EXPERIENCE AND REGULATORY ACTIVITIES ON ADVANCED INSTRUMENTATION AND CONTROL SYSTEMS APPLIED TO NUCLEAR POWER PLANTS IN KOREA

Presented at

IAEA Advisory Group Meeting
on
Advanced Control Systems to Improve Nuclear Power Plant
Reliability and Efficiency
Vienna Austria, March 13 - 17, 1995

by
Bok-Ryul KIM

KOREA INSTITUTE OF NUCLEAR SAFETY
INSTRUMENTATION & CONTROL GROUP

ABSTRACT

This paper describes the status for applying microprocessor-based systems to nuclear power plants in Korea and the regulatory activities performed by Korea Institute of Nuclear Safety (KINS). And this presents the development of safety and regulatory technology for advanced I&C systems that has been carried out as a part of the next generation reactor development program in Korea.

1. INTRODUCTION

There are two types of nuclear power plants under construction with microprocessor-based I&C systems in Korea. One is Yonggwang nuclear power plant, units 3 and 4 that are 2-loop pressurized water reactors provided by ABB Combustion Engineering. The other is Wolsong nuclear power plant, units 2, 3 and 4 that are CANDU-PHW reactors supplied by Atomic Energy of Canada Limited.

The Yonggwang units 3 and 4 have an electrical output of 1050 MWe each unit. The units were constructed in the late 1989 and will be commercially operated in April 1995 successively. The Yonggwang units 3 and 4 employ dedicated microprocessor-based logic circuits into Interposing Logic System (ILS). The korean utility, KEPCO didn't consider to use microprocessor-based ILS at an early stage, but changed the analog-based to digital-based ILS during the design phase due to obsolescence and difficulty in obtaining replacement components.

Each of Wolsong units 2, 3, and 4 has a net electrical output of 663 MW(e) and is similar as Pt. Lepreau G.S. and Gentilly-2 in Canada, and the Wolsong 1 plant in Korea. The construction of Wolsong units was started successively since 1991 and the commercial operation will begin with 1997 for unit 2. These units are doing 21 new design changes relevant to licensing requirements and about 100 upgrades with utility requests compared with reference plants. These units employ Programmable Digital Comparators to determine trip functions and implement the more extensive formal verification, validation and testing of new software and hardware in compliance with the Canadian Software Standards.

2. YONGGWANG INTERPOSING LOGIC SYSTEM

2.1 SYSTEM ARCHITECTURE[1]

The Interposing Logic System is a fully integrated, complete, and operable microprocessor-based control system supplied by Forney International Inc. The ILS receives plant operator command inputs from control modules mounted on control panels, plant process and equipment operating status inputs, and inputs from other control systems and performs on-off logic operations. The ILS provides a suitable output signal to control plant equipment and control module indicating lamps, and to operate the plant annunciator, computer, and other control systems.

Each field device is an independent subsystems with its own dedicated control board. A typical subsystem consists of a control board and one-to-three I/O boards. For applications requiring grouping of field devices, a single-loop control board can interface with up to 128 I/O boards, providing 1024 field I/O points. Outputs of these boards directly accommodate motor control and switchgear requirements, eliminating the need for interposing relays. Specifically designed on-board functions include field-coil continuity monitoring, control-power monitoring, control-power to logic-power conversion for nonreversing motor starter field devices, and local-control logic-bypass switches on board I/O boards.

Although each subsystem control board can monitor and control its specific field device, certain applications require permissives or interlocks from other field devices; e.g., pumps are on before valves are opened. This capability is provided by a master subsystem control board, which communicates with all loop subsystems and passes information between loops. Sometimes, this function is achieved by hardwiring outputs to inputs within the respective subsystems. This master subsystem also provides fiber-optic serial ports, and/or discrete I/O to external systems such as annunciators and plant computers.

A high speed, parallel-intercommunications bus, controlled by the master subsystem control board, provides communications between subsystems. The master subsystem monitors the functionality of all other subsystems, reports failures, and takes fail-safe action on data from failed subsystems. In addition, a watchdog relay monitors the master subsystem's control board for proper operation. In addition, operator interface on the ILS is provided by individual control-module inserts interface directly to corresponding loop control boards through prefabricated cables.

2.2 SOFTWARE OVERVIEW

Software programming uses address-table programming. The software is secured on non-volatile, erasable programmable read-only memory (EPROM). Various logic functions (e.g., AND, OR, memory, time delay, interlocks, etc.) are programmed on EPROM. The address table ties all logic functions together for a specific application. A dedicated EPROM is provided for each loop logic function. 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 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. It is composed of the AFS-SBC-01 and AFS-SBC-02 firmware, which take charge of Slave control and Master control, respectively. Each of the AFS-SBC-01 and AFS-SBC-02 is a complete computer system on a single printed circuit card. The CPU, Read/Write memory, programmable timers, I/O ports and drivers, priority interrupt logic, bus control logic, and memory expansion buffers all reside on the board.

2.3 SELFCHECKS AND DIAGNOSTICS

The ILS includes self-checking, auto-test features to detect malfunction of the boards, including control logic power failure, on a per loop basis.

The control board auto-test consists of a memory check to ensure that onboard memory is functional and that the address, control, data lines, and components are operational. The one-bit and eight-bit RAM is tested by first storing the memory data in a temporary location, then complementing the data, and writing it back to the same memory location. The same memory location then is re-read and compared to what was sent. If the data compares correctly, the data again is inverted and written to the memory location, re-read, and compared with what was written. If in either case the read data does not compare correctly with what was written, an auto-test failure flag is set and reported when normal program execution resumes. All RAM is tested in this manner.

All onboard EPROMs are programmed with a checksum in byte seven. The auto test routine independently calculates a checksum for each EPROM and compares it with the programmed checksum. Any calculated checksums that do not compare to the programmed checksums are alarmed as an auto-test failure flag and reported as a failure when normal program execution resumes.

During initial subsystem power-up, a failure of the auto-testing does not allow the power-up sequence to proceed, but results in a complete retry of auto-testing. LEDs on the control board indicate the status of the power-up auto-testing.

Transmitted data is sent with a parity bit and checksum bytes. The receiving subsystem ignores the data if parity or checksum is not correct. A loss of communication from a subsystem to the master is alarmed by either a watchdog alarm or by an individual or combined alarm.

2.4 EXPERIENCE AND REGULATORY ISSUES

The introduction of microprocessor-based ILS into the safety-related systems was first time in Korea, with KINS staff emprepared coupled with no previous experience and no consensus standard to apply yet. In particular, the software licensing difficulties arose due to a lack of adequate documentation for the design. Then, the staff required KEPCO to submit various design documents and operating experience and to perform the qualification tests, including EMI and surge withstand capability. So, KEPCO hired a third party to check the software integrity and then submitted the output to KINS. The review of submittals found that the rigorous and formal V&V was not performed and the documentation was not of adequate quality as it did not make review possible. And the programs would be difficult to maintain because of a lack of adequate documentation and trainning programs. The staff concluded that the microprocessor-based ILS did not design features detailed enough to defend against software common mode failures and required to install a hardwired backup panel to control safety-related equipment in Train B only, because A/E credited Train B equipment against design basis events. KEPCO additionally designed and completed to install the manual hardwired backup panel that is capable of

controlling and monitoring Train B equipment in Figure 1 and Table 1. After all, the staff agreed that the ILS was no longer an impediment to licensing. However, the ILS will have to be reviewed if there is any functional modifications.

3. WOLSONG PROGRAMMABLE DIGITAL COMPARATORS

3.1 PDC HARDWARE ARCHITECTURE

In the CANDU 600, two independent, fully capable, high-speed shutdown systems known as Shutdown System No. 1 (SDS1), and Shutdown System No. 2 (SDS2) are employed. SDS1 uses mechanical, spring-assisted, gravity drop absorber rods to effect reactor shutdown, while SDS2 uses gadolinium nitrate poison injection into the heavy water moderator liquid which surrounds the CANDU fuel channel assemblies.

The SDS1 PDC hardware is supplied by Asea Brown Boveri (ABB). It is based on the PROCONTROL P13 Programmable Process Control System[2]. This system provides a range of hardware modules which can be configured to perform data acquisition and control functions. Modules plug into ABB's standard P13 racks and backplanes. The modules communicate via a proprietary bus called the Local Bus. The electrical signals comprising the Local Bus are carried by signal traces on the backplane. These signal traces can be extended to multiple racks by the use of special cables.

The SDS2 PDCs are based on equipment manufactured by PEP Modular Computers of Germany. The equipment was supplied by Marsh Instrumentation of Burlington, Canada (Marsh). The computer is a VME (Versabus Module European) based system.

3.2 SOFTWARE DEVELOPMENT PLAN

SDS 1 SOFTWARE DEVELOPMENT PROCESS

The SDS1 software is developing with Integrated Approach (IA) development process as shown in Figure 2. The IA promises a formal, yet cost-effective solution to the development of critical systems where functionality is added at each stage of the process but never re-specified.

Computer System Requirements (CSR) contain a graphical data-flow specification of the required system behaviour. The requirements are also presented hierarchically to give a top-down view of the system. Computer System Design (CSD) identifies the different design decisions about the implementation of the computer. The interface to the environment is finalized, self-checks and fail-safe measures are added, partitioning is performed, and any additional outputs needed for monitoring are identified. Software Design Description (SDD) contains a duplicate of the CSR graphical requirements and contains all the additional logic needed to implement the decisions of the CSD. The Object Code is translated directly from the SDD without the need for a manual coding process. The "Simple and Direct Verification" verifies the object code generated against

the graphical SDD drawings.

SDS 2 SOFTWARE DEVELOPMENT PROCESS

The software development process for SDS2 is in full compliance with the Standard for Software Engineering of Safety Critical Software as shown in Figure 3. It should be noted that validation and reliability testing require inputs from the system design and the software requirements specification documents. The hazard analysis on the code is required.

3.3 SELFCHECKS AND DIAGNOSTICS

The PDCs perform various selfchecks periodically and annunciate to the operator when a problem is detected. As a minimum, the following selfchecks are programmed into the software.

The checksum on PROM verifies its integrity in commensurate with the unavailability of the trip logic for the PDCs. The software sequence checks verify every program that no significant sections of program are being by-passed. On detection of error, open PDC alarm messages and stop updating the watchdog timer until the PDC is restarted.

The check on the analog I/O system converts a digital word to an analog voltage and output as an A/O. Read this analog voltage as an A/I, then convert it back to a digital word and finally compare it with the original word. The checks on the digital I/O system open and close each test D/O once per hour, read the status of it as a D/I and check that the D/I is in the correct state.

The check on PDC bus disturbance is to identify if there is any problem with the data transmission on the local. On detection of error, open PDC alarm message D/Os, and stop updating the watchdog timer until the PDC is restarted.

3.4 EXPERIENCE AND REGULATORY ISSUES

Programmable Digital Comparators used on Wolsong units 2, 3 and 4 are implemented with the stringent AECB licensing requirements for shutdown system QA. A significantly more rigorous program of software design documentation and testing is required for the PDC functions. The software development for SDS1 and SDS2 is based on Joint Ontario Hydro and AECL Standard for Software Engineering of Safety Critical Software and address AECB concerns on Darlington trip computer software. The PDC software is developing with 5 engineering design phases; system definition phase, design phase, coding phase, testing phase, and validation phase. And the current design is in coding and unit testing phase in the life cycle. KINS agreed the status of PDC software.

4. DEVELOPMENT OF SAFETY AND REGULATORY TECHNOLOGY FOR ADVANCED I&C SYSTEMS IN KOREA

4.1 BACKGROUND

The project entitled "Development of Safety and Regulatory Technology for Next Generation Reactors in Korea" is performed in three phases from 1992 to 2001, based on the incorporation of new safety concepts ensuring a significant safety enhancement in order to establish stable energy supply and improve public acceptance to nuclear power plants. The primary focus of the project is given to the development of the safety and regulatory requirements for the licensing review of the next generation reactors to be developed and then commercialized. The phase I effort has been completed last year and performed the comprehensive feasibility study for development to safety and regulatory requirements. The phase II project keeps on developing the requirements from 1995 to 1998. The phase III project will be continued up to 2001 year. KINS made the basic hierarchy of safety and regulatory requirements in order to develop the requirements in a systematic and consistent way.

4.2 RESEARCH ACTIVITIES OF I&C BRANCH

During phase I, I&C branch has performed various subtasks related to advanced I&C, electrical and human factors issues according to the flow diagram for development as shown in Figure 4. This study has dug out the major safety policy issues and regulatory directions for advanced reactors, safety issues related to EPRI/URD and CE System 80+ and provided the drafts to establish regulatory requirements for the issues to be revised or supplemented in view of the design concepts of advanced reactors. The KINS will research the following items during the phase II project and provide their regulatory positions and procedures.

- Software Quality Assurance Activities
- Common Mode Failure by Software, including D-I-D and Diversity
- Independent Backup Controls and Displays of Critical Safety Functions
- EMI/RFI Sensitivity Issues of Digital-based Systems, e.g. EMC Design and Practices and EMI Verification and Validation
- Radiation Sensitivity of Smart Electronics
- Commercial Dedication Issues
- Human Factors Considerations in the Design of Advanced Control Room
- NRC's Policy Issues Relating to Advanced Reactors[3]
  - Electrical Distribution
  - Defense against Common Mode Failures in Digital I&C Systems
  - Control Room Annunciator (Alarm) Reliability
  - Role of the Passive Plant Control Room Operator

5. CONCLUSIONS

There are two types of reactors under construction with microprocessor-based I&C systems in Korea. The introduction of microprocessor-based systems into the safety-related systems was first time in Korea, with KINS staff emprepared coupled with no

previous experience and no consensus standard to apply yet. In particular, the software licensing difficulties arose due to a lack of adequate documentation for the design. KEPCO additionally designed and completed to install a hardwired backup panel that can control and monitor Train B equipment. After all, the staff agreed that the ILS was no longer an impediment to licensing.

Programmable Digital Comparators used on Wolsong units 2, 3 and 4 are implemented with stringent AECB licensing requirements and standard for Software Engineering of Safety Critical Software. The status of PDC software design is in coding and unit testing phase in the life cycle. The KINS staff agrees with it.

The second phase project will keep on developing the regulatory requirements for next generation reactors in Korea, based on the results of phase I.

6. REFERENCES

[1] Technical Manual, "Forney Interposing Logic System", Vol. 1, October 1992
[2] "Shutdown System No. 1, Part 7 - Programmable Digital Comparator Hardware", 86-68200-DM-007
[3] USNRC SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs", April 2, 1993

Table 1

Listing of Parameters at ILS Backup Panel

Item	Parameters	. Equipment No.
1	SIT 1 Vent Valve	SI-613
2	SIT 2 Vent Valve	SI-623
3	SIT 3 Vent Valve	SI-633
4	SIT 4 Vent Valve	SI-643
5	LPSI MINI Flow Isolation Valve	SI-659
6	PZR Auxiliary Spray Control Valve	CV-203
7	RCP Control Bleed Off Containment Isolation Valve	CV-505
8	Letdown Isolation Valve	CV-151
9	Charging Pump 2	CV-02P
10	Swing Charging Pump 3	CV-03P
11	Component Cooling Water Pump 1	CC-01PB
12	Component Cooling Water Pump 2	CC-02PB
13	Component Cooling Water Pump 3	CC-03PB
14	Essential Service Water Pump 1	SX-01PB
15	Essential Service Water Pump 2	SX-02PB
16	Steam Atmospheric Dump Valve	MS-178
17	Steam Atmospheric Dump Valve	MS-185
18	Steam Atmospheric Dump Isolation Valve	MS-106
19	Steam Atmospheric Dump Isolation Valve	MS-108
20	Motor Driven Aux. Feedwater Pump 1	AF-01PB
21	Diesel Driven Aux. Feedwater Pump 2	AF-02PB
22	Aux. Feedwater Flow Isolation Valve 36	AF-036
23	Aux. Feedwater Flow Isolation Valve 43	AF-043
24	Aux. Steam Generator Level Control Valve 46	AF-046
25	Class 1E Diesel Generator Supply PCBs	AP-01SB
26	RCFC 01CB High Speed	VP-01CB
27	RCFC 02CB High Speed	VP-02CB
28	Supply Air Fan 01CB	VC-01CB
29	Return Air Fan 02CB	VC-02CB
30	Emergency MU Fan 03CB	VC-03CB
31	Train B Zone Isolation Dampers	VC-Y0094B
32	Steam Atomspheric Dump Valve	MS-178
33	Steam Atomspheric Dump Valve	MS-185
34	Aux. Feedwater Cross-Tie Valve	AF-038
35	Aux. Cross-Tie Isolation Valve	AF-049

Figure 1. ILS BACKUP PANEL

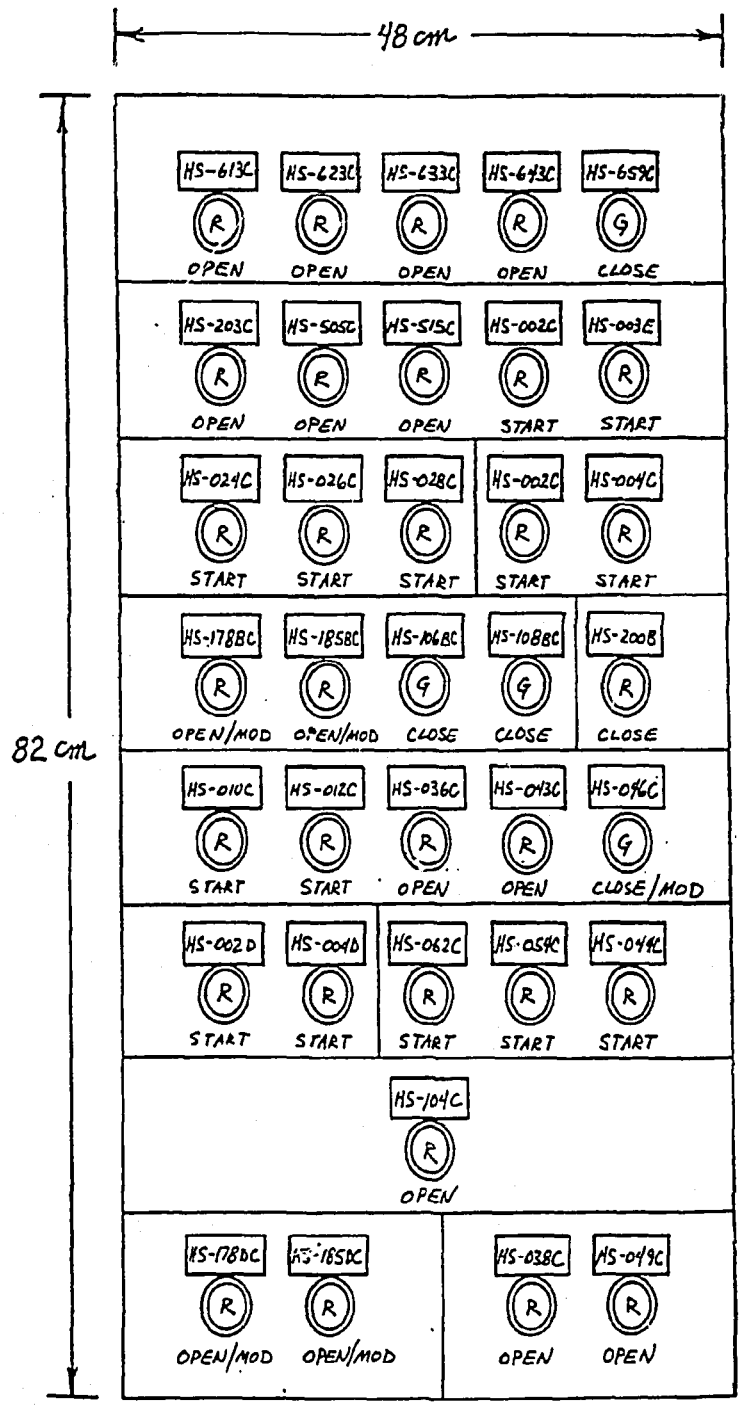


Figure 2. SDS1 Integrated Approach Development Process

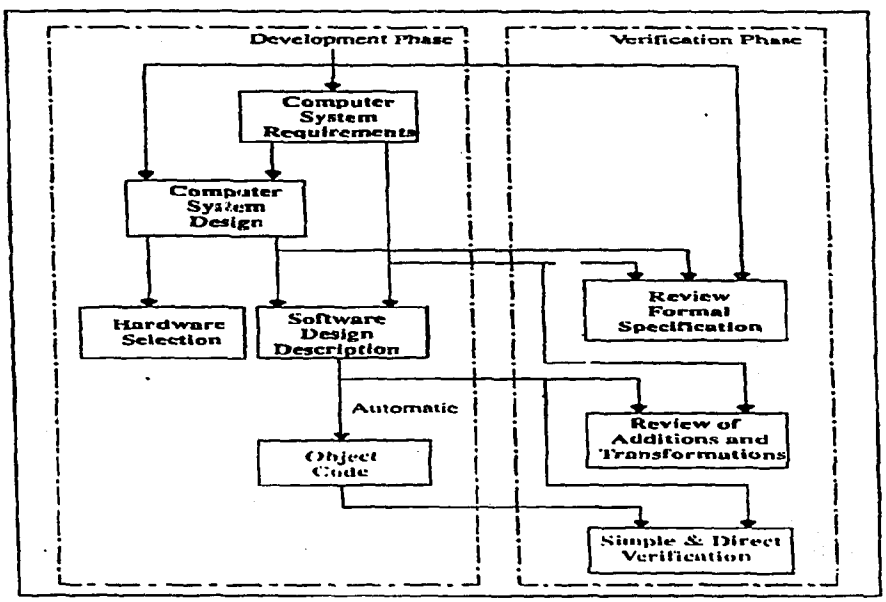


Figure 3. Schematic of Software Engineering Process

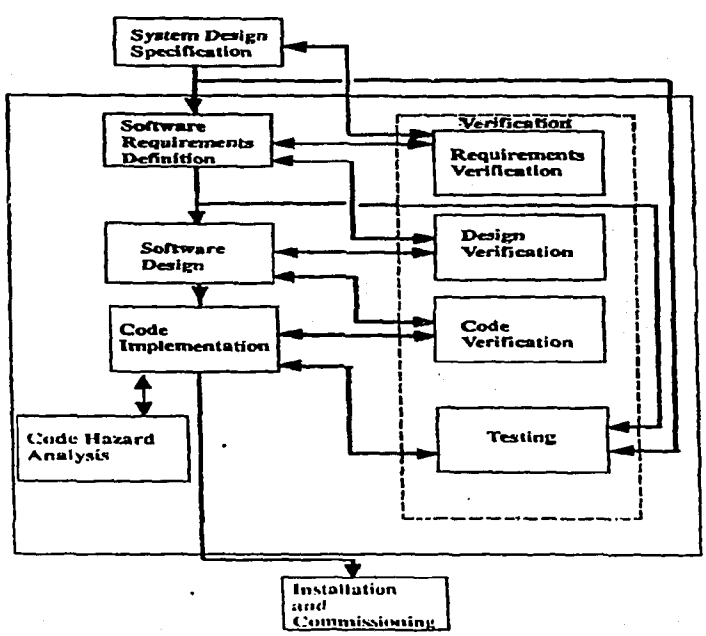
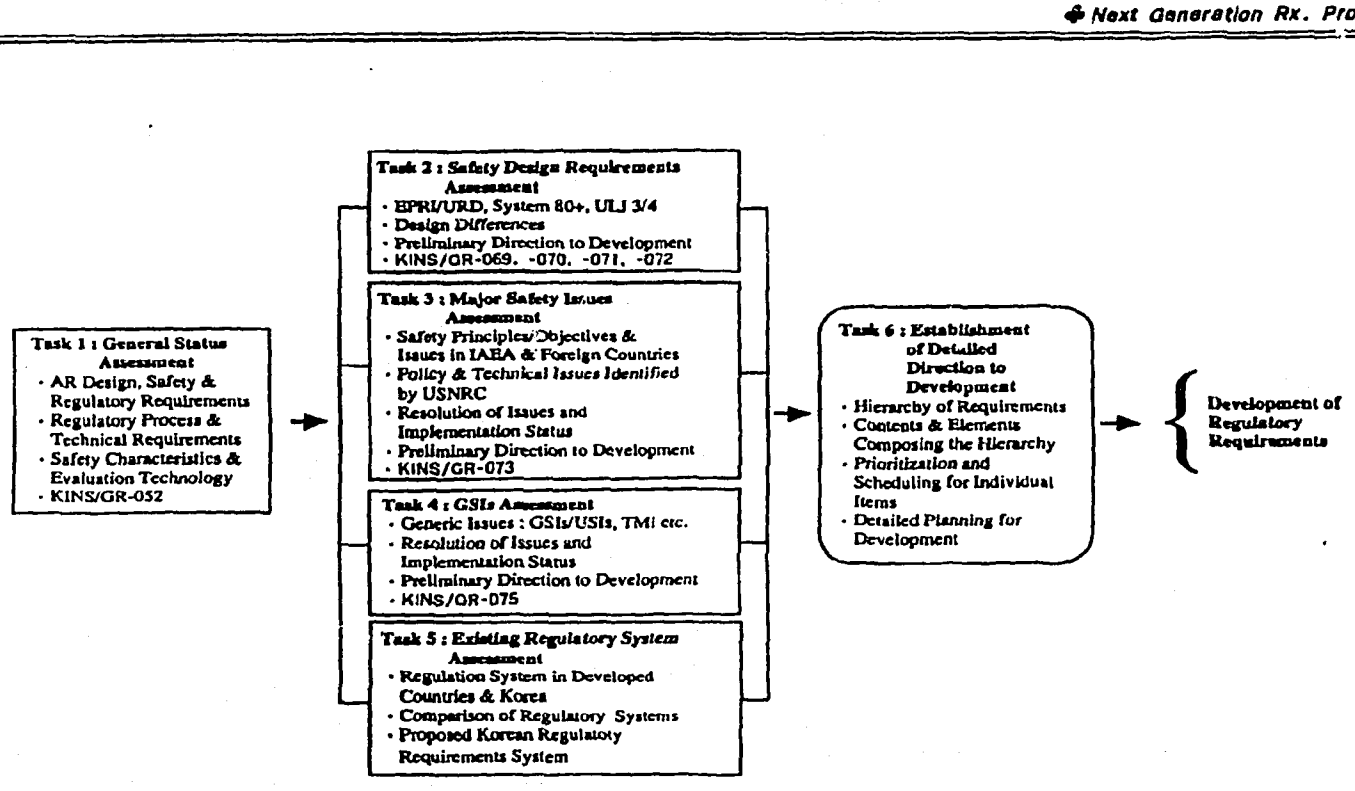


Figure 4. Flow Diagram for Development of Safety & Regulatory Requirements



EXPERIENCE AND REGULATORY ACTIVITIES ON ADVANCED INSTRUMENTATION AND CONTROL SYSTEMS APPLIED TO NUCLEAR POWER PLANTS IN KOREA

Vienna Austria, March 13 - 17, 1995

Presented by

Bok-Ryul KIM

KOREA INSTITUTE OF NUCLEAR SAFETY

INSTRUMENTATION & CONTROL GROUP

■ YONGGWANG NUCLEAR POWER PLANT UNITs 3 & 4

- 2-Loop PWR, 1050 MWe Each, Supplied by ABB-CE
- Commercial Operation in April 1995
- Employ Dedicated Microprocessor-based Logic Circuits to Interposing Logic System (ILS)

■ WOLSONG NUCLEAR POWER PLANT UNITs 2, 3 & 4

- CANDU-600 PHW Reactors Supplied by AECL
- Commercial Operation in 199[illegible] ; Unit 2
- Employ Programmable Digital Comparators to Trip Reactor

■ ILS SYSTEM ARCHITECTURE

- Supplied by Forney International, Inc.
- Single Dedicated Control Board and One-to-Three I/O Boards
- Single-loop control board for grouped devices interface with up to 128 I/O boards.
- On-board functions include field-coil continuity monitoring, control-power monitoring, etc.
- High-speed, Parallel Intercommunications Bus Controlled by Master Control Board
- Control Modules for operator Interfaces

■ ILS SOFTWARE FEATURES

- Address Table Programming Technique

- Various logic functions (e.g., AND, OR, memory, etc.) are programmed on EPROM.

- The address table ties all logic functions together for a specific application.

- The target ILS software is written in Intel 8085 assembly language using top-down modular design techniques.

■ SELFCHECKS AND DIAGNOSTICS

- Selfchecking, Auto-Test Features on a Loop Basis
- One-Bit and Eight-Bit RAM Loopback Checks on Control Boards
- All onboard EPROMs are programmed with a checksum in byte seven.
- Power-up Auto-testing
- LEDs on the contol board indicate the status of the power-up auto-testing.
- Transmitted data is sent with a parity bit and checksum bytes.

■ EXPERIENCE AND REGULATORY ISSUES

- Digital-based ILS was introduced first time in Korea.
- Software licensing difficulties arose due to a lack of adequate documentation of the design.
- Formal verification and validation was not performed.
- Korean utility, KEPCO hired a third party to verify its software integrity.
- Review of submittals found that the ILS did not have design features detailed enough to defend against software common mode failures.
- KINS required KEPCO to install a manual hardwired backup panel to perform emergency operating procedures.
- KEPCO installed a backup panel to control Train B equipment only.

■ SDS1 PDCs HARDWARE

- Based on ABB PROCONTROL P13 Protection Control Systems
- The modules communicate via a proprietary bus called Local Bus.

■ SDS2 PDCs HARDWARE

- Based on PEP Modular Computers of Germany
- The computer is a VME (Versabus Module European) based system.

■ SDS1 SOFTWARE DEVELOPMENT PROCESS

- Integrated Approach (IA) Development Process
- Graphical Requirements Specification
- Automatic Code Generation
- Unit and Subsystem Testing Combined

■ SDS2 SOFTWARE DEVELOPMENT PROCESS

- Compliance with the Standard for Software Engineering of Safety Critical Software
- Tabular Requirements Specification
- Manual Code Generation
- Unit and Subsystem Testing are *separate activities.*

■ SELFCHECKS FOR PDCs

- EPROM Checksums
- Software Sequence (or "Thread") Checks
- Analog Input/Output Loopback Checks
- Digital Input/Output Loopback Checks
- Local Bus Signal Disturbance Checks
- External Watchdog
- Watchdog ensure general system integrity.
- Other checks detect specific failures

■ EXPERIENCE AND REGULATORY ISSUES

- Based on Joint Ontario Hydro/AECL Standard
- Address AECB Concerns on Darlington Trip Computer Software
- Incorporated AECB Comments on Earlier Drafts
- The PDC software is developing with 5 engineering design phases.
  - System Definition Phase
  - Design Phase
  - Coding Phase
  - Testing Phase & Validation Phase
- The current design status is in coding and unit tests phase in the software life cycle.
- So far, KINS has agreed the software development process.

■ DEVELOPMENT OF SAFETY & REGULATORY TECHNOLOGY FOR ADVANCED I&C SYSTEMS

- Being performed in three phases from 1992 to 2001
- The primary focus is to develop safety and regulatory requirements for next generation reactors.
- Phase I project was completed last year.
- Will provide regulatory positions for the followings during the phase II projects up to 1998:
  - Software Quality Assurance Activities
  - D-I-D & Diversity
  - EMI/RFI Sensitivity Issues
  - Radiation Sensitivity of Smart Electronics
  - Commercial Dedications
  - Human Factors Considerations
  - NRC's Policy Issues Implementation for Advanced Reactors

■ CONCLUSIONS

- KINS will require the defense-in-depth and diversity assessments of the proposed digital-based I&C system to the applicant in order to demonstrate that the design against common mode failures is adequately considered.

- KINS will require the installation of hardwired backup system, if necessary.

- KINS has been evaluating the Wolsong software in detail and has discovered so far they are fully diverse and are developed with rigorous standards.

- KINS will establish regulatory positions for the outstanding issues relevant to digital-based I&C systems during the second phase.

Figure 1. ILS BACKUP PANEL

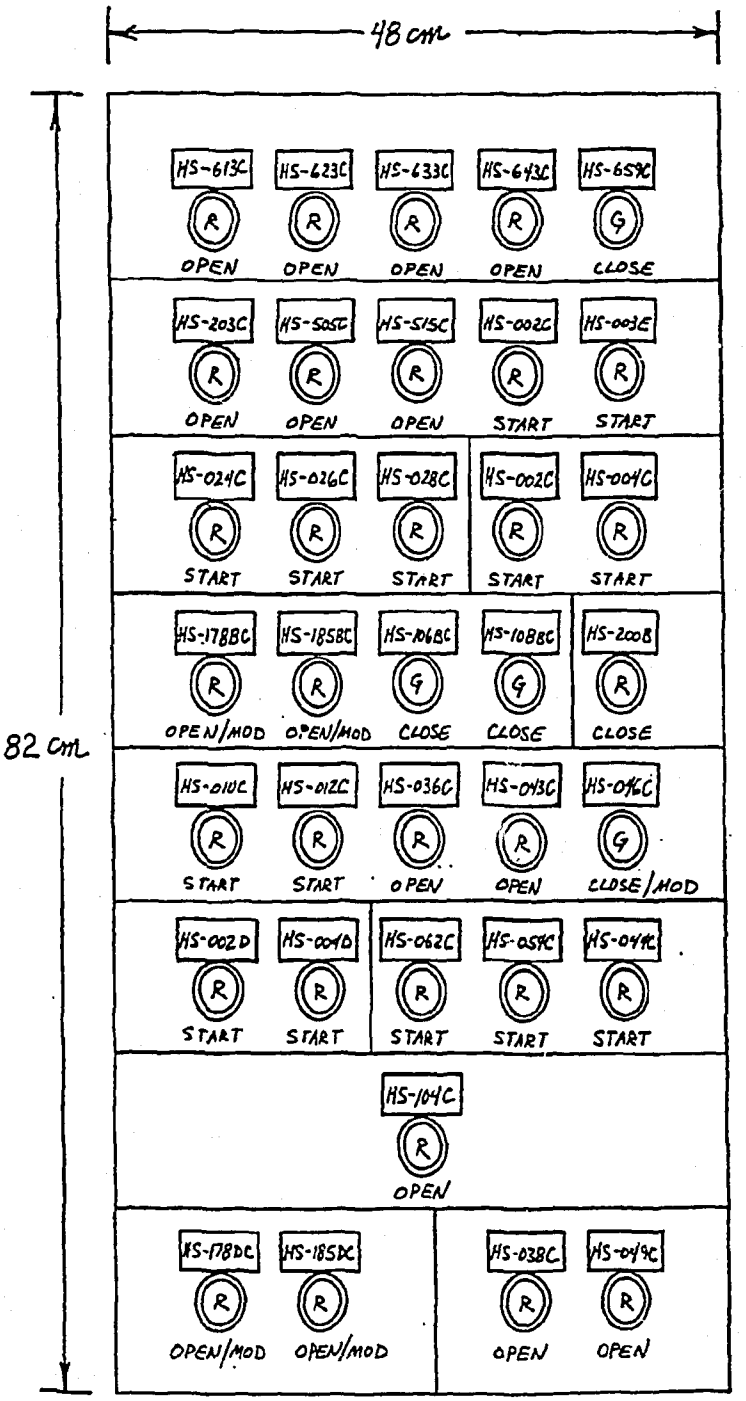


Figure 2. SDS1 Integrated Approach Development Process

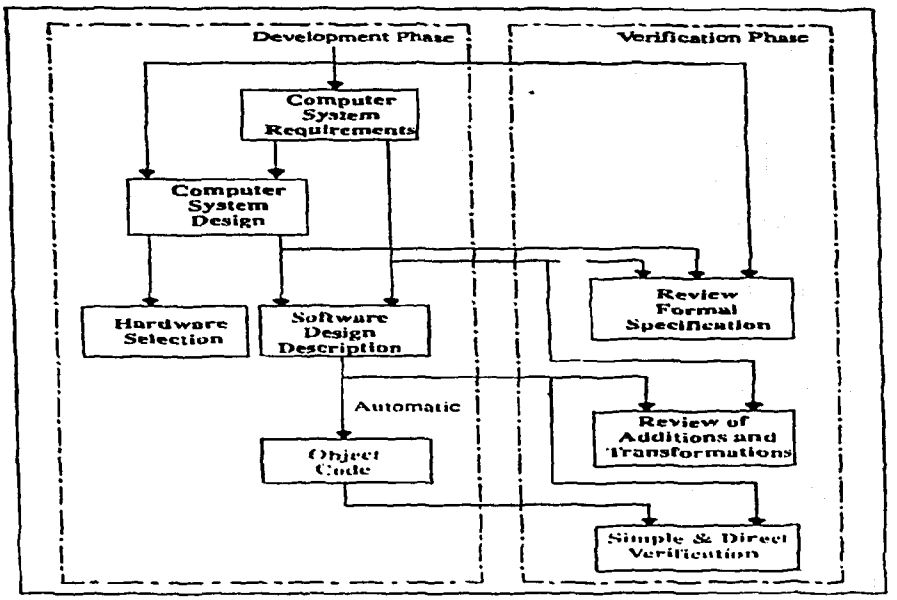


Figure 3. Schematic of Software Engineering Process

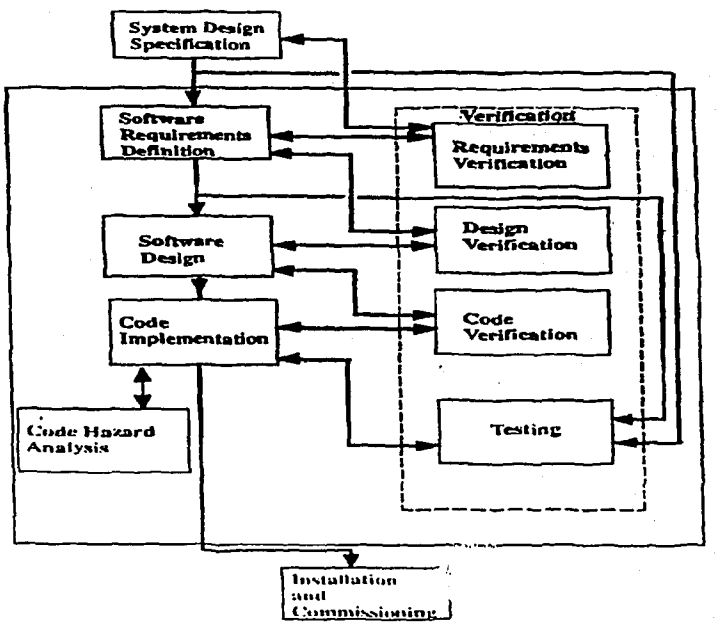


Figure 4. Flow Diagram for Development of Safety & Regulatory Requirements