에너지공학, 제24권 제1호(2015)
Journal of Energy Engineering, Vol. 24, No. 1, pp.123~131(2015)
http://dx.doi.org/10.5855/ENERGY.2015.24.1.123

스마트그리드 체제에 따른 EMS의 보안 평가를 위한 정량적 방법론에 관한 연구

우필성·김발호†
홍익대학교

(2014년 11월 20일 접수, 2015년 2월 5일 수정, 2015년 2월 6일 채택)

A Study on Quantitative methodology to Assess Cyber Security Risks of EMS

Pil Sung Woo, Balho H. KIM†
Hongik University

(Received 20 November 2014, Revised 5 February 2015, Accepted 6 February 2015)

요 약

스마트그리드는 저탄소 녹색성장의 선도 프로젝트로 추진하는 핵심과제로 전력산업의 환경변화에 적응하고 에너지이용 효율을 제고하기 위한 새로운 전력시스템이다.

현 전력계통은 폐쇄적인 EMS(Energy Management System)를 기반으로 운영되어 최소한의 보안강도가 보장되었지만, 스마트그리드 하에서는 개방형 통신망과 연계되면서 기존의 사이버 보안 위협들이 전력시스템으로 유입된다. 또한 EMS와 같은 제어시스템은 실시간 특성이 강하게 요구되며, 높은 수준의 가용성(낮은 고장 빈도와 신속한 복구)이 필요하다. 즉, EMS의 사이버 위협은 IT시스템에 비해 보다 복잡하고 치명적인 요인이 된다.

본 논문에서 갈수록 증대하고 있는 스마트그리드 보안 측면의 문제들을 정의하고, 피상적으로 머물던 스마트그리드의 사이버 위험 문제를 물리적 전력계통과 연계하고 모델링하여 수치로 산출할 수 있는 정량화 방법론을 제시하였다.

주요어 : 스마트그리드, EMS, 사이버보안, 최적조류계산, 조류추적법

Abstract - This paper aims to identify and clarify the cyber security risks and their interaction with the power system in Smart Grid. The EMS and other communication networks interact with the power system on a real time basis, so it is important to understand the interaction between two layers to protect the power system from potential cyber threats. In this study, the optimal power flow(OPF) and Power Flow Tracing are used to assess the interaction between the EMS and the power system. Through OPF and Power Flow Tracing based analysis, the physical and economic impacts from potential cyber threats are assessed, and thereby the quantitative risks are measured in a monetary unit.

Key words : Smart Grid, EMS, Cyber Security, OPF, Power Flow Tracing

1. 서 론

현재 전력산업은 대내외적으로 다양한 환경적 변화에 직면하고 있다. 그 중의 하나로 스마트그리드는 저탄소 녹색성장의 선도 프로젝트로 추진하는 핵심과제로 전력산업의 환경변화에 적응하고 에너지이용 효율

†To whom corresponding should be addressed.
School of Electronic & Electrical Engineering, Hongik University, 72-1 Sangsu-dong, Mapo-gu, Seoul 121-791, Korea
Tel : 02-320-1462 E-mail : bhkim@hongik.ac.kr

을 제고하기 위한 새로운 전력시스템이다.

그러나 전력시스템은 실시간 특성이 강하게 요구되며, 높은 수준의 가용성(낮은 고장 빈도와 신속한 복구)이 필요하다. 기 특성은 전력시스템의 사이버 위협을 IT 시스템에 비해 보다 복잡하고 치명적으로 만드는 요인이 된다. 즉, 일반적인 통신 네트워크와 달리 전력시스템은 하부의 전력계통과 연결되고 상호 응동되기 때문에 사이버 측면에서의 위협이 큰 규모의 물리·재무적 피해로 직결된다.

반면 전력시스템 및 스마트그리드에 대한 사이버 보안 문제가 이슈가 되고 있음에도 불구하고, 현재까지의 연구는 기존의 통신 네트워크 범주를 벗어나지 못하고 있다. 이는 통신시스템과 전력시스템을 동시에 이해할 수 있는 전문 인력이 부족하기 때문으로 분석되며, 전력계통의 특성을 반영한 사이버 보안 연구가 필요하다고 판단된다.

따라서 본 논문에서는 갈수록 증대하고 있는 스마트그리드 보안 측면의 문제들을 명확히 정의하고, 전력시스템과의 연계성을 구체화하는 데 그 목적이 있다. EMS와 같은 정보시스템과 전력계통의 상호작용에 대한 구체적인 모델링을 통해 위험을 평가하는 방법론을 제안하고, 사례연구를 통하여 향후 스마트그리드 체제에 따른 전력계통의 안전운영을 도모할 수 있는 특화된 보안대책 수립하였다.

2. 스마트그리드 구축 시 전력시스템 운영 변화

2.1. 현 전력시스템 운영

현재 전력망은 폐쇄형 구조로 운영되며, 전력의 원활한 공급을 위한 최소의 데이터 교환만을 수행하고 있다. 또한 전력공급 시스템은 발전소에서 가정에 이르기까지 단일방향의 통신체제로 운영되며 <Fig. 1>과 같이 크게 EMS, SCADA, RTU로 구성되며, 각 장치들은 통신설비(TCP & Serial)로 연계되어 있다[2].

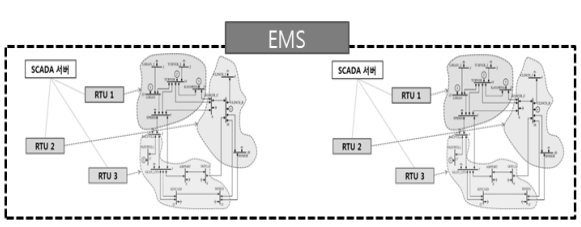


Fig. 1. 현 전력제어의 EMS 구조

2.2. 스마트그리드 체제에 따른 전력시스템 운영

우리나라의 스마트그리드 도입은 에너지 비용의 감소, 신재생에너지 발전의 확대 여건 마련 및 수출 산업화 등 국제경쟁력 확보 차원의 전략적 추진 성격이 강하다. 스마트그리드 관련 연구는 전력 IT로써 산업통산자원부가 주도하고 송배전, 통신, 분산전원 등의 분야에서 전력선통신 기술, 배전지능화 기술 등의 연구를 수행하고 있다.

이에 따라 정부는 제주도를 스마트그리드 실증단지로 선정하고 2010년부터 본격적으로 기술실증에 착수한 뒤, 2011년부터 시범도시를 중심으로 대규모 보급을 추진 중에 있다. 2020년까지 소비자 측 지능화를 완료하고, 2030년까지 국토 전체의 전력망지능화를 완료할 계획이다[1].

3. 스마트그리드 체제에서 전력시스템의 위험 정량화 방법

보안 취약성에 대한 SANS의 정의에 따르면[7], 일반적으로 IT분야에서 사이버위험은 취약성, 위협, 자산들이 조합되어 실질적으로 발생 가능한 위험으로 정의한다.

<Fig. 2>과 같이 취약성이란 위협과 자산 간의 관계를 정의하는 매개변수로 인식할 수 있고, 위협은 사이버 공격을 의미하며 독립변수로 인식할 수 있다. 마지막으로 자산은 취약성으로부터 위협이 발발한 경우의 피해규모를 의미한다.

기 관점에서 위협(T), 취약성(V), 자산(A)로 정의하면 위험(R)에 대하여 식(1)과 같이 정리할 수 있다. 식(1)은 전력시스템에서 실질적으로 발생 가능한 피해규모를 의미한다.

$$R = T \times V \times A \tag{1}$$

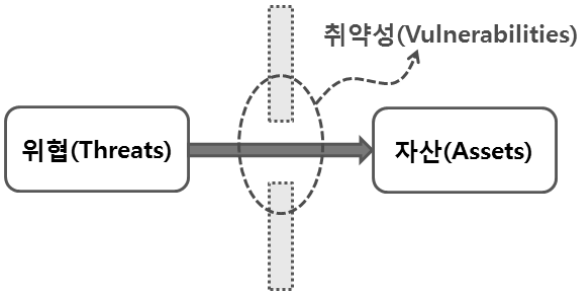


Fig. 2. 취약성의 개념 및 역할

상기 식을 기본으로 각 요소에 대해 상세히 정의함으로써 위험을 정량화 할 수 있는 체계를 수립할 수 있다. 각 요소 중에서 T와 V는 정보계층의 요소로 정의하고, 국내외의 선행연구를 기반으로 정량화하였다. A의 경우에는 전력계통의 측면에서 정량화하였다.

최종적으로 사이버 위험을 전력계통의 신뢰도 관점과 유기적으로 연계하기 위해, 전력계통 운용의 핵심기술인 최적조류계산(Optimal Power Flow, OPF)와 조류추적법(Power Flow Tracing)을 적용하여 전력계통에 실질적 영향을 미치는 물리·경제적 효과들을 정량적으로 분석하여 종합적인 신뢰도 평가 방안을 제안하였다.

3.1. 정보계층의 정량적 모델링

정보계층 요소의 정량적 모델링에 관한 선행연구들의 분석 한 바, 스마트그리드에서 사이버 위협 및 취약성을 정량화하기 위해 주로 Attack Graph를 통해 공격을 정의하고[10], 해당공격 유형별로 발생 가능한 확률을 적용함으로써 위험성을 측정하려는 시도를 하였다[3-5].

본 논문에서는 선행연구의 데이터를 기반으로 다속성을 고려한 정량적 평가 방법 중의 하나인 AHP(Analytic Hierarchy Process)의 과정 일부를 본 연구에 적용하였다.

3.1.1. 취약성(V) 정량화

본 논문에서는 15종의 사이버 위협을 선별하고, 전력시스템의 구성요소와 개별 사이버 위협의 인과관계에 따라 취약성을 정량화하였다. 전력시스템은 통상적으로 EMS 의 제어를 통해 운영되므로 2장에서 기술된 EMS의 구성요소로 정의하였다.

<Table 1>에서 음영부분(V)은 해당 취약성에 의하여 실질적인 위험이 발생함을 의미한다. 반면 미 음영부분(0)은 사이버 위협의 가능성이 없음을 의미한다.

취약성이란 위협이 자산에 대해 현실화되는 확률 개념으로 생각할 수 있으므로 $0 \leq$ 취약성(V) ≤ 1의 값을 갖게 된다. 여기서 1은 <Fig. 2>에 따라 위협이 통과되어 자산에 연결됨을 의미한다. 취약성은 절대적으로 정의될 수 없기 때문에 2가지의 가정을 세웠다.

첫째, 과거의 데이터가 부재할 경우 위협의 확률은

Table 1. IT 위협요소에 따른 EMS 구성요소의 취약성 분석

시스템 구성 / 위협의 종류	EMS 서버	SCADA 서버	통신 네트워크		RTU
			TCP/IP	Serial	
Eavesdropping	V	V	V	V	V
Traffic Analysis	0	0	V	V	0
EM/RF Interception	0	0	0	0	V
Indiscretions by Personnel	V	V	0	0	0
Media Scavenging	V	V	0	0	0
Trojan Horse	V	V	0	0	V
Trapdoor(Backdoor)	V	V	0	0	V
Service Spoofing	V	V	0	0	V
Masquerade	0	0	0	0	V
Bypassing Controls	0	0	0	0	V
Authorization Violations	V	V	0	0	V
Physical Intrusion	V	V	V	V	V
Replay	0	0	0	0	V
Theft & Illegitimate Use	0	0	0	0	V
Denial of Service	V	V	V	0	0

50%이다.

둘째, 보안강도는 EMS의 구성요소에 따라 다르므로 각 요소별 상대적 순위를 적용한다.

즉, 보안강도는 서버 단이 가장 강하고 하위 구성요소일수록 작다고 생각할 수 있다. 따라서 취약성은 서버 단(EMS, SCADA) < TCP/IP구간 < Serial구간 < RTU의 수준으로 정의하였다.

기 가정을 적용하면, <Table 2>와 같이 취약성의 정량적 수치를 산출 할 수 있다. 여기서 취약성 수치가 높을수록 사이버 위협에 쉽게 노출되어 있음을 의미한다.

3.1.2. 사이버 위협(T) 수준 정량화

위협에 대한 정량적 수치는 기 분석된 취약성을 기반으로 가로축(EMS 구성요소), 세로축(사이버 위협)에 대하여 각 축에 따른 잠재적 피해규모에 따라 상대적인 순위를 부여하였다. 상대적 순위가 부여된 각 축은 다시 정규화를 하였다. 여기서 정규화는 위협의 크기가 1이고, EMS의 개별 요소들의 위협 수준을 차등 부여됨을 의미한다.

<Table 3>은 EMS의 구성요소의 잠재적 피해규모에 따라 상대적 순위(4~1)를 부여하였다.

순위 산정기준은 다음과 같다. 서버단의 경우 위협에 노출되었을 때 그 잠재적 피해가 가장 크므로 4를 부여한다. RTU의 경우 최하위 말단이므로 상대적으로 가장 낮은 1을 부여한다. 또한 취약성 분석(표 1)을 기반으로 EMS의 구성요소에 해당이 없는 경우는 0을 부여한다.

마지막으로 가로축을 기준으로 해당위협의 크기를 1이라 가정하고 정규화를 적용한다.

<Table 3>은 EMS구성요소 별 잠재적 피해에 따른 정규화 결과이다.

Table 2. 취약성 정량화 산출

	EMS 서버	SCADA 서버	TCP/IP 통신	Serial 통신	RTU
취약성	0.057	0.057	0.051	0.057	0.278

Table 3. EMS 구성요소(가로축) 별 잠재적 피해에 따른 정규화

시스템 구성 / 위협의 종류	EMS 서버	SCADA 서버	통신 네트워크		RTU	정규화
			TCP/IP	Serial		
Eavesdropping	0.29	0.29	0.21	0.14	0.07	1
Traffic Analysis	0.00	0.00	0.67	0.33	0.00	1
EM/RF Interception	0.00	0.00	0.00	0.00	1.00	1
Indiscretions by Personnel	0.50	0.50	0.00	0.00	0.00	1
Media Scavenging	0.50	0.50	0.00	0.00	0.00	1
Trojan Horse	0.40	0.40	0.00	0.00	0.20	1
Trapdoor(Backdoor)	0.40	0.40	0.00	0.00	0.20	1
Service Spoofing	0.40	0.40	0.00	0.00	0.20	1
Masquerade	0.00	0.00	0.00	0.00	1.00	1
Bypassing Controls	0.00	0.00	0.00	0.00	1.00	1
Authorization Violations	0.40	0.40	0.00	0.00	0.20	1
Physical Intrusion	0.29	0.29	0.21	0.14	0.07	1
Replay	0.00	0.00	0.00	0.00	1.00	1
Theft & Illegitimate Use	0.00	0.00	0.00	0.00	1.00	1
Denial of Service	0.40	0.40	0.20	0.00	0.00	1

Table 4. 위협의 종류(세로축) 별 위험도에 따른 정규화

시스템 구성 / 위협의 종류	EMS 서버	SCADA 서버	통신 네트워크		RTU
			TCP/IP	Serial	
Eavesdropping	0.04	0.04	0.13	0.20	0.04
Traffic Analysis	0.00	0.00	0.00	0.00	0.00
EM/RF Interception	0.00	0.00	0.00	0.00	0.04
Indiscretions by Personnel	0.04	0.04	0.00	0.00	0.00
Media Scavenging	0.04	0.04	0.00	0.00	0.00
Trojan Horse	0.08	0.08	0.00	0.00	0.08
Trapdoor(Backdoor)	0.08	0.08	0.00	0.00	0.08
Service Spoofing	0.08	0.08	0.00	0.00	0.08
Masquerade	0.00	0.00	0.00	0.00	0.12
Bypassing Controls	0.00	0.00	0.00	0.00	0.12
Authorization Violations	0.12	0.12	0.25	0.40	0.12
Physical Intrusion	0.12	0.12	0.25	0.40	0.12
Replay	0.12	0.12	0.00	0.00	0.12
Theft & Illegitimate Use	0.12	0.12	0.00	0.00	0.12
Denial of Service	0.16	0.16	0.38	0.00	0.00
정규화	1	1	1	1	1

Table 5. 위협 수준의 정량화 결과

시스템 구성 / 위협의 종류	EMS 서버	SCADA 서버	통신 네트워크		RTU
			TCP/IP	Serial	
Eavesdropping	0.01	0.01	0.03	0.03	0.00
Traffic Analysis	0.00	0.00	0.00	0.00	0.00
EM/RF Interception	0.00	0.00	0.00	0.00	0.04
Indiscretions by Personnel	0.02	0.02	0.00	0.00	0.00
Media Scavenging	0.02	0.02	0.00	0.00	0.00
Trojan Horse	0.03	0.03	0.00	0.00	0.02
Trapdoor(Backdoor)	0.03	0.03	0.00	0.00	0.02
Service Spoofing	0.03	0.03	0.00	0.00	0.02
Masquerade	0.00	0.00	0.00	0.00	0.12
Bypassing Controls	0.00	0.00	0.00	0.00	0.12
Authorization Violations	0.05	0.05	0.00	0.00	0.02
Physical Intrusion	0.03	0.03	0.05	0.06	0.01
Replay	0.00	0.00	0.00	0.00	0.12
Theft & Illegitimate Use	0.00	0.00	0.00	0.00	0.12
Denial of Service	0.06	0.06	0.08	0.00	0.00
합산	0.29	0.29	0.16	0.09	0.58

가로축과 유사한 방식으로 위협의 종류별(세로축)에 대해서도 취약한 정도에 따라 상대적인 순위를 부여하였다. 먼저 정보보안의 3대 요소인 CIA의 개념을 적용하여 위협을 분류하였다. 즉, 15가지의 위협에 대해 기밀성(Confidentiality), 혼재(기밀성 + 무결성), 무결성(Integrity), 가용성(Availability)의 4가지 영역으로 구분하고 각각의 위협은 해당 영역으로 분류하였다.

통상적으로 전력시스템은 제어시스템 기반으로 운영되어 IT시스템에 따른 보안 위협 수준이 아닌 제어시스템의 보안 위협 수준을 적용하였다.

제어시스템 상에서는 가용성 > 무결성 > 혼재 > 기밀성의 순으로 중요하므로 각 영역에 순차적으로 4, 3, 2, 1의 상대적 순위를 부여하였다. 마지막으로 개별 위협 수준의 크기를 1이라고 가정하고 정규화 하였다. 여기서 1은 개별 위협에 가질 위험의 수준을 의미한다. <Table 4>는 위협 종류 별 위험도를 정규화한 결과이다.

최종적인 위협의 정량화를 위해, 두 표(Table 3, Table 4)의 행렬요소 간 곱으로 정량화 하였다. 행렬요소 간의 곱의 결과는 임의의 사이버 위협이 1회 발생 시 각 위협별 및 시스템 구성성분별로 분담하게 되는 위협의 수준을 의미한다. <Table 5>는 최종 위협 수준의 정량화 결과이다.

4.2. 전력시스템에서 자산(A)의 정량화

전력계통 시스템에서의 자산은 EMS를 구축하기 위한 전체 요소의 가치를 의미한다.

자산의 가치를 정량화하기 위해 통신설비의 소실가치와 해당 설비가 위협에 노출되었을 때 발생할 수 있는 기대정전비용만을 고려하였다.

$$A_n = \sum_{k=1}^{P} (LV_n^k(P) + OC_n^k(P)) \cdots LV_n^k + OC_n^k \approx OC_n^k$$
$$= \sum_{k=1}^{P} (OC_n^k(P)) \quad (1)$$

여기서, P : 전력(MW)
k : k번째의 EMS의 하위 구성성분
A_n : n개의 EMS 구성성분의 자산가치
LV_n^k : 통신설비의 소실가치[원]
OC_n^k : 기대정전비용[원]

식(2)는 기 정의한 자산의 가치를 정량화함에 있어서 통신설비와 기대정전비용의 경제적 가치를 합산한다. 통상적으로 전력계통에서는 통신설비의 가치보다는 정전피해비용의 금액이 압도적으로 높기 때문에 기대정전비용으로 근사화 됨을 의미한다.

4.3. 전력계통의 정량적 모델링

특정 사이버 위협이 전력계통에 미치는 영향을 분석하기 위하여 전력시스템 운용의 핵심기술인 최적조류계산과 조류추적법을 이용하여 전력계통을 정량적으로 모델링하였다.

전력조류(Power Flow)는 특정 발전기의 발전량이 특정 부하로 얼마큼 유입되는지 파악할 수가 없다. 따라서 최적조류계산을 이용하여 임의의 계통에 대한 순 발전량(Net Generation)과 전력조류를 산출하였다. 산출된 데이터는 조류추적법을 통하여 발전단과 부하단의 상관관계를 파악하였다. 즉, 사이버 위험을 전력계통의 신뢰도 관점과 유기적으로 연계하여 사이버 위험과 전력계통의 신뢰도를 매개할 수 있는 지표를 정량화하였다.

4.3.1. 최적조류계산(Opimal Power Flow; OPF) 정식화

일반적인 OPF의 개념은 기술적, 물리적, 환경적 제약조건하에서의 경제급전계획을 의미하며 개념적으로는 경제급전계획과 전력조류계산을 동시에 수행하는 것이다. 이를 이용해서 순 발전량과 전력조류를 산출할 수 있다. 본 논문에 사용된 OPF의 정식화는 다음과 같다.

$$\underset{X_{i,g}}{MINMIZE} \sum_i \sum_g Cost_{i,g} \cdot X_{i,g} \quad (3)$$

제약조건 $$\sum_i Load_i = \sum_i \sum_g X_{i,g} \quad (4)$$

$$PF_{i,j,l} = \frac{\delta_i - \delta_j}{x_l} \quad (5)$$

$$X_{i,g} \le CAP_g \quad (6)$$

$$PF_{i,j,l} \le LTmax_l \quad (7)$$

여기서, i, j : 모선
l : 선로
g : 발전기
δ : 모선의 위상각
x_l : 모선 i과 j사이의 선로 리액턴스
$Cost_{i,g}$: g번째 발전기의 발전단가

CAP_g: g번째 발전기 용량
Load : i번째 모선의 부하
$LTmax$: 선로 용량
X_{ij} : 발전기 발전량
PF : 전력조류

목적함수인 식(3)은 발전비용 최소화이다. 제약조건에서 식(4)는 계통의 수급균형을 의미한다. 식(5)는 각 모선에서의 전력수급방정식을 의미한다. DC 최적조류계산을 사용하였기 때문에 전력조류는 위상차에 비례하고 선로 리액턴스에 반비례한다. 식(6)은 발전기 용량제약이고, 식(7)은 선로 용량제약을 의미한다.

4.3.2. 조류추적법

조류추적의 개념은 발전단과 부하단 사이에 연결된 전력조류를 기반으로 개별 발전기와 부하 단에 대한 상관관계를 파악하는 것이다. 이는 개별 발전기들이 특정 부하에 얼마만큼을 기여하는지 파악을 할 수 있으므로 외란 발생 시 정전의 규모 및 피해를 예측할 수 있다.

조류추적법은 수많은 방법이 있지만, 본 논문에서는 Felix F. Wu 외 2명이 고안한 조류추적법을 적용하였다[9]. Wu의 조류추적법은 그래프이론을 기반으로 계통 토폴로지에 관한 논점을 해결하기에 적합하며 전력조류에서 발전단과 부하단의 사이의 기여도를 빠르고 효과적으로 계산할 수 있다.

4.4. 사례연구

4.4.1. 모의 전력시스템 모델링

본 연구의 모의 전력계통은 3개의 발전기와 3개의 부하모선으로 구성이 되어있다.

부하는 서로 다른 속성의 부하(상업용, 산업용, 주거용)이고, 선로용량은 100MW로 동일하다고 가정하였다. 기 가정을 <Fig. 3>과 같이 도식화하였다.

<Fig. 3>을 바탕으로 모의 스마트그리드를 모델링하면 <Fig. 4>와 같다.

<Fig. 4>에서 각 선로성분은 통신선로인 TCP, Serial로 구성되어있다. 다음으로 SCADA 1은 모선 1, RTU1은 모선 6으로써 산업지역을 총괄한다. 이와 같은 개념으로 각각의 SCADA와 RTU는 모의 전력계통에서 해당 모선 역할을 한다.

마지막으로 시뮬레이션을 위해 발전기의 용량 및 단가, 부하 용량을 가정하였다.

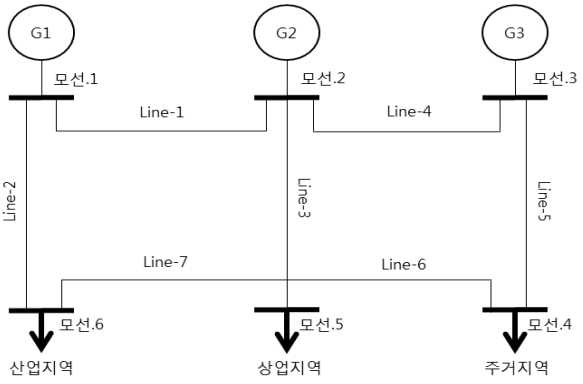


Fig. 3. 6모선 모의 전력계통

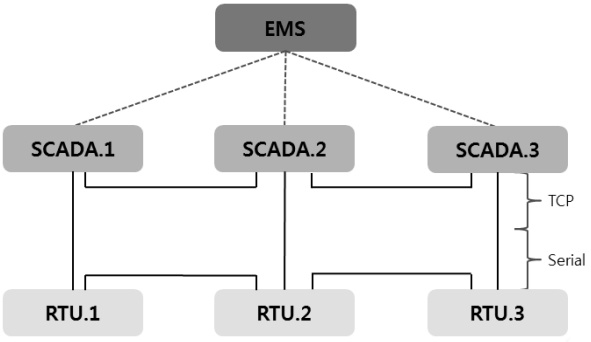


Fig. 4. 모의 스마트그리드 모델링

Table 6. 발전기의 용량 및 발전단가

	용량[MW]	발전단가[원/kW]
G1	100	8
G2	100	10
G3	100	15

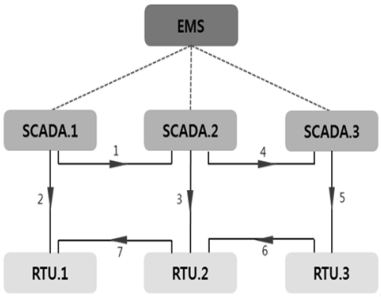
Table 7. 부하용량

	용량[MW]
주거지역	50
상업지역	80
산업지역	100

4.4.2. 사례연구 결과 및 분석

상기 모델링과 데이터를 바탕으로 산출된 최적조류계산 결과는 다음과 같다. <Fig. 5>에서 적색 화살표는 전력조류의 방향을 의미한다.

상기 최적조류계산의 결과를 기반으로 조류추적법을 이용하면 개별 발전기가 각 지역 별로 공급하는 전력량을 산출할 수 있으며 결과는 <Table 8>과 같다.



OPF	
	Net generation[MW]
G1	100
G2	100
G3	30
	Power Flow[MW]
1	6
2	94
3	82
4	24
5	54
6	4
7	6

Fig. 5. 최적조류계산 결과

Table 8. 조류추적법 결과

	주거지역	상업지역	산업지역
G1[MW]	1.257862	4.411292	94.33085
G2[MW]	20.96436	73.52152	5.514114
G3[MW]	27.77778	2.067183	0.155039

Table 9. 부하 속성별 기대정전비용(1시간)

	주거용	상업용	산업용
정전비용 [원/kW]	2,800	32,365	127,420

Table 10. 스마트그리드 구성요소 및 부하지역 별 정전비용[백만원]

	EMS	SCADA.1	SCADA.2	SCADA.3	RTU.1	RTU.2	RTU.3
	전체지역	산업지역	상업지역	주거지역	산업지역	상업지역	주거지역
정전비용	15,871	12,188	3,508	175	12,742	2,989	140
	L_TCP.1	L_TCP.2	L_TCP.3	L_TCP.4	L_TCP.5	L_TCP.6	L_TCP.7
	상업지역	산업지역	상업지역	주거지역	주거지역	상업지역	주거지역
정전비용	224	11,977	3,064	67	151	149	765
	L_Serial.1	L_Serial.2	L_Serial.3	L_Serial.4	L_Serial.5	L_Serial.6	L_Serial.7
	상업지역	산업지역	상업지역	주거지역	주거지역	상업지역	주거지역
정전비용	224	11,977	3,064	67	151	149	765

Table 11. 스마트그리드 네트워크 요소 별 위험(R) 산정 결과

	EMS	SCADA.1	SCADA.2	SCADA.3	RTU.1	RTU.2	RTU.3
위협(T)	0.29	0.29	0.29	0.29	0.58	0.58	0.58
취약성(V)	0.057	0.057	0.057	0.057	0.27	0.27	0.27
자산(A) [백만원]	15,871	12,188	3,508	175	12,742	2,989	140
위험(R)	266	204	59	3	2,055	482	23
위험률(%)	8.05	6.18	1.78	0.09	62.25	14.60	0.68
	L_TCP.1	L_TCP.2	L_TCP.3	L_TCP.4	L_TCP.5	L_TCP.6	L_TCP.7
위협(T)	0.16	0.16	0.16	0.16	0.16	0.16	0.16
취약성(V)	0.051	0.051	0.051	0.051	0.051	0.051	0.051
자산(A) [백만원]	224	11,977	3,064	67	151	149	765
위험(R)	2	95	24	0.53	1	1	6
위험률(%)	0.05	2.88	0.74	0.02	0.04	0.04	0.18
	L_Serial.1	L_Serial.2	L_Serial.3	L_Serial.4	L_Serial.5	L_Serial.6	L_Serial.7
위협(T)	0.09	0.09	0.09	0.09	0.09	0.09	0.09
취약성(V)	0.057	0.057	0.057	0.057	0.057	0.057	0.057
자산(A) [백만원]	224	11,977	3,064	67	151	149	765
위험(R)	1	59	15	0.33	1	1	4
위험률(%)	0.03	1.77	0.45	0.01	0.02	0.02	0.11

기대정전비용은 한국전기연구원의 선행연구를 참고했다[8]. 1시간 정전을 기준으로 각 부하 속성별 정의된 기대정전비용(Table 9)에서 각 지역별로 공급하는 전력량(Table 8)을 합산하면 결과는 다음과 같다.

<Table 10>에서 EMS는 통상적으로 전체 지역을 관리하므로 총 SCADA 서버의 정전비용으로 산출하였다. 또한 송전선로는 통신설비(TCP, Serial)로 구성된다고 가정하였으므로 통신설비 요소에 최적조류계산으로 산출된 전력조류 값을 합산하였다. <Table 10>은 사이버 공격에 의한 외란으로 모의계통에서 자산의 가치를 의미한다.

최종적으로 사이버 위협으로 인한 위험의 크기는 3장에서 정의한 식(1)을 적용하여 위협(T) × 취약성(V) × 자산(A)의 조합으로 산출하였다.

<Table 11>는 사례연구 데이터에 근거하여 최종적으로 산출된 위험의 화폐단위 결과이다. 상기 표를 분석하면 위험의 크기는 RTU가 가장 크게 나타났으며 그 중에서 산업지역의 RTU가 가장 위험함을 알 수 있다. 반면 EMS와 SCADA의 자산의 가치는 크지만 위협과 취약성의 정량화 수치가 낮으므로 위험 규모가 상대적으로 낮게 산출되었다. 물리적인 측면으로 해석하면, 사이버 위협이 발생할 경우 큰 피해가 발생되지만 위협에 노출될 가능성이 낮음을 의미한다. 통신 선로의 경우는 전력조류에 따라 위험정도가 상이함을 파악하였다.

5. 결 론

취약성을 개별적으로 확인하고 그에 대한 대책을 수립하는 것도 중요하지만, 일목요연하게 해당 취약성들을 정의하고 분류함으로써 전체 시스템 관리자 차원에서 적절한 보안자원과 예산을 배분하는 것도 매우 중요하다고 판단된다.

특히 다양한 계층과 시스템 구성요소가 존재하는 스마트그리드에 있어서 본 논문의 핵심 연구인 보안성 평가는 더욱 정성적 속성을 띄기 쉬운데, 정량적 틀을 통해 보안취약성을 체계적으로 정리하고 정량화함으로써 보다 효과적인 대책을 수립할 수 있다.

본 논문은 구체적으로 분석되고 인지되지 못한 스마트그리드 보안취약성을 명확하게 정의하고 분류함으로써 향후 보안대책과 솔루션을 개발할 수 있는 근거를 마련하는데 의의가 있다. 또한 기존 연구들이 이론적이고 방법론적인 측면에서 주로 접근이 이루어졌다면, 본 연구에서는 방법론과 더불어 구체적인 수치의 적용을 통해 현실에서 활용할 수 있는 측면에 무게를 두고 연구를 수행하였다. 향후연구로 실 계통에 본 논문의 정량화 방법론을 적용한다면 보다 유의미한 결과를 도출할 수 있을 것으로 판단된다.

감사의 글

이 논문은 2012년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2012R1A1A2007953)

Reference

1. 산업통산자원부, “스마트그리드 국가로드맵”, 2010
2. 한전 KDN, “송변전자동화시스템”, 2010
3. Lawrence Carin, George Cybenko, “Quantitative Evaluation of Risk for Investment Efficient Strategies in Cybersecurity, The QuERIES Methodology”, 2007
4. S. Massoud Amin, “Cyber and Critical Infrastructure Security - Toward Smarter and More Secure Power and Energy Infrastructures”, Canada-U.S. Workshop on Smart Grid Technologies at Vancouver, 2010
5. Matias Negrete-Pincetic, Felipe Yoshida, George Gross, “Towards Quantifying the Impacts of Cyber Attacks in the Competitive Electricity Market Environment”, 2009
6. Vulnerability Assessment, SANS Institute InfoSec Reading Room, http://www.sans.org/
7. 한국전력공사, 한국전기연구원, 서울대학교, “전기요금 수준별 적정 정전손해배상 범위설정 및 리스크 분산방안에 관한 연구”, 2011
8. Felix F.Wu, Yixin Ni, Ping Wei, “Power Transfer Allocation for Open Access Using Graph Theory-Fundamentals and Applications in Systems Withut Loopflow”, ieee transactions on power systems, VOL.15, NO.3, 2000
9. Chee-Wooi Ten and Chen-Ching Liu, "Vulnerability Assessment of Cybersecurity for SCADA Systems, IEEE Transactions on Power Systems", 2008