Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.2, Apr. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.2.363

소프트웨어 생명주기 단계별 사이버보안 평가 방법론 제안

서 달 미,[1†] 차 기 종,[1‡] 신 요 순,[1] 정 충 희,[2] 김 영 미[2]
[1](주)엔에스이, [2]한국원자력안전기술원

Assessment Method of Step-by-Step Cyber Security in the Software Development Life Cycle

Dal-mi Seo,[1†] Ki-Jong Cha,[1‡] Yo-Soon Shin,[1] Choong-Heui Jeong,[2] Young-Mi Kim[2]
[1]NSE Inc, [2]Korea Institute of Nuclear Safety

요 약

기존의 원자력발전소 계측제어 시스템은 아날로그 기술 기반으로 설계 및 운영되어 왔지만, 정보기술(IT)의 발달로 신규 원자력발전소에는 점차 디지털 기반 기술이 도입되고 있다. 디지털 기반 기술은 여러 가지 순기능에 반하여 사이버 위협에 취약한 측면이 존재하며 이로 인해 시스템 상에 안전성과 신뢰성에 악영향을 끼치고 발전소 전체에 심각한 영향을 미칠 수 있다. 그러므로 원자력발전소에 탑재되는 소프트웨어는 개발 초기 단계부터 사이버보안 요소들을 고려하여 설계되고 각 단계마다 사이버보안 평가를 통하여 사이버보안에 대한 신뢰 수준을 측정하고, 기술적·관리적·운영적 측면에서의 사이버보안 척도가 요구된 바와 같이 이행되는지를 확인하는 것이 필요하다. 그러나 현재 이러한 사이버보안 평가 방법을 포함한 전반적인 사이버보안 프로그램이 마련되어 있지 않은 실정이므로 본 논문에서는 원자력발전소와 관련된 규제요건 및 기술표준문서를 기반으로 원자력발전소의 소프트웨어 생명주기 단계별 사이버보안 활동과 평가 항목을 도출하여 소프트웨어 생명주기 단계별로 사이버보안 평가가 가능한 방법을 제안한다.

ABSTRACT

Instrumentation and control(I&C) system has been mainly designed and operated based on analog technologies in existing Nuclear Power Plants(NPPs). However, As the development of Information Technology(IT), digital technologies are gradually being adopted in newly built NPPs. I&C System based on digital technologies has many advantages but it is vulnerable to cyber threat. For this reason, cyber threat adversely affects on safety and reliability of I&C system as well as the entire NPPs. Therefore, the software equipped to NPPs should be developed with cyber security attributes from the initiation phase of software development life cycle. Moreover through cyber security assessment, the degree of confidence concerning cyber security should be measured and if managerial, technical and operational work measures are implemented as intended should be reviewed in order to protect the I&C systems and information. Currently the overall cyber security program, including cyber security assessment, is not established on I&C systems. In this paper, we propose cyber security assessment methods in the Software Development Life Cycle by drawing cyber security activities and assessment items based on regulatory guides and standard technologies concerned with NPPs.

Keywords: software development life cycle, cyber security assessment, cyber security in nuclear power plants

접수일(2014년 12월 24일), 수정일(2015년 1월 21일), 게재확정일(2015년 2월 17일)

† 주저자, dalmi.seo@nsetec.com
‡ 교신저자, kjcha@nsetec.com(Corresponding author)

I. 서 론

정보시스템 분야에서는 일찍이 사이버 위협에 대응하기 위한 정보보안의 중요성을 인식하고, 다양한 사이버 위협의 분석 및 대응기술을 연구하여 왔으나 이에 비해 원자력발전소 계측제어 시스템은 정보기술 분야에서 이미 큰 현안으로 부각되어 왔던 사이버보안의 중요성과 필요성을 인식하지 못하고 있는 실정이다.

이는 원자력발전소 계측제어 시스템의 특성 상, 사회 구성원이 쉽게 사용할 수 있는 일반적인 컴퓨터나 통신망을 사용하지 않고, 폐쇄 망 내에서 특화된 하드웨어 및 소프트웨어를 사용해온 환경적인 차이 때문이기도 하다[1]. 미국 CMU 소프트웨어 공학연구소의 보고서에 따르면 소프트웨어 보안 취약점의 70%가 설계과정의 오류로부터 발생하며 미국 Microsoft 社는 개발단계에서 SDL(Security Development Lifecycle) 적용 시 보안 취약성이 50% 이상 감소한다고 보고하고 있다[2][3].

이에 따라 국민의 안전과 직결된 원자력발전소에서도 소프트웨어 개발 생명주기 초기 단계에서부터 사이버보안을 고려하여 신뢰성 및 보안을 위협하는 요소들로부터 안전성을 확보해야 한다. 원자력발전소 계측제어 시스템은 일반 IT 시스템과 비교해 볼 때 폐쇄성, 자원의 특수성, 운용 가용성 등의 측면에서 차이점이 있으므로 일반 IT 시스템에서의 사이버보안성 평가 방법 등을 원자력발전소 계측제어 시스템에 직접 적용하기에는 어려움이 따른다.

따라서 본 논문에서는 원자력발전소 규제지침 및 기술표준에서 제시하는 사이버보안 통제 항목들을 비교 및 분석하며 해당 결과를 각 소프트웨어 생명주기 단계에 적용하여 원자력발전소에 특화된 소프트웨어 생명주기 단계별 사이버보안 평가 방법을 제안한다. 본 논문의 2절에서는 기존 일반 IT 시스템과 원자력발전소 계측제어 시스템의 사이버보안 평가 방법에 대한 관련 연구를 기술하고, 3절에서는 본 논문이 제안하는 사이버보안 평가를 위한 평가 항목 도출 방법에 대해 기술한다. 4절에서는 상기 평가 항목을 기반으로 소프트웨어 생명주기 단계별 사이버보안을 평가하기 위한 평가 방법론을 제안하며 결론으로 끝을 맺는다.

II. 관련 연구

본 절에서는 기존에 연구된 일반 IT시스템의 소프트웨어 생명주기 단계별 사이버보안 방법과 원자력발전소 계측제어 시스템의 사이버보안 평가 방법에 대해 기술한다.

2.1 일반 IT 시스템의 소프트웨어 생명주기 단계별 사이버보안 방법

2.1.1 MS-SDL 방법론

MS-SDL은 마이크로소프트에서 개발 생명주기 내에 각 단계별 활동을 정의하여 소프트웨어 보안을 강화하기 위해 개발한 보안 개발 생명주기(SDL : Security Development Lifecycle)를 말한다.

2012년 5월 발표된 SDL 5.2는 Fig. 1.과 같이 Pre-SDL, Requirements, Design, Implementation, Verification, Release, Response, Post-SDL의 7단계로 구성되어 있다.

각 단계별 보안활동을 필수/권고를 구분하여 제시하여 사이버보안 활동을 선택적으로 수행할 수 있도록 제시하였다[3].

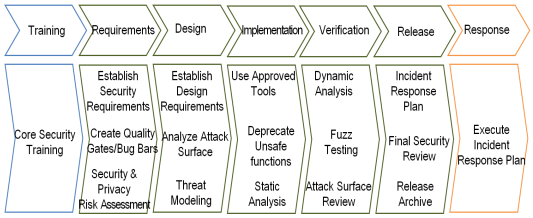

Fig. 1. MS-SDL

2.1.2 CLASP 방법론

CLASP(Comprehensive Lightweight Application Security Process)는 Secure Software Inc사에서 소프트웨어 개발 생명주기에서 보안 구축에 필요한 지침과 핵심 활동(activity-driven)을 정의한 방법론을 말한다.

CLASP는 Concepts View, Role-Based View, Activity-Assessment View, Activity-Implementation View, Vulnerability View의 5가지의 관점(View)으로 구성되어있다. 각 관점별로 활동을 정의하고 타 관점과 유기적인 결합 과정을 제공한다는 점에서 다른 방법론과 차이가 있다고 할 수 있으며 7개의 지침과 20개의 핵심보안활동을 제공하고 있다[4].

2.1.3 Seven-Touchpoint 방법론

Gary McGraw가 제안한 Seven-TouchPoint는 실무적으로 이미 검증된 보안 방법론 중 하나이다. McGraw가 발견한 본 방법론의 핵심은 개발 생명주기를 구성하는 단계별 활동을 보안 기능과 직접적 관계 활동과 간접적 관계 활동으로 구분하는데 있다. 보안 기능의 직접적 관계 활동을 분류해냄으로써 보안성 강화 활동 7가지를 집중적으로 관리하도록 하고 있다.

제안하는 강화 활동 7가지는 Code Review (Tools), Architectural risk analysis, Penetration testing, risk-based security tests, abuse cases, security requirements, security operations이며 각 강화활동 별로 Fig. 2.와 같이 화살표에서 가리키는 단계를 집중 관리하도록 하고 있다[5].

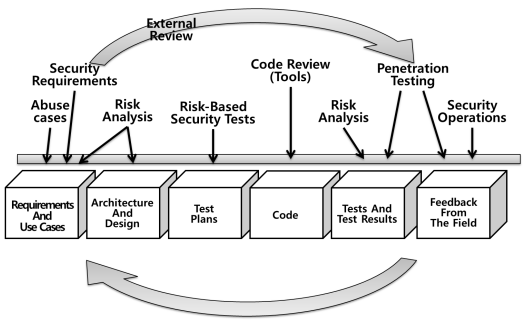

Fig. 2. Seven-Touchpoint

2.2 원자력발전소 계측제어시스템의 사이버보안 평가

Youngdoo Kang and Kil To Chong[1]은 안전에 중요한 원자력발전소 계측제어 시스템의 사이버보안성을 평가하기 위한 체계적인 공정(프로세스, Process) 방법론을 기술하였다. 이를 위해 원자력발전소의 계측제어 시스템에 대한 설계 특성과 운영 특성, 사이버보안 침해사례 조사와 원전 계측제어 시스템에 내재되어 있는 사이버보안의 취약성에 대해서 분석하였다. 이러한 조사 및 분석을 토대로, 소프트웨어 툴을 통해 원자력발전소 계측제어 시스템에 적용 가능한 정성적 사이버보안성을 평가할 수 있는 방법을 기술하였다. 제안하는 평가 방법론은 원자력발전소 계측제어 시스템의 기술적 측면, 관리적 측면 및 운영 특성이 고려되었으며. 사이버 위협에 대한 정성적 위험도 분석 기법을 통해 취약성을 제거하거나 위험으로부터의 영향을 최소화시킬 수 있는 통제항목을 도출하였다. 해당 논문에서 제시하는 통제항목에 대한 예시는 Table 1.과 같다.

또한 사이버보안성 평가를 위한 위 5가지의 분류를 각각 여러 개념으로 추가 분류하고 가중치를 부여하여 종합적인 사전 사이버보안성 평가의 정성적 결과를 제공하였다.

Table 1. Sample questionnaire in five categories

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?
Technical	Is there access control requirements?
	Is there a process of encryption if needed?
Physical	Is there a physical security perimeter?
	Are there media and document handling processes?
Personnel	Are there personnel screening programs?
Policy	Is there a password management policy?
	Is it in compliance with relevant law and regulation?

III. 제안하는 소프트웨어 생명주기 단계별 사이버보안 평가 방법 도출 및 내용

상기의 일반 IT 시스템 사이버보안성 평가 방법[3]~[5]은 원자력발전소 계측제어시스템에서 요구하는 소프트웨어 개발 생명주기와는 차이가 있으며 원자력발전소 계측제어시스템의 특성상 사회 구성원이 쉽게 사용할 수 있는 일반적인 컴퓨터나 통신망을 사용하지 않고, 폐쇄 망 내에서 특화된 하드웨어 및 소프트웨어를 사용해온 환경적인 차이 때문에 직접 적용하기에는 추가적인 연구가 필요할 것으로 판단된다.

원자력발전소 계측제어시스템의 사이버보안 평가[1]에서는 원자력발전소의 특성을 분석하여 사전 사

이버보안성을 평가할 수 있는 결과를 도출하였다. 이와 추가로 본 논문에서는 소프트웨어 개발 생명주기 초기 단계에서부터 사이버보안을 고려하여 신뢰성 및 보안을 위협하는 요소들로부터 안전성을 확보하기 위한 사이버보안 통제 항목을 도출하였다. 제안하는 방법은 원자력발전소 규제지침 및 기술표준을 기반으로 소프트웨어 생명주기 단계별 사이버보안 활동 및 산출물, 사이버보안 평가 테이블, 사이버보안 평가 통제항목, 통제항목의 중요도 등급 기준을 도출하였다. 추후 협의를 통해 원자력발전소 계측제어시스템의 사이버보안 평가[1]에서 제시하는 소프트웨어 툴을 통한 사이버보안 평가방법에 본 연구의 결과물을 결합한다면 시너지 효과가 발생될 것으로 예상한다.

3.1 원자력분야 사이버보안 기술표준 및 지침 분석

본 논문에서는 원자력발전소 계측제어시스템 소프트웨어 개발 시 적용할 수 있는 규제지침 및 기술표준을 분석하여 소프트웨어 생명주기 단계별 사이버보안 활동, 활동에 따른 산출물, 사이버보안 통제항목, 통제항목의 중요도 등급 기준을 도출하였다. 각 규제지침 및 기술표준에 대한 내용은 다음과 같다.

3.1.1 원전 안전계통의 디지털 컴퓨터 사용

국제전기전자기술자협회(IEEE, Institute of Electrical and Electronics Engineers)에서는 원전 안전계통에서의 디지털 컴퓨터 사용과 관련하여 2010년에 IEEE Std. 7-4.3.2를 발표하였다. 안전계통의 기준 사항들을 기술하고 있으며, 소프트웨어 개발 시 소프트웨어의 품질 측정 기준, 확인 및 검증 요건 및 접근 통제 등의 내용을 포함한다. 특히 접근통제에서는 물리적 보안과 더불어 소프트웨어 생명주기 단계별로 잠재적인 취약점을 다루도록 명시하고 있으며 폭포수 생명주기를 기반으로 하여 단계별 요건들을 명시하고 있으며, Table 2.와 같다[6].

3.1.2 소프트웨어 생명주기 단계별 사이버보안 활동 지침

미국국립표준기술연구소(NIST, National Institute of Standards and Technology)에서 발표한 SP 800 Series에서는 컴퓨터 보안과 관련된 여러 가이드라인을 제시하고 있다.

Table 2. IEEE Std. 7-4.3.2 suggested security activities in the software development life cycle

Software development life cycle phase	Cyber security activities
Concept	Identification of safety system security capabilities Assessment of security to identify potential security vulnerabilities
Requirements	Definition of the security functional performance requirements for the complete system life cycle
Design	Translation of security requirements identified in the specification requirements
Implementation	Implementation of hardware configuration and set-up, software coding and testing
Test	Test security functions of system security requirements
Installation and checkout	Installation, verification, and validation of security features in the target environment
Operation and maintenance	Periodic testing, monitoring, review of system logs, real-time monitoring
Retirement	Assessment the effect on system interfaces of removing the system security functions

NIST SP 800-64 (Rev.2), "Security Considerations in the Development Life Cycle"은 소프트웨어 생명주기를 시작, 개발 및 요건, 구현 및 평가, 운영 및 유지보수, 폐기 단계로 나누고 각 단계에서 이행하여야 하는 사이버보안 활동과 산출물에 대하여 기술하고 있다.

Fig. 3.은 NIST SP 800-64(Rev.2)에서 제시하고 있는 소프트웨어 생명주기를 도식화 한 것이다.

시작 단계에서의 사이버보안 활동에는 기밀성, 무결성, 가용성 측면에서의 초기 보안 계획, 시스템 분류, 보안시스템개발프로세스 확립 등이 있으며 이러한 활동 후 관련 문서들을 산출하도록 기술하고 있다. 개발 및 요건 단계에서는 보안 요건 분석 및 보

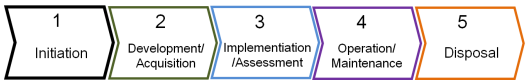

Fig. 3. Software Development Life Cycle Phases

안 아키텍처를 설계하고, 구현 및 평가 단계에서는 시스템과 운영 환경을 통합하고 전체시스템에 대하여 보안 인증 활동을 한다. 운영 및 유지보수 단계에서는 운영 중인 시스템에서 발생하는 변경된 사항들이 보안에 영향을 끼칠 수 있기 때문에 지속적인 모니터링을 하며 시스템에 대한 형상관리를 수행하여야 한다. 폐기 단계에서는 하드웨어 및 소프트웨어를 폐기하기 전에 관련 계획을 구축하고 중요한 정보는 별도 보관을 하며 관련 규정 및 정책에 따라 연관 시스템을 종료한다.

Table 3.은 NIST SP 800-64(Rev.2)에서 기술하고 있는 소프트웨어 생명주기 단계별 사이버보안 활동을 나타낸 표이다[7].

Table 3. NIST SP 800-64(Rev.2) Suggested security activities in the software development life cycle

Software development life cycle phase	Cyber security activities
Initiation	Security categorization Preliminary risk assessment
Development/Acquisition	Risk assessment Security controls development
Implementation /Assessment	System integration Security assessment
Operation /Maintenance	Configuration management Continuous monitoring
Disposal	Media sanitization Information preservation

3.1.3 미국 원자력규제위원회 사이버보안 지침

미국 원자력규제위원회(NRC, Nuclear Regulatory Commission)는 2010년 원전 사이버보안과 관련된 규제지침 Regulatory Guide 5.71을 발표하였다. 기술적, 운영적 및 관리적 측면에서 고려하여야 할 사이버보안 통제 항목들을 18개의 패밀리로 나누어 제시하고 있으며 그 내용은 Table 4.와 같다[8].

Table 4. RG 5.71 suggested security controls

Class	Family	ID
Technical Security Controls	Access Controls	B.1
	Audit and Accountability	B.2
	Critical Digital Asset and Communications Protection	B.3
	Identification and Authentication	B.4
	System Hardening	B.5
Operational Security Controls	Media Protection	C.1
	Personnel Security	C.2
	System and Information Integrity	C.3
	Maintenance	C.4
	Physical and Environmental Protection	C.5
	Defensive Strategy	C.6
	Defense-in-Depth	C.7
	Incident Response	C.8
	Contingency Planning	C.9
	Awareness and Training	C.10
	Configuration Management	C.11
Management Security Controls	System and Service Acquisition	C.12
	Security Assessment and Risk Management	C.13

3.1.4 NIST SP 800-53(Rev.4)

미국국립표준기술연구소(NIST)는 연방정보시스템 및 산업제어시스템의 보안 가이드라인을 제정하고 2013년 네 번째 개정본을 발행하였다. 개정본에서는 모바일 및 클라우드 컴퓨팅, 애플리케이션 보안, 펌웨어의 무결성, APT 공격, 개인정보보호 등의 사이버보안 문제들을 포함하고 있다. 개인정보보호와 관련된 통제항목은 본 연구에서는 다루지 않으므로 관련 내용은 기술하지 않았으며, 보안 통제항목은 Table 5.와 같다[9].

3.1.5 DHS

미국의 부시대통령은 2001년 9·11 테러 이후 국토안보부를 신설하였고 국토안보법(HSA, Homeland Security Act)을 제정하였다. 국토안보부는 종래 FBI에 속해있던 국가기반시설보호센터(NIPC)와

Table 5. NIST SP 800-53(Rev.4) suggested security controls

Class	Family	ID
Technical Security Controls	Access Control	AC
	Audit and Accountability	AU
	Identification and Authentication	IA
	System and Communications Protection	SC
Operational Security Controls	Awareness and Training	AT
	Configuration Management	CM
	Contingency Planning	CP
	Incident Response	IR
	Maintenance	MA
	Media Protection	MP
	Physical and Environmental Protection	PE
	Personnel Security	PS
	System and Information Integrity	SI
Management Security Controls	Security Assessment and Authorization	CA
	Planning	PL
	Program Management	PM
	Risk Assessment	RA
	System and Services Acquisition	SA

상무부의 CIAO 등 기존의 부서들을 통합하고 물리적 보안 및 사이버보안의 총괄 조정업무를 담당한다[11]. 이 지침은 2011년 미 국토안보부에서 발표한 산업제어시스템의 보안에 대한 7번째 개정본이며 사이버보안의 정책, 인적 자원에 대한 보안, 위험 관리 및 평가 등의 보안 통제 항목들을 제시하고 있으며 Table 6.과 같다[10].

3.2 제안하는 소프트웨어 생명주기 단계별 사이버보안 평가 방법

3.2.1 평가 항목 도출

원자력발전소의 규제자료 및 산업표준 문서에서 제시하고 있는 보안 통제항목을 비교 및 분석하여 소프트웨어의 생명주기 단계별 사이버보안을 평가하기 위한 평가 항목을 도출하였다. 해당 평가 항목의 도출을 위하여 미국 원자력 규제 위원회(NRC)의 Regulatory Guide 5.71, 미국 국립 표준 기술연구소(NIST)의 SP 800-53(Rev.4), 미국국토안보부의 Catalog of Control Systems Security(Rev.7) 및 미국원자력에너지협회(NEI, Nuclear Energy Institute)의 08-09(Rev.6)를 비교 및 분석하였다. RG 5.71에서는 보안 통제항목을 3개의 클래스(기술적, 운영적 및 관리적), 18 패밀리, 147 컴포넌트, NIST SP 800-53(Rev.4)도 18 패밀리 198 컴포넌트, DHS는 19 패밀리 250 컴포넌트, NEI[12]는 17 패밀리 138 컴포넌트를 제시하고 있다. Fig. 4.는 RG 5.71을 중심으로 NIST SP 800-53(Rev.4)와 미국 국토안보부의 지침자료에서 제시하고 있는 보안 통제항목 간의 연

Table 6. DHS suggested security controls

ID	Family
2.1	Security Policy
2.2	Organizational Security
2.3	Personnel Security
2.4	Physical and Environmental Security
2.5	System and Services Acquisition
2.6	Configuration Management
2.7	Strategic Planning
2.8	System and Communication Protection
2.9	Information and Document Management
2.10	System Development and Maintenance
2.11	Security Awareness and Training
2.12	Incident Response
2.13	Media Protection
2.14	System and Information Integrity
2.15	Access Controls
2.16	Audit and Accountability
2.17	Monitoring and Reviewing Controls System Security Policy
2.18	Risk management and Assessment
2.19	Security Program Management

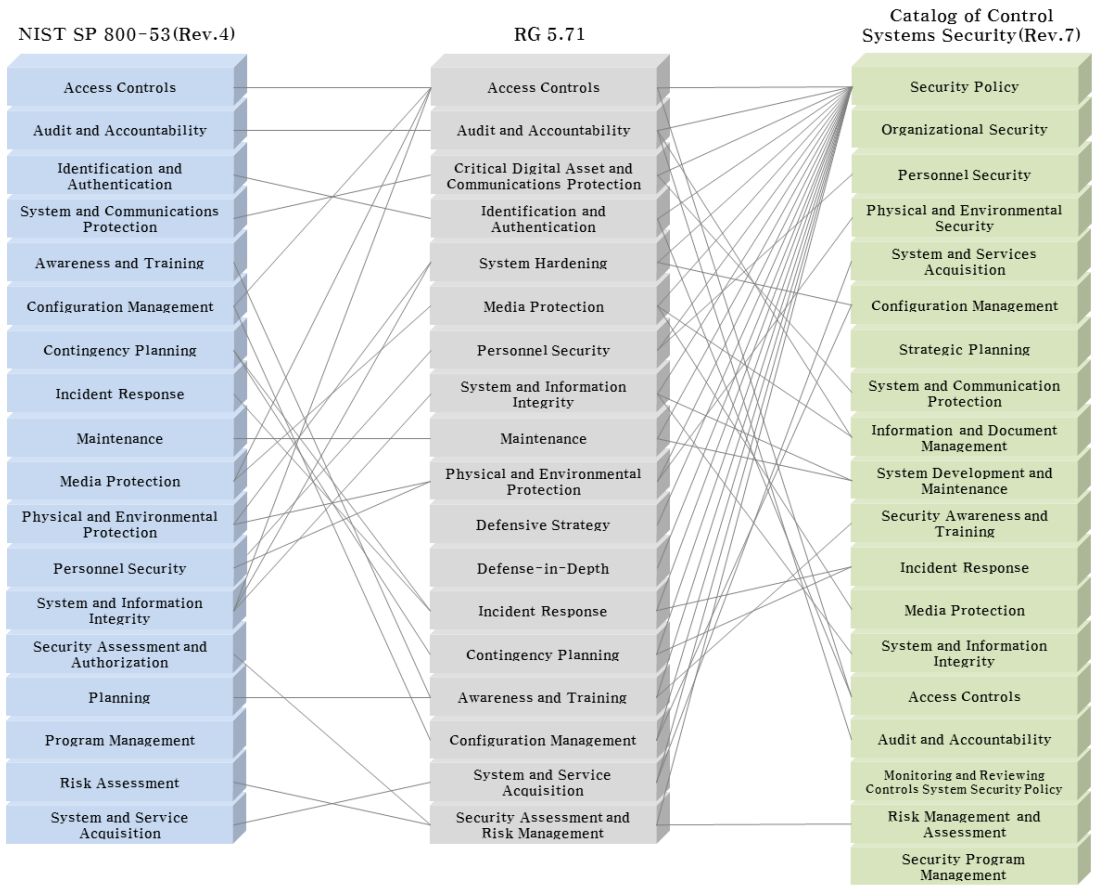

Fig. 4. Correlation among security controls

관 관계를 도식화한 것이고, Table 7.은 RG 5.71을 중심으로 각 자료별 보안 통제항목들의 관계를 표로 정리한 것이다.

Table 7. Mapping security controls : RG 5.71, NIST SP 800-53(R4), DHS, NEI

Security Controls	RG 5.71	NIST 800-53 (R4)	DHS	NEI 08-09 (R6)
Access Controls	B.1	AC	2.15	D.1
Audit and Accountability	B.2	AU	2.16	D.2
Critical Digital Asset and Communications Protection	B.3	SC	2.8	D.3
Identification and Authentication	B.4	IA	2.15	D.4
System Hardening	B.5	PE, SI	2.6	D.5
Media Protection	C.1	MP	2.13	E.1
Personnel Security	C.2	PS	2.3	E.2
System and Information Integrity	C.3	SI	2.14	E.3
Maintenance	C.4	MA	2.10	E.4
Physical and Environmental Protection	C.5	PE	2.4	E.5
Defensive Strategy	C.6	-	-	E.6
Defense-in-Depth	C.7	-	-	-
Incident Response	C.8	IR	2.12	E.7

Security Controls	RG 5.71	NIST 800-53 (R4)	DHS	NEI 08-09 (R6)
Contingency Planning	C.9	CP	2.12	E.8
Awareness and Training	C.10	AT	2.11	E.9
Configuration Management	C.11	CM	2.6	E.10
System and Service Acquisition	C.12	SA	2.5	E.11
Security Assessment and Risk Management	C.13	-	2.7	E.12
-	-	CA PL PM	2.1 2.2 2.7 2.8 2.9 2.17 2.18	-

(-) Represent the corresponding entry does not exist or cannot respond to one of the items.

이러한 연관 관계를 바탕으로 Fig. 5.와 같이 소프트웨어 생명주기 각 단계에서 고려할 사항들을 추출하였으며, Table 8.은 소프트웨어 생명주기 단계 중 폐기 단계에서 고려하여야 하는 보안 통제 항목 가운데 일부 예시를 나타낸 것이다.

Table 8. Security controls in disposal phase

Software development life cycle phase	security controls
Disposal	Access controls
	Audit and accountability
	Media Protection
	Personnel Security
	Configuration

3.2.2 평가 고려사항 도출

소프트웨어 생명주기 각 단계에서 고려해야 하는 사이버보안 요소를 3.2.1절에서 도출한 평가 항목으로부터 추출하였으며 추출한 요소는 Fig. 5.에서 확인할 수 있다. 또한 각 평가 항목에 대한 사이버 위협 발생 가능성과 그에 따른 영향성을 고려하였고 체크리스트 기법으로 각 평가 항목을 평가한다. 발생가

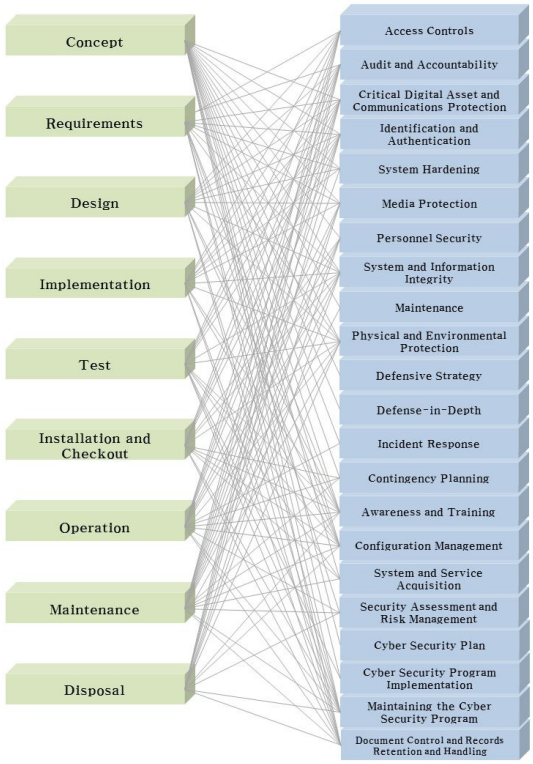

Fig. 5. Mapping software development life cycle phases and security controls

능성은 NIST SP 800-53(Rev.4) Appendix에서 기술하고 있는 우선순위를 참조하여 1~3수준으로 분류하였으며 영향성은 평가 항목의 중요도에 따라 1~5수준으로 분류하였다.

Table 9. Level for likelihood of occurrence(LL)

Level	Qualitative Value	Description
LL3	High	Resulting from vulnerability, likelihood of occurrence for threat is very high.
LL2	Moderate	Resulting from vulnerability, likelihood of occurrence for threat is somewhat.
LL1	Low	Resulting from vulnerability, likelihood of occurrence for threat is very low.

SDLC Phase	Cyber Security Activities	Implementation of Cyber Security Activities	Security Controls	Level of Likelihood (LL)	Level of Impact (IL)	Level of Cyber Security (CSL)
Concept	Planning	Y	Personnel Security	LL3	IL5	CSL5
Concept	Planning	Y	Awareness and Training	LL1	IL3	CSL3
⋮	⋮	⋮	⋮	⋮	⋮	⋮

Fig. 6. Table of assessment of cyber security

발생가능성은 평가 항목이 취약점으로 작용하여 위협요소가 발생할 가능성 수준을 나타내며 Table 9.와 같다.

Table 10. Level of Impact(IL)

Level	Qualitative Value	Description
IL5	Very High	Resulting from vulnerability, the integrity and availability of the system is affected. And it could be expected to have multiple severe or catastrophic adverse effects on system.
IL4	High	Resulting from vulnerability, the integrity and availability of the system is affected. And it could be expected to have severe adverse effects on system.
IL3	Moderate	Resulting from vulnerability, the integrity and availability of the system is affected. And it could be expected to have serious adverse effects on system.
IL2	Low	Resulting from vulnerability, the integrity and availability of the system is affected. And it could be expected to have limited adverse effects on system.
IL1	Very Low	Resulting from vulnerability, the integrity and availability of the system is affected. And it could be expected to have negligible adverse effects on system.

영향성 수준은 보안 특성인 기밀성, 무결성 및 가용성 중 중요도가 높은 가용성과 무결성에 영향을 줄 수 있는 정도를 나타내며 Table 10.과 같다.

사이버보안 평가 수준을 산정하기 위하여 평가 항목에 발생 가능성과 영향성 수준의 값을 부여하고 Table 11.의 사이버보안 수준을 기반으로 각 단계별 사이버보안 평가 수준을 산정한다.

앞서 분석한 소프트웨어 생명주기 단계별 보안 활동과 통제 항목을 바탕으로 Fig. 6.과 같이 사이버보안 평가 테이블을 작성한다. 소프트웨어 생명주기 사이버 보안 활동의 수행 여부와 산출물을 점검하고, 발생 가능성과 영향성에 따른 최종 사이버보안 수준을 도출한다.

Table 11. Level of Cyber Security(CSL)

Level for likelihood of occurrence (LL)	Level of Impact(IL)				
	IL5	IL4	IL3	IL2	IL1
LL3	CSL5	CSL5	CSL5	CSL4	CSL3
LL2	CSL5	CSL4	CSL4	CSL3	CSL2
LL1	CSL4	CSL4	CSL3	CSL2	CSL1

IV. 기존 사이버보안 평가 방법과의 비교

본 절에서는 상기에서 기술한 기존 사이버보안 평가 방법과 제안한 사이버보안 평가 방법과의 비교결과를 기술한다. Table 12.에서 상기 4개는 기존 사이버보안 평가 방법과 제안한 사이버보안 평가 방법을 비교한 결과이며 아래 5개는 원자력 규제지침 및 기술표준과 비교한 결과이다. Table 12.에서 확인할 수 있는 바와 같이 제안된 사이버보안 평가 방법은 기존 사이버보안 방법[1]과 다르게 원자력 발전

소 소프트웨어 생명주기 각 단계인 개념, 요건, 설계, 구현, 시험, 설치 및 운영, 유지보수, 폐기 단계에서 사이버보안 활동과 평가 항목을 도출함으로써 각 단계에서 원자력 발전소 계측제어 시스템의 사이버보안성을 평가할 수 있는 방법론을 제시하였다. 또한 원자력 규제지침 및 기술표준[6]~[10]의 각 사이버보안 항목들을 조합하여 구성하였기 때문에 일반 IT 시스템에서 적용하는 사이버보안 평가 방법[3]~[5]과 다르게 원자력 발전소에 적용이 가능하다. 결론적으로 제안한 방법은 원자력분야에 적용가능하며 SDLC 단계에서 각 사이버보안 평가를 수행할 수 있는 방법이라는 것을 확인할 수 있다.

Table 12. Comparison Result

Categorize	SDLC	Assess-ment Level	Control Items	Applica-bility to NPPs
Youngdoo Kang[1]	X	O	O	O
MS-SDL [3]	O	X	O	X
CLASP[4]	O	X	O	X
Seven-Touchpoint[5]	O	X	O	X
IEEE 7-4.3.2[6]	O	X	O	O
NIST 800-64[7]	O	X	O	O
R-G 5.71[8]	X	O	O	O
NIST 800-53[9]	X	X	O	O
DHS[10]	X	X	O	O
Proposed	O	O	O	O

V. 결 론

원전 계측제어 시스템의 개발기관, 감사기관 및 규제기관의 많은 노력에도 불구하고 원전 계측제어 시스템의 특성 및 운영환경에 대한 정확한 분석을 통해 최상위 사이버보안 목표를 만족할 수 있는 상세 기술적 설계와 관리적 대응수단의 개발이 미흡한 실정이다. 따라서 본 논문에서는 원자력발전소 계측제어시스템에 사용되는 소프트웨어의 생명주기 각 단계에서 사이버보안을 평가할 수 있는 사이버보안 평가 항목을 도출하였고, 사이버보안 위협의 발생 가능성과 영향성 수준에 따라 사이버보안 수준을 산정할 수 있는 기준을 제안하였다.

본 연구의 결과물은 국내 원자력발전소 계측제어 시스템의 사이버 안전성 확보를 위한 정책 및 규제지침 개발시 기본 자료로 활용이 가능하며 규제지침을 통해 신규 및 가동중인 원전에서 발생할 수 있는 사이버공격에 대한 사전 방지 및 대응책을 마련하여 원전 안전성 향상을 달성하는데 이용될 수 있다.

차후 연구는 본 연구에서 제안한 사이버보안 방법론의 타당성 검증을 위해 원자력 발전소 사이버보안 평가 관련 과제를 수행하는 것이 중요할 것으로 판단된다. 이를 위해 원자력 발전소 계측제어 시스템의 기능 및 특성을 모두 만족할 수 있는 테스트베드 구축에 대한 선행 연구가 필요할 것이며 이에 따라 시스템 단위에서의 사이버보안 평가가 수행되어야 할 것으로 사료된다.

References

[1] Youngdoo Kang and Kil To Chong, "Development of Cyber Security Assessment Methodology for the Instrumentation & Control Systems in Nuclear Power Plants," Journal of academia-industrial technology, 11(9), pp. 3451-3457, Sep. 2010.

[2] James W. Over, Team Software process for Secure Systems Development, CMU Software Engineering Institute, Mar. 2002.

[3] Microsoft Corporation, Microsoft Security Development Lifecycle(SDL), Version 5.2, Microsoft Corporation, P.167, May. 2012.

[4] CLASP, https://www.owasp.org/index.php/Category: OWASP CLASP Project

[5] Gary McGraw, Software Security: Building Security In, Addison-Wesley Professional, P.448, 2006.

[6] IEEE Std. 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Aug. 2010.

[7] NIST SP 800-64(Rev.2), "Security

Considerations in the System Development Life Cycle," Oct. 2008.
[8] Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," Jan. 2010.
[9] NIST SP 800-53(Rev.4), "Security and Privacy Controls for Federal Information Systems and Organizations," Apr. 2013.
[10] U.S. Department of Homeland Security, "Catalog of Control Security : Recommendations for Standards Developers(Rev.7)," Apr. 2011.
[11] Sang-Hyun Lee, "Cybersecurity Laws in the U.S.:Focusing on Responses from the Legislative, the Judicial, and the Executive Body," Journal of the Korea Institute of Information Security and Cryptology,3(1), pp. 109-131, Jan. 2012.
[12] NEI 08-09(Rev.6), "Cyber Security Plan for Nuclear Power Reactors," Apr. 2010.

〈저자소개〉

서 달 미 (Dal-mi Seo) 정회원
2006년 2월: 충남대학교 컴퓨터공학과 졸업
2014년 8월: 충남대학교 컴퓨터공학과 석사
2011년 5월~현재: (주)엔에스이 선임연구원
〈관심분야〉 정보보호 표준, 평가 및 인증, 제어시스템 보안

차 기 종 (Ki-Jong Cha) 정회원
2010년 2월: 한밭대학교 정보통신공학전공 졸업
2012년 2월: 한밭대학교 정보통신공학과 석사
2012년 1월~현재: (주)엔에스이 선임연구원
〈관심분야〉 제어 시스템 보안, 디지털 계측 및 제어 시스템

신 요 순 (Yo-Soon Shin) 정회원
2010년 2월: 한밭대학교 정보통신공학전공 졸업
2012년 2월: 한밭대학교 전파공학과 석사
2013년 3월~현재: (주)엔에스이 선임연구원
〈관심분야〉 제어 시스템 보안, 디지털 계측 및 제어 시스템

정 충 희 (Choong-Heui Jeong) 정회원
1980년 2월: 아주대학교 전자공학 졸업
2000년 2월: 충남대학교 컴퓨터공학과 석사
2006년 3월: 충남대학교 컴퓨터공학과 박사과정 수료
1987년~1990년: 한국원자력연구소 연구원
1990년~현재: 한국원자력안전기술원 책임연구원
〈관심분야〉 디지털 계측 및 제어 시스템

김 영 미 (Young-Mi Kim) 정회원
1994년 2월: KAIST 전산학과 졸업
1996년 2월: 포항공과대학교 컴퓨터공학과 석사
2012년 2월: 충남대학교 컴퓨터공학과 박사
2002년 12월~현재: 한국원자력안전기술원 책임연구원
〈관심분야〉 소프트웨어공학