Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, November 2-3, 2006

Regulatory Approach on Digital Security of I&C Systems in Nuclear Power Plants

Youngdoo Kang, Choong Heui Jeong, Dai I. Kim
Korea Institute of Nuclear Safety, Daejeon, Korea, k407kyd@kins.re.kr; k148jch@kins.re.kr; dikim@kins.re.kr;

1. Introduction

By force of the rapid development of digital computers and information processing technologies, it is being greatly switched to computer-based technologies over the whole industries including the nuclear power plants. In spite of such a rapid expansion of computer-based technologies, the application of these to nuclear power plants has raised many questions regarding their safety and reliability. And recently, new and deep concerns about the digital security of computer-based instrumentation, control and information systems in nuclear power plants are increased. These systems used in computer-based infrastructure have new and high amount of security vulnerabilities from external threats that can target digital systems and internal inadequacy. Far more serious can be the potential loss of production, equipment damage, personal injury, compromise to the safety of an operation, and also may have ramifications beyond the targeted facilities and they may grievously damage the public health and the infrastructure of the host region or nation [1]. So it is needed to formulate a structured set of guidelines and procedures of instrumentation, control and information systems in nuclear power plants to define digital security, requirement and methodologies to mitigate the effects from threats of the targeted digital systems.

The objective of this paper is to discuss the regulatory approach on digital security of instrumentation, control and information systems in nuclear power plants.

2. Regulatory Approach

The digital security is established with proper concept and analysis to the target. Well-defined security risk assessment shall be performed to determine the security level. With these, security policy and security procedures should be established for those systems.

2.1 Necessity and Concept

Currently, instrumentation and control systems in nuclear power plants mainly consisted of individual, isolated computer with proprietary operating systems and networks. However, the designer and licensee tries to change this situation towards highly interconnected systems and applications employing widely used information technology such as Microsoft Windows and standard network protocols. Furthermore, virtual integrated communication between safety systems and non-safety systems such as Plant Information Systems is designed to apply the nuclear power plant for several reasons, e.g., ease of operation or economical benefits. However, this may increase the security vulnerabilities to the safety systems and in that case of the loss of availability would be happened to the safety systems which are caused from threat; it may bring significant consequences to the facilities and also to the public health. Inappropriate security aspect through the whole life time of digital systems may also cause a significant failure to the systems.

2.2 Scope

It should be included the safety I&C systems and also the non-safety I&C systems for applying the digital security activities with considering the possibility and consequence from the digital vulnerabilities. The safety I&C systems have the function for the safety of nuclear power plants and it should be guaranteed to perform their own function. So the safety I&C systems should be classified to apply the security requirements. And recently, safety I&C systems are designed with digital technologies and they are interconnected with the non-safety systems via communication networks. They send safety critical information to the non-safety systems such as plant monitoring and alarm systems. That should be one-way direction, but there still exist the possibility to penetrate the threat from non-safety systems. That may cause the event to the safety systems. And for guarantee the reliable and safe operation, non-safety I&C systems should be perform their own functions during normal condition without intrusion upon digital vulnerabilities. So, the non-safety I&C systems should be classified to apply the security requirements. And the measurement and test equipment, maintenance tools, development and configuration tools are also the classified.

2.3 Security Risk Analysis

It should be analyzed the security risk to the arranged systems for applying the security requirements. For the security risk analysis, it needs to assess each system with combination of the function, interconnection with other system, hardware types and configuration, operating and application software, communication protocols, etc,. The results of security risk analysis help to establish the security level and the Security Policy. Qualitative and quantitative analysis can be implemented for that analysis. Qualitative security risk analysis result can be the basis for estimation of the level of risk with vulnerabilities, threats and the consequences from loss of the security properties. With the results, consequence level and potentiality level can be identified of the vulnerabilities and threat.

2.4 Security Level

The results of the security risk analysis are the basis to expose specific vulnerabilities of the systems and to define the consequence level and potentiality level from threat. The consequence level is defined the severity of the systems following the threat. And the potentiality level is defined the frequency of the systems from the threat.

With the above two classification of level, the graded security level should be defined for applying the security activities to the targeted systems. Below table 3 shows the recommended graded security level.

Table 1. Graded Security Level

	C1	C2	C3	C4
P1	Security level A	Security level A	Security level B	Security level C
P2	Security level A	Security level A	Security level B	Security level C
P3	Security level A	Security level B	Security level C	Security level D
P4	Security level A/B	Security level C	Security level D	Security level D

The security level A requires the highest level of security to the systems because the potentiality from threats is higher and the consequences to the systems would be severe. On the contrary, the security level D requires the lowest level of security to the systems because the potentiality from threat is lower than the others and the anticipated consequences would be not severe to the systems. Following the above grades security level, the licensee should establish a typical approach for each security level and the systems should be applied the defined security activities throughout the whole life cycle.

2.5 Security Policy and Procedures

The vendor and licensee of digital I&C systems in nuclear facilities should establish the Security Policy of digital instrumentation, control and information systems for applying the security activities throughout the life cycle. The Security Policy is the root document with the purpose, scope, requirement, responsibilities, and exceptions for various subjects relevant for system security. Security Policy is a formal statement of what will and will not be done by persons and systems within an organization. It should contain the methodologies for risk analysis, audit, training, logging, and responses. Periodic software patch can be involved to that. And the vendor and licensee should establish the security procedures to implement the security activities throughout the life cycle. The security procedures should include the specific items to implement. It should be in accordance with the Security Policy.

3. Conclusion

Computer-based instrumentation, control and information systems in nuclear power plants should be secure to ensure the integrity of safety and reliability against the digital threats. This paper suggests the regulatory guidance and recommendation for applying the digital security to the computer-based nuclear instrumentation, control and information systems. It would be helpful to the licensee and vendor to establish a proper security goals and requirements for their systems.

As the contents in this paper, the regulatory agency of Korea, KINS, is in progress to publish the digital security guidance of instrumentation and control systems in nuclear power plants.

REFERENCES

[1] ISA-TR99.00.01-2004, Security Technologies for Manufacturing and Control Systems, March 2004

[2] ISA-TR99.00.02-2004, Integrating Electronic Security into the Manufacturing and Control Systems Environment, April 2004

[3] IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety – general requirements for systems, 2001

[4] IEEE Std. 7-4.3.2-2003, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

[5] U.S NRC Regulatory Guide 1.152, Rev.2, Criteria for use of computers in safety systems of nuclear power plants, January 2006.

[6] NIST SP 800-64, Rev.1, Security Considerations in the Information System Development Life Cycle, June 2004