원전 계측제어시스템의 사이버보안 요구사항

강영두[*], 정충희[*], 정길도[**]
한국원자력안전기술원[*], 전북대학교 전자정보공학부[**]

Introduction of Requirements and Regulatory Guide on Cyber Security of I&C Systems in Nuclear Facilities

Youngdoo Kang[*], Choong-Heui Jeong[*], Kilto Chong[**]
Korea Institute of Nuclear Safety[*], Chonbuk National University[**]

Abstract - In the case of unauthorized individuals, systems and entities or process threatening the instrumentation and control systems of nuclear facilities using the intrinsic vulnerabilities of digital based technologies, those systems may lose their own required functions. The loss of required functions of the critical systems of nuclear facilities may seriously affect the safety of nuclear facilities. Consequently, digital instrumentation and control systems, which perform functions important to safety, should be designed and operated to respond to cyber threats capitalizing on the vulnerabilities of digital based technologies. To make it possible, the developers and licensees of nuclear facilities should perform appropriate cyber security program throughout the whole life cycle of digital instrumentation and control systems.

Under the goal of securing the safety of nuclear facilities, this paper presents the KINS' regulatory position on cyber security program to remove the cyber threats that exploit the vulnerabilities of digital instrumentation and control systems and to mitigate the effect of such threats. Presented regulatory position includes establishing the cyber security policy and plan, analyzing and classifying the cyber threats and cyber security assessment of digital instrumentation and control systems.

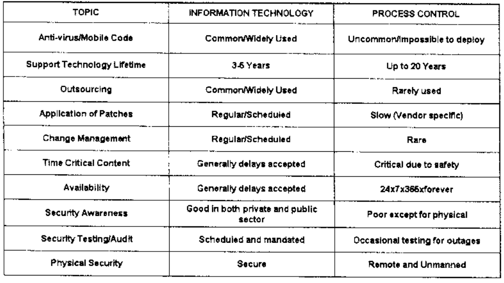
1. Nuclear Instrumentation and Control Systems Uniqueness

The Information Technology (IT) security threat environment is a fast changing, evolving scenario. Protection against the most prevalent malicious exploits at the present time, does not guarantee protection versus tomorrow's exploits.

For considering the cyber security of Instrumentation and Control Systems (I&C systems), it should be noted that many of cyber threats are from IT (Information Technology) fields. I&C systems had little resemblance to traditional IT systems in that I&Cs were isolated systems running proprietary control protocols using specialized hardware and software. Widely available, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of cyber security vulnerabilities and incidents. As I&C systems are adopting IT solutions to promote corporate connectivity and remote access capabilities, and are being designed and implemented using industry standard computers, operating systems (OS) and network protocols, they are starting to resemble IT systems. This integration supports new IT capabilities, but it provides significantly less isolation for I&C systems from the outside world than predecessor systems, creating a greater need to secure these systems. [5]

However, this may increase the vulnerabilities to the safety systems, and in that case of loss of availability would be happened to the safety systems which are caused from cyber threat. That may bring significant consequences to the facilities and also to the public health. Following to this brief case, the need to secure the digital I&C systems from cyber threats is increased as a point of safety of nuclear facilities. The cyber security program should be performed to meet confidentiality, integrity and availability criteria.

<TABLE 1> Differences between IT and I&C (security aspect)



TOPIC	INFORMATION TECHNOLOGY	PROCESS CONTROL
Anti-virus/Mobile Code	Common/Widely Used	Uncommon/Impossible to deploy
Support Technology Lifetime	3-5 Years	Up to 20 Years
Outsourcing	Common/Widely Used	Rarely used
Application of Patches	Regular/Scheduled	Slow (Vendor specific)
Change Management	Regular/Scheduled	Rare
Time Critical Content	Generally delays accepted	Critical due to safety
Availability	Generally delays accepted	24x7x365xforever
Security Awareness	Good in both private and public sector	Poor except for physical
Security Testing/Audit	Scheduled and mandated	Occasional testing for outages
Physical Security	Secure	Remote and Unmanned

1.2 Key Attributes for Cyber Security of I&C Systems in Nuclear Facilities

Confidentiality is the property that sensitive information is not disclosed to unauthorized individuals, entities or process. In many cases,

Integrity is the property that sensitive data have not been modified or deleted in an unauthorized and undetected manner.

Availability is the property of timely, reliable access to information by authorized entities.

Protecting the above confidentiality, integrity and availability (C.I.A) attributes of electronic data or computer systems including processes and procedures for prevention, detection, response and mitigation or recovery from potential computer security events.

2. Regulatory Position

This paper presents the regulatory position on cyber security program of I&C systems as below. Each should be implemented throughout the whole life cycle of I&C systems.

- Targets of cyber security program
- Establishment of cyber security policy and plans
- Cyber threat analysis
- Cyber security assessment
- Implementation of cyber security program

2.1 Targets of Cyber Security Program

One is safety I&C systems and the other is non-safety. Safety I&C systems are relied upon to remain required functional during and following design basis event. Reactor Protection Systems and Engineered Safety Feature Actuation Systems are classified in safety systems. Non-safety I&C systems are those which do not have the safety function during and following design basis event but have the function for operating the nuclear power plants such as NSSS Control Systems and Plant Computer Systems.

To classifying the target systems of cyber security in nuclear facilities, those systems should be classified into the target systems of cyber security program(TCS) under the goal of ensuring the safety of nuclear facilities.

- Instrumentation and control systems that perform safety functions
- Digital equipment to develop, analyze and evaluate instrumentation and control systems that perform safety functions

For I&C systems and equipments other than the above, though all the cyber security program required in regulatory guide are not required, cyber threat assessment should be performed in order to guarantee that there is no effect or possibility to the safety functions from systems and equipments which are not classified into the TCS. One of reason is, safety I&C systems are currently designed to have interconnection with non-safety I&C systems via communication networks. Those send safety critical information to the non-safety systems such as Plant Monitoring Systems. That should be one-way communication. However, there still exist the possibility to penetrate the threat from non-safety I&C systems during maintenance period. And except for the regulatory aspect, non-safety I&C systems are critical to the licensee, so the non-safety I&C systems should perform their own functions during normal operation to ensure the safe operation.

2.2 Establishment of Cyber Security Policy and Plans

The developers and licensees of digital I&C systems should establish a Cyber Security Policy (CSP), which is the highest level of document, for performing the cyber security program related to digital I&C systems. The CSP should define the cyber security control items for all I&C

systems of nuclear facilities including the TCS. One thing that should be confirmed is that CSP only for the TCS is not effective to achieve the goals and is insufficient to respond to newly emerged cyber threats.

The CSP should specify the highest level of technical and managerial aspects with covering the purpose and responsibilities of cyber security of organization. Followings are items that can be included in the CSP established by the developers and licensees of the nuclear facilities.

- Cyber security organizations and personnel including roles and responsibilities
- Information classification and cyber security levels
- Access control and monitoring
- Communication network security
- Cyber security audit
- Physical security such as cabinet locks
- Cyber security incident response and awareness
- System development and maintenance
- Vulnerability analysis and periodic evaluation
- Other managerial and technical controls

2.3 Cyber Threat Analysis

To perform the cyber security program, the vulnerabilities of TCS should be analyzed and the cyber threats capable of exploiting the vulnerabilities should be defined. Furthermore, in order to ensure the defense in-depth and diversity of nuclear facilities and guarantee that there are no effects on safety, cyber threat should be analyzed for all of I&C systems including the TCS.

Cyber threat analysis includes;

- Analysis of the design/operation and maintenance characteristics of nuclear facilities
- Analysis of the cyber threats to the external environments of nuclear facilities
- Analysis of the interconnection between hardware and software configurations and between systems

The cyber threats to I&C systems of nuclear facilities, including the TCS could be classified into external and internal cyber threats.

2.4 Cyber Security Assessment

Cyber security assessment help to measure the degree of confidence one has that the managerial, technical and operational security measures work as intended to protect the system and the information it processes. Cyber security assessment should be periodically performed to ensure that security procedures are implemented properly, to ensure that classification guidance is effectively utilized, to ensure that security systems and security features operate as designed, and to monitor operational trends that indicate problems or future issues with information asset protection.

Cyber security assessments must be performed internally by facility security personnel (self-assessments), and can be performed externally by personnel from the regulatory authority and others.

Cyber Security risk assessment which is one part of cyber security assessment is a combination of threat, vulnerability and impact are identified and documented and appropriate protective controls are devised. It may endorse general risk management methodologies. It should be performed through possibility of threats (possibility level) and consequence (consequence level) that can affect to the safety of nuclear facilities for determining the best location to allocate resources. Vulnerabilities identified through the cyber security assessment should be eliminated with designing and implementing comprehensive technical and managerial controls for proper cyber security program. Risk is the chance of something happening that will have an impact on objectives. To identify, analyze, evaluate and treat the risks which are related to the cyber threats should be processed [4].

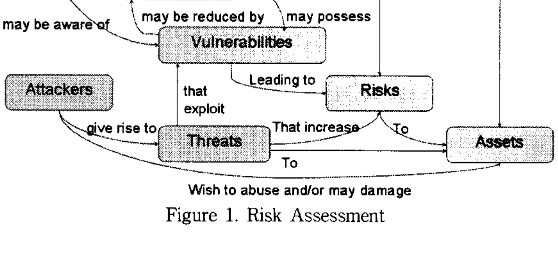


Figure 1. Risk Assessment

The threat and vulnerability assessment provides the basis for preparing the countermeasures required to prevent or mitigate the consequences of attacks against computer systems.

Considering the design/operation and maintenance characteristics of the TCS, cyber security assessment can be performed by assessment of hardware configuration, identification and verification of software, communication network scanning, analysis of software security guidelines, and assessment of interconnection characteristics with other systems.

Followings could be assessed:

- suitability of the cyber security policy and plans
- cyber security organization and management systems
- suitability of password management
- connection of communication networks and equipment
- suitability of information recording, storing and maintaining
- software integrity
- suitability of system development (including COTS)
- suitability of physical access
- periodic analysis/assessment and cyber security auditing

2.5 Implementation During Whole Life cycle

The cyber security program should be implemented according to the respective cyber security level to all of safety and non-safety I&C systems. Cyber security level is classified to ensure those program are implemented reasonably and properly according to the policy and requirements. The developers and licensees of nuclear facilities should represent that the cyber security level is established properly.

Followings can be included in the highest level of cyber security control items that the TCS should meet.

- multi-stage physical and cyber access control
  - · access control to the development environments
  - · prohibition of remote access
  - · one-way communication control signal (no handshaking)
- detection and protection of intrusion
- strict password management
- data integrity
  - · verification and validation for software integrity
  - · encryption methodology
- cyber security awareness and training
- periodic assessment
- high-level logging
- penetration tests through test-beds
- establishment of response systems
- strict cyber security audit

4. Conclusions

Under the goal of securing the safety of nuclear facilities, this paper presents the regulatory guide on cyber security activities to remove the cyber threats that exploit the vulnerabilities of instrumentation and control systems and to mitigate the effect from such threats. Presented regulatory position includes establishing the cyber security policy and plan, analyzing and classifying the cyber threats and cyber security assessment of digital instrumentation and control systems.

Further, this regulatory guide and position would be applied to retrofitting the nuclear I&C systems and new nuclear reactor constructions and operations. And for the more detailed regulation, quantitative cyber security risk assessment methodologies would be studied.

[References]

[1] Regulatory Guide, KINS/GT-N27, "Cyber Security of Instrumentation and Control Systems in Nuclear Facilities"

[2] ISO/IEC 27001, "Information technology - Security techniques - Information security management systems - Requirements"

[3] ISO/IEC 17799, "Information technology - Security techniques - Code of practice for information security management"

[4] U.S. NRC Regulatory Guide 1.152, Rev. 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" (2006)

[5] NIST SP800-82, "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security"