Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.2, Apr. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.2.425

안전한 전력 제어시스템 설계를 위한 위험관리 프레임워크 제안*

박 준 용,[1†] 신 수 민,[1] 송 경 영[2‡]
[1]동국대학교, [2]울산과학대학교

A Proposal of Risk Management Framework for Design as a Secure Power Control System*

Jun Yong Park,[1†] Sumin Shin,[1] Kyoung-Young Song[2‡]
[1]Dongguk University, [2]Ulsan College

요 약

지능형 전력망에서 전력 서비스의 효율성 및 상호운용성 확보를 위한 지능형 전력망과 외부망 연계로 인해 전력 제어시스템을 대상으로 한 공격 위협이 증가하고 사이버테러의 주요 목표가 되고 있어 이에 따른 안전한 시스템 설계가 중요한 화두로 등장하고 있다. 일반적으로 SSDLC를 적용하여 설계 단계에서부터 위험에 대한 관리를 하고 있으나 전력 제어 시스템의 특성을 고려한 사항은 부족한 실정이다. 따라서, 전력 제어시스템의 진단 모형 및 평가 프로세스 설계가 가능하고 정보보안 방향성 및 관련 지표를 제공하기 위해, IEC 62351 TC 57에서 제시한 운영 보안통제 사항 및 표준 아키텍처에 전사적 위험관리 프레임워크를 응용한 전력 제어시스템 위험관리 프레임워크를 제안하고자 한다.

ABSTRACT

In smart grid, enhancement of efficiency and interoperability of electric power system is achieved through the connection with outer network, and this induces that power grid system is threatened increasingly, becomes the main target of cyber terrorism, and is sincerely required to design the secure power system. Although SSDLC(Secure System Development Life Cycle) is used for risk management from the design phase, traditional development life cycle is somewhat limited for satisfaction of information security indicator of power control system. Despite that power control system should reflect control entities of information security considering its own characteristics, validation elements are insufficient to apply into real tasks based on existing compliance. To make design of diagnostic model and assessment process for power control system possible and to give a direction for information security and present related indicator, we propose the new risk management framework of power control system which is applied operational security controls and standard architecture presented by IEC 62351 TC 57 with enterprise risk management framework.

Keywords: Risk Management, SCADA Network, Secure Power Control, Smart Grid

Received(04. 09. 2015), Modified(1st: 10. 06. 2015, 2nd: 01. 05. 2016), Accepted(01. 31. 2016)
* 본 연구는 2013년도 산업통상자원부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다.(No. 20131020400760)
† 주저자, park1jun@naver.com
‡ 교신저자, kysong@uc.ac.kr(Corresponding author)

I. 서 론

지능형 전력망에서 전력 제어시스템(PCS: Power Control System)은 국가 중요기반 핵심 시설로써 SCADA(Supervisory Control and Data Acquisition) 망을 통해 전기, 가스, 수도, 교통 등 연계된 전력 설비의 가동 상태를 감시하고 설비에 부착된 센서를 통해 실시간으로 데이터를 취득 및 중앙 제어할 수 있다. 최근 지능형 전력망의 효율성에 관련된 외부망과의 연계가 주요 이슈로 등장하여 전력 제어시스템에 대한 공격 위협성이 증가하고 있고 사이버테러로 인해 전력 제어시스템 장애가 발생 시 엄청난 사회적, 경제적 혼란을 야기할 수 있어 이에 따른 안전한(Secure) 시스템 설계가 중요한 화두로 부각되고 있다. 또한 익숙하지 않은 차세대 기술로 발생할 수 있는 보안 취약성에 대하여 기업의 리더들은 최신 정보기술 트랜드에 대해 완전히 이해할 필요성이 있으며, 비즈니스 성과를 창출하는 동시에 위험을 관리할 수 있는 효율적인 보안과 리스크 관리 프로그램을 만들어 유지할 필요가 있다[1-2].

일반적으로 네트워크에 관련된 시스템 및 소프트웨어 개발 보안 프로세스는 SSDLC(Secure System / Software Development Life Cycle)에 준하여 요구사항 및 타당성 분석 단계에서부터 위험관리 기반으로 설계되어 적용되고 있으나 현존 SSDLC와 지능형 전력망 정보보호 요구사항의 연계성 미흡으로 산업 제어시스템(Industrial Control System)의 기업 정보보호 지수(indicator)를 측정하기에는 다소 제한적이다. 또한 정보보호 지수를 측정하기 위해서는 적절한 관리가 되어야 하며 전력 제어시설 및 SCADA 시스템을 포함한 연계된 제어장치 등의 상호운용성(interoperability)을 보장할 수 있는 평가 단위도 메인인 기업의 문화 및 조직, 정보보호 정책, 정보자산 관리, 법과 규제, 업무 연속성 관리, 정보화 사업 관리, 인적보안, 시스템 테스트, 응용 및 운영보안 프로세스 구성 등이 현존 위험평가 프로세스 요소와 매핑이 되어야 함에도 불구하고 평가 프로세스의 각 항목 및 요소들의 R&R(Role & Responsibility) 연계성이 미흡한 실정이다.

따라서 본 논문에서는 현재 일반적으로 적용되고 있는 정보보안 프레임워크를 통해 전력 제어시스템에서 요구되는 보안 요구사항을 중심으로 다각적인 진단 스킴을 생성할 수 있는 모형과 평가 프로세스 설계가 가능한 위험관리 프레임워크를 제안하고자 한다. 본 논문은 다음과 같이 구성되어 있다. 2장에서는 IEC TC 57에서 정의하고 있는 전력 제어시스템 보안 표준과 IEC TR 62351의 전력 제어시스템 운영을 위한 보안 아키텍처 및 핵심 보안기술, 전력 제어시스템의 위협 및 취약점을 분석하고, 3장에서는 전력 제어시스템 설계 단계별 영역에 대한 법률 및 기준과 보안 통제 관점으로 구성된 위험관리 프레임워크를 정의한다. 4장에서는 정의된 위험관리 프레임워크의 구성 영역을 진단 모형과 평가 프로세스 설계가 가능하도록 영역별 상세설명과 요구사항을 분석한 후, 마지막 5장에서는 전력 제어시스템 설계의 비즈니스 관점에서 관리적, 기술적인 평가가 가능하도록 위험관리 프레임워크를 정형화하고 향후 전력 제어시스템 설계 시 고려해야 할 보안요소를 통해 결론 및 제언을 하고자 한다.

II. 선행 연구 (위험관리를 위한 요구사항)

2.1 전력 제어시스템의 보안 관련 표준

국가 중요기반 시설을 보호한다는 측면에서 전력 제어시스템 보안기술 개발의 필요성을 인식한 IEC, IEEE P2030, SGIP(Smart Grid Interoperability Panel) 등 국제 표준화기구는 보안 요구사항과 아키텍처를 정의하고 NIST 및 DHS는 전력 제어시스템 및 네트워크 간 상호운용성과 사이버 보안성 확보를 위해 표준 가이드 및 시험·인증 체계 개발을 지속적으로 진행하고 있다. 현재 IEC TC 57에서 정의하고 있는 전력 제어시스템을 위한 통신 프로토콜 표준은 IEC 60870-5 Series, IEC 60870-6 Series, IEC 61850 Series, IEC 61970 Series, IEC 61968 Series 등이 제정되어 있으며, 전력 제어시스템 및 네트워크 간 상호운용성과 사이버 보안성 확보를 위한 대표적인 표준 프레임워크인 NIST SP 1108 "NIST Framework and Roadmap for Smart Grid Interoperability Standard v3.0"이 적용되고 있다[3-5].

NIST는 지능형 전력망에서 IEDs(Intelligent Electronic Devices) 및 AMI(Advanced Metering Infrastructure)에 대한 암호·인증 및 키 관리 기술의 개발 필요성을 인식하고 스마트그리

드 보안 가이드라인 문서 "NIST IR 7628"을 통해 스마트그리드 환경에 적합한 암호·인증 및 키 관리 요구사항을 정의하였다. IEEE P1711에서는 지능형 전력망 환경에서 데이터 기밀성과 무결성을 함께 제공하는 블록 암호 모드인 PE(Position Embedding) 모드를 표준화하였다[6].

2.2 전력 제어시스템 보안 아키텍처

IEC TC 57에서 정의된 전력 제어시스템 보안 아키텍처는 기밀성, 무결성, 가용성, 책임 및 보증 등 시스템의 품질 특성을 유지하기 위한 목적으로 적절한 보안 컨트롤을 사용하여 시스템을 구축하고 운영할 수 있는 프레임워크와 지침을 제공하고 있다. 특히 적절한 보안 통제는 일반적으로 기술 및 비즈니스 관련 자산을 기준으로 대상 시스템의 위협 및 위험 분석에 의해 결정된다. 따라서 위협 및 위험 분석은 기밀성, 무결성 및 인증을 위해 자신의 보안 요구에 대하여 다른 네트워크 요소 사이의 통신을 목표로 하기 때문에 타겟 시스템에 연계해서 단일 애플리케이션 도메인별 상이한 보안 요구사항을 반영하여 다른 보안 도메인으로 분류될 수 있다.

2.3 전력 제어시스템 핵심 보안기술 및 특성

2.3.1 전력 제어시스템 운영을 위한 핵심 보안기술

안전한 지능형 전력망 구축 및 운영을 위하여 우선 개발되어야 하는 핵심 보안기술은 크게 보안 기반기술, 보안 관제기술, 기기 보안기술로 분류될 수 있다.

첫째, 보안 기반기술에서는 스마트그리드 보안체계 연구에서 시작되어 전력 제어시스템 보안모델 및 보안체계를 바탕으로 지능형 전력망 구축 및 운영의 보안 요구사항인 기밀성, 가용성, 무결성, 인증, 부인방지를 기반으로 기기·시스템·네트워크의 취약성 분석 기술, 접근제어 기술, 단말기 보안모델 등과 운영 환경에 적합한 암호·인증 기술 개발이 요구된다.

둘째, 보안 관제기술에서는 보안 기반기술과 보안 관제 체계를 바탕으로 전력 제어시스템의 사이버위협을 사전에 감지하고 이상 징후 탐지 및 이벤트를 분석하여 대응방안을 수립하여야 한다.

셋째, 기기 보안기술에서는 지능형 전력망의 보안 모델과 보안체계를 바탕으로 관련 시스템에 설치되는 스마트 미터, 송·배전 센서, IEDs 등을 외부의 악의적 해킹으로부터 보호하는 기술 개발이 필요하다.

현재 전력 제어시스템은 운용 관리의 효율화 또는 원격 관리 등의 목적으로 개방화(Open)됨에 따라 사이버 공격자가 인터넷에 접속 후 제어시스템 관련 정보를 공개·열람하여 불법 프로그램 감염이나 불법 액세스 될 수 있는 위험을 높이고 있다. 따라서 전력 제어시스템의 주요한 특성인 "지속적인 가용성", "장기적(10~20년) 운용", "실시간 데이터 송·수신" 등을 보장할 수 있는 적절한 해결책이 강구되어야 하며, Table 1.에 언급된 전력 제어시스템 특유의 보안 요건과 방향성을 만족할 수 있어야 한다.

2.3.2 전력 제어시스템의 특성

전력 제어시스템과 비즈니스 IT시스템 사이에는 관리적, 운영적 차이가 존재하기 때문에 기존 IT시스템과는 달리 보안 제어 방법이 특성화되어 적절한 변경 적용이 요구된다. Table 2는 비즈니스 IT와 전력 IT의 보안 특성을 비교 정리하였다[7].

2.4 전력 제어시스템의 보안 위협 및 취약점 분석

2.4.1 전력 제어시스템의 보안 위협

전력 제어시스템에 대한 보안 위협은 적국, 테러리스트, 산업스파이, 불만을 가진 직원, 악의적인 침입자 등에 의한 악의적인 위협과 시스템 복잡성, 사람에 의한 실수 및 사고, 장치 고장과 자연재해와 같은 자연적인 위협 등 다양한 위협 인자에 의해 발생할 수 있다. 악의적인 위협 및 자연적 위협으로부터 제어시스템을 보호하기 위해서는 심층 방어(DID:

Table 1. Security requirement for PCS

Security Requirement	Policy Direction
1.Update or repair work does not stop system. 2.To minimize the impact on system performance. 3.Not applicable in a closed environment and the environment on a regular basis to maintain the patch secure conditions.	1. specific maintenance of security standards for power control system 2.Special measures of system(Lock Down) for the purpose introduction 3.resources development for organization/human

Table 2. Comparison for specification between Biz IT and Power IT

Category	Biz IT	Power IT
Anti-virus/ Mobile Code	Using a wide range of conventional	Non-conventional & limited installation
Risk manage-ment	- Data confidentiality & integrity - Limiting allowable momentary pause operation - Risk impacts business operations delayed	- Process availability, - Risk impact facility,
key of Security	- IT Asset & Data protection - Central server protection	Protective for slave device
Life support techniques	Average 3~5y	Max. 10~20y
Outsource	Using general	Do not use various
Patch	Regular & plan eligibility	Unplanned & certain parts supply
Change Management	Regular & plan eligibility	Management & highly complex
Time	The delay of time approved	Secure core time is required
Availability	24 x 365	Usually
Confidentiality	High	Common
Integrity	Medium	High

defense-in-depth) 전략을 수립할 필요가 있다.

2.4.2 전력 제어시스템의 보안 취약성

전력 제어시스템이 가지는 취약성은 아래와 같이 세 가지 분류의 취약성으로 구분해 볼 수 있다[8].

- **정책 및 절차 취약성**: 제어시스템 보안에 관한 정책 및 구현 절차가 불완전하거나 없는 경우에서 오는 취약성. 보안 정책은 패스워드 정책 또는 제어시스템에 연결 모뎀 등에 대한 보안 요구사항을 권고함으로써 취약성을 완화시킬 수 있다.
- **플랫폼 취약성** : HW(hardware), OS (Operating System), 제어시스템 애플리케이션을 포함하는 플랫폼의 결함, 잘못된 구성 또는 부실한 유지보수에서 오는 취약성. 이러한 취약성은 OS 및 애플리케이션 패치, 물리적 접근통제와 보안 소프트웨어(예, 백신)와 같은 다양한 보안 통제를 통해 완화될 수 있다.
- **네트워크 취약성** : 결함, 잘못된 구성 또는 부실한 관리와 다른 네트워크와의 연결성으로 인하여 발생하는 취약성. 이러한 취약성은 심층 네트워크 설계, 통신 암호화, 네트워크 트래픽 제한, 네트워크 컴포넌트에 대한 물리적인 접근통제와 같은 보안 통제를 통해 제거 또는 완화될 수 있다.

III. 전력 제어시스템 위험관리 프레임워크

3.1 개 요

전력 제어시스템을 위한 위험관리 프레임워크 연구는 위험관리 요구사항을 정의하고 일반적인 비즈니스 IT 시스템과의 특성 및 차이로 인해 기존의 보안 솔루션이나 위험평가 프로세스가 특화되어야 한다는 관점에서 시작하게 되었다. 따라서, 제안하고자 하는 전력 제어시스템의 위험관리 프레임워크는 전력 제어시스템의 특성을 고려하여 단계별 검증 요소, 법률 및 기준 관점, 보안 통제 관점에서 Fig. 1과 같이 제안한다.

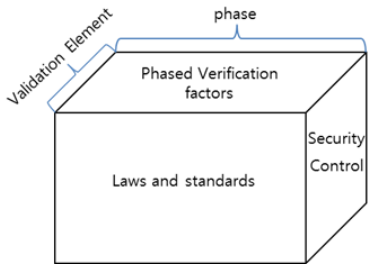

Fig. 1. Framework of risk management for PCS

3.2 단계별 검증 요소

단계별 검증 요소는 계획(plan), 설계(design), 구축(building), 운영(operate) 단계별 필수 검증 요소로 구분하였다. 단계에 적용한 구체적인 프로세스는 전력 제어시스템 정보보안 요구사항을 다루고 있는 IEC 62351 TC 57의 보안 평가를 위한 운영 프로세스를 기준으로 구성한다. Fig. 2는 단계별 설

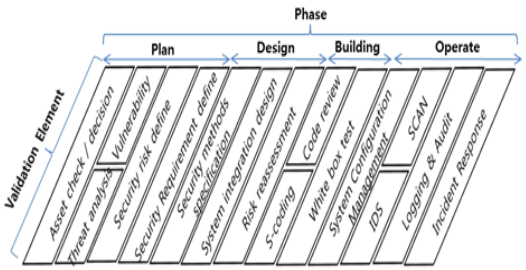

Fig. 2. Phase-wise verification elements

계 관점을 도시하였다.

- **계획** 단계 검증 요소 : 자산 확인 / 결정, 위협 분석, 취약점 분석, 보안 위험 정의, 보안 요구사항 정의
- **설계** 단계 검증 요소 : 보안 방법(수단) 명세, 시스템 통합 설계, 위험 재평가
- **구축** 단계 검증 요소 : 보안 코딩, 코드 리뷰, 화이트 박스 테스트
- **운영** 단계 검증 요소 : 시스템 형상관리, 침입탐지, 취약점 스캔, logging / audit, 사고 대응

3.3 법률 및 기준 관점

단계별 검증 요소와 보안 통제사항에 대한 근거는 글로벌 표준 IEC 62351 part10 운영 프로세스를 기반으로 지능형 전력망 운영 및 정보보호에 관련된 국내 법률과 표준을 고려하여 Fig. 3.과 같이 정의한다.

앞서 언급한 법률 및 기준 관점은 국내에서 적용되고 있는 항목을 언급하였으나, 실질적으로 제정된 법이나 기준은 국제 표준의 내용을 참고로 구성이 되어 있기 때문에 시스템 계획, 설계, 구축, 운영 관점 및 보안 통제 관점에서 기존의 법률 및 기준에 대한 준거성 항목을 적용하면 될 것으로 판단된다.

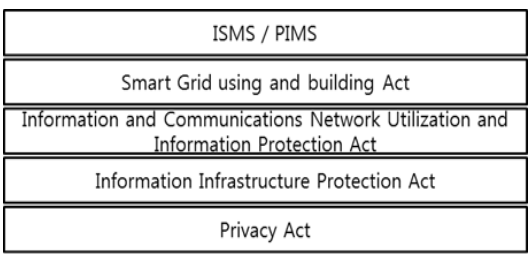

Fig. 3. Perspective for law and criteria

3.4 보안 통제 관점

보안 통제에 대한 관점은 정보자산 확인, 위협 분석 및 위험 정의, 영향도 분석 등 비즈니스 파급성에 직접 영향을 줄 수 있는 요소를 분석한다. 그 후에, 다양한 이해관계자의 기능들이 참여하여 위험을 감소시킬 수 있는 비용대비 효과적인 대책을 수립한다. 또한 전력 제어시스템의 모든 단계에서 적용되어야 하는 보안 통제요소를 정리하면 다음과 같다.

- 개인정보 보호
- 운영보안 관리
- 기밀성/무결성/가용성
- 인증/접근통제

3.5 전력 제어시스템 위험관리 프레임워크

전력 제어시스템의 위험관리 프레임워크는 제어시스템의 특성을 반영하여 단계별 검증 요소, 법률 및 기준, 보안 통제의 3가지 측면을 고려한 모형으로 구상하였으며, Fig. 4.와 같다.

전력 제어시스템(망)에는 다양한 소유권과 관리·운용 영역을 가지는 많은 전력 제어시스템들이 이해관계자들 간 및 현장 운영장치(IEDs, PLCs, RTUs)들 간의 서비스를 제공할 수 있도록 상호 연결되어 있으며, 전력 공급을 경제적으로 안전하고 신뢰성 있게 제공하기 위하여 가장 효율적인 통신 인프라에 대한 공격 가능 목표와 위협 모델링 문서에 위험 프로파일이 정의되어야 한다.

제어시스템의 보안을 위한 설계 스펙의 관점에서 위협은 가장 최우선으로 조사되어 시스템의 설계나 이행에 의해서 적절한 대응이 이뤄져야 한다[9].

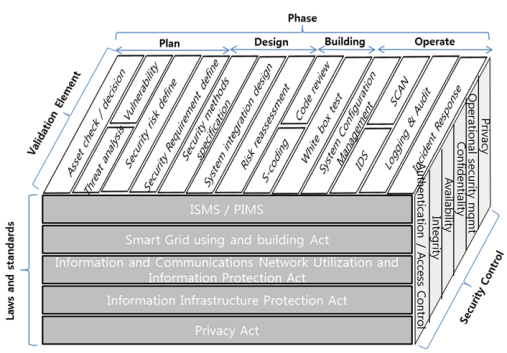

Fig. 4. Detailed framework of risk management for PCS

따라서, IT 기반 전력 제어시스템(망)의 위험관리 체계를 구축하기 위해 우선 추진되어야 할 사항은 위험평가 표준화 규격 및 구조를 정립하는 것이다. 이를 위해 첫째, 전력 제어시스템(망)에 적용해야 할 정책과 표준을 정의하고 둘째, 식별된 정보자산의 적합성과 비즈니스 적용을 위한 시험 및 평가 단계가 필요하며 셋째, 전력 제어시스템 정보자산별 보안 위협에 대한 대응방안을 결정해야 한다. 넷째, 정책 및 표준과 대응방안을 바탕으로 지능형 전력망 내 전력 제어시스템을 위한 위험평가 기반 구조가 정립되어야 한다. 전력 제어시스템 위험평가를 위한 비즈니스 프로세스는 계획, 평가, 보고, 취약점 개선, 검증 테스트 순으로 진행된다.

IV. 전력 제어시스템 위험관리 세부 구성 내용

4.1 단계별 검증 요소 - 계획 부문

4.1.1 자산 확인/결정

정보자산은 보안 위험과 관련이 있으며, 전력 송·배전 서비스 또한 정보자산과 프로세스의 결합된 결과이다. 따라서 서비스의 주체에 해당되는 정보자산을 식별하고 그 중요도를 산정하는 것이 필요하다. 정보자산의 중요도는 해당 정보자산이 주로 어떤 서비스를 제공하느냐에 따라 달라진다고 할 수 있다. 즉, 특정 정보자산이 중요한 서비스를 제공한다면 그 정보자산은 위험으로부터 보다 철저하게 보호 및 관리되어야 한다.

4.1.2 위협 및 취약점 분석

위협 및 취약점은 알려진 정보자산에서 출발하는데 여기서 반드시 위협과 취약점은 구분되어야 한다. 정보자산의 리스트를 중심으로 각 자산에 대한 공격 목표의 리스트를 검토하고 공격자가 정보자산을 어떻게 조작하는지 면밀히 분석할 필요성이 있다.

4.1.3 보안 위험 정의

위험의 기본적인 요소에는 유·무형 자산, 자산 가치, 위협 및 취약성, 보호 대책, 위협 요인의 결과와 발생 요인 등이 포함된다. 위험을 식별하고 정의하기 위한 프로세스는 정성적 또는 정량적인 위험 등급이 결정되어야 하며, 보안 관리자들의 브레인스토밍, 경영진의 위험관리 전략, 과거의 감사 결과, 기타 평가 등으로부터 위험을 정의할 수 있도록 해야 한다.

4.1.4 보안 요구사항 정의

- 위험 평가 정보를 보안 요구사항으로 변경
- 보안 요구사항을 실행
- 보안 요구사항이 시스템의 형상 변경 사항을 반영할 수 있도록 갱신
- 변경 요청이 위험관리 계획에 미치는 영향을 평가
- 보안 요구사항 실행을 모니터링
- 보안 요구사항을 위험관리 정책 및 절차와 연계

4.2 단계별 검증 요소 - 설계 부문

4.2.1 보안 방법(수단) 명세

비즈니스를 위해 합당하고 적절하면서 균형을 가질 수 있는 통제 및 보호시스템의 구축을 목표로 하는 동시에 보안 투자 수익률(ROSI)이 가장 높고 신속하게 효과를 볼 수 있는 방법(수단)에 우선순위를 부여해야 한다. 또한 위험을 적절히 완화시킬 수 있는 예방, 적발, 수정 및 복구 조치를 위해 위험관리의 목적을 전파하고 상응하는 조치들을 관리하여 적절하게 대응하는지 지속적인 모니터링을 해야 한다.

4.2.2 시스템 통합 설계

보안에 대한 인식도를 제고하고 명확한 위험관리 정책과 표준을 반영하여 비용 효과적이고 지속적으로 보안 이슈를 정의하여야 한다. 또한 전력 제어시스템에서 요구되는 상호운용성, 프로토콜 및 서비스 가용성, 신뢰성, 보안성을 고려하여 설계될 수 있도록 하고 중앙 집중화된 위험관리가 될 수 있도록 한다[10].

4.2.3 위험 재평가

식별된 정보자산에 대해 위협의 발생가능성 및 영향, 잠재된 위협이 취약점으로 전이될 개연성을 재확인하는 과정이다. 즉 관리하고도 남아있는 위험을 평

가하며 적절한 대응조치로 사라진 위험과 새로 등장한 위험에 대해 보완통제를 구현하는 것이라고 볼 수 있다.

4.3 단계별 검증 요소 - 구축 부문

4.3.1 보안 코딩

보안 코딩은 보안 정책과 SW 개발 단계에서부터 보안 약점을 제거할 수 있도록 하는 구현 메커니즘이라고 볼 수 있다. 일부 제어시스템을 확장하거나 새로운 임시적 방법을 사용할 때 추가적인 애플리케이션 보안이 필요하며, 악성코드가 사용자의 중요정보를 얻거나 바람직하지 못한 동작을 수행하지 못하도록 하는 방지책이라고도 볼 수 있다.

4.3.2 코드 리뷰

코드가 다른 코드에 의해 호출되지 않는 응용 프로그램에 포함되어 있으면 특별한 코딩 없이 간단하게 보안을 구현할 수도 있으나 악성코드가 사용자의 코드를 호출할 수 있다. 따라서 악성코드는 중요한 정보를 포함하는 필드나 속성 값을 읽을 수 있기 때문에 코드 리뷰를 통해 악성코드가 리소스에 액세스하는 것을 막을 수 있도록 해야 한다[11].

4.3.3 화이트박스 테스트

화이트박스 테스트를 통해 내부 소스코드의 동작을 개발자가 추적할 수 있기 때문에, 동작의 유효성 뿐만 아니라 실행되는 과정을 분석하여 코드가 어떤 경로로 실행되며, 불필요한 코드 혹은 테스트 되지 못한 부분을 확인할 수 있다[12].

4.4 단계별 검증 요소 - 운영 부문

4.4.1 시스템 형상관리

시스템 형상 요소의 기능적 특성이나 물리적 특성을 문서화하고 그들 특성의 변경을 관리하며, 변경의 과정이나 실현 상황을 기록·보고하여 지정된 요건이 충족되었다는 사실을 검증하는 것을 정의할 수 있다.

4.4.2 침입 탐지

침입 탐지는 취약한 서비스에 대한 네트워크 공격과 애플리케이션에서의 데이터 처리 공격, 권한 상승 및 침입자 로그인 / 침입자에 의한 주요 파일 접근 / 악성 소프트웨어와 같은 호스트 기반 공격을 포함한다.

4.4.3 취약점 스캔

본질적으로 전력 제어시스템의 운영 보안을 평가하는 중요한 절차는 시스템에 대한 취약점 스캔을 수행하는 것이다. 취약점 스캔은 시스템침입에 사용될 수 있는 취약한 부분을 찾는 것이다.

4.4.4 Logging / Audit

전력 제어시스템 운영 간 발생하는 로그의 보존 여부와 이를 통해 감사의 목적(도출된 위반사항에 대한 개선 조치 등)을 달성하기 위해 적절한 모니터링이 필요하며, 사고 예방을 위한 모니터링 및 추적을 위해 중요 시스템의 접속로그를 남겨야 한다.

4.4.5 사고 대응

사고 대응은 운영 보안에 대한 초동조치와 대응 프로세스, 보안사고 위험에 관련된 대응을 적절히 할 수 있도록 교육, 훈련 체계가 수립되어 있는지 반드시 고려해야 된다[13].

4.5 보안 통제 관점

4.5.1 인증 / 접근통제

식별된 사용자, 접근 통제규칙에 연관된 자원 등을 적절하게 인증할 수 있는 메커니즘을 구축하여 전력 제어시스템 등 정보자산에 대한 논리적 접근과 무분별한 사용자 권한부여 등을 제한하여야 한다.

4.5.2 가용성 / 무결성 / 기밀성

전력 제어시스템의 가용성을 보장하기 위해 악의적인 공격 등을 통하여 안정성 및 신뢰성이 무너지지 않

도록 인증, 인가, 책임추적성 체계가 먼저 이루어져야 한다. 무결성 측면에서 전력 제어시스템의 제어코드가 해커로부터 변조되어 전송되거나 잘못된 과금이 발생하도록 프로그램의 변조 공격이 이루어질 경우 전력망 운영에 지대한 영향을 미칠 수 있다. 기밀성을 위해 지능형 전력망의 전력 제어명령이나 AMI의 개인정보 등이 비인가자에게 노출이 되지 않도록 암호화, 접근통제 등을 강화할 필요성이 있다.

4.5.3 운영보안 관리

전력 제어시스템 운영에서 보안이란 정보자산에 대한 비인가 접근, 불법 노출 및 수정, 참조를 방지하는 정책과 기법을 모두 말하며, 중요 제어시스템을 외부의 침입으로부터 보호하는 것을 말한다. 운영보안이 제공하는 주요 기능은 시스템 메모리 보호, 접근통제, 식별 및 인증 등이 포함되는데 이는 제어시스템에 설치되어 있는 운영체제에 보안 커널을 추가함으로써 완화시킬 수 있다.

4.5.4 개인정보보호

전력 제어시스템(망) 내 개인정보를 활용하여 전자상거래, 고객관리 등 사회의 구성, 유지, 발전을 위한 필수적인 요소로서 기업의 입장에서 개인정보보호 정책을 비롯한 인증제도, 기술적 대책 등을 활용하여 지속가능경영을 위한 적절한 조치를 통해 개인정보 유출을 반드시 통제해야할 필요성이 있다.

V. 결 론

전력 제어시스템에 대한 위험관리는 전력 서비스의 목적을 달성하는데 위협과 장애가 되는 요소를 적절히 관리하는 것이다. 또한 일반적인 IT서비스에서 요구되는 품질과 안정성이 높은 서비스 제공이 되어야 한다. 따라서 전력 서비스의 품질과 안정성에 부정적 영향을 미치는 모든 중요한 요소를 포함해서 관리되어야 하며, 위험관리의 영역은 지능형 전력망에서 발생할 수 있는 보안 이슈뿐만 아니라 성능 및 용량관리, 형상관리, 장애관리 등의 이슈도 포함해야 한다.

물론 본 논문에서 제안한 위험관리 프레임워크를 전력 제어시스템 구성에 일괄적으로 적용하는 것은 일부 제한이 있어 보이지만 관련된 이해관계자 및 실무자들이 전력 제어시스템 설계 시 위험관리 관점에서 실효성 있는 구성에 대한 검증기준 및 근거가 되길 바라며, 향후 전문가들의 폭 넓은 지식을 적용하여 조직 내 위험진단 모형과 위험평가 프로세스를 구축하는데 많은 참고가 되었으면 한다.

References

[1] NIST, “NIST framework and Roadmap for smart grid interoperability standards, Release 3.0,“ pp.29, May. 2014.

[2] Gartner, “Gartner identifies the top 10 technologies for information security,” http://www.gartner.com/us/ symposium, pp. 1-2, Oct. 2014.

[3] NIST, “NIST framework and roadmap for smart grid interoperability standards, Release 1.0,” Jan. 2010.

[4] NIST, “NIST framework and roadmap for smart grid interoperability standards, Release 2.0,” Feb. 2012.

[5] NIST, ″NIST framework and roadmap for smart grid interoperability standards, Release 3.0,“ May 2014.

[6] BIR, “The five leading industrial in the future - technology development and status of participating companies ,” pp.311-313, Nov. 2011. from http://www.birbook.com

[7] IEC TR 62351-10, ″Power systems management and associated information exchange - data and communications security - Part 10 : security architecture guidelines,″ Oct. 2012.

[8] NIST, “Special publication 800-82, Revision 1 : Guide to industrial control systems (ICS) security,” pp.5, May. 2013.

[9] Microsoft, M. Curphey, J. Scambray, and E. Olson, Improving web application security threat and countermeasures, pp.45-48, Jun. 2003.

[10] W.V. Grembergen, Strategies for Information Technolies Governance, 1st

Ed., Idea Group Publishing, Jul. 2003.
〔11〕 Microsoft MSDN, "Developer network," from http://social.msdn.microsoft.com
〔12〕 Homeland Security, "Cyber security assessments of industrial control systems," Nov. 2010.
〔13〕 Young-dai Ko, Sang-jin Lee, "A proposal of personal information DB encryption assurance framework," pp.406-407, Korea Institute of Information Security & Cryptology(KIISC), 24(2), pp. 397-409, Apr. 2014.

〈저자소개〉

박 준 용 (Jun Yong Park) 학생회원
2000년 2월: 동국대학교 반도체과학과 졸업
2006년 2월: 영남대학교 컴퓨터정보통신공학과 석사
2012년 2월: 동국대학교 정보보호학과 석사
2014년 3월~2015년 6월 : 동국대학교 엔터테인먼트 컴퓨팅 연구센터 책임연구원
2014년 3월~현재: 동국대학교 정보통신공학과 박사과정
〈관심분야〉 정보보호, 위험관리, ISMS, PIMS, 전력망 보안

신 수 민 (Sumin Shin) 학생회원
2007년 2월 : 순천대학교 컴퓨터교육과 학사
2016년 2월 : 동국대학교 정보보호학과 석사
2016년 3월 ~현재: (주)씨에이에스 보안사업부 전략보안팀
〈관심분야〉 침투테스트, ISMS, 개인정보보호, 위험관리

송 경 영 (Kyoung-Young Song) 정회원
2004년 2월: 고려대학교 전기전자전파공학부 졸업
2010년 8월: 서울대학교 전기컴퓨터공학부 박사
2010년 8월~2012년 2월: LG전자 차세대통신연구소 선임연구원
2012년 3월~현재: 울산과학대학교 전기전자공학부 부교수
〈관심분야〉 스마트그리드 보안, 생체신호처리, 기계학습, 무선통신공학