Cyber Security in digitalized nuclear power plants

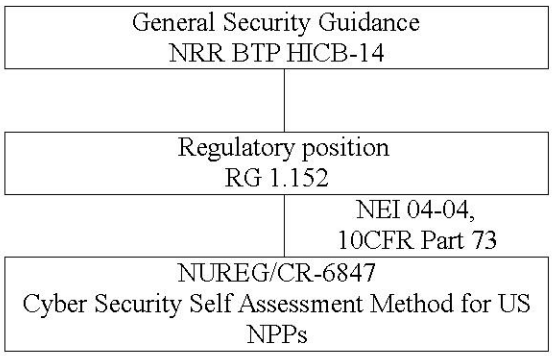
KwangYoung Sohn*, WooJune Yi
KoRTS Co. Ltd., 539-3 4fl. PyungChon-Dong DaeDuk-Ku Daejon Korea
kysohn@korts.co.kr, wjyi@korts.co.kr
SangYong Lee
SamChang Co. Ltd. Research Center, 974-1 KoYeon-Ri UngChon-Myeon UlJoo-Kun Ulsan Korea
lsy010@samchang.com

1. Introduction

This paper analyzes the cyber security issues pertaining to networks and general systems, and provides cyber security activity model. For this, the importance of security, and the domestic and international trends of cyber security are surveyed in order to introduce the strategies and countermeasures of cyber security which should be interfaced with Quality Assurance (QA) plan. Based on the result of cyber security model introduced in this paper, activities for cyber security, work load, necessary resources and process for activities, and duration could be estimated hopefully.

2. The trends in cyber security

The following is the international code and regulation approaches to cope with the cyber security for nuclear power plants.



In USA it is granted that there are malicious attacks and destructions for various control systems and protection systems. Thus they are trying to identify the weakness of the systems and set up the plans to cope with cyber threats. International Atomic Energy Agency (IAEA), Department of Homeland Security (DHS) and Department of Energy (DoE) are typical organizations establishing the various countermeasures against the cyber attacks. [3][7][8][9]

IAEA Draft Security Series classifies the I&C systems into zone-1 through zone-4 to apply the security plan for safe plant operation. Zone-1 is for the electro-technical systems and Instrumentation System, zone-2 for process-computing system, zone-3 for administrative computer system and zone-4 for external systems.

Nuclear Energy Institute (NEI) 04-04 [2], performed research through the contract with Pacific Northwest National Laboratory (PNNL) and NRC sponsorship, provides the five of cyber security model and trust levels. NRC performs the Digital System Research and established the documents for cyber security.

DHS and DoE [3] analyze the vulnerability of cyber threats and develop the procedure for cyber security. Also recently IEC organization is preparing the standard for cyber security as a separate issue [4].

Regulation guidance drafted by Korea Institute Nuclear Safety (KINS) [5] in 2006 is being revised based on the comments from the several organizations.

3. Security Characteristics and Target Classification

3.1 Cyber security for communication

All the communication connected between safety and non-safety systems could be a target of cyber security. Especially the remote access through the internet for the acquisition of the plant information and data, and the maintenance activities is the examples. Figure 1 indicates the layers of cyber security.

Modems and serial data links, one of the data communications including the IEEE 802.X series including wireless, Fieldbus, and others could be classified as a target for cyber security and they should be designed and maintained appropriately.

3.2 Platform Security

The targets of the platforms and countermeasures vary also. Putting an emphasis on the real-time and deterministic data processing in the platforms of the nuclear power plant, the functions and performance should not be affected by the security plans.

3.3 Human Security

Since one of the most important elements for security is a human. The element, a human, is the most important threats to intrude the computer systems. Thus human security which should be treated systematically according to the well defined procedure is an unlimited issue that could be overlooked.

3.4 Managerial Security

Managerial security is a total system security including the humans, the organizations, and procedures for the system operations and managements. Thus security activities considering internal and external human managements are closely related to the procedure for the system operation and Quality Assurance (QA) procedure.

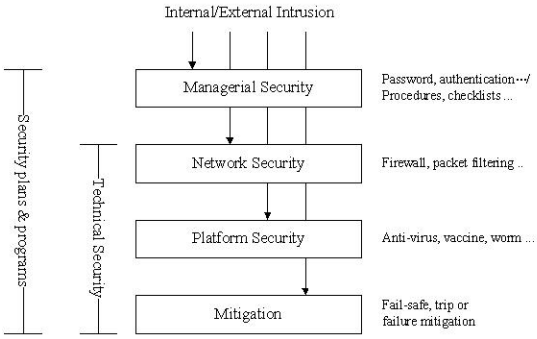


Figure 1 Hierarchical Countermeasure for cyber threats

4. Cyber Security for Nuclear Power Plants

According to the sources and targets of cyber attacks, we need to draw the security strategy and activity model for cyber security. Figure 2 indicates the activity model for cyber security in nuclear power plants.

5. Conclusion and Future Work

We remember the Y2K late in 1900s. we believe that nobody denies that the confirmation of the Y2K integrity for the plant I&C system is one of the contributions ensuring the plant safe operation. We should aware that Y2K is a transitional event in digitalized system, but cyber threats in digital plants are an ever-lasting threats while the plants is in operation.

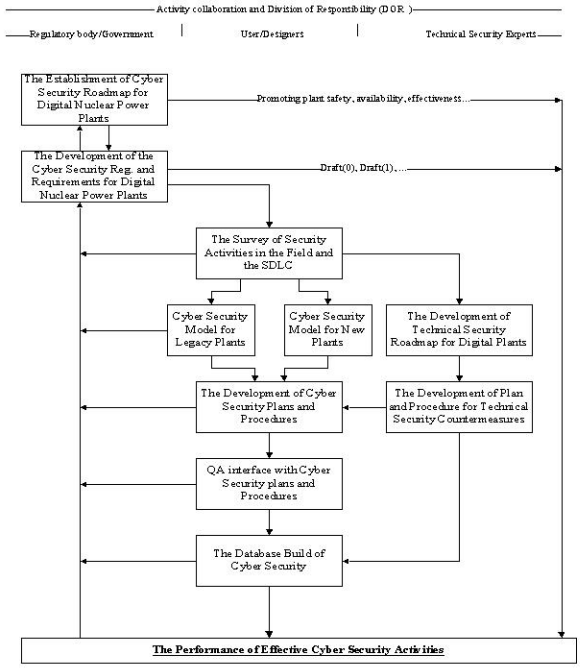


Figure 2 The Flow for Cyber Security Activity

References

[1] http://www.cromwell-intl.com/security/security-generalinfo.html

[2] Nuclear Energy Institute (NEI) 04-04, "Cyber Security Program for Power Reactors," Revision 1, dated November 18, 2005

[3] DOE &DHS, Roadmap to Secure Control Systems in the Energy Sector, Jan. 2006.

[4] Instrumentation and control systems important to safety - IEC 61500 Data Communication System

[5] Regulatory Guidance for Cyber Security in Digital I&C System, draft(02), KINS

[6] GMITS : Guidelines for the Management of IT Security), ISO/IEC, 1996

[7] GAO. 2004. Government Accountability Office. Critical infrastructure protection: Challenges and efforts to secure control systems (GAO-04-354). Washington, DC.

[8] The National Strategy to Secure Cyberspace, http://www.whitehouse.gov/pcipb

[9] Bush, President George W. 2003. Homeland Security Presidential Directive 7: Critical infrastructure identification, prioritization, and protection. Washington, DC. www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

[10] NRC Digital System Research plan, FY2005-FY2009, Instrumentation and Electrical Engineering Branch, Division of fuel, Engineering and radiological research office of nuclear regulatory research