한국산학기술학회논문지
Vol. 11, No. 9 pp. 3451-3457, 2010

Development of Cyber Security Assessment Methodology for the Instrumentation & Control Systems in Nuclear Power Plants

Youngdoo Kang[1*] and Kil To Chong[2]

[1]**Korea Institute of Nuclear Safety**

[2]**Division of Electronics and Information Engineering, Chonbuk National University**

원전 계측제어시스템에 대한 사이버보안성 평가 방법론 개발

강영두[1*], 정길도[2]

[1]한국원자력안전기술원, [2]전북대학교 전자정보공학부

Abstract Cyber security assessment is the process of determining how effectively an entity being assessed meets specific cyber security objectives. Cyber security assessment helps to measure the degree of confidence one has and to identify that the managerial, technical and operational measures work as intended to protect the I&C systems and the information it processes. Recently, needs for cyber security on digitalized nuclear I&C systems are increased. However the overall cyber security program, including cyber security assessment, is not established on those systems.

This paper presents the methodology of cyber security assessment which is appropriate for nuclear I&C systems. This methodology provides the qualitative assessments that may formulate recommendations to bridge the security risk gap through the incorporated criteria. This methodology may be useful to the nuclear organizations for assessing the weakness and strength of cyber security on nuclear I&C systems. It may be useful as an index to the developers, auditors, and regulators for reviewing the managerial, operational and technical cyber security controls, also.

요 약 사이버보안성 평가는 대상이 되는 시스템이 사이버보안의 목적에 효과적으로 부합하는지 여부를 판단하는 방법이다. 사이버보안성 평가는 시스템의 사이버보안에 대한 신뢰 수준을 측정하고, 관리적·기술적·운영 측면에서의 사이버보안 척도가 요구된 바와 같이 이행되는지를 확인하는 데 필요하다. 최근 원전 계측제어시스템은 디지털 기술의 적용으로 인해 사이버보안에 관한 기술적 및 관리적 대책이 수립되도록 요구되고 있으나, 동 시스템의 사이버보안성 평가 방법론을 포함한 전반적인 사이버보안 프로그램이 마련되어 있지 않은 실정이다.

본 논문은 원전 계측제어 시스템에 적합한 정성적 사이버보안성 평가 방법론을 제시한다. 제안되는 방법론은 원전 계측제어 시스템의 사이버보안에 대한 강점과 취약점을 평가함으로써 원전 계측제어 시스템의 사용자에게 도움이 될 수 있다. 또한, 이 방법론은 원전 계측제어 시스템의 개발자, 감사자 및 규제자가 사이버보안의 관리적, 운영적 및 기술적 통제 항목을 검토하는 지표로 활용될 수 있을 것으로 판단된다.

Key Words : Nuclear I&C Systems, Cyber Vulnerability, Cyber Security Assessment

1. Introduction

Whole industries including nuclear power plants are switching to computer-based technologies due to the rapid development of computers and information processing technologies. With the rapid expansion of computer-based technologies, those application to nuclear power plants has raised many questions regarding their safety and

*Corresponding Author : Youngdoo Kang(k407kyd@kins.re.kr)
Received August 18, 2010 Revised September 2, 2010 Accepted September 8, 2010

reliability. Recently, new and deep concerns about the cyber-security of computer based instrumentation, control, and information systems in nuclear plants were raised. There is a need to formulate a structured set of cyber security programs on instrumentation, control and information systems in nuclear power plants to protect the critical systems against cyber attacks.

1.1 Nuclear I&C Systems Uniqueness

Traditionally, 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. However, widely available, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of cyber security vulnerabilities and incidents to I&C systems. [5] This is why the cyber threats that exploit the Information Technology (IT) fields are fast changing and evolving scenario.

This may increase the vulnerabilities of safety I&C systems, and loss of availability of those systems may harm to the safety function of nuclear power plants for the cyber threats. 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.

[Table 1] Differences of Security aspect in IT and I&C

Topic	IT	I&C
Anti-virus/Mobile Code	Common/Widely Used	Uncommon/ Impossible to deploy
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	24*7*365
Secure 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

For those reason, cyber security program on nuclear I&C systems should be performed to meet confidentiality, integrity and availability criteria, but still have different aspect comparing with IT fields. Table 1 shows differences of security aspect between IT and I&C systems.

1.2 Cyber Security Assessment

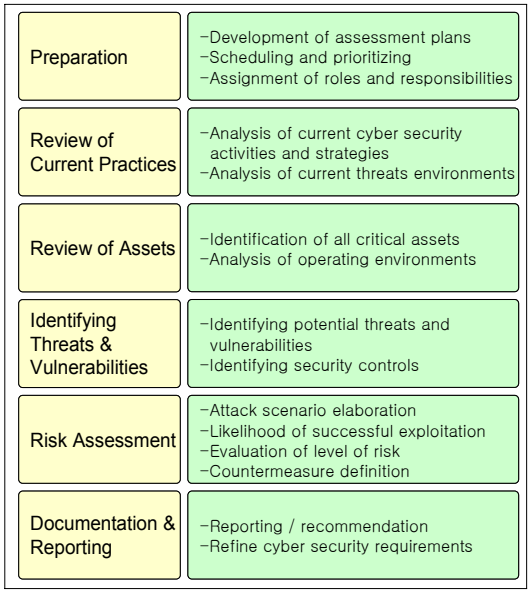
Cyber security assessment is the process of determining how effectively an entity being assessed meets specific cyber security objectives. [5] It is essential to know the strengths and weaknesses of the I&C systems against cyber threats that can exploits its electronic vulnerabilities. The assessment helps to measure the degree of confidence one has that the managerial, technical and operational security measures work as intended to protect the I&C systems. The cyber security assessment should be done periodically to ensure that the directions of management are implemented properly, security features operate as designed and new threats are identified and addressed.

The assessment covers all managerial, technical, organizational and operational areas of cyber security features on I&C systems which are;

a. cyber security policy and plans
b. organizational security
c. asset classification and control
d. personnel security
e physical and environmental security
f. communication and operation management
g. access control
h. system development and maintenance
i. compliance

The organization doing the assessment should perform each stage of the assessment process to ensure performance objectives and criteria are met through evaluation of cyber security threats and vulnerabilities. The assessors may identify new security controls by documenting and reporting all their findings.

The recommended cyber security assessment processes are as figure 1.



[Fig. 1] Cyber security assessment processes

2. Development of Cyber Security Assessment Methodology

2.1 Consideration on Nuclear I&C Systems

Cyber security assessment is an important process for determining the best allocation of the technical, managerial and operational countermeasures. Many of assessment tools and methodologies that exists such as testing, auditing, inspecting, examination or analyzing may be used to assess the security status of digital systems.

ISO/IEC 27001 is well-known international standard which defines the requirements for an information security management.[2] It is intended to bring information security under explicit management control with specifying eleven security control clauses to be organized and jointed information security. This standard might be the reference for the nuclear I&C systems to establish cyber security management systems. However, there is still need to exert effort in applying those existing methodologies and requirements to nuclear I&C systems since nuclear I&C systems and Information Technology (IT) fields have different environmental factors and operations. As shown in figure 1, there are several characteristics on nuclear I&C systems that differ from traditional internet-based information processing systems, including different risks and priorities.

For examples, nuclear I&C systems, especially the safety-related systems, shall be time-critical. In contrast, IT systems typically require high throughput, but can withstand substantial levels of delay and jitter. In a typical IT system, data confidentiality and integrity are the primary concerns, but nuclear I&C systems primarily concern availability attributes.

Also the nuclear I&C system has long lifetime with multiple of design and operational characteristics. The multiple lifetime phases and modes of operation may involve different systems and likewise different operational environments. An example is during an overhaul which often involve equipment replacement, modification and testing or which may require extra staff or third party or contractor access. Those different characteristics, considerations and diversity should be taken into account in the cyber security activities on nuclear I&C systems.

This means care should be taken for applying the existing references to the nuclear I&C systems, and considering the migration is required. For example, higher priority of confidentiality attribute in IT fields, such as protection of disclosing personnel information, is not the goal of nuclear safety.

2.2 Development of Assessment Questionnaires

This section presents the development of qualitative cyber security assessment questions which are appropriate to nuclear I&C systems with five categories (managerial, technical, physical, personnel, and policy aspect) to determine its cyber security status. These categories are derived from migration and modification of existing requirements in IT fields with considering the operation environments and objectives of nuclear I&C systems. This paper presents development of 162 questions for assessing the cyber security status on nuclear I&C systems. Samples of the questions are shown on figure 2.

There is a need for organizations in charge of nuclear facilities to identify and manage several cyber security activities in order to function properly. The managerial aspect of the survey has fifty-one (51) questions with the purpose of assessing the overall managerial processes of

cyber security on I&C systems. Topics included are requirements of managerial infrastructures, asset management, risk management, incident response process, operations management and continuity management for the nuclear I&C systems.

Technical controls to protect the classified asset are countermeasures which are implemented within systems, such as hardware, firmware and software including operating systems and applications. [3] Many organizations believe that implementing technical controls such as firewalls or Intrusion Detection Systems (IDS) can ensure the protection from cyber attacks but someone may still infiltrate the systems in spite all of these measure. The technical aspect of the survey composed of thirty-one (31) questions assesses the best allocation of technical controls.

Managerial	Can the cyber security officer manage the overall cyber security activities including asset management, risk management, incident response?
	Is there an asset classification scheme?
	Is there proper handling and labeling on classified asset?
	Is there proper back-up plans and implementation?
	Is there proper logging systems of I&C systems?
Technical	Is there proper documentation which is specifying the cyber security requirements for the new developed systems?
	Is there access control requirements?
	Is there an officer or manager who is in charge of managing the source code? Does he assigned by classified systems?
	Is there an access control process to the source code?
	Is there a process of encryption if needed?
Physical	Is there a physical security perimeter?
	Are there physical entry controls to the Main Control Room and Equipment Room?
	Are there equipments to protect from electric power failures?
	Are there media and document handling processes?
Personnel	Are there confidentiality understanding at initial part of procurement or agreement?
	Is there training programs and records of cyber security to the all employees and 3rd party users? Is it periodic?
	Are there personnel screening programs?
Policy	Is the cyber security policy approved by management?
	Is it disseminated to all employees and 3rd parties the easist way?
	Is there an encryption policy?
	Is there a password management policy?
	Is it in compliance with relevant law and regulation?

[Fig. 2] Sample questionnaire in five categories

Physical security is the controls for protecting the classified assets from environment or physical damages. Physical entry controls, working in secure areas and cabling security to prevent the eavesdropping of communication media should be implemented. The physical security aspect of the survey will evaluate the status of physical security through a set of eighteen (18) questions.

Based on experiences of cyber security on IT fields, the majority of security incidents are human related and the security of any computer depends largely on the behavior of all its users. Cyber security requirements of an organization should be understood by all its employees and any other third parties. The personnel security includes cyber security in job responsibilities, training programs, personnel screening programs, etc. This personnel or human aspect of the cyber security will be assessed through twenty-six (26) questions.

Cyber security policy should be approved by management, published, disseminated and announced to all employees and external parties. As a highest level of dictation for the cyber security of nuclear I&C systems, it should be reviewed and assessed periodically. There are thirty-six (36) questions in the survey that aims to evaluate whether it is proper to evaluate the cyber security policy.

2.3 Assessment Methodology

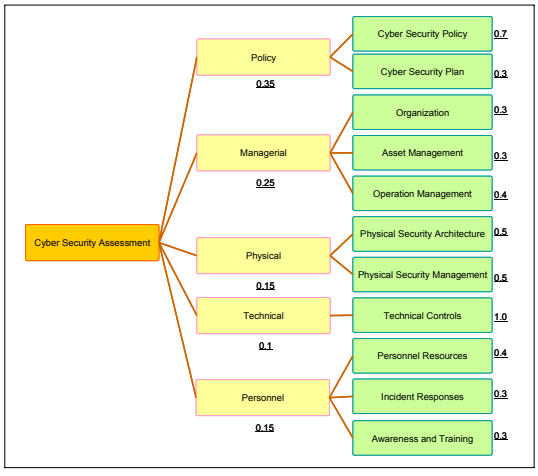
Once 162 questions in 5 categories have developed based on consideration and experiences of nuclear I&C systems, and migration from the practices in IT fields, there is a need on how to properly evaluate the answers to the 162 questions. A simple assessment methodology is suggested that may be helpful in the initial phase of system operations. One simple way of evaluating the answers, belonging to certain cyber security categories, is the calculation through the relative weights and the amount of positive answer. This can shows the overall and summarized results of each cyber security category.

Result = (number of positive answer / total number of answer) * relative weights

Determination of relative weights for the each category is based on the consideration of characteristics of and

experiences in operating nuclear I&C systems. One example is when we consider the characteristic based on ensuring the safe operation of nuclear I&C systems, availability attribute predominate rather than confidentiality and integrity. Physical security of nuclear facilities is traditionally much strict compared to other industries and with this in mind, higher weights can be give to managerial aspect compared to the physical aspect. The establishment of a structured set of cyber security is highly required in the initial phase of the assessment hence the weight of the policy aspect may be given greater value than the other aspects.

In one category, it could be classified into more several specific areas, except the technical controls for the reason of reducing the complexity. Figure 3 shows the determination of relative weights to the each cyber security category.



[Fig. 3] Cyber security categories with relative weights

The calculated results are utilized as an index for qualitative assessment of cyber security. It could generally include a 'grading criteria' of satisfactory, need improvement, and insufficiency. An assessor may assign the criteria to the results shown in Table 2 as an index of cyber security.

[Table 2] Table title

Result	Description
0 < result ≤ 0.4	Insufficiency
0.4 < result ≤ 0.8	Need Improvement
0.8 < result ≤ 1.0	Satisfactory, still need continuous management

2.4 Demonstration of Assessment

This section presents the development of a software tool that uses the suggested qualitative cyber security assessment methodology and its demonstration with developed software tool.

Table 3 shows the simple demonstration results based on relative weights.

[Table 3] Sample calculation for the assessment

Category	# of positive answers	# of questions	Relative weights	Result
Policy	22	36	0.35	0.214
Managerial	44	51	0.25	0.215
Physical	15	18	0.15	0.125
Technical	19	31	0.10	0.061
Personnel	14	26	0.15	0.080
Total				0.695

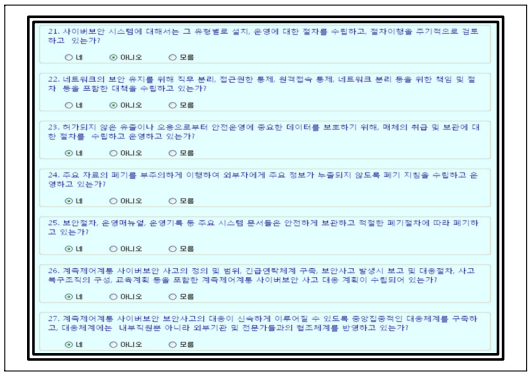
The answers are calculated through the suggested simple calculation. Consequently, the total result of this demonstration is 0.695. This table shows also that those systems should improve on policy, technical and personnel aspect of cyber security categories.

This methodology could be implemented through the software tool to support the licensee of nuclear facilities, and also to the developers and auditors. Although it does not provide specific methods of cyber security countermeasures, but gives overall and high-level of recommendation on each cyber security categories.

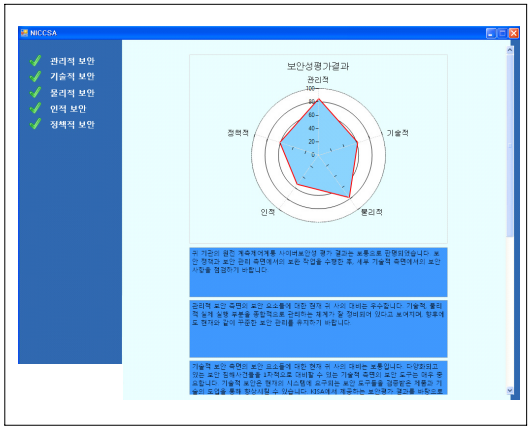
Shown in Figure 4 is the sample page of questions on managerial aspect in 5 categories of developed software tool during demonstration. The assessor can check 'positive' or 'negative' on each questions following the flow of the software tool.

Figure 5 to 7 show the result of the assessment. Figure 5 shows the reporting page of softwar tool that contains result in radial chart as figure 6, and overall result and

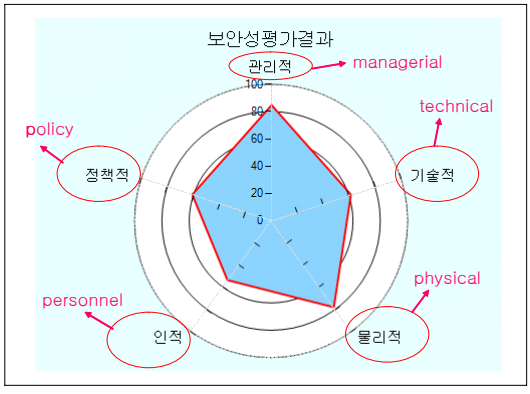
recommendation of the assessment as figure 7.



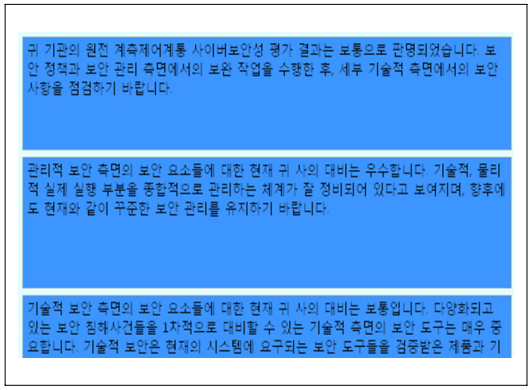
[Fig. 4] sample page of managerial aspect



[Fig. 5] Reporting page of software tool



[Fig. 6] Assessment result in radial chart



[Fig. 7] Sample overall result and recommendation

The overall cyber security status of nuclear I&C systems is rated as "need improvement" based on the output of the demonstration above. Each category is assessed based on grading criteria where it shows that the managerial aspect is satisfactory, still needs continuous management while the policy, technical and personnel aspect are determined as 'need improvement'. It might then generate a recommendation to upgrade or harden the systems to enhance the technical aspects.

This methodology and software tool is suggested for assessment of the overall and general cyber security status, but not for the specific. This means that the ways of detailed evaluation on each questions and development of countermeasures is the further duties.

3. Conclusions

Cyber attacks to nuclear I&C systems may results in endangerment of human and environmental safety. This is why nuclear I&C systems, especially those which perform the safety function, shall be protected from cyber attacks.

This paper suggests simple qualitative methodology of cyber security assessment which is appropriate for the nuclear I&C systems. Presented here are a total of 162 questions classified into five categories through several considerations of characteristics on nuclear I&C systems. A simple way of evaluating the answers is presented through relative weights in which the results show the overall cyber security status for each category and of the systems as a whole. A demonstration of the cyber security

assessment with the developed software tool based on the suggested methodology was also presented.

As the lack of practical methodology on cyber security assessment of nuclear I&C systems, proposed methodology in this paper might be useful as a cyber security index at an initial phase of system development life cycle and operation for the nuclear organizations to assess the strength and weakness of cyber security on nuclear I&C systems, and to the developers, auditors and regulators as well.

Based on proposed methodology, development of methodology of assigning detailed cyber security countermeasure on each category is needed as a further research.

References

[1] KINS Regulatory Guide, KINS/GT/N27, "Cyber Security of Instrumentation and Control Systems in Nuclear Facilities", Dec., 2007.

[2] ISO/IEC 27001, "Information Technology - Security Techniques - Information Security Management systems - Requirements"

[3] KINS/HR-994, "Cyber Security Evaluation Technique for Digital I&C Systems", Feb., 2010.

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

[5] NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security", Sep., 2008.

[6] NIST SP 800-115, "Technical Guide to Information Security Testing and Assessment"

[7] Min Sun Kim, "A Study on Analysing Framework of Information Security Management Systems for managing Business Risk", Journal of the Korea Academia-Industrial cooperation Society, Vol. 11, No. 2, pp. 703-708, 2010.

[8] Youn-Chong Kim, et al., "A Forecast Model for Information Security Certificate", KAIS Fall Conference, pp. 57-59, 2007.

Youngdoo Kang [Regular member]

- Feb. 1998 : Chonbuk National Univ., BS
- Feb. 2000 : Chonbuk National Univ., MS
- Sep. 2000 ~ current : Korea Institute of Nuclear Safety, Senior Researcher

<Research Interests>
Nuclear I&C Systems, Safety Systems, Cyber Security

Kil To Chong [Regular member]

- May. 1984 : Oregon State Univ., Mechanical Eng., BS
- Dec. 1986 : Georgia Institute of Technology., Mechanical Eng., MS
- May. 1993 : Texas A&M Univ., Mechanical Eng., Ph.D
- Mar. 1995 ~ current : Chonbuk National Univ., Dept. of Electronics and Information Engineering, Professor

<Research Interests>
Robotics, Marine Navigation, Control Systems