Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.4, Aug. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.4.867

원자력발전소 사이버보안 훈련을 위한 HIL(Hardware In the Loop) System 개발*

송 재 구,[1†‡] 이 정 운,[1] 이 철 권,[1] 이 찬 영,[2] 신 진 수,[1] 황 인 구,[1] 최 종 균[1]
[1]한국원자력연구원, [2]한국과학기술원

Development of Hardware In the Loop System for Cyber Security Training in Nuclear Power Plants*

Jae-gu Song,[1†‡] Jung-woon Lee,[1] Cheol-kwon Lee,[1] Chan-young Lee,[2]
Jin-soo Shin,[1] In-koo Hwang,[1] Jong-gyun Choi[1]
[1]Korea Atomic Energy Research Institute,
[2]Korea Advanced Institute of Science and Technology

요 약

원자력을 포함한 산업제어시스템에 대한 사이버보안 사건이 증가함에 따라 기술적 보안 조치와 더불어 사이버보안 교육 훈련 및 사이버 비상사건 대응 훈련이 요구되고 있다. 대상 설비를 운영 관리하는 담당자들에게 효과적인 사이버보안 인식 및 교육 훈련을 위해서는 센서 수준에서부터 발전소 운영 상태까지 사이버공격으로 인한 영향 분석이 가능한 훈련용 시스템이 요구된다. 이에 본 논문에서는 원자력 운영 상태를 모사하는 발전소 시뮬레이션과 특정 계통의 시뮬레이션 및 물리장치를 포함하는 원자력발전소 사이버보안 훈련용 HIL 시스템을 개발하였다. 이를 통해 계통담당자 및 사이버보안조직을 대상으로 하는 기술적 훈련, 사이버보안 조직 및 비상사건대응 조직을 대상으로 하는 특화된 사이버보안 훈련을 지원하고자 한다.

ABSTRACT

Security awareness and training are becoming more important as cyber security incidents tend to increase in industrial control systems, including nuclear power plants. For effective cyber security awareness and training for the personnel who manage and operate the target facility, a TEST-BED is required that can analyze the impact of cyber attacks from the sensor level to the operation status of the nuclear power plant. In this paper, we have developed an HIL system for nuclear power plant cyber security training. It includes nuclear power plant status simulations and specific system status simulation together with physical devices. This research result will be used for the specialized cyber security training program for Korean nuclear facilities.

Keywords: HIL, Nuclear I&C, Cyber Security Training

I. 서 론

원자력을 포함한 산업제어시스템에 대한 사이버 위협이 급격히 증가함에 따라 주요기반시설에 대한 사이버보안을 중대한 위협으로 인지하고 대응하기 위한 노력이 요구되고 있다. 이에 IAEA, KINAC,

Received(07. 03. 2019), Modified(1st: 07. 16. 2019, 2nd: 07. 22. 2019), Accepted(07. 22. 2019)
* 이 논문은 2019년도 정부(과학기술정보통신부)의 출연금으로 지원을 받아 수행된 주요연구사업임.
† 주저자, jgsong@kaeri.re.kr
‡ 교신저자, jgsong@kaeri.re.kr(Corresponding author)

NRC 등 원자력 전문기관과 표준 가이드를 제공하는 NIST는 사이버보안 기술 규제, 가이드 등을 개발하여 운영기관에 대응 방안을 제시하고 있다[1, 2, 3, 4, 5].

이러한 규제 및 가이드는 기술적 보안조치와 더불어 보안 인식교육 및 대응 훈련을 포함하는 관리적, 운영적 보안조치의 중요성을 언급하고 있다.

그러나 주요기반시설에 대한 사이버보안 대응이 필요하다는 인식과 적절한 보안조치를 적용하기 위한 노력이 시작되고 있는 단계에서 교육 및 훈련을 위한 관리/운영적 환경까지 동시에 준비하는데 어려움이 있는 것이 사실이다.

특히 KINAC RS-015에서는 사이버보안 훈련의 종류 및 대상으로, 계약업체 직원을 포함한 전 직원을 대상으로 하는 인식제고 교육, 계통담당자 및 사이버보안조직을 대상으로 하는 기술적 훈련, 사이버보안 조직 및 비상사건대응 조직을 대상으로 하는 특화된 사이버보안 훈련, 비상사건대응조직 및 계통 담당자를 대상으로 하는 비상사건대응 및 복구를 위한 교육 및 훈련을 시행하도록 요구하고 있다.

이 중 특화된 사이버보안 훈련은 데이터보안, 운영체제 보안, 응용시스템 보안, 네트워크 보안, 보안조치, 침입 분석, 비상사건 관리 및 대응, 디지털 포렌직, 침투테스트, 시스템 기능 등에 대한 최신의 기술 및 지식과 취약점 제거, 필수디지털자산에 대한 사이버보안 강화 및 사이버공격에 따른 영향을 최소화하기 위한 기술 및 도구의 사용에 관한 사항을 훈련 프로그램으로 포함하도록 명시하고 있다. 이와 같은 교육은 운영 중인 원자력발전소 계통을 대상으로 훈련하는데 많은 제약이 있다. 이를 이행하기 위해서는 원자력 시설의 필수디지털자산의 종류와 계통에 대한 강의와 더불어 Hands-on 훈련 지원이 가능하도록 구체적인 대상을 모사한 환경 구축이 요구된다. 하지만 이러한 환경은 개발하는 데는 대상 계통에 대한 정보 수집의 어려움과 동시에 상당한 시간과 예산이 요구된다.

이러한 이유로 사이버보안 훈련은 기존 IT 기반 환경에서 개발된 프로그램을 그대로 활용하려는 경향이 있다. 그러나, 원자력을 포함한 주요기반시설은 기존의 사이버보안 교육 대상인 PC 기반 인터넷 환경 및 모바일 환경과는 다른 기기의 사용, 운영환경의 차이, 알려지지 않은 취약성 정보, 전용 통신 프로토콜의 사용 등으로 전통적인 컴퓨터 기반 사이버보안 교육 방법을 그대로 활용한다면 교육효과가 매우 미진하게 된다. 이는 주요기반시설의 필수 요소들인 HMI, 제어기, 센서와 같은 하드웨어 특성과 설정값(Set-point), 제어 알고리즘, I/O 신호등 대상 계통의 운영환경을 모사하기 위한 정보의 제약 그리고 사이버 훈련에 용이하지 않은 환경 등에 기인 한다. 특히, 에너지, 교통, 통신 등의 주요기반시설 분야에 대한 각각의 운영환경 정보를 반영하지 않고서는 사이버 공격으로 인한 안전성/건전성 등 영향을 파악할 수 없으며, 동시에 훈련 대상으로써 활용의 가치가 낮아진다.

이에 본 논문에서는 원자력 분야에 대한 사이버보안 훈련에 활용하기 위해 복수 계통 중심으로 하드웨어 장치를 개발하고 발전소 운영을 모사하는 시뮬레이션과의 연계를 통해 센서 수준에서 부터 발전소 운영 상태까지 사이버 공격으로 인한 영향의 분석이 가능한 HIL(Hardware In the Loop) 시스템을 개발하였다.

II. 관련연구

본 장에서는 제어시스템 사이버보안 교육 및 시험을 위한 연구들을 통해 구축된 TEST-BED를 살펴본다. C. Foreman는 산업 제어시스템의 기본적인 동작원리, 네트워크에 대한 교육을 목적으로 PLC, 산업제어시스템에 적용 가능한 상용 방화벽과 상태 모사를 위한 PC 시뮬레이션을 반영한 TEST-BED를 구축한 사례를 보여준다[6]. 이러한 형태는 산업제어시스템의 전형적인 구성형태를 반영한 것으로, IT 전공자들에게 산업제어시스템의 기본 개념 교육을 위한 TEST-BED로 적합하다. G. A. Francia는 물리장치와 가상 장치를 결합한 Hybrid TEST-BED를 제안하고 있다. 제안한 TEST-BED는 외부 인터넷을 이용하여 가상 장치로 구성된 망과 물리장치로 구성된 망을 DMZ로 구분함으로써 네트워크를 이용한 다양한 사이버공격 시나리오를 제시함으로써 외부 인터넷에서 내부 제어망까지 공격 가능한 사이버공격 훈련에 활용하기 적합한 환경을 제시한다[7]. M. Domínguez 등은 제어시스템과 사이버보안 전문가 간의 지식 격차 해소를 위해 실제 물리장치로 구성된 TEST-BED를 구축하였다. 산업제어, 빌딩관리, 에너지 관리, 스마트시티 센서 네트워크 등 4가지 subsystem 시험 장비 개발을 통해 사이버 훈련을 위한 환경 구축 사례를 보여준다[8]. I. Ahmed 등은 기반시설에 대한

포렌직 연구를 위해 가스 파이프라인, 전력망, 정수처리에 대한 소형 물리모델을 개발하였다[9]. T. Alves 등은 가상화 모델을 이용한 사이버 시험으로 인한 상태 분석이 가능한 물리장치 개발의 한계를 극복하고자, 가상 TEST-BED를 구축하여 시험한 사례를 보여준다[10]. 이러한 기존 연구들의 공통점은 산업제어시스템에 대한 이해를 높이기 위해 제어시스템에서 사용하는 전용 하드웨어, 소프트웨어, 네트워크, 운영환경을 모사하기 위해 PLC 사용을 TEST-BED 구축의 핵심에 두거나, 시리얼 통신 등, 제어시설에서 사용하는 통신 프로토콜 사용을 통해 제어시스템에 유사한 환경을 개발하고자 하였다. 혹은 특정기능을 모사하는 모듈과 소형 물리장치를 연결하여 훈련용 Kit를 제공하고 있다. 이러한 접근은 사이버보안 관점에서 제어시스템 시험환경을 만들기 위한 노력으로 에너지, 통신, 교통, 금융, 의료 등 각 기반시설의 특성을 반영하기보다 기반시설의 일반화된 구성환경 중의 일부만을 반영하여 구축된다는 한계가 있다. 기존 TEST-BED는 IT 전문가들에게 제어시스템에 대한 사이버보안 교육에 활용하기 적합한 반면, 전체 시스템의 영향성을 분석할 수 없기 때문에 실제 기반시설 제어시스템을 운영/관리하는 담당자들에게 사이버보안 훈련 장비로 활용하기에는 부족한 측면이 있다. 이에 제어시스템을 운영/관리하는 담당자들의 이해를 바탕으로 사이버보안 훈련이 가능한 환경이 요구되며, 이는 기반시설 도메인에 따라 운영환경의 특성을 반영하여 개발되어야 한다.

III. 원자력발전소 사이버보안 훈련을 위한 HIL 시스템 설계 및 개발

3.1 원자력발전소 사이버보안 훈련 HIL 시스템의 기능 요건

HIL 시스템은 사이버보안 훈련을 목적으로 사이버공격단계, 영향 파급 단계에 따라 사이버보안 탐지 정보와 더불어 진단정보 분석 결과를 융합한 판단 및 대응 전략을 고민할 수 있는 환경을 지원할 수 있어야 한다. 이를 위한 주요 기능 요건은 다음과 같다.

- 발전소 복수계통의 고유 기능 모사(복수계통 시뮬레이션)
- 발전소 운영 시뮬레이션의 제어 및 모니터링 신호 연계
- 사이버보안 시험에 따른 시스템 프로세스 처리 상태 로그 저장 (사이버공격으로 인한 시스템 전반의 영향 파급 분석)
- 사이버보안 시험 시 제어기기 및 물리장치 영향성 식별
- 운영 중인 네트워크 데이터 정보의 취득 기능
- 시뮬레이션, 제어기기, 물리장치간의 상호 독립적 작동 및 제어를 통한 확장성 제공
- 사이버보안 대응 기술 적용을 위한 환경 제공

3.2 시스템 구성

본 연구에서 개발하는 HIL 시스템은 사이버보안 훈련 시 기기, 계통, 발전소로의 영향성 분석이 가능하도록 구성하였다. 이를 위해 그림 1과 같이 (A)가상 경수로 발전소 시뮬레이션 모듈, (B)복수계통 시뮬레이션 모듈, (C)복수계통 물리장치 그리고 각 모듈의 제어 태그 정보 송/수신 및 데이터 처리를 위한 (D)OPC UA 서버 모듈로 이루어진다.

물리장치는 전 계통을 모사할 수 없는 한계로 인해 구축 대상을 복수계통으로 한정하여 개발하였다.

다만, 계통의 확장과 사이버보안 대응 기술 반영을 쉽게 하기 위해 OPC-UA 표준 통신 프로토콜[11]을 사용하였으며, 발전소 전반에 대한 시뮬레이션 모사를 위한 상태 정보 일체를 태그정보로 정의하고 OPC-UA 서버를 통해 동기화하였다. 이러한 구조를 통해 향후 다른 계통이 추가될 경우 제어 신호에 대한 태그 정보를 활용하여 발전소 시뮬레이션 모듈과 물리장치 간의 영향을 주고받을 수 있는 확장성을 제공하도록 하였다.

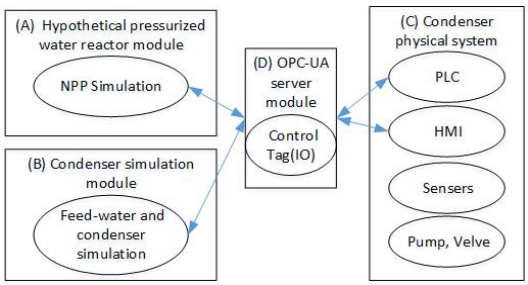

Fig. 1. Component of NPP Hardware In the Loop(HIL) System for Cyber Security Training

3.3 원자력발전소 사이버보안 훈련 HIL 시스템 설계 및 개발

HIL 시스템은 그림 2와 같이 물리적 부분과 사이버 부분으로 구분된다. (A)물리적 부분은 (a1)PLC를 중심으로 (a2)펌프, 밸브 제어와 센서 정보, (a3)진단정보 처리 및 제어기능을 수행한다. (B)사이버 부분에서는 (b1)복수계통 시뮬레이션을 중심으로 (b2)제어 로직, (b3)모니터링 및 로그, (b4)스캐쥴링 정보 처리 기능을 수행한다. (C)HMI 역시 사이버 부분으로 사용자 인터페이스에 따라 (c1)펌프 밸브등 신호 제어, (c2)주요 설정값 변경 기능을 지원 한다. 또한 모든 정보는 통신을 통해 태그값으로 (D)가상 경수로 발전소 시뮬레이션과 동기화 되어 주요 제어 변수가 전달된다. 이를 통해 발전소 운영 상태 변화에 직접적인 영향을 주고 그 결과를 확인할 수 있다.

사이버보안 훈련을 위해서 주요 제어 로직, PLC 및 엔지니어링 장치를 통한 사이버 침해가 가능하도록 네트워크를 구성한다. 또한 사이버공격 발생으로 인한 상태 변경 등을 추적하기 위해 (c3)상태 정보 모니터링 및 로그 정보 수집 모듈을 포함한다.

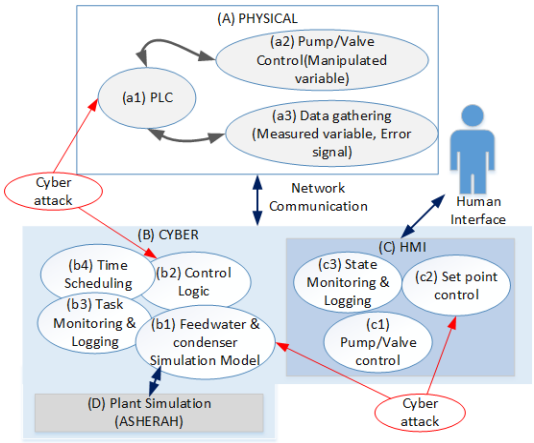

Fig. 2. Functions Design of NPP Hardware In the Loop(HIL) System for Cyber Security Training

3.3.1 발전소 시뮬레이션 모듈 개발

사이버 부분에서 발전소 운영 상태를 모사하기 위한 모듈로서 한국원자력연구원과 IAEA가 공동 개발 중인 가상 경수로 원자력발전소 모델 ASHERAH를 사용한다. 본 모델은 논문에서 제안하는 HIL 시스템에서 사이버보안 시험에 최적화된 가상의 발전소 모델로 발전소보호계통, 제어계통, 터빈, 복수계통과의 제어신호를 송수신하여 발전소 운영 전반에 대한 모사가 가능하도록 개발되었다. ASHERAH는 사이버보안 시험 및 교육을 목적으로 개발되는 최초의 프로젝트로, 국내 한국원자력연구원을 포함하여 13개국 17개 기관에서 참여하여 공동 개발 중이다[12].

3.3.2 발전소 시뮬레이션 모듈 개발

계통수준의 훈련을 위해서는 관련 계통에 대한 운영상황을 상세히 제공할 필요가 있다. 이에 원자력발전소를 구성하는 수많은 계통 중에서 복수계통모듈을 사이버 시뮬레이션으로 개발하였다. 복수계통은 발전소의 터빈으로부터 배출되는 증기를 응축하며, 응축된 복수는 복수기의 온수조에 수집된 후 복수계통에서 가열되어 급수계통으로 이송하는 역할을 한다[13]. 이러한 복수계통은 원자력 발전소의 원자로형에 의존적이지 않고 대부분 유사한 형태로 구성이 가능하다는 특징이 있다. 이에 발전소의 복수계통에 대한 기본 개념을 설계에 반영하여 시뮬레이션 코드를 개발하였으며, 물리 시스템과 연계를 위해서 수위 정보와 직접 관련된 압력, 유속 등을 중심으로 입출력 값을 제어하기 위해 Matlab Simulink로 시뮬레이션 코드를 개발하였다[14]. 이를 통해 터빈 출력 값, 터빈 정지 신호, CoolingWaterPump, Airpump, Condenstate Pump 등을 입력 받아 계산된 수위 정보를 물리시스템에 출력 신호로 전달한다. 동시에 물리 시스템으로부터 수위 및 펌프 제어 정보를 수신하여 물리 시스템의 상태정보를 발전소 시뮬레이션에 전달 할 수 있도록 한다. 물리적 장치에서는 탱크 수위변화에 따라 밸브, 펌프가 자동조작되며 그 결과를 전달하여 가상 경수로발전소 시뮬레이션에 복수계통의 상태 값을 실시간으로 반영한다. 결과적으로 실제 발전소에서 복수저장탱크로부터 복수를 유입시키거나 복수저장탱크로 복수를 방출하여 설정된 수위가 유지되도록 자동적으로 제어하고 감시하는 기능을 모사하게 된다.

3.3.3 복수계통 물리장치 모듈 개발

PLC를 통해 복수계통 수위를 제어하기 위해 펌프, 밸브, 센서를 적용한 주요 물리장치 부분은 시뮬

레이션 정보와 HMI로 부터 제어되는 복수계통이 물리적으로 복수 유입 및 방출을 통해 어떻게 운영되는지 직관적으로 식별 가능하도록 개발하였다.

본 장치는 복수계통 시뮬레이션과 발전소 시뮬레이션 모듈과의 제어신호를 동기화함으로써 가상 모듈의 변화에 따라 복수계통 수조 상태가 반영되며, 그 반대인 물리장치의 복수계통 수조 상태 변화가 발생하는 경우 시뮬레이션에 상태 정보가 반영된다.

그림 3은 개발된 복수계통 물리 장치로 사용자가 수위, 밸브, 펌브, 제어기 오류상태, HMI 변화를 쉽게 인지하도록 구성하였으며, 사이버 시험으로 인한 오작동을 대비하여 비상 전원 차단기를 적용하여 훈련 시 사고를 방지하고자 하였다.

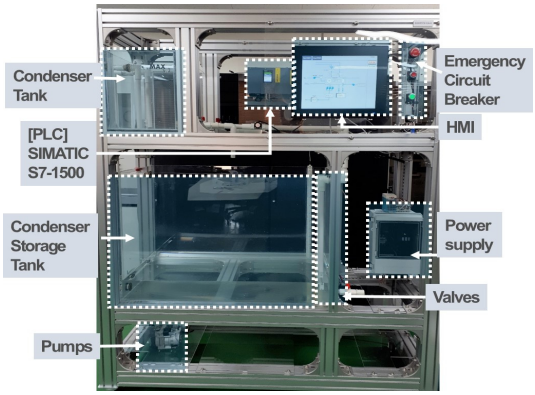

Fig. 3. KAERI Feed-water and condenser physical system

IV. 훈련 활용방안

본 연구에서 구현한 HIL과 사이버보안 교육 및 시험을 위한 구축된 기존 TEST-BED의 훈련 활용 범위를 비교하기 위해서 (A)제어 네트워크 분석 지원, (B)제어처리 분석 지원, (C)단위 계통 수준 분석 지원, (D)TEST-BED 대상 도메인 전체 시스템의 영향 분석 지원 가능 여부를 식별한 결과 표 1과 같은 차이가 있음을 확인하였다.

- (A)제어 네트워크 분석 : 대상 시스템에서 사용하는 제어 네트워크 통신 정보를 모사하고 분석하는 수준으로 관련 통신 다이어그램 및 프로토콜 지원
- (B)제어처리 분석 : 제어공정 절차에 대한 분석으로 PLC를 기준으로 데이터 송/수신 상황 및 PLC 처리 현황을 분석하는 수준으로 제어정보 송/수신 및 물리장치 제어를 위한 로직 사용. 제어기로 부터 상태 정보를 실시간으로 수집할 수 있는 환경지원
- (C)단위 계통 수준 분석 : 하나의 단위 시스템 수준에서 제어정보에 따라 일련의 과정을 모사하고 분석하는 수준으로 정상상태에서 계통 운영 정보 필요. 시뮬레이션 또는 물리장치로 단위 계통을 모사하여 사이버 공격 시나리오에 따른 상태변화 확인 지원
- (D)전체 시스템 분석 : 계통 처리 정보에 근거하여 서로 다른 단위 시스템간의 영향 및 구성된 전체 시스템으로의 영향을 분석하는 수준으로 계통간의 상시 영향을 모사하기 위한 정상상태 운영 정보

Table 1. Functional Scope of our HIL System and other ICS TEST-BEDs

TEST- BED	Target Domain/ Purpose of Use	(A)Control Network Analysis Support	(B)Controller level Status Analysis	(C)System Impact Analysis	(D)Plant Level Impact Analysis
C. Foreman.[6]	ICS/Education	O	O	X	X
G. A. Francia[7]	ICS/Training	O	O	△	X
M. Domínguez[8]	ICS/Training	O	O	△	X
I. Ahmed[9]	ICS/Testing	O	O	O	X
T. Alves. [10]	ICS/Testing	O	O	△	X
Proposed HIL System	NPP/ Training	O	O	O	O

O : 기능 적용, △ : 확장 가능, X: 기능 없음

지원

제안하는 시스템은 발전소 전체 상호 영향을 모사할 수 있다는 특징으로 인해 아래와 같이 원자력발전소 사이버보안 관계자를 대상으로 사이버보안 시나리오 개발, 영향성 시험, 보안 통제 항목 식별 및 적용성 평가에 대한 훈련에 활용 가능하다.

- 시나리오 개발 : 시뮬레이션의 제어로직 변조, HMI의 Set-point 값 변조, 밸브 및 펌프 제어 변조, 특정 센서 값 변조 등의 사이버 공격과 PLC에 직접적인 공격을 통해 제어 상실 등을 유발하고 이로 인해 발전소 전체에 가용한 영향성을 반영한 사이버보안 시나리오 개발 활용
- 영향성 시험 : 시나리오에 근거한 침투시험을 통해 물리적 장치와 사이버 시뮬레이션의 상태 변화 그리고 발전소 모델의 변화 분석 활용
- 사이버사건 식별을 위한 보안 통제항목 정의 : 시나리오 및 영향성에 근거하여 요구되는 보안 기능 및 정보 식별 활용
- 보안 기능 활용 훈련 : 가용한 보안 기능을 HIL 시스템에 적용하여 사이버 공격 발생시 대응 절차 및 기능 활용 방안 훈련 활용

그림 4는 HIL 시스템을 이용한 사이버보안 훈련의 활용 사례의 하나로 HMI Logic Tampering 공격 시나리오를 보여준다. 본 시나리오는 운전원 입장에서 사이버공격으로 계통의 비정상 상황이 어떻게 만들어지고 대응해야 하는지를 설명하기 위해 작성되었다. 훈련의 몰입감을 주기 위해 실제 사이버공격시 어떠한 기술과 과정이 필요한지를 설명하고, 단계별 공격자의 흔적을 추적하기 위해 수집되어야 하는 정보와 분석시 필요한 보안 기술을 훈련에 포함한다.

원자력발전소는 외부 네트워크를 통해 제어시스템 접근이 원천적으로 차단되어 있기 때문에 시나리오는 내부자 위협으로부터 시작되며, 사이버공격으로 운전원이 운영 시스템의 이상을 적시에 인지하지 못하도록 정교한 공격을 시도하여 디지털 자산의 단순 고장/정지뿐만 아니라 정교한 제어가 가능함으로 보여주고자 하였다.

이를 위해 시나리오에서는 최초 공격자가 대상 시스템 정보 취득을 위해 디지털 자산의 루트 쉘을 취득함으로써 내부 운영 정보를 수집/분석 가능한 조건을 제공한다. (a) 공격자는 HIL 시스템의 HMI 로직 프로그램 변조를 시도하기 위해서 스위치에 연결된 디지털 자산으로부터 대상 HMI 의 취약성 식별 및 루트 쉘을 취득한다. (b) 공격자는 알람 설정값등 특정 제어정보만 조작 가능하도록 프로그램 변경을 목적으로 한다. 이를 위해 구동중인 HMI의 정상상태 분석과 더불어 이를 변조하기 위해 필요한 취약성 정보를 식별한다. (c) HMI 로직 변조를 위한 악성 코드를 제작한다. (d) 해당 코드를 HMI에 업로드 하고, (e) 원격 쉘, 또는 bad USB 등을 이용하여 악성코드 실행을 유도한다. (f) 정상적인

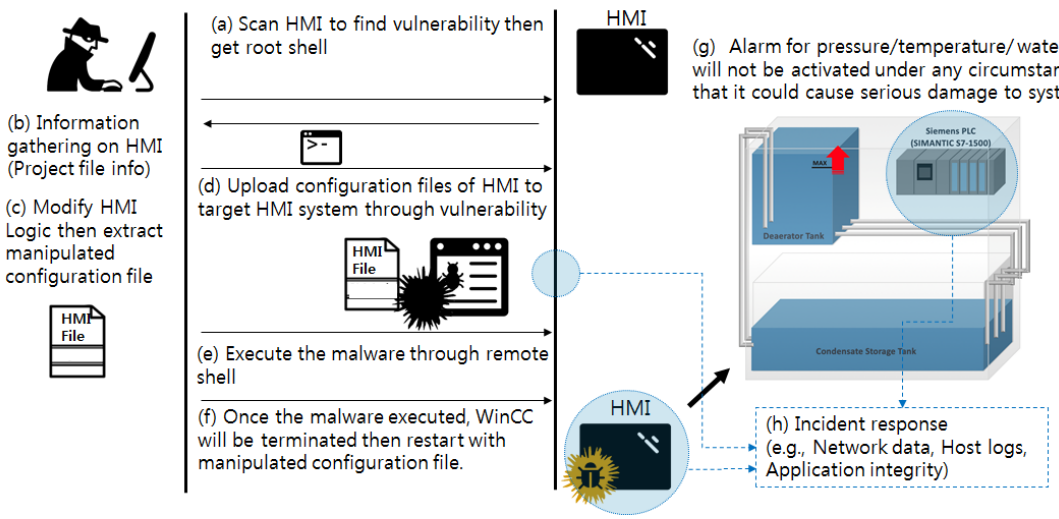

Fig. 4. Cyber Security Training Scenario using HIL

HMI 로직 프로그램을 강제 종료 시킨 이후 변조된 HMI 로직이 실행된다. (g) 변조된 HMI 로직은 사용자에게 압력/온도/수위 정보에 대한 정상 알람 정보를 제공하지 못하도록 알람 설정값을 조작함으로써 운전원이 물리적 장치의 상태 변화를 오판하도록 유도하고 적시에 계통에 문제가 있음을 판단하지 못하게 함으로써 운영에 치명적인 문제를 야기하게 된다.

해당 시나리오에 따라 변조된 HMI 코드를 제작함으로써 실제 시스템에 미치는 영향을 파악하였으며, 이때 교육 참여자들은 사이버공격으로 인해 물리적 시스템 변화와 HMI 정보 차이로 인해 운전원이 처하게 되는 상황 훈련하게 된다. 또한 발전소 시뮬레이션의 변화를 추적하여 복수계통의 영향으로 인해 발전소 타계통의 영향을 확인하게 된다. (h) 교육 참가자는 시나리오에 따라 사이버공격 대응 훈련으로 디지털 자산의 식별을 통해 PLC, HMI, 스위치 등 필수 디지털 자산이 사이버공격 대상이 될 수 있음을 확인하게 된다. 또한 필수디지털자산의 매체통제 현황을 확인함으로써 물리적 통제의 중요성을 인지하게 된다. 교육 참가자들은 계통의 네트워크 패킷, 필수 디지털 자산의 진단 및 보안 로그, 응용프로그램 및 데이터의 무결성 확인 방법을 훈련함으로써 사이버보안 사건대응 훈련을 수행한다.

V. 결 론

원자력발전소 디지털 시스템을 대상으로 별도의 사이버 훈련 환경을 구축하는 것은 예산과 더불어 관련 정보 취득 및 자료 공개의 한계로 구현에 어려움이 따른다. 이를 해결하기 위해서 발전소 운영을 모사하는 시뮬레이션을 개발하고 특정 계통의 제어상황을 단순화하여 모사한 물리적 장치를 개발함으로써 사이버공격으로 인한 시스템의 영향성을 분석할 수 있을 것이다. 이에 본 논문에서는 발전소 타입에 종속되지 않는 계통 중 복수계통을 선정하여 사이버 물리 장치 기반 HIL 시스템을 개발하였다. 특히, 계통의 운영, 하드웨어 및 소프트웨어 정비(관리), 사이버 사건으로 인한 단위 계통 및 전체 시스템 영향성 분석과 사이버사건 대응 훈련에 활용하도록 HIL 시스템 활용 방안을 제시하였다. 본 HIL 시스템은 국내외 원자력 및 주요기반 시설 사이버보안 관계자들에게 사이버공격 시나리오, 취약성 분석 대응 훈련을 지원할 예정이다. 이를 위해 국제원자력기구 IAEA, 국내 원자력 및 보안 전문기관과의 협력을 통해 지속 확장 개발 할 예정이다.

References

[1] Regulatory Guide 5.71, “Cyber security programs for nuclear facilities,” U.S. Nuclear Regulatory Commission, Jan. 2010.

[2] Regulatory Standard 015, “Regulatory standard on computer security of nuclear facilities,” KINAC, Dec. 2016.

[3] NIST SP800-53A Revision 1, “ Guide for assessing the security controls in federal information systems,” NIST, Jun. 2010.

[4] International Atomic Energy Agency Nuclear Security Series No.17, “Computer security at nuclear Facilities,” IAEA, Dec. 2011.

[5] International Atomic Energy Agency Nuclear Security Series No.23-G, “Security of nuclear information implementing guide,” IAEA, Feb. 2015.

[6] C. Foreman and W. Lafayette, “Educational modules in industrial control systems for critical infrastructure cyber security,” 122nd American Society for Engineering Education Annual Conference & Exposition, Jun. 2015.

[7] G. A. Francia, “Scenario-based learning approach to industrial control systems security training,” The 2018 International Conference on Security and Management, USA, pp. 111-116, Aug. 2018.

[8] M. Domínguez, M. A. Prada, P. Reguera, J. J. Fuertes, S. Alonso, and A. Morán, “Cybersecurity training in control systems using real equipment,” IFAC-Papers OnLine, vol. 50, no. 1, pp. 12179-12184, Jul. 2017.

[9] I. Ahmed, V. Roussev, W. Johnson,

and S. Senthivel, "A SCADA system testbed for cybersecurity and forensic research and pedagogy," pp. 1-8, Dec. 2016.
〔10〕 T. Alves, R. Das, A. Werth, and T. Morris, "Virtualization of SCADA testbeds for cybersecurity research : a modular approach," Computer & Security, vol. 77, pp. 531-546, Aug. 2018.
〔11〕 OPC Foundation, "Unified architecture," https://opcfoundation.org/about/opc-technologies/opc-ua/ (accessed May 21, 2019).
〔12〕 International Atomic Energy Agency, "Enhancing computer security incident analysis at nuclear facilities," https://www.iaea.org/projects/crp/j02008 (accessed May 21, 2019)
〔13〕 Jae Geun Kim, Nuclear power plant system, 1st Ed., Yeungnam University Press, Jul. 2013.
〔14〕 MathWorks, "Simulink," https://kr.mathworks.com/products/simulink.html(accessed May 21, 2019).

〈저자소개〉

송 재 구 (Jae-gu Song) 정회원
2006년 2월: 한남대학교 멀티미디어학과 졸업
2008년 2월: 한남대학교 멀티미디어학과 석사
2011년 8월: 한남대학교 멀티미디어학과 박사
2013년 3월~현재: 한국원자력연구원 선임연구원
〈관심분야〉 사이버보안, 원자력 계측제어

이 정 운 (Jung-Woon Lee) 정회원
1979년 2월: 한양대학교 기계공학과 졸업
1981년 2월: 한국과학기술원 기계공학과 석사
1990년 5월: University of Iowa Biomedical Engineering 박사
1990년 11월~현재: 한국원자력연구원 책임연구원
〈관심분야〉 산업제어시스템 사이버보안

이 철 권 (Cheol kwon Lee) 정회원
1980년 2월: 경북대학교 전자공학과 졸업
1985년 2월: 동아대학교 전자공학과 석사
2006년 8월: 충남대학교 전자공학과 박사
1985년 3월~현재: 한국원자력연구원 책임연구원
〈관심분야〉 원자력 계측제어, 원자력 사이버보안

이 찬 영 (Chanyoung Lee) 학생회원
2015년 2월: 한국과학기술원 기계공학과 졸업
2017년 2월: 한국과학기술원 원자력 및 양자공학과 석사 졸업
2017년 3월~현재: 한국과학기술원 원자력 및 양자공학과 박사과정
〈관심분야〉 원자력공학, 제어공학, 전자공학, 통신공학

신 진 수 (Jinsoo Shin) 정회원
2012년 2월: 경희대학교 원자력공학과 졸업
2013년 8월: 경희대학교 원자력공학과 석사
2017년 8월: 경희대학교 원자력공학과 박사
2018년 9월~현재: 한국원자력연구원 박사후연구생
〈관심분야〉 정보보호, 사이버보안, 원자력공학

황 인 구 (Inkoo Hwang) 정회원
1986년 2월: 인하대학교 전기공학과 졸업
1990년 2월: 인하대학교 전기공학과 석사
2015년 2월: 충남대학교 전기공학과 박사
1986년 2월~현재: 한국원자력연구원 책임연구원
〈관심분야〉 원자력 계측제어 기술, 계측신호 처리, 공정 계측

최 종 균 (Jong-gyun Choi) 정회원
1994년 2월: 한양대학교 원자력공학과 졸업
1996년 2월: 한국과학기술원 원자력공학과 석사
2001년 8월: 한국과학기술원 원자력공학과 박사
2001년 9월~현재: 한국원자력연구원 책임연구원
〈관심분야〉 원자력공학, 안전성평가, 원자력사이버보안