Journal of the Korean Institute of Illuminating and Electrical Installation Engineers (2011) 25(6) : 90~99
DOI : 10.5207/JIEIE.2011.25.6.090

논문 25-6-12

SCADA 시스템의 보안취약성을 고려한 정전비용 산정기법에 관한 연구

(A Study on Estimation Method of Outage Cost caused by Vulnerabilities of SCADA System)

김발호* · 강동주
(Balho H. Kim · Dong-Joo Kang)

Abstract

As power industry evolves into Smart Grid scheme, previously closed power systems are being integrated into public communication networks. It increases the controllability and efficiency of the system, but also accompanies many cyber threats having existed in the Internet to the SCADA system. Therefore it is required to apply security countermeasures to the Smart Grid, which brings about investment costs. There have been few approaches to assess risks from cyber attack especially in electric power industry. So this paper proposes a methodology to assess quantitative impacts of various types of cyber attacks to a power system, and also shows the feasibility of the method through a case study.

Key Words : Smart Grid, Security, Cyber Attack, Risk Assessment, Quantitative Impact

1. 서 론

본 논문은 SCADA 시스템에 상존하는 잠재적 사이버 위험이 전력계통의 정전에 미칠 수 있는 잠재적 위험을 분석하고 이를 정량적인 수치화할 수 있는 방법을 제안하는 것을 목적으로 한다. 이를 통해 SCADA 시스템에 상존하고 있는 해킹 위협을 미연에 방지하기 위한 대책 수립 시 효율적인 투자의사결정에 대한 근거를 제공할 수 있다. 현재까지의 SCADA 시스템은 외부 통신망과 분리되어 폐쇄적으로 운영되고 있기 때문에 상대적으로 사이버 공격에 안정적일 수 있다. 그러나 앞으로의 스마트그리드 체제에서는 AMI 및 각종 센서네트워크와 연계되면서 공용망과의 연결이 불가피하게 된다. 이 경우 인터넷망에 존재하고 있는 다양한 위협이 그대로 SCADA 망으로 전이될 수 있기 때문에 이에 대한 대책 수립이 시급한 시점에 있다. 이러한 SCADA망의 보안취약성과 관련해서는 많은 연구들이 진행되고 있다 [1-3]. 보안 문제라는 것은 원인이 되는 위협이 항상 진화하고 늘 새로운 취약성이 등장하기 때문에 완벽한 방어는 불가능하다. 또한 예산 제약과 시스템 효

* 주저자 : 홍익대학교 전자전기공학부 교수
Tel : 02-320-1462, Fax : 02-320-1193
E-mail : bhkim@hongik.ac.kr
접수일자 : 2011년 3월 28일
1차심사 : 2011년 4월 1일, 2차심사 : 2011년 4월 26일
심사완료 : 2011년 5월 12일

율성에 미치는 영향 때문에 무한정 보안을 강화할 수도 없다. 이러한 맥락에서 잠재적 위험과 비용 투입을 동시에 최소화할 수 있는 전략적 의사결정이 필요하며, 위험을 정량적으로 모델링 할 수 있는 프레임워크가 요구된다. 전력시스템에서 위험이 실현되면 정전이라는 결과로 나타나는데, 이 때 정전으로 인해 발생하는 비용을 정전비용이라고 한다. 정전비용은 그림 1과 같이 크게 미시적 방법과 거시적 방법이 사용되는데 부하종류별(주거용, 산업용, 상업용)로 구분하여 산정된 비용을 적용하기로 한다.

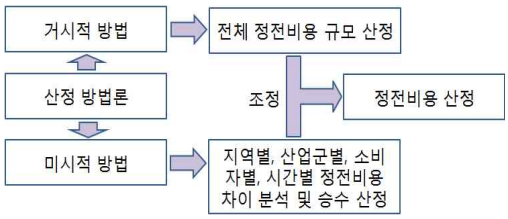

그림 1. 정전비용 산정의 2가지 방법
Fig. 1. Two Approach to Outage Cost

특정의 사이버 공격이 전력시스템에 영향을 주게 되고, 이것이 부분적 혹은 전체적 정전을 유발하였을 경우에 미치는 잠재적 비용을 평가한다면, 이 값이 해당 위험으로 발생할 수 있는 잠재적 피해금액이라고 간주할 수 있다. 여기에 해당 이벤트(사이버 공격 내지 위협)가 발생할 확률, 해당 이벤트에 의해 정전이 발생할 확률을 등을 고려한다면, 해당 이벤트의 잠재적 피해비용을 계산할 수 있다. 또한 이러한 과정에서 보안설비 내지 대책을 적용함으로써 감소시킬 수 있는 비용을 계산하면 비용 · 편익 분석을 할 수 있고, 이를 통해 효율적인 의사결정에 대한 답을 얻을 수 있다. 본 논문은 이러한 의사결정 과정을 정량적으로 모델링하는 과정에 대한 아이디어를 제공하며, 사례연구를 통해 그러한 접근과정의 효율성을 검증하는 형태로 진행하였다.

2. SCADA 시스템과 정전

전력시스템은 그림 2에서 보는 바와 같이 크게 2가지 인프라로 구성되어 있는데, 하나는 전력계통이고, 다른 하나는 그러한 전력계통을 감시하고 운영하기 위한 통신 인프라인 SCADA 시스템이다.

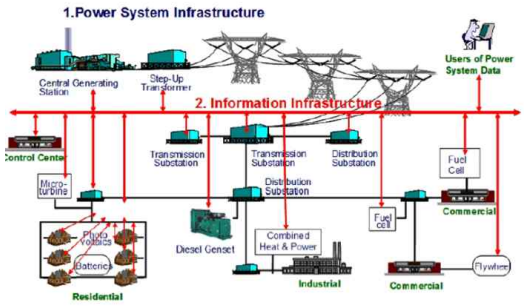

그림 2. 전력시스템을 구성하는 2가지 인프라
Fig. 2. Two infrastructures of Power System

기존전력 분야에서 신뢰도라고 하면 물리적 계통에서의 안전도(security)측면만이 고려되어 왔는데, 연간 특정 설비의 우발적인 고장정지율(FOR)을 고려하여 신뢰도 및 정전비용을 산정하여 왔다. 그러나 이러한 우발적 설비의 고장정지 외에도 최근 통신 네트워크와의 연계가 강화됨에 따라 의도적인 제3자에 의한 사이버 공격에 대한 잠재적 위협이 증가하고 있는 추세에 있다. 따라서 그림 3과 같이 2가지 인프라의 상호작용을 포괄하는 신뢰도 개념이 필요하며, 그에 기반한 정전비용의 산정 및 잠재적 위험성이 정량적으로 모델링되어야 한다.

3. SCADA 시스템과 사이버 위협

그림 3. 전력계통과 SCADA 시스템 간의 상호작용
Fig. 3. Interactions btw Different Layers

SCADA 시스템의 사이버 보안에 대한 취약성은 특성 상 정성적인 속성에 가깝다. 이러한 정성적인 속성을 구성하는 다양한 요소들을 세분하여 분석·분류하고 각 요소별 가중치 부여 및 비중을 산정함으로써 점차 정량화 시키는 것이 그러한 신뢰도 특성을 반영하는 핵심 과정이라 할 수 있다.

이러한 개별 요소를 정의하는데 있어서는 공격의 대상 및 범위, 공격의 유형, 전력계통의 동태적 상황 등 다양한 요소들이 존재하기 때문에 굉장히 많은 상태(status)의 조합이 정의되고 분석되어야 한다. 본 연구에서의 핵심은 SCADA 시스템에 대한 보안취약성을 정의하고 정량화하는 방법에 있다고 할 수 있다. SCADA 시스템은 상단의 SCADA 서버, 하단의 RTU들, 그리고 둘 사이를 연결하는 통신 네트워크의 3부분으로 구성되어 있으며, 시스템이 광역화 될 경우, 중간에 Sub-SCADA 서버가 존재하는 형태의 계층적 구조를 형성하기도 한다.

3.1 SCADA 시스템에 대한 위험 정의

표 1. SCADA 시스템에 대한 공격유형 [4]
Table 1. Attack Types to SCADA System

공격 유형	공격 종류 및 동기
① 서비스 거부 공격	서버 다운을 통한 시스템 중지
② 시스템 파일 삭제	서버 다운을 통한 시스템 중지
③ 제어권 획득	산업 시설 및 기타 설비에 대한 훼손
④ 키로깅	아이디, 비밀번호, 시스템 설정값 등의 정보 수집
⑤ 시스템 설정값이나 데이터 변경	시스템 고장이나 비효율 초래
⑥ 경영 혹은 재무 데이터에 대한 접근	데이터를 훔쳐 다른 회사에 팔거나 배상금을 노림
⑦ 그래픽 상의 데이터 값을 변경	잘못된 경보를 발생시켜 시설이나 플랜트를 다운시켜 위험하게 만듦
⑧ 데이터베이스의 로그인 기록을 획득, 변경, 삭제 하는 공격	악의적인 목적으로 프로세스의 설정값과 기업의 데이터를 변경
⑨ 유지관리 DB에 대한 접근	회사의 데이터를 획득, 변경, 삭제하고자 함

표 2. 공격에 의한 잠재적 피해 종류 [4]
Table 2. Potential Damage by Attacks

공격 유형	잠재적 피해	공격 강도	소요 시간
①	서버 다운을 통한 시스템 중지	2	약5분
②	서버 다운을 통한 시스템 중지	4	약15분
③	산업 시설 및 기타 설비에 대한 훼손	1	약60분
④	아이디, 비밀번호, 시스템 설정값 등의 정보 수집	4	약15분
⑤	시스템 고장이나 비효율 초래	2	약45분
⑥	데이터를 훔쳐 다른 회사에 팔거나 배상금을 노림	5	약30분
⑦	잘못된 경보를 발생시켜 시설이나 플랜트를 다운시켜 위험하게 만듦	2	약45분
⑧	악의적인 목적으로 프로세스의 설정값과 기업의 데이터를 변경	3	약45분
⑨	회사의 데이터를 획득, 변경, 삭제하고자 함	4	약30분

현재 SCADA 시스템에 대한 보안 연구는 시작단계로 아직까지 경험에 의해 정확히 보고된 사례는 없으며, 연구단계에서의 분석이 이루어지고 있는 단계이다. Pollet 등은 SCADA 시스템에 대한 공격 유형을 표 1과 같이 분류하였다[4]. 이는 일반적인 해킹 공격 중에서 SCADA 시스템에도 적용될 수 있는 공격을 정리한 것으로 모두 서버단 측에 대한 공격이라고 할 수 있다.

표 1의 개별적인 공격 패턴들은 표 2에서 정리된 바와 같이 잠재적인 피해를 초래하게 된다. 우측의 공격강도는 해당 공격이 성공했을 때 발생할 수 있는 피해의 정도를 상대적인 순위 형태로 표현한 것이다. 이러한 공격강도에 대한 순위는 이후 잠재적 정전비용의 산정에 적용한다.

①~⑨에서의 공격 유형을 비교해보면, 공격 강도에서도 어느 정도 나타나듯이, 시스템의 제어권을 완전히 확보하는 경우, 그림 4에서와 같이 부분적인 제어권이나 데이터 변경이 가능한 경우, 과도한 부하로 서버에 무리를 주는 경우, 재무적 정보를 취득하는 경우 등으로 나누어볼 수 있다. 이러한 4가지 유형의 공격 중 재무적 정보 취득은 직접적인 제어시스템과는 관련성이 적으므로 제외하면, 정전에 영향을 미치는 사이버 공격 유형은 3가지로 최종 축약될 수 있다.

그림 4. 공격유형 분류
Fig. 4. Classification of Attack Types

Matias Negrete-Pincetic 등도 경쟁적 전력시장 환경에서 사이버 공격의 영향을 정량화하기 위한 연구를 수행하였는데, 그림 5와 같이 크게 4가지 공격 유형을 정의하고 위험의 정도와 공격의 어려운 정도에 따라 비교하였다[5]. 그림 5에서 중간자 공격(man-in-the-middle) 공격은 송신단과 수신단의 중간에서 송신단 측에는 수신자로 수신단 측에는 송신자로 위장하는 수법이다. 중간자 공격은 IPSec[1]에서의 ESP[2]와 같은 보안 수단이 없는 경우 데이터 스트림의 불법 수정이나 거짓 데이터 스트림의 생성을 수반할 수 있다.

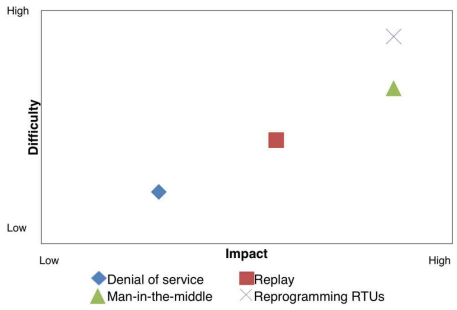

그림 5. 공격의 영향과 난이도
Fig. 5. Impact versus difficulty chart

1) IP(Internet Protocol) packet에 암호화와 인증기능을 추가하여 보안성을 강화한 프로토콜 버전. IP+Security의 의미
2) Encapsulating Security Payload의 약자로 기밀성, 원본 데이터의 인증, 무결성과 같은 보안 서비스를 지원하기 위하여 설계된 프로토콜로 IP 데이터그램 안에 들어감.

특히 이러한 중간자 그림 6과 같이 이루어지며, 공격은 현재 기본적인 암호화도 수행되고 있지 않는 SCADA 통신에서 더욱 위협적일 수 있다. 중간자 공격을 할 수 있는 위치를 확보하면, 신분위장(masquerade), 재전송(replay), 메시지 불법수정, 서비스거부공격(DoS) 등 다양한 세부 공격을 수행할 수 있다.

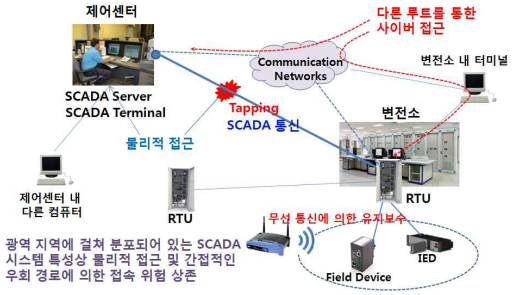

그림 6. SCADA 시스템에서의 중간자 공격
Fig. 6. Man-in-the-middle Attack on SCADA

SCADA 시스템은 물리적으로 제어센터와 RTU 간의 거리가 멀리 떨어져 있기 때문에 이러한 공격 가능성은 더욱 높아진다. 특히 오늘날은 전자 신호만으로 프로토콜을 파악하고 해석할 수 있는 다양한 상용 프로토콜 분석기(protocol analyzer)와 선로 탭핑(tapping) 기술이 발전하고 있기 때문에 이러한 위협의 가능성은 보다 높아지고 있는 추세에 있다.

다양한 문헌에서 다양한 공격 유형들을 정의하고 있는데, 상기에서 언급한 바와 같이 어떤 공격 형태는 한 공격이 성공하고 난 뒤의 후속적인 공격 형태일 수도 있고, 또는 독립된 형태일 수도 있다. 또는 한 공격의 결과 형태로 나타나는 현상을 독립적인 공격 형태로 분류한 것도 있는데 이에 대한 정리가 필요할 것으로 판단된다. 공격에 대한 분류가 일단 체계적으로 이루어져야 잠재적 위험에 대한 평가를 정량화할 수 있기 때문이다.

3.2 위협의 체계적 분류와 정량화

그림 4의 공격 유형들을 분석해보면, 크게 제어권을 획득한 경우와 획득하지 못한 경우로 나뉠 수 있다.

제어권이 확보되면 보다 위험한 공격이 가능하고, 그렇지 못할 경우 지역적인 공격을 통한 부분적 제어권의 탈취나 원활한 동작에 지장을 주는 경우도 있다. 본 연구에서는 그림 7과 같은 형태로 공격 유형을 분류하였다.

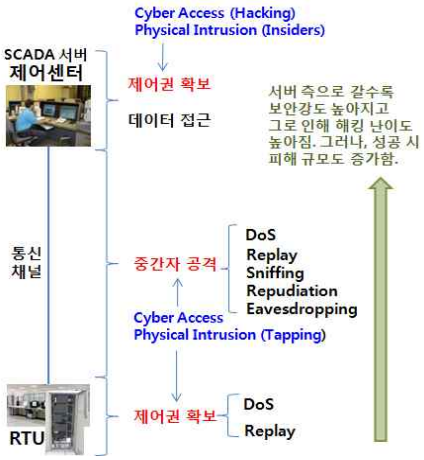

그림 7. 계층별 공격유형 분류
Fig. 7. Hierarchical Attack Types

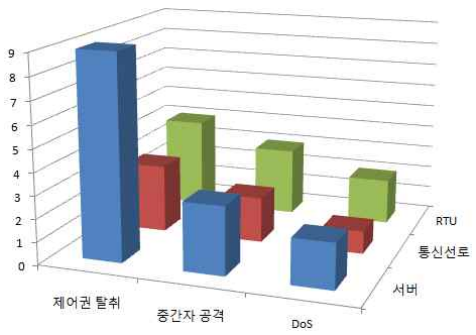

그림 8. 공격의 난이도 분포
Fig. 8. Difficulty level of Attack Types

통상적으로 DoS 공격이 가장 용이하나 피해 정도는 경미하고, 제어권을 탈취(침범) 당하는 것이 가장 난이도는 높으나 성공 시 피해가 클 수 있다. 그 사이에 존재하는 것이 중간자 공격 정도라고 인식할 수 있고 중간자 공격을 통해, DoS 리플레이 등의 다양한 2차적 공격이 가능하다. 따라서 본 연구에서는 공격 유형을 크게, ① DoS, ② 중간자 공격, ③ 제어권 탈취로 구분한다. 단 제어권 탈취에 대한 공격도 대상이 제어센터의 SCADA 서버인지, RTU인지에 따라 잠재적 피해 정도가 다르다. 서버의 경우는 제어권이 탈취될 경우 전체 정전으로 이어질 수 있고, RTU의 경우는 부분 정전 내지 시스템 비효율 정도의 결과에 그치게 된다. 이러한 공격유형 및 대상에 대한 조합을 공격 난이도에 대한 분포로 나타내면 그림 8과 같다.

본 연구에서는 경우의 단순화를 위해 정전에 대한 결과만을 고려하고 각 이벤트가 정전에 미치는 확률을 공격 난이도에 근거하여 가정하는 형태를 적용하였다. 과거의 데이터가 있으면 좋겠지만 이러한 사이버 해킹에 의한 정보는 공개되지 않기 때문에 통상적인 정전 확률에서 몇 % 정도를 사이버 해킹에 의한 것으로 가정하는 형태를 취하였다.

4. 정전비용의 고려

정전비용에 대한 연구는 학계와 연구계를 통해 다양하게 이루어져 왔다. 본 연구에서는 국내외 연구결과를 참조하여 산업용, 상업용, 주거용에 대한 정전비용을 적용하기로 한다. 먼저 산업용 수용가의 경우는 2008년 한국전기연구원에서 수행한 연구결과를 참조한다[6]. 이 연구는 설문조사 방식으로 산업용 수용가들에 대한 정전비용을 실제로 설문조사하였기 때문에 소비자 입장에서의 실제 피해금액을 비교적 정확하게 반영하고 있다고 볼 수 있다. 그림 9는 정전시간 별 정전비용을 보인 것으로 18개 업종에 대한 것이다. 좌측에 표시된 숫자는 18개 업종에 대한 시간별 평균 정전비용으로 각각 20분(88,125[원/kW]), 30분(129,380[원/kW]), 1시간(169,068[원/kW])을 대표적으로 표기한 것이다. 그림 10은 20분 정전을 기준으로 부하종류별로 정전비용을 비교하여 나타낸 것이다.

국내외 다양한 연구사례를 참고할 경우 30분에 해당하는 상업용 정전비용의 크기는 산업용 정전비용 대비 1.17배 정도 높은 것으로 추정된다[6-7]. 주거용 부하에 대해서도 다양한 연구들이 수행되어 왔지만, 본 연구에서는 거시적 방법론에 기반하여 산정된 정전비용을 적용하기로 한다[8]. 해당 연구결과에 의한 정전비용의 수준은 3,000[원/kW-h]이다.

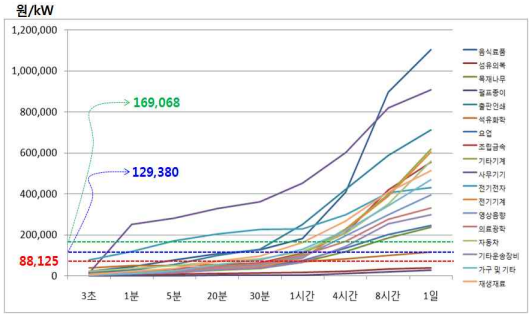

그림 9. 용량 단위 정전비용
Fig. 9. Outage Cost per Unit Capacity

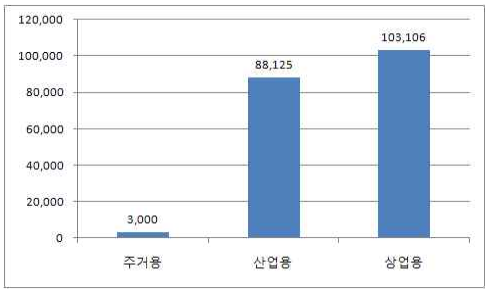

그림 10. 부문 별 정전비용[원/kW-h]
Fig. 10. Outage Cost of Each Customer Sector [Won/kW-h]

5. 사례연구

본 연구의 사례연구를 위해서 다음과 같은 샘플 계통을 구성하였다. 발전소는 2개로 구성되어 있으며, 부하는 3개의 지역에 산업용, 상업용, 주거용 부하가 흩어져 있다고 가정한다. 송전선로는 각 발전소별로 2개씩 각 부하 사이트로 연결되어 있다. 정전이 발생하는 이유는 다양하게 존재할 수 있는데, 다음과 같이 정리해 보았다.

① 발전설비용량보다 수요가 높은 경우
② 발전설비 중 1개 이상 탈락(trip)되는 경우
③ 송전선로 중 1개 이상 탈락(trip)되는 경우
④ SCADA 서버 이상 (자연고장 + 외부공격)
⑤ 통신선로 이상 (자연고장 + 외부공격)
⑥ RTU 고장 (자연고장 + 외부공격)

①~③은 그림 11의 예제 전력계통 상에서 발생할 수 있는 사고와 관련한 것이다.

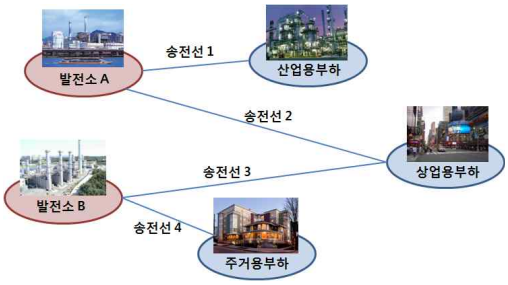

그림 11. 샘플 전력계통 구성
Fig. 11. Configuration of Example System

전력계통 측면의 이러한 토폴로지와는 별개로 그림 12의 시스템은 그림 11의 전력계통을 운영하는 SCADA 시스템 측면에서의 구성을 보인 것이다. ④~⑥은 SCADA 네트워크 상에서 발생할 수 있는 사고에 대한 것이며, 각 발전소는 RTU를 통해 SCADA 서버와 연결되어 있고, 각 부하들은 변전소 RTU를 통해 역시 SCADA 서버와 연결되어 있다. 주거용과 상업용의 경우는 동일 변전소, 산업용은 별개의 변전소를 통해 전력을 공급받고 있다고 가정한다.

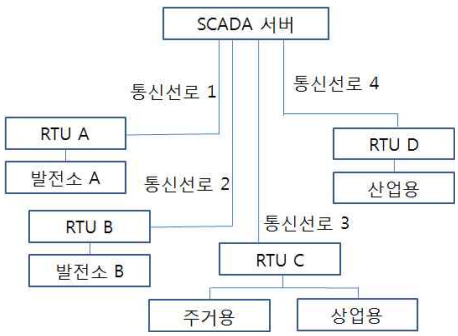

그림 12. SCADA 시스템 연결도
Fig. 12. SCADA System Configuration

2개의 발전소는 각각의 고장정지 확률을 가지고, 4개의 송전선로 역시 개별 송전률을 가지게 된다. 각 부하들은 상 · 중 · 하의 부하수준에 따른 확률분포를 가지게 된다. SCADA 시스템의 경우는 각 장치가 이상이 발생하더라도 그것이 물리적 전력계통의 정전으로 모두 귀결되는 것은 아니므로 적절한 확률을 부여하여 사건을 모델링하였다. SCADA 서버가 고장나면 하부의 통신선로나 RTU가 영향을 받고, 전력계통 시

스템의 모든 요소에도 영향을 미치게 된다. 그림 13은 이러한 관계도를 나타낸 그림이다.

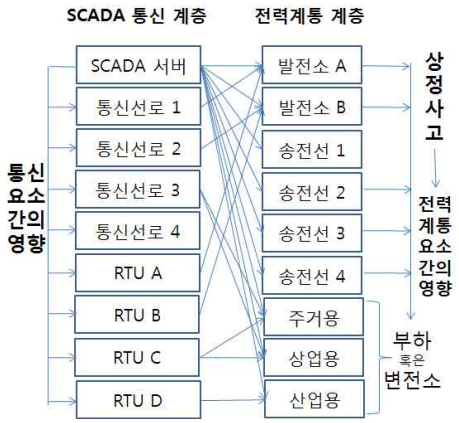

그림 13. 시스템 구성요소 간의 상호작용
Fig. 13. Interaction between Components

SCADA 서버, 통신선로, RTU 등이 사이버 공격을 받을 경우 물리적 전력계통 요소(발전소, 송전선, 부하)에 영향을 주는 관계도를 도식화한 것이다. SCADA 시스템과 전력계통 사이에 링크할 수 있는 경우의 수에 따라 다양한 관계가 형성될 수 있다. SCADA 서버의 이상은 전 시스템의 모든 구성요소에 잠재적으로 영향을 미칠 수 있다. 통신선로의 이상은 해당 지역을 연결하는 부하나 발전기에 이상을 일으킬 수 있으며, RTU의 이상 역시 해당 발전기나 지역의 정전에 영향을 미칠 수 있다. 표 3은 각 공격유형이 개별 시스템 구성요소에 적용되는 관계를 표현한 것이다. 1이면 영향을 미친다는 것이고, 0이면 미치지 않는다는 것이다.

표 3. 시스템 구성요소 별 공격유형
Table 3. Attack Types on Components

		제어권 탈취	중간자 공격	DoS
	SCADA서버	1	0	1
	통신선로 1	0	1	0
통	통신선로 2	0	1	0
신	통신선로 3	0	1	0
시	통신선로 4	0	1	0
스	RTU A	1	0	1
템	RTU B	1	0	1
	RTU C	1	0	1
	RTU D	1	0	1

그림 14는 표 3의 각 공격유형이 시도되어 성공할 확률과 그로 인해 실제 시스템 컴포넌트가 이상(정전에 영향을 주게 되는 경우)을 일으키는 경우에 대한 확률을 부여한 것이다.

그림 14. SCADA 시스템 요소 고장확률
Fig. 14. Outage Probabilities of SCADA System Components

동일한 공격 유형일지라도 SCADA 서버와 RTU의 보안 강도는 다르기 때문에 침투 성공확률에 변화가 있으며, 서버일수록 보안의 강도가 높기 때문에 침투 성공확률은 낮아진다. 그림 14의 결과로부터 개별 공격 유형이 실제 SCADA 시스템 구성성분의 고장으로 연결될 수 있는 확률은 두 매트릭스의 결과를 곱하여 그림 15와 같은 형태로 도출될 수 있다.

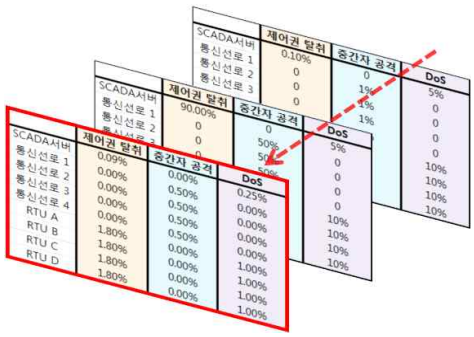

그림 15. 사이버 공격에 의한 FOR
Fig. 15. FORs by Cyber Threats

표 4는 그림 15의 개념에 근거하여, 사이버공격이 성공하였을 경우 정전에 미치는 상관관계를 표현한

행렬이다. 3가지 종류의 부하에 영향을 미치는 것은 사이버 공격에 의한 직접적인 통신장애에 의해 발생할 수도 있고(위쪽 채색된 부분), 1차적으로 전력계통 성분(발전소, 송전선로)이 영향을 받고, 이를 통해 상정사고의 2차적인 형태로 정전에 영향을 미치는 경우(아래쪽 채색된 부분)이다.

표 4. 전력계통과 SCADA 시스템 간 상관관계
Table 4. Correlation between SCADA & Power System

		발전		송전				변전 · 배전 (부하)		
		발전소 A	발전소 B	송전선 1	송전선 2	송전선 3	송전선 4	주거용	상업용	산업용
통신시스템	SCADA 서버	50%	50%	50%	50%	50%	50%	0%	0%	0%
	통신선로 1	30%	0%	0%	0%	0%	0%	0%	0%	0%
	통신선로 2	0%	30%	0%	0%	0%	0%	0%	0%	0%
	통신선로 3	0%	0%	0%	0%	0%	0%	25%	20%	0%
	통신선로 4	0%	0%	0%	0%	0%	0%	0%	0%	20%
	RTU A	50%	0%	0%	0%	0%	0%	0%	0%	0%
	RTU B	0%	50%	0%	0%	0%	0%	0%	0%	0%
	RTU C	0%	0%	0%	0%	0%	0%	50%	50%	0%
	RTU D	0%	0%	0%	0%	0%	0%	0%	0%	50%
전력계통	발전소 A	0%	0%	0%	0%	0%	0%	25%	50%	100%
	발전소 B	0%	0%	0%	0%	0%	0%	100%	50%	25%
	송전선 1	0%	0%	0%	0%	0%	0%	0%	0%	100%
	송전선 2	0%	0%	0%	0%	0%	0%	0%	50%	0%
	송전선 3	0%	0%	0%	0%	0%	0%	0%	50%	0%
	송전선 4	0%	0%	0%	0%	0%	0%	100%	0%	0%

상기의 데이터들은 통상적인 인식에 바탕을 두고 사례연구를 위해 가정된 데이터이다. 전력시스템의 사이버 보안과 관련하여 통계 데이터는 존재 여부가 불투명하고 있더라도 공개가 어렵다. 더군다나, 우리나라에서 전력시스템에 대한 사이버 보안 문제가 이슈가 된 것은 최근 스마트그리드에 대한 연구가 본격화되면서부터이고 폐쇄적 시스템으로 오랜 시간 유지되어 왔기 때문에 실제 데이터를 확보하기는 거의 불가능하다고 할 수 있다. 이러한 배경을 고려하여, 표 4의 데이터를 근거로 사이버 보안과 정전 간의 상관관계를 구해보면 다음의 그림 16과 같다.

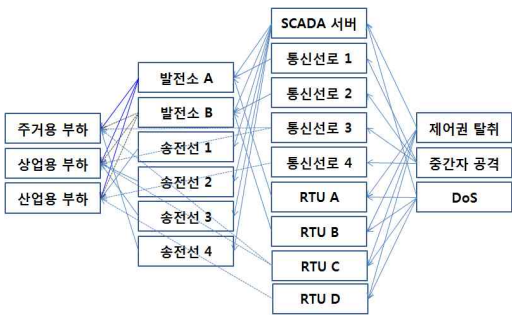

그림 16. 사이버 공격의 영향 분석
Fig. 16. Impacts of Cyber Attacks

다양한 형태의 사이버 공격이 있을 수 있겠지만, 본 논문에서는 제어권 탈취, 중간자 공격, DoS의 3가지로 정의하였다. 사이버 공격은 1차적으로 통신인프라인 SCADA 시스템에 영향을 주고, SCADA 시스템의 장애는 수용가의 정전이나 2차적으로 전력계통에 영향을 주게 된다. 전력계통 이상은 다시 수용가의 정전으로 이어질 수 있다. 그림 16은 이러한 관계를 도식화한 것이다.

$$P(OC_{total}) = \sum_{i=1}^{n} OC_i \cdot PO_i \quad (1)$$

$P(OC_{total}) \rightarrow$ 총 정전비용의 기댓값
$PO_i \rightarrow$ i 부하의 $Probability\ of\ Outage$ (정전확률)
$i = 1,2,3 \rightarrow$ 주거용, 상업용, 산업용 부하

수식 (1)에서 정전확률(PO_i)은 전력계통(P)의 고장정지율(FOR)에 의한 것과 SCADA(S) 시스템의 고장정지율이 조합되어 일어난다. 전력계통을 물리적으로 공격하는 경우는 없다고 가정하면, 즉 전력계통의 고장은 모두 우발적인 경우라면, SCADA 시스템으로 인해 정전이 발생할 수 있는 확률은 상기에서 설명한 바와 같이 SCADA 시스템의 데이터 이상으로 생긴 정전과 물리적 시스템에 영향을 미쳐 정전이 발생하는 2가지 경우로 구분할 수 있다. 이를 수식으로 표현하면 (2)와 같다.

$$PO_i = \sum_{j=1}^{l} FOR_{ij}(S) + \sum_{j=1}^{l}\sum_{k=1}^{m} FOR_{jk}(S) \cdot FOR_{ik}(P) \quad (2)$$

$$\begin{aligned} FOR(S) = {} & FOR(SCADA\ Server) \\ & + FOR(Comm.1) + FOR(Comm.2) \\ & + FOR(Comm.3) + FOR(Comm.4) \\ & + FOR(RTU1) + FOR(RTU2) \\ & + FOR(RTU3) + FOR(RTU4) \end{aligned}$$

$$\begin{aligned} FOR(P) = {} & FOR(Gen.A) + FOR(Gen.B) \\ & + FOR(Trans.1) + FOR(Trans.2) \\ & + FOR(Trans.3) + FOR(Trans.4) \end{aligned}$$

j = SCADA 시스템 컴포넌트(l개)
k = 전력계통 구성 컴포넌트(m개)

이러한 고장정지율(FOR)과 컴포넌트 간 관계에 근거하여 각 부하의 정전확률을 구하면 그림 17~19와

같다. 그림 17을 예로 들면 우측 3가지 공격 유형에서 좌측의 3가지 부하로 연결되는 경로를 따라 각 부하종류 별 사이버공격에 의한 정전확률을 구할 수 있다.

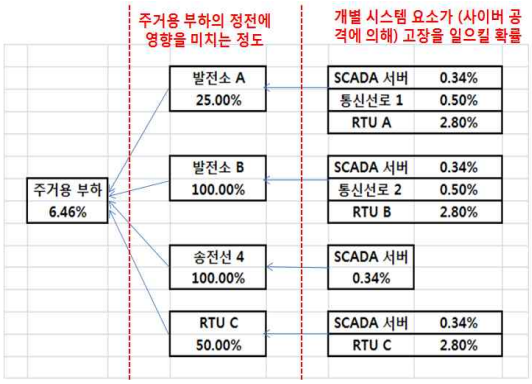

그림 17. 사이버 공격에 의한 주거용의 정전확률
Fig. 17. Outage Probability of Residential Load by Cyber Attacks

이와 같이 각 부하 종류별 (사이버 공격이 있을 경우)의 정전확률을 추정할 수 있다. 따라서 이 경우의 정전비용은 그림 10의 정전비용에 그림 17~19의 정전확률을 곱하여 잠재적 기대비용을 추정할 수 있고, 그림 20과 같이 도식화할 수 있다.

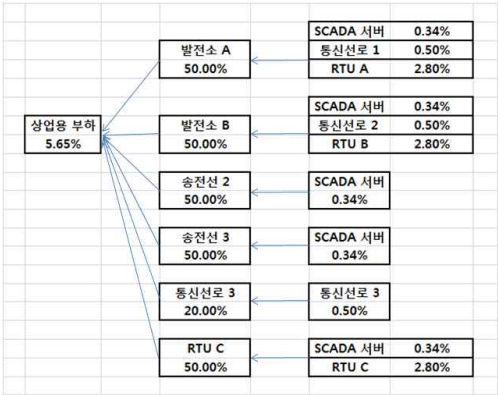

그림 18. 사이버 공격에 의한 상업용의 정전확률
Fig. 18. Outage Probability of Commercial Load by Cyber Attacks

그림 20은 정전이 발생했을 경우의 각 수용가에 대한 정전비용 비교와 사이버공격이 이에 기여하는 부문을 도식화한 것이다.

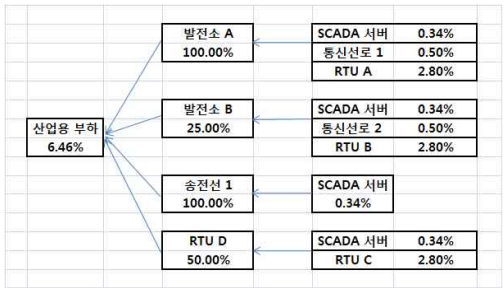

그림 19. 사이버 공격에 의한 상업용의 정전확률
Fig. 19. Outage Probability of Commercial Load by Cyber Attacks

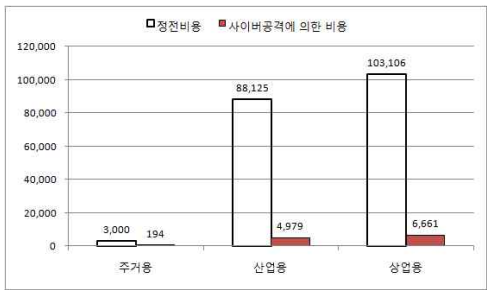

그림 20. 사이버 위협에 의한 정전비용 비교
Fig. 20. Comparison of Expected Outage Costs by Cyber Attacks

6. 결 론

본 논문에서는 사이버 공격에 의한 잠재적 정전비용을 추정해보고자 하였다. 일단 정전이 발생했을 경우의 정전비용은 다양한 연구를 통해 추정되고 있지만, 실제로 사이버 공격에 의한 잠재적 피해요소가 얼마나 되는지 정량화하기 위한 노력은 상대적으로 거의 연구가 진행되고 있지 못하다. 이는 전력시스템의 계통과 통신 인프라 간에 상호작용을 정량화하는 작업으로서 차원이 다른 문제이고 상관관계가 분석된 경우가 거의 없기 때문에 까다로운 작업이라고 할 수 있다. 특히 사이버 보안 이슈의 경우는 다른 이슈와는 달리 정보공개가 거의 되지 않고 있기 때문에 이러한 측면에서 어려움이 있었다. 그러나 이러한 접근은 꼭 필요하며 향후 사이버 보안 설비를 구축하고 적정 투자선을 찾기 위한 합리적 근거를 마련해 줄 수 있을 것으로 판단된다. 보안의 경우는 지속적인 투자가 필요하고 상한선이 없기 때문에 이러한 근거가 마련되

지 못할 경우 과투자의 위험이 존재하기 때문이다. 본 논문은 그러한 측면에서의 첫 시도로서 비교적 간단한 사례연구를 통해 개념을 구조화했지만 향후 보다 심도 깊은 연구를 통해 이러한 위험평가를 자동화할 수 있는 툴을 설계해보고자 하며, 본 연구는 그러한 진행선상에서의 초석을 다지는 단계라고 나름의 의의를 부여할 수 있다. 사례연구를 통해서도 알 수 있듯이 해킹가능성이 낮지만 발생 시 피해규모가 큰 서버와, 해킹가능성이 상대적으로 용이한 개별 컴포넌트에 대한 균형 잡힌 보안대책 적용이 필요한 것으로 판단된다.

감사의 글

이 논문은 2009학년도 홍익대학교 학술연구진흥비에 의하여 지원되었음.

References

〔1〕 Schainker, R., Douglas, J., Kropp, T., "Electric Utility Responses to Grid Securities Issues", IEEE Power & Energy Magazine, March/April 2006.
〔2〕 Coutinho, M.P., Lambert-Torres, G., da Silva L.E.B., Lazarek, H., "Detecting Attacks in Power System Critical Infrastructure Using Rough Classification Algorithm", Proceedings of the First International Conference on Forensic Computer Science, No.1, Vol.1, November 2006, pps. 93~99, Brasil.
〔3〕 Bigham, J., Gamez D., and Ning Lu, "Safeguarding SCADA Systems with Anomaly Detection", V.Gorodetsky et al.(Eds.):MMM-ACNS 2003, LNCS 2776, pp.171-182, Springer-Verlag Berlin Heidelberg, 2003.
〔4〕 Pollet, Jonathan, "Developing a Solid SCADA Security Strategy", Plant Data Technologies, August 8, 2002.
〔5〕 Mitias Negrete-Pincetic, Felipe Yoshida, George Gross, "Towards Quantifying the Impacts of Cyber Attacks in the Competitive Electricity Market Environments", PowerTech 2009.
〔6〕 한국전기연구원, 인천대학교, "계통계획을 위한 산업용 수용가의 공급지장비 조사 연구", 산업자원부, 2008. 02.
〔7〕 Michael J. Sullivan et al, How to Estimate the Value of Service Reliability Improvements, http://certs.lbl.gov/pdf/lbnl-3529e.pdf.
〔8〕 한국전기연구원, TWBP 시장에서의 가격상한 설정에 관한 연구, 한국전력거래소, 2003.10.
〔9〕 W. E. Montgomergy(1972), "Markets in Licenses and Efficient Pollution Control Programs," Journal of Economic Theory, Vol.5, Issue 3, pp.395~418.

◇ 저자소개 ◇

김발호(金發鎬)
1962년 7월 12일생. 1984년 서울대학교 전기공학과 졸업. 1984~1990년 한국전력공사 전력경제연구실 근무. 1992년 Univ. of Texas at Austin 전기공학과 졸업(석사). 1996년 동대학원 졸업(박사). 현재 홍익대학교 전자전기공학부 교수.

강동주(姜東周)
1975년 9월 9일생. 1999년 홍익대 공대 전자전기제어공학과 졸업. 2001년 동대학원 전기정보제어공학과 졸업(석사). 2001년~현재 한국전기연구원 근무. 현재 홍익대학교 공대 전자전기공학부 박사과정 재학중.