ISSN 1975-8359(Print) / ISSN 2287-4364(Online)
The Transactions of the Korean Institute of Electrical Engineers Vol. 67, No. 12, pp. 1577~1586, 2018
http://doi.org/10.5370/KIEE.2018.67.12.1577

전력계통 제어시스템 구조에 따른 사이버 보안대책 수립

Establishment of Cyber Security Countermeasures amenable to the Structure of Power Monitoring & Control Systems

우 필 성* · 김 발 호†
(Pil Sung Woo · Balho H. Kim)

Abstract - The emergence of the Smart Grid is an integrated solution for the next generation power system that combines IT technology in the power system to create optimal energy utilization and various services. However, these convergence technologies (power systems and information communications) are not only improving the related technologies but also producing various problems especially exposure to cyber risk. In particular, the intelligent power grid has security vulnerabilities through real-time information sharing among various organically linked systems, and it is more complicated than the cyber risk problem in the existing IT field and is directly connected to national disaster accidents. Therefore, in order to construct and operate a more stable smart grid, this paper analyzes the system of power system control system in Korea, and proposes a cyber security element definition and a countermeasure establishment method of power monitoring & control systems based on security standards of smart grid (No. SPS-SGSF-121-1-1).

Key Words : Smart grid, Power control system, EMS, SCADA, DAS, Cyber security, security standards

1. 서 론

현 전력산업은 대내외적으로 다양한 환경적 변화에 직면하고 있다. 특히 지능형전력망 구축과 신재생에너지 활성화 정책 등으로 전력산업의 인프라 변화는 필연적이며, 관련 기술 고도화를 견인하여 단순 전력공급의 역할을 넘어 새로운 가치를 창출하는 플랫폼으로 변모 중이다[1],[2],[3]. 즉, 지능형전력망 구축은 기존의 전력계통에 정보통신기술이 융합되어 공급자와 소비자간 실시간 정보 교류로 최적 에너지 제어가 가능하며 다양한 서비스를 창출할 것이지만 사이버 위협에의 노출 등 많은 난제 또한 양산하였다.

현 전력계통 제어시스템은 폐쇄적인 구조로 운영되고 있기에 통신 프로토콜의 보안성을 기본적으로 보장되었으나, 지능형전력망의 순기능인 실시간 정보 활성화, 마이크로그리드 및 수요반응(DR; Demand Response) 시장 등의 등장은 다수의 통신접속점을 생성하고, 이는 보안 취약성으로 직결되어 블랙해커의 침투경로로 악용될 것이다.

이와 함께 전력계통의 물리적 특성은 고수준의 가용성을 요하므로, 전력계통에서의 사이버 위협 문제는 기존의 IT분야에 비해 보다 복잡하고 방대한 피해를 초래할 수 있다.

† Corresponding Author : Dept. of Electronic and Electrical Engineering, Hongik University, Seoul, Korea.
E-mail : bhkim@hongik.ac.kr
* Electrical Safety Research Institute, Korea Electric Safety CO., Korea.(wps@kesco.or.kr)
Received : October 24, 2018; Accepted : November 28, 2018

우리나라의 경우, 악성코드를 이용한 사이버 공격으로 원전 도면 등 한국수력원자력의 내부 정보 유출사례가 있었으며[4], 같은 해 글로벌 최대 해킹 행사(DEFCON)에서는 지능형전력량계에 대한 다양한 해킹 방법을 발표하여 관련 시스템의 보안 취약성을 지적한 바 있다. 또한 우크라이나에서는 사이버 공격으로 발전소 내부 네트워크에 악성코드가 유포되어 8만여 가구에 전력공급이 중단되는 사례가 있었다[5].

본 논문에서는 우리나라 전력계통 제어시스템 체계를 분석하고 스마트그리드 보안 표준서(표준번호 : SPS-SGSF-121-1-1)를 기반으로 관련 제어시스템별 보안대책을 제시한다.

2. 우리나라 전력계통 제어시스템 체계

우리나라 전력계통은 〈그림 1〉과 같이 EMS(Energy Management System)를 중심으로 발전·송전·배전계통 별 제어시스템과 연계되어 운영되고 있다[6]. 현재 중앙 EMS, 후비제어센터(천안 EMS)와 제주 EMS가 운영 중이며, 송변전계통의 경우 기본적으로 원방감시제어시스템(SCADA; Supervisory Control and Data Acquisition System)에 의해 송배전 관련 전력설비를 제어하고 자료를 취득한다.

데이터의 전달 체계의 경우, EMS를 기준으로 345kV 이상의 변전소와 발전소는 전용 원격단말장치(RTU; Remote Terminal Unit)를 통해 EMS와 직접 데이터를 송수신하고, 154kV 이하 변전소는 지역급전소(RCC; Regional Control Center)를 통해 EMS와 통신한다.

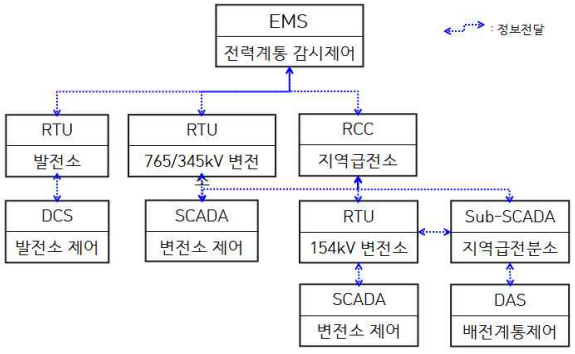

그림 1 전력계통 제어시스템 체계
Fig. 1 Frame of Power Control System

본 장에서는 기 기술된 전력계통 제어시스템 체계에 대해 세부적으로 각 분야별 제어시스템 구조 및 기능 등을 분석한다.

2.1 전력계통 제어시스템(EMS)

EMS는 전력계통을 상시 모니터링하고 제어하는 관리시스템으로서 계통 운영 관련 최적화 프로그램으로 구성되고, 다양한 시스템과 유기적으로 연계되어 최적계통운영을 담당한다.

EMS는 기본적으로 발전기에 대한 급전지시 및 154kV 이상 주요 송·변전 설비에 대해 감시 및 제어한다. EMS의 역할은 크게 3가지로 발전계획, 계통해석, 하위시스템 감시제어로 분류할 수 있으며 기 분류에 따른 주요 기능은 〈표 1〉와 같고[7], 해당 기능을 수행하기 위한 각 계통의 제어시스템 별 취득 정보는 〈표 2〉과 같다[6].

표 1 EMS의 주요 기능
Table 1 Key function of EMS

	주요 기능
발전계획	경제급전(ED; Economic Dispatch), 급전지시, 자동발전제어(AGC; Automatic Generation Control), 예비력관리(Reserve Management) 등
계통해석	상태추정, 최적조류계산(OPF; Optimal Power Flow), 안전도제약 OPF(SCOPF; Security-Constrained Opimal Power Flow), 상정사고 분석 등
하위시스템 감시·제어	발전소 전용 RTU, 765/345kV 변전소 전용 RTU, RCC(154kV 변전소)

표 2 EMS의 취득 정보
Table 2 Acquisition information of EMS

계통	상태정보		아날로그정보	
발전계통 (수력, 화력, 원자력, IPP발전)	MCD	· 154kV 이상 재폐로 CB	MW	· 발전단 MW · 송전단 MW(step-up TR 2차) · Target MW(Set Point)
			Hz	· 상용 주파수
			MW	· 154kV 이상 T/L, M.Tr · Start-UP Tr(Gen 접속 제외) · Local Load · Aux. TR
	Status	· Gen. CB, DS · 154KV 이상 CB, DS · Gen AGC Control · 고장파급방지장치 Ry 상태 · UFR Ry 상태 · 운전 Mode(S/T, S/T+G/T) · G/F On/Off	MVAr	· 송전단 MVAr (step-up TR 2차) · 154kV 이상 T/L, M.Tr
			kV	· Gen. · 154kV 이상 BUS별
			Gen. MW Limit	· High/Low (원전제외)
			Gen. MW 증감발률	· MW/Min.
			수위	· 저수위, 방수위
			MWh	· Gen.
송변전 계통 (765kV, 345kV, HVDC, SVC)	· 765kV 이상 CB 각상별(HSGS포함) · 154kV 이상 CB, DS · M.Tr 3차 CB · SVC CB/DS · SC/ShR CB · ULTC Remote/Local		MW/MVAr	· 154kV 이상 T/L, MTr · SVC(MVAr) · HVDC Line(MW, AMPS) · HVDC C.Tr
			kV	· 154kV 이상 BUS 별 · HVDC Pole
			Tap Position	· 345kV이상 MTr · HVDC C.Tr
			Hz	· 모선주파수
송변전 계통 (154kV)	· 154kV CB, 모선연결 DS · SC/Sh.R 1차측 CB(23kV) · UFR Ry 동작 상태		MW/MVAr	· 154kV T/L, MTr
			kV	· 154kV BUS별

2.2 발전/송·변전/배전계통 별 제어시스템

먼저 발전기는 1차 에너지원(발전원)의 종류에 따라 제어방식이 상이하지만, 국내 대부분 중앙급전발전기는 분산제어시스템(DCS; Distributed Control System)에 의해 제어되며 발전기 내부 설비에 대한 전체 데이터(연료소비량, 터빈온도, 보일러 상태정보, 소내소비전력량 등)를 일정한 시간주기마다 온라인으로 취득한다[8]. 취득된 발전기 데이터는 EMS 전용 RTU를 통해 직접 송수신하여 전력계통의 실시간 수급균형을 유지한다.

다음으로 송·배전계통은 한국전력공사의 송전계통운영센터 및 송변전사업소 단위의 지역급전소(RCC)와 배전운영센터로 계층화되어 운영 중이며, 관련 시스템 간 유기적인 관계는 〈그림 2〉와 같다[9]. 송·변전 설비에 대한 각종 정보를 모니터링 및 제어하기 위해 일반적으로 SCADA 시스템을 구축한다. 즉, SCADA 시스템은 변전소에 있는 각종 전력설비에 대한 정보를 감시·계측하여 광역지역단위의 RCC에 해당 정보를 제공하며, 운전원의 조작에 의하여 설비를 제어하는 송·변전계통에 대한 자동제어시스템이다.

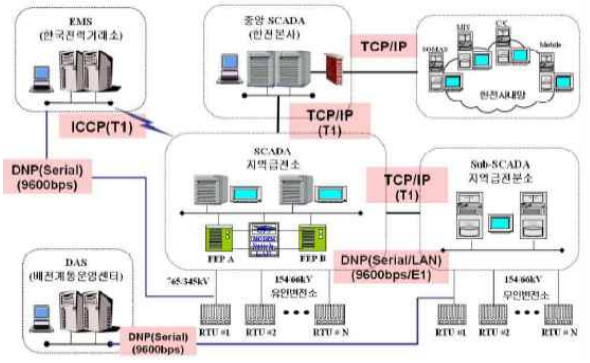

그림 2 송배전계통 자동화 시스템
Fig. 2 Automation system of transmission and distribution

배전계통의 경우 배전자동화시스템(DAS; Distribution Automation System)에 의해 제어된다[10]. DAS는 배전설비에 대한 현장정보(상태정보, 전류/전압, 고장유무 등)를 상시 모니터링하고 고장 발생시 고장구간의 자동화개폐기를 제어하여 정전구간 축소 및 정전시간을 단축시키는 시스템이다. 최근 마이크로그리드 등장과 지능형 전력계량 인프라(AMI; Advanced Mertering Infrastructure) 구축 프로젝트로 인하여 DAS의 기능이 고도화되고 역할 또한 확대 될 것으로 예상된다.

3. 전력계통 제어시스템의 사이버 보안 확보 방안

본 논문에서는 전력계통 제어시스템의 사이버 보안 확보 방안으로 우리나라에서 제정된 스마트그리드 보안 관련 표준서(표준번호 : SPS-SGSF-121-1-1)를 적용한다[11]. 본 표준서의 사이버 보안 확보 절차는 크게 4단계로 〈그림 3〉과 같다. 첫 번째 단계에서는 보안성 검토 대상의 존재 유무를 파악을 위해 보안성 확보 대상 식별하고, 두 번째 단계에서는 식별된 대상에 대해 예상되는 보안위협을 파악한다. 세 번째 단계에서는 잠재적인 보안위협에 대해 보안 요구사항을 도출하고, 마지막 단계에서 요구사항을 기반으로 보안대책을 제시한다.

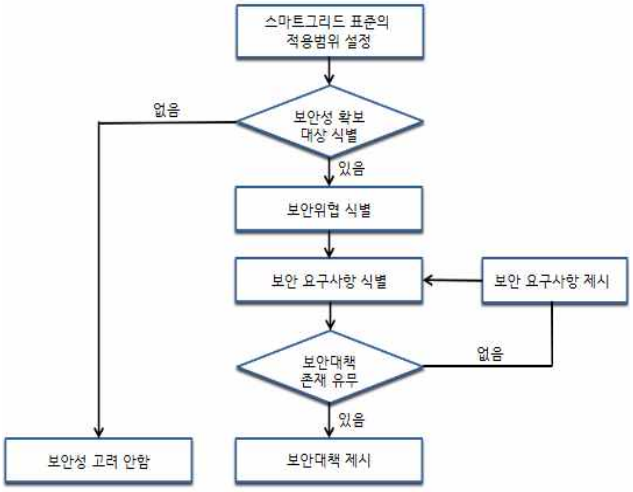

그림 3 사이버 보안 확보 절차
Fig. 3 Procedures for Securing Cyber Security

3.1 1단계-보안성 확보 대상 식별 기준

보안성 확보가 필요한 대상 식별을 위해 본 보안 표준서는 3가지의 대상 식별 방안을 제시한다.

먼저, 표준화 대상의 유형에 따른 보안성 확보 대상 식별 방안으로 개발하고자 하는 대상이 본 표준서에서 정의된 보안 표준화 대상별 유형에 해당되는지 여부를 판단하는 것이다. 두 번째 방안으로는 통신 및 데이터 등의 특성에 따른 보안성 확보 대상 식별이다. 기 방안은 표준서에서 정의된 통신, 네트워크, 데이터 특성을 목록화한 체크리스트를 활용하여 판단하는 방법이다.

마지막 세 번째 방안으로 위험도 판단 기준에 따른 보안성 확보 대상 식별방안이다. 본 방안은 정보보안의 3대 요소인 기밀성(개인적 및 재산적 정보를 보호하기 위한 수단을 담고 있는 정보에 대한 접근과 노출에 대해 승인된 제한 유지), 무결성(정보에 대한 부인방지와 인증성 보증을 포함하여 부적절한 정보의 수정이나 파괴 방지), 가용성(정보에 대한 적시적 및 신뢰성 있는 접근과 사용을 보장)에 대한 잠재적인 영향력(위험도)을 파악하는 것으로 잠재적인 영향력에 대한 정의는 〈표 3〉과 같다.

상기 3가지 식별 기준 중 하나라도 해당되면 보안성을 확보할 것을 권고하여, 본 논문에서는 세 번째 방안인 위험도 판단 기준에 따른 보안성 확보 대상 식별방안을 적용한다.

3.2 2단계-보안위협(Treat) 정의 및 식별

본 단계에서는 다양한 스마트그리드 기술을 대상으로 발생 가

능한 위협을 정의하고, 1단계의 보안성 확보 대상에 대한 특정 보안위협을 식별할 수 있도록 세분화하였다. 보안위협은 〈표 4〉와 같이, 11가지의 대분류에 24가지의 소분류로 정의하였다.

3.3 3단계-보안 요구사항(Security Requirements; SR)도출

보안 요구사항 도출 단계에서는 2단계에서 도출한 보안 확보 대상별, 보안위협에 대응하기 위한 보안 요구사항을 도출하는 단계로서, 총 16가지의 요구사항으로 〈표 5〉와 같다.

3.4 4단계-보안대책(Security Countermeasure; SC) 수립

보안대책 제시 단계는 앞서 도출한 보안 요구사항들을 충족시킬 수 있는 보안대책들을 제시하는 단계로써, 정보보안의 3대 요소를 기반으로 단계별 위치매핑을 통해 보안대책을 수립한다. 이를 도식화 하면 〈그림 4〉와 같다. 보안대책을 수립시 관련 개발자의 스킬, 보안설비에 대한 투자규모 등으로 인하여 다양한 방법이 존재하므로 본 논문에서는 3단계에서 도출된 보안 요구사항에 대한 기본적인 대책을 제시한다.

표 3 위험도 판단 기준에 따른 표준화 대상 식별
Table 3 Identification of standardization target according to risk criteria

보안 목표	잠재적 영향		
	낮음	중간	높음
기밀성	정보가 허가되지 않은 유출은 조직의 운영과 자산 또는 개인에게 한정된 부정적 영향을 예상	정보가 허가되지 않은 유출은 조직의 운영과 자산 또는 개인에게 심각한 부정적 영향을 예상	정보가 허가되지 않은 유출은 조직의 운영과 자산 또는 개인에게 극심한 또는 재앙적인 부정적 영향을 예상
무결성	정보의 허가되지 않은 수정 또는 파괴는 조직의 운영과 자산 또는 개인에게 한정된 부정적 영향을 예상	정보의 허가되지 않은 수정 또는 파괴는 조직의 운영과 자산 또는 개인에게 심각한 부정적 영향을 예상	정보의 허가되지 않은 수정 또는 파괴는 조직의 운영과 자산 또는 개인에게 극심한 또는 재앙적인 영향을 예상
가용성	정보 시스템에 대한 접근 및 사용 중단은 조직의 운영과 자산 또는 개인에게 한정된 부정적 영향을 미칠 것으로 예상	정보 시스템에 대한 접근 및 사용 중단은 조직의 운영과 자산 또는 개인에게 심각한 부정적 영향을 미칠 것으로 예상	정보 시스템에 대한 접근 및 사용 중단은 조직의 운영과 자산 또는 개인에게 극심한 또는 재앙적인 부정적 영향을 미칠 것으로 예상

표 4 11가지 보안위협에 대한 정의
Table 4 Definition of 11 Threats

보안위협	세분화
(T1)기기 및 시스템에 저장된 데이터의 유출	(T1-2)중요도 낮은 데이터
	(T1-3)중요도 높은 데이터
(T2)통신 데이터의 유출	(T2-2)중요도가 낮은 통신 데이터
	(T2-3)중요도가 높은 통신 데이터
(T3)기기 및 시스템 저장 데이터의 삭제	(T3-2)중요도가 낮은 데이터의 삭제
	(T3-3)중요도가 높은 데이터의 삭제
(T4)기기 및 시스템 저장 데이터의 변조	(T4-2)중요도가 낮은 저장 데이터의 변조
	(T4-3)중요도가 높은 저장 데이터의 변조
(T5)통신 데이터의 변조	(T5-2)중요도가 낮은 통신 데이터의 변조
	(T5-3)중요도가 높은 통신 데이터의 변조
(T6)통신 데이터의 위조	(T6-2)중요도가 낮은 통신 데이터의 위조
	(T6-3)중요도가 높은 통신 데이터의 위조
(T7)물리적 접근을 통한 기기 조작	(T7-1)물리적 공격 위협이 낮은 기기의 물리적 접근
	(T7-2)물리적 공격 위협이 높지만 피해 파급효과가 낮은 기기의 물리적 접근
	(T7-3)물리적 공격 위협이 높지만 피해 파급효과가 높은 기기의 물리적 접근
(T8)기기 및 컴퓨팅 장치의 네트워크 부당 접속	(T8-2)필드 네트워크에 부당 접속
	(T8-3)운영 네트워크에 부당 접속
(T9)행위의 부인	(T9-2)개인 및 측정장치(센서) 등에 피해가 발생하는 행위의 부인
	(T9-3)단체 및 산업, 국가 등에 피해가 발생하는 행위의 부인
(T10) 담당자, 기기, 프로세스 등이 허용되지 않은 기능 사용	(T10-1)데이터 읽기와 관련된 허용되지 않은 기능 사용
	(T10-2)데이터 생성 또는 조작과 관련된 허용되지 않은 기능 사용
	(T10-3)제어와 관련된 허용되지 않은 기능 사용
(T11)자원의 과도한 사용	(T11-2)일반 시스템 자원의 과도한 사용
	(T11-3)네트워크 자원 또는 중요 시스템의 자원을 과도하게 사용

표 5 보안 요구사항의 정의

Table 5 Definition of security requirements

보안 요구사항	세분화
(SR1) 안전한 로컬 및 원격 접속 방안	(SR1-2)로컬 및 원격 접속을 위한 계정 설정
	(SR1-3)로컬 및 원격 접속을 위한 계정 설정 기능과 무선 및 원격 로그인 절차 시 암호화 통신 기능
(SR2) 조건 별 사용자의 접근 권한 설정 방안	(SR2-2)가부 결정 수준의 접근권한 설정
	(SR2-3)기기 자원과 보안설정 실행 수준에 따라 사용자 접근 권한 설정
(SR3) 저장된 개인정보 및 전력 운영정보의 유출 방지 방안	(SR3-3)중요 정보 암호화 기능
(SR4) 저장된 암호학적 중요 정보의 유출 방지 방안	(SR4-3)검증받은 S/W 보안 모듈 또는 HSM(Hardware Security Module)을 사용하여 암호화와 관련된 일련의 과정 수행 및 암호화 관련 중요 정보 생성 및 저장 기능
(SR5) 기기 및 시스템에 저장된 중요 정보의 변조 여부 확인 방안	(SR5-3)해시 알고리즘으로 저장된 데이터 변조 또는 삭제 여부 확인 기능
(SR6) 기기 침해사고 발생시 사고분석을 위한 로그 생성, 저장, 전송 방안	(SR6-1)기기에서 1개월 이상의 로그 저장 또는 실시간으로 로그 서버에 전송
	(SR6-2)기기에서 3개월 이상의 로그 저장 또는 실시간으로 로그 서버에 전송
	(SR6-3)기기에서 6개월 이상의 로그 저장 또는 실시간으로 로그 서버에 전송
(SR7) 통신 개체 인증 방안	(SR7-2)단방향 인증 기능
	(SR7-3)상호 인증 기능
(SR8) 응용 계층 서비스 단의 정보 전달에 있어서 네트워크 구조 및 서비스 데이터 특성에 따라 End-to-End 무결성 제공 여부	(SR8-2)Hop-by-Hop 구간별 메시지 인증코드(MAC)를 통한 무결성 제공
	(SR8-3)End-to-End 구간의 메시지 인증코드(MAC)를 통한 무결성 제공
(SR9) 응용 계층 서비스 단의 정보 전달에 있어서 서비스 데이터 특성에 따라 End-to-End 기밀성 제공 여부	(SR9-2)Hop-by-Hop 구간의 데이터 암호화를 통한 기밀성 제공
	(SR9-3)End-to-End 구간의 데이터 암호화를 통한 End-to-End 기밀성 제공
(SR10) 응용 계층 서비스 단의 정보 전달에 있어서 서비스 데이터 특성에 따라 부인방지 기능 제공 여부	(SR10-2)특정 주기로 서비스 데이터 전송 시, 부인방지 서비스 제공을 위한 전자서명 기능 탑재
	(SR10-3)서비스 데이터 전송 시마다 부인방지 서비스 제공을 위한 전자서명 기능 탑재
(SR11)연계 장치에서 네트워크 접근제어 방안	(SR11-2)기기 MAC(Media Access Control) 주소, IP 주소 등을 통한 비인가 트래픽 접근제어 제공
	(SR11-3)데이터 무결성 기능을 통한 비인가 트래픽 접근제어 제공
(SR12)DDoS 공격의 영향을 경감시키거나 제한할 수 있는 방안	(SR12-2)인가되지 않은 트래픽 또는 비정상적인 트래픽 탐지 및 차단 기능
	(SR12-3)통신 프로토콜 개발 시 DDoS 공격을 고려한 설계
(SR13)통신 프로토콜 설계 시, MAC 값 필드를 고려한 통신 데이터 구조 설계	(SR13-3)데이터 무결성 제공을 위한 MAC 값 필드 및 보안 관련 컨텍스트를 고려한 통신 데이터 구조 설계
(SR14)안전한 통신 프로토콜 사용	(SR14-3)SNTP, SNMP, FTP, HTTP의 경우 보안 기능을 지원하는 프로토콜 사용
(SR15)개체 인증, 데이터 무결성 및 기밀성 제공을 위해 안전한 암호 알고리즘 선택 및 사용 방안	(SR15-3)대칭키의 경우 보안강도 128 비트 이상의 암호 알고리즘, 공개키의 경우 보안강도 112 비트 이상의 암호 알고리즘 선택 및 사용
(SR16) 스마트그리드 기기가 외부 환경에 노출될 경우, 물리적인 공격으로부터 안전할 수 있도록 하는 방안	(SR16-1)물리적인 접근 제한
	(SR16-2)물리적인 보호 장치 설치 및 접근 탐지 기능
	(SR16-3)탬퍼 탐지(Tamper Proof) 및 탬퍼 방지(Anti-Tampering) 기능

4. 사례연구

4.1 사례연구 전제

스마트그리드 사이버보안 확보 방안을 기반으로 전력계통 제어시스템 별 사이버보안 대책 수립을 위한 사례연구를 수행한다. 보안확보 검토 대상은 제2장에 기술된 EMS, DCS, SCADA, DAS, RTU으로 국한한다.

본 사례연구는 다음과 같이 사이버보안 대책을 위한 단계별 위치매핑을 위해 스마트그리드 보안 표준서에서 정의한 기준들을

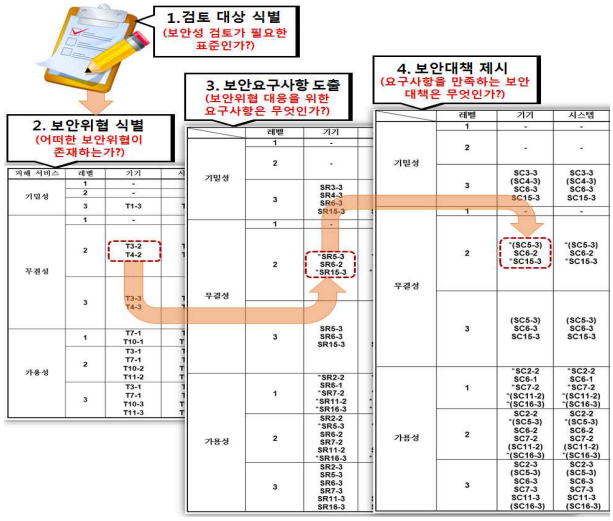

그림 4 대책 수립을 위한 단계별 위치매핑
Fig. 4 Step-by-step location mapping for countermeasures

표 6 보안위협에 따른 보안 요구사항
Table 6 Security Requirements about Security Threats

보안위협	보안 요구사항
	시스템 및 기기
T1	SR3, SR4, SR6, SR15
T2	SR7, SR9, SR15
T3	SR6
T4	SR5, SR6, SR15
T5	SR7, SR8
T6	SR7, SR8
T7	SR6, SR16
T8	SR1, SR2, SR7, SR11
T9	SR4, SR7, SR10
T10	SR2, SR6
T11	SR12

적용한다.

4.2 전력계통 제어시스템 별 사이버 보안대책 수립

전력계통 제어시스템 별 사이버 보안대책 수립을 위해 우선적으로 보안성 확보 대상을 식별한다. 본 사례연구에서는 3.1절에 기술된 세 번째 방안으로 위험도 판단 기준을 통해 보안성 확보 대상을 파악하였다. 〈표 3〉의 위험도 판단 기준을 기반으로 전력계통 제어시스템별 보안성 확보 대상을 파악하면 다음과 같다.

통상 전력계통 제어시스템에서 가용성을 최우선으로 하며 [12], [13], [14], 계통별 제어시스템의 유기적인 연계운영 체계를 고려하여 가용성에 대해 모든 요소가 동일하게 '높음'으로 정의한다.

표 7 시스템 및 기기에 대한 단계별 위치매핑
Table 7 Step-by-step location mapping

	위험도	(2단계)보안위협 식별	(3단계)보안 요구사항	(4단계)보안대책
		시스템 및 기기		
기밀성	1	-	-	-
	2	T1-2 T2-2	*SR3-3 *SR4-3 SR6-2 SR7-2 SR9-2 *SR15-3	*SC3-3 *(SC4-3) SC6-2 SC7-2 SC9-2 *SC15-3
	3	T1-3 T2-3	SR3-3 SR4-3 SR6-3 SR7-3 SR9-3 SR15-3	SC3-3 (SC4-3) SC6-3 SC7-3 SC9-3 SC15-3
무결성	1	-	-	-
	2	T3-2 T4-2 T5-2 T6-2 T9-2	*SR4-3 *SR5-3 SR6-2 SR7-2 SR8-2 SR10-2 *SR15-3	*(SC4-3) *(SC5-3) SC6-2 SC7-2 SC8-2 SC10-2 *SC15-3
	3	T3-3 T4-3 T5-3 T6-3 T9-3	SR4-3 SR5-3 SR6-3 SR7-3 SR8-3 SR10-3 SR15-3	(SC4-3) (SC5-3) SC6-3 SC7-3 SC8-3 SC10-3 SC15-3
가용성	1	T7-1 T10-1	*SR2-2 SR6-1 SR16-1	*SC2-2 SC6-1 (SC16-1)
	2	T3-2 T7-2 T10-2 T11-2	SR2-2 SR6-2 SR12-2 SR16-2	SC2-2 SC6-2 (SC12-2) (SC16-2)
	3	T3-3 T7-3 T10-3 T11-3	SR2-3 SR6-3 SR12-3 SR16-3	SC2-3 SC6-3 (SC16-2) (SC16-3)

* : 상위 요구사항으로 대체하여 사용
( ) : 보안대책으로 적용할 표준 미식별 → 별도의 보안책 필요

기밀성은 계통별 제어시스템 중 배전계통을 제외하고 '높음'으로 설정한다. 배전계통의 경우 임의의 외란에 대해 국소적인 정전이 예상되고, 초고압 관련 계통에 비해 종속사고(cascaded outage)가 상대적으로 소규모이므로 '중간'으로 설정하였다. 또한 전력시스템 보안과 관련된 다양한 국제표준에서는 기기의 특성에 따라 기밀성을 요구하지 않는 경우도 많으며[5], 환경에 따라 선택사항으로 지정하고 있으므로 정보송수신 기기인 RTU에 대해서

표 8 전력계통 제어시스템별 위험도 결과
Table 8 Result of risk by power control systems

제어분야	시스템 및 기기	기밀성	무결성	가용성
전력계통	EMS	높음	높음	높음
발전계통	DCS	높음	높음	높음
송변전계통	SCADA	높음	높음	높음
배전계통	DAS	중간	중간	높음
정보송수신	RTU	중간	중간	높음

도 '중간'으로 설정한다.

마지막으로 무결성은 정보의 위·변조에 대한 피해효과도 중요한 고려 사항이므로 실제 입출력 데이터에 대한 제어기능을 갖는 요소 중 종속사고의 영향력이 큰 범위에 대해 '높음'으로 설정하였다. 다만 상대적인 정전피해에 대한 파급력과 단순 데이터의 수집 기능을 갖는 시스템 및 장치는 잠재적 영향이 미미하다고 판단되어 '중간'으로 평가한다.

다음으로 2단계인 보안성 확보 대상에 대한 관련 보안위협을 식별하고자 총 11가지 보안위협(표 4번)을 기반으로 전력계통 제어시스템 별 해당 보안위협을 파악한다. 먼저 11가지 보안위협 중 정보에 대한 보안침해 관련 위협(T1~T6)에 대해 분석하면 〈표 9〉와 같다. 〈표 9〉에서 중요도는 피해수준과 파급효과의 결과 중 최상의 기준으로 적용하였으며, 각 시스템의 정보 특성에 따라 (T1)에서 (T6)까지 표준 보안위협을 파악하였다.

상기 위협(T1~T6)들을 제외한 나머지 보안위협에 대한 식별하면 다음과 같다. 물리적 접근 보안위협(T7)에 대해 분석시 〈표 10〉에, 네트워크 부당 접속(T8)과 행위의 부인 관련 위협(T9)에 대해 정리하면 〈표 11〉과 같다. 이외 보안위협(T10, T11)에 대해서는 〈표 12〉와 〈표 13〉과 같이 정리할 수 있다.

2단계의 전력계통 제어시스템 별 식별된 보안위협을 정리하면 〈표 14〉과 같다. 다음으로 식별된 보안위협 정보(표 14)와 보안위협에 따른 보안요구사항(표 6) 및 단계별 위치매핑(표 7) 자료를 활용하여 보안 요구사항을 도출(3단계) 후 이에 따른 대책을 수립(4단계)한다. 본 연구에 활용된 보안 표준서에서는 대상 표준의 기능을 고려하여 무관한 보안 요구사항이 존재한다고 판단될 경우 제외시킬 수 있다고 언급되어 있지만, 본 사례연구에서는 도출된 보안 요구사항을 모두 고려하여 이에 상응하는 보안대책을 수립한다. 이에 따른 결과는 〈표 15〉와 같다.

〈표 15〉의 결과를 분석해보면, EMS, DCS, SCADA, DAS은 시스템으로 분류되어 보안대책에 대한 항목들이 유사함을 알 수 있

표 10 물리적 접근 보안위협(T7) 식별
Table 10 Identification of physical access security threats (T7)

대상	장소 위험도	피해파급	T7
EMS	하	상	T7-1
DCS	하	상	T7-1
SCADA	하	상	T7-1
DAS	중	상	T7-3
RTU	하	하	T7-1

표 11 네트워크 부당 접속과 행위의 부인 위협 식별
Table 11 Identification of threats to network denial of access and denial of conduct

대상	네트워크 부당 접속(T8)	행위의 부인(T9)
EMS	T8-3	T9-3
DCS	T8-3	T9-3
SCADA	T8-3	T9-3
DAS	T8-3	T9-3
RTU	T8-2	T9-2

표 12 허용되지 않은 기능에 대한 사용위협(T10) 식별
Table 12 Identification of usage threats (T10) for unauthorized functions

대상	기능유형	접근 가능성	T10
EMS	시스템 제어	가능성 없음	-
DCS	시스템 제어		-
SCADA	시스템 제어		-
DAS	시스템 제어	가능성 있음	T10-3
RTU	데이터 읽기	가능성 없음	-

표 13 과도한 자원 사용 위협(T11)
Table 13 Excessive resource use threat (T11)

대상	자원유형	대상 중요도	T11
EMS	시스템	상	T11-3
DCS	시스템	상	T11-3
SCADA	시스템	상	T11-3
DAS	시스템	상	T11-3
RTU	기기	중	T11-2

표 9 정보 관련 보안위협(T1~T6) 식별
Table 9 Identification of information-related security threats (T1-T6)

대상	피해수준	파급효과	중요도	T1	T2	T3	T4	T5	T6
EMS	상	상	상	T1-3	T2-3	T3-3	T4-3	T5-3	T6-3
DCS	상	상	상	T1-3	T2-3	T3-3	T4-3	T5-3	T6-3
SCADA	상	상	상	T1-3	T2-3	T3-3	T4-3	T5-3	T6-3
DAS	중	중	중	T1-3	T2-3	T3-3	T4-3	T5-3	T6-3
RTU	하	중	중	T1-2	T2-2	T3-2	T4-2	T5-2	T6-2

표 14 전력계통 제어시스템별 보안위협 식별
Table 14 Identification of security threats by power control systems

보안위협 11종			T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11
EMS	보안위협 식별		T1-3	T2-3	T3-3	T4-3	T5-3	T6-3	T7-1	T8-3	T9-3	-	T11-3
	위험도	기밀성	3	3	-	-	-	-	-	-	-	-	-
		무결성	-	-	3	3	3	3	-	-	3	-	-
		가용성	-	-	3	-	-	-	1	-	-	-	3
DCS	보안위협 식별		T1-3	T2-3	T3-3	T4-3	T5-3	T6-3	T7-1	T8-3	T9-3	-	T11-3
	위험도	기밀성	3	3	-	-	-	-	-	-	-	-	-
		무결성	-	-	3	3	3	3	-	-	3	-	-
		가용성	-	-	3	-	-	-	1	-	-	-	3
SCADA	보안위협 식별		T1-3	T2-3	T3-3	T4-3	T5-3	T6-3	T7-1	T8-3	T9-3	-	T11-3
	위험도	기밀성	3	3	-	-	-	-	-	-	-	-	-
		무결성	-	-	3	3	3	3		-	3	-	-
		가용성	-	-	3	-	-	-	1	-	-	-	3
DAS	보안위협 식별		T1-3	T2-3	T3-3	T4-3	T5-3	T6-3	T7-3	T8-3	T9-3	T10-3	T11-3
	위험도	기밀성	3	3	-	-	-	-	-	-	-	-	-
		무결성	-	-	3	3	3	3	-	-	3	-	-
		가용성	-	-	3	-	-	-	3	-		3	3
RTU	보안위협레벨		T1-2	T2-2	T3-2	T4-2	T5-2	T6-2	T7-1	T8-2	T9-2	-	T11-2
	위험도	기밀성	2	2	-	-	-	-	-	-	-	-	-
		무결성	-	-	2	2	2	2	-	-	2	-	-
		가용성	-	-	2	-	-	-	1	-	-	-	2

표 15 위치매핑 기반 보안대책 수립
Table 15 Establishment of security measures based on location mapping

	위험도	시스템									기기		
		EMS			DCS 및 SCADS			DAS			RTU		
		2단계	3단계	4단계	2단계	3단계	4단계	2단계	3단계	4단계	2단계	3단계	4단계
기밀성	1	-	-	-	-	-	-	-	-	-	-	-	-
	2	-	-	-	-	-	-	-	-	-	T1-2 T2-2	*SR3-3 *SR4-3 SR6-2 SR7-2 SR9-2 *SR15-3	*SC3-3 *(SC4-3) SC6-2 SC7-2 SC9-2 *SC15-3
	3	T1-3 T2-3	SR3-3 SR4-3 SR6-3 SR7-3 SR9-3 SR15-3	SC3-3 (SC4-3) SC6-3 SC7-3 SC9-3 SC15-3	T1-3 T2-3	SR3-3 SR4-3 SR6-3 SR7-3 SR9-3 SR15-3	SC3-3 (SC4-3) SC6-3 SC7-3 SC9-3 SC15-3	T1-3 T2-3	SR3-3 SR4-3 SR6-3 SR7-3 SR9-3 SR15-3	SC3-3 (SC4-3) SC6-3 SC7-3 SC9-3 SC15-3	-	-	-
무결성	1	-	-	-	-	-	-	-	-	-	-	-	
	2	-	-	-	-	-	-	-	-	-	T3-2 T4-2 T5-2 T6-2 T9-2	*SR4-3 *SR5-3 SR6-2 SR7-2 SR8-2 SR10-2 *SR15-3	*(SC4-3) *(SC5-3) SC6-2 SC7-2 SC8-2 SC10-2 *SC15-3
	3	T3-3 T4-3 T5-3 T6-3 T9-3	SR4-3 SR5-3 SR6-3 SR7-3 SR8-3 SR10-3 SR15-3	(SC4-3) (SC5-3) SC6-3 SC7-3 SC8-3 SC10-3 SC15-3	T3-3 T4-3 T5-3 T6-3 T9-3	SR4-3 SR5-3 SR6-3 SR7-3 SR8-3 SR10-3 SR15-3	(SC4-3) (SC5-3) SC6-3 SC7-3 SC8-3 SC10-3 SC15-3	T3-3 T4-3 T5-3 T6-3 T9-3	SR4-3 SR5-3 SR6-3 SR7-3 SR8-3 SR10-3 SR15-3	(SC4-3) (SC5-3) SC6-3 SC7-3 SC8-3 SC10-3 SC15-3	-	-	-
가용성	1	T7-1	SR6-1 SR16-1	SC6-1 (SC16-1)	T7-1	SR6-1 SR16-1	SC6-1 (SC16-1)	-	-	-	T7-1	SR6-1 SR16-1	SC6-1 (SC16-1)
	2	-	-	-	-	-	-	-	-	-	T3-2 T11-2	SR6-2 SR12-2	SC6-2 (SC12-2)
	3	T3-3 T11-3	SR6-3 SR12-3	SC6-3 (SC12-3)	T3-3 T11-3	SR6-3 SR12-3	SC6-3 (SC12-3)	T7-3 T10-3 T11-3	SR2-3 SR6-3 SR16-3 SR12-3	SC2-3 SC6-3 (SC16-2) (SC16-3)	-	-	-

다. 다만 DAS의 가용성이 타 시스템에 비해 취약하게 분석되었고, 이에 적합한 보안대책을 요구한다.

다음으로 단순 정보전달의 기능을 수행하는 RTU는 시스템에 비해 상대적으로 낮은 단계(2단계)의 보안대책 수립을 요한다. 그러나 최근 통신기술의 발달로 인하여 RTU에도 제어기능을 보유하여, 기능의 범위가 확대되고 추세이므로 지속적으로 업데이트된 보안대책이 필요할 것으로 사료된다.

5. 결 론

본 논문은 갈수록 증대하고 있는 전력계통의 사이버 보안 문제들을 명확하게 정의하고 관련 제어 시스템과 사이버 보안 문제의 연계성을 구체화 하는데 목적이 있다. 즉, 전력계통 제어시스템 간의 유기적 관련성, 기능 등을 토대로 시스템 별 사이버위협을 식별한 후 보안대책을 제시함으로써 사이버보안 대책 수립 프로세스를 구체화하였다.

본 연구는 정성적인 보안대책 수립 기법으로 다소 주관적인 결과로 인식될 수 있으나, 스마트그리드 보안에 대한 국가 표준을 기반으로 선행연구 결과를 통해 객관성을 제고하였다. 다만 전력 기술과 정보통신 기술을 융합하는 방법론 적 특성 상 정량적 결과 도출에 한계는 피하라 수 없지만 추가 연구를 통해 개선이 가능할 것으로 판단된다.

우리나라의 경우, 전력계통의 특수성이 반영된 사이버보안 기준이 구체적으로 정립되지 않은 상태로서 관련 연구가 진행 중에 있다[15].

성공적인 스마트그리드 운영의 기본은 안전성과 보안성 확보라 판단되며, 향후 전력계통의 물리적인 지표가 반영된 사이버 보안 기준이 마련될 경우, 보다 유의미한 사이버보안 대책 방안이 강구될 것이다.

감사의 글

본 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임.
(No. 2015R1D1A1A01057823)

References

[1] "National Road-map for Smart Grid", *Ministry of Knowledge Economy*, 2010.

[2] "The 1st Basic Plan for Smart Grid", *Ministry of Knowledge Economy*, 2012.

[3] "The 2nd Basic Plan for Smart Grid", *Ministry of Trade, Industry and Energy*, 2018.

[4] Pil Sung Woo, Sang Sun Hwang, Soon Hyun Hwang, Balho H. Kim, "Risk assessment for Security of Power Information Control System", to be published. 2018.

[5] Kyung Sub Lee, "A study on KEPCO AMI system security policy in compliance with domestic legal regulations and standards", *MS thesis. Department of Cyber Security, Korea University. Korea*: 2015.

[6] Korea Electrotechnology Research Institute, "A Study on Establishment of Smart Grid-based System Operation and Information Process", *Korea Power Exchange*, 2011.

[7] Young Chang Kim, "Understanding of the power industry," *The Korean Institute of Electrical Engineers*, 2012.

[8] Korea Electrotechnology Research Institute, "A Study on Estimation of Generator Start-up Cost and Improvement of Application standard", *Korea Power Exchange*, 2012.

[9] Ju Heon Lee, Sang Joong Lee, "An Accuracy Improvement on Acquisition Time of SCADA RTU Status Events", *The Transactions of the Korea Institute of Electrical Engineers*, vol. 62, no. 3, pp. 332-341, 2013.

[10] B. N. Ha, S. W. Lee, C. H. Shin, I. Y. Seo, M. H. Park, G. G. Yun, I. K. Song, B. S. Lee, J. C. Lee, W. Nam Koong, "Development of Intelligent distribution auto- mation system with the function of suvstation SCADA, power quality monitoring and diagnosis condition monitoring", *Transactions of the Korea Institute of Electrical Engineers*, 2010.

[11] "Requirements for Ensuring of Smart Grid Standards (SGSF-121-1-1)", Korea Smart Grid Association, 2014.

[12] TS System Ltd., Yonsei University, Korea Power Exchange, "Evaluation of Network facility and Operation System for Smart Grid", *Ministry of Trade,* Industry and Energy, 2013.

[13] Rajendra Kumar Pandey, Mohit Misra, "Cyber Security Threats - Smart Grid Infrastructure," I EEE, 2016.

[14] Pil Sung Woo, Balho H. Kim, "Methodology of Cyber Security Assessment in the Smart Grid," *Journal of Electrical Engineering and Technology*, pp. 495-501, The Korean Institute of Electrical Engineers, 2017.

[15] Dong Joo Kang, Huy Kang Kim, "A Study on Application in Korea and Analysis of NERC Regulations for Establishment of Reliability Standard for Power System from the Viewpoint of Cyber Security", *Journal of The Korea Institute of Information Security and Cryptology*, vol. 25, no. 5, pp.18-25, 2015.

저 자 소 개

우 필 성 (Pil Sung Woo)

1987년 5월 6일생. 2012년 배재대 광전기공학과 졸업. 2014년 홍익대 전기정보제어공학과 졸업(석사). 2016년 동 대학원 전기정보제어공학과 박사수료. 현재 한국전기안전공사 전기안전연구원 재직중.
관심분야 : 스마트그리드, 최적화이론
E-mail : wps@kesco.or.kr

김 발 호 (Balho H. Kim)

1962년 7월 11일생. 1984년 서울대학교 전기공학과 졸업. 1984~1990년 한국전력공사 전력경제연구실 근무. 1992년 Univ. of Texas at Austin 전기공학과 졸업(석사). 1996년 동 대학원 전기공학과 졸업(공학박사). 19997년~현재 홍익대학교 전자전기공학부 교수.
관심분야 : OPF, 최적화이론, 전력경제(시장)
E-mail : bhkim0711@gmail.com