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.2013.23.3.445

전력 SCADA 시스템의 사이버 보안 위험 평가를 위한 정량적 방법론에 관한 연구

강 동 주,[1†] 이 종 주,[1] 이 영,[2] 이 임 섭,[3] 김 휘 강[4‡]
[1]한국전기연구원, [2]국방대학교, [3]한국전력거래소, [4]고려대학교

Quantitative Methodology to Assess Cyber Security Risks of SCADA system in Electric Power Industry

Dong-joo Kang,[1†] Jong-joo Lee,[1] Young Lee,[2] Im-sop Lee,[3] Huy-kang Kim[4‡]
[1]KERI, [2]KNDU, [3]KPX, [4]Korea University

요 약

본 논문은 제어시스템에서 사이버 위협과 취약성을 평가하기 위한 정량적 모델링에 관한 연구이다. SCADA (supervisory control and data acquisition) 시스템은 대표적인 제어시스템이고 전력계통에서 가장 큰 규모를 형성하고 있다. SCADA 시스템은 초기에는 지역적으로 고립된 시스템이었으나 통신 및 제어기술이 발전하면서 광역으로 확대되어 왔다. 스마트그리드는 에너지 시스템과 IT 시스템을 통합하는 것이며, 이러한 통합의 과정에서 IT 시스템 상에서 존재하던 위협이 제어시스템으로 옮겨오게 된다. 전력시스템은 실시간 특성이 강하게 요구되며, 이는 전력시스템의 사이버 위협을 IT 시스템에 비해 보다 복잡하고 치명적으로 만드는 요인이 된다. 예를 들어, 기밀성이 IT 시스템에서 가장 중요한 요소인데 반해 가용성은 제어시스템에서 가장 중요한 고려 사안이다. 이러한 맥락에서, 보다 체계적인 방식으로 전력시스템의 사이버 위험을 평가하는 과정이 요구된다. 일반적인 관점에서 위험이란, 위협, 취약성, 자산의 곱으로 산출되며 본 연구는 전력시스템 구성요소 별로 위험을 정량적으로 분석할 수 있는 프레임워크를 제안한다.

ABSTRACT

This paper is about the study to build a quantitative methodology to assess cyber threats and vulnerabilities on control systems. The SCADA system in power industry is one of the most representative and biggest control systems. The SCADA system was originally a local system but it has been extended to wide area as both ICT and power system technologies evolve. Smart Grid is a concept to integrate energy and IT systems, and therefore the existing cyber threats might be infectious to the power system in the integration process. Power system is operated on a real time basis and this could make the power system more vulnerable to the cyber threats. It is a unique characteristic of power systems different from ICT systems. For example, availability is the most critical factor while confidentiality is the one from the CIA triad of IT security. In this context, it is needed to reflect the different characteristics to assess cyber security risks in power systems. Generally, the risk(R) is defined as the multiplication of threat(T), vulnerability(V), and asset(A). This formula is also used for the quantification of the risk, and a conceptual methodology is proposed for the objective in this study.

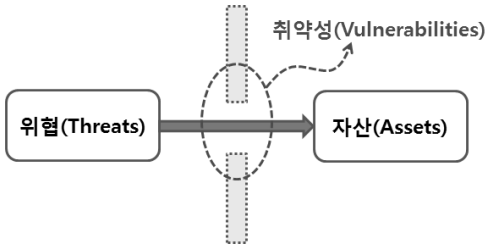
Keywords: SCADA, Smart Grid, Cyber Security, Quantitative Methodology, Risk, Threat, Vulnerability

접수일(2013년 2월 15일), 수정일(2013년 5월 20일), 게재확정일(2013년 5월 22일)

† 주저자, djkang@keri.re.kr
‡ 교신저자, cenda@korea.ac.kr(Corresponding author)

I. 서 론

보안 취약성(vulnerability)에 대한 SANS의 정의[1]에 따르면, 취약성이란 외부의 위협이 시스템에 유입될 수 있도록 하는 통로와 같고, 이러한 차원에서 보안상 문제점(security hole)이라고 생각할 수 있다. 이러한 취약성이 얼마나 존재하는가에 따라 해당 시스템의 위험 정도가 결정된다. [그림 1]은 이러한 개념을 도식화한 것으로 위협(threat)이 존재하더라도 취약성이 존재하지 않는다면 그 위협이 정보자산(information asset)에 영향을 미칠 수 없지만, 취약성으로 인해 외부의 위협이 정보자산에 영향을 미치게 된다. 따라서 취약성 평가란 이러한 약점들을 사전에 찾기 위한 일련의 과정이라고 볼 수 있다. 이러한 취약성들을 개별적으로 확인하고 그에 대한 대책을 수립하는 것도 중요하지만, 취약성을 발생가능성과 피해에 따라 사업영향평가(business impact analysis) 를 수행하여 전체 시스템 관리자 차원에서 적절한 보안자원과 예산을 배분하는 데 의사결정 지원을 할 수 있는 것 역시 중요한 작업 중 하나이다.



[그림 1] 취약성의 개념

특히, 다양한 계층과 시스템 구성요소가 존재하는 전력시스템이나 스마트그리드에 있어서 이러한 보안성 평가는 더욱 정성적 속성을 띄기 쉬운데 이와 같은 정량적 틀을 통해 보안취약성을 체계적으로 정리하고 정량화함으로써, 보다 효과적인 대책을 수립할 수 있다. 본 연구는 물리적으로 구분되는 개별 시스템 요소에 대한 보안평가 항목을 수립하고, 이를 정량화하는 방법론을 제공함으로써 보안관련 책임자의 대비책 수립 시 의사결정에 도움을 줄 수 있는 틀을 제공할 수 있도록 하였다.

II. 선행 연구

스마트그리드나 전력시스템에서 사이버 위협이나 취약성을 정량화하기 위한 일부 선행 연구들이 이루어져 왔다. 주로 Attack Graph를 통해 공격을 정의하고, 해당 공격 유형별로 발생 가능한 확률을 적용함으로써 위험성을 측정하려는 시도를 하였다.

Matias Negrete-Pincetic 등은 경쟁적 전력시장에서 사이버 공격에 의한 효과를 정량화하기 위한 연구를 수행하였는데, 아직까지 축적된 데이터베이스가 부족한 현실을 감안하여, 전력시스템의 설비 간 상대적 중요성과 피해정도, 공격용이성 등을 고려하여 순위를 매기는 형태로 위험의 정도를 정량화하였다[6].

Nian Liu 등은 Attack Graph와 MCDM을 이용하여 전력시스템에 대한 공격 루트를 규명하고 이에 대한 위험을 정량화하기 위한 연구를 수행하였다. 이를 통해 통상적인 확률론적 위험분석 관점에서 사이버 보안에 대한 분석 및 모델링을 수행하였다[11].

Pravin Chopade 등은 그래프 이론과 소셜 네트워크 이론을 전력 네트워크의 강인성을 분석하는데 적용하였으며, IEEE 118 모선을 구체적 사례로 도입하여 임의의 공격에 견딜 수 있는 내구성을 테스트하였다[12].

Deepa Kundur 등은 스마트그리드에 대한 사이버 공격 영향을 분석하고 표현할 수 있는 프레임워크를 제안하였다. 전력시스템은 전력계통과 통신 인프라의 결합이므로 이 둘의 관계를 그래프 이론을 통해 결합하였으며 인과관계에 기반하여 도식화하였다[13].

Jin Wei 등은 전력시스템에서의 주요 이슈 중에 하나인 안정도 문제를 다룸에 있어서, 사이버-물리 계층 구조를 적용하고, 시스템을 영역별로 분할하여 에이전트 개념을 적용함으로써 기존의 대형 문제를 분할하여 푸는 형태로 새로운 개념을 제시하였다. 에이전트 간에는 관계와 네트워크를 형성함으로 이러한 이론을 실제 통신 인프라로 구현함으로써 시스템 구성요소 간 상호작용이 보다 활발하도록 의도하였다. 현재 전력시스템에서의 운영관점 문제점에 소셜 네트워크 기반의 이론을 적용함으로써 새로운 관점에서 기존 문제의 해법을 제안하고 있다[14].

기타 국내 논문의 경우는 SCADA 통신의 통신 측면에서 암호화나 키교환 알고리즘을 중심으로 수행되고 있다[15],[16].

이와 같이 스마트그리드의 위험 정량화와 관련한 사이버 보안 연구는 순수한 사이버 보안 측면에서 잠재적 위협을 검토하는 측면, 사이버-물리 계층 간의 상호작용을 모델링하는 측면, 이러한 과정에서 그래프

이론을 이용하여 기존의 전력시스템 분석에 새로운 해석구조를 적용하는 측면 등으로 구분할 수 있다.

III. 분석 모델의 수립

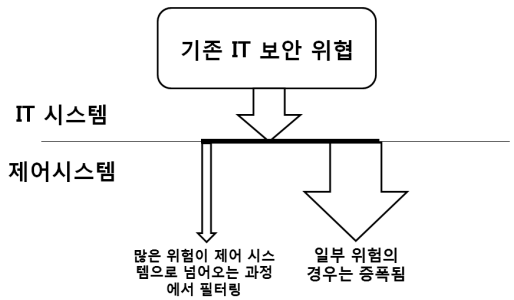
취약성 평가(vulnerability assessment)란 임의의 정보자산 상에서의 취약성을 규명하고, 정량화하고, 순위를 매기는 일련의 과정을 의미한다. 사이버 위협이나 취약성을 정의하고 분류하는 것은 매우 어려운 작업 중의 하나이다. 취약성 분석은 정보시스템, 에너지시스템, 상수도 시스템, 교통시스템 등 다양한 분야에 적용될 수 있다[2]. 재난관리 분야에 있어서 취약성 분석이란 잠재적 피해규모(피해인원 및 금액)를 평가하는 작업도 포함된다. 전력분야에서의 정전비용평가도 고장률과 피해비용 등을 동시에 고려하기 때문에 이러한 취약성 평가의 한 사례로 간주될 수 있다. 이러한 평가과정은 다양한 기관, 다양한 전문가들과 제조업자들에 의해 종종 동일한 취약성도 다른 이름으로 명명되고 중복적으로 기록될 수 있기 때문에 명확하게 정의하고 분류하기 어려운 측면이 존재한다. 일단 본 2장에서는 이러한 취약성을 평가하기 위한 여러 가지 인자(factor)들에 대해 우선적으로 정의하고, 이에 기반하여 3장에서 전체적인 이론적 틀을 구축하는 형태로 전개하기로 한다. [그림 1]에서 보듯이 취약성이란 위협과 정보자산 간의 관계를 정의하는 매개변수 내지 필터로 인식될 수 있다. 이러한 맥락에서, 위협, 취약성, 자산이 조합되어 실질적으로 발생 가능한 위험(Risk)이 정의된다. 위협(Threat)을 T, 취약성(Vulnerability)을 V, 자산(Asset)의 가치를 A로 표기하면, 위험(Risk)은 다음과 같이 정식화될 수 있다.

$$R = T \times V \times A \quad (1)$$

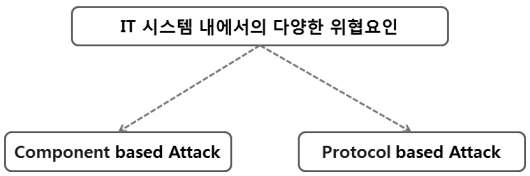
(1)식을 기본으로, 각 요소에 대해 상세히 정의함으로써 위험을 정량화할 수 있는 체계를 수립할 수 있다. 기존 IT 시스템에서의 취약성과 사이버 위협은 수십년간의 실제 사례를 통해 분석되어 왔다. 이중 일부는 제어시스템(control system)의 일종이라고 할 수 있는 전력시스템에도 그대로 적용될 것이고, 일부는 필터링 될 것이며, 또 다른 경우는 증폭될 수도 있을 것이다. 예를 들어, IT 시스템에서 약간의 통신지연은 허용되지만, 전력시스템에서의 통신지연은 제어작동 자체에 영향을 주면서 물리적 시스템의 붕괴(정전)로 이어질 수도 있다. 따라서, 우선 기존 IT 시스템에서의 보안위협을 분석하고, 전력시스템에 대한 적용 개연성에 대해 분석할 필요가 있다.

3.1 SCADA 시스템에서의 사이버 위협 분석

IT 시스템과 제어시스템은 프로토콜 상으로 확연히 구분되며, 프로토콜의 종류에 따라 영향을 줄 수 있는 위협도 달라지기 때문에 이에 근거하여 위협을 다르게 분석할 수 있다. 물리적으로 구분되는 컴포넌트 별로 공격이나 위협의 종류가 달라질 수 있고, 컴포넌트와 관계없이 사용 중인 프로토콜에 따라 존재하는 위협의 종류들이 존재한다. 컴포넌트는 개별 시스템에 대한 공격이고, 프로토콜은 네트워크를 대상으로 한 것으로 이해할 수 있다.



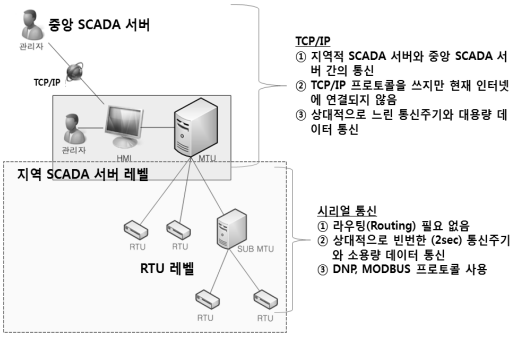
[그림 2] IT시스템과 제어시스템의 사이버 위협



[그림 3] 위협분류: 컴포넌트와 프로토콜 기반

따라서 상기의 2가지 공격 유형은 물리적 영역으로 볼 때는 [그림 3]와 같이 컴포넌트 기반의 공격은 개별 설비나 기기에 대한 공격이고, 프로토콜 기반 공격은 그러한 기기들을 연결하는 통신선로들에 대한 공격이다. SCADA 시스템의 경우도 지역(local) 시스템과 광역(global) 시스템으로 구분할 수 있는데, 2가지 시스템 영역은 TCP/IP 프로토콜과 시리얼(DNP, Modbus) 프로토콜 영역으로 구분된다.

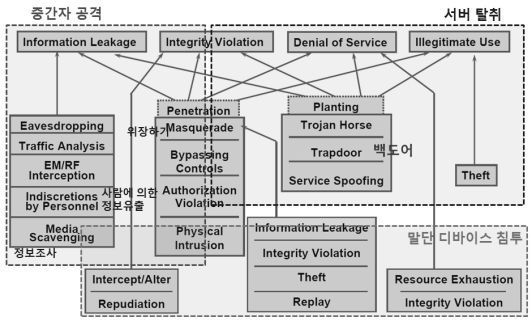
SCADA 시스템은 [그림 4]에서 보는 바와 같이



〔그림 4〕 SCADA 시스템의 구성

서버, 말단 기기, 중간의 통신 네트워크로 구성된다. 네트워크의 경우는 상부는 TCP/IP 프로토콜 기반의 시스템으로 구성되며, 하부단은 제어를 위한 시리얼 통신망으로 구성되어 있는 경우가 일반적이다. 이러한 SCADA 시스템의 기본구성을 기반으로 S. Massoud Amin이 2010년 3월 25일에 발표한 workshop 발표자료에 따르면, 기존 IT 시스템에서의 보안 위협은 〔그림 5〕와 같이 정의될 수 있다[3]. 상부 네트워크는 TCP/IP 기반이므로 기존 IT 시스템의 위협이 그대로 적용될 수 있고, 하부 네트워크는 시리얼 프로토콜이 가지는 고유 취약성에 의한 위험이 발생할 수 있다.

〔그림 5〕의 공격은 〔표 1〕에서 보는 바와 같이 SCADA 시스템의 세 부분(SCADA 서버, 통신 네트워크, RTU 및 단말기기)에 해당하는 공격으로 분류될 수 있다. 이러한 과정을 통해 기존 IT 위협요인들이 어떻게 SCADA 시스템에 적용되는지를 파악할 수 있다. SCADA 시스템은 크게 서버단과 RTU, 중간 통신 네트워크 부분의 3가지로 나누어져 있고, 이들 3가지 부분에 적용가능한 사이버 위협들을 분석함으로써 앞으로의 잠재적 위협요인을 진단해보는 형태로 접근한다. 이 중에는 실제 SCADA 시스템에 대한 적용이 부적절한 용어나 기법도 존재하지만, 〔표 1〕과 같이 1차적으로 정리한 다음 재정리하는 형태를 취하기로 한다.



〔그림 5〕 IT 시스템에서의 사이버 위협[3]

〔표 1〕 시스템 구성요소와 사이버 위협들

위협의 종류 \ 시스템 구성		SCADA 서버	통신 네트워크		RTU 및 말단기기
			TCP/IP	시리얼 (Serial)	
정보유출 (기밀성)	(1) Eavesdropping	V(01,01)	V(01,02)	V(01,03)	V(01,04)
	(2) Traffic Analysis	V(02,01)	V(02,02)	V(02,03)	V(02,04)
	(3) EM/RF Interception	V(03,01)	V(03,02)	V(03,03)	V(03,04)
	(4) Indiscretions by Personnel	V(04,01)	V(04,02)	V(04,03)	V(04,04)
	(5) Media Scavenging	V(05,01)	V(05,02)	V(05,03)	V(05,04)
	(6) Trojan Horse	V(06,01)	V(06,02)	V(06,03)	V(06,04)
	(7) Trapdoor (Backdoor)	V(07,01)	V(07,02)	V(07,03)	V(07,04)
	(8) Service Spoofing	V(08,01)	V(08,02)	V(08,03)	V(08,04)
정보의 무결성 훼손	(9) Masquerade	V(09,01)	V(09,02)	V(09,03)	V(09,04)
	(10) Bypassing Controls	V(10,01)	V(10,02)	V(10,03)	V(10,04)
	(11) Authorization Violations	V(11,01)	V(11,02)	V(11,03)	V(11,04)
	(12) Physical Intrusion	V(12,01)	V(12,02)	V(12,03)	V(12,04)
	(13) Replay	V(13,01)	V(13,02)	V(13,03)	V(13,04)
	(14) Theft & Illegitimate Use	V(14,01)	V(14,02)	V(14,03)	V(14,04)
자원의 가용성	(15) Denial of Service	V(15,01)	V(15,02)	V(15,03)	V(15,04)

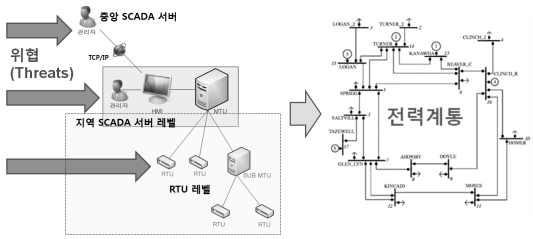
*용어설명: Eavesdropping: 감청, Traffic Analysis: 통신 데이터 패킷 분석, EM/RF Interception: 무선데이터패킷 가로채기, Indiscretions by Personnel: 사람의 실수로 인한 정보 유출, Media Scavenging: 정보매체 조사를 통해 해킹에 필요한 정보수집, Trojan Horse: 트로이 목마, Trapdoor (Backdoor): 백도어, Service Spoofing: 가짜 서비스를 통한 속이기, Masquerade: 위장하기, Bypassing Controls: 우회 조작, Authorization Violations: 허가 침해, Physical Intrusion: 물리적 침해, Replay: 재생공격, Theft & Illegitimate Use: 불법적 도용, Denial of Service: 서비스 지연공격

3.2 취약성 분석

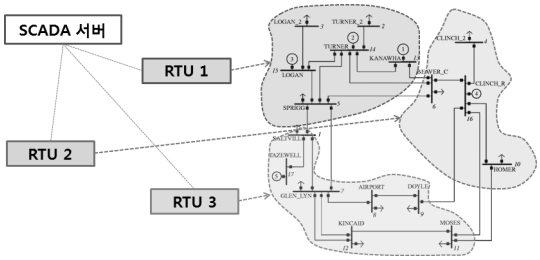
〔그림 5〕에서 규명된 사이버 위협들은 취약성에 의해 선별적으로 SCADA 시스템의 위험에 영향을 미치기 된다. 〔표 1〕에서 색칠된 부분은 해당 취약성에 의하여 실질적인 위험이 발생하는 부분에 대한 영역을 표현한 것이다. 색칠이 되지 않은 부분은 공격의 가능성이 없다는 의미이므로 정량적인 수치상으로는 0으로 표시되고, 음영으로 표시된 부분에 대해서는 통계치에 의한 실제 발생할 확률이나 추정치가 적용된다. 여기서의 취약성이란 위협이 정보자산에 대해 현실화되는 확률 개념으로 생각할 수 있으므로 $0 \leqq V \leqq 1$의 값을 가지게 된다.

3.3 정보자산 분석

정보자산의 가치를 평가하는 문제도 어려운 문제 중의 하나이다. IT시스템에서의 자산이란 네트워크 장비를 포함한 하드웨어 등의 유형자산과 소프트웨어, 지식정보 등의 무형 자산 등을 통칭한다. 모든 자산은 적절한 보호를 위하여 소유자와 책임 소재가 명확히 지정되어 있어야 하는데, 이와 같은 과정을 통하여 자산의 책임 추적성을 보장받을 수 있을 뿐만 아니라 정보자산 또한 적절히 보호받고 있는지도 알 수 있다〔4〕. 정보자산이 일단 시스템의 일부분이 되면 그 가치는 해당 기기나 설비의 구매가격 혹은 감가 상각된 경제적 가치만을 의미하는 것이 아니라, 그러한 정보자산의 보안성이 훼손됨으로써 발생할 수 있는 2차적인 피해비용도 고려되어야 한다. 특히, SCADA 시스템의 경우는 이러한 정보자산이 이웃한 정보자산 뿐 아니라, 전력계통과도 연계되어 있기 때문에 문제가 훨씬 복잡해진다. 따라서 전력시스템에서 자산의 가치는 해당 IT 설비가 공격당했을 때의 기대정전비용(expected interruption cost)으로 수렴한다. 정전비용은 다양한 정전비용 관련 연구를 통해 산출된



〔그림 6〕 SCADA 시스템의 위협과 전력계통 정전의 상관관계



〔그림 7〕 개별 RTU와 전력계통 지역 간 상관관계

결과를 적용하는 것으로 한다. 〔그림 6〕의 개념에 근거하여 지역별 RTU와 전력계통 모선 혹은 지역별 상관관계 개념을 도식화하면 〔그림 7〕과 같다.

개별 RTU에 대한 공격은 1차적으로 해당 지역에 대한 신뢰도를 떨어뜨리게 되며, 이러한 외란이 적절하게 진정되지 않을 경우 전체계통으로 확산될 우려가 있다.

3.4 위험 계산의 정식화

상기 절에서 정의된 위협(T), 취약성(V), 자산(A)의 정의에 따라 위험(R)은 (2)식으로 정식화된다. T_{ij}라는 표기에서 행렬의 행(row)을 의미하는 j ($j=1,2,3,4$)는 〔표 1〕에서 정의된 15가지 위협의 유형을 의미하고, 행렬의 열(column)을 의미하는 ()는 역시 〔표 1〕에서 정의된 SCADA 시스템의 구성요소, SCADA 서버, TCP/IP 네트워크, 시리얼 네트워크, RTU 및 말단기기 부분을 가리키는 것이다.

(2)식 위협(T) 행렬과 취약성(V) 행렬을 계산하면 다음의 식 (3)과 같이 정리된다. 여기서 는 〔표 1〕의 행이 가리키는 15가지 타입의 공격 유형을 가리킨다. 그리고, 아래첨자 01, 02, 03, 04는 〔표 1〕의 열에서 정의된 전력 SCADA 시스템의 4가지 구성요소인 SCADA 서버, TCP/IP 네트워크, 시리얼 네트워크, RTU 및 말단기기 부분을 가리킨다. 식 (3) 4×4 행렬에서 비대각 성분이 의미하는 것은 다른 부분간의 위협 상관관계를 의미하는 것으로, 예를 들어 SCADA 서버를 공격했는데, 통신 네트워크나 RTU가 고장날 확률을 의미한다. 물론 서버를 장악하면 통신 네트워크나 말단기기에 오염된 정보 혹은 잘못된 신호를 줄 수는 있겠지만, 본 논문에서는 직접적인 공격에 의한 고장만을 고려하여 2차적이고 간접적인 상관관계에 의한 피해는 없는 것으로 보고 비대각 성분(시스템 요소 간 correlation)은 0으로 설정한다.

$$\begin{bmatrix} R_1 \\ R_2 \\ R_3 \\ R_4 \end{bmatrix} = \begin{bmatrix} T_{0101}\ T_{0201}\ T_{0301} \cdots T_{1001}\ T_{1101}\ T_{1201}\ T_{1301}\ T_{1401}\ T_{01501} \\ T_{0102}\ T_{0202}\ T_{0302} \cdots T_{1002}\ T_{1102}\ T_{1202}\ T_{1302}\ T_{1402}\ T_{1802} \\ T_{0103}\ T_{0203}\ T_{0303} \cdots T_{1003}\ T_{1103}\ T_{1203}\ T_{1303}\ T_{1403}\ T_{1803} \\ T_{0104}\ T_{0204}\ T_{0304} \cdots T_{1004}\ T_{1104}\ T_{1204}\ T_{1304}\ T_{1404}\ T_{1804} \end{bmatrix} \begin{bmatrix} V_{0101}\ V_{0102}\ V_{0103}\ V_{0104} \\ V_{0201}\ V_{0202}\ V_{0203}\ V_{0204} \\ V_{0301}\ V_{0302}\ V_{0303}\ V_{0304} \\ V_{0401}\ V_{0402}\ V_{0403}\ V_{0404} \\ V_{0501}\ V_{0502}\ V_{0503}\ V_{0504} \\ V_{0601}\ V_{0602}\ V_{0603}\ V_{0604} \\ V_{0701}\ V_{0702}\ V_{0703}\ V_{0704} \\ V_{0801}\ V_{0802}\ V_{0803}\ V_{0804} \\ V_{0901}\ V_{0902}\ V_{0903}\ V_{0904} \\ V_{1001}\ V_{1002}\ V_{1003}\ V_{1004} \\ V_{1101}\ V_{1102}\ V_{1103}\ V_{1104} \\ V_{1201}\ V_{1202}\ V_{1203}\ V_{1204} \\ V_{1301}\ V_{1302}\ V_{1303}\ V_{1304} \\ V_{1401}\ V_{1402}\ V_{1403}\ V_{1404} \\ V_{1601}\ V_{1602}\ V_{1603}\ V_{1604} \end{bmatrix} \begin{bmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \end{bmatrix} \quad (2)$$

$$\begin{bmatrix} R_1 \\ R_2 \\ R_3 \\ R_4 \end{bmatrix} = \begin{bmatrix} \sum_{i=1}^{15} T_{i01} V_{i01} & \sum_{i=1}^{15} T_{i01} V_{i02} & \sum_{i=1}^{15} T_{i01} V_{i03} & \sum_{i=1}^{15} T_{i01} V_{i04} \\ \sum_{i=1}^{15} T_{i02} V_{i01} & \sum_{i=1}^{15} T_{i02} V_{i02} & \sum_{i=1}^{15} T_{i02} V_{i03} & \sum_{i=1}^{15} T_{i02} V_{i04} \\ \sum_{i=1}^{15} T_{i03} V_{i01} & \sum_{i=1}^{15} T_{i03} V_{i02} & \sum_{i=1}^{15} T_{i03} V_{i03} & \sum_{i=1}^{15} T_{i03} V_{i04} \\ \sum_{i=1}^{15} T_{i04} V_{i01} & \sum_{i=1}^{15} T_{i04} V_{i02} & \sum_{i=1}^{15} T_{i04} V_{i03} & \sum_{i=1}^{15} T_{i04} V_{i04} \end{bmatrix} \begin{bmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \end{bmatrix} \quad (3)$$

서로 다른 시스템 요소 간의 위협 상관관계를 0으로 보면, 식 (3)은 다음의 식 (4)와 같은 형태로 정리될 수 있다.

$$\begin{bmatrix} R_1 \\ R_2 \\ R_3 \\ R_4 \end{bmatrix} = \begin{bmatrix} \sum_{i=1}^{15} T_{i01} V_{i01} & 0 & 0 & 0 \\ 0 & \sum_{i=1}^{15} T_{i02} V_{i02} & 0 & 0 \\ 0 & 0 & \sum_{i=1}^{15} T_{i03} V_{i03} & 0 \\ 0 & 0 & 0 & \sum_{i=1}^{15} T_{i04} V_{i04} \end{bmatrix} \begin{bmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \end{bmatrix} \quad (4)$$

(4)의 식을 시스템 요소별로 유효한 위협성분에 한해서 풀어서 정식화를 하면 다음 식 (5)~(8)과 같다.

$$R_1 = A_1(T_{0101}V_{0101} + T_{0401}V_{0401} + T_{0501}V_{0501} + T_{0601}V_{0601} + T_{0701}V_{0701} + T_{0801}V_{0801} + T_{1101}V_{1101} + T_{1201}V_{1201} + T_{1401}V_{1401}) \quad (5)$$

$$R_2 = A_2(T_{0102}V_{0102} + T_{0202}V_{0202} + T_{1202}V_{1202} + T_{1402}V_{1402}) \quad (6)$$

$$R_3 = A_3(T_{0103}V_{0103} + T_{0203}V_{0203} + T_{1203}V_{1203}) \quad (7)$$

$$R_4 = A_4(T_{0104}V_{0104} + T_{0304}V_{0304} + T_{0604}V_{0604} + T_{0704}V_{0704} + T_{0804}V_{0804} + T_{0904}V_{0904} + T_{1004}V_{1004} + T_{1104}V_{1104} + T_{1204}V_{1204} + T_{1301}V_{1301}) + T_{1501}V_{1501}) \quad (8)$$

여기서, A_4는 n개의 RTU에 대한 자산 가치이므로, 이를 수식으로 표현하면 다음과 같고, 모든 RTU의 속성이 같다고 가정하면, 식 (9)를 (8)식에 대입하면 된다.

$$A_4 = A_4^1 + A_4^2 + A_4^3 + \ldots + A_4^k \quad (9)$$

정보자산 A_n^k의 가치는 통신설비의 소실가치(lost value), $LV_n^k(C)$와 해당 설비가 위협에 노출되었을 때 발생할 수 있는 기대 정전비용(outage cost), $OC_n^k(P)$로 표현 가능하다. 여기서, C는 통신설비(communication infrastructure), P는 전력계통(power system)을 의미한다. 이러한 개념에 근거하여 정보자산의 가치를 일반적으로 정식화하면 다음과 같다.

$$A_n = \sum_{k=1}^{p} (LV_n^k + OC_n^k) \quad (10)$$

(9)식이 의미하는 바는 SCADA 시스템의 n번째 통신설비가 정보자산(A_n)으로서 가치(사고가 발생했을 경우의 피해비용)는 정보자산 자체의 소실가치(lost value) LV_n과, 정보자산이 소실됨으로써 발생하는 정전비용 OC_n을 합산한 것이다. 여기서 k는 n번째 자산의 하위 구성성분으로써 n번째 자산이 여러 하위요소로 구성되어 있을 때를 일반적으로 표현하기 위함이다. 〔그림 7〕의 예를 든다면, 말단 RTU 단이 3개의 RTU로 구성되어 있을 때 $k=3$으로 생각할 수 있다.

IV. 정량적 데이터의 산정

보안과 관련한 중요개념인 위협과 취약성은 모두 정성적 개념들이다. 따라서 정량적 모델 수립에 있어서 중요한 것은 이들 속성들의 정량적인 값을 산출하는 것이다. 그러나 타 분야하고는 달리 보안은 분야의 특성상 데이터 공개가 잘 되지 않고, 워낙 다양한 속성의 위협과 맥락이 존재하기 때문에 분류나 정량화의 작업이 매우 어렵다. Burris 등은 보안사고의 발생을 정량적으로 모델링하기 힘든 것이 보안사고의 발생이 반드시 보안강도에 반비례하는 것이 아니기 때문이라고 하였다. 이는 보안강도가 낮은 시스템에서도 보안사고가 발생하지 않을 수 있으며, 반대로 보안강도가 강한 시스템에서 보안사고가 발생할 수도 있는데 이는 보안사고에서 운(luck)이 중요한 역할을 하기 때문이라고 주장하고 있다[5]. 따라서 본 연구에서는 기존의 다양한 연구결과들을 참조하여 본 논문에서 정의한 15가지의 위협과 4개 부문에 대한 취약성에 대한 정량적 수치를 도출하고자 하였다.

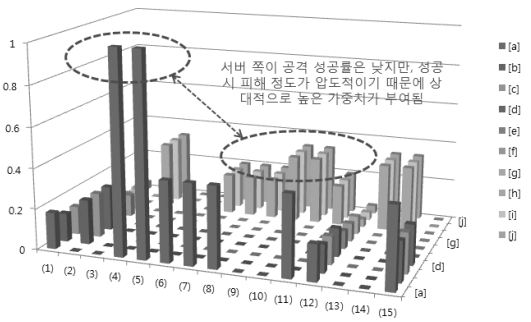
4.1 위협 수준의 정량화

사이버 보안사고가 현재 어떻게 발생하는지에 대한 정보는 정확히 알기 어렵고 보안위협이라는 것이 지속적으로 진화하고 새로운 위협요인이 등장하기 때문에, 정량적인 수치측면에 객관화된 값을 얻기는 힘든 측면이 있다. 또한 보안위협과 실제 취약성은 되도록 공개되지 않는 것이 일반적이고, 그에 따라 참조할만한 수치가 존재하지 않는다. 따라서 15개의 위협요인(T)에 대한 상대적인 잠재피해정도와 취약성(V)에 대한 순위를 매겨 잠재적인 취약성에 대한 척도를 산정한다. Matias Negrete-Pincetic 등은 전력시장에서 사이버 위협(공격)의 영향(impact)을 정량화하기 위한 연구를 수행하였는데, 해당 연구에서 4가지 공격의 유형의 난이도와 영향을 비교하였다. 4가지 공격의 유형은 서비스지연공격(DoS: Denial of Service), 재생공격(replay), 중간자 공격(man-in-the-middle attack), RTU 제어권 취득(reprogramming RTUs)이다. 난이도는 발생빈도(가능성)와 반비례 관계를 가지므로, 발생빈도 측면에서 '서비스지연공격 〉 재생공격 〉 중간자공격 〉 RTU제어권취득'의 순으로 정리할 수 있다[6]. 그 이외 다양한 연구에서 이러한 사이버 위협에 대한 정량화를 시도하였는데, 과거의 경험이나 난이도에 근거하여 주관적인 가중치나 점수를 매기는 형태로 비교되었는데, Burris[7]의 연구결과와 유사하게 가용성 측면에서의 공격이 내부 정보나 인증의 과정이 필요 없기 때문에 가장 쉬웠으며 그 다음이 기밀성이고, 가장 어려운 것이 무결성으로 조사되었다. 무결성의 경우는 데이터 손실과 같은 우발적인 피해 및 의도적인 조작의 가능성이 모두 존재하지만, 의도적인 조작의 측면에서만 본다면 기밀성을 보호하기 위한 보호조치(safeguard)를 우회해야 조작이 가능하기 때문이다. 제어시스템 상에서 위협요인에 대한 상대적인 피해정도(혹은 중요성)를 비교해보면 AIC 즉, 가용성(availability), 무결성(integrity), 기밀성(confidentiality)의 순으로 나열될 수 있고, 공격성공 난이도의 측면에서 본다면 무결성(I), 기밀성(C), 가용성(A)의 순으로 볼 수 있다. 위협에 대한 정량적 수치는 2가지 축에 대한 상대적인 순위를 매기는 형태로 산정한다. 일단, 가로축(열) SCADA 영역별(SCADA 서버, TCP/IP 구간, 시리얼 통신 구간, RTU 구간별로 잠재적 피해규모에 따라 4, 3, 2, 1의 가중치를 부여한다. 즉, 서버가 위협에 뚫렸을 때 그 잠재적 피해가 가장 크기 때문에 가장 높은 4를 부여하였고, RTU의 경우는 최하위 말단이므로 상대적으로 가장 낮은 순위인 1을 부여하였다. 0인 부분은 표 1에 따라, 개별 위협에 대해 SCADA 구성부문별로 해당사항이 없는 부분을 가리킨다. 모든 위협이 유효할 때(0인 부분이 없을 때)는 4, 3, 2, 1이 모두 부여되지만, 0인 부분이 있을 때는 해당 부분이 제외되고 순위가 매겨진다. 이러한 방법은 AHP (Analytic Hie-

〔표 2〕 구성요소(가로축) 별 중요도(잠재피해영향)에 따른 순위: 내림차순

	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)
	SCADA 서버	L_1^{TCP}	L_2^{TCP}	L_3^{TCP}	L_1^{Serial}	L_2^{Serial}	L_3^{Serial}	RTU1	RTU2	RTU3
(1)Eavesdropping	4	3	3	3	3	2	2	1	1	1
(2)Traffic Analysis	0	2	2	2	1	1	1	0	0	0
(3)EM/RF Interception	0	0	0	0	0	0	0	1	1	1
(4)Indiscretions by Personnel	1	0	0	0	0	0	0	0	0	0
(5)Media Scavenging	1	0	0	0	0	0	0	0	0	0
(6)Trojan Horse	2	0	0	0	0	0	0	1	1	1
(7)Trapdoor (Backdoor)	2	0	0	0	0	0	0	1	1	1
(8)Service Spoofing	2	0	0	0	0	0	0	1	1	1
(9)Masquerade	0	0	0	0	0	0	0	1	1	1
(10)Bypassing Controls	0	0	0	0	0	0	0	1	1	1
(11)Authorization Violations	2	0	0	0	0	0	0	1	1	1
(12)Physical Intrusion	4	3	3	3	2	2	2	1	1	1
(13)Replay	0	0	0	0	0	0	0	1	1	1
(14)Theft & Illegitimate Use	0	0	0	0	0	0	0	1	1	1
(15)Denial of Service	2	1	1	1	0	0	0	0	0	0

rarchy Process)[7]에서 비교대상 별 정량적 수치가 없을 때 대상 사이의 상대적 비교를 통해 수치를 산정하는 방법에서 부분적으로 차용한 것이다[8]. [그림 8]은 [표 2]를 정규화한 결과이다.



[그림 8] 구성요소(가로축) 별 중요도(잠재피해영향)에 따른 가중치 부여: 정규화

여기서 정규화의 의미란 개별 위협이 존재(공격 가능성)하고, 그 크기가 1이라고 가정했을 때 SCADA 시스템의 개별 요소들이 그러한 위험을 나누어가지는 의미이다. 즉, 서비스지연(DoS) 공격이 1회 이루어질 때 SCADA 시스템은 그러한 공격이 유효한 서버와 TCP/IP 구간에서 그러한 위협의 정도를 나누어 가지게 된다. 유사하게 해당 공격이 2회 이루어질 때, 그러한 위협은 2배가 되는 방식이다. 공격의 빈도에 대한 적용 크기는 국가나 지역별, 시스템별 과거실적 데이터에 근거하여 이루어질 수 있기 때문에 본 연구에서는 정규화한 값으로 가정한다. 유사한 방식으로 위협의 종류별(세로축)에 대해서도 취약한 정도에 따라 상대적인 순위를 부여할 수 있다.

세로축의 위협에 대해서는 기밀성, (기밀성+무결성) 혼재, 무결성, 가용성의 4가지 영역으로 구분하고 각 영역에 대해서는 동일한 순위를 부여한다. 상기에서 기술한 바와 같이 제어시스템 상에서는 가용성(A), 무결성(I), 기밀성(C)의 순으로 중요하기 때문에 해당 사항이 없는 경우는 0로 표현하고, 기타 [표 3]과 같이 정리된다. 그리고 [표 4]의 결과를 정규화하면 [표 4]와 같다. 임의의 사이버 위협이 존재하고

$$T = D_T \times I_T = \begin{bmatrix} 0.18 & 0.14 & 0.14 & 0.14 & 0.09 & 0.09 & 0.09 & 0.04 & 0.04 & 0.04 \\ 0 & 0.22 & 0.22 & 0.22 & 0.11 & 0.11 & 0.11 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.33 & 0.33 & 0.33 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.4 & 0 & 0 & 0 & 0 & 0 & 0 & 0.2 & 0.2 & 0.2 \\ 0.4 & 0 & 0 & 0 & 0 & 0 & 0 & 0.2 & 0.2 & 0.2 \\ 0.4 & 0 & 0 & 0 & 0 & 0 & 0 & 0.2 & 0.2 & 0.2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.33 & 0.33 & 0.33 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.33 & 0.33 & 0.33 \\ 0.4 & 0 & 0 & 0 & 0 & 0 & 0 & 0.2 & 0.2 & 0.2 \\ 0.18 & 0.14 & 0.14 & 0.14 & 0.09 & 0.09 & 0.09 & 0.04 & 0.04 & 0.04 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.33 & 0.33 & 0.33 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.33 & 0.33 & 0.33 \\ 0.4 & 0.2 & 0.2 & 0.2 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \bullet \begin{bmatrix} 0.04 & 0.13 & 0.13 & 0.13 & 0.2 & 0.2 & 0.2 & 0.04 & 0.04 & 0.04 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.04 & 0.04 & 0.04 \\ 0.04 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.04 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.08 & 0 & 0 & 0 & 0 & 0 & 0 & 0.08 & 0.08 & 0.08 \\ 0.08 & 0 & 0 & 0 & 0 & 0 & 0 & 0.08 & 0.08 & 0.08 \\ 0.08 & 0 & 0 & 0 & 0 & 0 & 0 & 0.08 & 0.08 & 0.08 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.11 & 0.11 & 0.11 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.11 & 0.11 & 0.11 \\ 0.12 & 0.25 & 0.25 & 0.25 & 0.4 & 0.4 & 0.4 & 0.11 & 0.11 & 0.11 \\ 0.12 & 0.25 & 0.25 & 0.25 & 0.4 & 0.4 & 0.4 & 0.11 & 0.11 & 0.11 \\ 0.12 & 0 & 0 & 0 & 0 & 0 & 0 & 0.11 & 0.11 & 0.11 \\ 0.12 & 0 & 0 & 0 & 0 & 0 & 0 & 0.11 & 0.11 & 0.11 \\ 0.16 & 0.37 & 0.37 & 0.37 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (11)$$

[표 3] 위협의 종류(세로축) 별 위험도에 따른 순위: 내림차순

	SCADA 서버	L_1^{TCP}	L_2^{TCP}	L_3^{TCP}	L_1^{Serial}	L_2^{Serial}	L_3^{Serial}	RTU1	RTU2	RTU3
Eavesdropping	1	1	1	1	1	1	1	1	1	1
Traffic Analysis	0	0	0	0	0	0	0	0	0	0
EM/RF Interception	0	0	0	0	0	0	0	1	1	1
Indiscretions by Personnel	1	0	0	0	0	0	0	0	0	0
Media Scavenging	1	0	0	0	0	0	0	0	0	0
Trojan Horse	2	0	0	0	0	0	0	2	2	2
Trapdoor (Backdoor)	2	0	0	0	0	0	0	2	2	2
Service Spoofing	2	0	0	0	0	0	0	2	2	2
Masquerade	0	0	0	0	0	0	0	3	3	3
Bypassing Controls	0	0	0	0	0	0	0	3	3	3
Authorization Violations	3	2	2	2	2	2	2	3	3	3
Physical Intrusion	3	2	2	2	2	2	2	3	3	3
Replay	3	0	0	0	0	0	0	3	3	3
Theft & Illegitimate Use	3	0	0	0	0	0	0	3	3	3
Denial of Service	4	3	3	3	0	0	0	0	0	0

그로 인한 위험수준이 1이라고 할 때, 개별 위험이 가질 위험의 수준에 대한 의미라고 해석할 수 있다. 즉, 특정 위협이 정해지면, 〔표 2〕의 값을 그대로 적용하면 되지만 어떤 위협인지 명확하게 구분되지 않는 미래상황을 상정할 때 각 위협 종류들에 대한 일종의 분포함수를 구성하는 것이다. 그러한 개별 위협이 발생할 확률이 동일하다고 가정했을 때 해당 위험이 발생했을 때 전력시스템에 영향을 미치는 위험도의 크기라고 해석할 수 있다.

〔표 2〕의 시스템 구성요소 별 위협에 대한 중요도(잠재피해영향)를 I_T(impact or importance), 〔표 4〕의 위협 종류 별 위험도를 D_T(Danger of threats)라고 표기하면 최종적인 위협(T)에 대한 행렬식은 D_T와 I_T의 행렬요소 간 곱(dot product)으로 (11)과 같이 정식화되고, 〔표 5〕와 같은 결과를 도출한다. 〔표 5〕은 임의의 사이버 위협이 1회 발생한다고 가정했을 때, 각 위협별, 시스템 구성성분별로 분담하게 되는 위협의 수준을 의미한다.

4.2 취약성 수준의 정량화

위협의 수준과 더불어, 그 위협이 실현되는 여부는 시스템의 취약성과 관련이 있다. 즉, 위협이라는 변수가 외생변수(外生變數, exogenous variable)라면 취약성은 보안에 대한 투자에 따라 높아지거나 낮아질 수 있는 내생변수(內生變數, endogenous variable)라고 볼 수 있다. 취약성은 〔그림 1〕에서 보듯이 일종의 필터라고 볼 수 있기 때문에 위협을 완전히 통과시킬 경우는 1, 그리고 점차 낮아져서 하나도 통과시키지 않을 때는 0으로 볼 수 있으므로 $0 \leqq V \leqq 1$의 값을 가진다고 볼 수 있다. 취약성의 경우도 절대적으로 정의될 수 없기 때문에 몇 가지 가정이 도입된다. 먼저, 과거의 데이터가 부재할 경우 가장 간단하게 생각할 수 있는 확률은 0.5(50%)이다. 즉, 위협이 존재할 경우 그 위협이 취약성을 통해 정보자산으로 침투할 수 있느냐 없느냐의 문제로 생각할 수 있다. 단 보안강도에 있어서 서버, 통신선로, RTU 단이 서로 다르므로 여기에 위협의 경우와 같이 상대적 순위를 매기고 50%의 취약성을 적용하기로 한다. 보안의 강도는 서버가 가장 강하고 하위로 내려갈수록 작다고 생각할 수 있으므로 SCADA 서버, TCP/IP 구간, 시리얼 구간, RTU의 수준으로 생각할 수 있다. 보안강도에 있어서는 일반적인 관점에서 골고루 적용된다고 가정하고 위협별로는 차등을 두지 않았다. 이와 같이 적용하여 〔표 6〕과 같은 결과를 산출하였다.

사례연구를 위해 3모선의 간단한 모의계통을 〔그림 9〕와 같이 상정한다. 모선 1과 2에 발전기가 연계되어 있고, 각 모선은 상업용, 산업용, 주거용으로 서로 다른 속성의 부하를 가진다. 전력계통의 모선 1, 2, 3은 각각 SCADA 시스템의 RTU1, RTU2, RTU3에 연결되어 있다고 가정한다. RTU가 사이버 위협요인에 노출되어 피해를 입으면 개별 RTU에 대응하는 전력계통의 모선들에 정전이 발생할 확률이 상승하게 된다. SCADA 서버가 공격을 받을 경우는 그 영향이 모든 지역과 모선에 영향을 미치고 전체 시스템에 대한 영향을 미치게 된다. SCADA 서버와 RTU1,

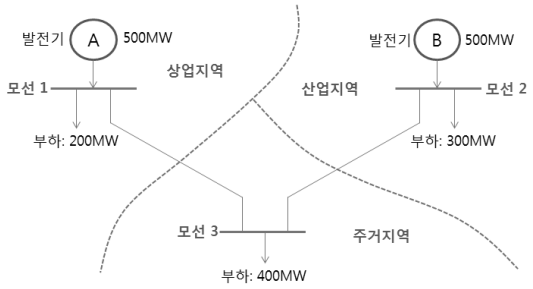
〔표 4〕 위협의 종류(세로축) 별 위험도에 따른 순위: 내림차순

	SCADA 서버	L_1^{TCP}	L_2^{TCP}	L_3^{TCP}	L_1^{Serial}	L_2^{Serial}	L_3^{Serial}	RTU1	RTU2	RTU3
Eavesdropping	1	1	1	1	1	1	1	1	1	1
Traffic Analysis	0	0	0	0	0	0	0	0	0	0
EM/RF Interception	0	0	0	0	0	0	0	1	1	1
Indiscretions by Personnel	1	0	0	0	0	0	0	0	0	0
Media Scavenging	1	0	0	0	0	0	0	0	0	0
Trojan Horse	2	0	0	0	0	0	0	2	2	2
Trapdoor (Backdoor)	2	0	0	0	0	0	0	2	2	2
Service Spoofing	2	0	0	0	0	0	0	2	2	2
Masquerade	0	0	0	0	0	0	0	3	3	3
Bypassing Controls	0	0	0	0	0	0	0	3	3	3
Authorization Violations	3	2	2	2	2	2	2	3	3	3
Physical Intrusion	3	2	2	2	2	2	2	3	3	3
Replay	3	0	0	0	0	0	0	3	3	3
Theft & Illegitimate Use	3	0	0	0	0	0	0	3	3	3
Denial of Service	4	3	3	3	0	0	0	0	0	0

〔표 5〕 위협 수준의 정량화 결과

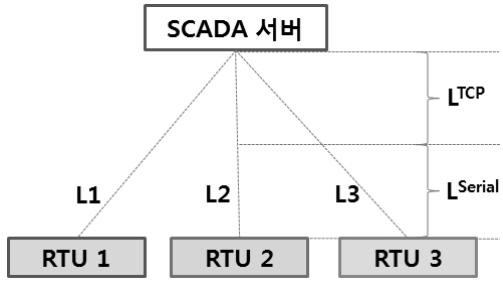
	SCADA 서버	L_1^{TCP}	L_2^{TCP}	L_3^{TCP}	L_1^{Serial}	L_2^{Serial}	L_3^{Serial}	RTU1	RTU2	RTU3	합산
Eavesdropping	0.0072	0.0182	0.0182	0.0182	0.018	0.018	0.018	0.0016	0.0016	0.0016	0.1206
Traffic Analysis	0	0	0	0	0	0	0	0	0	0	0
EM/RF Interception	0	0	0	0	0	0	0	0.0132	0.0132	0.0132	0.0396
Indiscretions by Personnel	0.04	0	0	0	0	0	0	0	0	0	0.04
Media Scavenging	0.04	0	0	0	0	0	0	0	0	0	0.04
Trojan Horse	0.032	0	0	0	0	0	0	0.0160	0.0160	0.0160	0.08
Trapdoor (Backdoor)	0.032	0	0	0	0	0	0	0.0160	0.0160	0.0160	0.08
Service Spoofing	0.032	0	0	0	0	0	0	0.0160	0.0160	0.0160	0.08
Masquerade	0	0	0	0	0	0	0	0.0363	0.0363	0.0363	0.1089
Bypassing Controls	0	0	0	0	0	0	0	0.0363	0.0363	0.0363	0.1089
Authorization Violations	0.048	0	0	0	0	0	0	0.0220	0.0220	0.0220	0.114
Physical Intrusion	0.0216	0.035	0.035	0.035	0.036	0.036	0.036	0.0044	0.0044	0.0044	0.2478
Replay	0	0	0	0	0	0	0	0.0363	0.0363	0.0363	0.1089
Theft & Illegitimate Use	0	0	0	0	0	0	0	0.0363	0.0363	0.0363	0.1089
Denial of Service	0.064	0.074	0.074	0.074	0	0	0	0	0	0	0.286
합 산	0.3168	0.1272	0.1272	0.1272	0.054	0.054	0.054	0.2344	0.2344	0.2344	

RTU2, RTU3를 연결하는 통신선로는 L1, L2, L3로 명명되며, 각각의 선로성분은 L_n^{TCP}와 L_k^{Serial}로 구성되어 있다. 발전기의 경우는 통상 EMS (Energy Management System)의 통제를 받으므로, 본 사례연구에서는 고려하지 않는다. 샘플계통에 지역별 구분을 둔 것은 지역 혹은 부하의 속성별로 정전비용을 구분하기 위해서이다.



〔그림 9〕 모의 전력계통

정전비용의 정량적 수치와 관련해서는, 〔표 7〕에서 보는 바와 같이 2008년 한국전기연구원에서 수행한 연구보고서를 참조하였다[9]. 18개 주요업종에 대한 정전비용을 2년간에 걸쳐 1,000개 이상의 샘플에 대해 설문조사를 통해 산출하였고, 관련 연구결과 중 가장 최근에 수행되고 상대적으로 심도 있는 연구이기 때문에 해당 연구의 결과를 본 연구의 사례연구에 적용하기로 하였다. 상기의 가정에 근거하여 해당 SCADA 시스템을 구성해보면 다음의 〔그림 10〕과 같다. 상기에서 정의한 정보자산의 가치를 정량화함에 있어서 통신설비와 정전비용의 경제적 가치를 합산하여 산출하는데, 통상적으로 전력계통에서는 정보자산의 가치보다는 정전피해비용의 금액이 훨씬 높기 때문에 $LV_n^k(C) \ll OC_n^k(P)$이 $LV_n^k(C) + OC_n^k(P) \approx OC_n^k(P)$로 근사화될 수 있다.



〔그림 10〕 모의 SCADA 시스템

1시간 정전을 기준으로 주거용은 2,800〔원/kW〕, 산업용은 127,420〔원/kW〕, 상업용은 37,365〔원/kW〕이다[10]. 이를 지역별 용량을 고려하여 합산하면 RTU1에서 관할하는 모선 1(상업지역)은 7,473〔백만원〕, RTU2에서 관할하는 모선 2(산업지역)은 38,226〔백만원〕, RTU3에서 관할하는 모선 3(주거지역)은 1,120〔백만원〕이다. 이를 정리하면 〔표 7〕과 같다. 〔표 7〕은 식 (2)~(10)에 표기된 정보자산의

〔표 6〕 취약성 지수 산출 (취약성이 높을수록 높은 수치)

	SCADA서버	L_1^{TCP}	L_2^{TCP}	L_3^{TCP}	L_1^{Serial}	L_2^{Serial}	L_3^{Serial}	RTU1	RTU2	RTU3
취약성 수준	0.0179	0.0357	0.0357	0.0357	0.0536	0.0536	0.0536	0.0714	0.0714	0.0714

〔표 7〕 SCADA 구성요소 및 대응지역 별 정전비용

	SCADA서버	L_1^{TCP}	L_2^{TCP}	L_3^{TCP}	L_1^{Serial}	L_2^{Serial}	L_3^{Serial}	RTU1	RTU2	RTU3
	전체 지역	상업 지역	산업 지역	주거 지역	상업 지역	산업 지역	주거 지역	상업 지역	주거 지역	산업 지역
정전비용 $OC_n^k(P)$ 〔백만원〕	46,819	7,473	38,226	1,120	7,473	38,226	1,120	7,473	38,226	1,120

가치(A)가 된다. 따라서 최종적인 사이버 위협으로 인한 위험(R)의 크기는 다음 〔표 5〕, 〔표 6〕, 〔표 7〕의 결과값 연산을 통해 구할 수 있다. 이는 식 (2)에 근거한 것으로 이를 통해 최종적인 위험(Risk)의 수준을 화폐단위로 산출할 수 있다. 다음의 금액은 1시간 정전에 대한 위험금액이고 24시간, 수일 단위로 확장될 경우 피해금액은 급속히 증가하게 된다. 특히 정전비용의 경우는 시간이 길어질수록 비선형적인 형태(지수함수)로 증가하기 때문에 그 피해규모가 매우 클 수 있다. 〔표 8〕은 본 사례연구 데이터에 근거하여 최종적으로 산출된 위험의 화폐단위 결과이다. 위협의 수준이 올라갈수록, 취약성이 낮아질수록, 자산의 가치가 올라갈수록 위험금액과 위험률은 상승할 수 있다. 〔표 8〕의 결과는 사이버 위협이나 공격이 존재할 경우 최소한의(단위) 예상피해 정도로 파악할 수 있다.

V. 결 론

본 논문에서는 날로 관심이 증가하고 있는 전력 SCADA 시스템의 사이버 위험을 평가할 수 있는 방법론에 대하여 제안하였다. 현재 전력시스템의 사이버 보안 연구는 날로 증가하고 있는 우려에 비해 구체화되지 못하고 있다. 그것은 전력시스템과 보안을 동시에 이해하고 있는 전문가가 부족하기 때문이며 그로 인해 전력시스템에 특화된 위험을 정확히 파악하지 못하고 있다. 대부분의 연구와 접근은 기존 IT 시스템에서 존재하고 있는 위험과 그에 대한 대응책을 되풀이하는데 그치고 있기 때문에 이러한 측면에서 전력시스템에 대한 보안 위험을 보다 구체화할 필요가 있다. 사이버 보안에서의 위험이란 위협(threat), 취약성(vulnerability), 자산(asset)으로 구성되는데 본 논문에서는 전력시스템에 특화된 위협과 취약성을 정의하고 이를 기반으로 위험을 정량화할 수 있는 방법을 제안하였다. 사이버 사고의 경우는 사고에 대한 정보가 잘 공개되지 않고, 시스템 마다 다양한 경우와 맥락을 가지기 때문에 정량화하기가 쉽지 않다. 사이버 위협과 취약성에 대한 수준은 과거의 데이터가 없기 때문에 상대적인 비교를 통해 정량화하는 방식을 적용하였다. 이러한 방법은 사회과학에서 자주 사용되는 다속성을 고려한 정량적 평가 방법 중의 하나인 AHP(analytic hierarchy process)에 기반한 것으로, 그 과정의 일부를 본 연구에 도입한 것이다. 그

〔표 8〕 위협과 취약성을 고려한 위험(risk) 산정 결과

	SCADA 서버	L_1^{TCP}	L_2^{TCP}	L_3^{TCP}	L_1^{Serial}	L_2^{Serial}	L_3^{Serial}	RTU1	RTU2	RTU3
위 협 (T)	0.3168	0.1272	0.1272	0.1272	0.054	0.054	0.054	0.2344	0.2344	0.2344
취약성 (V)	0.0179	0.0357	0.0357	0.0357	0.0536	0.0536	0.0536	0.0714	0.0714	0.0714
자 산 (A) 〔백만원〕	46,819	7,473	38,226	1,120	7,473	38,226	1,120	7,473	38,226	1,120
위 험 (R) 〔백만원〕	265.50	33.94	173.59	5.09	21.63	110.64	3.24	125.07	639.76	18.74
위험률(%) 〔위협 1건〕	0.57%	0.45%	0.45%	0.45%	0.29%	0.29%	0.29%	1.67%	1.67%	1.67%

다음은 자산의 정량화 문제인데, 전력시스템의 경우는 정보자산의 침해가 곧 전력계통의 운영과 신뢰도에도 영향을 줄 수 있기 때문에 이러한 잠재적 피해비용을 자산에 반영해줄 필요가 있다. 전력분야에서의 피해비용은 정전비용으로 귀결된다. 정전비용에 대한 연구는 국내외 다양한 연구기관과 학교에서 연구되어 왔기 때문에 이러한 결과 중 하나를 적용하였다. 본 연구는 사이버 위협을 정량화하기 위한 시발 단계의 연구로서 아직까지 보완하여야 할 점이 있다고 판단된다. 그러나 기본적인 구성과 방법론을 정의함으로써 향후 보다 상세한 연구를 하기 위한 근거를 마련하였다는데 의의가 있고, 향후 위협과 취약성을 보다 구체화하는 연구를 지속할 계획이다. 본 연구가 가지고 있는 고유의 의의 측면에서 본다면, 기존 연구들이 이론적이고 방법론적인 측면에서 주로 접근이 이루어졌다면 본 논문에서는 방법론과 더불어 구체적인 수치의 적용을 통해 현실에서 활용할 수 있는 측면에도 무게를 두고 연구가 수행되었다.

참고문헌

〔1〕 "Vulnerability Assessment," SANS Institute InfoSec Reading Room, http://www.sans.org/

〔2〕 "Vulnerability assessment", http://en.wikipedia.org/wiki/Vulnerability_assessment

〔3〕 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, Tuesday, March 25, 2010

〔4〕 홍승필, 김영철, "정보보호의 이해(Introduction to Information Security)," 길벗, pp. 5-12, 2004

〔5〕 Burris, Peter, and Chris King, "A Few Good Security Metrics," METAGroup, Inc. audio, 11 Oct. 2000. URL: http://www.metagroup.com/metaview/mv0314/mv0314.html (10 July 2001)

〔6〕 Matias Negrete-Pincetic, Felipe Yoshida, George Gross, "Towards Quantifying the Impacts of Cyber Attacks in the Competitive Electricity Market Environment," POWERTECH 2009, http://energy.ece.illinois.edu/gross/papers/powertech2009final.pdf

〔7〕 "Analytic Hierarchy Process," Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Analytic_Hierarchy_Process

〔8〕 Ernest H. Forman, "Decision by Objective: Analytical Hierarchy Process," http://www.dept.aoe.vt.edu/~cdhall/courses/aoe4065/AHPslides.pdf

〔9〕 한국전기연구원, 인천대학교, "계통계획을 위한 산업용 수용가의 공급지장비 조사 연구," 산업자원부, 2008.02.

〔10〕 한국전기연구원, 서울대학교, "전기요금 수준별 적정 정전손해배상 범위설정 및 리스크 분산방안에 관한 연구," 한국전력공사 영업처, 2011.04.

〔11〕 Nian Liu, Jianhua Zhang, and Wenxia Liu, "Security Assessment for Communication Networks of Power Control Systems Using Attack Graph and MCDM," IEEE Transactions on Power Delivery, pp. 1492-1500, 2010

〔12〕 Pravin Chopade and Dr. Marwan Bikdash, "Modeling for Survivability of Smart Power Grid when subject to severe emergencies and vulnerability," Southeastcon, 2012 Proceedings of IEEE, pp. 1-6, 2012

〔13〕 Deepa Kundar, Xianyong Feng, Shan Liu, Takis Zourntos, Karen L., Burtler-Purry, "Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid," 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 244-249, 2010

〔14〕 Jin Wei, Deepa Kundur, Takis Zourntos, "On the Use of Cyber-Physical Hierarchy for Smart Grid Security and Efficient Control," 2012 25th IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), pp. 1-6, 2012

〔15〕 오두환 식별된 저자, 최두식, 나은성, 김상철, 하재철, "ID 기반 암호 기법을 이용한 SCADA 시스템에서 비밀 키관리 및 복구 방안," 한국정보보호학회논문지 제22권 제3호, 2012.6, pp. 427-438, 2012년 6월

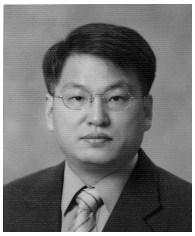
〔16〕 김영진 이정현 임종인, "SCADA 시스템의 안전성 확보방안에 관한 연구," 한국정보보호학회논문지 제19권 제6호, 2009.10, pp..145-152, 2009년 12월

〈저자소개〉

강 동 주 (Dong-Joo Kang) 정회원
1999년 2월: 홍익대학교 전자전기제어공학과 졸업
2001년 8월: 홍익대학교 전기정보제어공학과 석사
2009년 8월: 성신여자대학교 금융정보대학원 석사
2012년 2월: 홍익대학교 전기정보제어공학과 박사
2012년 8월~현재: 고려대학교 정보보호대학원 박사과정
2001년~현재: 한국전기연구원 차세대전력망연구본부 스마트전력망연구센터 선임연구원
〈관심분야〉 정보보호, 전력공학, 게임이론

이 종 주 (Jong-Joo Lee) 정회원
1999년: 수원대학교 전기공학과 졸업
2001년: 성균관대학교 정보통신공학부 석사
2008년: 성균관대학교 정보통신공학부 박사
2001년~2004년: 새턴정보통신(주) 개발팀장
2005년~2007년: 성균관대학교 정보통신용신기능성소재및공정연구소 연구원
2008년~현재: 한국전기연구원 차세대전력망연구본부 스마트전력망연구센터 선임연구원
〈관심분야〉 전력계통 신호처리, 임베디드 시스템

이 영 (Young Lee) 정회원
1999년 2월: 육군사관학교 경영학과 졸업
2003년 2월: 국방대학교 국방관리학과 석사
2010년~현재: 국방대학교 관리대학원 국방관리학과 박사과정
〈관심분야〉 SCM(risk resilience), logistics, complex network, typological robustness



이 임 섭 (Im-Sop Lee) 정회원
1981년 2월: 한국전력공사 입사
1989년 2월: 방송대학교 전자계산학과 졸업
2012년 8월: 고려대학교 정보보호대학원 석사
2001년 4월~현재: 한국전력거래소 근무(정보보호팀장)
〈관심분야〉 전력IT, 정보통신, 정보보호

김 휘 강 (Huy Kang Kim) 종신회원
1998년 2월: KAIST 산업경영학과 졸업
2000년 2월: KAIST 산업경영학과 석사
2009년 2월: KAIST 산업및시스템공학과 박사
2004년 5월~2010년 2월: 엔씨소프트 정보보안실 실장, Technical Director
2010년 3월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 온라인게임 보안, 네트워크 보안, 네트워크 포렌식