정 보 보 호 학 회 지
제24권 제5호, 2014. 10

지능형전력량계를 위한 안전한 유지보수 시스템 모델

유 현 우*, 김 신 규*

요 약

스마트그리드는 기존의 전력시스템에 ICT 기술을 융합하여 에너지 공급자와 소비자, 서비스 제공자가 실시간으로 상호작용할 수 있는 형태의 차세대 전력망을 의미하는 것으로, 최근 대두되고 있는 에너지 위기를 타개하기 위한 중요한 솔루션 중 하나로 인식되고 있다. 그 중에서도 특히 AMI 시스템은 다양한 부가서비스 제공을 가능케 하는 스마트그리드의 핵심요소로 주목받고 있다. AMI 시스템은 그 적용범위가 광범위하고 대부분의 시스템 구성 기기가 물리적 접근이 비교적 용이한 위치에 설치되어 물리적 공격 및 사이버 공격에 대해 비교적 취약한 특성을 띤다. 이러한 보안 위협에 대응하기 위해 DLMS/COSEM 및 국내 지능형전력량계-제2부 표준에서는 지능형전력량계가 갖추어야 하는 다양한 보안기능에 대해 정의하고 있다. 하지만 각 보안기능에 대한 세부 내용을 상기 표준에서 모두 정의하고 있는 것은 아니어서 이에 대한 검토 및 논의가 필요하다. 본 고에서는 DLMS/COSEM 표준과 지능형전력량계-제2부 표준에서 정의하고 있는 보안 기능에 대해 살펴보고, 상기 표준에서 정의하고 있지 않은 보안 기능 중 지능형전력량계 유지보수를 위한 안전한 현장접근 방안에 대해 제안한다.

Ⅰ. 서 론

스마트그리드는 기존의 일방향 전력시스템에 ICT(Information and Communications Technology) 기술을 융합하여 에너지 공급자와 소비자, 서비스 제공자가 실시간으로 상호작용할 수 있는 형태의 전력망을 의미하는 것으로, 최근 대두되고 있는 에너지 위기를 타개하기 위한 중요한 솔루션 중 하나로 인식되고 있다. 특히 그 중에서도 AMI(Advanced Metering Infrastructure) 시스템은 수요관리 및 수요반응, 실시간 요금제 등 다양한 부가서비스의 제공을 가능케 하는 스마트그리드의 핵심요소이자 필수요소로 주목받고 있다[1].

AMI 시스템은 국내 최다 공급 기반시설인 전력망 전반에 적용되며, 시스템 구성 기기의 대부분이 전주와 각 수용가의 내·외부와 같은 물리적 접근이 비교적 용이한 위치에 설치되어 다양한 물리적 공격 및 사이버 공격에 대해 비교적 취약한 특성을 띤다. 이미 2009년 미국 전력망에서 악성코드가 발견되었고, 이를 이용하여 전력공급을 차단할 수 있음이 CNN을 통해 보도된 바 있다[2]. 또한 미 FBI에서는 2012년 푸에르토리코에 설치되어 운영되던 스마트미터가 해킹, 전력 사용량이 조작되어 연간 400만 달러에 달하는 피해가 발생된 사례를 공개하기도 하였다[3].

국내 AMI 시스템에서 데이터를 생성, 관리하고 전달하기 위한 데이터 구조 및 프로토콜로는 국제표준인 IEC 62056으로 정의된 DLMS/COSEM이 주로 사용된다. 그리고 국내 표준인 지능형전력량계-제2부:통신 및 보안 기능(SPS-SGSF-05-2013-01) 표준에서는 DLMS/COSEM 표준을 기반으로 기본적인 통신기능과 다양한 보안 위협에 대비하기 위한 인증 및 접근제어, 데이터 암호화, 부인방지 등과 같은 보안 기능을 정의하고 있다. 하지만 각 보안기능에 대한 모든 세부 내용을 상기 표준에서 정의하고 있는 것은 아니며, 일부 시스템 사업자 및 서비스 제공자의 선택에 의존해야 하는 부분이 존재한다.

본 고에서는 AMI 시스템의 보안성 확보를 위해 DLMS/COSEM 표준과 국내 지능형전력량계-제2부 표준에서 정의하고 있는 보안 기능에 대해 살펴보고, 상기

본 연구는 2014년도 산업통상자원부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다. (No.2012101050004A)

* ETRI 부설연구소 (uwill@ensec.re.kr, skkim@ensec.re.kr)

표준에서 정의하고 있지 않은 보안 기능 중 지능형전력량계 유지보수를 위한 안전한 현장접근 방안에 대해 제안한다.

Ⅱ. 지능형전력량계 보안기능

DLMS/COSEM Application Layer 표준[4]과 국내 지능형전력량계-제2부 표준[5]에서 AMI 시스템의 보안성 확보를 위해 제시하는 보안 기능을 종합하면 크게 접근보안, 통신보안, 기기보안의 3 가지로 나눌 수 있다. 이 중 접근보안과 통신보안 기능은 AMI 기기 간 상호운용성 확보가 반드시 필요한 항목이다. 반면 기기보안 기능의 경우 기기 자체적으로 동작하는 기능으로 각 제조사의 기기가 각기 다른 방식으로 해당 기능을 제공하여도 무방하다. 각 보안 기능에 대한 세부 사항은 [표 1]과 같으며, 이 표의 IEC 62056-5-3, 지능형전력량계 제2부 항목에 기입된 번호는 해당 보안 기능과 관련된 각 표준문서의 Section 번호를 의미한다.

[표 1]에 나타난 각 세부 기능별 보안 요구사항 및 관련 사항은 다음과 같다.

- (접근보안>기기인증>비밀키 인증) LLS
  - DLMS 클라이언트와 서버간 AA(Application Association) 설립 시, 클라이언트가 제시하는 LLS 패스워드가 정확한 경우에만 AA가 정상적으로 설립되어야 함
  - LLS 패스워드 변경 기능을 제공해야 함
- (접근보안>기기인증>비밀키 인증) HLS
  - DLMS 클라이언트와 서버간 AA 설립 시, Challenge-Response 방식의 상호인증이 완료된 경우에만 AA가 정상적으로 설립되어야 함
  - DLMS/COSEM 표준 제시 HLS 인증 메카니즘 중 보안성이 가장 높은 GMAC 방식만을 사용하도록 지능형전력량계-제2부 표준에서 정하고 있음
- (접근보안>기기인증>공개키 인증) PKI 기반 인증
  - DLMS 클라이언트와 서버간 AA 설립 시, PKI 기반의 X.509 ECDSA, RSA 인증서를 이용한 클라이언트, 서버간 상호인증이 정상적으로 이루어진 경우에만 AA가 정상적으로 설립되어야 함
  - 지능형전력량계-제2부 표준에서 정의하고 있는 보안 기능으로 인증서 관리 및 인증 절차에 대한 세부 사항은 정의하지 않고 있음
- (접근보안>접근권한) 인증수준별 접근권한 관리
  - 지능형전력량계 제어 및 운용 DLMS Object에 대한 Read, Write 권한을 기기 인증 수준에 따라 제한하여야 함
- (통신보안>기밀성 및 무결성) 통신데이터 암호화
  - AES-GCM-128 및 ARIA-GCM-128 암호화 알고리즘을 지원해야 하며, 이를 이용해 통신데이터의 암호화 및 인증을 수행해야 함
  - DLMS/COSEM 표준에서는 보안 Suite으로 AES-GCM-128을 제시하고 있으나, 지능형전력량계-제2부 표준에서 ARIA-GCM-128를 추가로 정의하고 있음
- (통신보안>기밀성 및 무결성) 암호화 키 관리
  - 통신데이터 암호화에 사용되는 Master Key, Global Key, Dedicated Key를 안전하게 생성하고 공유해야 함
  - Key 생성 방안에 대해서는 정의하지 않고 있음
  - DLMS/COSEM 표준에서 Global Key, Dedicated Key를 공유하는 방안에 대해 세부적으로 정의하고 있으나 Master Key 공유 방안에 대해서는 정의하고 있지 않음
  - Key 전달 방법으로 DLMS/COSEM 표준에서는 Key Wrapping using AES-128 Key Wrap(IETF RFC 3394), 지능형전력량계-제2부 표준에서는 128

〔표 1〕 지능형전력량계 보안기능

분류			세부 기능	IEC 62056-5-3	지능형 전력량계 제2부
접근 보안	기기 인증	비밀키 인증	LLS (Low Level Security)	5.3.3	5.2
			HLS (High Level Security)	5.3.4	5.2
		공개키 인증	PKI 기반 인증	-	5.2
	접근권한		인증수준별 접근권한 관리	5.3	5.2
통신 보안	기밀성 및 무결성		통신데이터 암호화	5.4.4	5.1.2
			암호화 키 관리	5.4.7.3	5.5
	부인방지		디지털서명	-	5.4
기기 보안	데이터 저장 보안		저장데이터 암호화	-	5.1.3
			데이터 저장 정책	-	5.1.3
	감사		이벤트 로그 저장	-	5.6

비트 블록 암호 알고리즘 ARIA-제2부 : 운용모드(KS X 1213-2)의 Key Wrap 모드를 참조하도록 정의함

- (통신보안>부인방지) 디지털서명
  - PKI 기반의 ECDSA, EC-KCDSA, RSASSA-PSS 방식의 전자서명을 통해 통신데이터 부인방지를 보장할 수 있어야 한다.
  - 지능형전력량계-제2부 표준에서 정의하고 있는 보안 기능으로 디지털서명 생성 및 검증 절차 등에 대한 세부사항은 정의하지 않고 있음
- (기기보안>데이터 저장 보안) 저장데이터 암호화
  - AES-GCM-128 및 ARIA-GCM-128 암호화 알고리즘을 지원해야 하며, 이를 통해 중요 저장데이터의 암호화 및 인증을 수행해야 함
  - 저장데이터 암호화 키는 안전하게 생성하고 보관해야 함
- (기기보안>데이터 저장 보안) 데이터 저장 정책
  - 기기 운영을 위해 필요한 최소 정보를, 최소 기간 동안만 저장해야 함
  - 저장 정보의 종류 및 암호화 대상, 저장 기간 등에 대한 세부 사항은 서비스 제공자의 결정에 따르도록 함
- (기기보안>감사) 이벤트 로그 저장
  - 기기에서 발생하는 이벤트 로그를 정확한 시간정보와 함께 저장해야 하며, 용량 부족 등의 사유로 데이터가 소실되지 않도록 해야 함
  - 저장된 로그 정보에 대해 '데이터 저장 보안'이 적용되어야 함

Ⅲ. 지능형전력량계 유지보수용 현장접근 방안

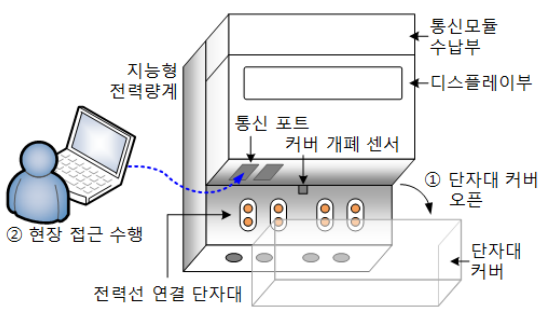
앞서 살펴본 바와 같이 지능형전력량계와 같은 AMI 기기의 보안성 확보를 위해서는 접근 기기의 인증과 통신데이터의 암호화가 필수적이다[6]. 이러한 인증 및 암호화와 같은 보안 기능의 지원은 동일 AMI 네트워크에 참여하여 사전에 암호화 키 공유가 정상적으로 이루어진 기기 간에만 가능하다.

하지만 실제 AMI 시스템 운영환경에서 AMI 네트워크 내 기기 간 통신만 이루어지는 것은 아니며, 유지보수를 목적으로 각 기기에 대한 현장접근이 필요한 경우 또한 발생될 수 있다. 매우 특수한 경우를 제외하고는 유지보수 인력이 각 AMI 기기 간에 안전하게 공유된 암호화 키를 현장에서 확인할 수 있는 방법은 없다. 따라서 유지보수 인력이 현장접근 기기를 이용하여 지능형전력량계에 접근하는 경우 HLS 이상 수준의 기기 인증 및 통신데이터 암호화가 불가능하며, 이에 대한 대책 마련이 필요하다. 본 장에서는 지능형전력량계의 유지보수를 위한 안전한 현장접근 방안에 대해 제안한다.

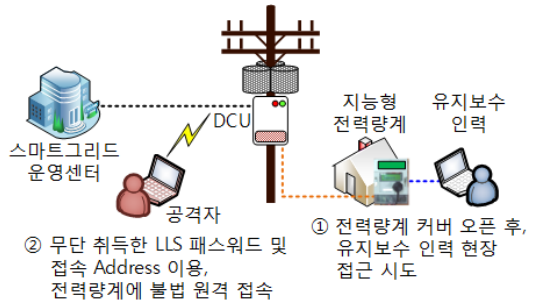
3.1. LLS 인증을 이용한 현장접근 방안

유지보수 대상 지능형전력량계에 설치된 암호화 키를 알 수 없는 상황에서, 현장접근 기기 인증을 수행할 수 있는 가장 간단한 방법은 DLMS/COSEM 표준에서 정의하고 있는 LLS 방식을 이용하는 것이다. LLS 인증은 단순 패스워드 방식의 단방향 인증 방안으로 구현 및 수행 절차가 간단하다는 장점이 있다. 하지만 지능형전력량계-제2부 표준에서는 중요 정보에 대한 접근 및 설정 변경은 HLS 이상의 인증 받은 기기만이 수행할 수 있도록 정의하고 있어, 단순 LLS 인증 방식을 유지보수 용도로 사용하기에는 부적합하다. 이러한 문제점을 해결하기 위해 현장접근 기기의 통신 Address를 특정하고, 해당 특정 Address로 접근하여 LLS 인증을 받은 기기에 한하여 HLS 인증 기기와 유사한, 유지보수 용도에 적절한 수준의 접근 및 제어 권한을 부여하는 방안을 고려할 수 있다.

하지만 상기 방식 역시 패스워드와 해당 Address가 유출되는 경우 이를 이용하여, 누구나 원격에서 AMI 네트워크를 통해 지능형전력량계에 접근할 수 있다는 문제점이 있다. 패스워드 및 현장접근 Address가 유출된 경우, 원격 무단 접근을 막기 위해서 지능형전력량계의 단자대 커버를 사용할 수 있다. [그림 1]과 같이 대



〔그림 1〕 LLS 인증과 단자대 커버 개폐여부를 이용한 지능형 전력량계 현장접근 방안



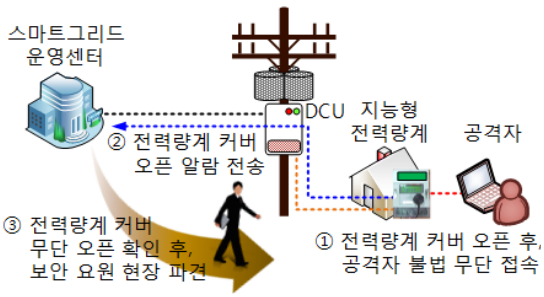
〔그림 2〕 LLS 인증과 단자대 커버 개폐여부를 이용한 지능형 전력량계 현장접근 방안 공격 시나리오

부분의 국내 지능형전력량계는 통신 포트 및 전력선 연결 단자대를 보호하기 위한 커버를 구비하고 있으며, 보안 및 안전성의 이유로 커버의 개폐를 감지할 수 있는 센서가 장착되어 있다. 이를 이용하여 지능형전력량계는 정상적으로 커버가 오픈된 경우에만 유지보수 인력이 현장에 접근하였다고 판단, LLS 방식을 이용한 현장접근을 허용할 수 있다. 이렇게 LLS 인증, 현장접근 Address에 전력량계 커버 개폐여부를 추가로 활용하는 경우 지능형전력량계에 대한 무분별한 원격 무단 침입을 방지 할 수 있다.

하지만 이러한 방안을 사용하는 경우에도 지능형전력량계는 여전히 다양한 취약점에 노출될 수 있다. 그 중 가장 보편적으로 생각할 수 있는 공격 시나리오는 [그림 2]와 같으며 그 절차는 다음과 같다.

① 지능형전력량계 유지보수 사유 발생 시, 유지보수 인력 현장에 접근하여 커버 오픈 및 현장접근 시도
② LLS 패스워드 및 접근 Address를 무단 취득한 공격자는 원격지에서 지속적으로 해당 전력량계에 접근을 시도하다가, 현장의 유지보수 인력이 커버를 오픈하는 시점에 무단 원격 접속 성공

이러한 무단 원격 접근을 원천적으로 차단하기 위해서는 별도로 마련된 현장접근용 통신포트가 필요하다. 즉, 유지보수 대상인 지능형전력량계는 커버가 정상적으로 오픈되고, 현장접근 Address를 갖는 기기가 현장접근용 통신포트를 통해 LLS 인증을 정상적으로 완료한 경우에만 유지보수용 현장접근 기기의 접근을 허가해야 한다. 이러한 방안을 통해 공격자가 원격에서 지능형전력량계에 무단 접근을 시도하는 것을 원천적으로 차단할 수 있다.



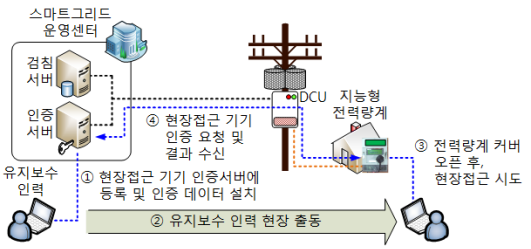
〔그림 3〕 LLS 인증, 단자대 커버 개폐여부, 별도 현장접근용 포트를 이용한 지능형전력량계 현장접근 방안 공격 및 대응 시나리오

지금까지 설명한 현장접근 방안은 비교적 저비용으로 상당히 합리적인 수준의 보안성을 확보할 수 있는 방안이다. 하지만 이 역시도 완전한 보안대책이라 보기는 어렵다. 특히, 공격자가 원격지가 아닌 지능형전력량계 설치 위치에 직접 접근하여 커버를 무단으로 오픈하고 별도 통신포트를 통해 접근을 시도하는 것 자체를 막을 수는 없다. 다만 전력량계에 커버 개폐 여부를 감지하여 운영센터의 관리자에게 알람을 전송하는 기능을 추가로 구현하는 경우, [그림 3]과 같이 보안 요원을 신속하게 현장에 파견, 조치를 취할 수 있다. 상기 경우에 대한 공격 및 대응 절차는 다음과 같다.

① 공격자는 공격 대상인 지능형전력량계에 물리적으로 접근하여 커버를 오픈하고, 무단으로 취득한 LLS 패스워드 및 접근 Address를 이용하여 현장접근용 포트를 통해 전력량계에 접근
② 전력량계는 커버가 오픈되는 것을 감지하는 순간, 알람을 발생시켜 이를 운영센터의 시스템 관리자에게 알림
③ 관리자는 해당 커버 오픈이 사전에 인가된 유지보수 등의 사유에 의한 것인지 확인한 후, 무단 오픈이 확인되는 경우 즉시 보안 요원을 해당 현장에 파견

3.2. 원격 인증을 이용한 현장접근 방안

앞 절에서 설명한 LLS 인증을 기반으로 한 현장접근 방안보다 더욱 높은 보안성을 갖는 유지보수용 현장접근 방안은 바로 원격지의 신뢰할 수 있는 인증센터를 통해 현장접근 기기의 인증을 수행하는 방안이다. 본 방안의 구현을 위해서는 보다 높은 비용과 노력이 소요되



〔그림 4〕 원격 인증을 이용한 지능형전력량계 현장접근 방안

지만, 공격자의 무단 접근을 원천적으로 차단할 수 있는 보안성이 매우 뛰어난 방안이다.

본 방안의 구현을 위한 시스템 구성 및 접근 시나리오는 [그림 4]와 같다. AMI 서비스를 운영하는 서비스 제공자는, 원격검침 데이터를 저장하는 검침서버 외에 현장접근 기기의 등록 및 인증을 위한 인증서버를 별도로 마련해야 한다. 신뢰할 수 있는 인증센터 또는 인증서버의 위치는 [그림 4]와 같이 운영센터 내부이거나, 별도로 분리된 제 3의 기관이어도 무방하다. 다만 급작스럽게 동시 다발적으로 발생할 수 있는 유지보수 상황에 보다 신속하게 대응하기 위해서는 운영센터 내부에 인증서버를 두는 것이 신규 현장접근 기기의 등록 및 인증에 유리할 것으로 판단된다. 인증서버를 이용한 현장접속 절차는 다음과 같다.

① 지능형전력량계의 유지보수 사유 발생 시, 유지보수 인력은 현장접근 기기를 인증 서버에 등록하고 인증 데이터를 현장접근 기기에 설치함
② 유지보수 인력은 상기 현장접근 기기를 가지고 유지보수 대상 전력량계 설치 현장에 출동
③ 유지보수 인력은 전력량계 커버 오픈 후, 현장접근 시도
④ 지능형전력량계는 현장접근 기기에 설치된 인증데이터를 인증서버로 전송하고, 현장접근 기기에 대한 인증이 정상적으로 완료된 경우 유지보수용 현장접근 허가

현장접근 기기를 인증하기 위해 사용되는 인증 데이터로는 암호화 키, PKI 기반 인증서 등 안전한 인증 방식이라면 무엇이든 적용 가능하다. 또한 본 방안을 응용하여 유지보수 사유 및 인력의 등급에 따라 각기 다른 수준의 권한을 갖는 인증 데이터를 현장접근 기기에 설치하여 상황에 적절한 최소 권한만이 부여되도록 제어할 수 있다.

원격 인증을 이용하는 본 방안은 별도의 인증서버 설치 및 운용, 인증 데이터 교환을 위한 프로토콜 설계 등이 추가로 필요하다. 이렇듯 그 구성이 비교적 복잡한 탓에 시스템의 구축 및 운용에 보다 높은 비용이 소요되나, 인증되지 않은 공격자의 무단 접근을 원천적으로 차단할 수 있다는 측면에서 큰 장점을 갖는다.

Ⅳ. 결 론

본 고에서는 AMI 시스템에 대한 보안 위협에 대응하기 위해 DLMS/COSEM 표준과 국내 지능형전력량계-제2부 표준에서 정의하고 있는 보안기능들을 종합하여 살펴보고, 상기 표준에서 정의하고 있지 않은 보안 기능 중 지능형전력량계 유지보수를 위한 안전한 현장접근 방안에 대해 제안하였다.

안전한 현장접근 방안으로 본 고에서는 각각 LLS 인증과 원격 인증을 이용하는 두 가지 방안을 제안하였다. 전자는 비교적 저비용으로 매우 합리적인 수준의 보안성을 확보할 수 있는 방안이나, 공격자의 무단 접근을 100% 차단할 수는 없었다. 반면 후자는 그 시스템 구성이 복잡하여 높은 수준의 구축 및 유지 비용이 소요되지만 공격자의 무단 접근을 완전하게 차단할 수 있는 방안이었다.

상기 두 가지 방안 중 어떠한 방안이 지능형전력량계에 적합한지에 대한 논의를 위해서는 AMI 시스템에 대한 사이버 공격 피해 사례 및 피해 규모, 각 서비스 제공자별 AMI 시스템 구성 등에 대한 연구가 선행되어야 한다.

참 고 문 헌

[1] 최인지, 박병석, 유현우, 윤명용, 이상염, 윤종호, “스마트 그리드를 위한 지능형 원격검침 프로토콜 설계 및 구현”, *2011년도 대한전자공학회 하계종합학술대회 논문집*, 34(1), pp. 3-6, 2011.
[2] 정교일, 박한나, 정부금, 장종수, 정명애, “스마트그리드의 안전성과 보안 이슈”, *한국정보보호학회지*, 22(5), pp. 54-61, August 2012.
[3] “FBI: Smart Meter Hacks Likely to Spread”, *Kerbs on Security*, April 2012.
[4] Electricity Metering Data Exchange - The

DLMS/COSEM – Part 5-3: DLMS/ COSEM Application Layer, IEC 62056- 5-3, June 2013.
[5] 지능형전력량계-제2부 : 통신 및 보안 기능, SPS-SGSF-05-2013-01, May 2013.
[6] 최재덕, "스마트그리드 기기의 인증 및 키 관리 보안 동향", *전자공학회지*, 40(10), pp. 40-50, October 2013.

〈저자소개〉

사 진

유 현 우 (Yoo Hyunwoo)
비회원

2009년 2월 : 고려대학교 전파통신공학과 졸업
2011년 2월 : 고려대학교 컴퓨터·전파통신공학과 석사
2011년 3월~2013년 11월 : 한국전력공사 전력연구원 연구원
2013년 12월~현재 : ETRI 부설연구소 연구원
관심분야 : 스마트그리드 보안, 제어시스템 보안, 상호운용성 시험 시스템

사 진

김 신 규 (Kim Sinkyu)
정회원

2000년 2월 : 연세대학교 기계전자공학부 졸업
2002년 2월 : 연세대학교 컴퓨터과학과 석사
2014년 2월 : 연세대학교 컴퓨터과학과 박사
2003년 12월~현재 : ETRI 부설연구소 선임연구원
관심분야 : 스마트그리드 보안, 국가기반시설 보안, 취약점 분석