情 報 保 護 學 會 誌
第22卷 第5號, 2012. 8

스마트그리드에서의 CPS (cyber-physical system) 시뮬레이션 구현을 위한 제반 연구이슈 및 방법론 검토

강 동 주*, 김 휘 강**

요 약

스마트그리드는 전력시스템과 이를 제어하기 위한 통신 인프라를 중심으로 다양한 시스템이 서로 통합되는 종합적인 플랫폼으로 이해할 수 있다. 기존에 각기 독립적으로 운영되는 시스템과 통신 인프라가 통합되기 시작하면서 다양한 상호작용이 파생되고 그로 인해 잠재적인 보안 측면의 위험성도 커지게 된다. 전통적인 전력시스템은 폐쇄적인 SCADA 네트워크를 기반으로 운영되었기 때문에 최소한의 보안강도가 보장되었지만, 스마트그리드 하에서는 개방형 통신망과 연계되면서, 기존의 사이버 보안 위협들이 전력시스템으로 유입하게 된다. 기존의 IT 시스템과는 달리 전력시스템과 같은 제어시스템은 물리적 작동과 공정이 수반되기 때문에 새로운 위험이 발생하기도 하고 기존의 위험이 증폭되기도 한다. 전력시스템에서는 가용성이 그 무엇보다 중요하기 때문에, 스마트그리드 체제하에서의 다양한 위협요인을 미리 파악하고 이에 대비한 계획을 수립함으로써, 그러한 가용성의 수준을 유지할 필요가 있다. 이를 위해서는 기존의 사이버 위협이 어떠한 경로를 통해 전력시스템에 영향을 미치게 되며 그로 인한 잠재적 위험이 얼마나 되는가를 평가할 필요가 있다. 그러나 스마트그리드는 아직까지 구축중인 미래형 시스템이고 누적된 과거 데이터가 없기 때문에 가상의 하드웨어 기반 테스트베드 내지 소프트웨어 기반의 시뮬레이션 모델을 통해 이를 사전적으로 테스트할 필요가 있다. 또한 스마트그리드는 서로 다른 IT 시스템과 물리적 설비들이 결합되는 복잡한 시스템이라는 측면에서, 잠재적으로 발생 가능한 다양한 위험을 분석하고 평가할 수 있는 모델의 수립이 요구된다. 본고에서는 그러한 CPS 기반 시뮬레이션 모델에 대한 현재의 연구동향을 검토하고, 향후 실질적으로 구현하기 위한 방안을 제안하고자 한다.

Ⅰ. 서 론

사이버-물리시스템(Cyber-Physical System, 이하 CPS)이란 하나의 시스템 상에서 사이버 계층과 물리적 계층이 서로 긴밀하게 조합을 이루어 상호작용하고 있는 시스템을 의미하고 이러한 과정에서 컴퓨팅, 네트워킹, 물리적 공정이 결합하는 개념이다. 여기서의 사이버 계층이란, 전산기반의 시스템, 소프트웨어 계층 통신 네트워크 등을 의미하는데, 산업용 제어시스템 분야에서 통상적으로 이러한 역할을 수행하는 통신 인프라를 SCADA 시스템으로 통칭하고 있다. 물리적 계층이란 사이버 계층의 모니터링 및 제어를 받으면서 물리적인 동작이나 기능을 수행하는 시스템을 의미한다. 현대 문명의 근간을 이루고 있는 주요 인프라들, 전력, 가스, 열 등과 같은 에너지 시스템, 상하수도, 교통 등이 대표적인 사례이다. 한 때 유행했던 유비쿼터스란 개념도 이러한 사이버-물리시스템 연계 개념의 연장선상에 있다고 볼 수 있으며, 주요 인프라 뿐만 아니라 삶의 다양한 서비스 분야로까지 전방위적으로 확장된 미래 비전으로 해석할 수 있다.

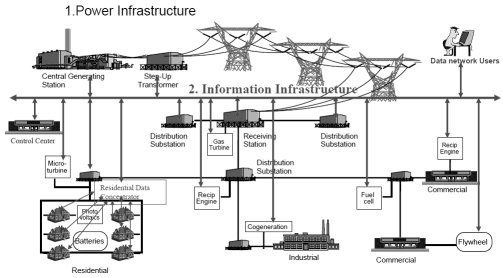
스마트그리드란 개념은 최근 전 지구적인 기후변화와 화석에너지 고갈에 대한 위기감이 커지면서 주목을 받기 시작하였고, 유명한 저널리스트인 토마스 프리드만이 그의 저서인 '코드그린'에서 사용하면서 유명해졌고 이후 보편적으로 사용되고 있다. 프리드만은 해당 저서에서 스마트그리드를 에너지 인터넷이라고 개념화하고 있는데, 이는 인터넷이 다양한 지역적 통신 네트워크를 연계하여 글로벌 네트워크화 되었듯, 에너지 시스템

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

도 다양한 에너지원과 지역적인 에너지 시스템을 하나로 통합하여 언제 어디서든 효율적인 방식으로 에너지를 사용할 수 있도록 하는 것이다. 통신 네트워크가 TCP/IP라는 프로토콜로 표준화되었듯이, 다양한 에너지원은 전기에너지로 표준화되고 있는 시점에 있고, 스마트그리드 기반의 전력시스템은 이러한 목표를 구현하기 위한 다양한 통합 기술의 장이 되고 있다. 문제는 이러한 과정에서 워낙 다양한 통신 네트워크와 물리적 설비·기기들이 연계되다 보니, 운영이나 보안 측면에서도 수많은 변수가 생겨난다는데 있다. 시스템의 복잡도가 증가할수록 외란에 의한 불확실성은 증가하게 되며, 이는 시스템의 신뢰성이나 보안을 유지하는데도 큰 난제가 될 것으로 전망된다. 특히, 스마트그리드는 수많은 이종 시스템의 결합체로서 일관된 보안정책을 적용하기가 어려우며, 통신 시스템에서는 허용되는 약간의 통신 지연도 동기화된 전력시스템에서는 광역정전을 유발하는 치명적인 요인으로 작용할 수 있기 때문이다. 그러나 현재 스마트그리드와 관련된 보안연구는 대부분 기존의 정보통신 네트워크 상에 머물고 있으며, 전력시스템과의 상호작용을 고려하지 못하고 있다. 전력시스템에서는 가용성이 가장 중요하기 때문에 사전적인 방어 못지않게 공격 이후의 완화 및 복구대책이 중요하고, 이는 CPS 측면에서 사이버 보안을 연구해야 하는 중요한 이유이기도 하다. 이러한 맥락에서, 스마트그리드의 CPS를 연구하기 위한 방법론적인 틀을 분석하고 향후 구현 방법을 제안하고자 한다.

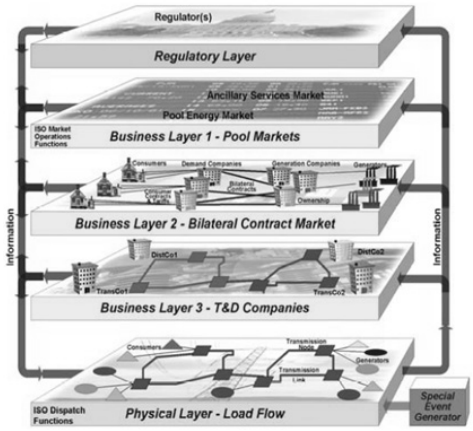
Ⅱ. 스마트그리드에서의 보안 특성

스마트그리드 보안은 다른 산업분야와는 다른 특성이 있고 이를 제대로 이해할 필요가 있다. 스마트그리드는 전력시스템(power infrastructure)과 정보인프라(information infrastructure)로 구성되어 있는데, 여기서 전력시스템이란 발전, 송전, 배전을 포괄하는 물리적 에너지 생산 및 유통 서비스이고, 정보인프라는 SCADA-EMS[1]를 중심으로 한 통신제어 시스템을 의미한다[그림 1][1]. 스마트그리드에서의 보안 문제는 이러한 2가지 사이의 상호작용을 이해하는 것이 가장 중요하다고 할 수 있다.



〔그림 1〕 스마트그리드의 주요 2가지 인프라

전력산업은 [그림 2][2]에서 보는 바와 같이 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. 전력시장을 운영하기 위해서는 상기의 제어시스템뿐만 아니라 과금을 위한 AMI[2]와 시장운영 관련 시스템이 필요하기 때문에 [그림 2]와 같은 다층적 구조를 구현하기 위해서 물리적으로는 통신 네트워크 상에서 이종 시스템 간 연계가 발생하게 된다.



〔그림 2〕 전력산업의 계층적 구성도

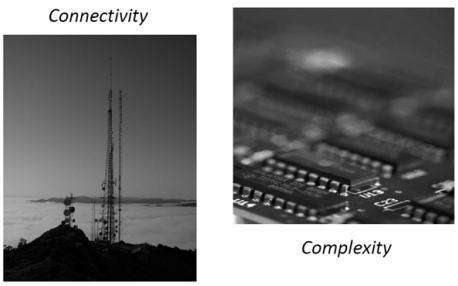
전력계통이 스마트그리드 하에서 보다 다양한 구성요소 및 통신 네트워크와 연계되면, 이러한 계층구조는 더욱 복잡해질 것이다. 따라서 이렇게 증가하는 연결성과 그로 인해 증가하는 복잡성의 맥락에서 기존의 IT

1) Energy Management System.

2) Advanced Metering Infrastructure.

시스템 상에서의 보안위협이 어떻게 전력계통으로 전이되는지를 이해할 필요가 있다. 연결성의 증가로 인해 시스템이 거대화되고 접속점이 증가하여 그만큼 위협요인이 침입할 루트가 많아지게 되고, 복잡성으로 인해 특정 위협에 대한 일관된 보안정책을 적용하는 것이 힘들어지게 된다. 스마트그리드 체제하에서 이렇게 증가하게 되는 연결성 및 복잡성과 더불어 전력시스템 운영의 실시간성은 기존 보안 위협이 스마트그리드로 유입되는 과정에서 다양한 변태를 일으키게 될 가능성이 높다고 할 수 있다.

- **위험의 2가지 측면: 연결성과 복잡성**
- **연결성: EMS의 직접적(물리적) 연계면 분석**
- **복잡성: 간접적인 연결(EMS-SCADA-말단기기: 데이터의 무결성 측면)과 위협의 다양성**

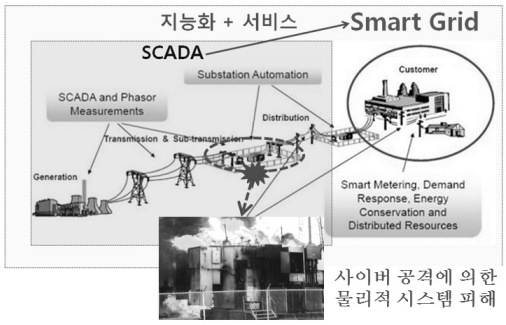


〔그림 3〕 스마트그리드에서 증가하는 연결성과 복잡성[3]

더불어, SCADA 시스템에 최종소비자들이 편입되면서 공용 통신망과의 연계는 피할 수 없는 대세가 되고 있으며, 최종소비자단에서 많은 접점이 생겨나면서 그만큼 잠재적인 위협이 유입되는 경로가 점차 다양해지고 있다. 홈 네트워크 기반의 스마트 홈이 확장되고 최종소비자들이 전력시장의 능동적 주체로 참여하게 되면 프라이버시 이슈와 더불어 사이버 보안에 대한 잠재적 위협 요인은 더욱 증가할 것으로 전망된다.

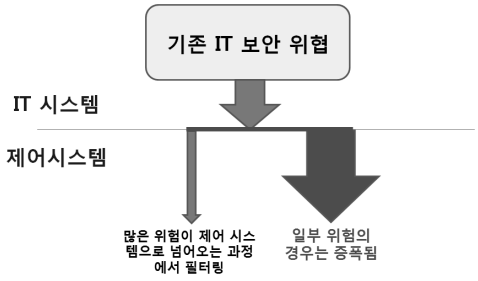
외부망과 연계된 홈 네트워크를 플랫폼으로 하여 실시간요금제(RTP[3])의 적용과 수요반응, 스마트 미터링을 통한 에너지 사용량의 측정과 과금체계 등이 폭넓게 적용될수록 최종소비자와 전력시스템의 상호작용성은 강화될 것이기 때문에 이에 대한 대비가 필요하다. 이러한 환경에서 기존 IT 시스템의 다양한 위협들이 스마트그리드로 유입될 것으로 우려된다.

3) Real Time Pricing.



〔그림 4〕 최종소비자와의 연계와 사이버 위협 증대

두 시스템의 특성이 매우 상이하기 때문에, [그림 5]에서는 보는 바와 같이 일부 위험성은 제어시스템으로 적용되는 과정에서 오히려 약화될 것이고 일부 위험은 그러한 과정에서 증폭될 수 있다.

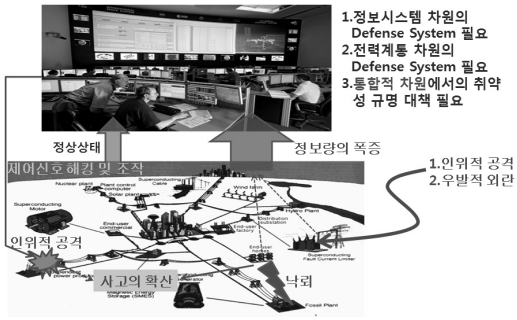


〔그림 5〕 IT 보안위협의 제어시스템 적용과정

IT 시스템 상에서 요구되는 정보의 기밀성은 제어시스템 상에서는 상대적으로 중요도가 떨어질 수 있는데, 이는 제어데이터 자체의 경우는 직접적인 재무적 가치와의 연계가 떨어지기 때문이다. 대신 가용성이 매우 중요한데 이러한 측면에서 IT 시스템에서는 허용되는 일정 수준의 통신지연도 제어시스템 상에서는 큰 문제를 초래할 수 있다. 그러므로 보안솔루션을 적용하는 과정에서도 이러한 가용성을 고려하여 솔루션 자체가 너무 무겁지 않도록 하여야 한다. 보안의 강도가 높아질수록, 적용 솔루션의 수가 많아질수록 가용성을 저해할 측면이 크기 때문에 보안강도와 가용성 사이의 최적화된 균형이 중요하다.

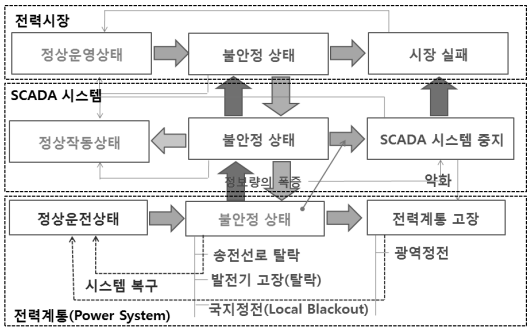
이와는 대조적으로 [그림 6]에서와 같이, 사이버시스템(통신망)과 물리시스템(전력계통)의 상호작용을 이용하여, 역으로 전력시스템을 먼저 공격하여 bottom-up 방식으로 제어정보망을 이상을 유도하는 형태도 가능하

다. 제어시스템은 고장시(비상시)에 데이터가 폭주하는 특성이 있기 때문에 이를 이용하여 정보시스템에 과부하를 걸리게 할 수 있다.



〔그림 6〕 SCADA와 전력계통의 상호작용

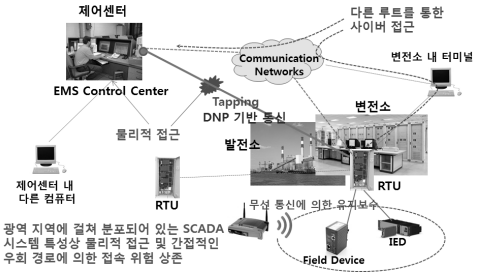
SCADA 시스템과 전력계통 사이의 상호작용을 보다 상태도(state diagram) 형식으로 도식화하면 [그림 7]과 같다. 이는 [그림 2]에서와 같은 전력산업의 다양한 계층을 전력계통, SCADA 시스템, 전력시장의 3계층(layer)으로 분류하고, 계층 간의 운영 상태가 서로 다른 계층에 미치는 영향을 이해할 수 있다. SCADA 시스템에 대한 보안 위협은 상위의 전력시장 운영 및 하위의 전력계통 운영 모두에 영향을 줄 수 있으며, 반대로 전력시장과 전력계통 운영의 이상이 잘못된 정보와 데이터 부하를 전달하여 [그림 6]에서와 같은 유형의 이상을 초래할 수도 있다.



〔그림 7〕 전력시스템 계층 간 상호작용 프로세스

Ⅲ. 스마트그리드에서의 사이버 위험과 정량적 모델링

전력시스템은 기본적으로 다음 그림과 같은 구성을 가지며, 이러한 기반시설이 외부의 공용 네트워크와 연계될 때 스마트그리드 버전으로 진화하게 된다. 크게 3부분으로 구분될 수 있는데, 제어센터와 말단기기(RTU와 IED) 그리고 2개 통신단을 연결하기 위한 통신 채널로 구분할 수 있다. 따라서 사이버 위험도 이러한 3가지 구역에 대해 적용될 수 있다.



〔그림 8〕 SCADA 시스템의 구성과 잠재적 위협

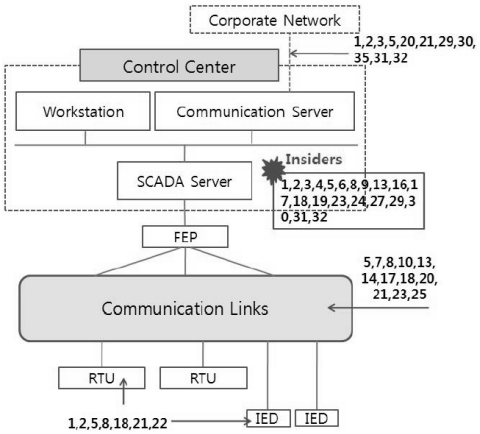
이와 더불어, 스마트그리드에서의 사이버 위험을 평가하기 위한 연구도 진행 중인데, 기존 IT 시스템 상에서의 위협 요인들이 스마트그리드에 어떻게 전이되는지에 대한 기초적인 연구를 수행하는 형태로 진행되고 있으며, 기존의 개별 사이버 위협을 SCADA 시스템에 대응시키기는 형태로 진행되고 있다[3].

〔표 1〕 대표적인 사이버 위협요인

1. Authorization Violation	9. Information leakage	17. Sabotage	25. Traffic Analysis
2. Bombs (Logic or Time)	10. Intercept/ Alter	18. Scavenging	26. Trap Door/ Back Door
3. Browsing	11. Interference Database Query Analysis	19. Spying	27. Trojan Horse
4. Bypassing Controls	12. Masquerade	20. Service Spoofing	28. Tunneling
5. Data Modifications	13. Physical Intrusion	21. Sniffers	29. Unauthorized Access Violations of Permission
6. Denial of Service	14. Replay	22. Substitution	30. Unauthorized Access Piggybacking
7. Eavesdropping	15. Repudiation	23. Terrorism	31. Virus
8. Illegitimate Use	16. Resource Exhaustion	24. Theft	32. Worm

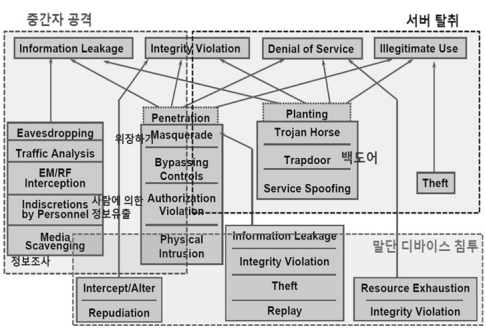
공격 유형들이 시스템 구성요소별로 명확하게 구분되지 않는 측면도 있지만 IT 시스템 상의 사이버 위협들을 전력시스템과 연계하기 위한 초기시도라는 측면에서 의미를 가진다고 볼 수 있다. 또한 이러한 접근방식

은 시스템의 연결성이나 구성요소가 고도화 될수록 어려워지는데, 예를 들어 현재의 RTU가 IED로 고도화되면 더 많은 기능과 연결성을 가지게 되고 이는 더 많은 위협에 노출되는 결과를 초래할 것이기 때문이다.



〔그림 9〕 SCADA 시스템에 대한 위협 적용

S. Massoud Amin 역시 유사한 주제에 대해, 전력시스템 전문가의 관점에서 상기의 위협 요인들이 스마트그리드의 기밀성, 무결성, 가용성 측면에서 어떻게 분류될 수 있는가를 소개하였다[그림 10][4].



〔그림 10〕 스마트그리드에서의 사이버 위협 적용 분류

이러한 선행연구에 근거하여 이를 표 내지 행렬 형태로 정리하면 다음 [표 2]와 같다. [표 1]과 [그림 10]에서의 위협유형들 중에서 중복되고 유사한 유형들을 정리하여 15개로 축약하고, 이들 유형들이 각 시스템 도메인(domain) 별로 적용가능한지 여부에 대해 구분하였다. 적용되는 곳은 1(채색된 셀), 적용되지 않는 곳은 0(투명한 셀)으로 하여 취약성 여부를 평가해 볼 수 있다. 해당 위협이 해당 도메인에 적용된다면 그 부분은 특정 위협에 대해 취약성을 가진다는 의미이다. 예를 들어, DoS 공격은 SCADA 시스템에서도 TCP/IP를 사용하는 상위 통신 구간에는 적용되지만, 하위단의 시리얼 통신 구간에서는 적용되지 않는다. 시리얼 통신에는 라우팅 기능이 존재하지 않고, 정해진 시간 주기로 1:1 통신이 이루어지거나, 1:n일 경우는 브로드캐스팅 방식으로 이루어지기 때문이다. 물론 데이터 사이즈 자체가 너무 커지거나 통신시간이 지연되면 통신자체가 불능이 될 수 있다.

〔표 2〕 위협들과 SCADA 구성요소 간 대응관계

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

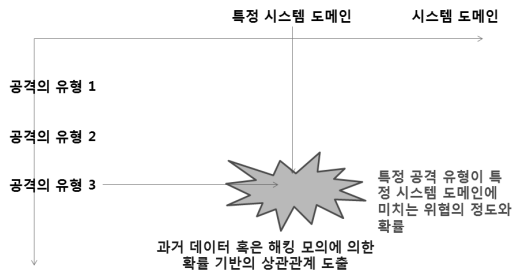
위협요인이 정의되면, 위협, 취약성, 자산이 조합되어 발생 가능한 위험(Risk)도 정의될 수 있다. 위협을 T(Threat), 취약성을 V(Vulnerability), 자산을 A(Asset)로 표기하면, 위험 R(Risk)은 다음 식 (1)과 같이 정식화된다. 해당 식은 다양한 분야의 위험평가에서 일반적으로 사용되는 수식으로서 최종적으로는 화폐단위로 표현된다.

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

이 식에 상기 [표 2]를 적용하면, 다음 그림에서와 같

이 행렬식으로 표현될 수 있다. 이러한 정식화 과정에 기반하여 위험을 정량적으로 평가할 수 있고, 정량적으로 평가된 위험은 보안 솔루션을 적용하기 위한 기술적·경제적 최적가치를 판단하기 위한 기준 근거로 활용될 수 있다.

[표 2]의 행렬은 특정 위협이 특정 시스템 도메인에 어떠한 영향이나 위험을 주는지에 대한 일종의 정량적 함수관계를 평가할 수 있는 틀을 제공하며, [그림 11]과 같은 개념으로 도식화되는데 여기서의 중요한 문제는 그러한 관계의 정량적 수치를 산출하는 것이라고 할 수 있다.



〔그림 11〕 위협(공격)과 시스템 도메인의 연계

[그림 12]는 [그림 11]의 위험 평가과정을 행렬대수식(matrix algebra) 형태로 정식화한 것이다.

$$R = T \times V \times A$$

위험 위협 취약성 정보자산

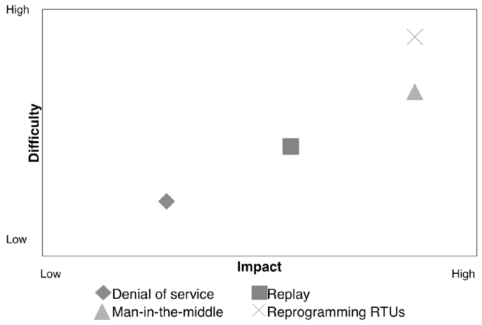
$$\begin{bmatrix} R_1 \\ R_2 \\ R_3 \\ R_4 \end{bmatrix} = \begin{bmatrix} T_{0101} & T_{0201} & T_{0301} \cdots & T_{1001} & T_{1101} & T_{1201} & T_{1301} & T_{1401} & T_{01501} \\ T_{0102} & T_{0202} & T_{0302} \cdots & T_{1002} & T_{1102} & T_{1202} & T_{1302} & T_{1402} & V_{1502} \\ V_{0103} & V_{0203} & V_{0303} \cdots & V_{1003} & V_{1103} & V_{1203} & V_{1303} & V_{1403} & V_{1503} \\ V_{0104} & V_{0204} & V_{0304} \cdots & V_{1004} & V_{1104} & V_{1204} & V_{1304} & V_{1404} & V_{1504} \end{bmatrix} \begin{bmatrix} V_{0101} & V_{0102} & V_{0103} & V_{0104} \\ V_{0201} & V_{0202} & V_{0203} & V_{0204} \\ V_{0301} & V_{0302} & V_{0303} & V_{0304} \\ V_{0401} & V_{0402} & V_{0403} & V_{0404} \\ V_{0501} & V_{0502} & V_{0503} & V_{0504} \\ V_{0601} & V_{0602} & V_{0603} & V_{0604} \\ V_{0701} & V_{0702} & V_{0703} & V_{0704} \\ V_{0801} & V_{0802} & V_{0803} & V_{0804} \\ V_{0901} & V_{0902} & V_{0903} & V_{0904} \\ V_{1001} & V_{1002} & V_{1003} & V_{1004} \\ V_{1101} & V_{1102} & V_{1103} & V_{1104} \\ V_{1201} & V_{1202} & V_{1203} & V_{1204} \\ V_{1301} & V_{1302} & V_{1303} & V_{1304} \\ V_{1401} & V_{1402} & V_{1403} & V_{1404} \\ V_{1501} & V_{1502} & V_{1503} & V_{1504} \end{bmatrix} \begin{bmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \end{bmatrix}$$

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

〔그림 12〕 위험(Risk)의 정식화

사이버 보안의 특성상 과거 경험에 대한 데이터를 얻기가 쉽지 않은데다 스마트그리드의 경우는 미래 시스템이고 전력시스템 환경에 따라 그러한 데이터가 천차만별로 편차를 보일 수 있기 때문에, 그나마 존재하는 데이터의 활용도 쉽지 않다. 이러한 맥락에서 생각할 수 있는 대안 중의 하나로 위협(공격)유형별로 잠재적 위험과 난이도의 상대적 크기를 비교하여 순위를 매기는 방식이 있을 수 있다.

Mattias Negrete-Pincetic은 대표적인 4가지 사이버 공격 유형들에 대한 상대적인 비교연구를 수행하였다 [그림 13][5]. 그러나 이러한 위험에 대한 상대적인 크기는 시스템 도메인에 따라 달라질 수 있는데, 예를 들어 DoS 공격의 경우 일반 IT 시스템에 비해 제어시스템에서는 가용성 훼손으로 훨씬 큰 피해를 초래할 수 있다.



〔그림 13〕 Impact vs. Difficulty Chart

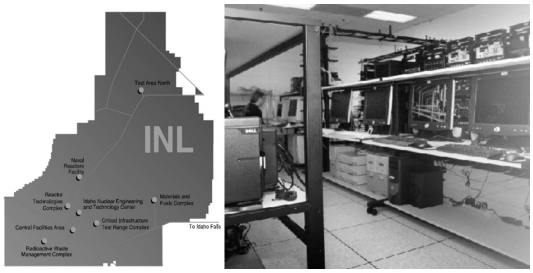
선행연구를 참고해 볼 때, 과거의 데이터에 의존하여 위험평가에 필요한 수치를 얻는 것은 무의미해보이며, 이러한 맥락에서 테스트베드 및 CPS 시뮬레이터 구축 필요성이 제기된다. 실질적으로 세계 각국에서는 스마트그리드의 보안 위험을 평가하기 위해 CPS 기반의 시뮬레이터를 구축하기 위한 노력을 진행 중에 있으며, IV절에서 이러한 내용에 대한 연구 동향과 개념적인 제안을 소개하고자 한다.

Ⅳ. 스마트그리드 CPS기반 시뮬레이터

4.1 국외 연구 사례 (방법론 및 구현 시스템)

스마트그리드 사이버 보안과 관련하여 가장 앞서 있는 미국에서는 National Lab들을 중심으로 관련 연구가 진행되고 있는데, 특히 전력 SCADA 시스템의 사이버

보안 관련 테스트베드 분야에서는 INL과 SNL을 들 수 있다[4]. INL은 국가인프라테스트베드(CITR : Critical Infra Test Bed)를 구축하였는데, 이를 통해 국가의 인프라 시스템을 테스트하고 테러리스트들의 사이버 공격에 대한 대응을 모의해 볼 수 있게 하였다. CITR은 여러 가지 하위 시뮬레이션 설비를 포함하고 있는데, [그림 14]는 INL의 사이버 보안과 관련한 테스트베드를 보이고 있다.



〔그림 14〕 INL의 사이버 보안 테스트베드

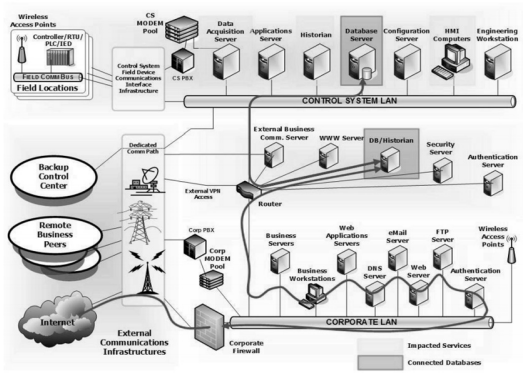
INL에서는 이와 같은 테스트베드에 근거하여 제어시스템에 적용되는 기기(임베디드 펌웨어 기반)들을 중심으로 사이버 위험요인들을 테스트하였고 다음과 같은 주요 이슈들을 선정하였다.

- 네트워크 장치의 백도어(backdoor)와 보안상 문제점(security hole)
- 공개 프로토콜 상의 취약성
- 필드 디바이스(field device)에 대한 공격
- 데이터베이스(database) 공격
- 통신 하이재킹(hijacking)과 중간자 공격

보안대책과 폐쇄성이 높은 SCADA 시스템의 속성을 고려할 때, 상기의 공격 중에서 관계형 데이터베이스의 특성에 근거한 SQL 기반의 구조적 데이터베이스 속성을 활용한 공격이 가장 현실성이 높은 공격 패턴으로 고려되고 있다[그림 15].

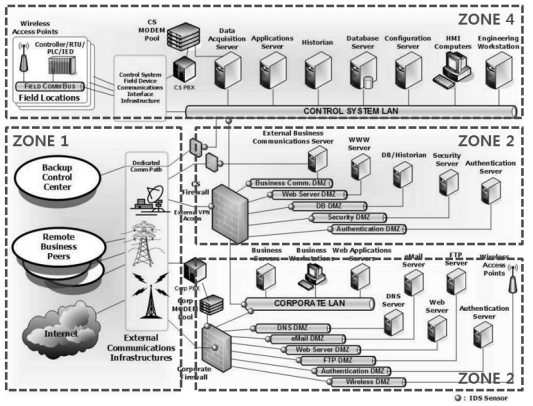
SCADA 시스템은 실시간 차원에서는 분리되어 있더라도, 경영의사결정을 위해 경영시스템 및 기업망(corporate network)과 가끔씩 연동할 수밖에 없다. 상대적으로 접근이 용이한 기업망이나 외부 접속점 데이터베이스에 악성코드나 멀웨어(malware)를 심어두고,

4) Idaho National Lab, Sandia National Lab.



〔그림 15〕 데이터베이스 기반의 공격

간헐적인 연동이나 긴 주기의 정보교환 과정에서 SCADA 내부망으로 침투해 들어가는 방식이다[6]. 이에 대한 대비를 위해 [그림 16]과 같이 구역(zone)을 구분하여, 방화벽이나 침입탐지시스템 등의 보안솔루션을 적용함으로써, 침입이 어디에서 발생했는지에 대한 추적과 피해 확산방지를 용이하게 할 수 있다.

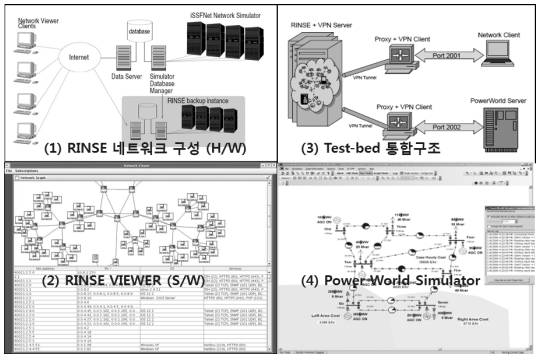


〔그림 16〕 방화벽과 IDS 기반의 보안대책

기타 다양한 대학 연구소에서 스마트그리드의 사이버보안 테스트베드 및 시뮬레이션 모델을 구축하기 위한 연구를 수행하고 있다. Illinois Urbana-Champaign 대학전기공학과가 대표적인 사례로 SCADA 사이버보안 테스트베드를 개발 중에 있는데, 통신 네트워크용 에뮬레이터와 전력시스템 모의 솔루션을 결합하여 통신시스템 상에서의 사이버보안 위협이 전력시스템에 미치는 영향을 평가할 수 있도록 의도하였다.

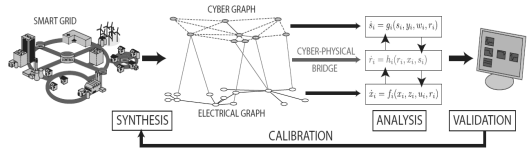
시뮬레이션 테스트베드의 구조는 RINSE[5]라는 네트

워크 에뮬레이터와 지역별 전력망을 가상적으로 구현한 Network Client, 전력계통 운영 시뮬레이션을 수행하기 위한 서버(Power World Simulator 사용) 등으로 구성된다. 즉, RINSE를 통해 통신 네트워크 운영환경이 모의되고 이것이 Network Client를 통해 전력시스템 모의환경으로 넘어가는 구조이다. 즉, RINSE는 통신 네트워크 환경을 구현하고 Power World는 전력시스템 운영환경을 구현하는 기능을 담당하게 된다.



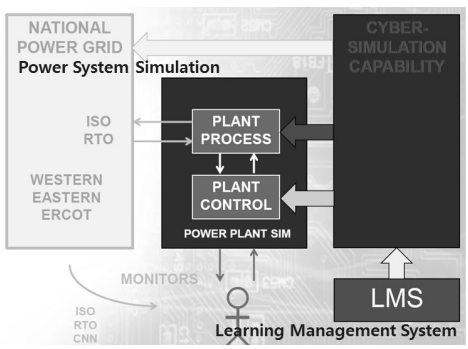
〔그림 17〕 RINSE 기반의 스마트그리드 테스트베드

텍사스 A&M 대학에서도 그래프 이론(graph theory)에 근거하여 사이버시스템과 전력시스템 사이의 관계를 정량적으로 모델링하기 위한 연구를 수행하고 있고[7], Iowa 대학에서는 사이버 위협으로 인한 전력시스템의 위험을 정량적으로 측정하기 위한 연구를 수행하고 있다.



〔그림 18〕 상호작용의 정량적 모델링[7]

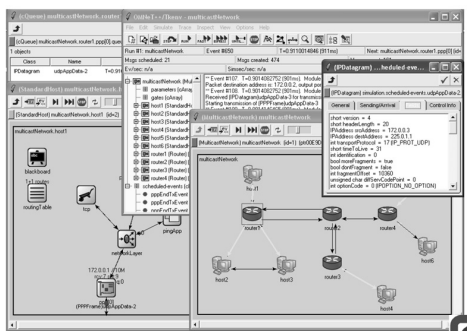
General Dynamics사는 CPS 기반의 전력시스템 사이버보안 시뮬레이터를 개발하였다. 사이버 위협에 대한 다양한 상황을 모의하고 이를 학습관리시스템(LMS[6])으로 학습하고 분석하여 운영자가 시뮬레이션 기반의 간접적 경험을 누적함으로써 잠재적 위험 상황들에 대해 이해할 수 있도록 의도하고 있다. 제어설비시스템에는 다양한 전력전자기술과 임베디드 기반의 제어기술이 적용되고, 이는 해킹을 위한 잠재적 경로가 된다. 이러한 사례를 보인 것이 [그림 19]인데, 특정 발전소나 설비의 제어기기로 접근하여 해당 설비의 물리적 제어권을 확보하고 이를 통해 전체 계통의 안정도에 영향을 미치는 방식으로 사이버 공격을 의도할 수 있다. 이러한 맥락에서 시뮬레이션 툴 역시 [그림 19]와 같은 구조로 구성될 수 있다.



〔그림 19〕 교육 및 시뮬레이션 솔루션

4.2 CPS 기반의 스마트그리드 테스트베드 구현방안

4.1에서 소개된 국외 사례를 참조하여 스마트그리드 CPS 모의를 위한 툴을 구현함에 있어서, 새로운 시스템을 만드는 방법보다는 기존의 툴들을 최대한 활용하여 연계하는 방법이 보다 효율적일 것일 판단된다. 기존의 툴들은 꽤 오랜 시간 사용되면서 그 신뢰성이 어느 정도 검증되었고, 이러한 측면에서 시간과 비용을 줄이고 적정 수준의 신뢰성을 확보할 수 있다.

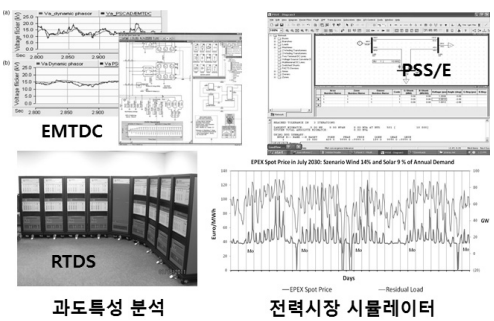


〔그림 20〕 OMNet T++ GUI

5) Real-time Immersive Network Simulation Environment for Network Security Exercises.
6) Learning Management System.

먼저 통신 분야를 생각해볼 때, 통신 네트워크 상에서의 데이터 트래픽을 모의하기 위한 다양한 툴들이 존재한다. 통신 분야에서 대표적으로 사용되고 있는 시뮬레이터 툴로서 NS2가 있고, GUI 측면이 보다 강화된 툴로서 OMNet T++이 있다[8][그림 20].

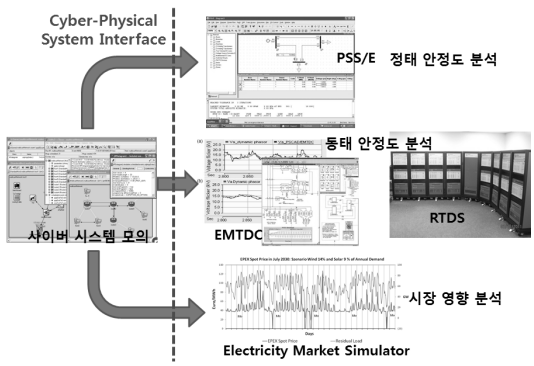
전력분야에서도 다양한 시뮬레이션 툴들이 존재한다. 전력계통을 시뮬레이션 하기 위한 하드웨어 혹은 소프트웨어 기반의 툴들이 존재하고, 전력시장을 모의하기 위한 전력시장 시뮬레이터들도 출시되어 있다. 전력계통은 단일 시스템으로는 매우 거대한 시스템이고, 그로 인해 시뮬레이션 목적에 따라 다양한 용도의 툴들이 개발되었다. 전력계통에는 시뮬레이션 시간구간에 따라 과도안정도와 정태안정도 개념이 존재하는데, 과도안정도란 시스템에 외란이 가해진 후 1~2초 이내의 과도특성을 분석하는 것이고, 정태안정도란 특정 이벤트 발생시(발전기나 송전선로의 탈락 등), 과도특성이 안정화된 이후의 정태적인 시스템 특성의 변화를 보는 것이다. 이러한 2가지 관점의 시뮬레이션은 별개의 툴로 수행되어야 하는데, 전력시스템에 대한 동특성과 정태적 특성을 동시에 모델링하고 연산하는 것은 현재의 PC 사양으로는 감당하기 힘든 연산상의 과부하를 초래하기 때문이다.



〔그림 21〕 전력분야의 다양한 시뮬레이터

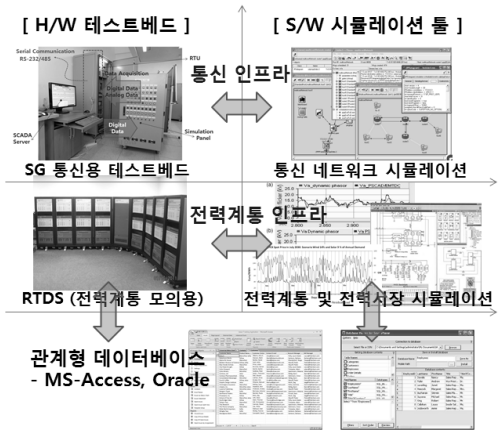
따라서 과도 특성을 분석하는 경우는 EMTDC라는 툴이 많이 쓰이는데, 소프트웨어 기반의 툴로서 시스템의 특정 지점에서 전력시스템을 축약하여 모의하는 형태를 취하게 된다. 실제 시스템에 대한 실시간 시뮬레이션이 필요한 경우는 하드웨어 기반의 RTDS를 통해 수행하게 된다.

실시간 시뮬레이션일 필요가 없으면서, 대규모 시스템(송전시스템 레벨)에 대한 정태적 안정도 분석을 수행할 경우는 PSS/E가 많이 사용되어 왔고, 전기자동차 및 분산형전원 등 배전계통 시뮬레이션이 필요할 경우는 Digsilent가 최근 많이 사용되고 있다. 그리고 상위계층에서 전력시장을 모의하기 위한 툴들도 많이 개발되었는데 전력계통의 이상은 전력시장에 영향을 주고, 전력시장의 모든 거래들은 IT 인프라 상에서 이루어지므로 시장과의 상호작용도 분석할 필요가 있다. 즉 사이버 위협은 SCADA 및 통신 인프라, 전력계통, 전력시장의 3계층에 영향을 미치게 되므로 이들 계층 간의 상호작용을 동시에 고려할 수 있는 통합적인 시뮬레이터 개발이 필요하다. 이러한 맥락에서 다음 [그림 22]와 같은 기존 툴 간의 결합을 통해 해당 3계층에 대한 통합적인 시뮬레이션이 수행 가능하다.



〔그림 22〕 CPS 통합 시뮬레이션 개념도

툴 간의 결합을 위해 별도의 컴포넌트 프로그램이 사용될 수도 있고, 이것이 어려울 경우 상용 데이터베이스



〔그림 23〕 CPS 통합 시뮬레이션 개념도

를 통해 간접적으로 연계하는 대안도 있다. 최근 상용 시뮬레이터 프로그램의 경우 스프레드시트나 데이터베이스와의 연계를 기본적으로 제공하고 있기 때문에 이를 통해 데이터베이스를 간접적인 통신 채널로 활용하여 데이터를 교환할 수 있다.

[그림 23]은 이러한 연계개념을 도식화한 것으로 관계형 데이터베이스(RDBMS) 기반으로 다양한 컴포넌트 툴을 연계하는 개념을 보인 것이다.

Ⅴ. 결 론

해외의 경우 전력시스템에 대한 보안연구는 CPS의 개념 하에서 전력계통(제어시스템)과 SCADA(IT시스템) 간의 상호작용을 시뮬레이션 하는 형태로 옮겨가고 있다. 본문에서 언급하였듯이, 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. 본 연구에서는 이러한 제반적인 위험 분석을 위해, 기존 보안이론의 기본적 요건(기밀성, 무결성, 가용성)을 기반으로 정량적 위험평가를 위한 프레임워크를 수립하고, CPS 기반의 시뮬레이션 방법을 모듈 기반으로 구현할 수 있는 방법론을 제안하였다.

현재 단계에서 그러한 시뮬레이션 툴을 처음부터 새로 설계하고 개발할 수는 없기 때문에, 기존의 상용 툴들을 최대한 활용해서 현실적으로 구현하는 방법을 제안하였다. 이러한 측면의 편의성과 더불어, 신뢰성 측면에서도 개별적으로 검증된 모듈(혹은 컴포넌트)을 사용함으로써 전체적인 시뮬레이션의 신뢰성을 높일 수 있다. 물론 이러한 상용 툴들을 결합하는 과정에서 서로 간 혹은 공용 데이터베이스와의 인터페이스 프로그램이 필요하고, 무엇보다 상위 UI(사용자 인터페이스) 차원에서 유기적인 결합[9]을 통해 사용자가 복잡하고 많은 정보를 쉽게 이해할 수 있도록 설계되어야 한다. 이는 시각화(visualization) 문제와도 연계되는데, 이러한 맥락에서 시각화는 정보의 이해를 돕는 1차적 기능을 넘어 다양한 하위 컴포넌트를 상위 관점에서 단일 프로세스로 통합하는 역할도 맡게 될 것이다. 따라서 스마트그리드 계층(layer)들에 대한 다양한 위협요인에 대한 분석을 유기적으로 통합하여 규명하고 이를 운영자가 쉽게 이해할 수 있도록 하는 것이 CPS 기반 시뮬레이션의 목적이자 중요한 구축관점이라고 요약할 수 있다.

참고문헌

[1] Frances Cleveland, *International Standards for the Smart Grid - Power System Functions, Interoperability, and Information Models*, Xanthus Consulting International.

[2] Electricity Market Complex Adaptive System (EMCAS) - Model Introduction, Argonne National Laboratory, Decision and Information Science Division, Center for Energy, Environmental, and Economic Systems Analysis, 2008.

[3] 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.

[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, 2010.

[5] Matias Negrete-Pincetic, Felipe Yoshida and George Gross, *Towards Quantifying the Impacts of Cyber Attacks in the Competitive Electricity Market Environment.*

[6] 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.

[9] Dong-Joo Kang, Dong-Kyun Kang, and Balho H. Kim, *Visualization Issues of Mass Data for Efficient HMI Design on Control System in Electric Power Industry - Visualization in*

Computerized Operation & Simulation Tools, International Association of Societies of Design Research Conference Seoul, 2009.

〈著者紹介〉

강 동 주 (Dong Joo Kang)
정회원

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

김 휘 강 (Huy Kang Kim)
종신회원

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