Regular paper
Journal of the KIECS. pp. 1-8, vol. 11, no. 1, Jan. 31 2016, t. 69, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2016.11.1.1

원전 사이버보안을 위한 접근제어 요건분석 및 구현방안

김도연*

Implementation Plan and Requirements Analysis of Access Control for Cyber Security of Nuclear Power Plants

Do-Yeon Kim*

요 약

원자력발전소는 주요 국가기반시설로 보호되고 있으며, 계측제어계통은 보호, 제어 및 감시등의 기능을 수행하는 원전을 구성하는 핵심 설비로서, 과거의 아날로그 장비에서 컴퓨터와 네트워크에 기반 한 디지털 기술로 진화하고 있다. 또한, 계측제어계통에서는 대부분 원전용 제어기를 사용하지만, 일반적인 IT 자원의 사용도 증가하고 있는 실정이다. 스턱스넷으로 인한 원자력 시설의 제어기 침해 사고 및 여타 원전의 사이버 사고로 인해 원자력발전소에 대한 사이버보안 문제가 대두되고 있다. 본 논문에서는 원전 사이버 보안을 위해 규제지침의 접근제어 요건분석을 통하여 원전 계측제어계통에 적용 가능한 혼합형 접근제어 모델을 제시하였다. 제안하는 혼합형 접근제어 모델은 가동 중인 국내 원전 및 건설 중인 신규 원전에 구현하여, 원전의 안전성을 효율적으로 증대 시킬 수 있을 것으로 판단된다.

ABSTRACT

The Nuclear Power Plants(: NPP) are being protected as national infrastructure, and instrumentation and control(: I&C) systems are one of the principle facilities of the NPP, which perform the protection, control, and monitoring function. The I&C systems are being evolved into digitalization based on computer and network technology from analog system. In addition, the I&C systems are mostly employ the specialized logic controllers which are dedicated for the NPP, but the usage of generalized IT resources are steadily increased. The cyber security issues for the NPP are being emerged due to cyber incidents by Stuxnet and various accidents in the NPP. In this paper, hybrid access control model is proposed which are applicable to I&C system by analyzing the access control requirements specified in regulatory guides. The safety of in-service and under construction of NPP are effectively increased by applying proposed hybrid model.

키워드

Cyber Security of Nuclear Power Plants, Access Control, Stuxnet
원전 사이버 보안, 접근 제어, 스턱스넷

I. 서 론

원전의 계측제어계통은 원전을 안전하게 운전하기 위해 계측, 제어, 보호 및 감시 기능을 수행하는 설비로서, 아날로그 기술에서 컴퓨터와 데이터통신망을 기반으로 하는 디지털 기술로 빠르게 진화하고 있다. 또

* 교신저자 : 순천대학교 컴퓨터공학과
• 접 수 일 : 2015. 10. 26
• 수정완료일 : 2016. 01. 13
• 게재확정일 : 2016. 01. 24
• Received : Oct. 26, 2015, Revised : Jan. 13, 2016, Accepted : Jan. 24, 2016
• Corresponding Author : Do-Yeon Kim
Dept. of Computer Engineering, Sunchon National University,
Email : dykim@sunchon.ac.kr

한, 원전 계측제어계통에서 기존에 사용하던 산업용 제어기기 대신 일반적인 IT 자원을 사용하는 비율이 증가하고 있어, 원전의 사이버 보안 문제가 제기되고 있다[1]. 사이버 공격에 의해 원전 계측제어계통을 대상으로 임의 조작이 발생하면 원전의 운영 중단 및 파손 등의 심각한 사태를 야기시킬 수 있다. 지금까지 원전의 계측제어계통은 전용 통신망의 사용, 고유의 운영체제의 사용 등으로 인하여 사이버 위협에 안전하다고 여겨져 왔지만, 원전 계측제어시스템의 개방화 및 표준화에 의해 사이버 위협에 대한 취약점이 증가하고 있으며, 최근 국외에서 수집된 사이버 침해 사례를 보면 더 이상 해킹 및 사이버 테러 등의 사이버 위협에 안전 할 수 없는 현실이다 [2]. 원자력발전소 계측제어계통은 일반 IT 시스템과 비교해 볼 때 폐쇄성, 자원의 특수성, 운용 가용성 등의 측면에서 차이점이 있다. 폐쇄성은 인터넷과 같은 외부 네트워크와 분리된 내부의 필드 장비들만 연결하는 폐쇄적인 네트워크를 사용하면서 독자적인 설비 시설에서 개별적으로 운영되는 특징이 있으며, 특수성은 독자적인 프로토콜 및 임베디드 운영체제가 사용되고 하드웨어 역시 독자적인 변형을 가지는 장비가 사용되며, 가용성은 상시 작동할 수 있도록 운영되는 특징을 가지고 있다[3]. 원전 계측제어계통은 주요 기반시설로써 사이버 공격으로 인해 기능이 마비되면 국민의 생명, 생활, 재산, 국가 경제에 중대한 영향을 끼쳐 국가경제에 커다란 혼란을 초래할 수 있는 관계로, 원전 계측제어계통에 대한 사이버 보안은 강화되어야 한다[4-6]. 본 논문에서는 원전 사이버 보안을 위해 정의된 규제지침의 접근제어 요건분석을 통한 구현방안에 대해 논하고자 한다. 2장에서는 원자력 설비 및 시설들에 대한 사이버침해 사례를 열거하고, 3장에서는 규제지침 및 관련 연구 동향에 대해 기술하며, 접근제어를 위한 보안통제 요건을 4장에서 기술하고, 5장에서는 요건분석을 통한 원전 적용 방안에 대해 논하고자 한다.

II. 원자력시설의 사이버보안 침해 사례

2.1 부쉐르 우라늄 농축시설 사고

스턱스넷(Stuxnet)은 2010년 이란의 부쉐르 우라늄 농축시설의 원심분리기 가동을 중단시킨 웜-바이러스 형태의 사이버 공격 코드이다. 스턱스넷은 원심분리기를 기동시키는 SCADA 시스템 중 독일 지멘스(Siemens)사의 SIMATIC PCS7 시스템을 공격하도록 설계 되어 있으며, PCS7의 다양한 컴포넌트 중 SIMATIC WinCC7와 SIMATIC Step7이라 불리는 통합 관리 도구를 공격 대상으로 삼고 있다. 스턱스넷은 Step7의 일부 구성 요소를 자신이 생성한 파일로 교체시켜 산업자동화 제어 시스템을 모니터링 하거나 임의의 블록(악성 명령어 블록)을 생성시켜 제어하게 된다. 이렇게 장악된 시스템은 공격자가 제어하게 된다[7].

2.2 Davis-Besse 원전 사고

2003년 SQL 슬래머 웜이 미국 오하이오에 위치한 Davis-Besse 원자력발전소의 감시계통 컴퓨터에 감염되어, 관련 설비의 작동이 5시간 이상 불능 상태로 유지되었으며, 여타 발전소 제어 망 통신에도 영향을 미친 것으로 보고되었다[8].

2.3 Browns Ferry 원전 사고

2006년 두 개의 원자로 재순환 펌프의 고장으로 수동 정지되는 사고가 발생했다. 발전소컴퓨터시스템 네트워크에 연결된 이중의 PLC에 의해 작동되도록 설계된 재순환펌프의 VFD(: Variable Frequency Drive) 제어기가 반응하지 않았다. 조사결과, 발전소컴퓨터시스템 네트워크의 과도한 트래픽으로 기인된 사고로 분석되었으나, PLC 자체의 고장인지, 아니면 과도한 네트워크 트래픽으로 인한 VFD 제어기의 미 반응 결과인지에 대한 확인은 이루어지지 않았다. 이는 확인되지 않은 네트워크의 취약점으로 인한 정지사고로 추측할 수 있다[9].

III. 규제지침 및 연구 동향

미국의 원자력규제위원회(Nuclear Regulatory Commission)는 원자력 시설의 디지털 컴퓨터와 통신

시스템, 네트워크를 사이버 공격으로부터 보호하기 위한 규제지침으로 Regulatory Guide(: RG) 5.71을 발간하였다. RG 5.71은 미 연방법 10CFR73.54에서 명시한 사이버보안에 대한 법령을 보다 구체화한 규제지침으로 사이버 공격으로부터 보호해야 하는 디지털 자산을 식별하여 주요 디지털자산(Critical Digital Asset)이라 명명하고 있다. 규제지침은 식별된 방어 아키텍처와 포괄적 보안 통제수단을 적용하여 CDA의 사이버 보안 위협 가능성을 처리하도록 하고 있으며, 사이버 보안 적용 범위를 SSEP(: Safety, Security, Emergency Preparedness) 기능을 수행하는 CDA로 규정하고 있다. RG 5.71은 1) 디지털 컴퓨터와 통신시스템, 네트워크를 분석, 2) CDA 식별, 3) 방어 아키텍처 적용, 4) CDA의 잠재적 사이버 위험 처리의 과정을 수행하는 사이버 보안 프로그램을 작성하고, 사이버 보안 수명주기 활동을 이행하는 사이버 보안 프로그램 유지하도록 명하고 있다 [10]. 원전 안전성 확보를 위해 국내/외적으로 규제기관에서 원전 사이버보안에 대한 규제지침개발 및 규제대상 범위 확대가 이루어지고 있으며, 이에 상응하는 원전 사이버보안 구현은 물리적 격리 및 전략 이행계획 수립 등으로 이루어지고 있다. 지속적으로 보편화되어 가는 사이버 공격기술에 대해서는 산업계 보안기술의 적용으로 이루어지고 있으나, 디지털화가 진행 중인 원전에 대한 고도화된 특정 대상 공격에 대해서는 첨단 기술개발을 통해 선제적 대응 기술 개발 노력이 필요하다. 미국의 경우, 기존 원전은 계측제어계통이 아날로그시스템이 대부분이고 디지털 기술이 적용되는 신규 원전에 대한 건설이 활발하지 않음에도 불구하고, 사이버보안에 대한 필요성을 인식하고 원전 적용 기술 개발이 활발히 진행 중이다. 국내에서는 원전 디지털 안전계통을 국산화하는 과정을 통하여 개발되는 계통에 대한 취약점 분석이 수행된바 있다. 다른 나라에 비해 신형 원전 개발과 신규 원전 건설 및 원전 해외수출이 활발한 국내에서는 사이버보안에 대한 체계적인 연구를 위하여 기술체계 분석 및 방향 설정을 수립한 후에 원전 특성에 맞는 기술개발 추진이 필요한 실정이다[11].

원전 계측제어계통은 크게 원전 안전을 보장하기 위한 안전계통과 효율적인 전력생산과 관련한 비 안전계통으로 구분된다. 안전계통은 원전 운전 시 이상상태가 발생하면 즉시 원자로를 정지시키고 안전 상태로 유지시키는 원전 고유한 시스템이다. 안전계통은 대부분 공급회사가 제한적인 원자력 전용의 장비를 사용하고 있으며, 이들은 예상가능한 모든 원전 사고 상태에서도 운전이 가능하도록 설계된다. 비 안전계통은 원전의 효율적인 운전에 필요한 제어계통 및 감시계통으로 구성되며, 일부 상용 장비를 채택하고 있지만, 많은 부분에서 원전 사업자가 요구하는 설계사양을 만족하도록 재설계되어 있다. 전 세계적으로 가동중인 원전은 외부 망 차단을 통해 원전 계측계통에 대한 원격 사이버 공격이 가능한 접근경로를 원천적으로 차단하고 있다. 또한, 신규 원전의 경우 계측제어계통 설계과정에서 물리적 보안 및 접근통제 강화, 심층 방어구조 적용 등을 통해 사이버보안에 대한 대비를 하고 있다. 현재 계측제어계통에 직접 적용 가능한 사이버보안 기술이나 기기는 많지 않으며, 연구기관 산업체가 이들 개발을 위한 관 연구개발을 추진중에 있다[12].

Ⅳ. 접근제어를 위한 보안통제 요건

원자력발전소의 사이버보안에 적용되는 규제지침은 R.G. 5.71[8]로서, 원전의 안전계통, 안전기능에 중요한 계통, 보안기능, 비상대응설비 및 이들을 보완하는 계통 및 장비들에 적용되는 디지털 컴퓨터, 통신계통 및 네트워크를 보호할 목적으로 활용된다. 본 규제지침에서는 원전의 사이버보안계획서 작성을 통한 기술적인 통제, 운영적인 통제 및 관리적인 통제를 적용하도록 규정하고 있다. 본 논문에서는 기술적인 통제의 항목 중의 하나인 접근제어와 관련된 규제 요건에 대해 논한다.

○ 접근제어 정책 및 절차

유틸리티는 공식적이고, 문서화된 접근제어 정책 및 절차를 개발하고 주기적으로 검토해야 하며 다음 사항에 대해 언급해야 한다.

- 접근제어 권한 및 특권
- CDA(: Critical Digital Asset) 관리
- 패스워드 및 키 데이터베이스 보호
- CDA 감사
- 직무 분리

○ 계정관리
- CDA 계정에 대한 문서화 및 관리
- 접근제어목록과의 일치성 여부 판단을 위한 CDA 계정 검토
- 접근 권한 부여 및 업무 기능 변화에 따른 검토
- CDA 계정 관리를 위한 자동화된 기법 도입

○ 접근강제
- 할당된 인가에 대한 강제
- 사용자 권한 특권 할당
- CDA에 대한 보안정보 및 특권의 정의 및 문서화
- 보안정보 및 특권에 대한 접근 제한

○ 정보흐름강제
- 정보흐름 강제를 위한 문서화
- 불법 및 비인가 정보흐름의 발견, 저지 및 예방을 위한 실시간 기능 구현
- 하드웨어 형태의 단방향 정보흐름 구현
- 동적인 정보흐름 제어 방법 구현

○ 기능분리
- 업무분장 및 기능분리에 대한 문서화
- 할당된 접근허가를 통한 CDA 기능 분리
- 대체 통제 방법 구현
- 보안기능의 제한

○ 권한최소화
- 최대한 제한된 권한 및 특권의 할당
- 권한 및 특권의 최대한 제한을 위한 CDA 구성
- 대체 통제 방법 구현

○ 실패한 로그인시도
- 유효하지 않은 접근시도를 제한하기 위한 보안 통제 구현
- 접근 시도를 제한하는 정책 구현
- 대체 통제 수단 및 대책에 대한 문서화

○ 시스템 사용통지
- 제한된 시스템의 사용 및 감사 목적으로 시스템 사용을 감시, 기록하는 등의 시스템 사용 통지 메시지를 제공
- CDA 시스템은 사용전 승인 및 비밀, 보안을 제공하는 메시지 사용

○ 이전 로그인통지
- 성공적인 로그온 이전의 실패한 로그온 횟수 및 마지막 로그온 시간 및 날짜를 표시할 수 있도록 CDA 구성

○ 세션 잠금
- 30분 이내에 활동이 없을 경우 세션락을 개시
- 사용자가 직접 세션락을 개시할 수 있는 기능 제공
- 신분 확인 및 인증을 통해 접근을 재설정할 때까지 CDA 상에 세션락을 유지
- 대체 통제 수단 및 대책에 대한 문서화

○ 감시 및 검토
- 접근제어 통해 사용자 활동의 문서화, 감시 및 검토
- 사용자 활동 검토를 촉진하는, 지원할 수 있는 자동화된 기법을 CDA상에 적용

○ 확인 및 인증 없이 허용된 활동
- 정상 및 비정상 조건 시 확인 및 인증 없는 사용자의 특정 행동의 인식 및 문서화
- 확인 및 인증 없이, 주어진 임무 수행에 필요한 행동 허용

○ 자동 표시
- 민감한 정보 보호를 위한 표준화된 명명규칙 구현
- 소프트 및 하드 카피 출력물 표시를 위한 CDA 구성

○ 자동표지
- 소프트 및 하드카피 정보의 저장, 처리 및 전송을 위한 라벨링

○ 네트워크 접근제어
- CDA 보안을 위한 완화 기법의 문서화 및 적용

○ “공개/비 안전” 프로토콜 제한
- 보안 통제가 부족한 프로토콜 사용 시, 네트워크 및 버스통신을 보호할 목적으로 하는 추가적인 예방책 구현 및 문서화
- 동일 경계를 제외한 곳에서의 명령을 개시하는 프로토콜을 금지
- 안전에서 비안전한 상태로의 CDA 변화를 야기하는 명령어를 개시하는 프로토콜을 금지

○ 무선 접근제한
- 보안 제어기기를 통해서만 무선 접근을 허용
- 안전 및 안전에 중요한 기능을 수행하는 CDA에 대한 무선 기술은 허용하지 않음
- 사용하지 않을시 무선 기능을 비활성화
- 무선 기술의 이행지침 및 사용 제한을 수립
- 비인가 무선 접근 파악을 위한 스캔을 수행

○ 비 안전 및 불량 연결
- CDA에 적용된 변화 및 수정을 확인
- CDA가 벤더 연결 및 모뎀과 같은 불량 연결 및 비안전한 상황이 아님을 확인

○ 휴대용 및 이동기기를 위한 접근제어
- 휴대용 및 이동기기들의 통제를 위한 이행 지침, 사용 제한 설정 및 문서화
- CDA에 접근하는 기기의 인증, 감시 및 통제
- CDA 레벨에 맞게 이동기기의 보안 및 건전성이 유지되는지 강제 및 문서화
- 이동기기는 보안 레벨을 변경하지 않고 단지 하나의 보안 레벨에서 사용됨을 강제 및 문서화

○ 사유 프로토콜의 가시성
- 가시성이 결여된 사유의 프로토콜을 사용시, 대체 통제 수단 및 대책을 구현

○ 3자 제품 및 제어
- 3자 제품의 보안 기능의 부족으로 기인되는 취약점을 완화시키기 위한 대체 통제 수단 및 대책 구현

○ 외부시스템 사용
- 하이 레벨에서의 외부시스템 접근이 허용되지 않음을 보장
- 동등한 보안 척도가 보장되지 않는 한 외부시스템의 CDA 접근 불허 및 통제되는 정보의 처리, 저장 및 전송을 불허

○ 공개 접근 가능한 내용
- 공개적으로 접근 가능한 정보를 게시할 수 있는 인증된 사용자를 지정
- 정보를 게시할 수 있는 인증된 사용자의 훈련
- 게시된 정보가 시스템에 보안에 영향을 미치지 않고, 사이버 공격에 도움이 되지 않다는 것을 보장

Ⅴ. 요건분석 및 구현방안

5.1 접근제어 요건 분석

원전 규제지침 R.G. 5.71에서 정의한 접근제어 요건들은 모두 23개로서 다음과 같은 항목으로 분류할 수 있다.

1) 행정적인 정책 및 절차와 관련된 요건
2) 접근제어 모델 요건
3) 시스템 기능 분리를 요하는 요건
4) 문서화 및 검토와 관련된 요건
5) 이동기기 사용, 무선접근 및 외부연결 제한 요건

원전 계측제어계통은 에어 갭을 유지하는 독립된 네트워크 구조로 설계된 관계로 외부 연결 및 무선 접근을 엄격하게 제한하고 있다. 또한, 시스템의 기능 분리를 요하는 요건은 계통의 재설계를 요하는 부분으로 본 논문에 언급하기에는 적절하지 않은 항목으로 판단된다. 또한, 정책 수립 및 절차 작성, 각종 문서화 및 검토를 통한 접근제어 요건들도 원전 계측제어계통의 운영 현장에서 행하지는 항목으로 판단된다. 본 논문에서는 원전 규제지침 R.G. 5.71에서 정의한 접근제어 요건 중 원전 계측제어계통의 특성을 고려하여 적용 가능한 혼합형 접근제어 모델을 제안 한다.

5.2 접근제어 모델

허가되지 않은 자원의 사용과 허가도지 않은 방법을 통한 자원 사용을 제어하는 접근제어 모델은 다음과 같이 세 가지의 형태로 분류 된다[13].

1) 임의접근제어(DAC) : 접근을 요청하는 자의 신원, 어떤 사람이 접근 승인이 되는지(또는 승인이 안 되는지)를 말해주는 접근 규칙들(승인)에 기반 하는 접근제어를 지칭한다.

2) 강제접근제어(MAC) : 보안레이블(시스템 자원이 얼마나 민감하고 중요한지를 나타냄)과 보안허가증(어떤 시스템 개체가 특정 자원에 접근할 수 있는지를 나타냄)을 비교하는 것에 기반 하는 접근제어를 지칭한다.

3) 역할기반 접근제어(RBAC) : 시스템 내에서 사용자가 가지는 역할들, 그리고 그 역할을 맡은 사용자에게 어떤 접근이 허용되는지를 말해주는 규칙들에 기반 하는 접근제어를 지칭한다.

5.3 원전 계측제어계통 적용 방안

원전의 계측제어계통은 수행하는 기능의 중요도에 따라, 보호계통, 제어계통 및 감시 계통으로 구분 되어 있다. 본 논문에서는 보호계통중의 하나인 원자로보호계통의 운영 특성에 적합하며, 기존의 접근제어 모델들을 혼합한 형태의 접근제어 모델을 제안 한다. 원자로 보호계통은 발전소 운전 변수가 설정된 제한치를 초과할 경우에 원자로를 자동으로 정지시켜, 핵연료 피복재의 과열을 방지하고 원자로 냉각계통의 건전성을 유지시켜 준다. 원자로 보호계통은 4개의 독립된 채널로, 각 채널은 비교논리모듈, 동시논리모듈, 유지보수시험 모듈 및 운전원 모듈로 구성되어 있다[14]. 비교/동시 논리 모듈은 다수의 제어기를 사용한 자동화 시스템이고, 사용자 연계가 이루어지는 부분은 유지보수/운전원 모듈이다. 비교/논리 모듈의 기능은 사전에 정의된 입출력만을 처리하며 정해진 노드와의 통신만을 허용하는 시스템으로, 보안레이블과 보안허가증을 활용하는 강제접근제어(MAC) 모델의 적용이 타당한 것으로 판단된다. 또한, 사용자 연계가 필요한 유지보수/운전원 모듈은 유지보수자 및 운전원의 업무를 활당하고, 접근 여부를 허가하는 역할기반 접근제어(RBAC) 모델 적용이 타당한 것으로 판단된다.

VI. 결 론

본 논문에서는 원전 사이버 보안을 목적으로 사전에 정의된 규제지침의 접근제어 요건분석을 통하여 원전 계측제어계통에 적용 가능한 혼합형 접근제어 모델을 제시하였다. 특히, 역할기반 접근제어(RBAC) 모델 사용을 위해서는 전력시스템의 접근제어모델 표준인 IEC 62351-8[15] 적용이 필요할 것으로 판단된다. 본 연구에서 제안한 원전 계측제어계통에 대한 혼합형 접근제어 모델은 가동 중인 국내 원전 및 건설 중인 신규 원전에 적용하여, 원전의 안전성을 효율적으로 증대 시킬 수 있을 것으로 판단된다.

감사의 글

This paper was supported by Sunchon National University Research Fund in 2014.

This work was supported by the Nuclear Safety Research Program through the Korea Radiation Safety Foundation (KORSAFe), granted financial resource from the Nuclear Safety and Security Commission (NSSC), Republic of Korea (No.1403025)

References

[1] M. Chung, W. Ahn, B. Min, and J. Seo, "A Study on Method to Establish Cyber Security Technical System in NPP Digital I&C," *J. of the Korea Institute of Information Security & Cryptology*, vol. 24, no. 3, 2014, pp. 561-570.

[2] Y. Choi, Y. Choi, J. Lee, J. Cho, I. Koo, and S. Hong, "Study on the Construction of Cyber Security for the Nuclear Power Plants," *Fall Conf. from Korea Society of IT Services*, vol. 16, Seoul, Korea, Nov., 2009, pp. 537-538.

[3] Y. Cha, B. Cho, and J. Na, "Security Technology Trends and Prospective of Industrial Control System," *KEIT (Korea Evaluation Institute of Industrial Technology) PD Issue Report,* vol. 13, no. 6, Jun., 2013, pp. 79-100.

[4] D. Kim, "Security Criteria for Design and Evaluation of Secure Plant Data Network on Nuclear Power Plants," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 9, no. 2, 2013, pp. 267-271.

[5] D. Kim, "Vulnerability Analysis for Industrial Control System Cyber Security," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 9, no. 1, 2013, pp. 137-142.

[6] I. Koo, K. Kim, S. Hong, G. Park, and J. Park, "Digital Asset Analysis Methodology against Cyber Threat to I&C System in NPP,"

J. of the Korea Institute of Electronic Communication Sciences, vol. 6, no. 6, 2011, pp. 839-847.

[7] N. Falliere, L. O. Murchu, and E. Chien, *Win32.stuxnet Dossier.* Cupertino, CA, USA, Symantec Security Response, 2011.

[8] NRC Information Notice 2003-14, "Potential Vulnerability of Plant Computer Network to Worm Infection," *Nuclear Regulatory Commission,* Mar., 2003.

[9] NRC Information Notice 2007-15, "Effects of Ethernet based, no-safety related controls on the safe and continued operation of nuclear power stations," *Nuclear Regulatory Commission,* Sep., 2007.

[10] US NRC, "Cyber Security Programs for Nuclear Power Facilities," *NRC Regulatory Guide 5.71*, Jan., 2010.

[11] C. Park, "Current Status for Cyber Security of Nuclear Power Plants and Long-term R&D Strategy", *J. of Electrical World*, vol. 430, 2012, pp. 59-65.

[12] C. Lee, "Trend of Technology of instrumentation and control system in Nuclear Power Plants," *J. of The Korea Institute of Information Security & Cryptology*, vol. 22, no. 5, 2012, pp. 28-34.

[13] W. Stallings and L. Brown, *Computer Security - principles and practice, 2nd ed.* Essex: Pearson Education, 2012.

[14] D. Lee, C. Lee, I. Hwang, and I. Oh, "Development of the Digital Reactor Safety Systems," *Korea Atomic Energy Research Institute: Daejeon, Technical Report KAERI/RR-2914,* Apr, 2007.

[15] IEC Std. 62351-8, *Power System Management associated information exchange - Data and Communication Security - Part 8 : Role-based Access Control.* International Electronical Committee, Geneva, Switzerland, 2014.

저자 소개

김도연(Do-Yeon Kim)

1986년 충남대학교 계산통계학과 졸업(이학사)
2000년 충남대학교 대학원 정보통신공학과 졸업(공학석사)
2003년 충남대학교 대학원 컴퓨터공학과 졸업(공학박사)
1986년～1996 한국원자력연구원 선임연구원
1997년～2008 한국전력기술(주) 책임연구원
2008년～현재 순천대학교 컴퓨터공학과 교수
※ 관심분야 : 영상보안, 산업제어시스템보안, 패턴인식, 컴퓨터비전