Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.3, June 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.3.471

원전 사이버보안 체계 개발 방안에 대한 연구

한 경 수,† 이 강 수‡
한남대학교 컴퓨터공학과

development plan of nuclear cyber security system

Kyung-soo Han,† Gang-soo Lee‡
Computer Engineering, Hannam University

요 약

산업제어시스템은 초기에 주로 아날로그 형태로 구축되었다. 그러나 산업발전에 따라 운영에 필요한 센서들이 증가하면서 시스템이 복잡해지고 정밀함이 요구되어 디지털 설계의 필요성이 높아졌다. 그런 필요성에 발맞추어 디지털 시스템들의 안정성은 크게 향상되었고, 최근에는 원전을 포함한 대부분의 제어시스템들이 디지털로 설계되고 있다. 산업제어시스템의 디지털 활용이 점차 개방화·표준화되면서 잠재적인 사이버 위협세력에 의한 제어시스템 침투 및 파괴 가능성이 매우 높아졌다. 이에 따라 국내·외에서는 위협의 식별과 효과적인 대책마련을 위하여 다양한 노력을 기울이고 있다. 본 논문은 관련지침 분석을 통해 제어시스템과 원전제어시스템의 공통되는 보안요구사항을 취하고, 향후 원전 인·허가 요건으로 필수적인 원전 사이버보안 체계 개발방안을 제안한다.

ABSTRACT

Industrial control system was designed mainly in the form of analog in early days. However, necessity of digital system engineering is increasing recently because systems become complicated. Consequently, stability of digital systems is improved so most industrial control systems are designed with digital.

Because Using digital design of Industrial control system is expanded, various threatening possibilities such as penetration or destruction of systems are increasing enormously. Domestic and overseas researchers accordingly make a multilateral effort into risk analysis and preparing countermeasures. In this paper, this report chooses common security requirement in industrial control system and nuclear control system through relevant guidelines analysis. In addition, this report suggests the development plan of nuclear cyber security system which will be an essential ingredient of planning approvals.

Keywords: Industrial control system, nuclear cyber security, nuclear security requirement

I. 서 론

산업제어시스템(Industrial Control System)이란 전력, 가스, 에너지설비, 철도 산업 등 대규모 산업 플랜트를 운영 관리하는 핵심 시스템으로 주요 하부구조에서 자주 사용되는 여러 가지 형태의 제어 시스템을 포함하는 일반적인 의미로 사용된다.

이러한 산업제어시설 전반에 PC나 소프트웨어 및 통신망의 적용이 확대되면서 산업제어시스템 보안에 대한 관심이 증가하고 있다. 일례로 2009년 이란의 핵시설에 'Stuxnet'악성코드가 감염되어 우라늄 원심분리기 가동이 중단되는 사태가 발생하였으며, 2011년 10월에는 제어시스템의 정보수집 및 유출을 목표로 제2의 'Stuxnet'으로 불리는 'Duqu' 악성코드가 발견되었다.

접수일(2013년 02월 18일), 수정일(2013년 5월 2일), 게재확정일(2013년 06월 07일)
† 주저자, psksmail@hnu.kr
‡ 교신저자, gslee@eve.hannam.ac.kr (Corresponding author)

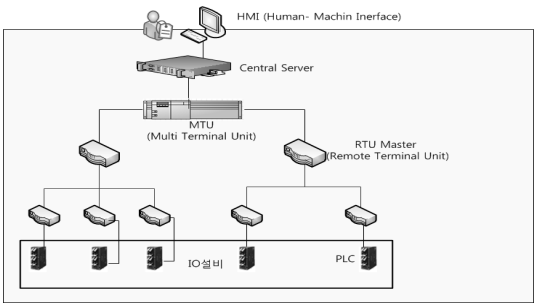
사이버공격에 의한 산업시설의 가동중단 및 오작동은 국가적으로 막대한 손실을 초래할 뿐만 아니라 국민의 생명위협과도 직결된다. 따라서 제어시스템의 사이버보안 적용은 필수적으로 요구된다.

본 논문은 계측제어시스템으로 운영되는 가동원전에 사이버보안을 적용하기 위한 기초 연구로 전체적인 구성은 다음과 같다. 2장에서는 일반적인 제어시스템과 원전 계측제어 시스템에 대한 개요와 정보보안에 대해서 알아본다. 3장은 원전 보안체계를 위한 제어시스템 관련된 지침들을 분석하며, 4장에서는 원전 사이버보안과 관련된 규정 및 지침을 분석한다. 5장에서는 원전 사이버보안 체계 개발을 위한 방안을 제시하며 6장에서 결론을 맺는다.

II. 제어시스템 정보보안

2.1 일반적인 제어시스템

국가적인 대규모 플랜트 시설들을 제어하는 산업제어시스템은 대표적으로 SCADA(Supervisory Control And Data Acquisition)시스템이 있다. 플랜트 상태를 감시하고 제어하기 위해 산업체에서 사용되는 시스템으로써 기록을 남기기 위한 설비가 제공된다.



〔그림 1〕 일반적인 SCADA시스템 구성도〔1〕

이러한 환경을 원방감시제어시스템, 분산제어시스템(Distributed Control System,이하 DCS) 또는 산업제어시스템이라 한다. 마스터-슬레이브 형태의 시스템인 SCADA는 하나의 마스터 노드를 갖는다. 마스터 노드는 슬레이브 노드에 명령과 프로세스 응답을 보내며, 슬레이브 노드는 마스터 노드의 요청 없이 데이터를 전송할 수 없고 다른 슬레이브와 통신할 수 없다. 하지만 국제 해킹보안 컨퍼런스 POC2011에서 Dismal이라는 공격 툴로 SCADA시스템의 마스터와 슬레이브에 악의적 명령을 내릴 수 있는 시연이 있었다. 네트워크 IP만 알면 공격이 가능하며 산업시설에 따라 어떤 시스템을 사용하고 있는지 정보를 수집할 수 있는 기능을 가지고 있다.

정보통신기술이 발달하고 네트워크 기술이 표준화되면서 산업제어시스템의 외부 공격에 대한 취약성 등과 같은 보안상의 과제가 지적되고 있다. 그동안 대규모 플랜트 시설들은 물리적 보안에만 주력했지만 앞으로는 해킹, 웜, 바이러스 등을 이용한 전자적 침해 행위에 대항하여 시스템을 안전하게 보호하기 위한 보안 요구사항이 필수적이다.

2.2 원전 계측제어시스템

일반적인 제어시스템의 개념으로 운영된다고 할 수 있는 원전계측설비(Man-Machine Interface System)는 계측제어(Instrumentation and Control 이하 I&C)와 주제어실 Man-Machine Interface을 포괄하는 개념이다. 편의성을 위해 인간공학과 결합되었다는 의미에서 Man-Machine Interface라는 표현이 들어간다〔2〕.

I&C계통의 분류는 원자로보호계통, 연동계통, 안전정지계통의 계측설비 및 안전관련 정보 등은 발전소 설계기준사건(Design Basis Event)에 대비하여 설계된다. DBE는 초기사건의 범주 내에서 정량적 분석을 통해 성능지수에 가장 큰 영향을 미치는 경계사건을 선택하여 결정된다〔3〕.

I&C 시스템은 원전 운전에 대한 보호와 감시 및 시스템 제어기능을 수행하며, PLC(Programmable Logic Controller) 및 DCS를 기반으로 설계, 제작된다.

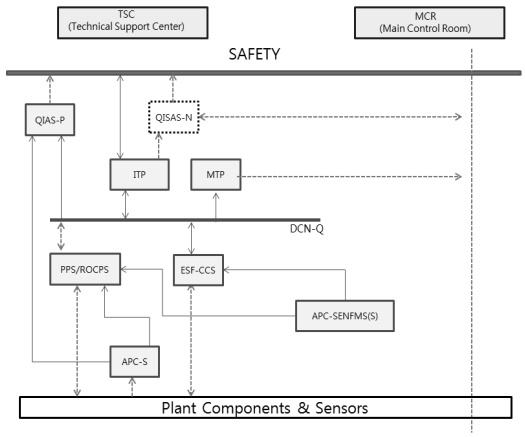
일반적으로 PLC의 중앙처리 장치인 CPU는 마이크로프로세서 및 메모리로 구성되며, 인간의 두뇌 역할을 한다. 입·출력부는 외부 기기와 신호를 주고받으며, 전원부는 각 부에 전원을 공급하는 역할을 한다. 주변 장치인 PC나 레이저 거리 센서(Laser Sensor Handy Loader)는 PLC내의 메모리에 프로그램을 기록하는 기능을 담당한다〔4〕.

2.3 원전 I&C 사이버보안 대상

미국 원자력규제위원회의 규제지침(Regulatory Guide 5.71 이하 RG 5.71)에 근거하여 계측제어계통의 안전 및 관련된 기능을 수행하는 시스템 또는

기기를 필수 계통으로 분류하고, 필수 계통은 사이버 공격이나 테러 등의 위협으로부터 고유기능 수행에 영향 받지 않도록 보호되어야 한다.

국내에서도 원자력 규제지침서 8.22절에 원자로시설의 안전 보장을 목표로 하는 사이버보안 필수적용 범위를 디지털기반 계측제어계통 및 기기로 지정하고 있다. 아래 [그림 2]는 신울진 1,2호기의 안전계통에 해당하는 사이버보안 적용범위를 구분한 것이다.



[그림 2] 신울진 1,2호기 사이버보안 적용 범위[5]

필수적용 대상 이외의 안전기능을 수행하지 않는 계측제어계통 및 기기는 규제지침에서 요구하는 모든 사이버보안 활동의 이행을 요구하지 않지만, 이들 계통 및 기기로부터 발생하는 사이버 위협으로 인해 안전기능 수행에 영향이 없음을 보장하기 위한 사이버 위협 분석은 요구된다.

III. 제어시스템 보안요구사항 동향 분석

3.1 공통평가기준

공통평가기준 CC(Common Criteria)은 정보보호제품의 보안성을 평가하기 위한 국제 기준(ISO 15408표준)이다. 보안기능의 안전성과 신뢰성을 국가차원에서 보증하여 정보보호시스템을 안전하게 사용할 수 있도록 지원하는 제도이다.

정보기술 제품 및 시스템의 보안기능과 보안기능의 평가과정에 적용되는 보증수준에 대한 공통의 요구사항을 제시함으로써 독립적으로 수행한 보안성 평가 결과들 간의 상호 비교를 가능하게 한다. CC의 보안기능요구사항은 주로 IT정보보호제품을 평가하기위해 주로 사용되고 있지만, 오직 IT제품에만 국한되지 않는다.

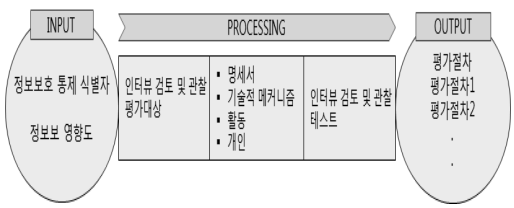
아래 [표 1]은 공통평가 기준 보안기능요구상의 전체적인 구조를 나타낸다. 클래스, 패밀리, 컴포넌트, 엘리먼트의 계층관계를 갖으며 보안기능 및 보안메커니즘을 정의하는데 표준이 될 수 있는 기능 컴포넌트의 집합이라고 할 수 있다.

[표 1] 공통평가 기준 보안기능 요구사항 구조[6]

구 분	설 명	예 제
클래스	동일한 보안목적을 가지는 패밀리들의 모음	FAU (보안감사)
패밀리	동일한 보안목적을 가지지만 강조점이나 엄격함이 서로 다른 컴포넌트의 모음	FAU_ARP (보안감사 자동대응)
컴포넌트	엘리먼트의 집합으로서 보호프로파일, 보안목표명세서, 패키지에 포함될 수 있는 가장 작은 선택단위	FQU_ARP.1(보안 경보)
엘리먼트	분할할 수 없는 보안요구사항의 최소단위	FAU_ARP.1.1

3.2 SP 800-53A 정보보호 통제 평가 지침

NIST SP 800-53A(Guide for Assessing the Security Controls in Federal Information Systems and Organizations)는 2010년 6월 미국 국가표준기술 연구소의 정보보호 통제 평가지침이며, 연방기관 정보시스템의 보안대책 선택 지침을 제공한다. 정보를 처리, 저장, 전송, 수신하는 정보시스템에 적용하며 평가 대상은 명세서, 기술적 메커니즘, 활동 및 개인 등 4가지 객체를 포함하고 있다.



[그림 3] 정보보호 통제평가 절차 개발을 위한 프레임워크[7]

- 명세서: 정책, 절차, 계획서, 정보보호 요구사항, 아키텍처 설계 등 기술한 문서
- 메커니즘: 하드웨어, 소프트웨어, 펌웨어 등
- 활동: 백업이나 네트워크 트래픽 모니터링과 같은 시스템 지원 및 보호 활동
- 개인: 명세서, 메커니즘, 활동을 적용하는 개인이나 집단

평가 방법은 인터뷰, 검토 및 관찰(examine), 테스트로 구분되는데, 방법의 주요 속성으로 적용범위(scope), 적용대상(coverage) 및 심도(depth)를 고려하고 있다. 적용대상은 모든 방법에 적용되며 부록 D에 각 평가 방법에 대한 구체적인 정보를 수록하고 있다. 심도는 인터뷰와 검토 및 관찰에 적용되며, 적용범위는 테스트방법에만 적용된다.

〔표 2〕 NIST SP 800-53A의 보안요구사항[7]

Class	Family	식별
기술	식별 및 인증 (Identification and Authentication)	IA
	접근제어 (Access Control)	AC
	감사 및 책임 추적성 (Audit and Accountability)	AU
	시스템 및 통신 보호 (System and Communications Protection)	SC
운영	인적자원 보안 (Personnel Security)	PS
	물리적, 환경적 보호 (Physical and Environment Protection)	PE
	비상계획 (Contingency Planning)	CP
	형상관리 (Configuration Management)	CM
	유지보수 (Maintenance)	MA
	시스템 및 정보 무결성 (System and Information integrity)	SI
	미디어 보호 (Media Protection)	MP
	사고 대응 (Incident Response)	IR
	인식제고 및 훈련 (Awareness and Training)	AT
관리	위험평가 (Risk Assessment)	RA
	계획 (Planning)	PL
	시스템 및 서비스 구매 (System and Services Acquisition)	SA
	인증/승인 (Certification, Accreditation and Security Assessments)	CA

3.3 NIST SP 800-53 R3 보안기능 요구사항

NIST SP 800-53 Revision3는 특정 산업기관의 장비, 또는 정보의 흐름을 검사하는 절차와 개념을 설명하기 위해 확장된 문서다[8]. 정보시스템과 제어시스템의 운영적 차이를 고려하여 기존의 NIST SP 800-53A의 보안요구사항 일부를 제외시켰다.

산업제어시스템에 대한 최소한의 보안요구사항을 나타내며 〔표 3〕는 기존 SP 800-53A와 보안기능요구사항의 차이를 나타낸다.

〔표 3〕 SP 800-53A 와 Revision3 비교

Class	SP-800-53A	SP-800-53-R3
관리	RA	○
	PL	
	SA	
	CA	○
운영	PS	
	PE	○
	CP	○
	CM	
	MA	○
	SI	○
	MP	○
	IR	
	AT	
기술	IA	○
	AC	○
	AU	○
	SC	

3.4 국토안보부 제어시스템 지침

2001년 9.11테러 이후 부시대통령은 미국 행정부 내의 각 부처에 분산된 대 테러기능을 통합할 목적으로 '국토안보법'을 제정하고, FBI의 국가기반시설보호센터와 상무부의 CIAO등을 통합한 국토안보부를 신설하였다. 연방정부에 관한 정보보안활동의 관리, 감독권을 부여받았고, 물리적 보안 및 사이버보안의 총괄 조정업무를 담당한다[9].

2003년 부시대통령은 국가 사이버보안 대응 시스템 구축, 국가 사이버보안 위협과 취약성 감소 프로그램 실시, 보안인식 및 훈련프로그램운영, 정부 영역 사이버보안 강화 및 국가 보안과 국제 사이버보안 활동 협력의 강화라는 5가지 목표를 위시한 '국가 사이

버안보를 위한 국가전략'을 발표하였다.

미 정부가 이러한 업무권한을 국토안보부에 일임하면서 국토안보부의 역할은 더욱 중요해졌다. 이후 NIST에 연방정보 및 정보시스템의 보안강화를 위한 관련지침과 표준을 개발, 제정하도록 하여 연방정보보안의 기능을 담당하도록 하였다.

국토안보부의 2009년 9월 '제어시스템 보안 카탈로그'는 제어시스템에 대한 통제항목을 상위 수준의 지침으로 개발한 것이다. SP 800-53A의 구조와 유사하며 19개의 패밀리 계층을 가지고 있다.

IV. 원전 ICS관련 사이버보안 지침 분석

원자력 규제 기관은 사이버테러에 대비한 법령을 공포하고, 그 대책을 원전에 적용하도록 요구하고 있다. 미국 원자력 규제위원회 (Nuclear Refulatory Commission, 이하 NRC)에서 2006년 발행한 규제지침 Regulatory Guide 1.52(Rev.03)는 최초의 관련 인허가지침이며, 2010년 규제지침 RG 5.71을 발표하면서 사이버보안의 적용범위를 안전관련 MMIS계통에서 보안시스템과 비상대책시스템으로 확대하고 있다.

〔표 4〕 제어시스템 카탈로그와 SP 800-53R3 비교

Class	제어시스템 카탈로그	식별	SP 800-53-R3	식별
기술	접근통제	1	접근통제	AC
	감사 및 책무	16	감사 및 책무	AU
	시스템 및 통신보안	8	시스템과 통신보안	SC
	식별 및 인증	15		
운영	매체보호	13	매체보호	MP
	인사보안	3		
	시스템과 정보 무결성	14	시스템과 정보 무결성	SI
	시스템 개발 및 유지보수	10	유지보수	MA
	물리적 및 환경적 보안	4	물리적 및 환경적 보호	PE
	사건대응	12		
			비상계획	CP
	보안 인지 및 훈련	11		
	형상관리	6		
관리	시스템 및 서비스 획득	5		
	위험관리 및 평가	18	보안평가/인가	CA
	보안정책	1		
	제어시스템 보안정책 감시 및 검토	17		
	전략적 계획	7		
	조직 보안	2		
	정보 및 문서관리	9		

한국원자력안전기술원(Korea Institute of Nuclear Safety, 이하 KINS)에서도 2007년 규제지침 GT-N27을 발표하고, 신규 원전에 사이버보안 대책 기술을 적용하도록 권고하고 있다. 또한 국가정보원에서도 2010년 국내 가동원전에 대해 사이버보안 취약성분석 및 대책을 수립하도록 요구하고 있다〔10〕.

4.1 국내 KINS 계측제어 계통의 사이버보안 정책

KINS는 원자력의 생산 및 이용에 따른 방사선 재해로부터 국민을 보호하고 공공의 안전과 환경을 보전하기 위해 설립된 원자력 안전규제전문기관이다〔11〕. 2011년 원전 규제지침에 8.22절 "계측제어계통의 사이버보안"을 추가시켰다.

〔표 5〕 KINS 원전 계측제어 사이버보안 정책 항목〔12〕

정 책	내 용
사이버보안 정책	필수 디지털 보호대상의 관리적 사항
	사이버보안조직 및 인적자원에 관한 사항
	사이버보안 대상의 분류 및 사이버보안 수준에 관한 사항
	접근제어 및 감시에 관한 사항
	통신망 보안에 관한 사항
	사이버 보안에 관한 사항
	캐비닛의 시건장치 등을 포함한 물리적 보안에 관한 사항
	사이버보안사건 대응 체계에 관한 사항
	시스템 개발 및 유지보수에 관한 사항
	취약성 분석 및 주기적 평가에 관한 사항
	기타 관리적 및 기술적 사항

즉, 원자로 시설 안전 계측제어계통이 디지털 기반기술 취약성을 악용한 사이버 위협에 대응할 수 있도록 설계되고 운영됨을 보장한다는 것이다. 디지털-기반 기술의 본질적인 특성을 악용한 사이버 위협으로 인해 안전기능을 수행하는 디지털 계측제어계통이 요구되는 기능을 상실한다면, 해당 원자로시설의 안전상에 중대한 문제가 생길 수 있다.

4.2 미국 RG 5.71 원전사이버보안 지침

미국 원자력규제 위원회는 2010년에 원전사이버보안 적용범위를 원전 계측제어계통, 보안시스템 및 비상대책시스템으로 확대한 규제지침 RG 5.71을 발표

하였다. 부록 부분에 통제 항목이 기술되어 있으며 〔표 6〕과 같이 구분할 수 있다.

〔표 6〕 RG 5.71 보안통제 항목〔13〕

Class	Family	식별
기술	접근통제	B.1
	감사 및 책임성	B.2
	핵심 디지털 자산 및 통신보안	B.3
	식별 및 인증	B.4
	시스템 강화	B.5
운영	매체 보호	C.1
	인사보안	C.2
	시스템 및 정보 무결성	C.3
	유지보수	C.4
	물리적 및 환경적 보호	C.5
	방어 전략	C.6
	심층방어	C.7
	사건대응	C.8
	안전, 보안, 및 비상 준비성 기능의 비상계획/연속성	C.9
	의식 및 훈련	C.10
	형상관리	C.11
관리	시스템 및 서비스 획득	C.12
	보안평가 및 위험 관리	C.13

기술적 통제 요구사항은 RG 5.71 APPENDIX B 부분의 모든 통제 항목을 포함한다. 운영적 보안통제 요구사항은 RG 5.71 APPENDIX C 부분의 통제번호 C.1 매체보호 ~ C.11 형상관리이며, 관리적 보안통제 요구사항은 통제번호 C.12 시스템 및 서비스획득 ~ C.13 보안평가 및 위험관리로 나눌 수 있다. “원자력 설비를 위한 사이버보안 프로그램”인 이 지침에 근거하여 계측제어 계통의 안전 및 안전에 관련된 기능을 수행하는 기기를 필수 계통으로 분류하고, 필수 계통은 사이버 공격이나 테러 등의 위협에도 고유 기능 수행이 영향을 받지 않도록 설계되어야 한다.

V. 원전 사이버 보안체계 개발 방안

국내 원전 근무자들은 기술적으로는 사이버보안과 관계가 없다는 인식이 있었다. 하지만 미국 원전 제어통신망을 겨냥한 공격사례와 이란의 ‘Stuxnet’, 기반시설 및 제어시스템을 대상으로 한 정보수집 목적의 악성코드 ‘Duqu’, ‘Flame’등이 발견됨에 따라 국내 원전도 제어시스템 공격이 가능해질 것으로 예상된다. 따라서 원전을 겨냥한 사이버 공격에 대한 보안대책을 세워야하며 전체적인 보안체계는 다음과 같아야 한다.

- 사이버 보안 정책 및 계획문서의 개발필요
- 사이버보안 조직의 구성과 사이버 위협의 분석 계획
- 사이버 보안성평가

원전의 사이버보안을 고려한 계측제어 시스템 설계 시 RG 5.71의 보안통제를 수용하기 위한 활동을 모델링 하였다. 조직 운영의 보안 책임자들을 구분하고 지침의 통제항목을 수행하기 위해 문서 및 정책을 개발하거나 참조하는 구조를 제안한다.

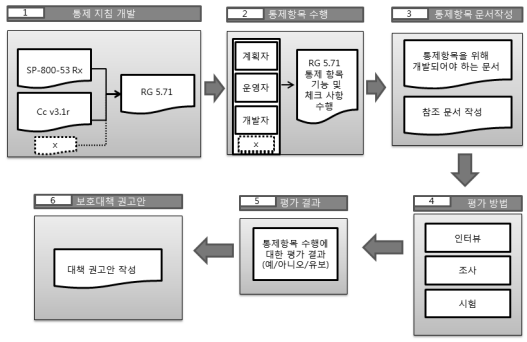
5.1 사이버보안 구축 지원 시스템 체계

원전 사이버보안 보안통제를 이행하기 위해서는 RG 5.71을 기준으로 제어시스템 보안기능 요구사항을 위주로 다루는 SP 800-53-R3와 참고할 사항으로 CC V3.1r의 보안기능 요구사항을 체크리스트 항목으로 제시하는 것이 이상적이다. 하지만, 향후 원전 사이버보안 상세 이행지침이 개발 되어질 것으로 보이며, 제어시스템 설계 및 개발에 필요한 보안이행 체크리스트의 질의 항목은 업데이트 되어져야 한다.

통제 항목을 수행하기 위해서는 우선 조직의 명확한 보안 책임자 구분이 필요하다. 〔그림 4〕는 본 논문에서 제안된 원전 사이버보안 평가 체계를 나타낸다.

조직의 보안담당자 RG 5.71의 통제항목을 수행하기 위해서는 각각의 통제항목에 필요한 문서 및 정책을 개발해야한다. 이를 위해 기능 및 체크사항에는 통제항목에서 필요로 하는 개발 문서나 정책 및 절차 등의 내용을 담고 있다.

기능 및 체크사항이 예외사항 없이 수행이 되면 인터뷰/조사/시험을 거쳐 통제항목의 적용을 확인한 후 최종적으로 통제항목수용에 대한 평가결과를 얻을 수 있다. 위와 같은 방법은 향후 디지털 계통을 위한 보



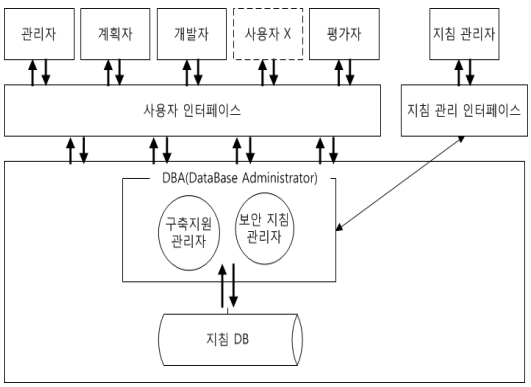
〔그림 4〕 제안된 사이버 보안 평가 모델

안 장비의 인허가를 위해 평가 방법론을 이용한 평가 인증 문서로 활용될 수 있다.

5.2 지침 데이터베이스 구조

원전 각 보안 책임자별로 인터페이스를 구축하고 통제지침데이터베이스에서 필요한 활동을 수행한다. 지침 관리자 DBA(Data-Base Administrator)는 DB시스템과 관련된 모든 자원을 기획, 통제 하며 전체적인 관리 운영을 책임진다.

특히 저장될 데이터의 형태, 구조 등 데이터베이스의 저장에 관한여러 가지 사항을 정의하는 기능, 데이터베이스의 자료를 사용자가 이용할 수 있도록 요구에 따라 검색, 갱신, 삽입, 삭제 등을 지원하는 기능, 데이터의정확성과 안전성 유지를 위한 데이터의 무결성 유지, 보안, 병행 수행 제어 등을 수행하는 관리 기능을 제공해야 한다.



〔그림 5〕 지침 데이터베이스 구조

지침 DB는 NRC에서 개발 중인 원전 사이버보안 관련 규제지침을 각각의 역할자들이 확인할 수 있게 질의하는 내용으로 제시하기 때문에 구축지원 관리자는 각각의 인터페이스에 지침 DB 질의 내용을 제공할 수 있어야한다. 지침 관리자는 지속적으로 개발되는 사이버보안 이행지침을 DB에 업데이트 시켜야하며, 지침DB에 접근하는 구축지원 관리자와 보안지침관리자의 DB는 분리되어 운영하는 것이 이상적이다.

VI. 결 론

본 논문은 제어시스템 사이버보안과 관련된 지침 등을 통해 보안기능요구사항을 도출하고, 설계된 I&C시스템의 사이버보안 검증을 위한 자료를 제시할 수 있도록 제안하였다. 특히 원전 안전계통 I&C시스템에 적용되는 보안지침 이외에도 공통평가기준의 운영환경에 대한 주기적인 보안성 검토, 형상관리, 감사를 위한 사이버보안 지침을 수용 하여 보다 폭넓은 보안제어를 가능하게 할 수 있어야한다.

공통평가 기준의 적용은 원전에 도입될 정보보안제품의 보안요구사항으로 사이버보안 대상시스템에 존재하는 위협별 대책마련을 위한 보안목적을 설정하고 시스템의 설계가 일관성 있게 진행되기 위한 기초 연구가 될 수 있다.

원자력발전소 I&C 설계문서 보안과 운영 특수성으로 인해, 정보기술 분야에서의 사이버 보안성평가 방법 등을 원전의 계측제어 시스템에 직접 적용하기에는 어려움이 따른다.

원전의 사이버보안 체계를 고려하기 위해서는 계측제어시스템의 특성 및 운영환경에 대한 정확한 분석이 선행되어야하며, 이후 분석된 내용을 바탕으로 상위 사이버보안 목표를 만족할 수 있는 상세기술적설계와 관리적 대응수단이 개발되어야 한다.

하지만 현재는 미국의 지침을 따라갈 수밖에 없는 실정이다. 원전 사이버 보안은 향후 국내 신규 및 가동 원전과 관련시설에 반드시 적용하여야 하는 기술이며 원전의 인허가 요건이다. 따라서 향후 산업제어시스템의 특성인 가용성을 보장 및 운영 단계에서 요구되는 대상 I&C 시스템에 대한 위험분석 및 평가 체계를 향후 과제로 남긴다.

참고문헌

〔1〕 NIST, Special Publication 800-52, "Guide to Industrial Control systems(ICS) Security," June. 2011.

〔2〕 KINS/HR-1011, "Methodology Development for Establishment of Licensing Basis Events and Safety Analysis of GEN-IV Reactors," February. 2010.

〔3〕 KINS/RG-N08.01, 한국원자력안전기술원, "계측제어계통의 안전등급 분류기준 및 체계," pp. 594, 2011년 7월.

〔4〕 NUPIC2012 원전계측제어 심포지엄, "건설원전 사이버보안 적용현황," 2012년 11월.

〔5〕 http://www.hrd.go.kr/jsp/HRDP/HRDP400/HRDP420/HRDP421/HRDP421_1

List.jsp,
〔6〕 CC, "Common Criteria for Information Technology Security Evaluation," Version 3.1 Revision 3, CCMB-2009-07-001, http://www.commoncriteriaportal.org, July. 2009.
〔7〕 NIST, Special Publication 800-53A Revesion 1, "Guide for Assessing the Security Controls in Federal information Systems and Organizations," June. 2010.
〔8〕 NIST, Special Publication 800-53 Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," August. 2009.
〔9〕 이상현, "미국의 사이버보안 법제도,"internet and information security, 제3권 제1호, pp. 109~131, 2012년 1월.
〔10〕 권기춘, "명품 원전mmis를 위한 원자력과 IT융합," 정보통신산업진흥원, 2010년 9월.
〔11〕 www.kins.re.kr, "About KINS".
〔12〕 KINS/RG-N08.01, 한국원자력안전기술원, "계측제어계통의 안전등급 분류기준 및 체계," pp.684, 2011년 7월.
〔13〕 NIST, Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," January. 2010.

〈저자소개〉

한 경 수(Kyung-soo Han) 정회원
2011년 2월: 한남대학교 컴퓨터공학과 졸업
2013년 3월~현재: 한국대학교 전자공학과 석사
〈관심분야〉 소프트웨어공학, 보안공학, 정보보호이론, 제어시스템 사이버보안

이 강 수(Gang-soo Lee) 정회원
1983년 3월: 서울대학교 전산학(이학 석사)
2013년 3월: 서울대학교 전산학 박사(이학 박사)
1987~현재: 한남대학교 컴퓨터공학과 교수
〈관심분야〉 소프트웨어공학, 보안공학, 멀티미디어교육, 제어시스템 사이버보안