논문 2012-07-32

사이버-물리 시스템의 보안 프레임워크 개발을 위한 보안 요구사항 분석 연구

(The Study on the Cyber Security Requirements of Cyber-Physical Systems for Cyber Security Frameworks)

박 수 열, 최 욱 진, 정 보 흥, 김 정 녀, 김 주 만*
(Soo-Youl Park, Wook-Jin Choi, Bo-Heung Chung, Jeong-Nyeo Kim, Joo-Man Kim)

Abstract : A cyber-physical system(CPS) is a collection of cyber and physical components that interact with each other to achieve a particular application. Here, the CPS is emerged the reliability and security problems. Particularly, the defect of reliability in the data/control transmission under the CPS can lead to serious damage. We discuss the reliability and security problem on CPS architecture. Then we would suggest the considerations of cyber security in industrial control systems built with CPS.

Keywords : Cyber-physical systems, Cyber security, Embedded systems

Ⅰ. 서 론

IT기술의 점진적인 발전으로 인해 자동차, 항공, 철도, 교통, 전력, 국방, 자동화 생산 등 다양한 산업분야에 IT 기술이 점차 보편화되어 왔으며, 과거 기계식 및 유압식으로 제어되었던 제어 시스템에 IT 임베디드 컴퓨팅 및 네트워킹 기술을 적용함으로써 생산비용을 절감하고 신뢰성 및 성능을 크게 향상시켜왔다. 하지만 점차 증가하는 소프트웨어 복잡도로 인해 결함 발생 가능성이 증가하였고 이를 해결하기 위해 신뢰성 검증의 개발 비용 및 개발 기간이 증가하는 문제가 발생하였다. 게다가 태스크의 최악실행시간(WCET: Worst Case Execution Time)은 프로세서 아키텍처의 파이프라인, 메모리 계층 구조, 병렬 처리, 멀티코어 등 확률적으로 다뤄야 하는 불확실한 요소가 계속 증가하여 WCET을 예측하기가 매우 힘들어 졌다. 또한 소프트웨어의 증가는 제어 네트워크의 패킷 증가로 이어졌으며 네트워크 효율성을 극대화하기 위해 최악응답시간(WCRT: Worst Case Response Time)을 고려해야 한다. 이처럼 임베디드 시스템의 복잡도는 점점 증가하고 있다.

Lee, E.A. [1]는 제어 시스템의 복잡도 증가 문제는 제어 시스템과 IT기술 간의 차이점이 원인이라고 보고 있으며, 미래의 제어 시스템을 구현하기 위해서는 제어 시스템에 적합한 IT기술의 핵심 추상화 및 소프트웨어, 하드웨어, 네트워크의 기술에 변화가 필요하다고 보고 있다. 이러한 IT 분야의 재연구가 사이버-물리 시스템 연구의 출현 배경으로 볼 수 있다.

사이버-물리 시스템의 응용 분야는 고신뢰성이 요구되는 시스템으로 결함 발생 시에 범국가적인 인적 물적 손실을 초래할 수 있다. 또한 컴퓨팅 및 네트워킹이 사이버-물리 시스템의 핵심 기술로 사용될 것이기 때문에 사이버 위협이 더욱 증가할 것이다.

본 논문은 분산 제어 시스템 및 사이버-물리 시스템에서 예상되는 사이버 보안 취약점을 분석하고 이를 해결하기 위한 보안 대응책에 대해 연구하였으며 구성은 다음과 같다. 제 Ⅱ장에서는 사이버-물리 시스템의 개념을 기술하고. Ⅲ장에서는 보안 연구의 사례 연구로서 분산 제어 시스템의 구조 및 취약성, 사고사례를 살펴본다. 그리고 Ⅳ장에서 사이버-물리 시스템에서 요구되는 보안 대응책을 정리하고, 마지막 Ⅴ장에서 본 연구의 결론을 맺는다.

* 교신저자(Corresponding Author)
논문접수 : 2012. 08. 10., 수정일 : 2012. 09. 19.,
채택확정 : 2012. 10. 04.
박수열, 최욱진, 김주만 : 부산대학교 IT응용공학과
정보흥, 김정녀 : 한국전자통신연구원

ⓒ J. IEMEK 2012 Oct.: 7(5) 255-265
ISSN : 1975-5066

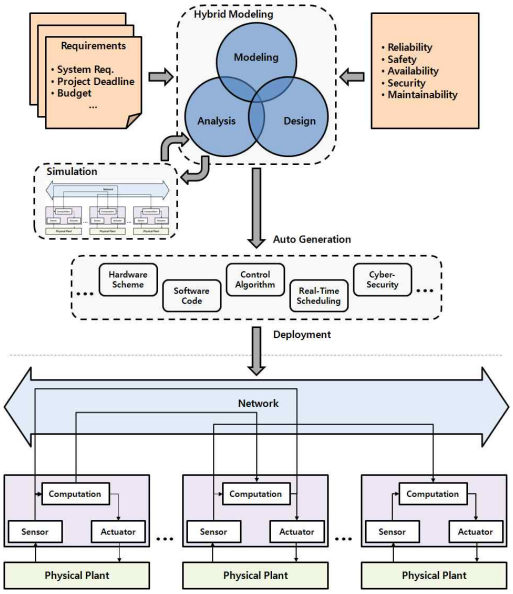


그림 1. 사이버-물리 시스템 아키텍처
Fig. 1. Cyber-Physical Systems Architecture

Ⅱ. 사이버-물리 시스템

IT기술의 점진적인 발전으로 인해 다양한 산업 분야에 IT 기술이 점차 보편화되어 왔으며, 과거 기계식 및 유압식으로 제어되었던 제어 시스템에 IT 임베디드 컴퓨팅 및 네트워킹 기술을 적용함으로써 생산비용을 절감하고 신뢰성 및 성능을 크게 향상시켜왔다. 현재 이러한 임베디드 기술은 제어 시스템에 없어서는 안 될 핵심 기술로 자리 잡았다.

하지만 미래의 제어 시스템의 구현에 있어 현재의 IT기술이 갖는 자원의 제약성과 서비스 연동의 결여 및 표준화 미흡으로 확장 개발에 많은 어려움을 예상하고 있으며, 이러한 문제를 해결하고 신뢰성, 확장성 및 안정성을 확보하기 위하여 하드웨어, 소프트웨어, 네트워크 등 모든 IT 분야의 재연구가 필요하다고 보고 있다. 즉 이러한 모든 IT 분야의 재연구의 필요성이 사이버-물리 시스템 연구의 출현 배경으로 볼 수 있다 [1].

사이버-물리 시스템(Cyber-Physical Systems: CPS)은 자동차, 항공, 제조 및 국가 기반 시설(국방, 우주, 화학, 도시기반, 에너지, 국민건강, 교통 분야 등)을 포함하는 제어 시스템(Control Systems) 분야에 혁신적인 발전에 기여할 수 있는 IT 기반 기술을 찾아 한계를 극복하기 위한 연구이다. 즉 기존의 제어 시스템에 컴퓨팅과 네트워킹을 더욱 강화함으로써 물리적 요소와 더욱 긴밀히 작용하는 혁신적인 고신뢰성 분산 제어 시스템의 구축을 돕는 기술을 의미한다.

사이버-물리 시스템으로 볼 수 있는 미래의 제어 시스템들은 21세기의 IT 혁명을 뛰어 넘는 잠재력을 지니고 있다. 시간 정밀도 및 안전이 중요한 스마트 그리드(Smart Grid)의 전력 분산 제어와 교통 시스템의 안전성과 효율성을 상당히 개선 할 수 있고, 네트워크 자율 주행은 무인자동차시스템 뿐만 아니라 군사 시스템, 재난 복구 기술에 응용 할 수 있다. 네트워크 빌딩 제어 시스템(HVAC: Heating, Ventilation, and Air Conditioning)은 에너지 효율성을 개선하여 화석연료의 의존성 및 온실가스 배출을 상당히 줄일 수 있다. 이러한 사이버-물리 시스템의 응용 도메인들은 현재 직면한 에너지 부족, 지구온난화, 인구고령화 문제를 해결 할 수 있는 엄청난 경제적 파급효과를 지니고 있다.

사이버-물리 시스템은 그림 1과 같이 물리적 환경의 정보 수집, 탐색 및 제어를 위한 임베디드 시스템들이 네트워크망에 연결되어 전체 가상 제어 시스템을 구성하는 고신뢰성을 추구하는 분산 네트워킹 시스템이다. 사실 이러한 시스템의 형태는 기존의 임베디드 시스템 및 분산 제어 시스템에서도 볼 수 있지만, 사이버-물리 시스템 기술은 컴퓨팅 및 네트워킹의 신뢰성 향상 기술 외에도 시스템 모델링, 설계, 분석, 시뮬레이션 기술 등 시스템 개발에 필요한 모든 기술을 포함하고 있다. 물론 이러한 노력은 제어 시스템의 특정 도메인 내에서도 각각 연구 중에 있으며, 일부 중복되는 부분도 있다.

사이버-물리 시스템의 응용 도메인들은 기존의 임베디드 시스템 및 분산 제어 시스템과 같이 시스템의 안전을 위한 고신뢰성이 요구되며, 에너지, 실시간성, 메모리 사이즈, 무게, 개발비용 및 유지보수 비용 절감 등의 효율성을 반드시 고려해야만 한다 [2].

신뢰성 요구사항(Dependability Requirements)은 신뢰성, 안전성, 정비성, 가용성, 보안성의 5가지 측면을 요구한다. 첫째, 시스템의 결함 발생률을 확률적으로 최소화하여 신뢰성(Reliability)을 보장해야 한다. 둘째, 시스템이 어떠한 피해도 발생하지 않도록 안전성(Safety)을 유지해야 한다. 셋째, 시스템에 결함이 발생할 경우 확정적 시간 내에 시스템을 복구 또는 교체 가능한 정비성(Maintainability)을 지녀야 한다. 넷째, 시스템은 항상 사용가능한 가용성(Availability)을 유지해야 하며, 신뢰성 및 정

비성과 연관성이 깊다. 다섯째, 보안성(Security)을 반드시 보장해야 한다.

신뢰성 요구사항과 더불어 5가지 효율성을 고려해야 한다. 첫째, 제어 시스템의 실시간성을 반드시 보장해야 한다. 둘째, 성능 범위 내에서 에너지를 최소한으로 사용해야 한다. 셋째, 한정된 자원(개발 기간 및 비용) 내에서 최적화 개발이 필요하며, 관리 및 유지보수 비용 또한 고려해야 한다. 넷째, 임베디드 시스템의 한정된 자원 제약사항으로 CPU/MCU성능 및 메모리 최적화를 고려하여 설계해야 한다. 넷째, 임베디드 시스템의 이동성 및 크기, 위치를 고려하여 하드웨어의 경량화, 집적화, 또는 분산화해야 한다.

이러한 요구사항과 효율성 고려사항은 현재의 임베디드 시스템 및 분산 제어 시스템에서도 요구되지만 사이버-물리 시스템은 더욱 복잡한 시스템이므로 설계 및 구현 복잡도가 기하급수적으로 증가하게 된다. 사이버-물리 시스템은 이러한 복잡도를 해결해야 한다.

Ⅲ. 사이버-물리 시스템의 잠재적 사이버 보안 위협

사이버-물리 시스템은 무인자동차 및 항공분야 뿐만 아니라 산업기반 및 국가기반시설을 구축하는 “관리 감독 자료 수집“(SCADA: Supervisory control and data acquisition) 시스템을 대체하는 시스템으로 발전할 것이다. 사이버-물리 시스템에서 신뢰성을 보장하지 못한다면 범국가적 피해 및 인명사고로 이어질 수 있다. 본 절에서는 사이버-물리 시스템의 응용 도메인인 일부 제어 시스템의 구조를 살펴보고 사이버-물리 시스템에서 발생할 수 있는 잠재적인 사이버 보안 위협에 대해 살펴본다.

1. 산업 제어 시스템

산업 제어 시스템(ICS: Industrial Control Systems)은 여러 타입의 제어 시스템을 포함하는 용어로서, 주요 기반 시설 및 산업 시설에서 볼 수 있는 SCADA 시스템, 분산 제어 시스템(DCS:Distributed Control Systems), 프로그램 로직 컨트롤러(PLC: Programmable Logic Controller) 등 다양한 시스템이 혼합되어 구성된다 [3].

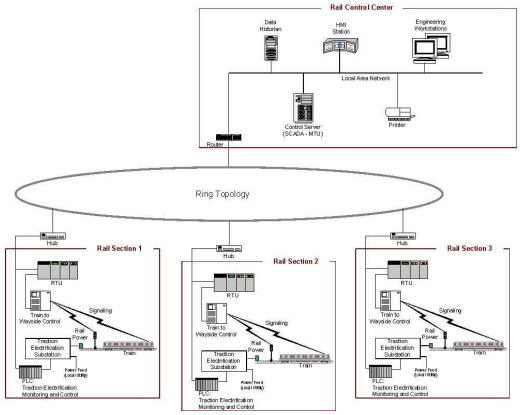


그림 2. SCADA 시스템 구성 [3]
Fig. 2. SCADA Architecture [3]

1.1 SCADA 시스템

SCADA 시스템은 중앙 집중 자료 수집 및 제어 시스템으로서 지형적으로 광범위하게 분포된 시스템들을 제어하는 분산 시스템이다. 수자원 공급 및 폐수처리 시스템, 오일 및 천연가스 배송관, 스마트 그리드, 철도관리 시스템과 같은 분산 시스템에 사용되며 실시간 제약조건과 고신뢰성이 요구된다. SCADA 컨트롤 센터는 원거리 지역을 통신 네트워크로 모니터링하고 제어한다. 현장의 제어 장치들은 중앙 시스템으로부터 받은 제어 커맨드로 밸브 등을 제어하고, 센서 시스템으로부터 데이터를 수집하고 현장의 환경 상태를 감시한다. 제어 시스템의 특성상 하부 네트워크는 필드버스(FieldBus)로 구성되어 있으며, 중간 네트워크는 산업용 이더넷(Industrial Ethernet), 상위 네트워크는 인트라넷(Intranet)으로 구성된 계층적 네트워크 형태를 가진다. 하부 네트워크에는 센서와 액추에이터가 연결된 RTU(Remote Terminal Unit) 및 PLC로 연결되어 있다 (그림 2).

1.2 분산 제어 시스템

분산 제어 시스템(DCS)은 전력 생산, 수자원 정화, 화학, 식품, 자동차생산과 같은 제어 산업 공정에 광범위하게 사용되고 있다. DCS는 세부공정 제어를 담당하는 서브-시스템들을 감독한다. 생산 및 공정 제어는 일반적으로 피드백(feedback) 또는 피드포워드(feed forward)로 명시된 설정 값을 자동으로 유지한

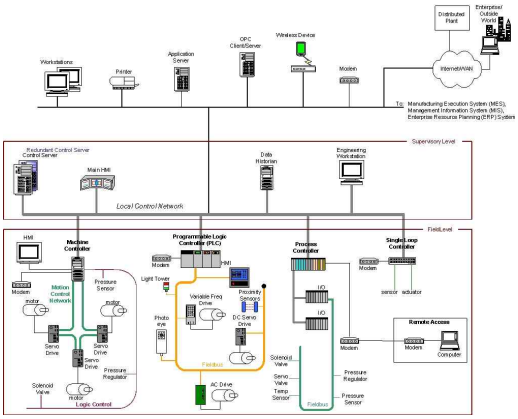


그림 3. 분산 제어 시스템 구성 [3]
Fig. 3. DCS Architecture [3]

다. DCS 아키텍처는 다음 그림 3과 같다.

1.3 프로그램 로직 컨트롤러

프로그램 로직 컨트롤러(PLC)는 SCADA 및 DCS에서 사용하는 제어 시스템이며 대부분의 산업 공정에서 사용하고 있다. PLC는 I/O제어, 타이밍, PID제어, 통신 등과 같은 특정 기능 수행을 하며, 응용에 따라 구성이 다양하다 (그림 4).

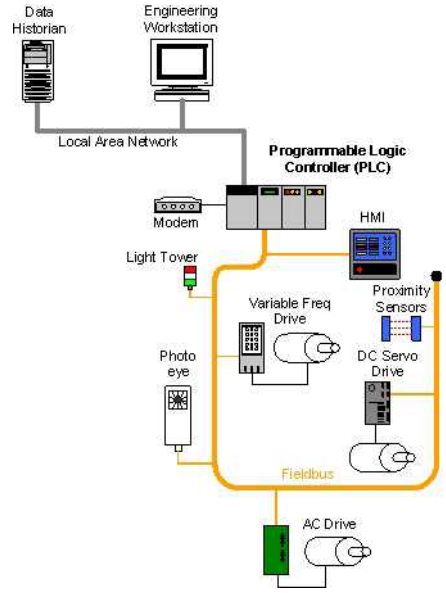


그림 4. 프로그램 로직 컨트롤러 구성 [3]
Fig. 4. PLC Architecture [3]

2. 보안 취약성 및 사고 사례

산업 제어 시스템은 마이크로프로세서 및 네트워크의 혁명 시기인 1980~1990년대에 개발되었고, 1990년 후반에 들어 인터넷 기술을 도입한 이후 외부 네트워크와의 연결이 점차 늘어나고 있다. 산업 제어 시스템들은 성능, 신뢰성, 안전성, 유연성의 요구 조건을 만족하도록 대부분 독자적인 하드웨어, 소프트웨어, 통신 프로토콜을 사용하여 외부 네트워크로부터 격리되어 설계되었으나 운용 효율성을 위해 외부 상호시스템의 연결이 점차 늘어나고 있다. 그리고 SCADA 시스템에 사용된 프로토콜은 과거 벤더 별 독립 프로토콜을 사용하였으나 표준화 기술의 발전과 더불어 표준 프로토콜을 사용함으로써 사이버 공격자들이 내부 프로토콜을 알기 쉬워졌다. 또한 인터넷의 보급으로 SCADA 시스템의 설계 문서에 쉽게 접근 가능하며, 해킹툴을 사용한 사이버 공격 또한 쉬워졌다. 이러한 변화로 인해 과거에는 볼 수 없었던 새로운 위험과 취약성이 점차 증가하고 있다.

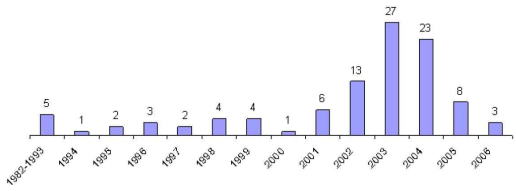


그림 5. 연간 산업안전사고 [3]
Fig. 5. Industrial Security Incidents by Year [3]

제어 시스템에 대한 사이버 사고를 살펴보면 IT 시스템에 노출된 취약성과 제어 시스템에서 발견된 취약성 간의 유사한 경향을 살펴볼 수 있다. 제어 시스템 및 공정에 직접적인 영향을 주는 보안 사고를 다루는 “Repository of Industrial Security Incidents (RISI)”는 고의적인 무단 원격 액세스, DoS(Denial of Service) 공격, 악성코드 침투와 같은 사고뿐만 아니라 고의성 없는 사이버 사고들도 포함하고 있으며, 신뢰성의 피해 정도를 평가하여 등급을 매기고 있다. 그림 5는 1982년도에서 2006년 사이의 사고 동향을 나타내며, 2001년부터 사고가 급격히 증가함을 알 수 있다. 2006년 6월 시점으로 119건의 사고가 조사되어 데이터베이스에 기

록되었고, 이와 더불어 15개의 사고 접수 건은 진상조사 전 시점이라 그림 5에는 포함되지 않았다.

특정 제어 시스템을 목표로 한 공격 사례는 대표적인 예로서 Stuxnet을 들 수 있다. Stuxnet은 지멘스사(SIEMENS)의 SCADA 장비로 구축된 이란의 원자력발전소의 폭발을 시도한 바이러스로서, 설계문서 해킹, USB를 통한 침투, DLL (Dynamic Linking Library)의 변경, PLC의 펌웨어 변경 등 지금까지 발견된 바이러스 중 가장 정교한 것으로 알려져 있다 [4]. 그림 6은 CSADA 시스템을 공격한 Stuxnet의 공격 경로를 나타낸다. 스마트 그리드는 광역 네트워크 특성으로 불가피하게 보안에 취약한 이더넷을 기반으로 구축이 예상되며 Stuxnet과 같이 사이버 공격의 목표물이 될 것이다. 스마트 그리드의 사이버 공격 피해는 대규모정전사태(Black Out)가 발생 가능하며 이는 생산시설 가동 중단 및 의료서비스 중단 등의 도미노사태로 이어질 수 있어 국가 전체에 인적 물적 피해를 초래할 수 있다 [5].

또한 자동차에서도 사이버 공격이 가능하다는 연구 결과가 있다. 최근 차량의 OBD-II (On-Board Diagnostics)에 스마트폰을 연결하거나 네비게이션 또는 오디오와 같은 컴퓨팅 요소가 차량 내부 CAN(Controller Area Network) 네트워크와 연결되어 무선 인터넷을 통한 다양한 편의 서비스를 제공하고 있으며 서비스를 계속 확대해 나가고 있다. 이러한 차량 내부와 차량 외부 통신을 연결하는 장치들로 인해 자동차전자제어 시스템에도 고의적인 사이버 공격으로 차량 ECU(Electronic Control Unit)의 오동작을 일으킬 수 있다. CAN네트워크는 CSMA/CA(Carrier Sense Multiple Access / Collision Avoidance) 브로드캐스팅 방식의 통신으로 메시지의 실시간성을 보장해 주지만 쉽게 도청 가능하며 보안에 매우 취약하다 [6].

앞서 살펴본 제어 시스템의 취약점을 정리해 보면 다음과 같다. 첫째, 인터넷의 발전으로 공개기술과 관련된 문서 취득이 쉬워졌고 제어 시스템 개발 시 여러 기업 및 기관이 참여하기 때문에 사이버 공격자들에게 악용될 수 있는 설계 자료의 유출 가능성이 커졌다. 둘째, 제어 시스템의 광역 네트워크 망은 개발 예산 문제로 인해 이더넷 프로토콜을 불가피하게 사용함으로써 사이버 공격에 노출되었다. 셋째, CAN통신과 같은 대부분의 제어 네트워크 기술들은 보안이 전혀 고려되지 않아 사이버 공격에 매우 취약하다. 넷째, 사이버 공격에 노출된 범용 운영체제를 일부 시스템으로 구성한 제어 시스템은

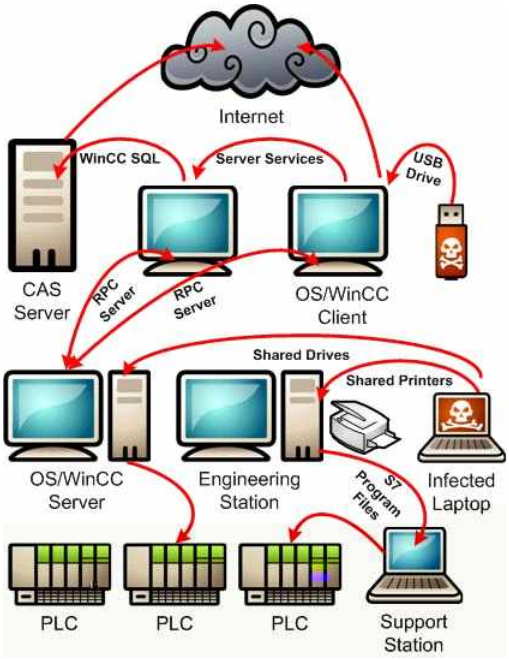


그림 6. 지멘스 PCS 7 오브젝트를 공격한 Stuxnet [7]
Fig 6. Stuxnet hitting Siemens PCS 7 objects [7]

보편화된 사이버 공격 기술에 노출되어 있다. 다섯째, USB 및 고장진단장치를 비롯한 모든 외부 연결장치에 대해 사이버 공격 가능성에 대한 인식이 부족하였다. 여섯째, 제어 시스템을 이루는 서브시스템들의 지형적 접근의 어려움이나 편리성 등의 문제로 사이버 보안에 취약한 무선통신 또는 제어네트워크를 통한 원격진단 및 시스템 업그레이드 등의 유지보수를 하기 때문에 이러한 백도어는 항상 존재하며 사이버 공격자들에게 악용될 우려가 있다.

Ⅳ. 안전한 사이버-물리 시스템을 위한 사이버 보안 대응책

1. 보안의 원칙

사이버-물리 시스템 구조의 각 계층에는 각종 위협에 대한 세가지 원칙 즉, 기밀성, 무결성 그리고 가용성을 가진다. 이것은 일반 보안의 원칙이기도 하지만 특히 사이버-물리 시스템의 응용 도메인인 국가기반시설의 중요한 역할로 볼 때, 이러한 원칙이 반드시 지켜져야 할 것이다. 이들 세 가지 원칙 중 어느 하나라도 위배된다면 시스템의 신뢰

표 1. 악의적 사이버 위협
Table 1. Adversarial Threats

위협 요소	내용
Attacker	해커의 실력을 과시하기 위한 공격.
Bot-network operators	시스템에 침입하여 접근 권한을 취득, 스팸 및 악성코드 등을 배포함.
Criminal Groups	금전적 이득 목적의 범죄 집단의 공격.
Foreign Intelligence services	외교기밀정보를 수집하는 간첩 활동.
Insiders	불만을 가진 내부 관계자.
Pishers	개인 또는 소규모 조직의 금전적 이득을 목표로 공격. 스팸 및 스파이웨어/악성 코드를 사용.
Spyware/ Malware	악의적 개인이나 조직은 스파이웨어 및 악성 프로그램을 제작하고 배포.
Terrorists	주요 인프라를 공격, 국가 안보 위협.
Industrial spies	지적 재산권 및 노하우 취득 목표.

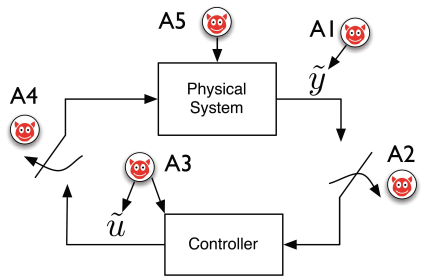


그림 7. 사이버-물리 시스템 공격 [8]
Fig. 7. Attacks on Cyber-Physical Systems [8]

성은 보장되지 않는다. 사이버 보안의 가장 중요한 원칙이며, 이러한 세 가지 원칙하에 다양한 보안 이슈를 고려 할 수 있을 것이다.

첫째, 기밀성(Confidentiality)은 권한이 없는 사람이나 객체로부터 정보의 유출을 막고자 함에 있다. 기밀성의 부재는 정보유출 문제로 이어진다. 둘째, 무결성(Integrity)은 데이터 또는 자원의 신뢰성을 말하며 정보에 대한 정보의 변경이나 훼손을 방지하는데 있다. 무결성의 부재 또한 시스템의 오동작을 유발하여 막대한 피해를 입게 될 것이다. 셋째, 가용성(Availability)은 어떤 권한이 없는 사람이나 객체에 의해 시스템 가동이 중지되는 일이 없게 하는데 있다. 시스템이 중지된다는 것은 치명적 결과를 초래할 수 있다.

표 2. CPS와 IT시스템의 차이점
Table 2. Differences of between CPS and IT Systems

분류	IT시스템	사이버-물리 시스템
성능	비실시간성 일관된 응답성 빠른 처리 지연 및 지터 허용가능	실시간성 시간중요 응답성 적시성 처리 지연 및 지터 허용불가
가용성	재부팅 허용. 가용성 결함은 운영요구사항에 따라 허용.	가용성으로 재부팅 허용불가. 또는 중복 시스템 사용으로 재부팅하여 가용성 유지. 운영중단은 사전 계획 실시. 철저한 사전 테스트 필요.
위험관리	데이터 기밀성과 무결성이 주요 목표. 내고장성이 필수는 아님. 결함의 주요 위험은 비즈니스의 지연 측면.	생명 안전이 주요 목표. 내고장성이 필수. 순간적 운영 중단도 허용하지 않을 수 있음. 결함은 환경 영향과 생명, 장비, 생산의 손실 발생.
보안 설계 초점	정보 보호에 중점. 중앙서버의 보호 필요.	모든 시스템 및 정보 보호.
보안 솔루션	일반적 IT시스템에 설계된 보안 솔루션.	보안 솔루션이 시스템의 가용성을 손상시키지 않아야 함.
시스템 운영 및 변경 관리	범용 시스템으로 설계. 자동 업그레이드.	보안 패치에 앞서 CPS 테스트베드에서 시스템 전반에 걸쳐 철저한 테스트를 진행하여 무결성 및 가용성을 유지해야 함.
자원 제약	보안 솔루션을 지원하기 위한 충분한 자원을 가짐.	시스템 특성 상 메모리 및 리소스 부족으로 보안 기능 추가의 어려움이 있음.
통신	표준 통신 프로토콜.	다양한 프로토콜이 혼재되어 네트워크가 상당히 복잡함.

2. 사이버 공격 정의 및 보안 위협 요소

사이버-물리 시스템의 안전 위협은 적대국가, 테러 집단, 산업 스파이, 침입자에 의해 발생하거나, 시스템의 복잡도, 인간 오류 및 사고, 장비 고장 및 자연재해 등 다양하다. 표 1은 악의적 사이버 위협 요소를 나타낸다.

사이버-물리 시스템에 대한 악의적인 공격 경로는 그림 7과 같다. A1과 A3는 센서 또는 컨트롤러에서 거짓 정보를 전송하는 디셉션(deception)공격을 나타낸다. 공격자(adversary)는 비밀키를 획득하거나 일부 센서(A1) 또는 컨트롤러(A3)를 손상하여 공격할 수 있다. A2와 A4는 DoS 공격을 나타낸다. 공격자는 통신 채널에 부하를 가중시키거나, 송수신 데이터를 차단하고 라우팅 프로토콜을 공격한다. A5는 액추에이터 또는 플랜트에 대한 물리적 공격을 나타낸다 [8].

3. IT보안과 CPS보안 차이점

사이버-물리 시스템은 이기종의 유무선 네트워크와 다양한 프로토콜의 혼재되고 제어 시스템의 특징을 가지므로 기존 인터넷 등에서 발생되는 보안 고려사항과는 다른 특징을 많이 가지고 있다. 사이버-물리 시스템의 실시간성의 특성상 보안 소프트웨어 및 보안 하드웨어는 시스템의 가용성에 영향을 주어서는 안 되며 보안 시스템의 업그레이드 등의 이유로 재부팅이 불가능하므로 재부팅이 불가피 할 경우를 대비한 중복 시스템을 도입하여 가용성을 유지해야 한다. 또한 내고장성(Fault-tolerant)을 반드시 유지해야 하므로 사이버 공격 시 예상되는 결함 단계를 설정하고 대책을 마련해야 하고 사이버-물리 시스템도 현재의 임베디드 시스템과 같이 자원제약을 고려하여 보안 솔루션을 적용해야 한다. 표 2는 사이버-물리 시스템과 IT시스템의 차이점을 나타낸다 [3].

4. 위험 분류

사이버-물리 시스템을 이루는 서브시스템들의 기능에 따라 안전중요도는 다르다. 일부 서브 컴포넌트 시스템의 결함은 전체 시스템 운영에 미비한 장애를 초래하는 반면, 어떤 시스템들은 전체 시스템을 마비시키는 치명적 손상을 초래할 수 도 있다. 예를 들어, CPS-스마트 그리드에서 각 가정의 전력 사용량에 대한 일부 보안 침입은 전체 성능에 큰 영향을 미치진 않지만, 이 정보를 취합한 시 단위의 정보들에 대한 침입은 전체 시스템의 운영 성능에 큰 피해를 입힐 수 있다. 반면, CPS-메디컬의 경우 개인 프라이버시를 침해 할 수 있는 작은 정보단위 조차 매우 중요한 경우도 있다. 따라서 사이버-물리 시스템은 응용 도메인에 따라 사이버 보안정책은 다르게 적용되어야 하며 프라이버시 보호와 같은 운영목적 이외의 피해에 대해서도 반드시 고려해야 한다.

사이버-물리 시스템의 서브 컴포넌트의 결함 발생 시 피해정도를 예상하여 DO-178B의 위험 단계와 같이 분류하여 보안대책을 세울 수 있을 것이다. 표 3은 사이버-물리 시스템의 위험단계를 나타낸다.

표 3. 사이버-물리 시스템 위험 단계
Table 3. CPS Criticality Level

위험단계	영향
4	CPS의 운용통제가 불가능하여 치명적인 손상 및 대규모 재앙 발생(환경 파괴 및 인명 피해)
3	CPS에 치명적 손상을 입으며 정상적인 운용이 매우 힘들어짐. 적절한 대응을 하지 않을 경우 4단계로 진행
2	CPS 운용에 일부 장애가 있으나 위험한 수준은 아님
1	장애 상태가 2단계보다 덜한 상태
0	시스템의 운영에는 영향을 미치지 않는 일부 장애

5. 사이버 보안 대응책

사이버-물리 시스템의 응용 도메인은 매우 다양하며 보안요구사항 또한 적용 도메인 및 서브시스템에 따라 다양하다. 본 절에서는 사이버-물리 시스템에서 공통적으로 요구되는 최소한의 보안 대책에 대해 기술한다.

5.1. 일반적인 보안 요구사항

(1) 시스템 상호 인증: 인가된 시스템 간의 안전한 통신을 보장하기 위해 상호 인증이 요구된다.

(2) 사용자 인증: 사이버-물리 시스템은 운영자의 직접적인 조작을 최소화한 완전 자율 시스템을 목표로 한다. 하지만 임무지령, 유지보수, 비상사태 등과 같은 운영관리에 운영자의 개입을 완전히 배제할 수 없다. 비권한자의 불법적 접근을 막기 위해 신원확인을 위한 사용자 인증이 필요하다.

(3) 암호화: 사이버-물리 시스템의 네트워크에 불법으로 접속하여 패킷 위변조를 발생하는 중간자 공격(man-in-middle attack)이 발생한다면 네트워크 내의 다른 시스템들을 혼란시키거나 시스템 상호인증 과 같은 중요한 정보가 유출될 수 있으므로 기밀성을 유지하기 위해 암호화가 필요하다.

(4) 접근 제어: 접속하는 시스템의 역할에 따라 허용할 수 있는 서비스의 범위를 제한해야 한다. 이는 사이버 공격에 시스템이 오염되었을 경우 피해를 최소화할 수 있다.

(5) 방화벽: 패킷 위변조의 중간자 공격이 발생할 경우 이를 감지하고 필터링 할 수 있는 네트워크 방화벽이 필요하다. 또한 물리적으로 동일한 네트워크라도 방화벽을 사용하여 논리적으로 격리함으로써 접근가능성을 최소화해야 한다.

(6) 중복성 및 내고장성: 사이버-물리 시스템에서 가용성은 필수요소다. DDoS/DoS와 같이 가용성에 손실을 주는 공격 발생한다면 시스템은 신뢰할 수 없을 것이다. 이러한 실패 단일 지점

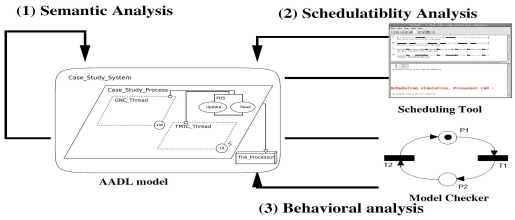


그림 8. AADL 모델 개발 [9]
Fig. 8. Exploiting AADL models [9]

(Single Point of Failure)을 없애기 위해 백업 네트워크 등을 대비하여 가용성을 유지해야 한다. 또한 사이버 공격으로 인해 일부 시스템이 손상되더라도 전체 시스템 운영의 피해를 최소화해야 한다.

(7) 네트워크 모니터링: 침입탐지, 네트워크 결함 등을 감지하기 위해 네트워크 모니터링이 필요하다. 또한 네트워크에서 데이터 패킷 흐름을 추적할 수 없다면 사이버 공격의 발생 시간, 발생 경로 등의 정확한 파악이 불가능 할 것이다. 그러므로 네트워크 패킷 추적이 가능한 데이터를 전용 데이터 저장 서버에 보관하여 보안 문제 발생 시에 추적 가능해야 한다.

(8) 백도어 관리: 사이버-물리 시스템은 대규모 분산 시스템이기 때문에 유지보수 편리성을 위한 원격 시스템 업그레이드와 같은 백도어가 반드시 존재한다. 백도어가 해커에 노출될 경우 시스템의 안전은 보장되지 않으므로 철저히 관리되어야 한다.

5.2. 정책상의 보안 요구사항

(1) 설계 문서 보호 : 설계 문서가 사이버 공격자에게 노출되지 않도록 문서 암호화 등의 정책 도입이 요구된다.

(2) 직원의 윤리 교육 강화 : 내부 불만을 가진 직원은 사이버 테러 집단이 원하는 인적 물적 피해를 쉽게 유발할 수 있으므로 직원 윤리 교육이 반드시 필요하다.

5.3. 사이버 보안 솔루션의 도구 통합 필요성

사이버-물리 시스템의 보안 메커니즘은 시스템의 타이밍 변화에 영향을 줄 수 있으며 이는 제어 시스템의 성능에 영향을 끼칠 것이다. 또한 보안 소프트웨어, 보안 하드웨어, 모니터링 장치와 같은 보안 메커니즘과 개발비용, 에너지 소모, 컴퓨팅 및 네트워크 이용률(utilization) 손실과의 trade-off가 반드시 필요하다. 그러므로 다른 자원들과 마찬가지로 사이버 보안 정책 또한 모델링 및 설계 도구에 통합되어야 할 것이다.

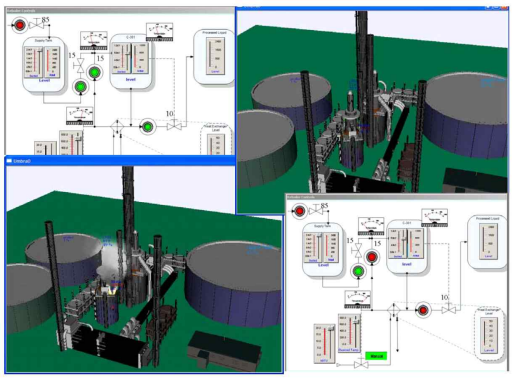


그림 9. 사이버 공격 피해의 전후 상황에 대한 소형 정제소의 VCSE 모델
Fig. 9. VCSE model of a small refinery before and after a damaging cyber attack

보안 메커니즘의 도구 통합에 앞서 보안정책이 컴퓨팅 및 네트워킹에 영향을 주는 상관관계를 분석하고 핵심 추상화에 대한 연구가 선행되어야 할 것이다. 임베디드 시스템에서 태스크 스케줄링 연구는 비율 단조 스케줄링(RMS: Rate Monotonic Scheduling) 및 최단 마감 우선 스케줄링(EDF: Earliest Deadline First)을 기반으로 하여 전력 절감 실시간 태스크 스케줄링 연구 [10]를 비롯한 다양한 연구가 진행된 반면, 제어 시스템의 특성상 사이버보안을 고려한 태스크 스케줄링 연구는 부족하였다 [11]. 또한 제어네트워크에서 내고장성을 유지하기 위한 연구는 많았지만 사이버보안을 고려한 기술 및 연구가 부족한 것으로 보인다 [12].

Ayan Banerjee 등 [13]은 제어 시스템 분석 및 설계 도구인 AADL(Architecture Analysis and Design Language)를 사용하여 BAN(Body Area Network) 기반 CPS-메디컬 분야를 연구 중에 있다.

AADL은 SAE(Society of Automotive Engineers)에서 표준으로 지정한 디자인 언어로서 분산 제어 시스템뿐만 아니라 항공전자의 ARINC653 설계 또한 가능한 범용 도구로 발전

하고 있으며 보안 솔루션을 적용한 설계에 적합할 것으로 보인다. AADL은 이클립스 기반의 OSATE 도구와 TOPCASED 도구를 통해 지원하며, Simulink 연동, UML2.0을 임베디드 시스템 모델링에 적합하게 변형한 MARTE(Modeling and Analysis of Real Time and Embedded Systems)와의 연동, 소스 자동생성 도구인 Ocarina와의 연동, 시뮬레이션 도구인 Maude와 연동 등 다양한 지원 도구와 연동된다 [9, 14](그림 8). 또한 사이버-물리 시스템 설계에 부족한 부분의 보완하기 위해 CPS Annex를 연구 중에 있으며 Annex 표준 등록을 목표로 하고 있다. 여기서 Annex란 UML에서 프로파일의 개념과 같이 확장의 개념이다 [15]. 그리고 사이버-물리 시스템의 유지보수 및 운영자 교육을 위한 시뮬레이션 개발 또한 필요하다. Sandia National Lab. [16]에서 연구한 VCSE(Virtual Control System Environments) (그림 9)와 같은 제어 시스템 시뮬레이션환경도 동시에 개발하여 시스템 분석가에게 사이버 보안 위협 분석을 위해 제공하고 시스템 운영자에게 사이버 보안 이슈 교육 목적으로 사용 가능하도록 해야 할 것이다.

V. 결 론

본 연구는 사이버-물리 시스템의 보안 프레임워크 설계를 위한 기초 연구로서 먼저 사이버-물리 시스템의 정확한 정의에 대해 우선 살펴보았다. 사이버-물리 시스템의 응용 도메인 일부는 현재의 SCADA 시스템으로 구축된 국가기반시설을 대체할 것으로 예상되며 이러한 국가기반시설에 대한 사이버 공격은 범국가적인 인적 물적 피해를 입게 될 것이므로 사이버 보안정책이 반드시 고려되어야할 것이다.

본 논문에서는 IT 보안 정책을 그대로 활용할 수 없는 사이버-물리 시스템의 포괄적인 보안 요구사항에 대해 연구하였지만, 응용 도메인에 따라 보안 요구사항이 크게 달라질 수 있으므로 향후 특정 도메인에 대한 세부적인 보안 연구가 반드시 필요할 것이다. 또한 보안 솔루션은 사이버-물리 시스템의 가용성에 영향을 줄 수 있으므로 모델링 도구에 통합된 설계가 반드시 필요할 것이다.

본 연구의 결과는 사이버-물리 시스템의 보안 프레임워크 설계 연구의 기초 연구로 활용할 계획이며, AADL 도구를 활용하여 사이버-물리 시스템의 사이버 보안 연구를 확장해 나갈 계획이다.

참고문헌

[1] E.A. Lee, “Computing Foundations and Practice for Cyber-Physical Systems: A Preliminary Report,” Technical Report No. UCB/EECS-2007-72, Electrical Engineering and Computer Sciences, University of California at Berkeley, 2007.

[2] H. Kopetz, "Real-Time Systems - Design Principles for Distributed Embedded Applications," Springer, 2011.

[3] K. Stouffer, J. Falco, K Scarfone, "Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology (NIST), 2011.

[4] N. Falliere, L.O. Murchu, E. Chien, “W32. stuxnet dossier,” White paper, Symantec Corp., Security Response, 2011.

[5] G.N. Ericsson, "Cyber security and power system communication—Essential parts of a smart grid infrastructure," IEEE Transactions on Power Delivery, Vol. 25, No. 3, pp.1507-1507, 2010.

[6] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel and others, “Experimental Security Analysis of a Modern Automobil,e” Proceedings on IEEE Symposium on Security and Privacy, pp.447-462, 2010.

[7] www.isssource.com/stuxnet-report-ii-a-worm%E2%80%99s-life/

[8] A.A. Cardenas, S. Amin, S. Sastry, “Secure Control: Towards Survivable Cyber-Physical Systems,” Proceedings on ICDCS'08, pp.495-500, 2009.

[9] J. Hugues, B. Zalila, L. Pautet, F. Kordon, "Rapid prototyping of distributed real-time embedded systems using the aadl and ocarina," Proceedings on RSP'07, pp.106-112, 2007.

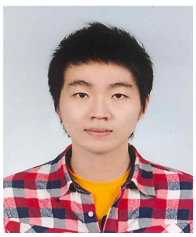
[10] 조수연, 김남진, 이은령, 김재영, 김주만, “자동차 전장 시스템에서 주기 및 비주기 태스크를 위한 실시간 스케줄링,” 대한임베디드공학회논문지, Vol. 6, No. 02, pp.55-61, 2011.
[11] L. Sha, T. Abdelzaher, K.E. Årzén, A. Cervin, T. Baker, A. Burns, G. Buttazzo, M. Caccamo, J. Lehoczky, A.K. Mok, "Real time scheduling theory: A historical perspective," Journal Real-Time Systems, Vol. 28, No. 2, pp101-155, 2004.
[12] N. Navet, F. Simonot-Lion, “Automotive Embedded Systems Handbook,” CRC Press, 2009.
[13] A. Banerjee, K.K. Venkatasubramanian, T. Mukherjee, S.K.S. Gupta, "Ensuring Safety, Security and Sustainability of Mission-Critical Cyber Physical Systems," Proceedings on the IEEE, Vol 100, No. 1, pp.283-299, 2012.
[14] www.aadl.info
[15] S.K.S Gupta, T. Mukherjee, G. Varsamopoulos, A. Banerjee, "Research directions in energy-sustainable cyber-physical systems," Sustainable Computing: Informatics and Systems, Vol. 1, No. 1, pp.57-74 , 2011.
[16] M. McDonald, J. Mulder, B. Richardson, R. Cassidy, A. Chavez, N. Pattengale, et. al., "Modeling and Simulation for Cyber-physical System Security Research, Development and Applications," Sandia National Laboratories, Tech. Rep. Sandia Report SAND2010-0568, 2010.

저 자 소 개

박 수 열 (Soo-Youl Park)

2004년 밀양대학교 정보통신공학과 학사.
2004~ 2007년 퓨전소프트㈜ 주임연구원.
2008~2011년 하이버스테크㈜ 선임연구원.
현재, 부산대학교 IT응용공학과 석사과정.
관심분야: 임베디드 시스템, RTOS, 분산제어시스템.
Email: fireman@pusan.ac.kr

최 욱 진 (Wook-Jin Choi)



2012년 국민대학교 전자공학과 학사.
현재, 부산대학교 IT응용공학과 석사과정,
현재, 한국전자통신연구원 모바일보안연구팀 위촉연구원.
관심분야: 임베디드 시스템, RTOS, 모바일 보안.
Email: wtonic@pusan.ac.kr

정 보 흥 (Bo-Heung Chung)

1996년 인하대학교 컴퓨터공학과 학사.
1998년 인하대학교 컴퓨터공학과 석사.
2002년 인하대학교 컴퓨터공학과 박사.
현재, 한국전자통신연구원 모바일보안연구팀 책임연구원.
관심분야: 모바일 보안, 시스템·네트워크보안, 데이터베이스 보안.
Email: bhjung@etri.re.kr

김 정 녀 (Jeong-Nyeo Kim)

1987년 전남대학교 전산통계학과 학사.
1996년 OSF/RI 공동연구 파견(미국)
2000년 충남대학교 컴퓨터공학과 석사.
2004년 충남대학교 컴퓨터공학과 박사.
2005년 Univ. of California, Irvine Post-Doc.
현재, 한국전자통신연구원 모바일보안연구팀장 책임연구원.
관심분야: 모바일 보안, 시스템·네트워크보안, 보안OS 등.
Email: jnkim@etri.re.kr

김 주 만 (Joo-Man Kim)

1984년 숭실대학교 전산학과 공학사.
1998년 충남대학교 컴퓨터공학과 석사.
2003년 충남대학교 컴퓨터공학과 박사.
1985 ~2000년 ETRI 책임연구원(운영체제 연구팀장).
1995 ~1996년 Novell Inc. 방문연구원.
현재, 부산대학교 IT응용공학과 교수.
관심분야: 임베디드 시스템, RTOS, 분산병렬처리, 고장허용시스템.
Email: joomkim@pusan.ac.kr