Preprints of the 19th World Congress
The International Federation of Automatic Control
Cape Town, South Africa. August 24-29, 2014

Programmable Controller with Flexible Redundancy for Safety Functions in a Nuclear Power Plant

Kwang-Seop Son * **Dong-Hoon Kim** * **Jinpyo Noh** ** **Jaehyun Park** **

* *Korea Atomic Energy Research Institute, Daejeon, Korea, (email:dhkim4@kaeri.re.kr, ksson78@kaeri.re.kr)*
** *Department of Information and Communication, Inha University, Incheon, Korea, (email:jpnoh@emcl.org,jhyun@inha.ac.kr)*

Abstract: This paper presents the redundancy architecture of the Programmable Logic Controller called the Safety PLC(SPLC) for the safety functions such as reactor protection in a nuclear power plant. The architecture of the SPLC is designed to switch flexibly redundancy model between the Dual Modular Redundancy(DMR) and Triple Modular Redundancy(TMR). Using this flexible redundancy architecture, the controller can be optimally configured to the application area, and the reliability and availability of the overall system can be increased because redundancy model varies as failures occur. The operating system of the SPLC is also specially designed to guarantee the strict real-time operation using the non-preemptive state-based scheduler and the supervisory task that manages timing violation of each task. The data communication of the SPLC uses the deterministic state-based protocol based on the Guaranteed Time Slot(GTS) protocol. The reliability analysis results show that MTTF of SPLC is 41,630 hours, which is about 15% and 50% more reliable than the TMR or DMR architecture, respectively.

Keywords: Nuclear plant, fault-tolerant systems, programmable controllers, reliability analysis, redundancy control

1. INTRODUCTION

Control systems in a safety-critical environment such as a nuclear power plant, a high speed train, or an aircraft, are required to have the high-level of reliability because a single failure in such control systems may result in a huge catastrophe. Hence, the controllers used in such a safety-critical system are specially designed using a fault-tolerant architecture with multiple redundancy to maintain the high reliability. In a nuclear power plant, the control systems related to the reactor protection and safety features are classified as safety-related region and are required to have much more reliable architecture, which includes Reactor Protection System(RPS), Reactor Core Protection System(RCOPS), Engineered Safety Features Component Control System(ESF-CCS), Qualified Indication, and Alarm System(QAIS-P). For this safety-related control region, to the law and regulations, only specially designed control systems can be used. To achieve this high standard of reliability, legacy control systems used in the old nuclear power plants were designed based on the analog circuits and electro-mechanical relays. However, since large number of analog components have been discontinued in mass-production, Programmable Logic Controller(PLC)-based digital control system have been introduced even in the safety-related regions. For this, various redundant architecture(Dwyer (2012) and Jiang and Yu (2012)), fault detection algorithm(Dorr et al. (1996)), and network protocols(Kim et al. (2000) and Sul et al. (2012)) have been proposed. In Korea, the Ul-Jin 5 and 6 plant which have started the commercial operations in 2005 were the first nuclear power plants that adopted the digital control systems in the safety-related region. Since then, most of recently designed nuclear power plants including the Sin-Kori and Sin-Ul-Jin plants in Korea also use the digital control systems in the safety-related region. For this migration, the requirements and characteristics for the digital PLC in a nuclear power plant has been studied(Kwon and Lee (2009)). In order to use the digital controllers in the safety-related regions, they must be specially designed and verified to meet the standards and regulations. These qualified controllers are classified as the Q-Class controllers. There are only a few Q-class digital controllers in the market. One of the Q-class digital controllers used in a nuclear power plant is the Advant AC-160 model from ABB (2001). AC-160 was originally developed for the commercial non-safety functions, but through the Commercial Grade Item Dedication(CGID) process, it was approved to be used in the safety-critical region. The redundancy of AC-160 is the dual redundancy model. It uses two different networks: high-speed point-to-point network with speed of 3.1 Mbps between safety controllers and MVB-based multi-drop network(1.5 Mbps) for control and monitoring purpose, respectively. Another Q-class digital controller is the POSAFE-Q model from PonuTech that is also based on the dual redundancy structure(PonuTech

Copyright © 2014 IFAC

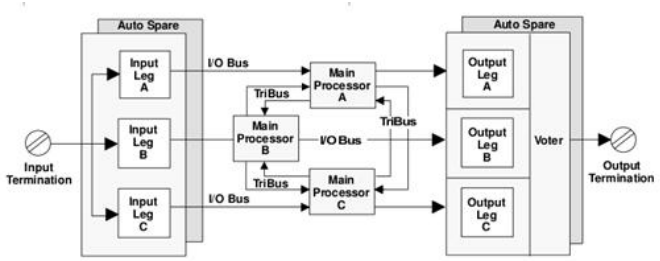

Fig. 1. Structure of Tricon controller

(2009), and Cha et al. (2006)). The network protocol used in the POSAFE-Q model is ProfiBus. Both the AC-160 and POSAFE-Q controllers have dual redundancy with hot-standby policy. This means that only one of the two modules is in operation and the other module is ready to operate when a fault occurs in the operating module. In this hot-standby policy, fault detection measured in the Fault Coverage Factor(FCF) and data coherency are very important to ensure correct handover between the active and standby modules without data loss and control signal bumping.

On the contrary, the Tricon control system from Invensys Inc. is based on the triple redundancy architecture as shown in Fig. 1(Invensys Systems Inc. (2007)). There are three active processing modules in operation that calculate control output simultaneously and determine output values using the majority voting algorithm. To help voting, high speed serial bus, TriBus, is provided between three processing modules for high speed data exchange among the processors. To provide the redundancy in I/O modules, each I/O module has triple I/O legs through which input values are distributed to three different processors and output values are again voted in the output module. The triple redundancy in I/O module provides a very high level of reliability and lessens the probability of common cause failure.

Since both dual and triple redundancy have their own advantage over each other, this paper introduces a new programmable controller for the safety-related functions in a nuclear power plant, called *SPLC(PLC for safety function)*, based on the flexible architecture that can switch dual or triple redundancy upon specific circumstances.

2. REQUIREMENT FOR NUCLEAR POWER PLANT CONTROLLER

Since the controller for a safety-related function should be strictly designed to meet industry standards and regulations including IEEE standard and US Regulatory Guide, the requirement to design them should be clearly identified. Since IEEE standard recommends eliminating the risk of Common Cause Failure(CCF) at the module and system levels(IEEE (1994)), redundancy should be implemented at the processing modules, I/O modules, and communication networks.

The other key feature is the independence that means each module or sub-system should independently operate from each other and a failure in a part should not propagate to the other. For this, communication between safety-related controllers should be uni-directional and have a

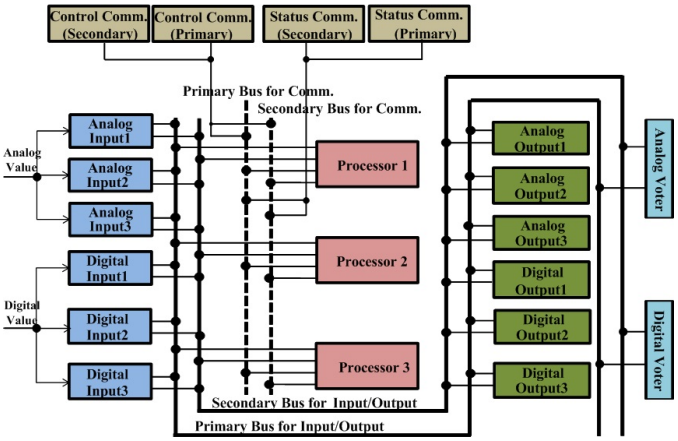

Fig. 2. Structure of SPLC

buffer logic in it. And for the safety purpose, the data flow through the communication network should only be uni-directional from the safety region to non-safety region, which means that no data flow from non-safety to safety region is permitted.

Deterministic operation is another key feature for the controllers to meet. From the IEEE standard, tasks of safety-related functions should perform their own functions without any interruption to the pre-defined schedule. Following design criteria were selected for the SPLC with consideration for the above mentioned requirements.

- The redundancy of the input/output module and processor module used in the SPLC should be flexible.
- 2 out of 3 voting and hot-standby policy should be used in the TMR(Triple Modular Redundancy) and DMR(Dual Modular Redundancy) configuration, respectively.
- The fault detection and fail-safe function should be performed by the data receiving module.
- The Operating System(OS) of the SPLC should have the non-interruptable and deterministic task scheduling.
- The scan time of safety critical applications should be less than 25 *msec*.
- The data communication of the SPLC should be deterministic and satisfy the independence among the separated channels.
- The safety data communication should support upto 64 nodes with at least 20 Mbps of network bandwidth.

3. STRUCTURE OF SPLC

To the design constraints described in the previous section, SPLC is designed to have the dual and triple redundant architecture as shown in Fig. 2.

3.1 Flexible Redundancy

The redundancy concept of SPLC is using the triple redundancy in active module such as the processor module and I/O module that needs independent decision and active control functions and dual redundancy in passive components including back-plane, communication network, and power supply that requires minimum redundancy to avoid Common Cause Failure(CCF).

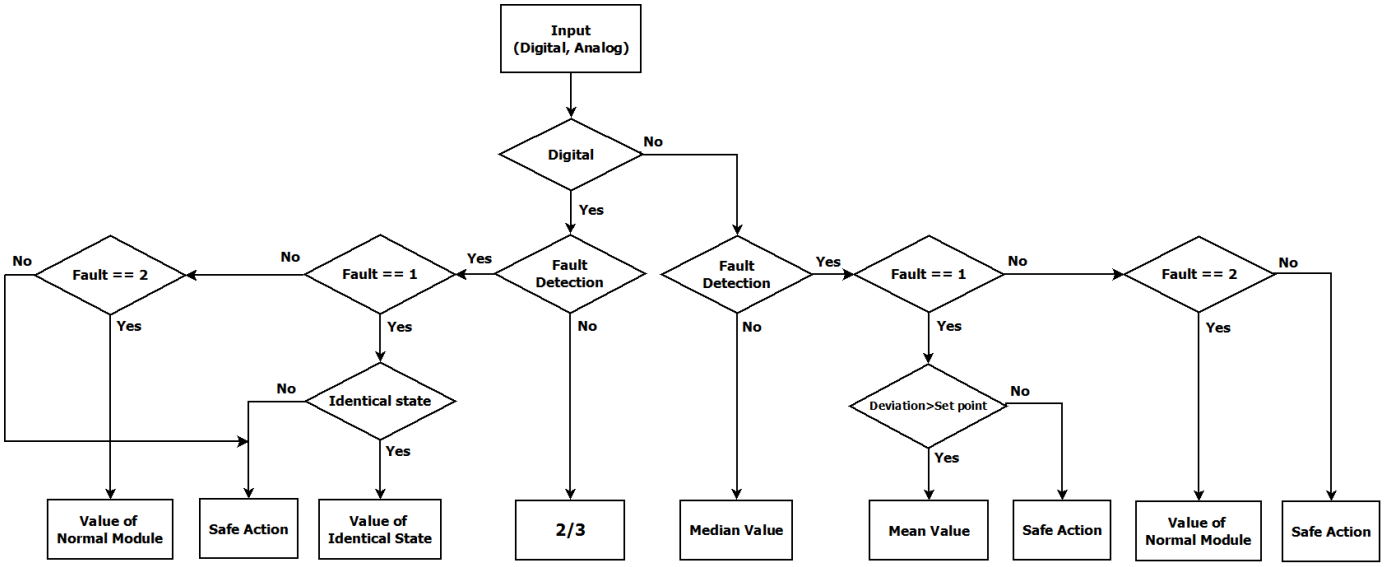

Fig. 3. Output value decision algorithm

However, since not all safety-related functions require TMR-level reliability, DMR configuration can be used in active modules as well to reduce the complexity and cost. In Fig. 2, output module is configured as DMR while input and processing module are configured as TMR. Even in the TMR configuration, if a failure occurs in a certain module, the DMR configuration is automatically selected and the control functions are reconfigured at the operating system level. This reconfiguration increases the availability and the reliability of the overall system as analyzed in Section 4. In the DMR configuration, either the hot-standby operation or parallel operation with voting logic is used to select the primary module, while only the hot-standby policy is applied in the passive modules. For the input and output modules, voting logic can be used to get the correct input and output values.

3.2 Output Value Decision Algorithm

The decision of output value depends on the number of healthy modules in each redundant configuration. For the digital output, if every module is working correctly in the TMR configuration, 2-out-of-3(majority voting) is used. In the DMR configuration or in the TMR configuration with one malfunctioning module, if two values(states) are identical, it is used as the output value. However, two values are different, safe action(safe state) is automatically selected. If only one module is working correctly either in the DMR or TMR configuration, the normal value from the working module is used.

In analog case, the normal output value is defined as the median value in the TMR configuration. However, in the DMR configuration including the case of one module fails in the TMR configuration, if the difference between two values is larger than the threshold value, both modules are ignored and the safe action is processed. Otherwise, the average value is used as the output value. If only one module is working correctly either in the DMR or TMR configuration, the value from working module is used as the output value.

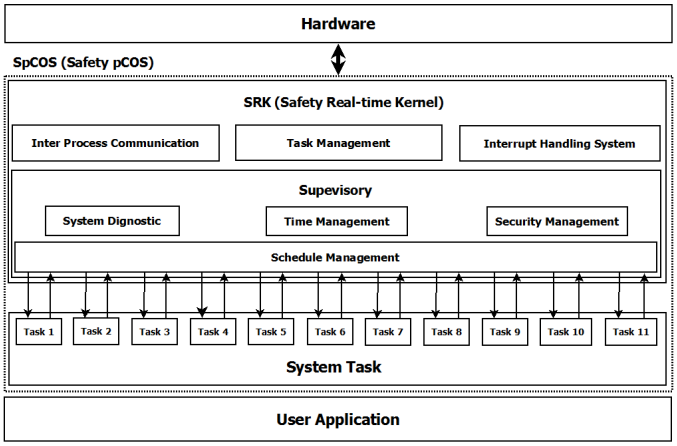

Fig. 4. Operating System

Fig. 3 shows the output value decision algorithm used in the digital and analog output voters in detail.

3.3 Communication Network

Communication network used in SPLC can be divided into two different purposes: inter-node and intra-node network. As for the inter-node network, a time-sharing deterministic communication is implemented, which is based on the Guaranteed Time Slot(GTS) mechanism that is originally proposed in the IEEE 802.15.4 standard(IEEE (2011)). Since the performance of the GTS protocol was analyzed in many literatures(Koubaa et al. (2006) and Yoo et al. (2010)), it can be used as a inter-node network if sufficient network bandwidth is provided. In SPLC, upto 128 nodes can communicate over 100 Mbps Ethernet-based GTS protocol. FPGA-based GTS controller showed that the effective communication speed is 20 Mbps and the end-to-end transmission latency is less than 50 *msec*.

Within a node, an intra-node network instead of a parallel bus is used among the processing modules and I/O modules. Current design uses EtherCAT protocol with 10 *msec* cycle time over 100 Mbps Ethernet as an intra-node

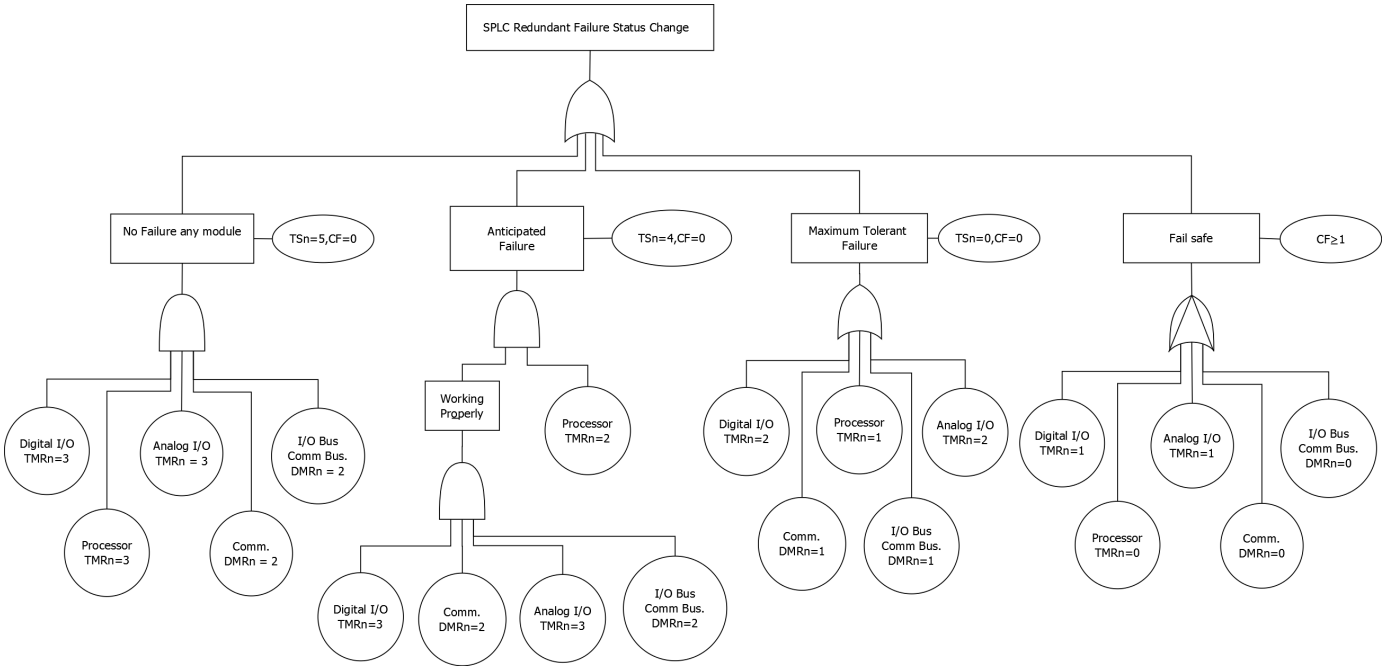

Fig. 5. Fault-tree Analysis

network but the other serial buses can be used in the implementation phase.

3.4 Operating System

Even though there are a few commercial operating systems that support hard real-time operations, most of the commercial operating systems hardly guarantee very strict deterministic operation that complied to the regulations and standards of the nuclear system. Hence, to meet the strict determinism defined in regulations, a new real-time kernel for SPLC, *Safety Real-time Kernel(SRK)*, was designed to ensure the deterministic operation of safety function without any interruption by other functions, including the system diagnostics and communications. Fig. 4 shows the internal blocks of SRK.

To guarantee the execution time of the safety function, the scheduler of SRK operates using a non-preemptive state-based scheduling policy. In addition to the non-preemptive scheduler, a special supervisory task module that takes care of time management, security management, and system diagnostics was used to guarantee the hard-real-time operation. The maximum resolution of the context switching time and the scan time of the application task are 5 *msec* and 25 *msec*, respectively.

Another key feature of SRK is to handle the redundancy structure according to the failure occurrence. Since SPLC is based on the flexible TMR redundancy, when a component fails, it automatically reconfigures the redundancy structure and, accordingly, the voting policy of the input/output and application tasks should be changed as shown in Fig. 3.

4. RELIABILITY OF SPLC

As described in the previous section, since the redundancy of SPLC changes as a fault occurs, the reliability of overall controller should be analyzed with considering this redundant mode changes. With reflecting this failure mode change of the flexible TMR model, the Fault Tree Analysis(FTA) chart of SPLC is shown in Fig. 5. In the chart, system state are classified into four categories: Total Success(TS), Minimum Anticipated Failure(MAF), Maximum Tolerable Failure(MTF), and Complete Failure(CF). For example, since the processor module is configured as the TMR, if one processor module fails, it goes to the MAF state. If two processor modules fail, system state falls into the MTF state because further failure causes the system failure(CF). The state transition in the FTA-tree is caused by a failure occurred in each module(processor, I/O card, bus, etc). Assuming these failures are independent, this state transition can be modeled as a Markov process. Fig. 6 shows the state transition of SPLC to the failure occurs and the probability of each state transition, $P_{MAF}, P_{MTF1}, P_{MTF2}$, and P_{CF}, depends on the redundancy structure and model. Using these probability values, the reliability of overall system is calculated as in (1).

$$\begin{aligned} R(t) = {} & (1 - P_{MAF} - P_{MTF1})R_{TS}(t) \\ & + (P_{MAF} - P_{MTF2})R_{MAF}(t) \\ & + (P_{MTF1} + P_{MTF2} - P_{CF})R_{MTF}(t) \\ & + P_{CF}R_{CF}(t) \end{aligned} \tag{1}$$

Based on the actual failure rate of each component module, such as the processor module, communication module, I/O modules, and etc, the probability of state transition is calculated as in (2). The earlier author's work showed the details of the failure rate and the FTA analysis results(Noh et al. (2013)).

$$\begin{aligned} R(t) = {} & 0.999953 \cdot R_{TS}(t) - \{3.92 \cdot R_{MAF}(t) \\ & + 3.92 \cdot R_{MTF}(t) + 4.70 \cdot R_{CF}(t)\} \times 10^{-5} \end{aligned} \tag{2}$$

By integrating (2), the Mean Time To Failure(MTTF) of SPLC is calculated as 41,630 hours that is about 97%

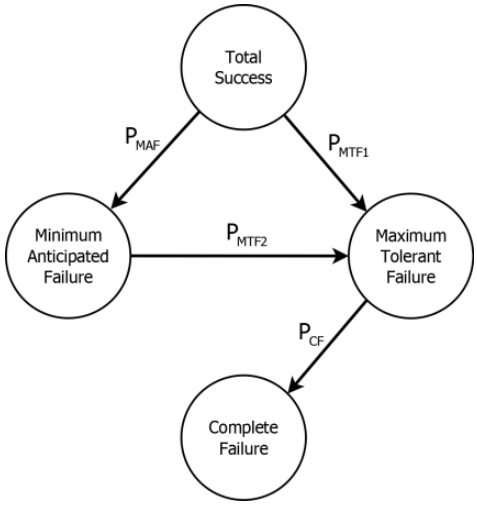

Fig. 6. State Transition

longer than the commercially used controller with the DMR architecture. Moreover, the reliability of SPLC is 0.84 as shown in Fig. 7 after 18 months(≈13,000 hours) that is the normal overhaul period to the regulations in the nuclear power industry. Compare to that of the TMR and DMR architectures, it is about 15% and 50% more reliable, respectively. Detailed calculation can be found in the author's earlier work(Son et al. (2013)).

5. CONCLUSION

This paper presents the redundancy architecture of the Programmable Logic Controller for safety functions in a nuclear power plant. The Safety PLC (SPLC) aims for the safety critical functions such as reactor protection in a Nuclear Power Plants. The architecture of the SPLC is designed to flexibly switch the redundancy model between the Dual Modular Redundancy(DMR) and Triple Modular Redundancy(TMR). Using this flexible redundancy architecture, the controller can be optimally configured to the application area and the reliability and availablity of overall system can be increased because redundancy model varies as failures occur. The operating system of the SPLC is designed to have the non-preemptive state based scheduler and the supervisory task managing the sequential scheduling, timing of tasks, diagnostic, and security to guarantee strict real-time operation. The reliability analysis results show that MTTF of SPLC is 44,000 hours, that is about 15% and 50% more reliable compare to the DMR and TMR architecture, respectively. Also to ensure the deterministic and high transmission capacity of the data communication, the network is designed to have the deterministic state-based protocol and effective transmission capacity of 20Mbps using a high switching device.

ACKNOWLEDGEMENTS

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

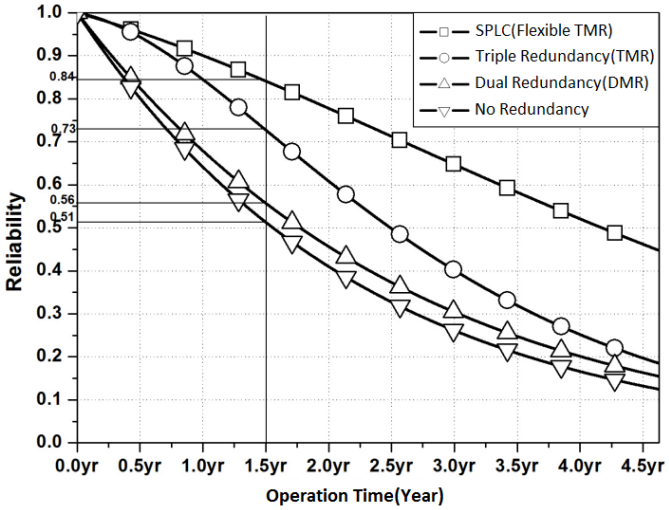

Fig. 7. Reliability

REFERENCES

ABB (2001). *Product guide: Advant controller 160, ver. 1.3*.

Cha, K., Kim, J., Lee, J., Cheon, S., and Kwon, K. (2006). Software qualification of a programmable logic controller for nuclear instrument and control applications. In *Proceedings of the 6th WSEAS International Conference on Applied Informatics and Communications*, 353–358. WSEAS.

Dorr, R., Kratz, F., Ragot, J., Loisy, F., and Germain, J.L. (1996). Detection, isolation, and identification of sensor faults in nuclear power plants. *IEEE Trans. Control Syst. Technol.*, 5(1), 42–60.

Dwyer, V.M. (2012). Reliability of various 2-out-of-4:g redundant systems with minimal repair. *IEEE Trans. Rel.*, 61(1), 170–179.

IEEE (1994). *IEEE Std. 7.4.3.2: Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*. IEEE, New York, USA.

IEEE (2011). *IEEE Std. 802.15.4: Standard for Local and metropolitan area networks - Part 15.4: Low-Rate Wireless Pernonal Area Networks (LR-WPANs)*. IEEE, New York, USA.

Invensys Systems Inc. (2007). *Tricon V10 hardware manual*.

Jiang, J. and Yu, X. (2012). Fault-tolerant control systems: A comparative study between active and passive approaches. *Annual Reviews in Control*, 36, 60–72.

Kim, H.S., Lee, J.M., Park, T., and Kwon, W.H. (2000). Design of networks for distributed digital control systems in nuclear power plants. In *International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies (NPIC&HMIT 2000)*.

Koubaa, A., Alves, M., and Tovar, E. (2006). GTS allocation analysis in IEEE 802.15.4 for real-time wireless sensor networks. In *20th International Parallel and Distributed Processing Symposium 2006*, 1–8. IEEE.

Kwon, K.C. and Lee, M. (2009). Technical review on the localized digital instrumentation and control systems. *Nuclear Engineering and Technology*, 41(4), 447–454.

Noh, J., Park, J., Son, K.S., and Kim, D.H. (2013). Development of the high reliable safety PLC for the

nuclear power plants. *J. of Inst. of Control, Robotics, and Systems(in Korean)*, 19(4), 328–333.

PonuTech (2009). *Product guide: POSAFE-Q Controller, ver. 1.0*.

Son, G.S., Kim, D.H., Son, C.W., Kim J.K., and Park J. (2013). Design of SPLC Architecture Used in Advanced Nuclear Safety System and Reliability Analysis Using Markov Model *Nuclear Technology*, 184(3), 297–309.

Sul, J., Kim, K., Kim, Y.S., and Park, J. (2012). Implementation of high-reliable MVB network for safety system of nuclear power plant. *The Transactions of The Korean Institute of Elecrical Engineers*, 61(6), 859–864.

Yoo, S.E., Chong, P.K., Kim, D., Doh, Y., Pham, M.L., Choi, E., and Huh, J. (2010). Guaranteeing real-time services for industrial wireless sensor networks with IEEE 802.15.4. *IEEE Trans. Ind. Electron.*, 57(11), 3868–3876.