Proceedings of the Korean Nuclear Society Autumn Meeting
Seoul, Korea, October 1995

Safety Review Experience of Computerized Logic System for YGN 3 and 4

Won Young Yun, Dai Il Kim, Jung Soo Koh, Bok Ryul Kim, Sung Hun Oh, and Jang Hyun Lim

Korea Institute of Nuclear Safety

Abstract

This article presents safety review experience of microprocessor-based Interposing Logic System(ILS) of Engineering Safety Feature Actuation System(ESFAS). The ILS is the first application of computerized logic design to safety system in Korean nuclear power plants without verification of the system reliability by proven technology concept. As a result of evaluation for the ILS, Korea Institute of Nuclear Safety(KINS) concluded that the microprocessor-based ILS is not acceptable in some features detailed enough to defend against software common mode failures(CMF). Therefore, we required licensee to install hardwired interlock signal configuration and a Hardwired Backup Panel to control safety-related equipment. We believe that the microprocessor-based ILS with the hardwired backup panel and inter-connection of interlock signal by hardwired configuration will improve the plant safety.

1. Introduction

The Yonggwang nuclear 3 and 4 (YGN 3&4) are 2-loop type pressurized water reactors provided by ABB Combustion Engineering with an electrical output of 1050 MWe per each unit. These units were constructed in the late 1989 and the commercial operation of YGN 4 is scheduled for March, 1996. The NSSS design for YGN 3&4 is an application of ABB-CE's standard system 80 design. The instrumentation and control system design in YGN 3&4, however, incorporates the evolutionary feature of the system 80 design such as computerized logic design in order to enhance the operability and maintainability of the plant. The ILS is a fully integrated microprocessor-based control system to generate the suitable output signal to operate the plant equipments such as motors, valves and other field devices including safety-related Engineered Safety Features(ESF) actuation

components. The ILS was developed by Forney International Inc. with the AFS-1000 System. From a regulatory point of view, the ILS is the first application of computerized logic design to safety system in Korean nuclear power plants without verification of the system reliability by proven technology concept. To this concern, this paper presents the design characteristics and the safety review experiences and inspection activities related to the YGN 3&4 ILS design.

2. Computerized Logic System Descriptions

2.1 System Configuration [1] [2]

The basic building block of the ILS is a standardized board rack assembly capable of housing up to five single-board computer boards and their associated I/O buffer boards. Each field device is an independent subsystem with its own dedicated control board as shown in Fig. 1(above). The ILS hardware design can be classified as the I/O buffer board, central processing unit (CPU), memories and data communication buses. Specifically designed on-board functions include field-coil continuity monitoring, control-power monitoring, control-power to logic-power conversion for non-reversing motor starter field devices, and local-control logic-bypass switches on board I/O boards. Thus, the ILS control system architecture accommodates a wide variety of functional I/Os, operator interfaces, and system configurations.

For the communication between the independent ILS trains, fiber-optic communication links are provided shown in Fig. 1(below). In all trains, redundant masters which have three links are provided, and each master has three links. The links both between the pair (trains AB and AE/trains AB and CE) and between related-pair (trains BB and BE/trains BB and DE) have maintenance subsystem interfacing capability. This means that the communication links can transmit the maintenance data. If the maintenance subsystem is plugged into AB, it can monitor the status in AE or CE through either of the links from AB to AE or from AB to CE. Likewise, if the maintenance subsystem is plugged into BB; it can monitor the status in BE or DE through either of the links from BB to BE or from BB to DE.

2.2 Software Programing and Operational Characteristics

The logic functions of the ILS are programmed on EPROM. The address table ties all logic functions together for a specific application. This method requires no programming language knowledge because the logic flow chart is the definitive program document. Program changes can be made by reading the functional logic drawing. Identical logic function of EPROMs can be used in different applications by altering the address table EPROMs. The target ILS software is written in Intel 8085 assembly language using top-down modular design techniques. The program is assembled, linked, and placed in an EPROM. Another EPROM containing the patch program are placed on main board. When the board is turned on, the code inside that application program is executed. While the applications program is being executed, it looks at the patch panel and performs its intended function with the patch panel. The applications program cannot be modified in the field. However, the EPROM that contains the patch-panel program can be modified in the field using the maintenance system.

3. Safety Review Experience and Results

We reviewed the ILS design in view of the safety based on many reference materials, such as regulatory codes, technical standard, design guidelines etc. The safety review scope of the ILS consists of general items, equipment qualification, isolation and interaction between 1E and non-1E, ground, power, testability, defense-in-depth diversity and factory testing. General items include functional requirement, independence of V/V organization, review of V/V program, configuration management, and evaluation of software development process and documentation. The detailed safety review activities can be explained as follows:

- Following the code development
- Examining the vendor/licensee interface and feedback process
- Reviewing software problem/error reports and resulting corrections
- Comparing the V/V process to ANSI/IEEE ANS-7-4.3.2-1982
- Interviewing personnel involved in the process
- Verifying the independence of the software verifiers
- Reviewing the development of the functional requirements and subsequent software development documents
- Reviewing software life-cycle and future vendor/licensee interface
- Reviewing the verification and validation(V/V) results
- Thread walk-through included physical configuration audit, factory test audit and site-test audit

According to above procedure and review items, we required the very comprehensive and detailed V/V work and related materials to ensure high quality of the ILS. In relation with this regard, we visited the manufacturer site to audit their activities and issued an extensive set of questions to the manufacturer in order to obtain confirmation and commitment to software V/V activities and a firm software configuration management program. And also we required submittal of various design documentations such as technical source code listings, integration/implementation plans, and V/V reports etc.. Additionally, we requested the licensee to demonstrate that there is sufficient defence against CMF of the ILS for all of the analyzed YGN 3/4 plant transients and accidents. Specifically, main concern of our review was concentrated on the possibility of CMF through programming error introduced into the software. To deal with this special susceptibility to CMF, we proposed to licensee two regulatory requirements as follows.

Firstly, in the case of YGN 3 & 4, the types of interlock signals consist of same loop, loop to loop within the same train and loop to loop within the different train. The number of interlock signals is shown in table 1.

It is data sharing that forms the bases for many of the advantages of digital computer technology over analog technology. However, this data sharing in digital system raise a critical safety issue with respect to the reliability of I&C systems. The root cause of this issue is that the use of shared data base and processing equipment may result in

Table 1: The number of interlock signal

Type Train	Train A(Ea)	Train B(Ea)
Same Loop	40	30
Loop to Loop Same Train	48	47
Loop to Loop Diff. Train	29	31

a design that has the potential to propagate a CMF of redundant equipment. That is, the consequence of a CMF resulted from data sharing can bring out a complete a loss of defense in depth design concept. In these points of view, data sharing in communication network in the ILS should be minimized in microprocessor-based digital system. Therefore, transmission method of interlock signals between loops was the great concern in the YGN 3&4 licensing review process: Transmission of interlock signal is controlled by master logic controller in the case of YGN 3&4. Thus, for the system configuration of communication network, we required that interlock signals of between loops should be designed by hardwired logic under the concept of no logic circuit sharing and dedicated microprocessor. This decision is based on that the hardwired design will enhance the system safety by reducing the possibility of the CMF. As a result, all of interlock signals were changed by hardwired configuration in YGN 3&4 ILS. After the hardwired connection of the interlock signals, we inspected whether response time meets allowable criteria between loops of interlock signals. We verified that the response time was to be within the allowable response time.

Secondly, through the evaluation of submitted manufacture documentations, we concluded that the microprocessor-based ILS had not reflected some design features detailed enough to defend against software's CMFs. Defense-in-depth had been considered to be a combination of system and intrasystem diversity, redundancy, performance, and reliability with the goal of achieving a high degree of safety and compensating for safety system weakness. Defense-in-Depth and CMF concepts appear in varying regulatory contexts including 10 CFR part 50, GDC 22, IEEE-603-1980, IEEE-379-1977 endorsed by Regulatory Guide 1.53 and SECY-93-087. We reviewed the specific software CMF to the ILS in YGN 3&4 applications. It is affirmatively considered in safety review that the characteristics of ILS architecture uses dedicated microprocessor system in each components control. Therefore, a failure of a certain component control loop would not result in the loss of all function. So, the remaining redundant channels are still avaliable if a software CMF is not postulated. Licensee provided extensive materials on the reliability of the ILS and comparison to the existing Solid State Interposing Logic System(SSILS). We agreed with licensee and A/E that the hardware of ILS is at least as reliable. But the software CMF concerns is still potential issue in reviewing safety of ILS. For the transients and accidents of YGN 3/4, we considered that a set of safety-grade displays and controls shall be provided for manual actuations independent of the ILS that are critical safety functions and monitoring of parameters. This back-up systems shall be independent and diverse from the ILS. We believes that this diverse backup actuation system meets the safety analysis requirements if a CMF of ILS is assumed. These additional backup design changes increase the level of system defense-in-depth and may improve some of the

assumptions used in probabilistic risk and equipment failure analyses.

As a result, we required licensee to install Hardwired Backup Panel to control safety-related equipment. Hardwired Backup Panel is to ensure hot shutdown of the plant using train B, when the CMF occurs to the ILS. Parameters installed in Hardwired Backup Panel were carefully selected by evaluating operation procedure and Parameters/systems of 35 were controlled in Hardwired Backup Panel. We also verified that the hardwired backup panel has the capability to shutdown the reactor in train B during the performance inspection period.

4. Conclusions

In relation to the licensing review of safety related software system design, the major safety issues are arising from the complexity of the software design process. To overcome this concern, various kinds of effort have been performed to develop the technical standards and design guidelines recently. However, because of the inherent design features of software programming, it is very difficult to establish the fixed regulatory rules, practically. The introduction of microprocessor-based ILS into the safety-related systems design was the first time in Korea. Thus, we required licensee to submit design document and operating experience related to software programming and hardware qualification tests, including EMI and surge withstand capability for ILS design. Based on the evaluation of those documentations, We concluded that the microprocessor-based ILS was not acceptable in some features detailed enough to defend against software CMFs. Therefore, we required licensee to install a Hardwired Backup Panel and transmission of interlock signals by hardwired configuration. Finally, after verifying the operational safety of ILS through the safety inspection.

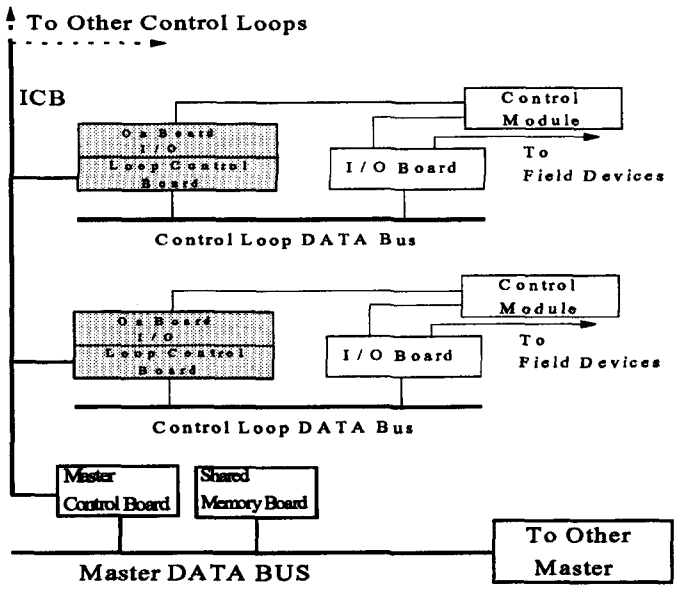
We approved the ILS system for YGN 3&4 nuclear power plants in the operating license stage. We believe that the microprocessor-based ILS system with the hardwired backup panel and inter-connection of interlock signal by hardwired configuration will improve the plant safety.

References

[1] Yonggwang Units 3&4, "Final Safety Analysis Report", Vol. 1, Korea Electric Power Corporation.

[2] Technical Manual, "Forney Interposing Logic System", Vol. 1, October 1992.

[3] D. R. Wallace,etal, " Control and Instrumentation", Nuclear Safety Vol. 35, No. 1, 1994.



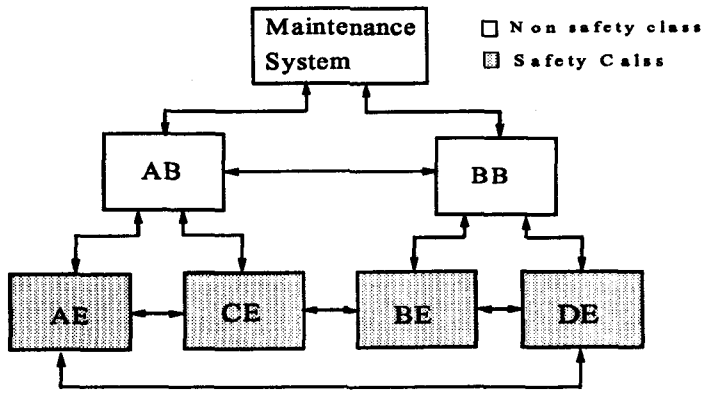


Fig.1: ILS block diagram(above) and Communication Network(below)