A Nuclear Safety System based on Industrial Computer

Ji-Hyeon Kim*, Do-Young Oh, Nam-Hoon Lee, Chang-Ho Kim, Jae-Hack Kim
Korea Electric Power Corporation - Engineering & Construction (KEPCO-E&C)
*jhkim10@kepco-enc.com**

1. Introduction

The Plant Protection System(PPS), a nuclear safety Instrumentation and Control (I&C) system for Nuclear Power Plants(NPPs), generates reactor trip on abnormal reactor condition. The Core Protection Calculator System (CPCS) is a safety system that generates and transmits the channel trip signal to the PPS on an abnormal condition. Currently, these systems are designed on the Programmable Logic Controller(PLC) based system and it is necessary to consider a new system platform to adapt simpler system configuration and improved software development process.

The CPCS was the first implementation using a micro computer in a nuclear power plant safety protection system in 1980[2] which have been deployed in Ulchin units 3,4,5,6 and Younggwang units 3,4,5,6. The CPCS software was developed in the Concurrent Micro5 mini-computer using assembly language and embedded into the Concurrent 3205 computer. Following the micro computer based CPCS, PLC based Common-Q platform has been used for the ShinKori/ShinWolsong units 1,2 PPS and CPCS, and the POSAFE-Q PLC platform is used for the ShinUlchin units 1,2 PPS and CPCS.

In developing the next generation safety system platform, several factors (e.g., hardware/software reliability, flexibility, licensibility and industrial support) can be considered. This paper suggests an Industrial Computer(IC) based protection system that can be developed with improved flexibility without losing system reliability. The IC based system has the advantage of a simple system configuration with optimized processor boards because of improved processor performance and unlimited interoperability between the target system and development system that use commercial CASE tools.

This paper presents the background to selecting the IC based system with a case study design of the CPCS.

Eventually, this kind of platform can be used for nuclear power plant safety systems like the PPS, CPCS, Qualified Indication and Alarm – Pami(QIAS-P), and Engineering Safety Feature-Component Control System (ESF-CCS).

2. Background

The PLC supports deterministic process scheduling with reliability but lacks flexibility so that the developer has to use a function block based development tool (e.g., ACC tools for Common Q and Pset II for POSAFE-Q) that has limited flexibility for software development. IC based platform supports wide functionalities with Integrated Development Environment (IDE) but additional Input/Output (I/O) expansion cards or special extensions must be integrated into the PC's operating system for the system purpose[3]. The Programmable Automation Controllers (PACs), have the advantage of both the PLC and IC, blending the PLC-style deterministic machine and the flexibility of an IC based operation in multiple domains with customized or restricted commercial operating systems.

In designing mathematically complex safety system software, developers need to consider 1) deterministic process control 2) minimized programming limitation by the operating system or customized development tools, 3) use of general development languages(e.g., C, C++) rather than ladder logic, 4) compatibility to CASE tools for designing, verification & validation and simulation, and 5) system performance.

PLC has advantages for deterministic process control with stable I/O but has functional limitations and is focused on programs that can be easily described in a data flow diagram. PAC is good for a deterministic process, with the functionality of a PC with multiple domain interconnectivity but still focus on enterprise integration for automation controllers with lack of general purpose CASE tool adaptability. The IC based system has wide functionality, but has a burden for safety system certification in regard to system software and equipments including the Processor and I/O boards.

Some major real time operating systems have obtained the certification for critical application, which makes it easier for safety system application on the IC based system. The open operating system in IC based safety system has slight programming limitations and supports commercial CASE tools with a modeling technique that provides great advantages in development, and verification and validation phase.

3. Case Study : IC Based CPCS

Wind River's VxWorks and QNX Software System's QNX have obtained IEC 61508 SIL3 certification. The IEC61508 industrial safety standard forms a basis for many derived standards, including the nuclear standard IEC 61513. The certifications provide the Board Support Package (BSP) for industrial processor boards and can accelerate system certification for safety critical systems. Several industries like aerospace and railway systems adapt IC based safety systems that are required to conform to the safety requirements of DO178B, IEC 61508 and IEC 60880, and there is a CASE tool(e.g., SCADE) that satisfies the IEEE-1012(2004) requirement for nuclear safety critical system development.

CPCS consists of two major subsystems. One is the safety related part that continuously calculates the Departure from Nucleate Boiling Ratio (DNBR) and the Local Power Density (LPD) to initiate a reactor trip during certain transient events to protect the reactor core, and the other is the MMI system part (OM, Operator Module) that displays the reactor condition and alarm status. The safety related part falls into the category of safety critical and the MMI part is important to safety.

The current design of the CPCS employs a PC node box for the OM with the QNX operating system and PLC for the algorithm processing part with three(3) sub racks of CPC, CEAC1, CEAC2 where each rack has two(2) processor boards with the operating system of modified Vertex, one(1) field bus communication board for intra channel communication, and I/O cards(Figure 1).

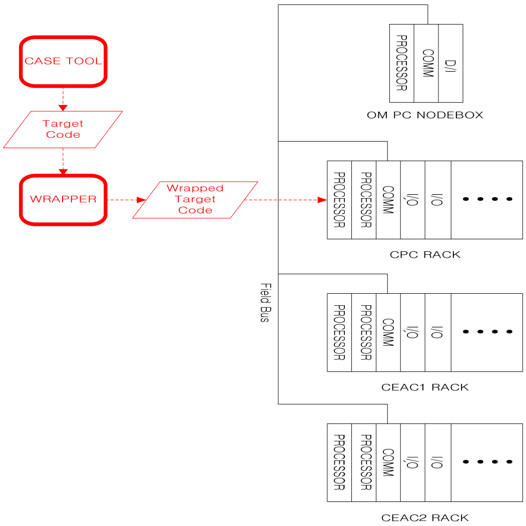

Figure 1. PLC Based CPCS Configuration

The adaption of IC based system in the safety related part can reduce the number of sub racks from three(3) to one(1) on the strength of CPU's performance (Figure 2). There are two(2) processor boards, one for CPC and CEAC algorithm and one for core element assembly position signal processing. In this configuration, the generated target code can be loaded into target processor board without any modification after the model based verification and validation through a CASE tool so that additional verification and validation is not required because of the wrapping process (Figure 2).

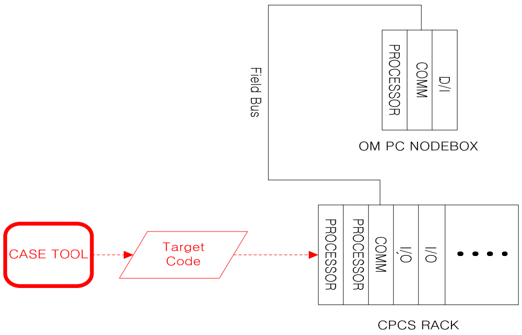

Figure 2. IC Based CPCS Configuration

4. Conclusion

The introduced IC based nuclear safety system has the advantages of a simplified system configuration as well as efficient software development methodology using safety software CASE tools. The system reduces the possibility of system trouble compared to complicated system communication with multiple racks. The feasibility of the nuclear safety critical system using the IC based system was already demonstrated for a reactor protection system[1] which uses the Versa Module Europe(VME) bus computer, whereas the suggested CPCS can be configured with compact PCI boards. For the next generation nuclear safety system, the IC based system can be used due to its compatibility with well-equipped CASE tools, and high CPU performance that can simplify the system configuration. Next step study will be the hardware and software qualification for the new generation NPP safety systems.

REFERENCES

[1] Hyun Kook Shin, Sang Ku Nam et al, "Development of Advanced Digital Reactor System using Diverse Dual Processors to prevent Common Mode Failure",pp33-44, Nuclear Technology, Vol.141, Jan.2003.

[2] Peter L. Hung, Core Protection Calculator System: Past, Present, and Future, Proceedings of the 18th International Conference on Nuclear Engineering ICONE18, May 17-21, 2010.

[3] Understanding Programmable Automation Controllers (PACs) in Industrial Automation, OPTO22 White Paper, 2007.