Study on the Position Enhancement for Cyber Security Organization of the Nuclear Facilities

Hyundoo Kim*

Korea Institute of Nuclear Nonproliferation and Control, 1534 Yuseong-daero, Yuseong-gu, Daejeon, Republic of Korea

*hdkim@kinac.re.kr

1. Introduction

The digital I&C systems and commercial programs adopted for the nuclear facilities are getting to be increased, compared with analog I&C systems and specifically private programs. Moreover, the trend of cyber threat is toward from individual attack to national scale attack by using special malware which is developed to attack the particular targeted system such as 'Stuxnet' in Iran, 'Energetic Bear' in U.S. and 'Black Energy' in Ukraine. In consequence of the trends, cyber threats and attacks can occur anywhere and at the any time.

2. Background of Cyber Security Organization

The Act on Physical Protection and Radiological Emergency, its enforcement decree and enforcement regulation were added or revised to enhance cyber security. Based on the laws, the Notice for details of Cyber Security Plan (CSP) was issued and KINAC's regulation standard, KINAC/RS-015 was developed to establish cyber security framework for the nuclear facilities against cyber threats and attacks.

Licensees planed 7 phases for the cyber security program to meet the Notice and KINAC's regulation standard and implement CSP. The 1st phase from among this plan is composition of cyber security organization and licensees have composited their cyber security organization since 2015.

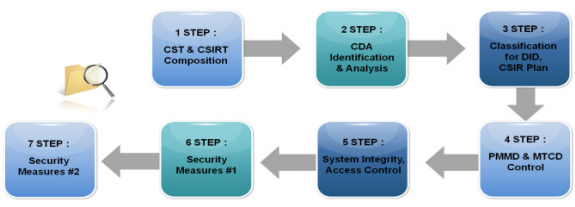

Fig. 1. Seven (7) Phases of the CSP.

3. Requirements for the QA organization

The cyber security organization for the nuclear facilities has been composited in accordance with CSP since 2015. But the requirements for the Quality Assurance (QA) organization have been studied and established for a long time and a lot of companies adopted and organized their QA team as one of Quality Assurance Programs, Plans or Activities.

3.1 Regulatory Guide 5.71

The Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities" in U.S. requires that licensees form a cyber security team (CST) including sponsor, manager and specialists by defining and documenting roles, responsibilities, authorities and functional relationships, which are detailed in the RG 5.71. The licensees' CST are required to have the authority to conduct an objective assessment, make determinations that are not constrained by operational goals, implement the defense-n-depth protective strategies and ensure the implementation of the security controls of the cyber security program [1].

3.2 KINAC/RS-015

The Regulation Standard KINAC/RS-015, "Security for Computer and Information of Nuclear Facilities" in ROK requires licensees to compose a CST with the sponsor, manager and specialists which is independent and separated from the system operation parties and define and document roles, responsibilities and authorities which are in KINAC/RS-015 [2].

3.3 ISO 9001

The International Standard ISO 9001, "Quality Management Systems – Requirements" requires that

the QA organization determine external and internal issues that are relevant to its purpose and its strategic direction and that affect its ability to achieve the intended result(s) of its quality management system. The organization also is required to determine the interested parties and the requirements of these interested parties that are relevant to the quality management system [3].

3.4 10 CFR 50 Appendix B

Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants" in Title 10, Code of Federal Regulations (CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities" requires that the persons and organizations performing QA functions have sufficient authority and organizational freedom including sufficient independence from cost and schedule to identify quality problems, to verify implementation of solutions and to report to a management level. Irrespective of the organizational structure, the individual assigned the responsibility for assuring effective execution of any portion of the QA program is required to have direct access to the levels of management necessary to perform QA function [4].

3.5 ASME NQA-1-1994

The American Society of Mechanical Engineers (ASME) committee on Nuclear Quality Assurance (NQA) through Basic Requirement 1, ASME NQA-1-1994 requires that the persons or organizations responsible for assuring that an appropriate QA program has been established and verifying that activities affecting quality have been correctly performed have sufficient authority, access to work areas, organizational freedom and direct access to responsible management at a level where appropriate action can be effected [5].

3.6 NUREG-0800

The Standard Review Plan (SRP) for the Review of Safety Analysis Reports for Nuclear Power Plants: Edition – Quality Assurance, NUREG-0800 Chapter 17 requires that licensees identify a management position that retains overall authority and responsibility for the QA program and this position has the following characteristics:

a. Is at the same or higher organization level as the highest line manager directly responsible for performing activities affecting quality such as engineering, procurement construction and operation and is sufficiently independent from cost and schedule.

b. Has effective communication channels with other senior management positions.

c. Has no other duties or responsibilities unrelated to QA that would prevent his full attention to QA matters [6].

4. Conclusion

The regulation requirements for the quality assurance organization of nuclear facility are more detailed, stronger and stricter than those for the cyber security organization. The Korea Institute of Nuclear Safety (KINS) applies, reviews and regulates above mentioned QA standards for the nuclear facilities to the Design and Construction Phases as well as the Operations Phase.

The regulation requirements for composing cyber security organization which is one of the security assurance activities should be further developed and strengthened.

REFERENCES

[1] U.S.NRC, Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities", January 2010.

[2] KINAC, Regulatory Standard KINAC/RS-015, Security for Computer and Information of Nuclear Facilities, October 2014.

[3] ISO, International Standard ISO 9001, "Quality Management Systems – Requirements", September 2015.

[4] U.S.NRC, https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-appb.html

[5] ASME, ASME NQA-1-1994 edition and 1995 addenda, "Quality Assurance Manual".

[6] U.S.NRC, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports on for Nuclear Power Plants: LWR Edition).