Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 24-26, 2012

A Study of PLC System Vulnerability Checklists in Nuclear Power Plants

Kijong Cha [a*], Giho Cho[a] , Jaehyoung Ahn[a], Youngmi Kim[b], Yongil Kwon[b]
[a] *Nuclear Safety Evaluation Ltd., 507 Convergence technology Research Commercialization Center,*
218 Gajeong-ro, Yuseong-gu, Daejeon, 305-700, Rep.of Korea
[b] *Korea Institute of Nuclear Safety, 62 Gwahak-ro, Yuseong-gu, Daejeon, 305-338, Rep.of Korea*
[*] *Corresponding author: kjcha@nse.re.kr*

1. Introduction

Because the design of the PLCs (Programmable Logic Controller) in the I&C (Instrument & Control) systems for NPP (Nuclear Power Plant) were carried out independently, the problems of cyber security were not addressed in the PLC system designs.

Recently, the analysis and the countermeasure development for the PLC systems became mandatory due to the developments in cyber-attack techniques and the increasingly revealed vulnerability to such attacks.

A comparative analysis on the cyber security checklist of PLC in industry control system and in NPP systems was carried out, and in this paper, the cyber security regulatory trend and the PLC usage status are described.

2. Cyber Security Regulatory Trend and PLC usage status in NPP System

2.1 Cyber Security Regulatory Trend

After the terrorist events of 9/11, the NRC (Nuclear Regulatory Commission) issued an advisory to power reactor licensees to enhance cyber security and mandated the power reactor licensees to implement Interim Compensatory Measures.

In 2010, the NRC published 10 CFR 73.54, “Cyber Security Regulation”, 2009 and RG 5.71 “Cyber Security Programs for Nuclear Facilities”.

Recently, the NRC amended RG 1.152 “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants” Rev. 3 so that it now requires “Secure Development Environment”[1][2].

In December 2011, the IAEA (International Atomic Energy Agency) published IAEA Nuclear Security Series NO. 17, “Computer Security at Nuclear Facilities”.

In 2007, the KINS (Korea Institute of Nuclear Safety) published KINS/GT-N27 “Cyber Security of Instrumentation and Control Systems in Nuclear Facilities”.

In 2011, the WG-NICCS (Working Group on Nuclear I&C Cyber Security) published KINS/ER-199 “Nuclear I&C Cyber Security Comprehensive Measures Technical Report”.

At present, depending on the Nuclear I&C Cyber Security Comprehensive Measures, WG-NICCS is carrying out a study on the detailed implementation and enforcement measures [3].

2.2 PLC usage status in NPP System

Digital systems have been used in non-safety equipment from South Korea’s first commercial NPP, Kori No.1, to later units such as YGN No. 1·2.

Beginning from YGN No. 3·4, Digital systems are also used in the protection and control systems.

In particular, PLC systems are used in the system responsible for the safety of NPP systems, and Shin Ulchin No.1·2, recently constructed nuclear plants, use the POSAFE-Q PLC in the protection and control systems. Table I shows the digital system usage status in NPP systems in Korea.

Table I: Digital system usage status in NPP

	Protection Systems	Control Systems
Kori No.1		DCS(Turbine Con.)

Kori No.1
(Upgraded in 1998)
		Spec200(Foxboro)
		DCS(Turbine Con.)

Kori No. 2, 3, 4 YGN No. 1, 2		Mark V(GE)

YGN No. 3, 4	CCC 3205
	(CPCS)
		Spec200(Foxboro)
		ILS(Forney)
		Mark V(GE)

Ulchin No. 3, 4
YGN No. 5, 6
	CCC 3205
	(CPCS)
		Spec200(Foxboro)
		PCS(Eaton)
		Mark V(GE)

Ulchin No. 5, 6	PLC(ABB-CE)
	CCC 3205
	(CPCS)
		Spec200(Foxboro)
		PCS(Omron, HFC)
		Mark VI(GE)

Shin Kori No. 1, 2
Shin Wolsong No. 1, 2
	PLC(ABB-CE)	Spec200(Foxboro)
		PCS(HFC),
		Ovation(W/H)
		Mark VI(GE)

Shin Kori No. 3, 4	PLC(ABB-CE)	PCS(ABB-CE)
		Ovation(W/H)
		Mark VI(GE)

Shin Ulchin No. 1, 2	PLC(Posafe-Q)	DCS (Woori Tech. INC) PLC(Posafe-Q) Mark VI(GE)

3. Cyber Security Checklists for PLC

3.1 Checklists on Industry Control Systems

Project basecamp performed the penetration tests based on 8 checklists [4].

- ✓ Upload/Download ladder logic.
- ✓ Spoof authentication/replay configuration.
- ✓ Upload custom firmware.

- ✓ Basic fuzz-testing.
- ✓ Backdoors.
- ✓ Undocumented functionality/ protocols.
- ✓ Web server vulnerabilities.
- ✓ Resource exhaustion attacks.

3.2 Checklists on the standard of Industry Control systems

30 vulnerability checklists are listed in NIST SP800-82 "Guide to Industrial Control Security" issued by the NIST (National Institute of standard and Technology) [5]. We analyzed the checklists for PLC of Vulnerability Checklist and the results are as follows.

- ✓ Platform composition: Lack of adequate password policy.
- ✓ Platform Software: No password used, Password disclosure, Denial of Service, Error handling of non-normal condition, Use of clear text, inadequate access controls applied.
- ✓ Network: Absence of authentication for data and equipment, Lack of integrity checking for communication.

3.3 Checklists on NPP Control System

RG 5.71, written based on NEI 08-09, presents 71 vulnerability checklists in five different items [6]. We analyzed the Checklists for PLC of Vulnerability Checklist and the results are as follows.

- ✓ Access Controls : Access control policy and procedure, Unsuccessful login attempts, Session locking, Permit the identification and authentication actions, Unidentifiable access, Use of external system
- ✓ Critical Digital Asset and Communications Protection : Critical Digital Asset and Communications Protection Policy and Procedures, Shared Resources, DoS Protection, Transmission Integrity, Transmission Confidentiality, Use of Cryptography
- ✓ Identification and authentication : Identification and Authentication Policies and Procedures, User Identification and authentication
- ✓ System Hardening : Removal of Unnecessary service and Programs, Operating System, Applications, Third –party Software Updates

3.4 Additional Checklists on Nuclear Control System

The checklists for PLCs in the protection systems in NPP are required for additional checklists as follows.

- ✓ Integrity of system check: As all devices on the nuclear power plant system are important components for safety, a large number of tests should be performed in the nuclear power plant systems during an operation to check the integrity of the systems. These tests involve the many features including automatic testing and self-diagnostic functions provided by the OS or the device. And, even when cyber violation occurs, the systems should show a normal operation.

- ✓ Mission time check: NPP systems have mission time requirements. Because safety analysis and safety evaluation is conducted on the basis of given mission time requirements, inspection activities should be conducted about mission time guarantee when the cyber violation occurred.

- ✓ Checking infringement propagation, etc.

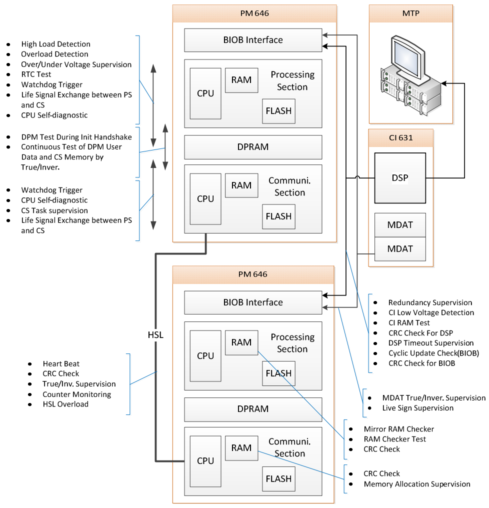

Fig. 1 Self-diagnosis Functions of PLC systems

4. Conclusions

In this paper, we describe cyber security regulatory trend and PLC usage status. We carried out a comparative analysis on the checklist for cyber security of PLC in industry control systems and in NPP systems.

However, as the technology evolves, the checklists for cyber security are changing constantly.

To enhance security of PLC in NPP systems, the security technology research and development suitable for environment of NPP systems is needed.

REFERENCES

[1] http://www.nrc.gov/about-nrc / regulatory / enforcement / safety-culture.html.
[2] REGULATORY GUIDE 5.71 CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES.
[3] KINS/ER-199 Nuclear I&C Cyber Security Comprehensive Measures Technical Report. 2011.
[4] http://www.digitalbond.com/tools/basecamp/.
[5] NIST SP 800-82-final Guide to Industrial Control System Security.
[6] NEI 08-09 Cyber Security Plan for Nuclear Power Reactors.