情 報 保 護 學 會 誌
第22卷 第1號, 2012. 2

# Homeland Security에서의 M2M(사물지능통신) 보안 동향

김 우 년*

요 약

홈랜드 시큐리티는 비군사적 위협으로부터의 국토안보를 의미하며, 정보보호, 물리보안, 무인경비, 산업 및 재해방지시스템 등을 연계하여 사이버 공격, 산업기술 유출 및 국제테러 등에 효과적으로 대응하는 IT 기반의 융·복합 분야를 통칭하고 있다. 홈랜드 시큐리티의 주요 영역은 여러 가지 분류가 가능할 수 있지만, 항공보안, 대량수송보안, 해양보안, 인프라보안, 사이버보안, 국경보안, 대테러 첩보, 비상대응 등으로 구분할 수 있다. 홈랜드 시큐리티의 영역중 사물지능통신이 제한적으로 활용되고 있으며 향후 활용이 확대될 것으로 예상되는 분야 중 하나는 스마트그리드를 포함한 사회기반시설 분야이다. 사회기반시설은 이미 사이버 보안위협에 노출되어 있으며, 향후 사물지능통신이 보편화되면 사회기반시설은 사이버공격의 핵심대상으로 더욱 부각될 것으로 예상된다. 본 고에서는 사회기반시설의 사물지능통신 현황 및 향후 전망을 살펴보고, 사회기반시설에 대한 사이버 보안위협 사례와 대응 현황에 대해서 소개한다.

## Ⅰ. 서 론

홈랜드 시큐리티(HLS : Homeland Security)는 2001년 9·11 테러이후 미국에서 국방분야와는 별개로 비군사적 위협에 대한 국토안보를 목적으로 국토안보법(홈랜드 시큐리티법)을 제정하고, 국토안보부를 신설함에 따라 확산된 용어로써, 정보보호, 물리보안, 무인경비, 산업 및 재해방지시스템 등을 연계하여 사이버 공격, 산업기술 유출 및 국제테러 등에 효과적으로 대응하는 IT 기반의 융·복합 분야를 통칭하고 있다[1]. 미국의 국토안보부는 홈랜드 시큐리티 구현을 위하여 "국민들에게 테러를 포함한 각종 위협으로부터 안전하고 빠른 회복력을 보유한 국가를 보장"한다는 임무아래 5가지 전략적 목표를 설정하여 추진하고 있으며, 이러한 전략적 목표 가운데 하나는 주요 사회기반시설에 대한 보호를 포함하고 있다[1].

홈랜드 시큐리티의 주요 영역은 항공보안, 대량수송보안, 해양보안, 인프라보안, 사이버보안, 국경보안, 대테러 첩보, 비상대응, CBRN(Chemical, Biological, Radiological, Nuclear: 화학, 생물학, 방사능, 핵무기) 보안으로 구분할 수 있다[2].

홈랜드 시큐리티의 주요 영역 중 인프라 보안은 주로 발전소와 국가의 전력 그리드, 가스관과 같은 주요 사회기반시설 및 설비를 보호하기 위한 분야이며, 사이버보안은 IT 기술의 발전으로 인터넷 중심의 글로벌 경제가 형성되고 DDoS 등의 사이버위협 수준이 크게 증가함에 따라 세계 각국의 관심이 커지고 있는 분야이다[2].

전력, 발전, 가스, 교통 등의 사회기반시설은 원격지에서 운영되는 설비의 상태 및 현황을 모니터링 및 관리하고 제어하기 위하여 중앙의 제어센터와 원격지 제어기기, 원격지 제어기기와 설비 사이에 정보통신기술을 접목하여 운용중에 있다. 원격지 설비의 상태 및 현황 정보는 주기적으로 자동 수집되고, 수집된 정보는 저장·분석되어 사용자에게 제공되며, 이상 상태 발생시 경고 정보를 사용자에게 제공하여 즉각적인 대응을 통해 인명 및 설비를 보호하도록 하는 등 사물지능통신을 이미 활용중에 있다. 이처럼 사회기반시설이 네트워크로 연결됨에 따라 사이버공격이 사회기반시설에까지 미칠 수 있게 되어, 심각한 국가운영의 위협이 되고 있다. 따라서 홈랜드 시큐리티 여러 영역 중에서 사회기반시

* 한국전자통신연구원 부설연구소(wnkim@ensec.re.kr)

설에 대한 사이버보안 확보는 안전한 국가운영을 위해서 매우 중요한 요소이다. 특히 최근의 사이버공격 유형이 실력과시용의 단순한 해킹, 금전적 목적의 소규모 그룹 해킹에서 국가혼란을 초래할 수 있는 사회기반시설에 대한 해킹, 국가 혹은 대규모 테러 집단이 가담한 조직적 해킹으로 발전함에 따라 사회기반시설에 대한 사이버공격 대응은 매우 중요하다.

본 고에서는 홈랜드 시큐리티 여러 분야 중에서 사회기반시설 중심의 인프라 보안 측면에서 사회기반시설의 사물지능통신 환경을 분석하고, 사회기반시설 사물지능통신에 대한 사이버공격 사례 및 보안위협을 분석한다. 또한 사회기반시설 보호를 위한 세계 각국의 보안현황과 국내 보안현황에 대해서 살펴보고자 한다.

## Ⅱ. 사회기반시설과 사물지능통신

사회기반시설을 운영하는 시스템들은 다양한 센서와 시스템을 구성하여 자동화된 운영을 수행하고 있으며, 이를 위해서 시스템과 센서, 시스템과 제어기기간의 지능화된 통신을 사용하고 있다. Machine to Machine (M2M)의 개념을 이미 구현하고 있는 것이다. 그리고 이러한 사물지능통신은 사회기반시설 시스템에 더 많이 도입되고 적용될 것으로 예상된다.

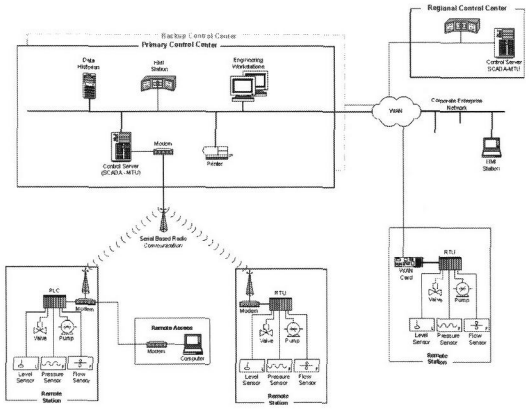
본 장에서는 이러한 사회기반시설을 운영하는 시스템의 구성과 사물지능통신 현황에 대해서 설명한다.

### 2.1 사회기반시설 시스템 구성

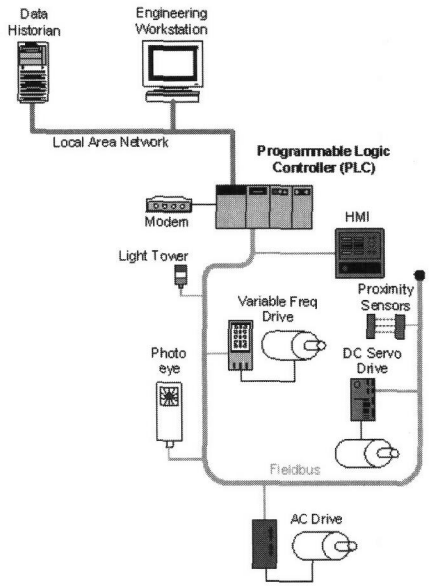
사회기반시설 시스템은 구성 및 특성에 따라 SCADA (Supervisory Control And Data Acquisition), DCS (Distributed Control System), PLC(Programmable Logic Controller)를 사용하는 기타 시스템의 3가지로 분류된다[4]. SCADA 시스템은 중앙 제어센터에서 원격지의 분산된 설비를 제어 및 모니터링하는 시스템이며, DCS 시스템은 동일한 지리적 위치 내에서 생산시스템을 제어하는데 사용되는 제어시스템이다[4]. [그림 1]은 SCADA 시스템의 일반적인 구성이다.

PLC는 SCADA와 DCS의 구성요소로 사용될 수 있으며, 산업 설비 및 프로세스를 실행하는 산업용 컴퓨터이다[4]. [그림 2]는 PLC 시스템 구성 예 이다.

사회기반시설 시스템은 중앙의 제어센터에서 원격지 설비의 상태 정보를 주기적으로 수집 · 저장 · 분석하며,




〔그림 1〕 SCADA 시스템의 일반적인 구성[4]

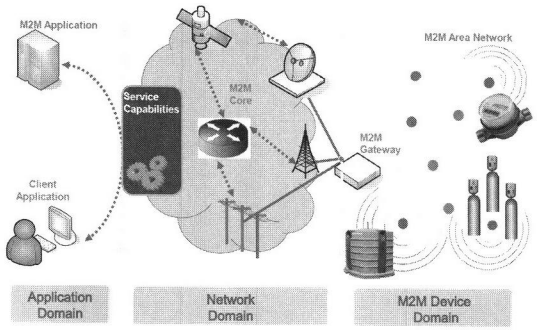



〔그림 2〕 PLC 시스템 구성 예[4]

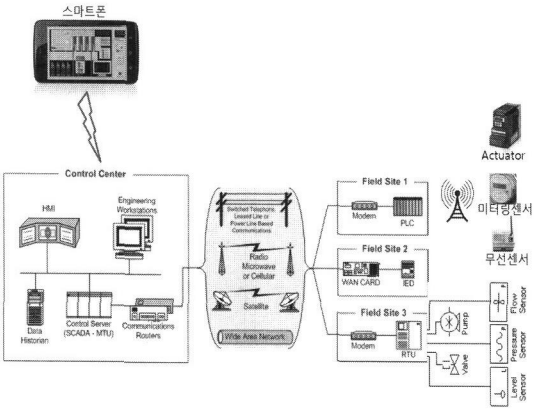
분석된 정보는 HMI(Human-Machine Interface)를 통해 사용자에게 표출된다. 사용자는 상태정보를 모니터링하고 필요시 원격지 설비에 제어명령을 내려 적절한 동작을 수행하도록 지시한다.

### 2.2 사회기반시설의 사물지능통신

사물지능통신은 나라마다 조금씩 다르게 정의하고 있지만 대체로 IoT(Internet of Things, ITU-T), M2M (Machine to Machine, ETSI), MTC(Machine Type Communications, 3GPP) 등으로 정의되고 있다[3].




〔그림 3〕 사물지능통신 구성도[7]




〔그림 4〕 사회기반시설 시스템의 사물지능통신 구성

사물지능통신은 M2M 장치 영역의 센서, 센서인 미터링 장치 등에서 수집한 정보를 M2M 게이트웨이를 통해 네트워크 도메인을 거쳐 M2M 응용프로그램이 포함된 응용 도메인으로 전송하는 구조로 되어 있다[7]. 전송된 정보는 응용 특성에 따라 분석되어 사용자에게 제공된다.

사회기반시설 시스템의 통신 구조는 [그림 4]와 같다. 제어센터는 원격지 제어기기인 PLC, RTU(Remote Terminal Unit), IED(Intelligent Electronic Device)에게 센서, 구동기(Actuator)의 상태 정보 수집을 주기적으로 자동요청하고, 원격지 제어기기는 요청받은 명령에 따라 센서, 구동기의 상태 정보를 수집한 후 네트워크를 통해 제어센터로 전송한다. 제어센터에서는 수집된 정보를 데이터베이스에 저장하여 관리하며, 정보 분석 응용을 이용하여 정보를 분석하고 HMI(Human-Machine Interface)를 통해 사용자에게 정보를 제공한다. 사용자는 HMI 등을 통해 원격지 센서 및 구동기 등의 상태를 파악하고, 이상이 발생하거나 조작이 필요한 경우 제어명령을 전송하여 구동기의 동작을 조절한다. 이와 같이 사회기반시설 시스템의 통신 구조는 [그림 3]과 같은 사물지능통신 구성과 동일한 구성으로 사회기반시설을 운용중에 있다.

현재 운영중인 사회기반시설 시스템은 원격지 제어기기와 센서 및 구동기와 연결이 M2M 수준의 IP 및 모바일 기반 통신을 지원하는 연결 구조가 일부 있지만 아날로그 기반으로 전용 장치와 직접 연결되어 운영되는 경우가 더 많다. 그러나 최근 개발되는 사회기반시설 시스템 구성요소는 M2M 기능을 내장한 원격지 제어기기와 연계하여 사용할 수 있는 IP 및 모바일 통신을 지원하는 M2M 장치들이 개발되고 있으며, 스마트폰 활성화에 따라 제어센터의 HMI 응용이 스마트폰 앱으로 개발되어 제공되고 있다. 사회기반시설에 활용되는 장치가 M2M을 지원하는 장치로 진화함에 따라 고려해야 할 보안위협도 증가하게 될 것으로 예상된다.

## Ⅲ. 사회기반시설 사물지능통신의 보안위협

본 장에서는 사회기반시설에서 발생했던 보안위협 사례를 분석하고, 사회기반시설이 사물지능통신으로 진화함에 따라 고려해야할 보안위협은 어떠한 것이 있는지 분석한다.

### 3.1 사회기반시설 보안위협 사례

사회기반시설에 대한 최근의 사이버 위협 사례로는 Stuxnet, Duqu, Night Dragon, Nitro, 일리노이주 수처리시스템 공격 등이 있다.

Stuxnet은 2010년 7월 이란의 원전시설 SCADA 시스템을 침투하여 원심분리기 오작동을 유발하였다[8]. Stuxnet은 네트워크를 통한 자동전파 및 이동저장장치를 통한 전파 방식을 채용하여 인터넷과 분리되어 운영되는 사회기반시설 시스템에 침투할 수 있도록 설계되었으며, PLC에 악성코드 블록을 다운로드하여 비정상 행위를 수행하도록 하였다[8].

Duqu 악성코드는 2011년 9월 발견되었으며, Stuxnet 개발자 그룹에서 개발한 것으로 추정되고 있으며, 감염 경로는 명확하지 않으나 정보수집 목적인 것으로 추정되고 있다[9].

Night Dragon 공격은 2011년 2월 발견된 것으로, 글로벌 에너지 기업을 대상으로 APT(Advanced Persis-

tent Threat) 공격을 하여 기업의 웹 서버 침투 후 기업 내부 네트워크 및 시스템으로 침투하여 기업의 중요 정보를 획득하고자 하였다[10].

Nitro 공격은 2011년 7월 발생한 공격으로, 화학 및 군사 분야 기업을 대상으로 사이버 공격을 감행하여 지적재산정보를 수집하고자 하는 목적으로 수행되었다[11].

2011년 11월에는 미국 일리노이주 수처리 제어시스템을 해킹하여, 원격에서 수처리 펌프를 제어한 사이버 공격이 발생하였다. 해당 공격은 유지보수 목적으로 공개되어 있는 서비스를 인터넷을 통해 원격 접근하여 이루어졌다[12].

사회기반시설은 사회기반시설 시스템과 연결된 인터넷, 이동저장장치를 이용한 감염, 유지보수 목적의 접근 경로 등에 의해 사이버침해를 받고 있다. 이러한 사이버 침해 경로는 향후 사물지능통신의 도입이 본격화되면 더욱 증가할 수 있다.

## 3.2 사회기반시설 사물지능통신의 보안위협 분석

사회기반시설에 IP 및 모바일 통신 기반의 사물지능통신 도입이 증가함에 따라 관련 기기의 개발도 활성화되고 있는 추세이다. 사회기반시설에 사물지능통신이 도입되면 사회기반시설 관리의 효율성이 증대되는 반면에 역으로 이를 악용한 사이버공격이 발생할 수 있다. 이전 절에서 다룬바와 같이 사물지능통신의 도입 초기인 현재도 주요 사회기반시설에 대한 사이버공격으로 인해 피해가 발생하고 있다. 본 절에서는 사회기반시설에 사물지능통신이 도입됨에 따라 발생 가능한 보안위협을 분석한다.

### 3.2.1 인터넷과 연결되는 제어기기

사회기반시설 시스템 중 제어기기는 원격지에서 운영되기 때문에, 제어기기에 대한 관리 및 유지보수가 쉽지 않다. 최근 개발되는 제어기기는 M2M 기능을 내장하여 원격지에서 관리가 용이하도록 지원하고 있다. 이로 인해 제어기기에 대한 관리상의 문제가 발생하여 인터넷을 통해 제어기기로 침입이 가능한 상황이 발생할 수 있다. 미국 ICS-CERT(Industrial Control System CERT)는 2010년 10월과 2011년 12월 2회에 걸쳐 사회기반시설이 인터넷과 연결되어 운영되고 있어 사이버 공격에 취약함을 경고하고 있다[5, 6].

인터넷과 연결된 제어기기의 취약요소는 접근에 따른 사용자 인증 기능의 부재, 기기 개발시 설정된 기본 인증정보의 변경없이 활용, 인증정보의 평문 전송으로 인한 인증정보 유출 등의 보안 취약점이 있다.

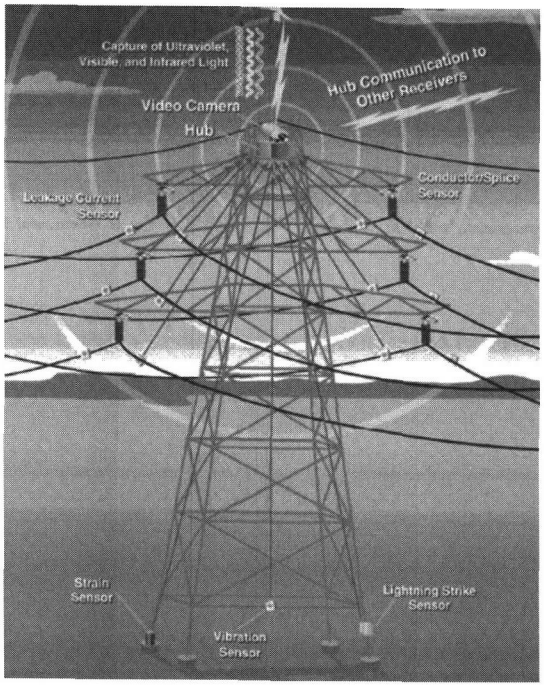
### 3.2.2 모바일 기기와 연결되는 제어시스템

최근 사회기반시설 시스템 개발사는 제어센터 업무의 효율성을 향상시키기 위하여 스마트폰, 태블릿 PC와 같은 모바일 기기에서 HMI 인터페이스를 통해 기반시설 운영현황을 모니터링할 수 있는 앱을 개발하여 출시하고 있다. [그림 5]는 아이폰용 HMI 앱을 검색한 것으로, 많은 시설들이 스마트폰과 연결될 수 있음을 확인할 수 있다. 사회기반시설이 모바일 기기와 연결됨으로써, 모바일 기기의 분실 및 앱의 접근제어 문제로 타인에게 사회기반시설 운영현황이 노출될 수 있으며, 임의로 접근할 수 있는 보안 취약점이 발생한다.

### 3.2.3 센서 정보 전송 취약점

스마트그리드를 포함한 사회기반시설의 지능화를 담당하는 요소는 각종 센서와 센서에서 수집된 정보를 전달하는 M2M 네트워크, 그리고 수집된 정보를 분석하여 조기에 대응함으로써 사회기반시설의 효율적인 관리가 가능하게 된다. [그림 6]은 송전선로에 설치된 각종 센서와 통신네트워크를 나타낸다. 센서로 수집한 정보는 무선통신으로 중간 수집장치로 취합되고, 중간 수집장치는 제어센터로 취합된 정보를 전송하는 과정을 거쳐 제어센터에서 관련 설비의 현황을 모니터링 하게 된


〔그림 5〕 스마트폰에서 구동되는 HMI 사례




〔그림 6〕 사회기반시설의 센서와 M2M 네트워크[7]

다. 이 과정에서 허가되지 않은 장치가 센서의 전송 정보를 수집 및 유출, 변조된 정보를 중간 수집장치로 전송, 사물지능통신 환경을 통해 중간 수집장치 및 제어센터로의 침투 등의 보안위협이 발생할 수 있다.

사회기반시설에 사물지능통신의 도입이 증가함에 따라 네트워크는 더 복잡해지고, 다양한 서비스와 통신기술이 도입될 것이다. 이에 따라 예측할 수 없는 다양한 보안위협이 지속적으로 대두될 것으로 예상된다.

## Ⅳ. 사회기반시설 사물지능통신 보안 동향

현재 운영중인 대부분의 사회기반시설은 제한적인 사물지능통신 환경을 사용하고 있으며, 원격지에 설치되는 설비의 대부분은 M2M 기능이 없는 전용 설비 위주로 운영되고 있다. 사회기반시설은 지역적으로 분산되어있는 시설들을 지능적으로 운영 및 관리하기 위하여 사물지능통신의 도입을 시작하고 있는 단계에 있다. 따라서 사회기반시설 사물지능통신에 대한 보안동향은 스마트그리드와 같은 국가적인 산업에서 고려하기 시작하는 등 초기 단계라고 볼 수 있다. 따라서 본 장에서는 2010년 Stuxnet이 이란 원전시설을 사이버 공격한 이후 크게 대두된 사회기반시설에 대한 세계 각국의 보안 동향에 대해서 설명하고자 한다.

### 4.1 미국

사회기반시설 보호를 위해 에너지부 중심의 "국가 스카다 테스트베드 프로그램(NSTB : National SCADA Testbed Program)"과 국토안보부 중심의 "제어시스템 보안 프로그램(CSSP : Control System Security Program)"을 운영하고 있다. NSTB 프로그램은 INL(Idaho National Lab.)을 포함한 6개 국립연구소 중심으로 2003년부터 전력분야의 17개 설비를 테스트베드로 구축하여 2010년까지 37개 제어시스템에 대한 취약성 분석을 수행하였고, 관련 보안기술 개발을 추진하고 있다[13]. 취약성 분석을 통해 통신 구간의 취약성을 식별하여 대책을 마련함으로써 사회기반시설에 대한 사이버공격을 예방하고자 노력하고 있다. CSSP에서는 2004년부터 INL 중심으로 제어시스템에 대한 취약성 분석, 제어시스템 특화 CERT(ICS-CERT)를 운영하고 있다[14]. 또한 사회기반시설 운영자, 개발자, 정부, 학계, 연구계 등이 참여하는 ICSJWG (Industrial Control System Joint Working Group) 운영을 통해 사회기반시설 취약점의 사전식별 및 완화대책 마련, 사회기반시설에 대한 사이버공격 예방 및 대응, 관련 정보의 공유를 통해 사회기반시설의 사이버 안전성을 확보하기 위해 노력하고 있다[14]. 특히 ICS-CERT에서는 사회기반시설 시스템의 보안취약점 및 대책을 발표하고, 사회기반시설의 인터넷 접속에 대한 보안 위험성을 지적하는 등 사회기반시설이 사물지능통신과의 결합으로 나타날 수 있는 보안 위험에 대처하기 위한 활동을 수행하고 있다.

### 4.2 EU

EU에서는 사회기반시설 보안을 위한 사례발굴 및 보안표준 개발을 위한 ESCoRTS 프로젝트[15], 유럽 SCADA Testbed 구축 프로젝트인 ESTEC[16], 그리고 사회기반시설의 취약성을 조사하고 완화대책을 마련하여 사이버공격으로부터 기반시설을 보호하기 위한 목적의 VIKING[17] 프로젝트를 추진하고 있다. EU에서도 미국과 동일하게 사회기반시설이 사물지능통신 환경으로 진화함에 따라 대두될 수 있는 사회기반시설 운영시스템의 사이버 안전성을 확보하기 위한 노력을 추진하고 있다.

### 4.3 한국

국내에서는 정보통신기반보호법에 의거 중요 사회기반시설을 주요정보통신기반시설로 지정하여, 주요정보통신기반시설에 대한 취약성 분석을 통해 사이버공격을 예방하는 활동을 수행해 오고 있다. 2010년 Stuxnet 발생 이후에는 사회기반시설을 운영하는 제어시스템 보안에 대한 관심이 고조되고 있는 실정이다. 특히 사물지능통신 환경이 적용될 것으로 예상되는 차세대 전력망인 스마트그리드 분야에서는 스마트그리드의 보안체계를 수립하고 및 스마트그리드를 보호하기 위한 보안기술 연구개발을 추진하고 있다.

## V. 결 론

지금까지 홈랜드 시큐리티 분야중에서 주요 사회기반시설을 운영하는 제어시스템과 제어시스템 환경에서의 사물지능통신 환경의 현황에 대해서 설명하였다. 사회기반시설은 사물지능통신 환경이 이미 제한적으로 사용되고 있지만 아직은 초기단계라고 볼 수 있으며, 세계 각국의 사회기반시설에 대한 사물지능통신 보안현황 역시 시작단계로 파악이 된다. 향후 사회기반시설 운영환경은 사물지능통신이 확대 적용되어 더욱 지능적으로 진화될 것으로 예상되며, 이러한 진화과정에서 반드시 사물지능통신의 사이버보안 위협에 대한 고려가 필요하다.

## 참고문헌


[1] 심인수, 이용균, "스마트 IT 신시장: Homeland Security 현황과 전망", *한국정보산업연합회*, pp. 1-4, 2011

[2] 주용완, "홈랜드 시큐리티 산업에 대한 이해와 대응방안", *정보통신산업진흥원*, pp.13-25, 2011.

[3] 김배억, "사물지능통신 정책추진 방향", *TTA Journal*, Vol. 134, pp. 34-41, 2011.

[4] Keith Stouffer, Joe Falco, and Karen Scarfone, Guide to Industrial Control Systems (ICS) Security, NIST SP800-82, pp. 2-1~2-13, June, 2011.

[5] ICS-ALERT-10-301-01, "Control System Internet Accessibility", ICS-CERT, October, 2010.

[6] ICS-ALERT-11-343-01, "Control System Internet Accessibility", ICS-CERT, December, 2011.

[7] D. Boswarthick, O. Elloumi, JM Ballot, "Smart Grids From the Machine to Machine Perspective," ETSI, April, 2010.

[8] Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier version 1.3", Symantec, November, 2010.

[9] "W32.Duqu The precursor to the next Stuxnet version 1.3," Symantec, November, 2011.

[10] "Global Energy Cyberattacks: Night Dragon," McAfee, February, 2011.

[11] Eric Chien and Gavin O Gorman, "The Nitro Attacks - Stealing Secrets from the Chemical Industry," Symantec, July, 2011.

[12] ICSB-11-327-01, "Illinois Water Pump Failure Report", ICS-CERT, November, 2011.

[13] http://www.inl.gov/scada/, "National SCADA Test Bed Program", 2012.

[14] http://www.us-cert.gov/control_systems/index.html, "Control System Security Program", 2012.

[15] http://www.escortsproject.eu/, "Security of Control and Real Time Systems", 2012.

[16] http://utmea.enea.it/projects/int/#estec, "ESTEC: The European Network of SCADA Security Test Centres for Critical Energy Infrastructure", 2012.

[17] http://www.vikingproject.eu/page16.php, "Modelling and assessment of Vulnerabilities of SCADA Systems and their effects", 2012.


## 〈著者紹介〉


사 진

**김 우 년 (Kim, Woo-Nyon)**
정회원
1996년 2월 : 안동대학교 컴퓨터공학과 졸업
1998년 2월 : 경북대학교 컴퓨터과학과 석사
2000년 2월 : 경북대학교 컴퓨터과학과 박사수료
2000년 3월~2003년 12월 : (주)니츠 선임연구원
2003년 12월~현재 : 한국전자통신연구원 부설연구소 선임연구원/과제책임
<관심분야> 정보보호, 제어시스템 보안