원자력 플랜트의 개량형 경보시스템 개발 및 평가 사례

(Practical Development and Evaluation of Advanced Alarm System for Nuclear Power Plant)

장 귀 숙 †
(Gui Suk Jang)

요 약 개량형 경보시스템은 원자력 플랜트의 경보 기능을 구현하기 위하여 최신 디지털 기술들을 적용한다. 신호검증 및 선진 경보처리 기술들을 제공하는 디지털 신기술의 사용은 제어실 운전원 연계를 향상시킨다. 본 논문은 원자력 플랜트의 개량형 경보시스템의 설계 공정, 신뢰도 예측 도구를 이용한 시스템 신뢰도 및 가용도 향상 평가, 인간공학적 성능 관점의 설계 전략 그리고 검증설비를 이용한 성능 분석의 결과 등과 같은 실제적인 구현 사례를 소개한다.

키워드 : 개량형 경보시스템, 신뢰도 평가, 인간공학

Abstract The advanced Alarm System (AS) employs modern digital technology to implement the alarm functions of the NPP(Nuclear Power Plant). The use of modern digital technology can provide advanced alarm processing in which new algorithms such as a signal validation, advanced alarm processing logic and other features are applied to improve the control room man-machine interfaces. This paper will describe the design process of the AS of NPP, improving the system reliability and availability using the reliability prediction tool, design strategies regarding the human performance topics associated with a computer-based AS and the results of the performance analysis using a prototype of the AS.

Key words : advanced alarm system, evaluation of reliability, human factors engineering

1. Introduction

The AS(Alarm System) of an NPP(Nuclear Power Plant) is to assist the operator to monitor the systems and processes and to take the necessary actions required to preserve normal operating conditions. Therefore, an advanced AS must present meaningful information only, and must not flood the operator with miscellaneous data that he does not have to act upon. AS is a primarily digital alarm system employing advanced alarm process logics and a VDU(Visual Display Unit) based control and a display for the alarms. AS is a part of an overall MMIS(Man-Machine Interface System) information/monitoring system which is composed of an Information Processing System(IPS), an Alarm and Indication System(AIS) and a Large Display(LDP), used for normal plant operations and post accident monitoring. The information/monitoring system of MMIS provides necessary data to maintain the plant availability and to support the plant operation in an efficient and safe manner. AS is developed as an integrated information system of MMI according to HSI(Human-System Interface) guidelines and the information hierarchy of MMIS(Man Machine Interface System). (HSI is that part of the system through which personnel interact to perform their functions and tasks. Major HSIs include alarms, information display, controls and procedures.) Alarm and setpoints should be designed so that only parameters and conditions that fall outside of the normal and expected range that require operator

† 정 회 원 : 한국원자력연구소 MMIS 기술개발 선임연구원
gsjang@kaeri.re.kr
논문접수 : 2004년 11월 4일
심사완료 : 2006년 4월 21일

attention or action are in the alarm state. An illuminated alarm display device indicates a deviation from the normal plant conditions. The AS displays priority 1 and 2 alarms according to a separation of the status alarms for the components that do not need an operator's action. The design goal of a AS is to reduce operator information overload, to reduce the potential of human errors through MMI improvement and to improve the cost effectiveness by using common design guidelines for both the NSSS(Nuclear Steam Supply System) alarms and the BOP(Balance Of Plant) alarms of research reactor.

2. Design of AS

2.1 A Design Goal and Requirements of AS

The AS combines the annunciation and alarm functions in a single system. The role of AS is to provide the information necessary to safely shutdown the reactor under all plant conditions, to monitor the plant parameters approaching or exceeding the operating limits and to minimize the number of alarms, and the alarms are grouped and prioritized. The AS is designed according to the requirements of the control room alarm reliability of US NRC's SECY-93-087, Item II.T. It has been reported that the alarm system for the ALWR should meet the applicable EPRI requirements for redundancy, independence, and separation [1,2]. The redundant alarm systems should be provided. These redundant systems need not comply with the single failure criterion, but independence between the systems should be equivalent to that of the protection systems. The AS is based on a redundant architecture based on a dual concept. The redundant systems shall inherently minimize the consequence of a failure. Diversity shall allow a continued plant operation with a failure in any of the information hierarchy elements. To avoid a common mode failure of the alarms, the AS uses IPS in the MCR (Main Control Room) by means of a diverse mean of the alarms. And the diversity is accomplished by using both the IPS and the AS implemented with different hardware and software to independently calculate and display the same validated process parameters and alarm conditions. The IPS shall independently check the alarm output of the AS and any discrepancies. The capability for a AS testing during power operation shall be provided. The hardware and software for AS have surveillance and diagnostic test capabilities. Automatic on-line surveillance tests shall continuously check for selected system (hardware and/or software) malfunctions. The malfunctions shall be indicated through the alarm display. The AS maintains a physical separation and electrical isolation of the redundant alarm systems. Independence of the data communication is as follows;

- between redundant alarm systems
- between the AS and other information systems
- between the AS and the safety systems

AS is isolated from the safety systems using fiber optic cable to prevent against an electrical fault propagation. The H/W and S/W used in AS are qualified in accordance with the H/W qualification procedure and S/W qualification procedure for the MMIS.

2.2 Design Strategies of AS

2.2.1 Functions of the AS

Alarm functions of AS provide priority 1, priority 2, and some priority 3 alarms using validated parameter signals based on the priority criteria of the information hierarchy for MMIS. Alarm functions are presented in a manner which prioritizes them so that the operator's response can be based on importance or urgency. Alarm functions are designed to minimize the number of alarms that occur in plant emergencies. Alarm functions of the AS encompass alarm reduction and suppression functions. Alarm functions reduce the number of alarm tiles to minimize the occurrence of information overload using the following methods.

- combining similar alarms under a single alarm tile
- combining separate channel alarms of the same parameter under a single alarm tile
- single alarm tile with a priority display
- alarm tile provides priority 1 & 2 conditions only

Alarm functions of the AS reduce the nuisance alarms by using dead band and time delay and they use the following techniques to help the operation quickly correlate the impact of the alarm

on the plant safety or performance [6,7].

- alarms are arranged by system a group to achieve spatial dedication
- alarms based on plant mode
- alarms based on equipment operating status
- alarms prioritized into operational categories

AS alarms are displayed in accordance with the visual and audible code strategy of the alarm priority based on the HSI for MMIS. The AS alarms are designed to display spatially dedicated continuously visible alarms with VDU-based alarm tiles and alarm lists.

2.2.2 Display and Control Strategies of AS

Alarm statuses of the AS are provided with audible tones, alarm tiles and alarm lists. The alarm tiles provide a mean for the operator to acknowledge the alarms, request additional data on the alarms, and to reset the cleared alarms. The alarm control and display shall be designed using the HSI guidelines of the alarms.

1) Alarm tiles/ Alarm lists Interaction

The alarm tiles provide the operator with a menu to request additional information about the alarm. The alarm list displays pages which provide additional alarm information. For an incoming alarm, the alarm tile flashes and an audible tone is generated for a 1-second duration. By pushing the alarm tile the operator acknowledges the alarm and a more detailed description of the alarm is provided in the alarm lists. Since each alarm tile may represent more than one alarm there is a distinct description for each possible alarm.

2) Priority of Alarm

When alarms are displayed separately from the detailed information, the detailed alarm information display provides an indication of the priority and status of the alarm condition. The display of lower important alarms is overridden by the display of the alarms with a higher importance. For a non-spatially dedicated alarm presentation such as alarm lists, sufficient display area is provided for the simultaneous viewing of all the high priority alarms.

3) Display of Alarm Status

New, acknowledged, and cleared alarm states have unique presentations to support the operator's ability to rapidly distinguish them from the others. New alarms are indicated both by visual (e.g, flashing) and audible means. If the operator is not currently using the VDU where a new, unacknowledged alarm message appears, the alarm system notifies the operator that a new alarm is available, the priority of the alarm, and the location where the alarm can be found. After the operator has acknowledged an alarm (e.g., pressed the acknowledge button) the alarm display changes to a visually distinct acknowledged state and the alerting function (e.g., audible tone) should cease. If the operator is required to notice when an alarm clears (i.e., the parameter returns to the normal range from an abnormal range), the return to normal conditions should be indicated by visual and audible means. The ring-back, alerting the operator when a parameter returns to normal, is not required for all the alarms but it is required when it is important that the operator knows immediately when the deviation has cleared, or when the deviation is not expected to clear for some time. Such cleared alarms provide a positive indication by initiating audible and visual signals. A technique that may be employed includes: a special flash rate(on half the normal flash rate to allow for discrimination).

4) Visual Coding Method

A flashing visual signal is included for important alarms. Flash rates should be from three to five flashes per second with approximately equal on and off times. For a display, such as lighted alarm tiles, the brightest state should be no more than 100% brighter than the inactivated state and a dim state should be at least 10 % brighter than the inactivated state.

5) Audible Coding Method

Distinct sounds/tones are provided in the MCR to indicate the following alarm information.

- Momentary alarm tone for new priority 1, 2 and 3 alarms
- Alarm reminder tone for priority 1, 2, and 3 new or cleared conditions (periodic every minute while unacknowledged)
- Cleared tone for cleared priority 1,2 and 3 alarms (upon becoming cleared)

Tone A and B is present respectively for 1 and

0.5 seconds. Tone B is present for 0.5 seconds and will repeat periodically, one every minute, until all new or cleared alarms are acknowledged. The signal intensity of those sounds is within the adjustable specified limits. Alarm tones can be suppressed in a manner that an important alarm tone occurs and the other tones are suppressed when several alarms occur simultaneously. Order of the important alarm tone is as follows;

- new priority 1 alarm, new priority 2 alarm, new priority 3 alarm, reminder tone, cleared tone

6) Organization of Alarms

Alarms within a display are grouped by function, system, or other logical organizations. The depth of the display level is 2. System/functional group is clearly delineated and labeled such that the operating crew can easily determine which system has alarms and those that have not yet cleared and which system is affected by a particular incoming alarm. Lists of the alarm messages are segregated by alarm priority with the highest priority alarms being listed first. In addition to priority grouping, operators should be given the capability to group the alarm message according to the relevant operationally categories, such as function, chronological order, and status(unacknowledged, acknowledged/active, cleared).

7) Alarm Control

The alarm control provided by the AS is used by the operator to perform the following control functions :

- Silence : The primary purpose of the auditory signal is to alert the operator to a new alarm. Auditory signals should be silenced manually by the operators unless they interface with other more critical operator actions.
- Acknowledge : An alarm acknowledgement control terminates the flashing of an alarm and continues at a steady illumination until the alarm is cleared. Acknowledgement is possible only from locations where the alarm message can be read.
- Reset : The reset control should place the alarm system in an unalarmed state after an alarm has cleared. Note that for some alarms may have an automatic reset, it is not necessary for operators to specifically know the reset condition. Manual reset sequence should be used where it is important to explicitly inform operators of a cleared condition that had once been deviant. An automatic reset sequence should be available where operators have to respond to numerous alarms or where it is essential to quickly reset the system.

AS follows the ring-back alarm sequences of KEPIC EMD2100. A sequence table of KEPIC EMD2100 describes the sequence actions and sequence states by lines of statements arranged in columns. They sometimes do not show all the aspects of the sequence, e.g, what happens when a push button is pushed out of sequence. Therefore, sequence diagrams of KEPIC EMD2100 are also included to allow the sequence to be completely defined. A sequence diagram has a block for each sequence state arranged to describe the sequence from the normal state through to the other sequence states and back to the normal state again. The normal alarm sequence and ring-back sequence may be distinguished by different flashing rates or by different audible tones. A manual reset is required to return to the normal state.

8) Auxiliary Sequence Options

The first out alarm feature is used when one alarm can trigger another alarm and some method is needed to determine which alarm tripped first. The first out alarm will be distinguished from subsequent alarms by a difference in the flashing rate. A first out reset push button is included to reset the first out indication. Test controls are available to initiate operational test conditions for all the essential aspects of the alarm system (including processing logic, audible alarms, and visual alarm indications). Periodic testing of the AS is required and controlled by administrative procedures.

2.3 Configuration of the AS

AS is a part of the AIS (Alarm and Indication System) for NPP. Equipment of the AS consists of the alarm processor 1, 2, the alarm test device 1, 2, the alarm display processor 1, 2, and alarm display device 1, 2. Alarm equipment is connected via the safety and non safety networks (subnet A,B,C,D

and subnet X,Y). The AS provides a high availability (99%) to support continuous plant operations. So, the AS shall be based on a redundant architecture. The sufficient redundancy of the AS is provided to allow for hardware maintenance without taking the entire system off-line. On line self-checks of the system health are periodically performed to allow for an early identification of the faults. AS is both flexible and expandable to adapt to the changing needs of the utility throughout the life of the plant. The AS provides extensive, reliable data communications to support the required system information exchange. Isolation is provided when a communication extends to the integrity of the transmitted data.

3. Development Process

The steps for the AS design process are described in Table 1, and the interface of the tasks is described in Figure 1. AS is developed and evaluated in accordance with the human factors engineering program plan (HFEPP), equipment qualification plan (EQP) for commercial products, and the S/W qualification assurance plan (SQAP) for MMIS. Also during the basic system design, an overall design process of AS is developed based on the human factor engineering design methodology,

Table 1 Design Process of the AS

	Task Description	Input Related to Task
1	Definition Role & Goal	-Analysis Result of HFEPP -Design Bases of MMIS -Information Hierarchy for MMIS
2	Decision of Alarm Function	-Analysis of Code & Standard -Analysis of Design Req't
3	Prep. of Alarm Inventory	-DR for I&C (NSSS, BOP) -P&ID, C&ID, CLD -System Design Document -Information for Safety Analysis
4	Detail Design of AS -Alarm Generation -Alarm Structuring -Alarm Presentation	-Human System Interface Guideline -Alarm Design Guideline
5	Decision Development Strategy of AS	-Procedure for H/W Development -Qualification Activity -Procedure for S/W Development -Reliability Prediction and Analysis
6	System Design for Alarm -System Req't -Interface Req't -System Spec.	-System Functions, Design Req't -Environment and Electrical Req't -Information of Interface Systems -H/W and S/W Requirement -Operation, Test and Maintenance Req't
7	Component Design for H/W& S/W Spec.	-Information of Detail H/W Spec. -Structure Analysis of S/W Req's

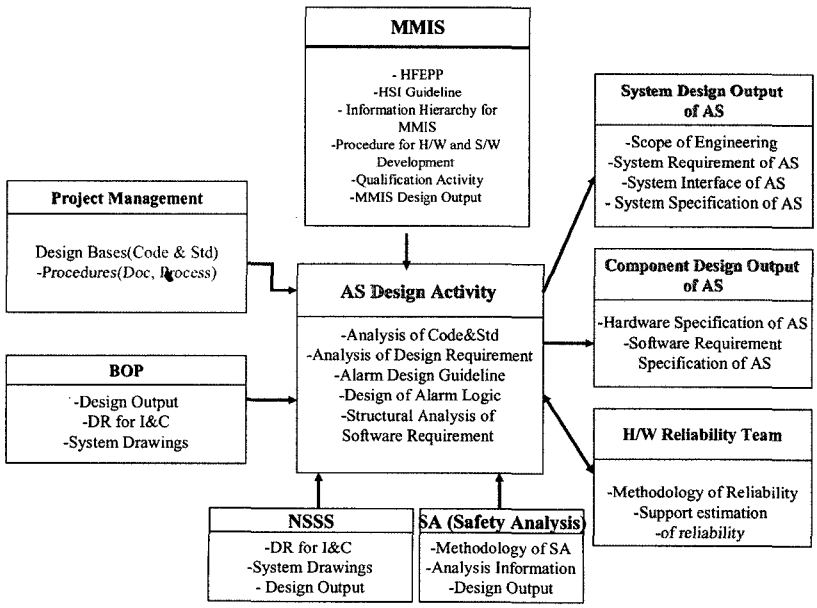

Fig. 1 Development Process of the AS

and a prototype is developed to verify the design and to evaluate the system's performance. Especially the software development of the AS is established on an integrated development plan through a software life cycle. The CASE tool as a software design assistance can enhance the productivity and reliability problem of the software with the automation of the program implementation, maintenance, analysis and design. Software engineering using CASE provides an interactive development environment in proportion to the use of the fast response function, exclusive use of the development resources, and the pre-control function of the faults.

4. Result of Performance Analysis using the Prototype of AS

4.1 Information for the Prototype of the AS

The prototype of the AS was developed to verify not only the major system functions and design requirements but the technologies which have not yet been implemented in conventional power plants. Table 2 shows the constraints for the prototype of the AS. The development environment information of the hardware and software for the prototype is as in Table 3. Figure 3 shows the board block diagram for the alarm processor board. Table 4 shows the memory information of the alarm processor board.

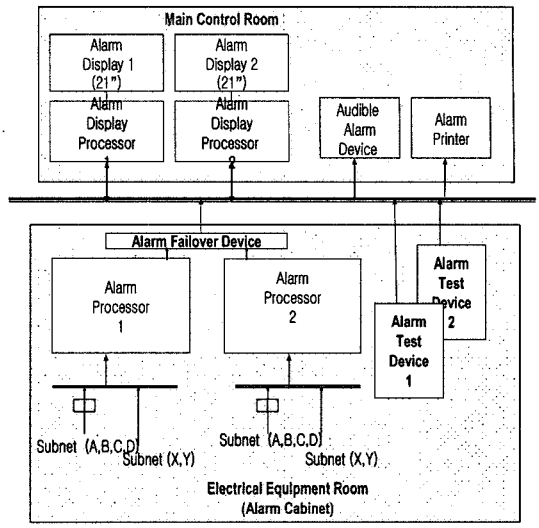

Fig. 2 Configuration of AS

Table 2 Constraints of Prototype of AS

Item	Constraints
Requirements	Apply Code & Standard Conformance
Selection for H/W and S/W	Set up Selection Criteria of H/W & S/W Except Qualification Requirements of H/W
Redundancy	Single Configuration
Communication	Ethernet is temporarily used (communication under design)
Alarm processing	Alarm Reduction for Partial Alarms Alarm Suppression for Partial Alarms
Alarm control	Ring back Alarm Control based VDU
Alarm display	Hyperbolic Visualization Techniques

Table 3 Development Environment Information of the Prototype

Item	H/W & S/W	Specification
Alarm Processor	Process Board	- Processor : TI DSP(TMS320C40) - Memory : Local and Global Memory EPROM, Flash Memory
	System Bus	VME BUS Controller : VIC608A
	Control Logic	7000A (ALTER)
Test Device	Personal Computer	- Pentium III 500MHz, Serial Port to Communication with Alarm Processor - 100/10-Base T
	DSP Board S/W Devl.	- Cross Development Environment - TMS320C40 Assembler, C Compiler, Linker - PC based DSP Board Emulation S/W : Board Support Library, Download DSP Program, Test of DSP board
Sub Rack	Standard(19")	- VME Bus Backplane - 3U Single Height
Alarm Display	Flat Panel PC	- Pentium III 500MHz, 512KB Cache, 384MB memory, 100/10-Base T - TFT Color, 64K color - Touch type : Analog Resistive
	S/W Devl.	Using QNX 4 OS and Photon MicroGUI

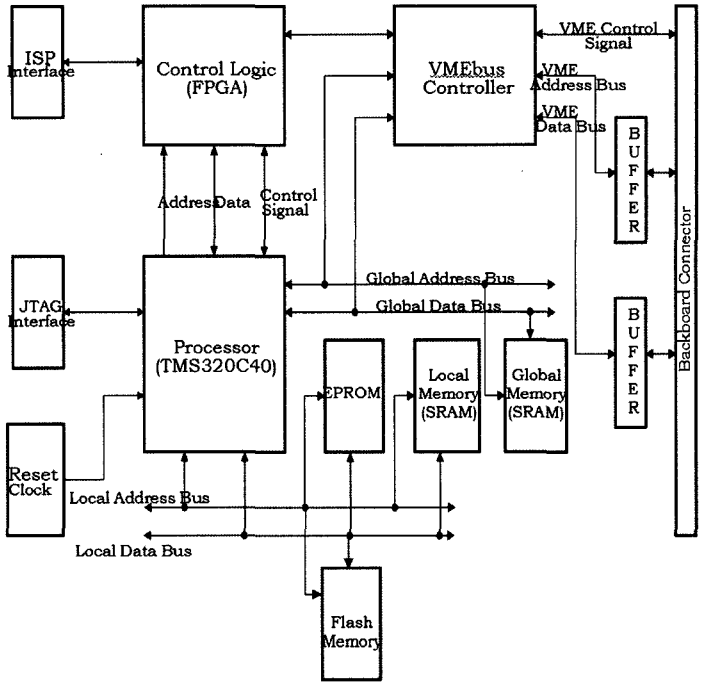

Fig. 3 Board Block Diagram for Alarm Processor Board

Table 4 Memory Information of Alarm Processor Board

Memory Type	Item	Specification
Local Memory	Model Number	K6R4016VIC - TC12
	Size	256K × 16bit × 2
	Read cycle Time	12ns
	Write Cycle Time	12ns
	Function	Application Software of Alarm Processing for Runtime
Global Memory	Model Number	K6R4016VIC - TC12
	Size	256K × 16bit × 2
	Read cycle Time	12ns
	Write Cycle Time	12ns
	Function	Data Operation of Alarm Processing for Runtime
Flash Memory	Model Number	AM29F080B - 90EC
	Size	1Mbypte × 8bit ×1
	Read cycle Time	90ns
	Write Cycle Time	90ns
	Initialization Count	Minimum 1,000,000 Program/Erase Cycle per Sector
	Gate-Type	Nor - Gate
	Function	Database Storage and Data Backup
Memory Type	Item	Specification
EPROM	Model Number	TMS27C256 - 15
	Size	32KB × 8bit × 1
	Read cycle Time	150 ns
	Function	Boot Loader and Application S/W of Alarm Processing

4.2 S/W Requirement Analysis and Design of the Prototype Using a CASE Tool

The S/W was developed with a top-down structure design approach using TeamWork (CASE

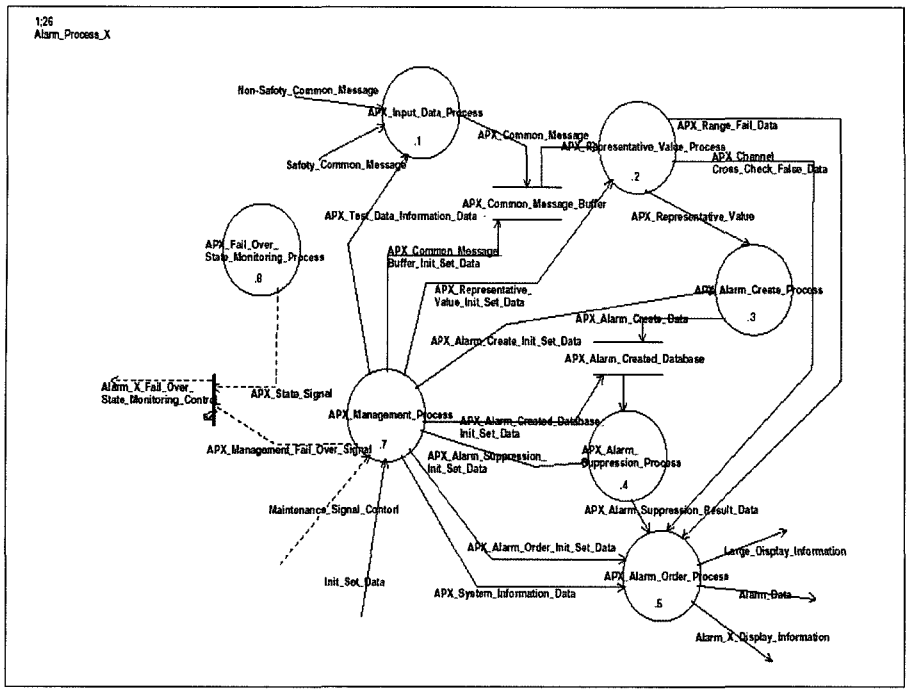

Fig. 4 Data Flow Diagram for AS

tool). The S/W deign used a hierarchical design structure and principles of the modular design with coherence and cohesive modules to reduce the complexity of the verification and validation. High level language was mainly used and assembly language was used only where sufficient performance can not be achieved through use of a high level language or where it is justified based on the the requirements. Figure 4 shows the DFD(Data Flow Diagram) of the S/W requirment analysis for the prototype of the AS.

4.2.1 APX_Input_Data_Prcoess

The module periodically collects the digitized data of an analog and contact type through a safety and non-safety network.

4.2.2 APX_Representative_Value

The module executes the logic to determine a single value that can be representative of a given parameter which is being sensed by multiple sensors. As a port of the validation algorothm, any sensor(s) which fails a cross channel deviation comparison is secluded from the valid parameter calculation.

4.2.3 APX_Alarm_Create_Process

Upon detection of the alarm conditions, the module processes the alarm processing alogorithm based on the validated variables to reduce the nuisance alarms efficiently and to allow the opeator to best focus his attentions. The applicable alarm logics are the plant operating mode dependency alarm with different setpoints, the equipment status dependency alarm, the deadband and the time delay.

4.2.4 APX_Alarm Suppression_Process

Irrelevant or unnecessary alarms are eliminated and less important alarms are suppressed. The applicable alarm suppression logics are cause-consequence processing and multi-setpoint relationships. And First-out procesing is provided to support the operators in determining the initiating cause of a reactor or trubine trip in the alarm system. By suppressing the minor alarms for a period of time after a reactor trip, the operator's attention would be directed towards the major problem when multiple alarms are present.

4.2.5 APX_Alarm_Order_Process

Alarms are prioritized by their importance to plant safety and its operation. The model indicates the relative importance of the alarms based on a

predefined set of conditions and relieves the operator of this time-consuming task when a major event is taking place. The alarm prioritization scheme depends on the alarm categorization stragety based on the information hierarchy for the MMIS.

4.2.6 APX_Management_Process

The module is provided to allow for the modification to the existing software and to minimize the mean-time-to-repair by generating meaningful error messages. The module recognizes a power failure and is capable of an automatic restart upon power restoration. The cold start software modle is executed when initially energizing the prototype hardware. The warm restart module attempts the continuation of the program without the hardware initialization.

4.2.7 APX_Fail_Over_State_Monitoring_Process

: not implemented

4.3 Result of the Functional and Performance Test of the Prototype for the AS

The functional and performace test of the prototype for the AS was done based on the test plan and test procedure. Table 5 shows each test item and the results of the alarm processor and alarm display. We can confirm the suitability of the design requirements of the AS through prototyping.

5. Relaibility Prediction and Analysis of the AS using a Prototype

The AS should be designed for an operational availability goal of 99%. The MTBF (Mean Time Between Failure) of the AS is more than 10,000 hours. Equipment that is easily accessible is assumed to be repaired within a short time period after the failure is detected. The MTBF should be confirmed by a reliability analysis based on the failure rate of the components.

5.1 Reliability Prediction and Analysis Tool (Relax)

A primary component of the reliability analysis is referred to as the failure rate, or the number of failures expected during a certain period of time. Calculation of the equipment failure rate, and the related MTBF of the prototype, is the basis of the Relax Reliability Prediction Software. Relax performs the reliability predictions and analyses on the electrical, electronic, mechanical, and electro-mechanical equipment. The Relax reliability prediction software is available based on various standards, including Telcordia (Bellcire), MIL-HDBK-217, CNET 93 and HRD5 [4].

5.2 Prediction of the Reliability

Electronic systems involve the utilization of very large numbers of devices which are very similar. It is difficult to test for the electronic component defects that do not immediately affect the performance. Very close attention must be paid to the electronics part reliability. The AS design involved a reliability team. A reliability prediction is the analysis of the parts and components in an effort to predict the rate at which an assembly or system will fail. The basis of the analysis is generally a

Table 5 Test Items and Test Results

Test Type	Test Items	Test Method
Static analysis	Structure Analysis - to confirm operation of conditional branch - to confirm to limit value - to confirm finish condition of subroutine	Test of individual software module using test tool (McCabe)
Review S/W Design Output using TeamWork	- Review of Software Requirement Specification (Context Diagram, Data Flow Diagram, DD) - Review of Software Design Specification (Structure Chart, Decision Table, Event Transition Table)	Independent review using checklist of requirement
Functional Test	- Alarm Processing, Display, Control - Analysis of Time Response	Using test case
Performance Test	- Analysis Memory Capacity - Analysis Response Time - Analysis Suitability of Memory Operation according to Operation Mode (initial, turn on., turn off, blackout)	Based information through and timing analysis using the worst test case

reliability prediction model. Reliability prediction models offer standard equations to calculate the failure rate of the components based on the component data and parameters. These parameters include the environment, temperature, quality and stress. When individual failure rates for the components are established, a simple summation of the component failure rates provides the failure rate for the higher level assemblies and systems.

5.3 MIL-HDBK-217 Prediction Method

MIL-HDBK-217 was an original standard for the reliability predictions. It was designed to provide reliability math models for nearly every conceivable type of electronic device. It is used by both commercial companies and the defense industry, and is accepted and known worldwide. MIL-HDBK-217 includes the ability to perform a parts count analysis or a part stress analysis. A parts count analysis is not as detailed as a part stress analysis, and is normally used early in a design when detailed information is not available, or a rough estimate of the failure rate is all that is required. A part stress analysis takes into account more detailed information regarding the components, and, therefore, offers a more accurate estimate of the failure rate. The parts stress analysis method requires a significant amount of design detail. Many of the details were not available in the early design stages of the AS.

5.4 Parts Count Reliability Method

The parts count reliability method can be used in the early design stage when detailed data is not available. The parts count reliability method is used for the generic part type, for the quality factor and the environmental factor. And the following information is required; generic part types (including complexity for microcircuits) and quantities, part quality levels, and the equipment environment. Equation of the parts count method is as follows.

$$\lambda_{EQUIP} = \sum_{i=1}^{i=n} N_i(\lambda_g \pi_Q)_i$$

λ_{EQUIP} = Total requirement failure (Filures/10^6 Hours)

λ_g = Generic failure rate for ith generic part (Filures/10^6 Hours)

π_Q = Quality factor for the i^{th} generic part

N_i = Quantity of the i^{th} generic part

N = Number of different generic part categories in the equipment

The prototype of the AS selected the parts count reliability method for its improvement by showing the highest contributors to a failure. Table 6 shows the results of the reliability prediction of a alarm processor board for the prototype. The total equipment failure rate of the alarm processor board is 0.8205. The need for a redundant or back-up system may be determined with the aid of reliability predictions. Also the maintenance strategy can make use of the relative probability of a failure's location, based on the predictions, to minimize the downtime. Reliability predictions are also used to evaluate the probabilities of the failure events described in the failure modes, effects and criticality analysis.

Table 6 Result of Reliability Prediction of an Alarm Processor Board for Prototype

(Condition: Quantity = 1, Quality Level = Commercial, Environment = Ground fixed, Uncontolled, Temp = 30)

Part Number(*)	Parts Count
TMS320C40FL60 (TMS320C40)	0.0609
VIC068A-NC (VIC068A)	0.0000
AM29F080B-90EC	0.1832
27C256-15 (27C256)	0.2443
K6R4016VIC-TC12 (K6R4016VIC-C)	0.1131
EMP7128STC100-15 (EMP7128EQI100-20)	0.2198
Total Failure Rate	0.8205

*If there is not component data in Relax, a similar component data is used for prediction.

5.5 Improving System Reliability and Availability Using the Relax RBD

There are several techniques that we can employ to improve the reliability, and/or availability of the AS design. Three common techniques that might be used are the parallel redundancy, standby redundancy, and spares. By using Relax's Reliability Block Diagram (RBD) tool, the effects of these methods can be investigated when determining if any of these techniques should be used before any

design changes. Since one of the main purposes of the RBD is to calculate the reliability and availability of a system based on the redundancies, it is useful to only analyze the AS at the level that includes redundancies. A reliability prediction model assumed that the configuration of the system was a simple one. As a system configuration becomes more complex, more complex calculation methods are required to calculate values like the failure rate, MTBF, reliability, and availability. The Relax RBD was used to calculate complex redundant systems that cannot be computed using the Relax Reliability Prediction portion of the program alone.

5.6 Result of the Analysis of the Reliability using Relax RBD

Table 7 shows the failure rate of a component of an alarm processor board for the prototype. Table 8 shows the various parameters and variables chosen for the analysis, as well as the availability, reliability and failure rate at specific time intervals. Standby redundancy is more effective than the parallel redundancy because the unit/junctions are not always operating. The results of the standby redundancy show its suitability for the MTBF and the availability and reliability requirements of the AS through the prototype.

6. Conclusion

The AS design has been attempted to resolve the problem that existed in the alarm system of the conventional plants and support the MMIS. To achieve this, we introduced advanced alarm processing methods based on a digital system, and a new display method, and an alarm control method based VDU (Visual Display Unit). The AS was designed as an integral part of the control room design and plant operation. It was therefore recognized that only good established design processes should be used. For optimizing the design and to meet the current licensing issues, the evaluation activities for the AS design were performed in accordance with the V/V and through the prototype development. This paper described the design process and strategies of the AS, results of the functional and performance tests using the prototype and the improvement of the system's reliability and availability by using the reliability prediction and analysis tools. In conclusion, the design of the AS should be continuously revised

Table 7 Failure Rate of Component of an Alarm Processor Board for Prototype (N: count, FR : Failure Rate, CFR : Combination of FR)

Part Number	Function	FR	N	CFR
TMS320C40FL60 (TMS320C40)	DSP Processor	0.01528	1	0.015281
VIC068A-NC (VIC068A)	VME Interface Controller	0.00312	1	0.003120
AM29F080B-90EC	Flash Memory	0.52425	1	0.52425
27C256-15 (27C256)	EEPROM	0.00571	1	0.005715
K6R4016V1C-TC12 (K6R4016V1V-C)	SRAM	0.00571	4	0.22860
EMP7128STC100-15 (EPM7128EQI100-20)	FPGA	0.659031	1	0.659031

Table 8 Result of Reliability Analysis

Hour	Reliability		Failure Rate		Availability	
	Parallel	Standby	Parallel	Standby	Parallel	Standby
0	1.00000	1.000000	0.000000	0.042247	1.000000	1.000000
20000	0.993435	0.995849	0.633273	0.365093	1.000000	1.000000
40000	0.975826	0.985806	1.136928	0.641669	1.000000	1.000000
60000	0.949867	0.970853	1.545742	0.881257	1.000000	1.000000
80000	0.917754	0.951851	1.883097	1.090811	1.000000	1.000000
100000	0.881270	0.929556	2.165296	1.275647	1.000000	1.000000
120000	0.841854	0.904625	2.404056	1.439893	1.000000	1.000000
140000	0.800658	0.877631	2.608012	1.586809	1.000000	1.000000
160000	0.758600	0.849074	2.783674	1.719000	1.000000	1.000000
180000	0.716402	0.819382	2.936038	1.838575	1.000000	1.000000
200000	0.674628	0.788928	3.069005	1.947256	0.999000	1.000000

for the whole process of the detailed design, to complement the detailed requirements.

참 고 문 헌

[1] NREG 0800, Section 7.5, Standard Review Plan.
[2] Staff Requirements Memorandum on SECY-93-087, Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs.
[3] KEPIC EMD 2100, Design and Control Sequences of Alarm, 2000.
[4] Relax Reliability Block Diagram, Relax Software.
[5] Cheol Kwon Lee, Seop Hur, Development of a New Indicator and Alarm System in NPPs, ANS, 1996.
[6] NUREG/CR-6105, Human Factors Engineering Guidance for the Review of Advanced Alarm Systems.
[7] NUREG 0700, Rev.02, Human-System Interface Design Review Guidelines.

장 귀 숙
1990년 영남대학교 전산공학과 학사. 1992년 경북대학교 컴퓨터공학과 석사. 1992년~현재 한국원자력연구소 선임연구원
관심분야는 실시간 데이타베이스, 실시간 시스템, 원자력 감시시스템 설계