Development of a Safety I & C System for NPP

Chang-Hwoi Kim, Joo-Hyun Park,Dong-Young Lee
Korea Atomic Energy Research Institute
chkim2@kaeri.re.kr

1. Introduction

Plant Protection System (PPS) in Nuclear Power Plant (NPP) trips the reactor and mitigate accident condition during the plant abnormal or accident conditions. PPS is safety grade system, and PPS shall be developed in accordance with safety design requirements. Analog logic and relay were used in the PPS before 1980's, and digital PPS were developed in 1980's. Board level digital equipment was used for PPS in Early of 1980's, but there were limitations in the expandability and maintainability. The PLC (Programmable Logic Controller) was used for PPS in later of 1980's, which was reliable and technically proved in many industrial fields. Digital PPS and safety grade PLC are developing in the Korea Nuclear Instrumentation and Control System (KNICS) R&D project. For the optimization of PPS design, the PLC shall meet communication, real time, reliability, performance, equipment hardware qualification, and software qualification requirements. The Digital PPS and PLC to be developed in KNICS R&D project will be used for I&C systems upgrade in operating NPPs and for new I&C systems in NPPs.

2. Design Trend of the Digital Plant Protection System in NPP

Westinghouse developed a digital protection system, named Q series, in 1978. This is an hybrid type protection system which is composed of analog and digital circuits. Westinghouse also developed the digital I&C system package, Eagle Family 21, in 1986. The Eagle 21 was applied to the Sizewell B and Temelin NPP. However, the Temelin NPP has not been operated commercially yet, because of license problems.

AECL developed a PDC (Programmable Digital Comparator) and applied it to the CANDU-6 NPP in 1970. In 1980, AECL developed a digital protection system SDS #1 and #2 and applied it to the Darington NPP.

Since the late 1980's, other nuclear vendors have modified and complemented the PLC whose reliability has been proven in the industry to develop a protection system.

Siemens developed a protection system package, named Teleperm XS, and applied it to the Parks NPP in Hungary. Teleperm XS uses profibus for a safety data network and an information data transmits through ethernet network (IEEE 802.3).

ABB-CE in USA developed a digital protection system with the Advant PLC (AC-160), which was licensed by COTS dedication and applied it to the Ulchin 5&6 NPP in Korea. The system transmits safety data via a HSL (High Speed Link) based RS-422 and information data via a AF-100 fieldbus. After Westinghouse took over the nuclear part from ABB-CE, the system name was changed to Common-Q. The Common Q is expected to be applied to the Singori 3&4 NPP in Korea.

Invensys in England carried out COTS dedication an Triconex PLC that had been used in the turbine control system in a NPP. However, NRC concluded that the Triconex PLC could be applied to the protection system package if the applied communication network satisfies the safety criteria.

3. KNICS Plant Protection System (PPS) Package

The main design features of the KNICS PPS Package are as follows:

- Satisfy APR 1400 design requirements
- Improved Availability by automatic on-line periodic testing
- Improved Reliability by redundant Bistable and Coincidence Processor
- Improved Maintainability by extended network

KNICS PPS Package consists of RPS and ESF-CCS (Engineered Safety Features-Component Control System). The platform of KNICS PPS package is POSAFE-Q which is developed by a PLC company in Korea. The design specification of the POSAFE-Q satisfies KNICS PPS requirements[1,2,3,4] and the general requirements for safety PLC[5].

The KNICS RPS has four channels which are located in electrically and physically isolated rooms. RPS generates the RPS trip and ESF actuation signals automatically whenever the monitored processes reach the predefined set points. The KNICS RPS has an on-line automatic periodic test capability for determining the system operability. BP, CP, ATIP(Automatic Test and Interface Processor), and OMs(Operator Modules) are included in the RPS channel.

BP determines the trip state by comparing the measured process variable with the predefined trip set point. The RPS is consisted of two BPs in a channel.

CP generates a trip signal by a two out of four voting logic. When a channel is bypassed, the trip signal is

determined by a two out of three voting. A channel has two CPs.

There is one ATIP in each RPS channel. The ATIP generates the test signals for the manual test and manual initiated automatic test. ATIP also performs RPS status indications, alarms, and healthiness tests to verify the operational status of BP and CP.

COM (Cabinet Operator Module) comprises of two parts: (a) a computer based part that provides the status information regarding the overall RPS equipment such as BPs, CPs, and ATIP and (b) a hardware based part that performs protection related controls such as a channel bypass and an initiation circuit reset.

The ESF-CCS has four divisions. Each division consists of a GC (Group Controller), LC (Loop Controller), CITP(Communication and Integrated Test Processor), and OMs.

The GC in each division has a redundant scheme and performs a full two out of four voting logic to actuate the ESF-CCS. The voting signals are transmitted from four redundant RPS channels.

LC receives the ESF-CCS actuating signals from the GC through the GN (Group Network), and then actuates the related components such as a pump or valve according to the sequence logic.

CITP can generate test signals for the GC such as the manual test and manual initiated automatic test. CITP, also, performs ESF-CCS status indications, alarms, and healthiness tests to verify the operational status of GC and LC[4].

4. POSAFE-Q PLC

The safety PLC, named POSAFE-Q which is developed by KAERI and POSCON, satisfies the Safety Class 1E, Quality Class 1, and Seismic Category I. The software such as the RTOS and the firmware are developed according to the safety critical software life cycle. Especially, the formal method is applied to design the SRS (Software Requirement Spec.) and SDS (Software Design Spec.) to be error-free. The developed software according to the software life cycle is verified by an independent software V&V team.

The main features of the safety PLC are as follows:

- Provide deterministic scheduling
- Provide Profibus-FDL protocol for safety data network
- Provide industrial standard profibus networks
- Satisfy IEC 1131-3 and simulation capability in engineering tool
- Provide loop back function for monitoring single channel failures
- Provide a redundant power

The overall response time from an input to the POSAFE-Q exceeding its trip conditions from the resulting outputs shall be 50ms or less. The target failure rate of each hardware modules in the POSAFE-Q is 10^{-6}/Hr including the random hardware failure rates[6].

The prototype for the POSAFE-Q was developed and the functional testing and equipment qualification tests are currently being prepared. Table 2 shows the main specifications of the POSAFE-Q, Teleperm XS, and AC-160.

5. Conclusion

In this paper, the design concepts of the plant protection system and safety PLC being developed by the KNICS project are introduced. KNICS PPS has a completely redundant architecture and an on-line automatic test function to improve the maintainability and reliability. And also, the safety PLC (POSAFE-Q) S/W and H/W are being developed according to the safety critical software life cycle and safety H/W criteria. Therefore, the safety critical software design and V&V methods, safety analysis methods, and qualified H/W design technologies will be accomplished in this project and extended to the related industries. It is expected that the digital plant protection system and POSAFE-Q being developed through the KNICS project could be applied to existing NPPs for replacement or to a new nuclear power plant.

REFERENCES

[1] KNICS-RPS-SDR101 Rev.00, “Design Requirements for Reactor protection System," Nov. 2001

[2] KNICS-RPS-DS101 Rev.01, “Design Specification for Reactor protection System," May. 2002

[3] KNICS-ESF-SDR101 Rev.00, “Design Requirements for Engineering Safety Feature-Component Control System," Nov. 2001

[4] KNICS-RPS-DS101 Rev.01, “Design Specification for Engineering Safety Feature-Component Control System," May. 2002

[5] EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants", Dec. 1996

[6] MIL STD 217F, "Reliability Prediction of Electric Equipment"