Development of the Safety Programmable Logic Controller (SPLC) used in the Nuclear Safety System

Kwang-Seop Son [a*], Dong-Hoon Kim[a], Chul-Woong Son [a]
[a]*Korea Atomic Engery Research Institute,1045 Daedeokdaero, Yuseong, Daejeon, 305-353*
[*]*Corresponding author: ksson78@kaeri.re.kr*

1. Introduction

As a part of the Nuclear Technology Development Program, we develop the high performable SPLC that is an advanced controller of the POSAFE-Q (Qualified Poscon Safety Programmable Logic Controller) developed by the KNICS (Korea Nuclear Instrumentation & Control System). In this paper, the key design features and detail designs of the architecture, OS (Operating System) and data communication of the SPLC are described.

2. Design Features

In this section, the design features related to the architecture, OS and data communication are described [1].

2.1 Architecture

The key design features of the SPLC are as follows;

- The redundancy of input/output module and processor module used in the SPLC is selectable.
- 2 out of 3 voting function and hot-standby function are basically served in the TMR (Triple Modular Redundancy) and DMR (Dual Modular Redundancy) respectively.
- The recovery function by the fault detection is performed by the receiving module.

2.2 Operating system

The key design features of the SPLC are as follows;

- The OS of the SPLC has the non-interrupt, deterministic task scheduling structure
- The scan resolution is less than 5msec
- The scan time of safety critical application program is less than 25msec
- The comprehensive diagnostic functions for every module used in the SPLC are provided
- The OS satisfies the safety critical software grade

2.3 Data communication

The SPLC data communication has the deterministic state based protocol, and high effective transmission capacity. The key features are as follows;

- The data communication of the SPLC is deterministic, and satisfy the independency among the separated channels
- The safety communication module is composed of the safety critical control network and the safety status networks that maintain the independency between these networks.
- The safety data communication is configured to 64 nodes to the max, more than 20Mbps of transmission capacity, and interfaced with an optical link

3. SPLC design

In this section, the detail designs of the architecture, OS and data communication are described.

3.1 Architecture

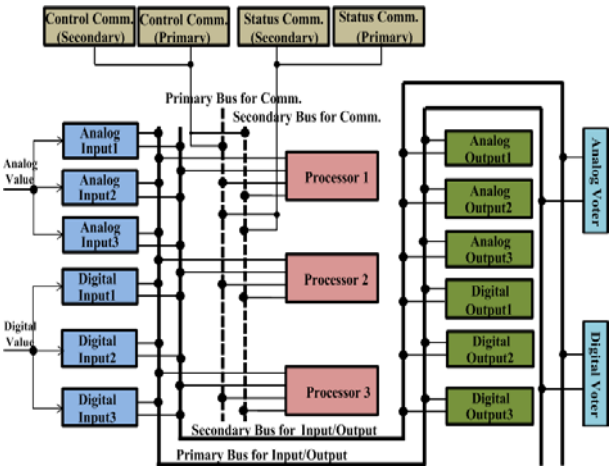

Fig. 1. SPLC basic architecture used in the nuclear safety system.

The SPLC is designed to have the structural flexibility. In other words, the input/output, processor module that requires the active decision could be maximally configured to the TMR, and the communication, bus, power module that requires a tolerant function are configured to the DMR. As shown Fig.1, the SPLC used in the nuclear safety system is designed to have the TMR in one rack to satisfy the simple structure, high reliability and availability. That is, the input/output, processor module are configured to the TMR, and the communication, bus module are configured to the DMR [2]. The communication module is composed of the control network module and

the status network module that satisfy the independency between these networks, and the bus is designed to the serial bus that has strengths in the redundancy, high speed, scalability.

3.2 Operating system

In general, because a commercial RTOS (Real Time Operating System) which normally uses a preemptive scheduling has an uncertainty such as infinite busy waiting, starvation, it is difficult to ensure the reliability when adopted in the nuclear safety system. Thus to have a deterministic, we develop a supervisory function in the SPLC OS as shown Fig.2. The supervisory controls tasks and time to enable the deterministic scheduling and sequential execution of tasks. The scheduling function is executed using a non-preemptive status based method which means that an executing task is not preempted by the other tasks. The execution time is assigned to the task in multiple of tick that is a minimal resolution, and tasks are sequentially executed [3].

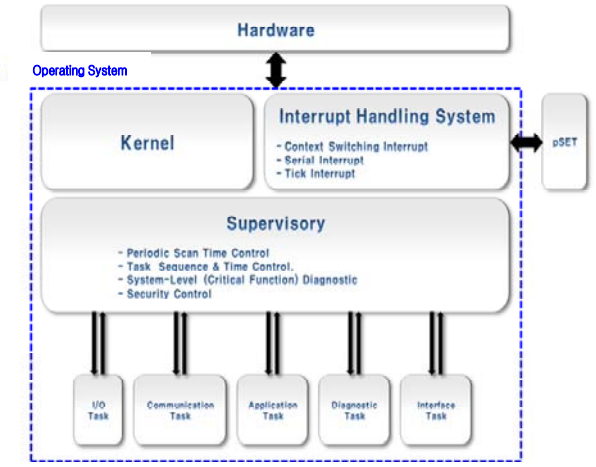

Fig. 2. OS structure

3.3 Data Communication

The data communication of the SPLC is designed to satisfy an effective transmission capacity of 20Mbps and transmission delay of 50msec. The protocol structure is composed of the PHY of IEEE 802.3 fast Ethernet, the MAC of the GTS (Guaranteed Time Slot) which is periodical and guarantees the transmission and the NETWORK of performing the association/disassociation of the network. As shown Fig.4, the communication networks used in the SPLC are composed of the communication switching device that performs a message switching and network management, and the communication node device that transmits/receives a message [4].

3. Conclusions

We develop the high performable controller, SPLC used in the nuclear safety system. To increase the reliability, the architecture is designed to have the MMR composed of the DMR and TMR, and to ensure the deterministic, the OS is designed to have the supervisory which controls tasks and time to enable the deterministic scheduling and sequential execution of the tasks. Also to ensure the deterministic and high transmission capacity of the data communication, the network is designed to have the deterministic status based protocol and effective transmission capacity of 20Mbps using a high switching device. When the development of the SPLC is complete, it is expected to be applied to the advanced nuclear safety system.

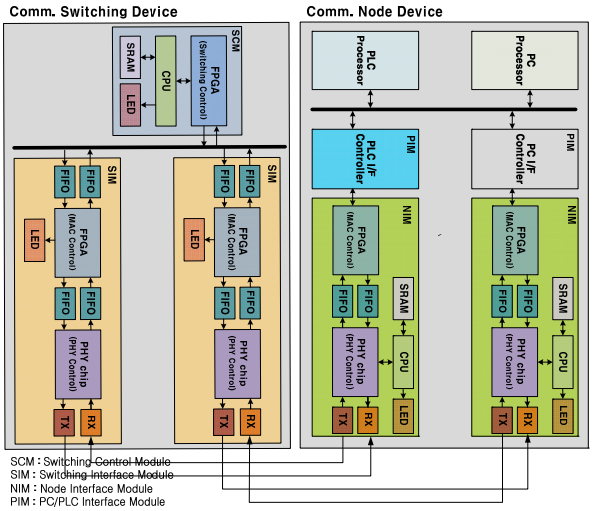

Fig. 3. Data communication structure

REFERENCES

[1] D. H. Yun, “Design Basis for SPLC (ANICS-SPLC-DB101)”, Posco ICT, 2011
[2] D. H .Yun, “Design Report for SPLC (ANICS-SPLC-DR101)”, Posco ICT, 2011
[3] M. G. Lee, “Detailed Design Report for SPLC (ANICS-SPLC-RR101)”, Posco ICT, 2012
[4] K. S. Son, D. H. Kim, “Development of Broadband-Nuclear Safety Data Link (B-NSDN), NuPIC Symposium in Korea, Autumn, 2011

ACKNOWLEDGMENT
This work was supported by the Nuclear Technology Development Program of the Korea Institute of Energy Technology Evaluation and Planning (KETEP) grant funded by the Korea government Ministry of Knowledge Economy (No. 2010161010001G)