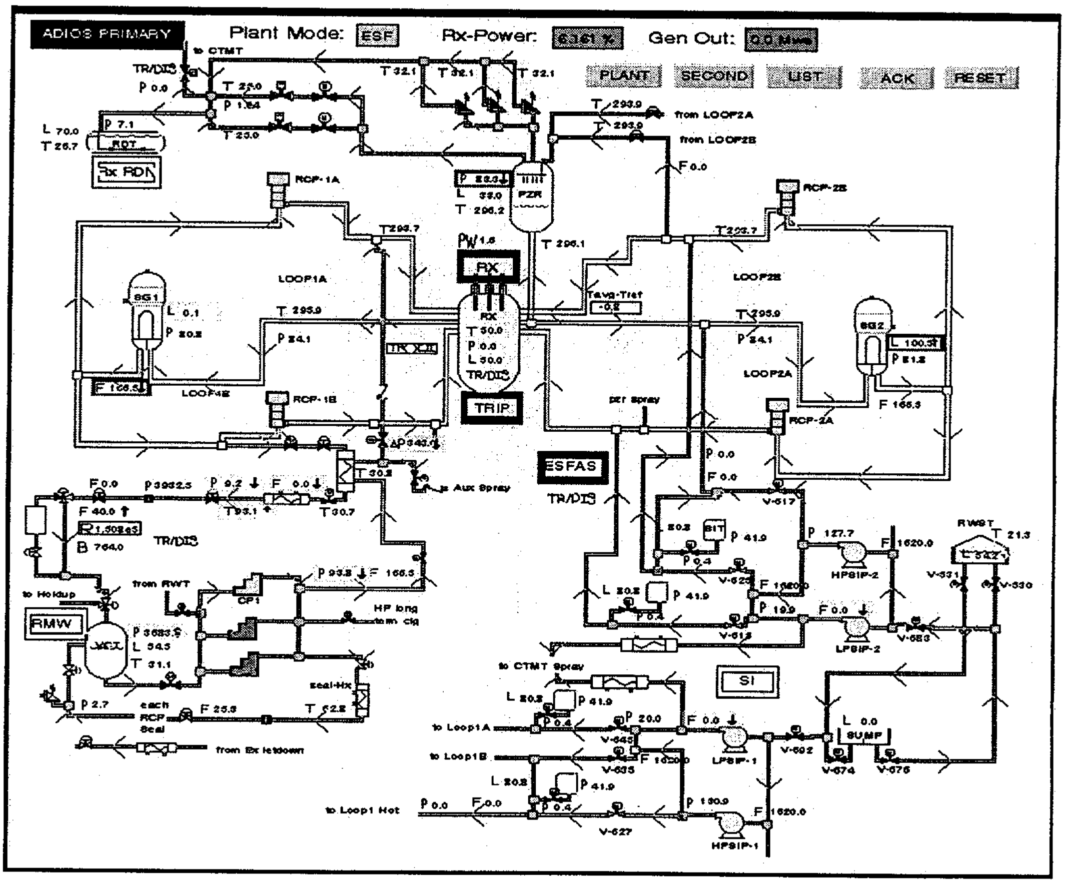


Figure 2. ADIOS Primary Overview Display

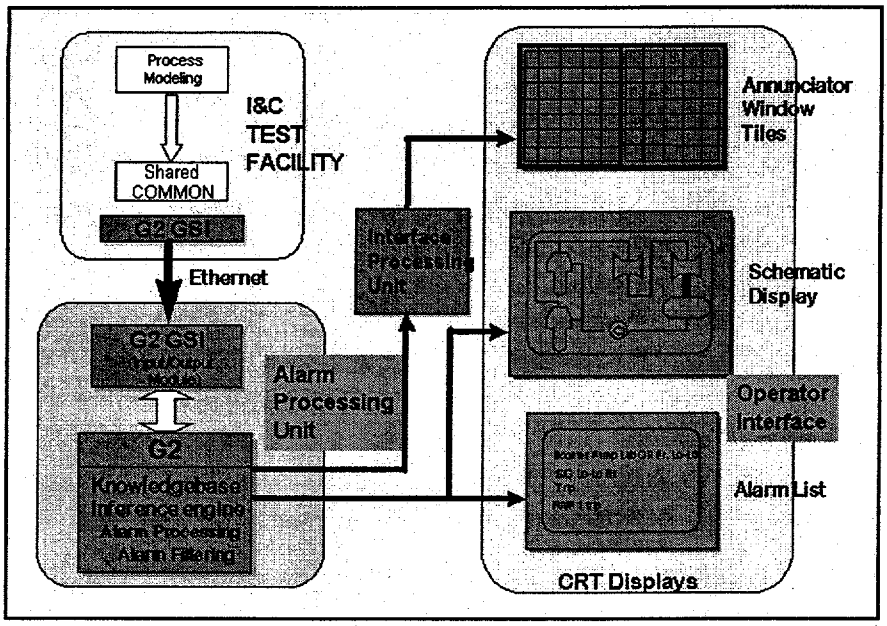
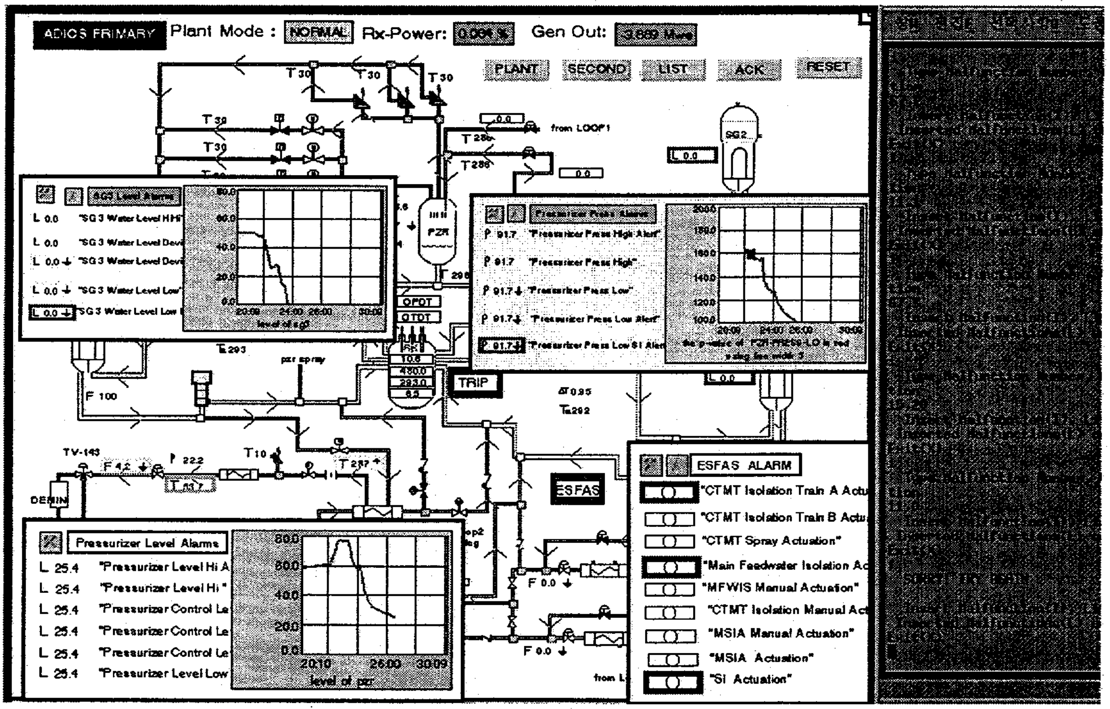


Figure 3. ADIOS Configuration



SG3 Level Alarms

L 0.0 "SG 3 Water Level HHi"
L 0.0 "SG 3 Water Level Devi
L 0.0 ↓ "SG 3 Water Level Devi
L 0.0 ↓ "SG 3 Water Level Low"
L 0.0 ↓ "SG 3 Water Level Low

Pressurizer Press Alarms

P 91.7 "Pressurizer Press High Alert"
P 91.7 "Pressurizer Press High"
P 91.7 ↓ "Pressurizer Press Low"
P 91.7 ↓ "Pressurizer Press Low Alert"
P 91.7 ↓ "Pressurizer Press Low SI Alert

Pressurizer Level Alarms

L 25.4 "Pressurizer Level Hi A
L 25.4 "Pressurizer Level Hi "
L 25.4 "Pressurizer Control Le
L 25.4 "Pressurizer Control Le
L 25.4 "Pressurizer Control Le
L 25.4 "Pressurizer Level Low

ESFAS ALARM

"CTMT Isolation Train A Actu
"CTMT Isolation Train B Actu
"CTMT Spray Actuation"
"Main Feedwater Isolation Ac
"MFWIS Manual Actuation"
"CTMT Isolation Manual Act
"MSIA Manual Actuation"
"MSIA Actuation"
"SI Actuation"

Figure 4. TMI-2 accident scenario display

SAFETY CRITICAL PROCESS VISUALIZATION FOR NPPs

Schildt, G.H

Senior Member of IEEE

Vienna University of Technology,
Institute of Computer-Aided Automation
A-1040 Vienna, Treitlstr. 1/183
e-mail: schi@auto.tuwien.ac.at

Keywords. *Safety critical process visualization, safe microprocessor system (SIMIS), fail-safe comparator, safety chain, dynamization principle, demonstration of double-channelled process visualization*

Abstract. *After an introduction to safety terms and to fundamental principle of an (2-of-2)-control system with fail-safe comparator a new concept is applied to safety critical process visualization for NPPs. The process visualization concept is based on a double-channelled image processing system. As a first approach we developed a double-channelled computerized visualization system consisting of two commercial microprocessors. But, because there is a certain double failure probability within each microprocessor (which may not be negligible), it would be useful to implement at least one visualization channel with a fail-safe operating microprocessor like SIMIS.. A periodic information switch presents alternately processed status information from one and the other information processing system. If there is any discrepancy between both image processing systems the corresponding process symbols are blinking on CRT. The necessary task to compare both results in a safe manner is assigned to the operator. Whenever any process symbol blinks the operator is forbidden to input safety critical commands. In order to check that the switch is changing its position periodically, the operator has to convince himself that the corresponding symbol related to the switch changes its position on the CRT periodically. Furthermore, for safety critical process visualization a coloured display is needed based on four fundamental colours (like red, green, blue and yellow). In order to make sure the operator that all necessary colours can be displayed on CRT correctly, a colour bar changes its dimension on the screen periodically, but with another frequency like the information switch. The presentation will be completed with a presentation of the functionality of the double-channelled process visualization for NPPs.*

1. INTRODUCTION

Before as a new approach a double-channelled process visualization is presented some fundamental terms in the field of safety technique have to be defined as follows:

- *safety critical system:* control system causing no hazard to people or material in case of environmental interference or system failure.
- *Safety:* property of an item to cause no hazard under given conditions during a given time; i.e. avoidance of undue fail conditions. Undue fail conditions may be caused by

technical system failures and malfunctions of an electronic device (e.g. interfered by electromagnetic noise).

- *Hazard:* condition of a system that cannot be controlled by given means and may lead to injuries to persons.
- *Safe system state:* property of a system state to cause no hazard to people or material. The safe system state can be reached by an orderly shutdown of NPP.
- *Fail-safe*: Technical failures within an item may lead to fail states of a safety critical system *(fail)*, which however have to be safe *(safe)*.

Because, up to now no fail-safe (one-channelled) computer is available, one has to apply a configuration of at least two commercial computers running parallely. Figure 1 shows a double-channelled control system, where both computers are fed with same input values from technical process. Normally, the results of both computer channels are fed to a fail-safe comparator, whose output enables a safe gate in case of equivalent results, represented by corresponding command telegrams /SCHI80/.

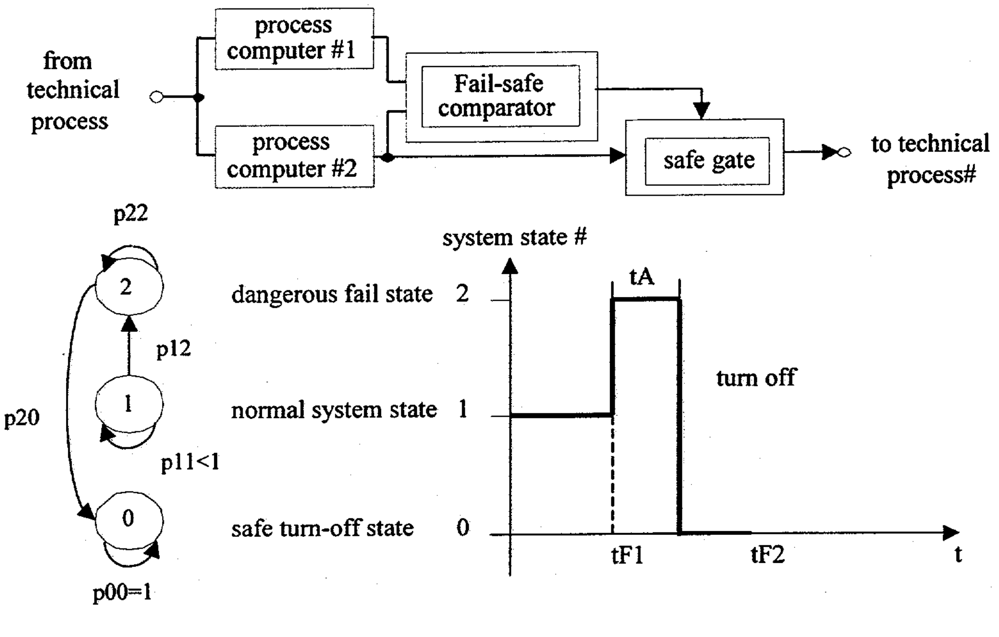


Figure 1: (2-of-2)-control system with fail-safe comparator

It is the full responsibility of the comparator to change over the system into a safe system state. The fail-safe comparator has to detect any inequality of generated results within a well-defined tolerance zone.

2. PROCESS VISUALIZATION

For visualization purposes computers may be used to support human decision makers. Computers have already been applied for visualization purpose in the field of aviation. One of the main advantages is a possible reduction of information presented to the pilot. There is a clear trend to introduce a computer-aided process visualization for I&C in NPPs. For safety related process visualization therefore the following concept is presented (figure 2):

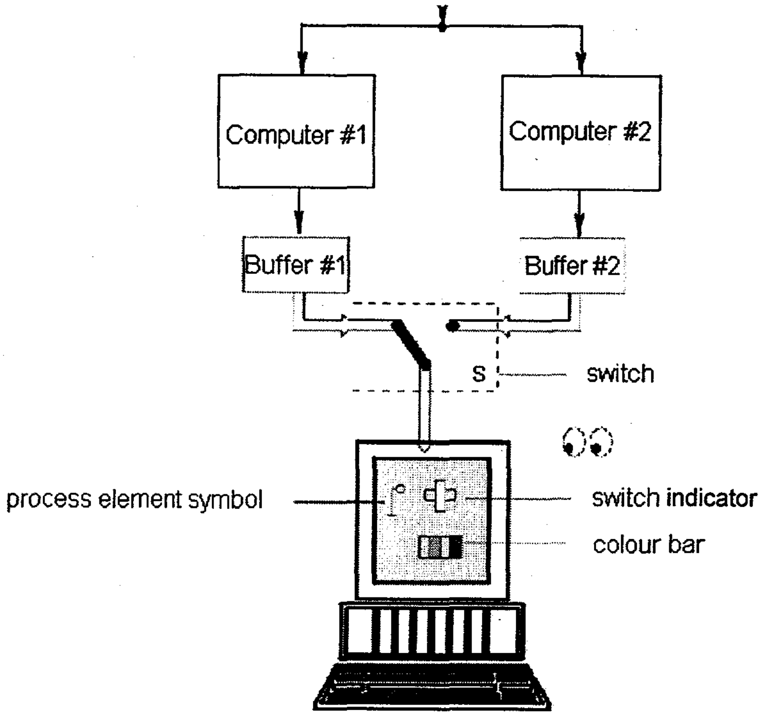


Figure 2: Process Visualization Concept

Measured values from different sensors, which are to be visualized are fed to two independent image processing systems, simultaneously. The output of each image processing system is a certain visualization of the technical process that represents the status of the reactor. Applying an electronic switch, which toggles in a certain succession (e.g. once a second) the process images are combined to a chopped picture, which is displayed on CRT.

If the contents of these two process images are identical, the operator will see a stable process visualization image. Otherwise, some process symbols will blink. Safety critical commands may be issued by the operator only, if no process symbol blinks. In order to guarantee that the periodical switch is indeed toggling an additional and corresponding process symbol is used. If the image currently displayed is derived from one processing unit, a vertical bar is displayed; if it is derived from the other a horizontal one is used.

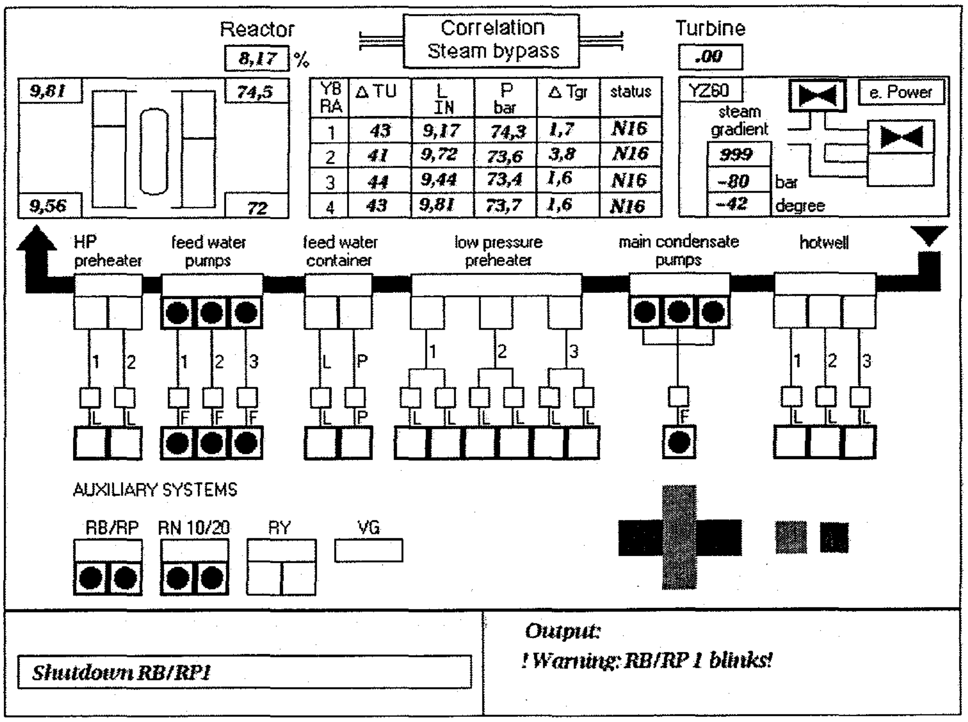
It could be possible that there is certain remaining probability that both image processing systems are failing. In this case one should apply a diverse system structure e.g. applying two different computers (like AMD ™ or INTEL ™). According to a double failure event within one processor system one should apply a double-channelled like SIMIS. There is a fail-safe computer system available to be implemented in the visualization system.

Usually, colours are used to convey status information in process visualization. If colours are used to indicate critical states or events, precautions are to be installed to ensure proper operation of colour display. Let us assume that a colour failure may have occurred for example that red colour cannon in a CRT has failed. In this case an alarming state of a process element cannot be displayed due to missing colour. An appropriate counter measure to this risk would be displaying a combined colour bar containing all relevant colours and changing its size of the bar, periodically. If possible the frequency of these changes should be different from the frequency of switch toggles, because of avoiding any common mode effect. In order to inform the operator that both image processing systems are still alive, two blinking symbols are displayed on CRT.

Altogether, an operator is allowed to perform safety critical operations only if the following conditions are hold:

1. None of the process symbols blinks.
2. The switch indicator changes its position, periodically.
3. The combined colour bar changes its size, periodically, but with another frequency than the switch indicator
4. The operator has to convince himself that both visualization channels are still alive due to two blinking separate symbols.

Additionally, safety critical commands are protocolled automatically on a *control and failure printer*, additionally without any chance for data manipulation. Figure 3 illustrates such a process visualization for NPP /ADR92/. It shows the usual display elements, the switch indicator, the combined colour bar, and the symbols for active image processing systems.



YB RA	ΔTU	L IN	P bar	ΔTgr	status
1	*43*	*9,17*	*74,3*	*1,7*	*N16*
2	*41*	*9,72*	*73,6*	*3,8*	*N16*
3	*44*	*9,44*	*73,4*	*1,6*	*N16*
4	*43*	*9,81*	*73,7*	*1,6*	*N16*

Shutdown RB/RP1

Output:
! Warning: RB/RP 1 blinks!

Figure 3: Process Visualization of NPP

3. CONCLUSIONS

After an introduction to safety terms a new double-channelled image processing system for NPP visualization was presented. The essential feature is that the necessary fail-safe comparator has been transferred to the operator in front of CRT. Another important feature of the presented concept is the application of dynamization principle in the field of safety critical operation. Thus, an operator may rely on coloured display on CRT and gets helpful assistance in decision making process.

Acknowledgement. The author wishes to thank Dr. Böck (Atominstitut der Technischen Universität Wien, Austria) and Mr. Felkel (Company Istec, Germany) for helpful discussions.

REFERENCES

/SCHI80/ Schildt, G.H.: *Grundlagen für Vergleicher mit Sicherheitsverantwortung*, Siemens Forschungs- und Entwicklungsberichte, 1980

/ADR92/ Adrian, H., Bücherl, A., Felkel, L., et al.: *Nutzung der Möglichkeiten von rechnergestützten Entscheidungshilfen zur sicherheitsgerichteten Unterstützung der Operateure in Kernkraftwerken*, Gesellschaft für Anlagen- und Reaktorsicherheit mbH (GRS), Garching (Germany), 1992

/SCHI93/ Schildt, G.H.: *A Double-Channelled Safety Critical Process Visualization*, IAEA Specialists Meeting on "Operator Support Systems in Nuclear Power Plants, Moscow", Russian Federation, May 17-21, 1993

IAEA Specialists' Meeting on
HMI for Off-normal and Emergency Situations in NPP,
26-28, Oct. 1999 Taejon, Rep. Of Korea

A Display System for Remote Users Using the Relational Data Model

Soon-Ja Song, Chul-Hwan Jung, Dong-Young Lee, Won-Man Park,
Kyung-Ho Cha, Jae-Chang Park, Kee-Choon Kwon
Korea Atomic Energy Research Institute
P.O.Box 105, Yusong, Taejon 305-353, Republic of Korea
(e-mail : songs@nanum.kaeri.re.kr)

ABSTRACT

The display system is one of the relevant Human-System Interfaces (HSI) such as alarms, controls, job performance aids, workstation and workplace layouts[1]. In nuclear power plants, display systems are used in operating and monitoring dynamic behaviors from the process and all instruments. Their use allows operators and other users to quickly interpret the state and performance of the machine and experiment. However, most current simulators and plants have supported their information in a fixed place. New technologies for communication and software afford data to remote users who are technical staffs and researchers studying abnormal status in distance. For various remote clients, data handling should be changed with a relational data model representing entity-relationship instead of a file system. In the developed display system of the compact nuclear simulator (CNS), and the instrumentation and control functional test facility (ICFTF), relational databases were designed for remote users, maintenance, upgrading and new display system. In this approach, the display system can increase the reliability but reduce retrieval time in sharing data between local and remote clients. In conclusion, since it is not limited by places, time and server types, all users approved by an authority can operate, monitor and use simulator plant data remotely or use the simulator at their desks.

I. Introduction

The display design on human performance and reliability are the most important objectives in the Nuclear Power Plants (NPP). In conventional control rooms, the large spatially fixed arrangement of controls, displays, and alarms support a rapid scanning and pattern-recognition approach to plant diagnosis. Information is primarily presented by detailed parameter indicators on a variety of analog devices or by reprocessing data for diagnosis. The computer based display systems represent information with text, image, audio, animation and etc.

In nuclear power plants, the display systems are used in operating and monitoring dynamic behaviors. Their use allows operators to quickly interpret the status of the plant process and performance of the machine and experiments via data acquisition and the monitoring system. In the case of simulators, the basic backgrounds for display systems are similar to real power plants. There are three kinds of simulators: full scope simulator, compact simulator and engineering simulator. A simulator is a task oriented display system, having CRT in an old simulator, LPDS for next generation, trends, axial curves computerized procedures, and other computerized operator support system.

KAERI has the CNS for trainees and research for BWR NPP in abnormal and steady states. It calculates small break LOCA in two-phase status, called SMABRE (SMAll BREak) code. In addition, KAERI has ICFTF that is to validate newly developed digital algorithms, alarm reduction algorithms, and the performance of operator support systems, etc. Both have been used for new operating support techniques such as abnormal transient diagnosis.

To develop new graphic display systems, the hardware and software environment of the CNS were completely replaced with new ones. During this progress, the plant code by FORTRAN was transferred into a HP workstation, but the graphic data did not move. For this reason, all graphic data should be recreated in another language. If graphic ASCII data were remained, the new display system would be upgraded and replaced faster than recreating.

The new Graphic System adopted C-like language (Picasso-3) and X-lib for developing graphic modules. As a developed graphic system is used, the upgraded CNS and the ICFTF can afford operator display systems and in addition, mimic having the similar information compared to large-display-screen in next generation control room.

The previous simulator had been supported in the fixed place. However, a new simulator can support the exchange of data between servers to execute all software and panels to display and control data through the local network and wide network. Therefore, it can support not only the same functions as the previous CNS but soft controls and connections to CNS from anyplace through networks. Both the changed environments of the database and communication afford to share information between all users regardless of limitations.

II. Upgraded CNS and ICFTF

The upgraded CNS is to train operators and to support researchers as a plant test-bed. ICFTF is to ensure the verification and validation of the function and performance of digital systems before installation NPPs.

1. Upgraded CNS

The CNS is a model that predicts the dynamic behavior of the nuclear power plants and includes models of their control systems. It consists of the plant process code, the plant controls, panels, display system. The panels are regarded as a compact control room. The user controls the simulated process by means of controllers and observes the response on instruments, digital displays, alarm annunciators located on the top of the control desk. The operator's panel is connected to the simulator through the HP workstation. The interface between the plant computer and the operator's panel in the console desk consists of custom fabrication by PLC. The graphic display system developed mimics and all sorts of trends to emulate KORI-3, 4 units.

2. ICFTF

The objective of the instrumentation and control functional test facility (ICFTF) is to validate newly developed digital control and protection algorithms, alarm reduction, and the performance of operator support systems, etc. The ICFTF software consists of mathematical modeling that simulates a three-loop pressurizer water reactor, 993Mwe Westinghouse plant. The supervisory program comprises all the instructions necessary to run the test simulator. The hardware equipment provides interface between host computer and simple test panel or developed target systems to be tested. The interface module can provide Ethernet or VXI interface to a developed prototype using shared memory and also provides the display page for the value of simulated variables. The graphic display system supports an easy and friendly user interface between ICFTF and users. The ICFTF is applied to advanced instrumentation and control prototype to test its performance and show good operational performance in normal and transient conditions. [2]

3. Plant Process and Control Module

The thermohydraulic model is based on separated field equations for the mass of two-phase fluid components, liquid and vapor, on separated liquid and vapor energy equations and on integrated field equations for mixture momentum. The mathematical modeling is based on the lumped parameter approach, allowing flexible control volume configurations. The heat conduction model is based on the volume-averaged temperature over the structure. The maximum time step of the transient calculation is defined by the Courant limit for fluid velocity, corresponding limit for heat flow and the depressurization rate of primary and secondary systems.

□ Components module

- heat transfer and critical heat flux correlation between structural parts and fluid.
- critical break flow correlation based on the Moody model
- simplified neutron kinetics model (point kinetics) for power decrease during reactor shutdown and a decay heat model.
- model for pressurizer heaters and relief valves.
- accumulator model
- pump model based on the two quadrant homologous curves, (for two-phase conditions, a two-phase multiplier is used)
- emergency coolant and make up pump description based on pump characteristics.
- steam generator secondary side is described separately.
- relief, safety and turbine bypass valves in the secondary side.

III. Display System Design

The Human-System Interface (HSI) includes all displays, alarms, controls, job performance aids, workstation and workplace layouts, as well as environmental conditions such as lighting, noise, temperature, and humidity. The HSI components through plant involve the main CR, remote shutdown station and those HSI components associated with the technical support center (TSC) and emergency operations facility (EOF). Users are defined as operators, shift supervisors, plant engineers, managers, administrative staff members, maintenance crew members, physicists, and thermohydraulics exerts, etc. Generally, a local and a remote user are classified by distance. Users connected to network, however, can not anymore distinguish in local and remote users. All users are not only local and but remote users logically in modern times. In the NPPs, various users acquire plant data to control, monitor and diagnosis through control and monitoring systems. For human-system interface, users need all sorts of display systems to represent information.

After TMI-2, developers in human-system interface, consider on reducing human errors and increasing human performance. On the other hand, other developers focus on analyzing data after emergency. Both users get information and data through control and monitoring system from the same plant database in their own ways. For example, during accidents, operators, technical staffs, and administrative staffs need urgent information from the plant almost at the same time. However, these three groups of users do not need the same information and the same form. They need text and graphic knowledge information for their purpose on their task. The existing plants can not support them flexibly and at the same time due to data processing constraint consisted of file system.

To design display system for sharing between remote users, it is needed to keep consistency, standardization, and acceptability by matching the HSI characteristics. The upgraded compact nuclear simulator adopted Picasso-3 graphical tool based on C-like language from HRP. This tool can provide interactive design, interactive testing and reusability of components to develop the display system easier than that of Xlib and Motif.

In this experience, the graphic software procedures for users have hardly changed, even though the graphic hardware environment has totally changed from that of the previous one. Most graphic application programs (tools) contribute to translate their graphic primitives into ASCII format for interfacing between other graphic tools. In the case of the CNS, all primitives in Micro VAX-II were thrown away because nobody could handle the graphic data.

The graphic data should be stored into databases with relationship for preparing current or near future environment. Otherwise, when the display system is changed, it would be costly and time consuming to rebuild and upgrade as if a new display system was developed. Graphic Primitives consist of line, circle, class and image, etc. Primitives can be handled with text data format to migrate to other computers or new systems. In the CNS and the ICFTF, graphic primitives are designed in reference to NUREG-0700 using minimum colors and appropriate HIS characteristics [3]. Those primitives stored graphical database as a type of libraries. To use the display system by both local server and remote clients, it needs user interface management through the local network and the wide network. Thereafter, a display environment of remote users should be set up very similar to the local display system using relational data model by database administrator.

1. Graphical Primitive Design

The CNS display system was developed with graphic data such as mimic, trends, and P&IDs. All pages and symbols were generated by the graphic editor(GED) in Picasso-3 language. In addition, the GED supports to program procedures for dialog between class tables. There is a certain database only for the graphic systems to support. With this database, application modules are independent to the plant process code.

Pages used on the display system are designed with text, trends, and component symbols. They are arranged to adjust in a screen size of a monitor with characteristics of human-system interface such as size, colors, and shapes. Their primitives are simple point, line, and circle. All graphic data are consisted with these primitives and extended primitives with color, pattern, and inheritance. In English charactery, primitives are a, b, and z letter. When using these primitives, we can make a sentence and integrate sentences into paragraph for documents. This process was extended to use graphic data in dealing with text data. General graphic application program consists of three parts: graphic primitives for drawing pages and symbols, dialog procedure for communicating among classes or symbols, and program procedures for executing all resources into process. Therefore, when the display system is developed, these three parts should be concern of maintenance, extension, and reusability.

In KAERI simulators, the graphic data can be divided into two databases, the graphic database and the text database having graphic attribute. Moreover, graphic application programs (procedure) in Picasso-3 are translated into text file to reuse procedures for developing another display system on different computer.

In Table 1, valve graphic primitives are shown for introducing a possibility of translation from graphic primitives to text data. These valve classes also show to be made with object-oriented methods.

Table 1. Graphic Primitive and Class

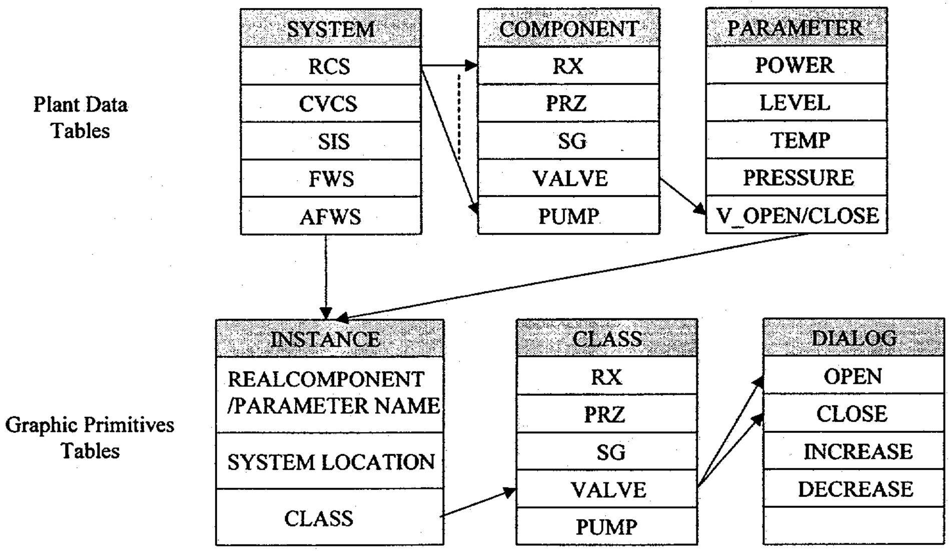
Class of Valve	Dialog of Valve	Instance of Valve
class Valve-1	Function `//pTALK	Instance CNS_Picasso_Lib.Valve-1.
int *state = 0;	Int isOpen()	BFV4782_V
Polygon	If(state != 0)	attribute state = `&BFV4782`;
NumberOfPoints = 4;	return *state==1;	x = 794;
Visibility = 1;	else	y = 431;
Colour = 31;	return 0;	visibility = 1;
Width = 2;		xReference = 794;
Pattern = `1`;	function `int ValveColour()	yReference = 431;
ScaleFactor = 1;	if(isOpen())	xScaleFactor = 0.424098;
Angle = 0;	return green;	yScaleFactor = 0.424098;
// end of class valve	else	rotationAngle = 0;
	return red;'	// end of instance BFV4782_V

2. Database Design[4]

Most current simulators, engineering codes and existing plant in NPPs do not use a relational database to handle their data. They use file systems that are binary files to speed up data processing time or ASCII files to store for reports. Old simulator codes programmed by FORTRAN were made some decades ago, so that its data processing systems are aged with data server.

In this situation, users related to NPPs hardly can access database for their purpose including display systems through servers and networks unless database administrator or experts for data processing help them. As mentioned, display systems affect users to increase the human performance of recognizing and analyzing all modes and status in NPPs. Therefore, database structure should be changed under current environment in existing plants. To avoid from reconstructing the plant database, relational data model was suggested to model the plant database with graphic data tables and text data tables (plant database). These tables describe entity-relationship in Table 2. Plant data tables are consisted of system table, component table, and parameter table. Graphic primitive tables divide into three parts: instance, class, and dialog. Unlike text tables, graphic primitives can be consisted with both graphic primitive tables and text graphic primitive tables. This concept will be contributed to all users using plant data.

Table 2. The Relationship between Plant Data and Graphic Data Tables



3. Remote User's Display System Design

Safety and reliability are the most important objectives in Nuclear Power Plants. During abnormal or emergency states, if operators and staffs watch the same information at their desks, they can recognize and analysis the situation faster than when they do not share such an information. There are many users related to NPP but they can not reach each other by limiting regulator rules, and blocking a lack of networks, and limiting software environments for display systems. Therefore, remote clients need a display system to increase reliability and availability of data when they want to watch at that point. Table 3, 4 are an example of the grouped data for different users. During operation, all the plant parameters are generated by the process and control system and its data is translated into display systems by the data acquisition system and monitoring system for operating, diagnosing or analyzing after abnormal activities. Both tables show the different data for users and display systems. For the graphic system, these variables are extracted from all file databases using relational data language.

To share data between local and remote places and the same and different graphic environment, first, user schema and external schema should be developed for users. Thereafter, both users can design their display system with RDM, supported by database management system (DBMS). To execute their tasks on the display systems, they should design application program interface (API) and user interface management (UIM)[5,6].

Table 3. Grouped User for Different Status

Modes	In operation	After accidents and Emergency
Users	Operators Shift Supervisors	Operators Technical Staffs Administrative Staff Members SA Researchers The Public

Table 4. Grouped Graphic Data

Class	Status	Instance
Valve-1	Action Events	Relation, Location
Valve-2	Action Event	Relation, Location
Reactor	Animation	Relation, Location

4. User Interface Management Design

User interface management should support to communicate between server and clients. When DBMS handles NPP data, it meets a few users and not much quantity of data compared with the bank's transaction. NPP data mainly come from data acquisition as well other monitoring or transaction system, but the number and size of its data are almost fixed. Therefore, data processing can be handled easily.

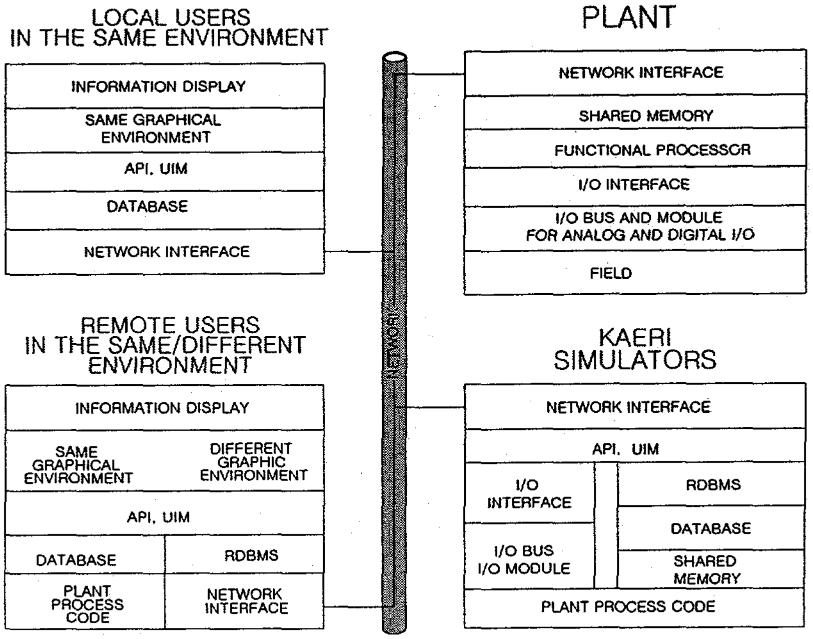


Figure 1. User Interface Management (UIM) between Users and Databases

Technologies of running external programs on the server side of a RDBMS support the database developer to program in a third-generation language (3GL) such as C, C++, or Visual Basic. There are two types of external programs: a user defined function (UDF), and a stored procedure. UDF can extend the functionality of the database by allowing users to define the structured query language (SQL-ISO/ANSI)) functions. As an example, the following SQL shows that 'plantdata' opens and select status from 'plantdata'.

SELECT status FROM plantdata WHERE user = 'technicalstaff'
SQL statement : SELECT column-list FROM table list
[WHERE], [ORDER BY], [GROUP BY], [HAVING], [UNION]

A stored procedure allows the database developer to break a database application program into a client part and a server part. The result of the execution by the stored procedure can be passed back to the client part, which is usually running on a different machine. When commercial RDBMS is used, the open database connection (ODBC) and application program interface (API) must be supported to connect among user application programs.

The following drawing shows a semantic flow among plant processes and remote users through API and network using a database.

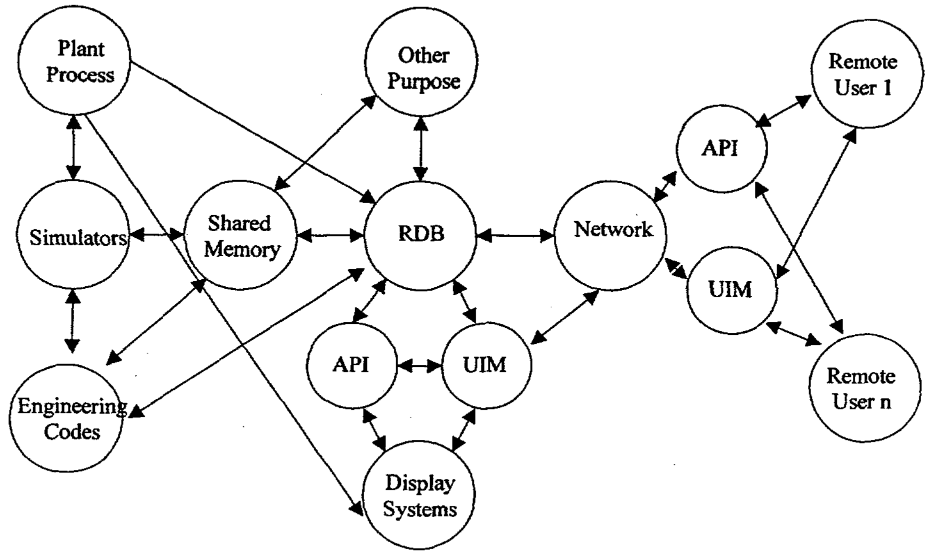


Figure 2. Semantic Network of the User Interface Management

IV. Conclusions

Until now, various researches on NPP are performed such as simulators, plant upgrade, maintenance, and computerized operator support systems. As display systems, they increase the human and plant performance in all operation modes. In the case of an abnormal status, the plant data should be distributed for operators, technical and authorized staffs. However, they are not in the same place, at the same time during an off-normal or emergency status.

While developing many task-oriented application programs such as alarm reduction, computerized procedures, and early fault detection, etc., the display system is attached to them. After developing a prototype, they are often not usable because the graphic hardware system and software tools do not run on the different environments. If the plant data and graphic data are dealt with relational database techniques, all users can get data easily from RDBMS under any environments. When the hardware and software environment changes later, because both life cycles are very short, RDBM supports for user interface management that can transfer the old system data to the new system data with minimum effort.

In the next approach, a design and an implementation of Web Pages (WEB) for intranet/extranet use in simulators will be performed, based on Hyper Text Markup Language (HTML), Extensible Markup Language (XML)[7]. It can provide modularity, portability, and usability to all users and for various purposes, such as operators, staffs, and for upgrading the display system environment.

ACKNOWLEDGEMENT

This work has been carried out under the nuclear research and development program in the Ministry of Science and Technology of Korea.

REFERENCES

[1] Human-System Interface Design Review Guideline NUREG-0700 Rev.1 Vol.1, 1996.

[2] Kee-choon Kwon, et.al. "The Real -Time Functional Test Facility for Advanced Instrumentation and Control in Nuclear Power Plants," IEEE Transaction on Nuclear Science, Vol. 46, No. 2, April 1999.

[3] Graphic Display Development Methodology, EPRI NP-4874, 1986.

[4] C.J Date "Database Systems" Vol. 1, Addison Wesley

[5] IEEE Guide for the Application of Human Factors Engineering in the Design of Computer-based Monitoring and Control Displays for Nuclear Power Generating Stations, IEEE Std 1289-1998, 1998.

[6] Distributed Digital Control and Monitoring for Power Plants, IEEE Std. 1046-1991, 1991.

[7] IEEE Recommended Practice for Internet Practices-Web Page Engineering-Intranet/Extrenet Applications, IEEE Std. 2001-1999, 1999.

INFORMATION AND DIAGNOSTIC SYSTEMS

Christian Hessler, Siemens AG KWU, Germany

ABSTRACT

This paper gives a brief overview of the basic concepts for process information and control implemented in SIEMENS KWU I&C systems for nuclear power plants. This concept emphasises at a first place an adequate level of automation, providing the operating staff with adequate time span allowing to comfortably assess and evaluate the situation before actions have to be taken. Where, in case of faults, corrective actions have to be taken, the operators are informed about the actual plant state based on information formats organised in a systematic manner and simplifying orientation and navigation. Where selection of the appropriate response is not evident, appropriate diagnostic information is included based on ergonomic principles, the main features being: implementation of a diagnostic system for I&C faults, operator guidance by using computer-based alarm sheets, and computerised support for the event identification for the event-oriented emergency procedures. Awareness of the overall plant state is assured by permanent critical safety function monitoring, implemented by using a set of dedicated safety function oriented operating formats.

Further development is currently under study, the most prominent features being automatic safety function monitoring complementing the role of the safety function formats, and advanced event diagnosis, based on Bayesian networks.

1 SHARING WORKLOAD BETWEEN THE OPERATOR AND THE I&C

Design of control rooms is intrinsically linked to the « Human factor » - the consideration of the impact of the « man-ware » in design, operation and maintenance of the plant. Even a completely automatically operated and maintained plant would know the human factor: maybe it will then no longer affect directly the plant, but indirectly: there would be no longer an « operator behaviour » to be analysed - it would have to be replaced by an analysis of the work results of the designer. However, the human factor itself would remain, now relegated completely to the design phase. However, this is not the trend: the operators will continue to play an essential operation in plant operation:

The operating staff will be always a valuable resource, playing an important role in plant operation, testing and maintenance:

- by completing the functions of the technical components and
- by covering their imprecision and lack of perfection, based on the human flexibility and adaptability to not precisely foreseen situations.

This important, active role in the function of the whole man-machine system « nuclear power plant » which can, on an economical basis, not be substituted by complete automation.

Of course, the human intervention has also to be seen as a factor of disturbance and of limited reliability the effects of which have to be taken into account in the design of all plant systems and functions, to assure a sufficient level of safety and availability of the plant. We could try to push these two roles more and more to the design phase - but then, as we have seen, we would replace the fallible operator by the fallible designer....

Consequently, the human factor has to be taken into account systematically in the design of a nuclear power plant. In fact, it is not only considered in the design of the man-machine interface in the proper sense (layout of the control room, of the operating means etc.) but **wherever** the tasks and the work environment of the operating staff are concerned. This requires especially that

(1) functions assigned to the operating staff, constitute consistent tasks and correspond to the abilities and strengths of the operating staff: appropriate degree of automation, appropriate number of tasks, appropriate sharing out among centralised and local operating actions,

(2) the man-machine interface strictly speaking (control room, screen-based and conventional control means, processing of information to be presented to the operators) optimally supports the tasks of the operators and minimises human error.

In order to avoid the basic modes and causes of human error:

A) objectively missing information

B) missing utilisation of objectively available information

C) erroneous utilisation of objectively available information,

the following design requirements have to be respected (the list is not exhaustive!):

- provide the **required information** (for A): this has to be assured by the consistent analysis and design of the requirements for plant control and monitoring in all plant situations
- make **easily** available and **apparent** the information which is necessary for a task (for B): this has to be assured by adequate ergonomic design of the information presentation on the MMI
- provide sufficient **grace time** for the perception of information and the elaboration of action plans (for B)
- impose a **well structured approach** for problem solution (for C): this has to be assured by providing operating procedures, or by providing means to evaluate action plans before execution
- facilitate the **evaluation of the effects** of any action, by providing information about the consequences and effects (for C)
- allow to **undo important actions** if they do not lead to the intended effects (for C)
- provide an **appropriate team organisation**, allowing the team members to discuss and check plans before implementing them (for C).

Making available appropriate grace time is a requirement on the design of the plant fluid systems, to be completed by appropriate automation.

Automation is intrinsically linked to the staffing concept, and to the mode of operation of the plant: both are fixed by the needs of the utility, and by the utilities policy for the composition of the operating team.

A direct link between staffing concept and degree of automation is given for tasks which are planned in advance, and where execution and progress may be paced by the operators: start-up of systems, alignment of circuits, filling of storage tanks...., tasks performed in the context of start-up, shutdown and maintenance of the plant. In this context, a low level of automation can be compensated for by a larger number of operators, provided that sufficient working places are foreseen for them.

Things are different when reactions to failures or rapid process variations in the context of transients have to be handled: here the reaction is paced by the needs of the process: only a limited time budget for reaction is available. For this situation, automation is a matter of required reliability of the reaction, and available reaction time. Balancing degree of automation and number of operators is only possible to a very small degree.

These considerations, roughly summarised on figure 1, lead to the following set of automation criteria, to be applied to the process control tasks. Whatever is the status of the plant, the following actions have to be automated:

- tasks requiring a **quick or highly reliable reaction** for safety reasons
- tasks requiring **quick reactions** to maintain **plant availability**
- **monotonous and repetitive functions**, leading typically to high **workload** (if not automated), as e.g. continuous control of state variables of the process

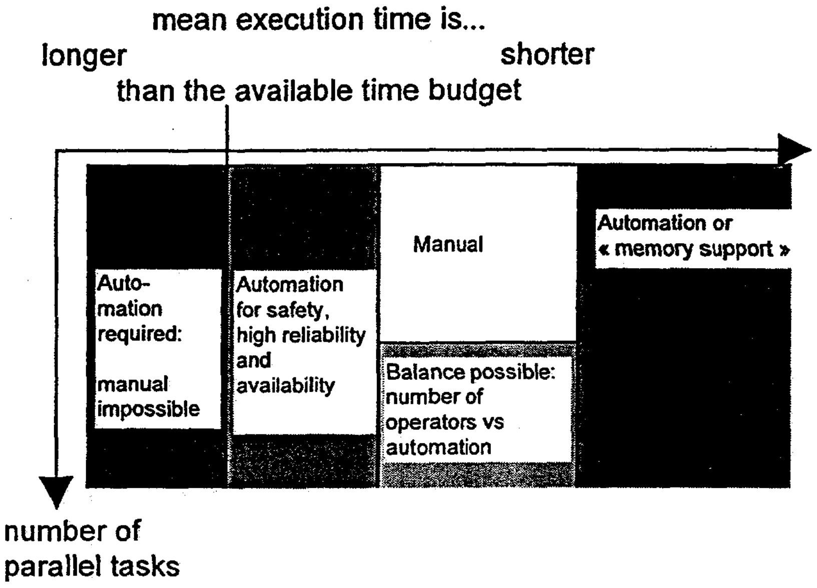

mean execution time is...
longer
shorter
than the available time budget
Auto-mation required:
manual impossible
Automation for safety, high reliability and availability
Manual
Balance possible: number of operators vs automation
Automation or « memory support »
number of parallel tasks

Figure 1: Summary of considerations for degree of automation and its relation to staffing

2 INFORMATION NEEDS AND SCREEN-BASED INFORMATION PRESENTATION

Of course, workload and human reliability is not only a matter of time available: the second essential factor are the information needs and the guidance of the staff, when facing simultaneous tasks.

2.1 BASIC INFORMATION NEEDS: OBJECTS OF VISUALISATION

From a theoretical point of view, four principal types of objects have to be presented to the operators allowing to understand and analyse the plant state, and to identify the adequate manual actions:

1) the equipment of the plant: fluid, mechanical, electrical and I&C systems and components (as far as the operators can act on them or information is necessary about),

2) the dynamics of the processes and the functional relationships between main process and sub-processes,

3) the functions of the automation (control loops, automatic sequences, protections..) and their relation with the state of the process,

4) the guidance for operation :

   - guidance for corrective actions in case of isolated disturbances and failures (response to alarms)
   - procedures guiding the operator during intentional changes of the state of the plant (normal operating procedures),
   - guidance for incidents and post-accident measures.

The information about the first three types of objects is communicated to the operating staff by state and status information and by alarms, independently from the technology of the man-machine interface systems:

- check back information of components (open, closed, on, off...)
- state information about systems (in operation / out of operation)
- check back of automatic actuation (actuation of a limitation, of a trip, of a component protection...)
- analogue information and associated limit values
- alarms indicating disturbances and failures of functions or systems.

In case of conventional control panels, these informations are communicated by discrete indicators, alarm slots, control tiles and recorders. Their arrangement on the panels, basically according to the flow schemes of the controlled systems, facilitates the link of the detail informations with the conceptual idea of the behaviour of the process and of the systems. Of course, this arrangement is a compromise to come up for the different types of needs (see above): a single arrangement of displays and indicators is used for the different purposes: monitoring, analysis of the plant state, detection of failures....

2.2 APPROACH FOR SCREEN-BASED VISUALISATION

A much more systematic approach, directly oriented on the different types information of needs of the staff, can be assured by screen-based process control: the same piece of information can be used in multiple different context, adapted to the specific task of the operator: it can be shown in formats serving for overall process monitoring, it can be shown in formats allowing to evaluate the consequences of an equipment failure, etc.

But of course, the basic features of screen-based information presentation has be respected: the overall vision has to be assured in spite of the specific properties of screen-based visualisation which is potentially handicapped by the limited size of the formats and the limited number of information in a single format.

Four essential methods are applied to come up for this:

1) **Hierarchic organisation** of the information, by providing a hierarchy of screen-based formats. This hierarchy starts at the top level with a few overview formats restricted to

essential plant state information, followed by a set of underlying formats with increasing level of detail. By this, any task of the operator can be supported by formats with an adequate level of detail.

2) Use of **large screens/** multi-screen-arrangements/ large panels providing less spatial restrictions

3) **Task-oriented presentation** of the same information in different arrangements, adapted to different tasks of the operator

4) Use of calculated, pre-processed and **condensed information**, allowing to grasp rapidly the state of a complex system (voting of several sensor signals in order to provide a single signal; summarising state and status information for a complex system, thus producing information as "available" or "in operation").

2.3 GUIDANCE IN FAULT DETECTION, DIAGNOSIS AND - MANAGEMENT

As a complement to the approach providing synthesis information, also « guidance » is needed which leads the operator in case of faults from summary information to the underlying details. The essential objectives to respect in this domain are:

- allow an evaluation of the priority, gravity and impact on safety and availability of an event in the context of overall plant state,
- support the diagnosis of the event: presentation of fault hypotheses and of the information necessary to evaluate these hypotheses
- guide the operators to the information and controls where they get the required detail information to plan and execute their (re-) action.

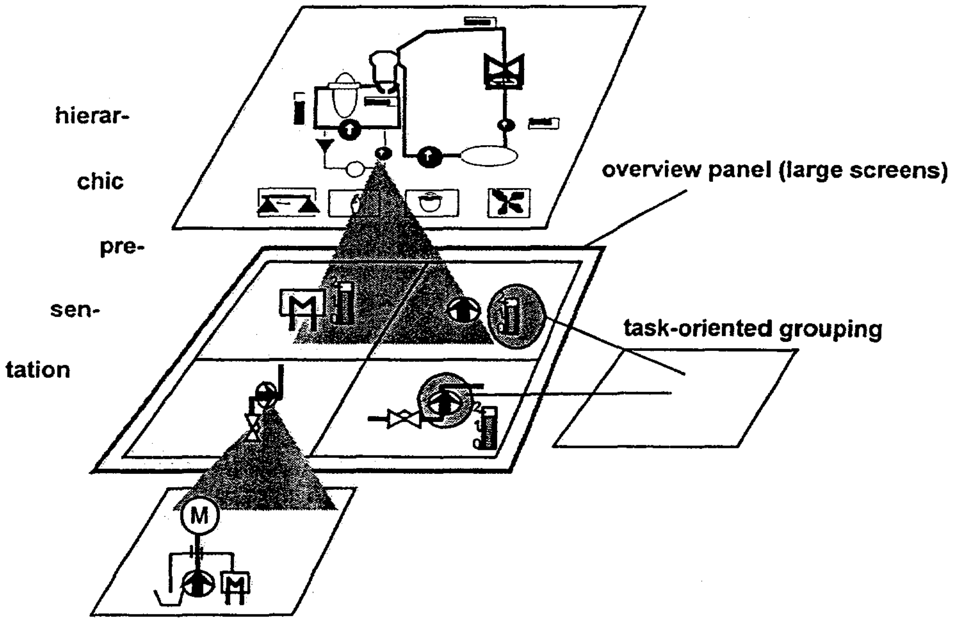


Figure 2: Different means used to assure good overall vision by screen-based visualisation

The application of the above given principles is of course not alone a matter of « scientific approach » but also strongly influenced by the expertise and « artistic » sense of the designers of screen-formats. Some examples are given, how they are applied to power plant visualisation and operator guidance.

3 APPLICATION OF THE PRINCIPLES

3.1 EXAMPLE 1: PLANT CIRCUIT FORMATS

A well known application of the above described principles is the hierarchic organisation of plant circuit formats:

- a set of detail circuit formats allows to visualise the whole plant on a high level of detail, each format dedicated to a single plant system (or even sub-system), with each valve, pump, automatism and sensor signal presented, which is to be accessed by the operators
- for presentation on a higher level of abstraction, state and status of the plant systems are summarised by synthetic status information, just providing the essential state and status information

  -> in/out of operation
  -> free of disturbance/degraded/unavailable
  -> possibly the mode of operation, and
  -> the presence/absence of new alarms
- this approach is pursued up to the top level format, presenting the whole plant in an adequately detailed level of abstraction, and providing optimal overview of the availability of all plant systems and circuits.
- all formats are linked one with the other by format links according to their functional role, thus allowing rapid navigation just by mouse-click between the different views, within one level of abstraction or changing the level of detail, according to the current task: evaluation of plant systems availability (high-level of abstraction); diagnosis of causes of failures (high level of detail...)... Of course, also the format links are animated, thus providing all necessary status information about the « functional environment » of a given plant system.

3.2 EXAMPLE 2: DIAGNOSIS OF I&C FAULTS

There are types of faults where correct operator response relies on "standard response patterns", thus minimising workload by access to formalised procedures:

I&C equipment faults are handled by "delegation" as long as they do not have an impact on the process: appropriate classification of I&C alarms allows the operator to distinguish rapidly if simply the I&C maintenance staff has to be informed (e.g. faults in redundant I&C equipment), or if an operator action is required.

In SIEMENS modern, digital I&C systems Teleperm XP and Teleperm XS, deep diagnosis of I&C faults is fully supported by the I&C system itself:

Most of the I&C components are equipped with self-surveillance features, and provide detailed diagnostic information. Additionally, the knowledge about the structure of the I&C system and about the properties of its components is made available to the I&C maintenance staff via "diagnostic stations": these present the whole I&C system in a hierarchic manner, showing the status of all components of the I&C system in many levels of detail, including display of the fault status according to the level (subsystem; cabinet; rack; I&C-board; fault message). Identification of a faulty component is then done simply by entering successively into the detail formats until the faulty component is identified.

Operator's, not I&C technician's action is typically required in case of blocked sequences. As a simple but very efficient diagnostic tool, animated function diagrams are used: in case of an I&C alarm signalling such a fault (announced by a specific I&C fault alarm), the operator is guided from the alarm sequence display (or from an alarm flag) to the operating format containing the concerned component, and obtains by one single mouse-click the associated function diagram; interlocks can be immediately detected and resolved, and appropriate actions easily identified.

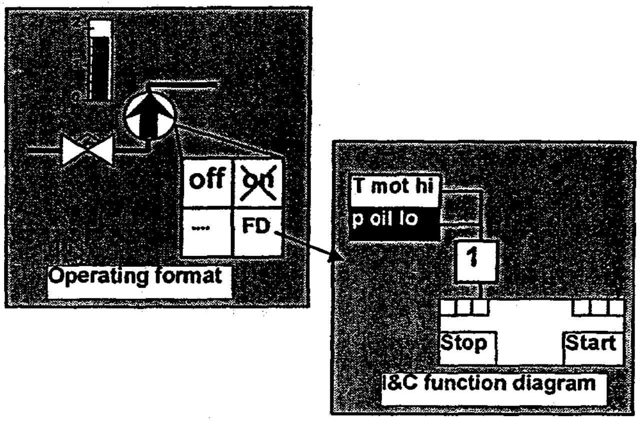


Figure 3: Visualisation of I&C functions by an animated functional diagram: the reason for interlocking of the start order of a pump is quickly found out in the associated animated functional diagram.

Both diagnostic functions do not necessitate specific engineering: the formats used for the diagnosis of I&C component faults as well as the animated function diagrams are side products of the engineering of the I&C system: hard ware structure diagrams as well as function diagrams are designed by the graphical engineering tool and form the basis for the configuration of the hardware of the I&C system, for the configuration of the networks and also for the code generation of the automation functions. Because of the principle of "forward documentation" the resulting diagnostic functions will always be consistent with the as-built status.

3.3 EXAMPLE 3: GUIDANCE ON THE BASIS OF ALARM RESPONSE PROCEDURES

Where specific, highly reliable response of the operators are required, more restrictive guidance is needed. For the response to individual faults of components and systems, this guidance is assured by "alarm response procedures" (alarm sheets), one specific part of the operating manual. These alarm sheets provide all the information necessary for the management of the faults linked to an individual alarm:

- description of the potential causes leading to a given alarm
- description of the symptoms linked to the different potential causes; this description allows the operators to perform the diagnosis (at least to the level of detail needed for the operator's actions)
- description of expected plant/system behaviour
- description of required operator actions.

This classic approach constitutes a first level of "diagnostic guidance" to the operators, fully sufficient in simple, pre-analysed situations.

As an increase of comfort, nowadays the alarm sheets are now available on-line, using a computerised operating manual. The alarm sheet linked to a given alarm is then available simply by clicking the alarm in the alarm sequence display (respectively in the command menu of an operating format) and immediately presented on the operating screen.

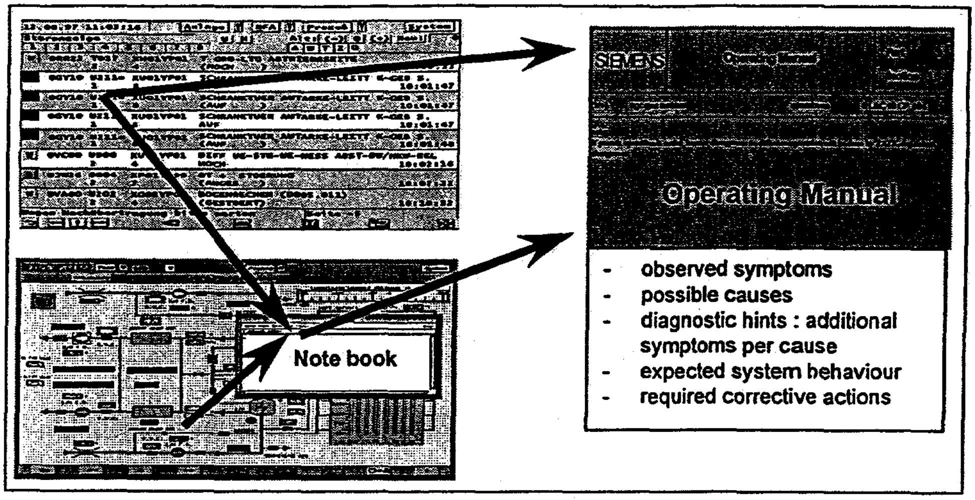

Operating Manual
Note book
- observed symptoms
- possible causes
- diagnostic hints : additional symptoms per cause
- expected system behaviour
- required corrective actions

Figure 4: Alarm-response procedure implemented in the computerised operating manual

3.4 EXAMPLE 4: ACCIDENT MANAGEMENT PROCEDURES

The Siemens/KWU accident management concept is based on a combination of the safety-function oriented and the event-oriented accident management approach (figure 5). The basic idea is that the operators perform after the onset of an incident situation an evaluation of the safety status of the plant, based on the safety function oriented operating manual, and then perform a rough diagnosis of the event, so as to classify it according to the different event-oriented procedures foreseen in the operating manual. If this classification is possible, the appropriate event-oriented procedure is selected and successively executed. The procedure then provides regular breaks where the critical safety functions of the plant are checked, and, where necessary, appropriate complementary actions performed.

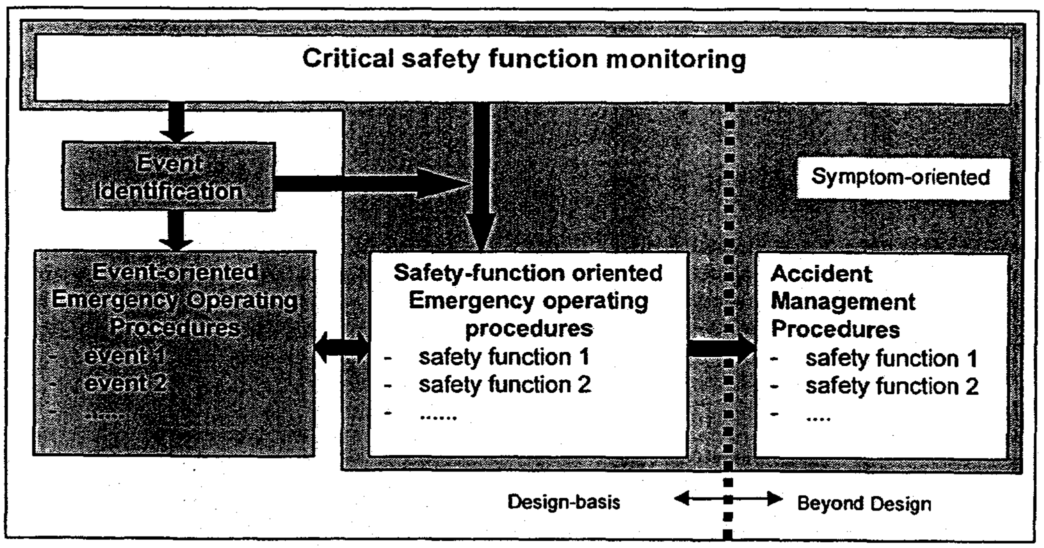


Figure 5: Siemens/KWU accident management concept

This is supported by a set of "safety-function display formats" grouping each all of the relevant process values and component status information relevant for a given safety function. In order to simplify overall monitoring, also summary icons resuming the status of every safety functions in several grades (OK, in danger, violated) can be foreseen, and thus allow to alert the operator much faster.

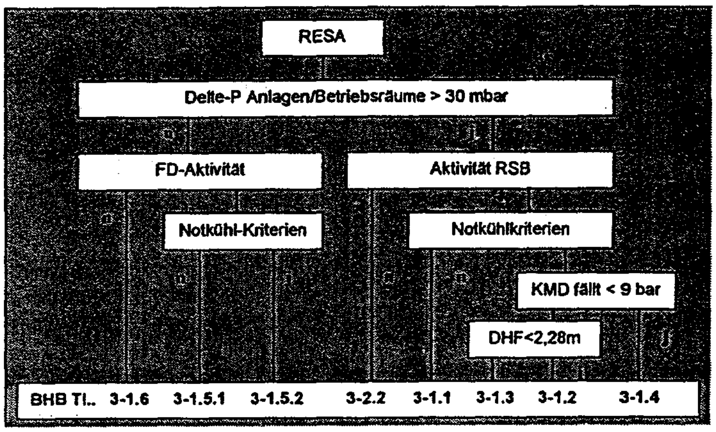

RESA
Delte-P Anlagen/Betriebsräume > 30 mbar
FD-Aktivität
Aktivität RSB
Notkühl-Kriterien
Notkühlkriterien
KMD fällt < 9 bar
DHF<2,28m
BHB TI.. 3-1.6 3-1.5.1 3-1.5.2 3-2.2 3-1.1 3-1.3 3-1.2 3-1.4

Figure 6: Accident decision tree (very simplified)

The classification of the type of the vent is performed using the so-called "accident decision tree", playing an important role in the overall procedure (figure 6). It constitutes the explicit diagnostic guidance required for this approach. The "classic" version is implemented as a paper-based procedure. An advanced version is implemented as an operating format, displaying directly the diagnosis proposed by the system as a result of the process parameters, and offering also complementary information for verification of the underlying process information.

This method works also in the case of multiple faults; however, in such cases the diagnosis may become more complicated because it necessitates typically the switch-over to the safety-function oriented approach providing additional, however less formalised guidance.

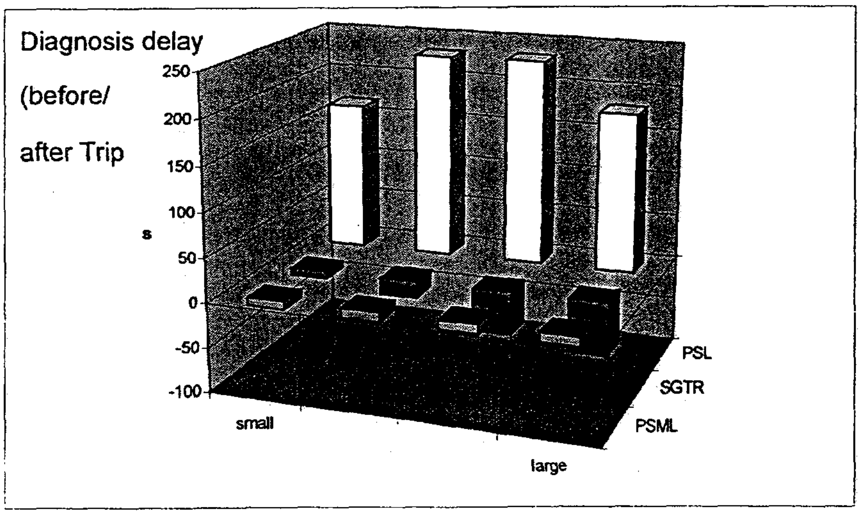


Figure 7: Delay of the event diagnosis (measured against the moment of reactor trip), performed by using a computerized Bayesian network, for different kinds of events and leak sizes. In many cases, the correct diagnosis would be already available before the trip.

One solution to be applied may be the use of more advanced diagnostic methods. The use of Bayesian networks as a very efficient diagnostic means is currently studied /5/. This approach offers two important advantages:

- the networks, when conditioned on the basis of extensive simulator runs covering all anticipated event combinations, allow to diagnose easily and efficiently single as well as multiple faults
- the diagnosis resulting from the network is available within a very short time interval, and the pertinence of the diagnosis could be evaluated on a "confidence factor" provided by the network.

Figure 7 gives an overview of the response time of the network for three types of events (pressurizer steam leak, steam generator tube rupture, small/medium primary leak). The response time (in many cases, the type of event is diagnosed BEFORE the reactor trip!) seems to be very promising.

However, the diagnosis of multiple events, and the integration into the overall process control concept necessitates still more detailed analysis. Only a concept which fits into the overall process control framework will be acceptable by the operators.

4 OUTLOOK AND SUMMARY

In plants which have been in operation now for 15 to 20 years, the modernisation or even the complete replacement of I&C system becomes an attractive option. The replacement of ageing, hard wired I&C systems by digital system should lead to clear economic improvements with respect to I&C service and maintenance:

- ■ the extensive use of standard equipment simplifies the management of spare parts
- ■ future supply with spare parts is assured on a long-term basis
- ■ automation functions are implemented by application software; this allows to reduce the amount and diversity of equipment, especially for nuclear specific functions
- ■ the more compact design allows for extension of functions that would not be possible in the older techniques because of space problems.

The switch-over to digital systems offers also a chance for clear improvements in plant operation and - management: introduction of digital systems in the control room by screen based monitoring and control introduces the following advantages:

- ■ better integration of process control and plant management functions
- ■ improved process visualisation
- ■ possibility, to include a computer-based operating manual directly into process control
- ■ advanced support of accident operation by task-oriented operating formats
- ■ improved detection and correction of I&C faults by online diagnostics
- ■ integrated, rapidly accessible documentation, consistent with the as-built status of the plant.

5 REFERENCES

/1/ Roth-Seefrid, H., Erdmann, J., Simon, L., Düll, M.: SIROG: a computer-based manual for situation related operator guidance. Halden programm group meeting on Man-Machine Systems Research. 30.10.-4.11.1994, Bolkeskjö, Norwegen.

/2/ Kraushaar, K.H.: Die Cockpit-Warte in Block 5 des Kraftwerkes Staudinger. VGB-Konferenz Leittechnik 1994, 12.-13. April 1994, Cottbus.

/3/ Guesnier, G., Heßler, C.: Milestones in screen-based process control. In:Kerntechnik 60 (1995) 5-6, pp. 225-231.

/4/ Achievements of the Halden reactor projects 1994-1996

/5/ Darken, C., Santoso, I., Erdmann, J.: Accident Diagnosis with probabilistic Reasoning (Jahrestagung Kerntechnik 1999, to be published).

accident conditions by four channel operator modules, which shall also be electrically isolated and physically separated.

- Manual reactor trip or system-level ESF actuation by the hardwired switches.

3. Design Details

The safety console is divided into two sections, monitoring and control sections. The upper section of the console accommodates the monitoring devices and the desk accommodates the soft-controller and switches. A menu-driven touch method is adopted for the operator input on both monitoring devices and soft-controllers, to simplify the man-machine interface (MMI) at this point. The size of the console will be determined to be suitable for one man operation and several design guides are referred to the display and soft-controller design [4]. A function analysis for SMART is performed for the systematic function-based display design and soft-controller layout.

3.1 Function Analysis

The function analysis is one of the major alternatives to incorporate human factors systematically into the man-machine interface system (MMIS) design [5]. In the analysis SMART function is decomposed from the operator point of view instead of system design and its results can help us in establishing the function structure essential to identify the MMIS

Table I. A Part of Function Analysis Tree to Achieve the SMART Power Production Goal

Function Goal : Power Production

Critical Function	**Major-function**	**Sub-Function**	**System Function**
Create Fission Energy	Control Reactivity	Control Rod	Regulate Shutdown Rod
		Control Boron	Inject Borated Water
			Regulate Regulating Rod
	Control Moderator Density	Control Moderator Temp.	Control FW Flow
		Control Moderator Pressure	Control PZR Pressure
Transfer Fission Energy	Maintain Coolant Inventory	Control Coolant Flow	Align V/Vs
			Control Makeup Water
		Maintain Coolant Purification	Connect Filters/Ion Exchanger
		Maintain Sub-cooled Margin	Control PZR Temperature
			Control PZR Pressure
			Control Main Coolant Pumps
			Regulate Control Rods
	Circulate Coolant	Maintain Forced Circulation	Control Main Coolant Pumps
		Maintain Natural Circulation	Control PZR Pressure
	Maintain Secondary Heat Sink	Supply Feed Water	Regulate Feed Water Flow

Table II. A part of Function Analysis Tree to Achieve the SMART Safety Goal

Function Goal : Safety

Critical Function	**Major-function**	**Sub-Function**	**System Function**
Isolate Rx Vessel		Isolate safeguard vessel	Close isolation V/Vs
		Isolate contain. vessel	Close isolation V/Vs
Maintain Vessel Environs Below Limited Values	Maintain S.V. environs	Control S.V. Temp.	TBD
		Control S.V. Press.	TBD
		Control S.V. combustible gas	TBD
		Reduce S.V. radiation level	TBD
	Maintain C.V. environs	** Same as "Maintain S.V. environs"	
Maintain Core Sub-criticality		Insert rods	Insert Shutdown Rod Regulate Regulating Rod
		Inject Borated Water	Control boron
Maintain Core Cooling	Maintain integrity of core coolable geometry	Control coolant flow rate	Compensate from ECCS tank Compensate from makeup sys.
		Maintain integrity of internal structure	No support systems
	Circulate coolant	Control forced circulation	Control MCPs
		Maintain passive circulation	Remove heat by secondary sys.
	Remove core heat	Remove heat by secondary sys.	Control steam & FW sys.
		Remove heat by passive RHR	Maintain flow path to ECT

design requirements and to design the function-based displays and controls.

The SMART function is decomposed systematically from three top goal functions to detailed component level functions for each goal. The function tree analyzed for each goal has more than seven function levels; critical function level, major function level, sub-function level, and so on. Table I presents a part of the function tree for the power production goal and Table II for the safety goal of SMART. The critical function level information and controls are located on the top page of displays and soft-controllers.

3.2 Design of Displays

The detail functions of each display device are determined from the information display hierarchy in Fig. 1. The operational information within SMART MCR are mainly presented through a large overview display, CRT displays, flat panel displays (FPDs). Besides them, the soft-controller can provide some dedicated information for a specific control action. Basically the operational information are categorized into three levels, critical function level, system level, and equipment and diagnostic level except for an overview.

The safety console displays consists of three kinds of FPDs. One FPD located in the center of the console provides the detail information necessary to operate the plant during abnormal conditions and accidents. Another two channelized FPDs present R.G. 1.97 category 1 variables. The other four FPDs are indicators displaying the parameters selected by the operator.

1) Detail Information Display

The conventional hardwired console spreads the information on the console through display devices and the operators can access them in parallel. However on the VDU-based compact workstation using a common device like CTR or FPD, it is not possible for the operator to access the information in parallel. To solve this problem, it is general to use the hierarchical information display structure.

This display adopts the three level function-based hierarchy as discussed above. That is, from this display the operator can get all information associated with the functions assigned to the safety console. The display has four first-level safety critical function screens as shown in Fig. 2(a) and the other critical function screens for power production and support functions. Each first-level screen has its own hierarchy from system function level in Fig. 2(b) to diagnostic function level. In addition the display contains a task-oriented startup screen to provide the detail information for startup operation and the emergency operating procedures for operator aids.

The display screens for continuous operation in the case of a failure of the main console are based on the power productions and support functions, and their information is scaled down to some degree compared to that of CRT screens on the main console used in normal operation. This means the depth of details of information is less than that of CRT.

2) Post-accident monitoring displays

The post-accident monitoring variables that are selected in SMART design based on the R.G. 1.97, are monitored by two channel displays electrically isolated and physically separated. The display screen in Fig. 3(b) is divided into four sections by the SMART system - reactor, containment, safeguard vessel and other systems. Each variable is real-time continuously monitored, and the operator can get its trend or equipment status information by touching the specific variable on the screen as shown in Fig. 3(a).

3) Indicators

The indicators provide the safety related and frequently used parameters important to operations during the reactor shutdown or performing other safety functions on the safety console. These include R.G. 1.97 Category 2&3 variables, major operating parameters, and ESF equipment status information, etc. They use some spatially dedicated displays for easy and rapid access to operators.

3.3 Design of controls

The controllers, the means for directly controlling the system equipment and inputting the operator's commands to the system, are designed to meet the requirements of the equipment controlled. Three kinds of controllers are provided as below. The controllers on the safety console are designed to be safety class except for a non-safety grade soft-controller used for continuous reactor operation.

1) Soft-controller

The soft-controller is an electronic device that performs an operator's control action by a software-driven device. In the SMART design, it provides the functions of switches, process controllers, operator modules, and other means for operator's input for test and maintenance. The key design concepts established are; the use of digital devices driven by software considering the limited space on the compact workstation, the provision for the function-based controller which contains both controls and information, and the acceptance by the regulatory requirements including digital equipment qualification and human factor concerns [6].

The controls for equipment on the soft-controller are grouped by function to provide easy access to a specific controller or effective navigation. Therefore each function-based controller displayed on a page is composed of multiple systems, and each system controller has several component controllers. The soft-controller is being developed to minimize the operator's workload to search for the related information from other display devices by providing them on the controller. We identified the operational information necessary to perform each function from the function analysis trees. Fig. 4(a) and 4(b) are typical process controller and switch design.

2) Operator module

The operator modules are man-machine interfaces for controlling and testing the reactor protection and ESF actuation systems, which are channellized independently. These provide not only the control means but the operating information about the controlled equipment and reactor trip or pre-trip alarms. Some other operator modules will be added on the test and maintenance consoles later.

3) Hardwired switch

A few of hardwired switches are arranged on the desk of the console to shutdown the reactor manually. They perform the system level actuation instead of component level actuation.

3.4 Prototype

A prototype of the safety console is fabricated to verify the design, and the developed displays and controls are combined with the prototype. Fig. 5 is a layout of the console, and the several color FPDs are used for displays and controls. At present we are discussing the validity of display design and the navigation method on the console. The displays and controllers are implemented with three types of FPDs and the personal computers using Windows 95 operating system and SL-GMS as a graphic user interface.

4. Conclusions and Further Works

A safety console is developed to be a seated-type compact console based on the VDUs driven by computer, which provides the monitoring and control means for the operators within the SMART MCR during the operations of a reactor safe-shutdown and mitigation of an accident. An information display hierarchy is developed for the function assignment of displays and controls of the console. The SMART function decomposed from the operator's point of view provides a basis of the function-based display hierarchy. The soft-controller, developed as a new MMI, is widely adopted for controls.

Through this study, it is believed that this systematic console design will be helpful for operation by reducing the operator's work load to respond to the abnormal states in the plant. Also, it will be possible to design the computerized control room only through this kind of console although there will be unanticipated defects in the application of function-based design technique and digital devices.

At this time we are preparing the anthropometry test to determine its size and layout, and in the future, the availability and suitability of console will be added together with a functional integration test of the displays and controls.

Acknowledgements

This study has been carried out under the Nuclear R&D Program by MOST in Korea.

References

[1] Development of MMIS Design Technology for Integral Reactor, KAERI/RR-1901/98, Mar., 1999 (in Korean)

[2] IEEE-603, "Criteria for Safety Systems for NPGS"

[3] IEEE-7.4.3.2, "Criteria for Digital Computers in Safety Systems of NPGS"

[4] NUREG-0700, "Human-System Interface Design Review Guideline",

[5] NUEG-0711, "Human Factors Engineering Program Review Model"

[6] C.K.Lee et al, "Development of Soft-controller for SMART Design", '98 IAEA Specialist's Meeting, Garching, German, Oct., 1998

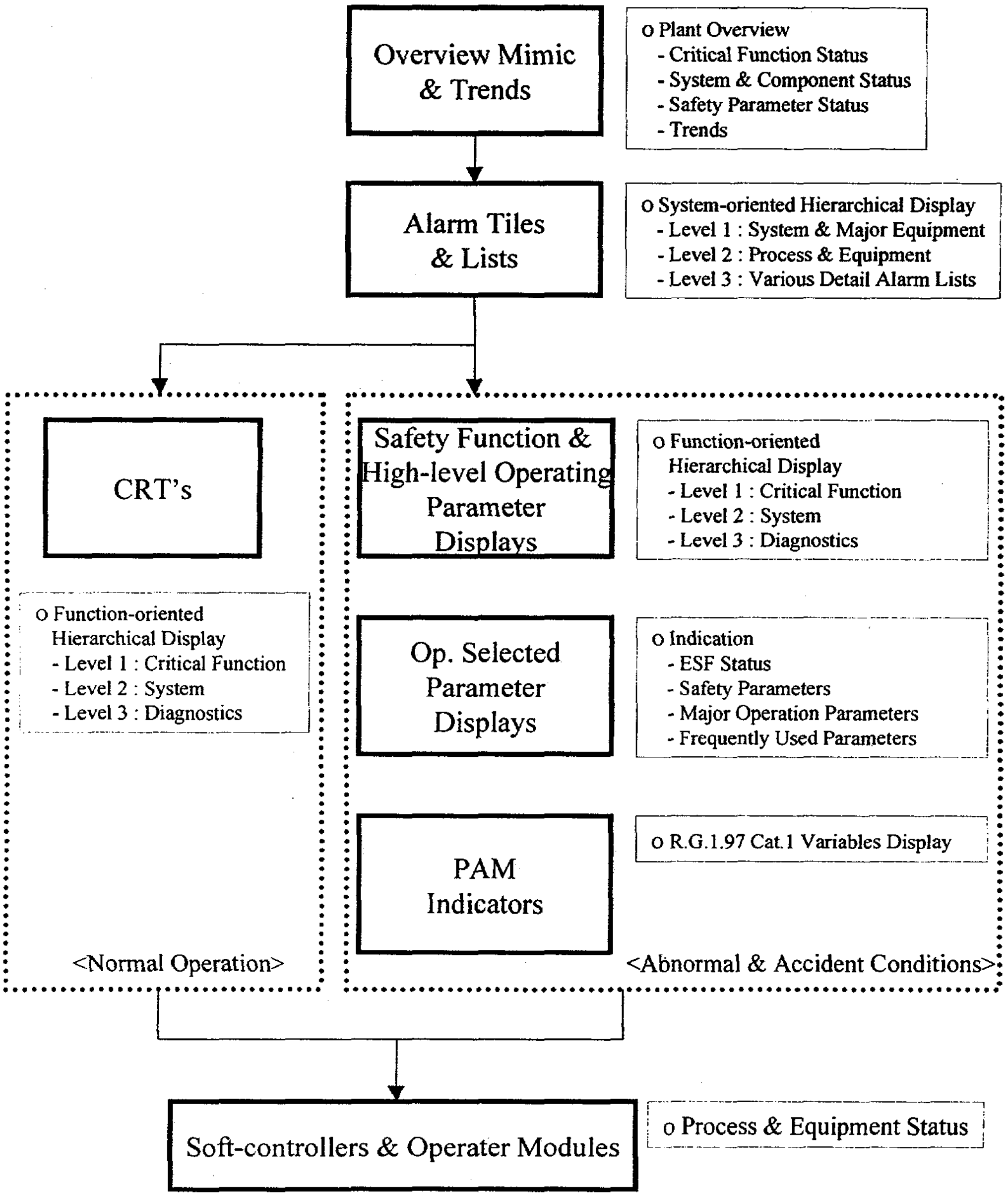
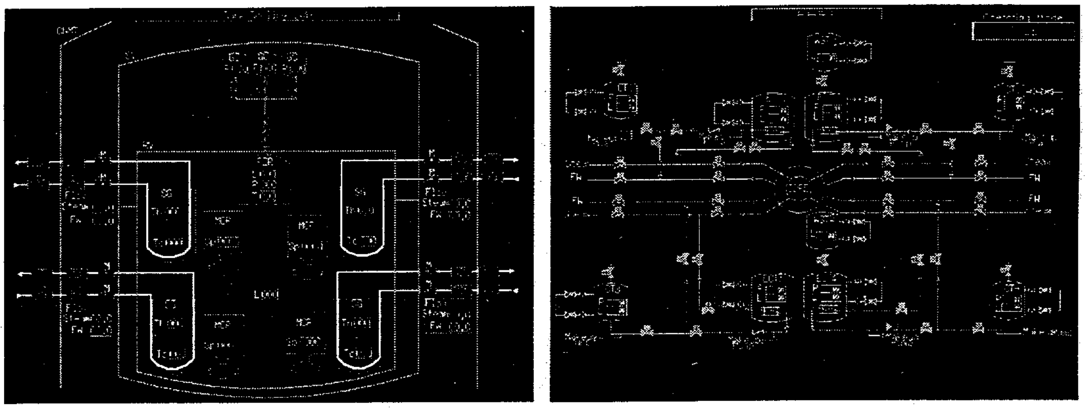
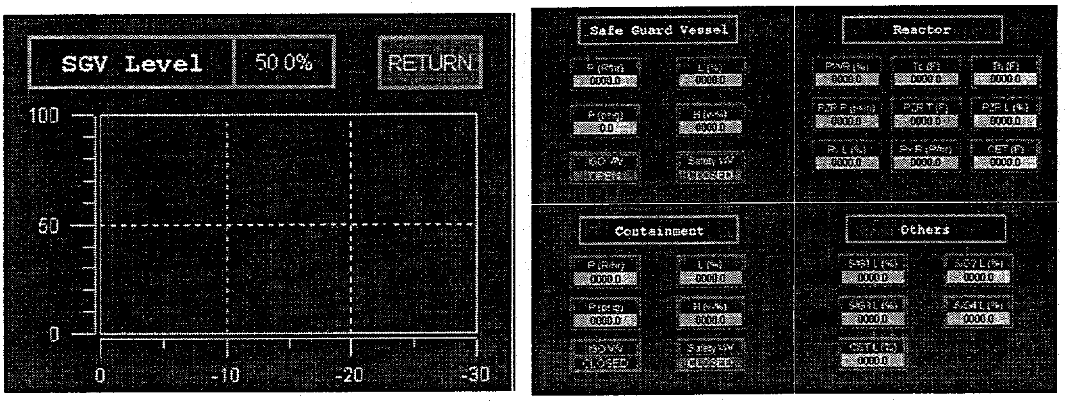

Overview Mimic & Trends
o Plant Overview
- Critical Function Status
- System & Component Status
- Safety Parameter Status
- Trends
Alarm Tiles & Lists
o System-oriented Hierarchical Display
- Level 1 : System & Major Equipment
- Level 2 : Process & Equipment
- Level 3 : Various Detail Alarm Lists
CRT's
o Function-oriented Hierarchical Display
- Level 1 : Critical Function
- Level 2 : System
- Level 3 : Diagnostics
<Normal Operation>
Safety Function & High-level Operating Parameter Displays
o Function-oriented Hierarchical Display
- Level 1 : Critical Function
- Level 2 : System
- Level 3 : Diagnostics
Op. Selected Parameter Displays
o Indication
- ESF Status
- Safety Parameters
- Major Operation Parameters
- Frequently Used Parameters
PAM Indicators
o R.G.1.97 Cat.1 Variables Display
<Abnormal & Accident Conditions>
Soft-controllers & Operater Modules
o Process & Equipment Status

Figure 1 Information Display Hierarchy in the SMART MCR



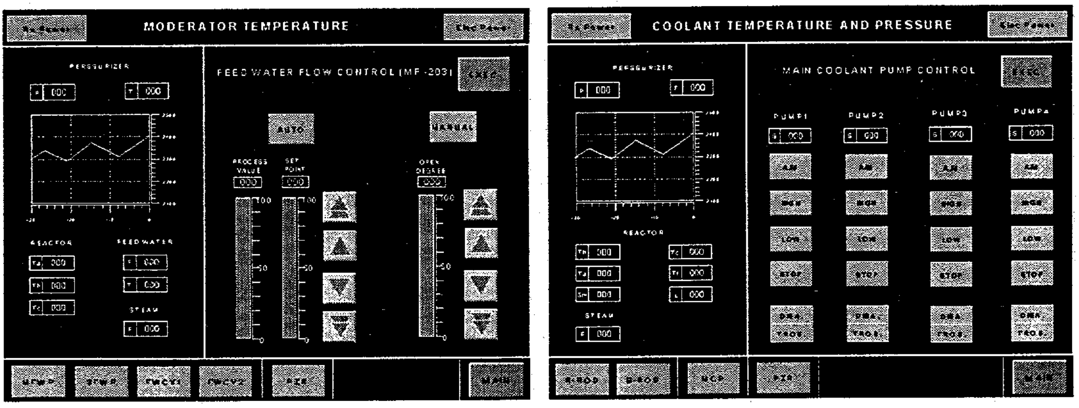
a) Level 1 Display b) Level 2 Display

Figure 2 Detail Information Display Screen (Typical)



a) Detail Display for a Specific Variable b) PAM Display Overview

Figure 3 Post Accident Monitoring Displays (Typical)



a) Process Regulating-type Controller b) Switch

Figure 4 Soft-controller Display (Typical)

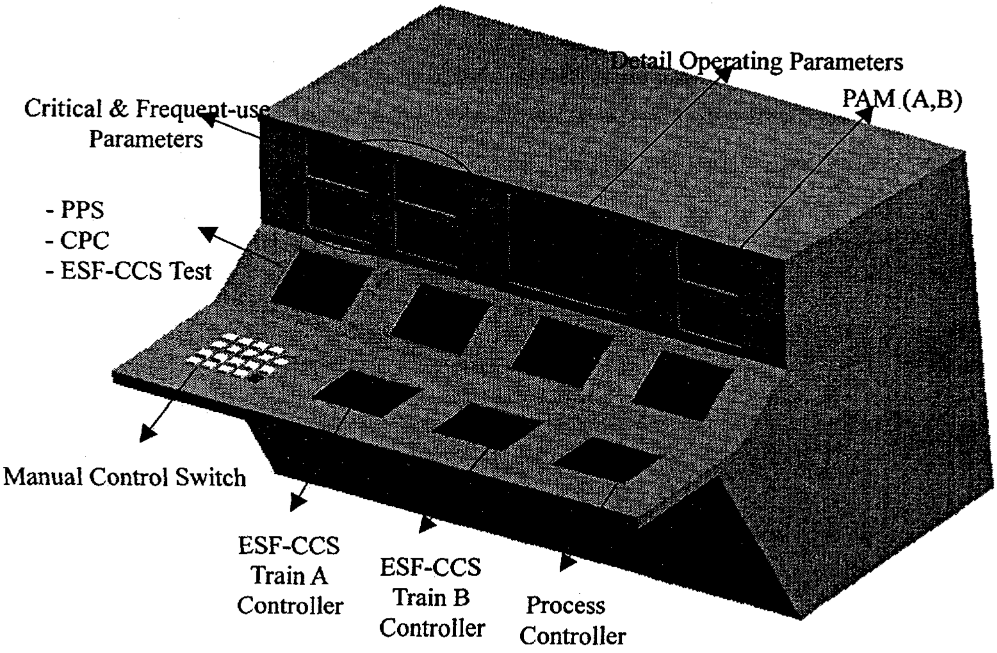


Figure 5 Safety Console Layout

SESSION 5

GENERAL DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS

IAEA Specialists' Meeting On Human-Machine Interface For Off Normal And Emergency Situation In NPP

Taejon, Republic Of Korea
26-28 October 1999

EXECUTIVE SUMMARY

The conference, organized and sponsored by the IAEA, KAERI and KOPEC, hosted topical experts from 9 countries at the KAERI Conference Center. Twenty technical papers (12 domestic and 8 foreign) were presented and discussed. In all 20 presenters and 40 other attendees as well as various observers from the host country participated in the 3 day conference and technical visit to the Yonggwang NPP.

Participating Countries:

- Austria
- Canada
- Federal Republic of Germany
- Japan
- Rep. of Korea
- Pakistan
- Russian Federation
- Sweden
- United States of America

Topical highlights of the conference were:

- Advanced Research on Informational Processing in Off Normal and Emergency Situations
- Plant Referenced Simulator Upgrades, Training and Testing
- Control Room Upgrades and Retrofits (CANDU and SMART)
- Next Generation Reactors (KNGR)
- Computerized Procedure Systems
- Alarm Diagnostic and Support Systems
- Human Factor Evaluative Processes
- Safety Critical Process Visualization
- Advanced Vibration Diagnostic System

Session 1- **Operational Experience With Human Machine Interface**

Chairs - Mr. Suk-Joon Park and Mr. Andrei Kossilov

- Papers from Korea, Japan, Pakistan and the USA dealt with current HMI operational activities in operating NPP's

Session 2- **Current Developments in HMI Systems For Off Normal And Emergency Conditions**

Chairs - Mr. Poong Hyun Seong and Mr. Gerhard Schildt

- Papers from Korea, USA, Canada and the Russian Federation focused on design approaches to operator support systems

Session 3- **Licensing Issues For Human Machine Interface**

Chairs - Mr. Won Young Yun and Mr. Brian Smith

- Papers from Korea dealt alarm processing systems, NPP fault diagnostic systems and safety parameter display and evaluation systems (SPADES)

Session 4- **Current Developments And Trends**

Chairs - Mr. Kee-Choon Kwon and Mr. Sigehiro Kono

- Papers from Austria, Germany and Korea focused on alarm diagnostic systems, safety critical process visualization, informational diagnostic systems and safety console designs.

Closing Session - **General Discussions, Conclusions, Recommendations And Future Activities**

Chairs - Mr. Hyun-Kook Shin and Mr. Richard P. Coe

- Session summaries were presented and discussed observations.
  - General Discussions and Conclusions
  - Recommendations and Future Activities

General Discussions and Conclusions

At the end of the meeting a closing session was held. Session Chairmen gave inputs to the closing session co-chair, Mr. Richard P. Coe and Mr. Hyun-Kook Shin. Each input was the highlights of session, observations and recommendations for the future activities.

- Mr. Richard Coe presented summaries of sessions one and two with his impressions:

I think international nuclear energy community is changing. The changes are in everything from existing instruments to next generation reactors. To me, as a participant, newly emerging technology that we shared over the couple of days was extremely impressive.

The highlight of the sessions one and two is the changes of processing information both in off normal and emergency conditions. Many key areas were presented here, including training NPP personnel and role of the simulator. Couple of papers dealt with control room upgrade and introduced how it is changing, showed us what the future looks like.

I was also keenly interested in the Korean next generation reactor KNGR that was discussed today. The computerized procedure system is another thing that a operator is going to look at in the future. It is something of great aid when operators are in off normal and emergency condition, if they can bring this information more rapidly and more concisely.

Advanced diagnostic system was also discussed here, showing some trend of great predictability and reliability in maintenance. It was a great impressive area.

- Mr. Hyun-kook Shin continued the summaries of sessions three and four and his observations :

In session 3, licensing issues for HMI was presented. Mr. Brian Smith, one of the session chair, indicated that the highlight of session was the evaluation of alarm processing systems. He also commented that a very detailed mathematical analysis on the effectiveness of the systems was presented, but little evidence of end-user (operator input) involvement was shown.

Mr. Won-Young Yun, indicated that the highlight of the session was "Application of Human Factor Engineering Program for Safety Parameter Display and Evaluation System (SPADES) design". And he expressed his observations, "most people are interested in engineering design, application issues and operational experience. So, the presentation should be focused on those related topics."

In session 4, future development and trend was presented and chaired by Mr. Kee-Choon Kwon and Mr. S. Kono. Mr. Kee-Choon Kwon indicated that new concept, fail-safe critical process visualization for NPPs was shown. The paper "Development of Alarm-Diagnosis Integrated Operator Support System", presented by Mr. Hwang, was very impressive to him. He extended his observation that computer-based alarm processing system would be a great aid to operators in off normal and emergency situations.

And I would like to add my observation; " In session 3, two papers were not directly related to licensing issues. But through these studies, by using new evaluation methods, human-machine related system can be easily reviewed and evaluated of its performance."

Recommendations and Future Activities

- Development of computer-based operator support system or control system should be considered in terms of human evaluation and safety of its function. It is recommended that these related areas will be studied in the future.

- More general topics for the specialists' meeting are suggested in order to draw more participants from the field engineers, plant operators and researchers. And if possible, it is recommended to invite the guest speakers from the fields of meeting topic.

- In this meeting, the topics of human machine interface are major issues, but most of presented papers were dealing with computer based systems and operator support systems. Hence, in the future, more of human factors oriented papers and technologies need to be invited for the meeting.

LIST OF PARTICIPANTS

LIST OF PARTICIPANTS

Name	Address & E-mail	Telephone	Fax.
AUSTRIA			
Gerhard H. Schildt	Mr. Gerhard H. Schildt Institute of Computer-Aided Automation Vienna University of Technology Treitlstr. 1/183 A-1040 Vienna Austria Email: schi@auto.tuwien.ac.at	+43 1 58801-18310	+43 1 58801 18391
CANADA			
Mark P. Feher	AECL 2251 Speakmann Drive Mississauga, Ontario L5K LB2 Canada feherm@aecl.ca	905 823 9040 ext. 3105	905 823 9754
J. McBeth	AECL - Korea 8th Floor, Duk Myung Building 170-9 Samsung-dong, Kangnam-ku Seoul South Korea 135-091 macbethm@aecl.ca	82 2 539 3030	82 2 567 0072
Brian E. Smith	Atomic Energy Control Board P.O. Box 1046, Station B 280 Slater Street Ottawa Canada K1P589 Canada smith.b@atomcon.gc.ca	613 943 8896	613 992 1921
GERMANY, FEDERAL REPUBLIC OF			
M. Lechleuthner	Siemens AG KWU, Dept. NLLZ P.O. Box 3220 D-91050 Erlangen Germany Lechleuthner@erl11.siemens.de	+49 9131 18 85468	+ 49 9131 18 5154
JAPAN			
Sigehiro Kono	Toshiba Corporation 8 Shinsugita-cho, Isogo-ku, Yokohama 235-8523 Japan shigehiro.kono@toshiba.co.jp	+81 45 770 2188	+81 45 770 2463
Masaya Kotoku	Fuchu Complex Toshiba Corporation Toshiba-cho, Fuchu-shi, Tokyo 183-8511 Japan masaya.kotoku@toshiba.co.jp	+81 42 333 2178	+81 42 333 0144

Name	Address & E-mail	Telephone	Fax.
KOREA			
Kee-Choon Kwon	KAERI P.O.Box 105, Yusong, Taejon 305-600, Korea kckwon@nanum.kaeri.re.kr	82-42-868-2926	82-42-868-8357
Suk-Joon Park	KOPEC P.O.Box 148, Yusong, Taejon 305-600, Korea sjpark@ns.kopec.co.kr	82-42-868-2543	82-42-861-1388
Hyun-Kook Shin	KOPEC P.O.Box 148, Yusong, Taejon 305-600, Korea hkshin@ns.kopec.co.kr	82-42-868-2745	82-42-861-1388
Jung-Taek Kim	KAERI P.O.Box 105, Yusong, Taejon 305-600, Korea jtkim@nanum.kaeri.re.kr	82-42-868-2926	82-42-868-8357
Yong-Hee Lee	KAERI P.O.Box 105, Yusong, Taejon 305-600, Korea yhlee1@nanum.kaeri.re.kr	82-42-868-2941	82-42-868-8357
In-Koo Hwang	KAERI P.O.Box 105, Yusong, Taejon 305-600, Korea ikhwang@nanum.kaeri.re.kr	82-42-868-2925	82-42-868-8357
Soon-Ja Song	KAERI P.O.Box 105, Yusong, Taejon 305-600, Korea songs@nanum.kaeri.re.kr	82-42-868-2958	82-42-868-8357
Dong-Young Lee	KAERI P.O.Box 105, Yusong, Taejon 305-600, Korea dylee2@nanum.kaeri.re.kr	82-42-868-2404	82-42-868-8357
Joo-Hyun Park	KAERI P.O.Box 105, Yusong, Taejon 305-600, Korea ex-hyun@nanum.kaeri.re.kr	82-42-868-8345	82-42-868-8357
Cheol-Kwon Lee	KAERI P.O.Box 105, Yusong, Taejon 305-600, Korea cklee1@nanum.kaeri.re.kr	82-42-868-8657	82-42-868-8655
In-Soo Koo	KAERI P.O.Box 105, Yusong, Taejon 305-600, Korea iskoo@nanum.kaeri.re.kr	82-42-868-2905	82-42-868-8655
Guen-Ok Park	KAERI P.O.Box 105, Yusong, Taejon 305-600, Korea gopark@nanum.kaeri.re.kr	82-42-868-2960	82-42-868-8655
Sang-Mun Suh	KAERI P.O.Box 105, Yusong, Taejon 305-600, Korea smsuh@nanum.kaeri.re.kr	82-42-868-8869	82-42-868-8655

Name	Address & E-mail	Telephone	Fax.
Hyun Gook Kang	KAERI P.O.Box 105, Yusong, Taejon 305-600, Korea ex-khg@nanum.kaeri.re.kr	82-42-868-8886	82-42-863-9860
Jong Hyun Kim	KAIST 373-1 KuSong-Dong, Yusong-Gu, Taejon, Korea jh2@cais.kaist.ac.kr	82-42-869-3860	82-42-869-3895
Poong Hyun Seong	KAIST 373-1 KuSong-Dong, Yusong-Gu, Taejon, Korea phseong@sorak.kaist.ac.kr	82-42-869-3820	82-42-869-3810
Won Young Yun	KINS 19 KuSong-Dong, Yusong-Gu, Taejon, Korea k034ywy@pinpoint.kins.re.kr	82-42-868-0237	82-42-861-0943
Yoon-Hyung Chung	KINS 19 KuSong-Dong, Yusong-Gu, Taejon, Korea k078cyh@pinpoint.kins.re.kr	82-42-868-0245	82-42-861-0943
Young Ju Kang	KEPCO 84-4 Bugu-ri, Buk-myun, Ulchin-Gun, Kyung Buk, 767-890, Korea yjkang@dava.kepco.co.kr	82-565-758-1110	82-565-758-1599
Sung-Bong Kim	KEPCO 84-4 Bugu-ri, Buk-myun, Ulchin-Gun, Kyung Buk, 767-890, Korea kimsbo@dava.kepco.co.kr	82-565-758-2810	82-565-758-2809
Yeong Cheol Shin	KEPRI 103-16, Munji, Yusung, Taejon, Korea ycshin@kepri.re.kr	82-42-865-5650	82-42-865-5504
Yong Kwan Lee	KEPRI 103-16, Munji, Yusung, Taejon, Korea leeyk@kepri.re.kr	82-42-865-5630	82-42-865-5504
Joong Nam Kim	KEPRI 103-16, Munji, Yusung, Taejon, Korea jnkim@kepri.re.kr	82-42-865-5653	82-42-865-5504
Eung Se Oh	KEPRI 103-16, Munji, Yusung, Taejon, Korea esoh@kepri.re.kr	82-42-865-5652	82-42-865-5504
Kyung Hun Chung	KEPRI 103-16, Munji, Yusung Taejon, Korea khchung@kepri.re.kr	82-42-865-5651	82-42-865-5504
Wan Hee Chae	KEPCO Knpd, 216, Kori, Jangan-Eup Kijang-Gun, Pusan, 619-711 Korea chawhee@dava.kepco.co.kr	82-51-726-3130	82-51-726-2813

Name	Address & E-mail	Telephone	Fax.
Tae Shin Park	KEPCO Knpd, 216, Kori, Jangan-Eup Kijang-Gun, Pusan, 619-711, Korea parkts@dava.kepco.co.kr	82-51-726-3133	82-51-726-2814
Bang Jin Lee	KEPCO Yonggwang Nuclear Power Plant Unit 3&4 514 Kyema-Ri, Hongnong-Eub, Yonggwang-Gun, Jeonnam, 513-880, Korea bangJin@dava.kepco.co.kr	0686-357-3450	0686-357-3303
Ki-Sang Song	KEPCO KEPCO Apt, Rm # 2-103 Hongnong-up Yonggwang-Gun, Jeonnam 513-880, Korea songksa@dava.kepco.co.kr	82-686-357-3410	82-686-357-3303, 2678
Hee Sang Noh	KEPCO 514 Kyema-Ri Hongnong-Eub Yongkwang-Gun, Jeonnam 513-880, Korea nohees@dava.kepco.co.kr	0686-357-2895	0686-357-2965
Hyo Je Ko	KEPCO 514 Kyema-Ri Hongnong-Eub Yongkwang-Gun, Jeonnam 513-880, Korea gohoj@dava.kepco.co.kr	82-686-357-2893	82-686-357-2965
Myoung Eun Chae	KEPCO 167, Samsung Dong, Kwang Nam Gu Seoul, Korea chaeme@dava.kepco.co.kr	02-3456-4954	02-3456-4999
Jong Ki Park	KEPCO 167, Samsung Dong, Kwang Nam Gu Seoul, Korea parkjgi@dava.kepco.co.kr	82-2-3456-4958	82-2-3456-4999
You Soo Lee	KEPCO 167, Samsung Dong, Kwang Nam Gu, Seoul, Korea LYS0821@dava.kepco.co.kr	02-3456-4959	02-3456-4999
Rin gi Kim	KEPCO 167, Samsung Dong, Kwang Nam Gu, Seoul 135-791, Korea ringgie@dava.kepco.co.kr	02-3456-4936	02-3456-4999
Jong Hyuk Kim	KEPCO Kyungbuk KyungJu-City YsngNam-Myun NaA-Ri 260 Wolsung Nuclear Power Plant 2 C & I Dept control@dava.kepco.co.kr	0561-779-3522	0561-779-3489
Jai-Bok Han	KOPEC P.O.Box 148, Yusong, Taejon 305-600, Korea jbhan@ns.kopec.co.kr	82-42-868-8190	82-42-861-1388

Name	Address & E-mail	Telephone	Fax.
Seung Han	KOPEC P.O.Box 148, Yusong, Taejon 305-600, Korea hanlee@ns.kopec.co.kr	82-42-868-2843	82-42-861-1388
Seung-Min Baek	KOPEC P.O.Box 148, Yusong, Taejon 305-600, Korea smbaek@ns.kopec.co.kr	82-42-868-8628	82-42-861-1388
Ki-Chang Son	KOPEC P.O.Box 148, Yusong, Taejon 305-600, Korea kcson@ns.kopec.co.kr	82-42-868-8667	82-42-861-1388
Il-Nam Choe	KOPEC 360-9 Mabuk-Ri, Kusung-Myun Yongin, Kyunggi-Do 449-910, Korea : inchoe@kopec.co.kr	82-331-260-6200	82-331-260-6000
Moon-Jae Choi	KOPEC 360-9 Mabuk-Ri, Kusung-Myun Yongin, Kyunggi-Do 449-910 Korea mjchoi@kopec.co.kr	82-331-260-6201	82-331-260-6000
Jin-Koo Kim	KOPEC 360-9 Mabuk-Ri, Kusung-Myun, Yongin Kyunggi-Do 449-910 Korea jinkoo@kopec.co.kr	82-331-260-6205	82-331-260-6000
PAKISTAN			
Tariq B. Tahir	KANUPP Karachi Pakistan knpc@khi.comsats.net.pk	92 21 920 2222	92 21 920 2240
RUSSIAN FEDERATION			
Alexandr Puzanov	Investigation and production enterprise TYRBOTEST Sverdlovskaya nab., 18 Saint-Peterburg Russia	+7 812 326 72 71	+7 812 326 72 95
Irina Puzanova	Investigation and production enterprise TYRBOTEST Sverdlovskaya nab., 18 Saint-Peterburg Russia	+7 812 326 72 71	+7 812 326 72 95
SWEDEN			
Carl Rollenhagen	SwedPower Box 527 16216 Stockholm Sweden carl.rollenhagen.swedpower.vattenfall.se	+46 87 397260	+46 87 396 900

Name	Address & E-mail	Telephone	Fax
USA			
Richard P. Coe	School of Business Studies The Richard Stockton College of NJ 118 East Wilmont Avenue Somers Point, New Jersey 08244 USA RPCoe@worldnet.att.net	609 927 3559	609 728 2696
Richard Brice	OAO Technology Solutions, Inc. Technical Interiors Division OAOT 2395 Pleasantdale Road, Suite 5 Atlanta, Georgia 30340 USA jkeller@oaot.com	770 840 0880	770 840 9685
IAEA			
M. Dusic (Scientific Secretary)	International Atomic Energy Agency Wagramer Strasse 5 P.O.Box 100 A-1400 Vienna, Austria E-mail: m.dusic@iaea.org	(+ 43 1) 2600 22522	43 1) 26007
A. Kossilov (Scientific Secretary)	International Atomic Energy Agency Wagramer Strasse 5 P.O.Box 100 A-1400 Vienna, Austria E-mail: A.Kossilov@iaea.org	(+ 43 1) 2600 22802	43 1) 26007

서지정보양식

수행기관보고서 번호	위탁기관보고서 번호	표준보고서 번호	INIS 주제코드
KAERI/TR-1456/2000	IAEA-J4-SP-1123		

제목/부제	원자력발전소 비정상 및 비상시 인간-기계 연계 기술
연구책임자 및 부서명	권 기춘 (MMIS 팀)
연구자 및 부서명	

출판지	대전	발행기관	한국원자력연구소	발행일	2000. 1. 10
페이지	224	도 표	있음(V), 없음( )	크 기	21x29.7 Cm

참고사항			
비밀여부	공개 (V), 대외비 ( ), __ 급 비밀	보고서종류	기술보고서
연구위탁기관			

초록 (15-20 줄내외)

원자력발전소는 인적오류에 의한 사고가 높은 비중을 차지하고 있으며, 따라서 인적오류를 줄이기 위한 인간-기계 연계의 향상에 노력을 기울이고 있다. 특히 사업자와 규제기관에서 많은 관심을 가지고 있다.
국제원자력기구(IAEA) 가 주관하고 한국원자력연구소와 한국전력기술주식회사가 주최한 "원자력발전소 비정상 및 비상시 인간-기계 연계 기술" 에 대한 전문가회의 (Specialists' Meeting)이 1999 년 10 월 26-28 일까지 한국원자력연구소에서 개최되었다. 이 회의에서는 9 개국에서 약 58 명의 전문가가 참석하여 "원자력발전소 비정상 및 비상시 인간-기계 연계 기술"에 대해서 현재의 개발동향 검토 및 미래의 개발방향에 대해서 토의하였다. 20 여편의 논문이 4 개의 세션으로 나누어 운전경험, 개발내용, 인허가 현안, 앞으로의 개발동향에 대해서 발표가 진행되었다.

주제명키워드 (10 단어 내외)

인간-기계 연계, 비정상 및 비상운전, 계측제어

BIBLIOGRAPHIC INFORMATION SHEET

Performing Org. Report No.	Sponsoring Org. Report No.	Standard Report No.	INIS Subject Code
KAERI/TR-1456/2000	IAEA-J4-SP-1123		

Title/Subtitle	Human-Machine Interface for Off normal and Emergency Situations in Nuclear Power Plants
Project Manager and Department	Kee-Choon Kwon (MMIS Team)
Researcher and Department	

Publication Place	Taejon	Publisher	KAERI	Publication Date	January 10, 2000
Page	224	Fig. & Tab.	YES(V), No( )	Size	21x29.7 Cm

Note	

Classified	Open (V), Restricted ( ), ___ Class Document	Report Type	Technical Report
Sponsoring Org.		Contract No.	

Abstract (15-20 Lines)

Many nuclear power plants (NPPs) have reported that a high percentage of all major failures in the plants are caused by human errors. Therefore, there has been much focus on elimination of human errors, enhancement of human performance, and general improvement of human machine interface (HMI). Both the utility management and the regulators are demanding improvement in this area.

The International Atomic Energy Agency (IAEA) Specialists' Meeting on "Human-Machine Interface for Off Normal and Emergency Situations in Nuclear Power Plants" was co-organized by the Korea Atomic Energy Research Institute (KAERI) and the Korea Power Engineering Company, INC (KOPEC), and took place in Taejon, Republic of Korea, 1999 October 26-28.

Fifty eight participants, representing nine member countries reviewed recent developments and discussed directions for future efforts in the Human-Machine Interface for Off Normal and Emergency Situations in NPPs. Twenty papers were presented, covering a wide spectrum of technical and scientific subjects including recent experience and benefits from Operational Experience with HMI, Development of HMI System, Licensing Issues for HMI and Future Development and Trends.

Subject Keywords (About 10 words)

Human-Machine Interface, Off Normal and Emergency Situation, I&C