정 보 보 호 학 회 지
제25권 제5호, 2015. 10

사이버 보안 관점에서의 전력시스템 신뢰도 기준 수립을 위한 NERC 규정 분석 및 국내 적용방안 연구

강 동 주*, 김 휘 강**

요 약

전력시스템은 설비계획 및 운영상의 신뢰도 확보를 위해 신뢰도 기준을 수립·적용하고 있다. 최근에 전력산업 및 스마트그리드에서의 사이버 보안이슈가 부각되면서, 신뢰도 기준에도 사이버 보안 관련 규정을 수립하기 위한 노력이 진행 중에 있다. 미국 전력산업의 경우, NERC라는 규제기관을 통해 사이버 보안과 관련한 신뢰도 기준들을 CIP(Critical Infrastructure Protection) 차원에서 수립하였으며, 이를 지속적으로 업데이트하고 있다. 우리나라의 경우는 아직까지 사이버 보안 관련 신뢰도 기준이 구체적으로 수립되지 않고 있으며, 이를 보강하기 위한 연구가 진행 중에 있다. 전력시스템에서의 사이버보안 이슈는 이를 모니터링하고 제어하기 위한 SCADA 시스템 및 기타 정보망 차원에서의 잠재적 위협과 더불어, 해당 정보인프라가 전력시스템과 상호작용함으로써 발생하는 복합적인 효과를 고려할 필요가 있다. 이러한 맥락에서 본 논문에서는 NERC 규정과 선행 연구사례들을 참고하여 국내적용을 위한 사이버 보안 신뢰도 기준수립에 대한 방향성을 제안하고자 한다.

Ⅰ. 서 론

SCADA 통신은 고유 프로토콜 기반의 전용망 상에서 이루어지고 있기 때문에 인터넷에 적용되는 어플리케이션 소프트웨어 차원의 보안정책 적용이 어려운 측면이 있다. 또한, SCADA 시스템의 실시간 특성을 고려할 경우 기존의 정보통신 시스템과는 차별화된 접근이 필요한데, SCADA 통신망의 위험은 2차적으로 물리적 전력계통에 영향을 주므로, 2가지 시스템 레이어 간 상호작용에 대한 이해가 필요하고 이를 위한 정량적 분석 모델이 필요하기 때문이다.

전용망에 한정됨으로써 보안 측면에서는 어느 정도 안전성을 확보했던 전력시스템은 AMI 도입 등에 따른 개방형 네트워크과 연계되고 있으며, IoT 개념과의 융합 과정에서 이러한 흐름은 더욱 가속화 될 것으로 전망된다. 스마트그리드 및 전력시장의 도입과 맞물려 각종 거래 데이터와 상업적 정보의 교환은 해킹에 대한 유인을 증가시킬 것이고 이에 대한 정부 차원에서의 대책이 필요하다. 그에 따라, 현존하고 있는 사이버 보안 위협은 더욱 심화되고 있으며, 이에 따라 전력망 신뢰도를 유지하기 위한 차원에서도 사이버 보안 문제도 보다 적극적으로 다룰 필요가 있다. 우리나라는 현재 신뢰도 기준을 수립하고 있는 단계에 있으며, 이 과정에서 사이버 보안 문제도 다루고 있다. 미국 신뢰도 규제기구인 NERC의 경우는 이미 사이버 보안 이슈를 전력시스템 신뢰도 측면에서 다루어 왔고, 이를 관련 규정에 반영하여 왔다 본 논문에서는 이러한 맥락과 선행연구에 근거하여 신뢰도 측면에서의 사이버 보안 규정수립 방향에 대한 검토해 본다.

Ⅱ. 사이버 보안을 위한 신뢰도 규정

전력계통 SCADA 시스템에서의 제어데이터부터 AMI 네트워크의 재무적 데이터에 이르기까지, 다양한 시스템 구성요소별로 보안 기술을 단계적으로 확보해 감으로써 현존하는 위험을 정확히 이해하고 대비할 필요가 있다. 아직까지 국내에서는 이러한 문제에 대한 체계적인 연구가 수행된 적이 없기 때문에 보다 명확한

* 한국전기연구원 (djkang@keri.re.kr)
** 고려대학교 (cenda@korea.ac.kr)

체계와 절차를 확립할 필요가 있다. 이러한 맥락에서 전력계통 신뢰도 측면과 연계하여 사이버 보안과 관련한 세부 기준을 수립할 필요가 있다.

2.1. NERC 관련 규정 분석

NERC 신뢰도 규정 중 전력시스템 운영과 연계되는 사이버 보안 관련 규정은 다음과 같다. 통신시스템 보안과 관련한 규정은 더 많지만, 본 논문에서는 전력시스템과의 상호작용과 관련한 내용에 국한하기로 한다. 다음은 주요 전력설비에 대해, 주요 책임당사자, 중요자산(critical asset) 및 중요정보자산(critical information asset)에 대한 내용들이다.

- **CIP‐002‐3** – Cyber Security – Critical Cyber Asset Identification (Responsible Entity)
- **CIP‐002‐3b** – Cyber Security – Critical Cyber Asset Identification (Critical Asset Identification Method)
- **CIP‐002‐3b** – Cyber Security – Critical Cyber Asset Identification (C. Measures)
- **CIP-002-5.1** – Cyber Security – BES Cyber System Categorization
- **CIP-002-5.1** – Cyber Security – BES Cyber System Categorization
- **CIP-002-5.1** – Cyber Security – BES Cyber System Categorization (4.2 Facilities)

상기 CIP-002-5.1 ‐ Cyber Security 중 별첨 형태로 되어 있는 Attachment 1 (Impact Rating Criteria)은 잠재적 사이버 사고의 Impact를 분석하는 내용이다. 이는 전력망-정보망의 상호작용 영향을 분석하는 내용으로 볼 수 있는데, 국내의 경우 NERC 안을 참고하여 국내 전압 및 시스템 계층별 적용기준을 수립하는 과정에 있다. 또한 같은 항목 내CIP-002-5.1 - Cyber Security - Guidelines and Technical Basis는 전력계통의 특정 운영 기능과 관련하여 책임 당사자(규제기관 및 시장참여자) 및 설비, 해당 기능을 담당하는 IT 설비에 대한 규정으로 전력계통에서의 특정 운영 기능 이상 시 원인 파악과 대응을 위한 가이드라인을 제시하고 있다. 이는 국내 전력계통에 대한 적용 시 계통운영보조서비스 관련된 내용으로 이해할 수 있다.

CIP‐002‐3b – Cyber Security – Critical Cyber Asset Identification는 중요자산을 정의하는 과정과 관련하여, 책임당사자들로 하여금 자체 수립한 위험평가 방법에 근거하도록 규정하고 있다. 하위 내용을 정리하면 다음과 같다.

- **R1.2.1.** 제어센터와 백업제어센터: 책임당사자(Responsible Entity)들이 수행하는 기능들을 총괄적으로 수행
- **R1.2.2.** 송전변전소: BES(Bulk Electric System)의 운영에 관여하는 송변전시설
- **R1.2.3.** 발전자원: BES 운영신뢰도에 영향을 주는 송전급 발전자원
- **R1.2.4.** 시스템 복구에 중요한 시스템이나 설비: Black Start 발전기나 초기시스템 복구의 중요 path에 위치한 송전선로나 변전시설
- **R1.2.5.** 공용제어시스템 하에서 300MW 이상의 자동부하감축을 수행할 수 있는 운전에 관여하는 시스템이나 설비
- **R1.2.6.** SPS(Special Protection System): BES 운영과 관련된 SPS 설비
- **R1.2.7.** 기타 BES 운영에 영향을 줄 수 있다고 판단하여 각 책임당사자가 위험평가에 포함시키는 설비

상기에 정의된 중요자산과 관련한 책임당사자의 역할과 관련해서는 다음과 같이 규정하고 있다.

- **M1.** 책임주체는 R1 요건에 따라 명세된 위험기반평가방법(risk-based assessment method)이 활용가능하도록 하여야 함.
- **M2.** 책임주체는 R2 요건에 따라 명세된 중요자산(critical asset)리스트가 활용가능 하도록 하여야 함.
- **M3.** 책임주체는 R3 요건에 따라 명세된 중요정보자산(critical cyber asset) 리스트가 활용가능 하도록 하여야 함.
- **M4.** 책임주체는 R4 요건에 따른 연별승인기록을 공개하여야 함.

중요자산의 정의에 이어 중요정보자산은 다음과 같이 정의된다. CIP-002-3b R3에서 중요정보자산은 주로 외부와의 연계기능에 초점을 맞추어 정의되는데, 최소한 다음의 1가지 속성을 포함하고 있도록 규정하고 있다.

1) 전자보안주변기기 외부와 통신하기 위한 라우팅 가능한 프로토콜 기반의 정보자산
2) 제어센터(control center) 내에서 라우팅 가능한 프로토콜을 사용하는 정보자산
3) 전화망으로 접근이 가능한 정보자산

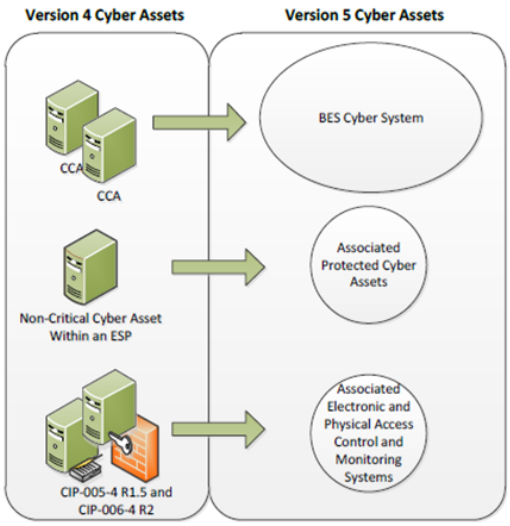
R4는 중요자산과 중요정보자산 지정과 관련한 연간 승인 문제에 있어서, 고위 간부 선에서 연 단위로 다음과 같은 내용을 제출하고 승인받도록 하고 있다.

(1) 위험기반평가방법(risk based assessment m-ethodology)
(2) 중요자산(critical asset) 및 중요정보자산(crit-ical cyber asset)에 대한 리스트에 대한 승인과정이 있어야 함.

CIP Cyber Security Standards와 관련하여 Version 4와 5의 가장 큰 차이는 기존 버전 4에서 중요사이버자산(Critical Cyber Assets)으로 규정하던 것을, 버전 5에서 BES사이버시스템(BES Cyber System)으로 규정한다는 것이다. 이러한 변화는 “NIST 위험관리프레임워크”에 대한 검토와 보안제어의 분류와 적용을 위한 대상으로서 “information system”이라는 유사용어를 사용한데서 기인한다. 즉, 특정정보자산의 물리적 실체보다는, 그러한 정보자산이 실제 BES 운영에 미치는 영향 기준으로 초점이 바뀌었다는 측면을 의미하는 것이고, 이는 사이버 보안에 있어서도 자산자체보다는 기능적 속성의 중요성을 보다 중시한다는 것이다.

버전 4→5 이전 과정에서, BES Cyber System은 단순히 Critical Cyber Assets의 grouping으로 볼 수 있다. CIP Cyber Security Standards “BES Cyber System” 용어 사용은 요건의 객체를 참조하기 위한 상위수준을 제공하기 위함이다. 예를 들어, 멀웨어 보호 시스템이 개별 정보자산에 적용되는 것이 아니라, 동일한 기능 수행을 위한 전체 시스템에 포괄적으로 적용되는 것을 의미한다.

신뢰도 규정은 송전급에 주로 적용되지만, 송전급에 영향을 미치는 배전서비스공급자와 관련하여 특별히 규정하고 있다. 배전서비스 공급자 중 BES 보호와 복구에 필요한 설비, 시스템, 장비 중 다음에 해당하는 것들 중 하나 이상을 보유한 사업자에 대해 신뢰도 규정의 적용을 받도록 한다.



〔그림 1〕 정보자산에 대한 규정 변화 (NERC)〔6〕

(1) Under-frequency load shedding & under-voltage load shedding (UFLS: 저주파수부하감축 & UVLS: 저전압부하감축)
- 부하감축 프로그램이 NERC나 지역신뢰도기준의 요건에 1개 이상 해당하는 경우
- 인간의 개입없이, 300MW 이상 용량으로, 책임주체에 의해 소유되는 공용제어시스템 하에서 자동부하감축(automatic load shedding)을 수행하는 경우

(2) NERC나 지역신뢰도기준의 요건에 1개 이상 해당하는 SPS나 기타 복구조치
- UFLS와 UVLS를 제외한 보호시스템이 1개 이상의 NERC나 지역신뢰도기준에 해당하는 송전시스템
- 복구 경로나 요소가 Black Start 자원이나 최초 연계점에 해당하는 경우

CIP-014-1 - Physical Security는 전력시스템 구성 설비들에 대한 물리적 보안 측면 보호 규정으로, 특정 설비와 관련한 물리적 사고 발생 시 전력계통 운영 측면에서의 대응 방안을 다루고 있으며, 발전설비, 송전선로 탈락사고와 cascading 위험 분석을 다루고 있다.

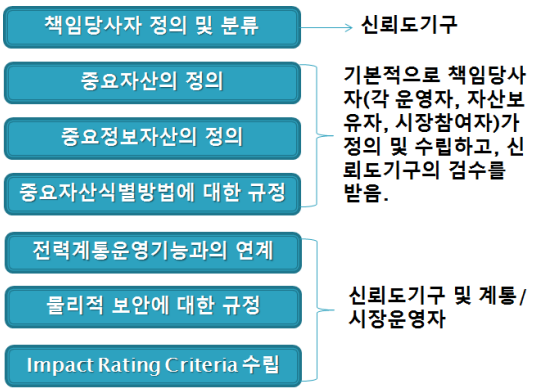
2.2. 국내 적용방안

국내적용에 있어서는 3.1절의 NERC 규정에 근거하

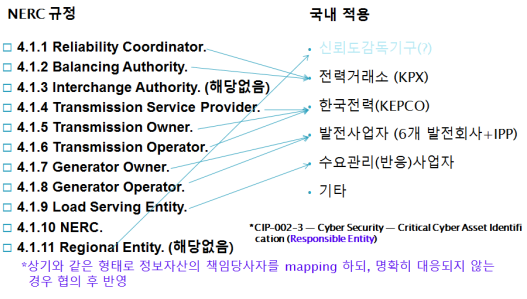
여 다음과 같은 신뢰도 기준안을 수립할 수 있다. 기본적으로 국내 시장에서의 책임당사자를 정의하고, 각 책임당사자들이 관리할 중요자산과 중요정보자산에 대한 정의가 필요하다. 이러한 과정에서 중요자산과 중요정보자산을 평가할 근거가 필요하며, 이러한 근거는 개념적 차원에서 범주가 정해지지만 사이버-물리 시스템(CPS: Cyber-Physical System) 기반으로 보다 상세한 평가가 필요하며, 이러한 과정은 다음 4장에서 소개된다. NERC안에 근거한 향후 국내 신뢰도 수립 기준은 다음과 같다.

NERC 규정을 참고하여 국내규정에 적용하는 과정에서의 이슈 중 하나는 책임당사자에 대한 정의이다. 비교적 유사하면서도, 미국과 우리나라의 시장구조 및 운영방식에 차이가 있기 때문에 약간의 수정이 필요하고, 다음과 같은 형태로 국내에 적용할 수 있다.

- 주부 제어센터 → 한국전력거래소(KPX), 송전급 변전소 → 한국전력
- 송전급시스템(Bulk Power Grid)에 직접 접속하는 발전설비 → 각 발전사업자 (접속설비 이슈에 따른, 한전과 발전사업자의 경계구분 필요) → 단 주기적인 평가 및 감독에 있어서 전력거래소가 관여
- 자체기동발전기(for Black Start) → 해당 발전사업자와 전력거래소
- 계통복구 경로에 해당하는 변전소 → 한국전력
- 300MW 이상급 부하관리설비와 연계된 시스템이나 시설 → 해당 수요관리사업자와 전력거래소 (*우리나라에선 기준 용량을 얼마로 할 것인가?)
- SPS: 해당 발전사업자, 전력거래소, 한전 → 관여하는 해당 자산에 대한 참여 주체들간 관할권 구분 필요



〔그림 2〕 국내 신뢰도 규정 수립 방향



〔그림 3〕 책임당사자에 대한 정의

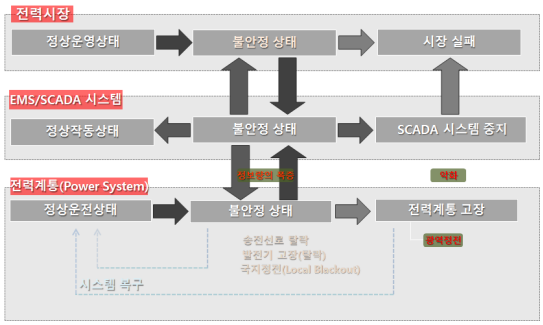
Ⅲ. 사이버 위협 영향 평가 및 CPS 기반 접근

3.1. 전력망-통신망 상호작용에 대한 연구배경

스마트그리드 보안은 기존의 통신분야에 한정된 보안 이슈와는 다른 특성이 있고 이를 제대로 이해할 필요가 있다. 스마트그리드는 전력시스템과 정보인프라로 구성되어 있는데, 여기서 전력시스템이란 발전, 송전, 배전을 포괄하는 물리적 에너지 생산 및 유통 서비스이고, 정보인프라는 SCADA-EMS를 중심으로 한 통신제어 시스템을 의미한다. 정보인프라와 전력인프라는 상호 연계되어 있으므로, 통신망에 유입된 사이버 위협이 어떻게 전력망에 영향을 미치는 정량적으로 분석할 수 있는 모델을 수립하는 것이 CPS 기반 연구의 주요 의의라고 할 수 있다. 스마트그리드에서의 보안 문제는 이러한 2가지 사이의 상호작용을 이해하는 것이 가장 중요하다고 할 수 있다.

전력인프라는 다시 전력계통, 전력시장 등의 다양한 계층으로 이루어져 있다. 전력시장은 전력계통을 운영하기 위한 IT 시스템 위에서 발생하는 일종의 전자상거래 기반으로 이루어지게 되며, 이는 IT 상의 보안위협이 전력계통 및 전력시장에까지 영향을 미칠 수 있음을 의미하는 것이다. SCADA 시스템과 전력계통 사이의 상호작용을 보다 상태도(state diagram) 형식으로 도식화하면 다음 그림과 같다. 이는 전력산업의 다양한 계층을 전력계통, SCADA 시스템, 전력시장의 3계층(layer)으로 분류하고, 계층 간의 운영 상태가 서로 다른 계층에 미치는 영향을 이해할 수 있다.

Chee-Wooi Ten과 Chen-Ching Liu는 CPS 기반으

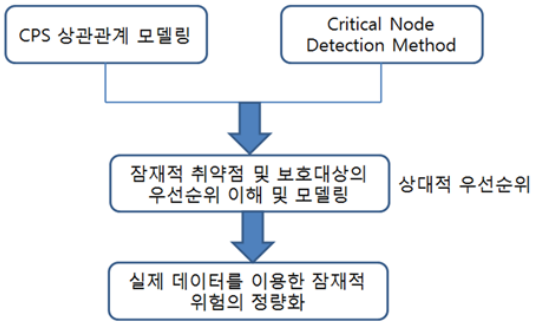


〔그림 4〕 전력시스템 계층 간 상호작용 프로세스

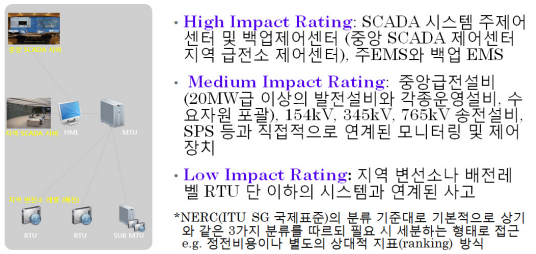
로 취약성을 평가하는 방법론을 제안하였다. 여기서 특정 공격 시나리오에 대해 통신망과 전력망을 각각 모의하고, 이에 대한 위험성을 시뮬레이션 결과에 근거하여 정량화하는 형태를 취하고 있다. 상기와 같은 시나리오에 따른 영향평가 방법론을 정리하면 다음과 같다. CPS 상관관계 모델을 통해, 특정 노드가 계통에 미치는 영향평가 측면(주로 수치상의 전압이나 전력용량)을 고려할 수 있고, 중요노드 추적법을 통해 네트워크 상의 위치에 따른 중요성을 정량적으로 측정할 수 있다.

아래 그림에서 보는 바와 같이 통신망과 전력망에 대한 시뮬레이션을 이원적으로 수행하고, 개별 변전소에 대한 제어능력 여부를 확인한 뒤, 제어능력이 없으면 다음 변전소로 넘어가고 제어능력이 있는 경우 공격 시나리오를 적용한다. 이는 외부 해킹공격에 의해, 해당 변전소의 제어능력이 임의의 외부공격자에게 넘어가는 시나리오를 상정한 것이다. 변전소에 대한 공격유형은 변전소에서 스위치를 개폐하는 형태로 이루어지는 형태로 가정할 수 있다.

NERC는 이러한 영향평가는 각 사업자가 근거자료를 만들고 평가를 수행하도록 하고 있으며, 해당 내용



〔그림 5〕 CPS 기반 중요자산 판별법



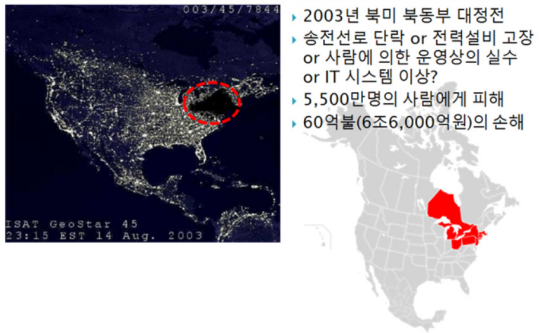
〔그림 6〕 전력계통에 대한 영향도 평가 등급 (3단계로 구분)

을 연 단위로 신뢰도 기구에 보고하고 평가받는 형태로 되어 있다. 신뢰도 규정 측면에서는 다음과 같이 3단계 수준으로 비교적 간단하게 구분하고 있다. 제어센터의 경우는 최상위 등급, 송전급은 중간 등급, 배전급 중 송전급에 영향을 미치는 설비에 대해서는 하위 등급이 부가된다.

3.2. 국내 적용방안

국내 신뢰도 기준 수립 시 중요자산에 대한 평가를 함에 있어서 우선은 NERC 규정상의 분류를 따르고, 더 세부적인 평가 및 상대적 우선순위 결정이 필요할 경우 본 연구의 이론적 방법에 따른 평가과정을 거쳐 중요도를 결정한다. 공급측과 달리 수요측에 물린 변전소를 평가할 경우는 공급용량이나 전압에 대한 기준을 적용하기 힘들기 때문에, 변전소 하단에 물리는 부하의 정전비용에 근거하여 위험의 정도를 결정한다. 우리나라의 경우는 주로 산업부하의 가치가 높기 때문에 부하군으로는 산업용 부하, 상업용 부하, 가정용 부하의 순으로 위험도의 우선순위가 결정된다.

북동부 대정전의 경우는 정전피해가 확산되는 대표적인 사례를 보인 것으로 설비운영상의 조치가 없을 경

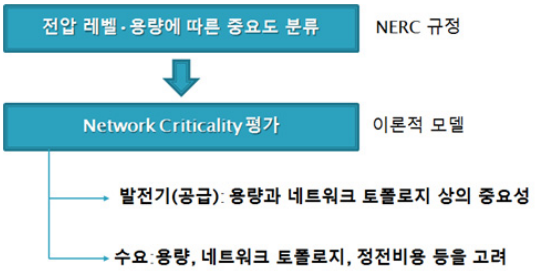


〔그림 7〕 북동부 대정전과 피해비용

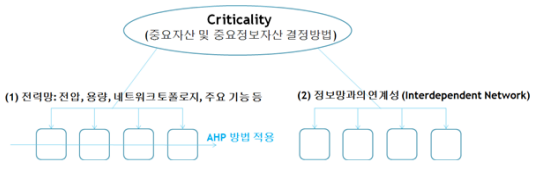
우 cascading failure에 의한 피해규모가 확산될 수 있음을 보인 것이다. 북동부 대정전의 경우, 임의사고(random outage)인가 사이버 공격에 의한 것인지에 대한 의견이 분분한 상태이지만 사고발생 최초지점에서의 네트워크 상황이나 후속대처(islanding)가 적절했다면 사고가 그렇게 확산되지는 않았을 것으로 판단된다.

현재 전력시스템의 사이버 보안 연구는 날로 증가하고 있는 우려에 비해 구체화되지 못하고 있다. 그것은 전력시스템과 정보망에서의 보안을 동시에 고려하지 못하고 있고, 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 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 정량화하거나 전문가들의 평가를 통해 중요도의 순서에 대한 랭킹을 정하는 방법이 있다.

실무적인 규정 차원에서는 NERC의 규정에 따라 전압 및 규모 수준으로 분류하는 방법과, 이론적인 방법으로는 네트워크 상에서 해당 노드의 중요성을 평가함으로써 세부 노드별로 평가하는 방법을 조합에서 사용할



〔그림 8〕 영향 평가 방법 (전압레벨, 설비용량, 네트워크 토폴로지, 정전비용 등을 고려)



〔그림 9〕 AHP 기반 중요노드(중요자산 및 중요정보자산) 평가 방법

수 있다. 이러한 방법은 정성적 속성을 정량적으로 평가하는 방법의 하나인 Analytic Hierarchy Process (AHP)를 사용할 수 있는데, 전력시스템의 경우는 정보자산의 침해가 곧 전력계통의 운영과 신뢰도에도 영향을 줄 수 있기 때문에 이러한 잠재적 피해비용을 자산에 반영해 줄 필요가 있다. 전력분야에서의 피해비용은 정전비용으로 귀결되기 때문이다.

Ⅳ. 결 론

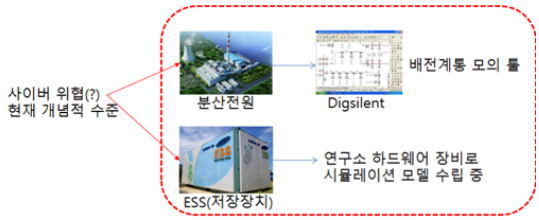
현재 사이버 보안 관점에서의 신뢰도 규정 수립 연구는 NERC 규정을 분석하고, 선행 연구결과를 바탕으로 국내 기준안을 수립하고 있는 시점에 있다. 더불어, 사이버 위협으로부터의 기인할 수 있는 위험을 평가하기 위해, CPS 기반에서 전력망과 정보망의 상호관계에 대한 다양한 이론적 연구를 분석하고 있다. 상호작용 영향평가에 대한 방법론은 기본적으로 각 책임당사자가 수립하도록 NERC 규정에 명시되어 있는바 본 연구에서는 적용 가능한 다양한 기법을 제안함으로써 향후 중요자산 및 중요정보자산 평가에 도움이 될 수 있는 근거 참고자료를 제안하는데 초점을 맞추고 있다.

CPS 기반으로 위험을 평가함에 있어서 연역적이고 절대적인 정량값을 산출하는 솔루션을 얻기란 현실적으로 불가능하기 때문에, 후보 시나리오를 선정하고 그에 대한 상대적인 평가를 하는 것이 실용적인 대안이 될 수 있다. 대표적으로는 임의의 발전소가 탈락한다고 가정했을 때, 이것이 계통에 미치는 영향을 시뮬레이션 툴로 모의하는 것이다. 대상은 기본적으로 중앙급전 발전기가 된다.

이외 대규모 신재생에너지 발전기의 경우도, 신뢰도에 영향을 줄 수 있는 공격 대상이 된다. 이 경우는 발전기를 탈락시킬 정도가 아니라도, 단순히 측정 데이터를 조작하는 것만으로도 시스템 균형에 영향을 줄 수 있다. 풍력발전은 그 변동성으로 전력계통에 주는 영향

〔그림 10〕 발전소 탈락 공격 시나리오

〔그림 11〕 풍력단지 공격 시나리오



〔그림 12〕 분산전원/ESS 공격 시나리오

도 크고, 중앙에서의 통제성이 약하며, ICT와의 연계성이 크기 때문에 주요 이슈가 될 수 있다.

배전계통 수준에서 접속되는 분산전원이나 수요도 임계치를 넘을 경우 신뢰도에 위험을 줄 수 있다고 가정한다. 특히, 분산전원이나 ESS는 ICT 설비와의 연계성이 크므로 그만큼 잠재적 위협이 크다고 할 수 있다.

해외의 경우 전력시스템에 대한 보안연구는 CPS의 개념 하에서 전력계통(제어시스템)과 SCADA(IT시스템) 간의 상호작용을 시뮬레이션을 수행하는 형태로 옮겨가고 있다. 스마트그리드의 경우에는 과거의 공격사례와 그로 인한 피해에 대한 데이터 확보가 용이하지 않고, 실제 시스템 상에서 테스트를 수행할 수도 없기 때문에, 테스트베드를 구축하여 다양한 시험과 시나리오를 예상해보는 과정이 필요하다. 따라서 신뢰도 규정에서 위험에 대한 세부적인 기준을 모두 제안하기는 현실적으로 불가능하므로 책임당사자들이 개별 중요자산 및 중요정보자산에 대한 위험도 평가와 그에 대응할 수 있는 지속적인 보안대책 확보 노력이 필요하다고 판단된다,

참 고 문 헌

[1] Tianbo Lu, Jinyang Zhao, Lingling Zhao, Yang Yi, and Xiaoyan Zhang, “Security Objectives of Cyber Physical Systems”, 2014 7th International Conference on Security Technology

[2] Hahn, A. Ashok, A. Sridhar, S. Govindarasu, M. “Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid,” Smart Grid, IEEE Transactions on, p847-855, 2013

[3] 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

[4] 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, 2010

[5] Dong-Joo Kang, Jong-Joo Lee, Seog-Joo Kim, Jong-Hyuk Park, *Analysis on cyber threats to SCADA systems*, Transmission & Distribution Conference & Exposition: Asia and Pacific, 2009

[6] NERC CIP Standards

[7] David Kuipers and Mark Fabro, *Control Systems Cyber Security: Defense in Depth Strategies*, Idaho National Lab, 2006

[7] Deepa Kundar, Xianyong Feng, Shan Liu, Takis Zourntos, Karen L. Butler-Purry, *Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid*, 1st IEEE International Conference on Smart Grid Communications (SmartGridComm), 2010

[8] Jianli Pan, *A Survey of Network Simulation Tools: Current Status and Future Developments*, http://www.cse.wustl.edu/~jain/cse567-08/ftp/simtools.pdf

〈저 자 소 개〉

강 동 주 (Kang Dong Joo)
정회원

1999년 2월 : 홍익대학교 전자전기제어공학과 학사
2001년 8월 : 홍익대학교 전기정보제어공학과 석사
2012년 2월 : 홍익대학교 전기정보제어공학과 박사
2001년 9월~현재 : 한국전기연구원 선임연구원
2012년 9월~현재 : 고려대학교 정보보호대학원 박사과정
관심분야 : 스마트그리드 정보보호, 전력시장 시뮬레이션, 소셜 네트워크

김 휘 강 (Kim Huy Kang)
종신회원

1998년 2월 : KAIST 산업경영학과 학사
2000년 2월 : KAIST 산업공학과 석사
2009년 2월 : KAIST 산업및시스템공학과 박사
2004년 5월~2010년 2월 : 엔시소프트 정보보안실장, Technical Director
2010년 3월~현재 : 고려대학교 정보보호대학원 조교수
관심분야 : 온라인게임 보안, 네트워크 보안, 네트워크 포렌식