Implementation of a RPS Cyber Security Test-bed with Two PLCs

Jinsoo Shin [a], Gyunyoung Heo [a], Hanseong Son [b*], Yongkyu An [c], Rizwan-uddin [c]
[a]*Department of Nuclear Engineering, Kyung Hee Univ., 1732 Deogyeong-daero, Yongin-si, Gyeonggi-do, Republic of Korea*
[b]*Computer and Game Science, Joongbu Univ., 201 Daehak-ro, Geumsan-gun, Chungnam, Republic of Korea*
[c]*Nuclear, Plasma, and Radiological Engineering, University of Illinois at Urbana-Champaign, Urbana, Illinois-61804, USA*
[*]*Corresponding author: hsson@joongbu.ac.kr*

1. Introduction

Cyber security issue has come to the fore in the field of nuclear power since the use of digital equipment has become inevitable. Many studies are being conducted on cyber security for nuclear facilities, analyzing cyber threat information and vulnerability of nuclear power instrumentation and control (I&C) system [1]. Our research team proposed the methodology to evaluate cyber security with Bayesian network (BN) as a cyber security evaluation model and help operator, licensee, licensor or regulator in granting evaluation priorities [2]. The methodology allowed for overall evaluation of cyber security by considering architectural aspect of facility and management aspect of cyber security at the same time. In order to emphasize reality of this model by inserting true data, it is necessary to conduct a penetration test that pretends an actual cyber-attack. Through the collaboration with University of Illinois at Urbana-Champaign, which possesses the Tricon a safety programmable logic controller (PLC) used at nuclear power plants and develops a test-bed for nuclear power plant [3], a test-bed for reactor protection system (RPS) is being developed with the PLCs. Two PLCs are used to construct a simple test-bed for RPS, bi-stable processor (BP) and coincidence processor (CP). By using two PLCs, it is possible to examine cyber-attack against devices such as PLC, cyber-attack against communication between devices, and the effects of a PLC on the other PLC.

2. Methods and Results

The objects of the test-bed and the Tricon are described in section 2.1 and section 2.2. The implementation of logics with the Tristation 1131 and the advantages of the test-bed and its application for the BN model are explained in section 2.3 and section 2.4, respectively.

2.1 BP and CP

RPS, one of safety systems of nuclear facilities, is the target of this model. The reason for selecting RPS as the target of cyber security test-bed is as follows. When a nuclear facility such as nuclear power plants is assumed to experience a cyber-attack, control system of the nuclear facility would be attacked, as well as critical safety systems that maintain safety of the facility when the facility becomes abnormal from attack against control system [4]. If RPS among safety systems is attacked, the facility cannot be shut-down and engineered safety features actuation system (ESFAS) signals generated by RPS can no longer operate properly. This can lead to a desirable situation for cyber-attackers. Based on this assumption, cyber security test-beds must be created for both control system and RPS system. In this study, the test-bed was first developed for RPS as a demo version.

RPS consists of BP, CP, ITP (interface and test processor) and MTP (maintain and test processor) [5]. BP has a function of sending trip information to CP when a signal that exceeds the set-point is generated. CP receives trip information from BP of various channels, evaluates this information using coincidence logic. ITP checks abnormality of devices by checking status of BP and CP, and MTP has an OS installed so that worker can perform work on RPS during maintenance time. ITP and MTP have no direct correlation with tripping of reactor. In this study, BP and CP which have direct correlation with reactor trip were selected to construct cyber security test-beds.

2.2 Tricon

The Tricon is used widely for emergency shutdown system (ESD), burner management system (BMS), fire and gas system (F&G) and turbo machine control. Tricon is a type of PLC used for 1E safety system at nuclear power plants. It is used as BP and CP of RPS. For safety purpose, tricon is based on Triple-Modular Redundant (TMR) architecture [6]. TMR uses three isolated parallel control system and a wide diagnostic function integrated with a system. Tricon uses triple time redundancy technique to provide high integrity, zero error and continuous process operation. No single point shows failure or error, and it is operated as a single control system from user perspective. Application setting for tricon is simple. A wide diagnostic function is internalized so that programmer can easily identify error, and diagnostic information is saved as system variables and provided to users.

The Tricon that uses TMR approach has the following advantages. 1) Extremely high safety integrity: As defined in emergency safety shutdown and functional safety standard, IEC 61508, tricon system can be used with applications that require safety integrity level 1, 2 or 3. 2) High availability: It can be operated with one, two or three functional main processors, and the system can be controlled without stopping when a module shows failure because the module can be replaced during system operation. 3) Low maintenance cost: Internal comprehensive diagnostic function accurately identifies error position to assign replaceable module.

Tricon used in this study has three main processors, one analog input / output, one digital input / output, and one communication module.

2.3 Implementation

Tristation 1131 with function block diagram was used to constitute logic of Tricon. One PLC was used as BP to have a logic that determines trip signal. Each signal determining trip was allowed to have digital signal of 1~5 volts, and the logic was made to generate abnormal signal when the value is larger or smaller than set-point like Fig. 1.

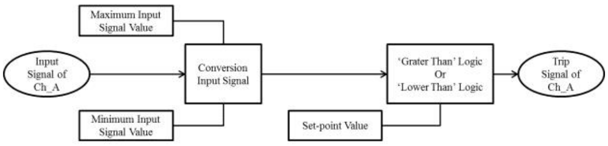
Maximum Input Signal Value
Input Signal of Ch_A
Conversion Input Signal
Minimum Input Signal Value
'Grater Than' Logic Or 'Lower Than' Logic
Set-point Value
Trip Signal of Ch_A

Fig. 1. BP logic of channel A for RPS in Tricon with Tristation 1131

CP is a logic that receives abnormal signal from BP and determines trip. Digital I&C was reflected to create a separate logic for each signal to perform independent calculation like Fig. 2.

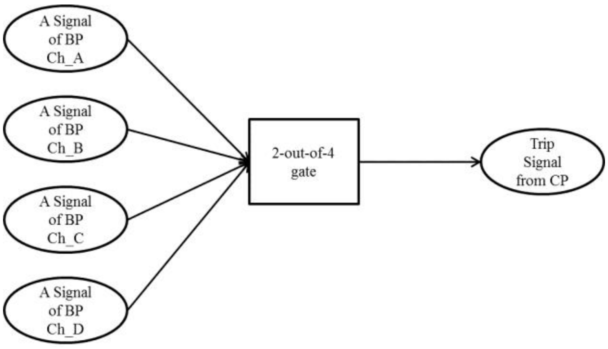

Fig. 2. CP logic of channel A for RPS in Tricon with Tristation 1131

PLC used in nuclear facilities, especially in critical class systems, maintains safety by TMR configuration. Safety is discussed on the technical level, but actual penetration test needs to find out the degree to which PLC can withstand cyber-attack. There are many teams that use such equipment to construct cyber test-beds and attempt penetration test about cyber-attack [7-8]. However, the focus of their research is on cyber security of an independent I&C devices and cyber security of entire nuclear power plant. Test-bed embodied using one PLC may be desirable for examining reliability of device from micro perspective, but it is somewhat inadequate for finding the effects of device that received cyber-attack on another device. Also, test-bed embodied for the entire power plant can examine the effects on the power plant from macro perspective, but extremely large down-scale of category can reduce reality in finding the effects among devices. This study attempts to construct cyber test-beds reflecting characteristics of devices that reflect correlation among devices and to obtain true data through penetration test.

2.4 Application to the BN model

True data about cyber-attack obtained from this penetration test-bed developed using two PLCs will be applied to the cyber security evaluation model.– The RPS model consists of two PLCs and two work stations, and it imitates fiber cable connection with other channels. This model was developed using BN to evaluate risk by considering architectural aspect of RPS and management aspect of cyber security at the same time [9]. NPT (node probability table) that shows relationship among nodes currently has default expert values, and the model is expected to become better suited for the site by adding true data obtained from penetration test.

3. Conclusions

Two PLCs were used to construct a test-bed for penetration test in this study. Advantages of using two or more PLCs instead of single PLC are as follows. 1) Results of cyber-attack reflecting characteristics among PLCs can be obtained. 2) Cyber-attack can be attempted using a method of attacking communication between PLCs. 3) By connecting two PLCs, the effects of attacking a PLC on the other PLC can be examined.

The scope of the test-bed embodied in this study was limited to penetration test, but true data will be obtained through a future study. True data obtained can be applied to existing cyber security evaluation model to emphasize reality of the model. They can also help reviewer or evaluator during cyber security evaluation on nuclear power facilities to decide priorities of evaluation.

Acknowledgement

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (MSIP) (Grant Number: NRF-2011-0031773)

REFERENCES

[1] J. G. Song, J. W. Lee, G. Y. Park, K. C. Kwon, D. Y. Lee, and C. K. Lee, An Analysis of Technical Security Control Requirements for Digital I&C Systems in Nuclear Power Plants, Nuclear Engineering and Technology, Vol.45, pp. 637-652, 2013.

[2] J. S. Shin, H. S. Son, and G. Y. Heo, Application of Bayesian Network Methodology for Evaluating Industrial Control System, Advanced Science and Technology Letters Vol.42, pp. 157-161, 2013.

[3] Y. An, C. Sollima, R. Uddin, D. Chen, Z. Kalbarczyk, T. Yardley, and W. Sanders, A Test Bed for Digital I&C and Cyber Security for NPPs, 9th International Topical Meeting on Nuclear Plant Instrumentation, Control & Human-Machine Interface Technologies (NPIC&HMIT), pp. 2496-2502, 2015

[4] S. Authen, J. E. Holmberg, Reliability Analysis of Digital Systems in a Probabilistic Risk Analysis for Nuclear Power Plants, Nuclear Engineering and Technology, Vol.44, pp. 471-482, 2012.

[5] D. Y. Lee, J. G. Choi, and J. Lyou, A Safety Assessment Methodology for a Digital Reactor Protection System, International Journal of Control , Automation, and Systems, Vol.4, pp. 105-112, 2006.

[6] Invensys Operations Management, Topical Report 7286-545-1, Revision 4, Triconex Topical Report, 2010.

[7] S. Merat, and W. Almuhtadi, Cyber-awareness Improvement using Artificial Intelligence Techniques, International Journal on Smart Sensing and Intelligent Systems, Vol.8, pp.620-636, 2015

[8] J. G. Song, J. W. Lee, C. K. Lee, K. C. Kwon, and D. Y. Lee, A Cyber Security Risk Assessment for the Design of I&C System in Nuclear Power Plants

[9] J. S. Shin, H. S. Son, and G. Y. Heo, Development of a Cyber Security Risk Model using Bayesian Networks, Reliability Engineering & System Safety, Vol.134, pp. 208-217, 2015.