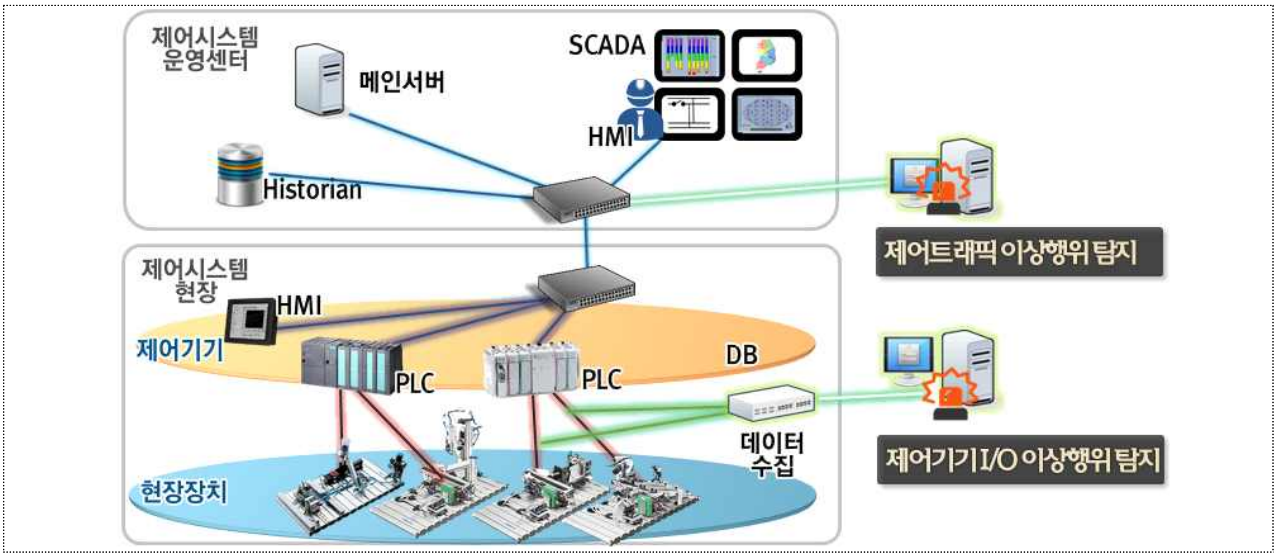
제어시스템 이상행위 탐지를 위한 제어트래픽 및 제어기기 I/O 데이터 감시기술

기술키워드	제어시스템, 네트워크 보안, 제어기기 보안, 기계학습								
지식재산권	출원 1건(대한민국) / 출원 예정 1건(대한민국)								
기술완성도 (TRL)	기초 실험	개념 정립	기능 및 개념검증	**연구실환경 테스트**	시제품 제작	시제품 성능평가	시제품 신뢰성평가	시제품 인증	상용품

기술개요

- 세부기술[1] - 제어트래픽 분석 및 이상트래픽 탐지기술
  - (Global탐지) 제어시스템 네트워크의 전 영역에서 시간에 따른 트래픽 전송흐름의 특성을 학습하고, 이를 기반으로 비정상적인 트래픽을 탐지하는 기술
  - (Local탐지) 제어기기 간에 전송되는 트래픽 특성과 payload 정보를 학습하고, 이를 기반으로 비정상적인 패킷 및 데이터의 전송을 탐지하는 기술
- 세부기술[2] - 제어기기 I/O 이상행위 탐지기술
  - 제어시스템 운영 중에 발생하는 제어기기 I/O의 특성을 학습하고 이를 기반으로 비정상적인 I/O를 탐지하는 알고리즘 및 SW
- 기술 구성도



기술성

- 제어시스템 스펙 및 구동원리 등 내부정보 없이 제어시스템 이상행위 탐지 가능
  - 현재 제조사 및 운영사의 보안 등을 이유로 내부정보를 얻기 어려운 경우가 많음
  - 운영 중 발생하는 데이터들로부터 정상 특성을 학습하고 이를 기반으로 이상행위를 탐지
  - 기계학습 연구의 패턴매칭, 딥러닝 기술들을 제어트래픽 및 I/O 데이터 특성학습에 활용

- 제어기기 간 통신 및 I/O 구간별 상관관계를 고려하여 이상행위 탐지 가능
  - 본 기술은 기존 전송패턴 학습을 통해 정상적인 트래픽전송이 이루어지고 있는지 확인할 수 있음
  - 특정 상대간의 통신을 허용/불가하는 ACL을 개선하여 어느 시점에 어느 정도의 양으로, 어떤 내용을 보내는지를 학습하고 이를 기반으로 트래픽을 감시
  - 제어시스템에서 발생하는 I/O 데이터에 대해 관계 설정 또는 한계치 설정 등 스펙에 기반을 둔 관리자의 개입 없이 학습을 통해 공격 의심 패턴 탐지 가능
- 외부에서 공격시그너처 정보 업데이트 없이 운영 가능
  - 다양한 제어기기에 특화된 수많은 공격들에 대한 공격시그너처를 개발하여 배포하기 어려워 공격시그너처 기반 보안장비들이 제어시스템에서 정상적으로 운영되지 않고 있음
  - 본 기술의 경우 외부 정보 업데이트가 필요 없어 운영현황에 맞는 보안장비 제작이 가능

시장성

- 리서치앤마켓 보고서(Research and Markets, 2017. 4. 27. icn매거진)에 따르면, 한국의 산업제어시스템(ICS) 보안시장은 ICS 장치에 대한 해킹 사건이 증가함에 따라 가속화 될 것으로 분석
  - 국내 ICS 보안시장이 2015년 125억원(1,100만 달러)에서 오는 2020년에는 913억원(8,050만 달러)에 달할 것으로 전망(연평균 48.8%의 고성장을 의미)
  - 아시아 지역에서의 산업제어시스템 보안시장 또한 연간 47.2%의 성장세를 통해 2020년에는 1조 8천 500억원(16억 3천만 달러)에 달할 전망
- 국내도 2014년 말 한국수력원자력 해킹사고를 기점으로 ICS 보안시장이 성장할 것으로 예측
  - NIST SP800-82(2015년에 rev2 발간)에서는 산업 제어시스템 보안을 위해 "시스템 간의 접근제어, 정보흐름 제어"를 수행할 것을 권고하고 있어 제어시스템 보안장비 도입수요가 늘 것으로 예측

기술 응용 분야

- 주요정보통신 기반시설 및 민간 영역의 산업제어시스템 등을 위한 보안장비 개발에 적용
  - 제어시스템 보안감시 영역을 네트워크 및 제어기기 I/O까지 확장 가능
- 제어시스템 뿐 아니라 폐쇄망 내 지정된 장비들로 구성된 시스템(ex. 금융, 의료) 영역에도 활용 가능

기술개발 완료시기

- 2017년 12월 완료

관련 특허 등 지식재산권

- (출원) 2017-0139078(2017. 10. 25. 대한민국) "네트워크에 대한 이상행위 탐지 방법 및 이를 이용한 장치"
- (출원) 2017-0143790(2017. 10. 31. 대한민국) "시스템 감시 장치 및 방법"

기타

- 해당 기술은 2개의 하위 기술로 구분할 수 있으며 각각 기술이전이 가능함(기술이전 상담 시 별도 문의)