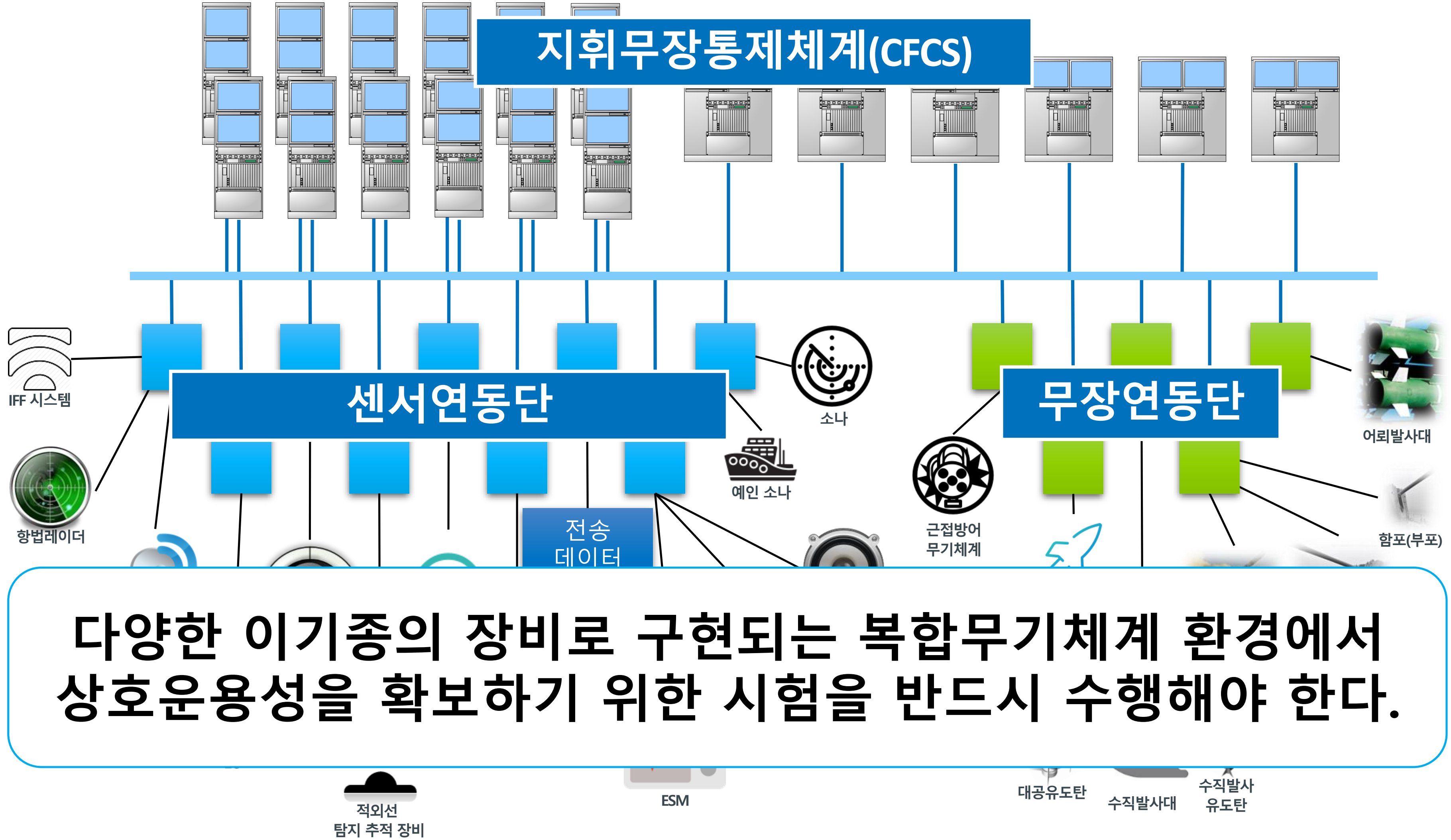
상호운용성 정보보호를 위한
머신러닝을 활용한 임베디드 시스템의 악의적인 동작 탐지 방안

한컴MDS
데이터 분석 · 보안 사업부

정보보호 위협 트렌드

- **전투 체계 구성 사례**



다양한 이기종의 장비로 구현되는 복합무기체계 환경에서 상호운용성을 확보하기 위한 시험을 반드시 수행해야 한다.

함정 전투 체계 구성 예

상호운용성을 확보하기 위한 법·규정

국방정보화 기반조성 및 국방정보자원관리에 관한 법률 [제 12553호, '14.5.9]

- 국방 정보화 정책 수립·추진에 대한 주체 및 절차, 국방 상호운용성 확보 명시

국방전력발전업무훈령 [제2114호, '17. 12. 29]

- 무기체계와 전력지원체계의 소요·획득·운영유지를 포함한 업무의 기본절차를 규정 및 지침 제공

국방 정보화업무 훈령 [제2129호, '18.2.5]

- 국방 상호운용성 기본 원칙, 기관간 업무분장, 주요 절차(제9장 상호운용성 관리)

국방상호운용성 관리지시 [제2016-017, '16.5.1]

- 표준, 연동, 평가의 분야별 업무 절차

상호운용성과 정보보호

- **상호운용성 시험 과정에 정보보호를 위한 평가 항목**

  국방상호운용성 관리지시에 정보보호 명시

  정보 유출 또는 위변조 대응책 마련 필요

제180조(상호운용성 개발시험 및 운용시험) ① 국본(정보화기획관실), 합참, 각 군은 개발시험평가, 운용시험평가 시 상호운용성 요구사항 충족 및 적합성 점검을 실시한다.

② 무기체계 및 전력지원체계별 세부 점검사항은 다음 각 호와 같다.

1. 개발시험평가
   가. 체계의 운용개념 및 체계 특성
   나. 체계 연동성 및 정보교환 능력
   다. 표준 및 아키텍처, 정보보호, 주파수 등을 포함한 상호운용성 기술적 검증
2. 운용시험평가
   가. 체계의 운용개념 및 체계 특성
   나. 체계 연동성 및 정보교환 능력
   다. 표준 및 아키텍처, 정보보호, 주파수 등을 포함한 내용 중 야전운용 필수요소

점검목록				사업 특성 분류				획득순기								구매
대분류	중분류	소분류	항목(○) 및 세부기준(-)	0	I	II	III	소요제기			선행연구	탐색개발	체계개발	개발시험	운용시험	
								장기신규	중기신규	중기전환						
정보보호	정보 보호 구현 방안		○ 정보보호 수준이 제시되었는가?	◎	◎	◎	◎	◎	◎	◎	×	×	×	×	×	×
			○ 네트워크 정보보호 대책이 수립되었는가?	×	◎	◎	◎	×	◎	◎	◎	◎	◎	◎	◎	◎
			○ 관제체계 목록이 식별되었는가?	×	◎	×	◎	×	◎	◎	◎	◎	◎	◎	◎	◎
			○ 키관리체계 구축방안이 식별되었는가?	×	◎	×	◎	×	◎	◎	◎	◎	◎	◎	◎	◎
			○ 응용체계 정보보호 대책이 수립되었는가?	×	◎	◎	◎	×	◎	◎	◎	◎	◎	◎	◎	◎
			○ 서버 정보보호 목록이 식별되었는가?	×	◎	◎	◎	×	◎	◎	◎	◎	◎	◎	◎	◎
			○ 단말기 정보보호 목록이 식별되었는가?	×	◎	◎	◎	×	◎	◎	◎	◎	◎	◎	◎	◎
	암호 장비 적용 방안		○ 암호장비 적용에 대한 적절성 검토 및 소요되는 암호장비가 식별되고, 암호장비 적용방안이 수립되었는가?	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎
	정보보호와 상호운용성 상관관계		○ 수립된 정보보호 구현방안 및 암호장비 적용방안이 연동대상체계와의 상호운용성 구현에 문제를 발생시키지 않는가?	×	◎	◎	◎	×	×	×	◎	◎	◎	◎	◎	◎
	사이버전 대비능력		○ 사이버전에 대한 방안이 계획/구현되었는가?	×	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	◎	×

정보보호를 위한 방호 체계

- **국방정보화 시스템 분류내 정보보호를 위한 방호 체계**

  대분류 : 기반 운용 환경

중분류	소분류	주요 해당 시스템
사이버방호 체계	공통/기반 보호체계	통합보안관제체계, 분석체계, 조사/추적체계, 교육/모의훈련체계, 국방인증체계, 암호장비
	네트워크 보호체계	침입차단/방지체계, 네트워크접근통제체계, 네트워크연동통제체계, 디도스대응체계
	ICT플랫폼 보호체계	서버중앙통제체계, 보안OS, 바이러스방역체계, 전자자료유출방지체계, 저장매체통제체계
	응용체계 보호체계	SW개발보안체계, 웹방화벽, 웹서비스통제체계
	보호관리체계	개인정보 보호관리체계, 취약점분석/보안성평가체계, 출입통제체계

대부분 네트워크와 PC기반의 정보보호를 위한 체계로 임베디드 기기의 정보보호를 위한 체계 보완이 필요하다.

사이버 공격의 진화

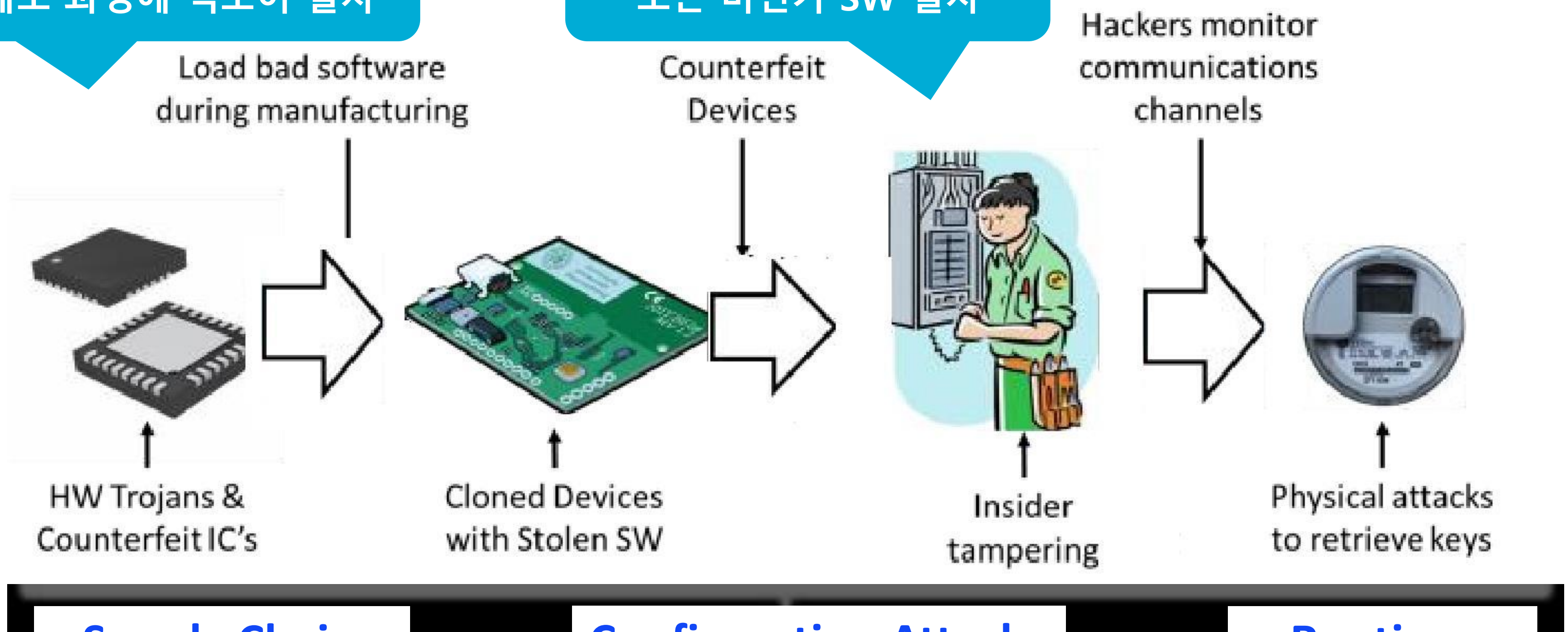
연도	사건	대상
2000	호주 오폐수처리 제어시스템 해킹사건	PC
2003	미국 원자력발전소 슬래머웜 침투	PC
2010	이란 핵 시설에 지멘스 PLC 대상 스턱스넷 공격	Embedded
2011	미국 무인기가 이란에 의해서 해킹된 후 나포	Embedded
2016	우크라이나 키에프 지역에 Industroyer를 이용한 공격으로 1시간 가량 정전 발생	Embedded
2017	Triton malware에 의해 중동 지역 시스템 셧다운	Embedded
2018	슈퍼마이크로사 보드에 중국 제조사에 의한 스파이칩 탑재	Supply Chain

최근 사이버 공격은 PC기반 시스템에서
임베디드 시스템과 공급망으로 공격대상을 확대

정보 보호 장치의 직접적인 공격을 넘어 더욱 다양한 방법으로 진화

위조 부품 또는
제조 과정에 백도어 설치

내부자에 의한 정보 탈취
또는 비인가 SW 설치



Supply Chain Attacks

Configuration Attacks With Insider Access

Runtime Attacks

조립, 납품 과정에
스파이 칩 내장

정보 보호 장치에 대한
직접적인 공격

현재 우리 군의 위변조 제품과 스파이칩 탑제여부 파악 방법

- **전체 도입되는 장비 중 시험대상으로 일부를 선정**

  테스트 되지 않은 장비에 발생하는 사이버 공격은 파악 불가

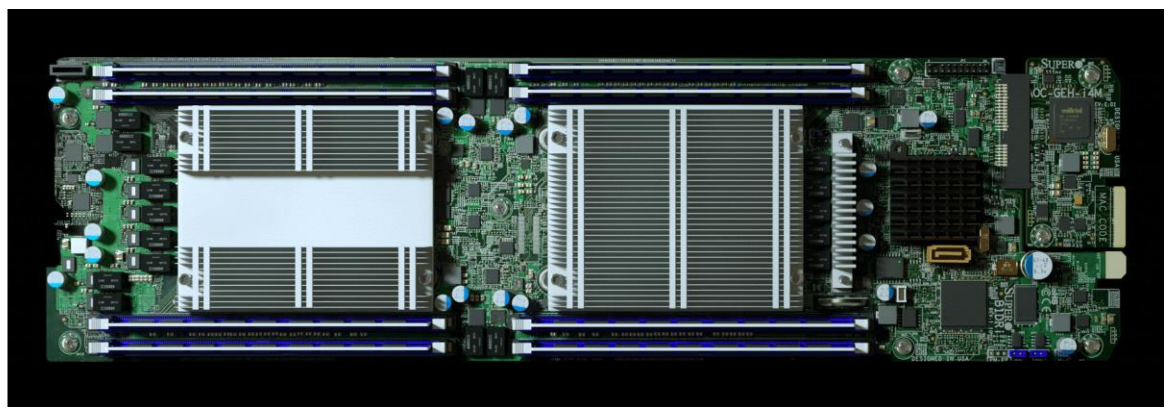
- **시험 대상의 모든 부품을 전수 조사**

  조사를 위해 인력, 시간, 비용의 대규모 투자 필요

- **일부 장비는 파괴 검사 수행 필요**

  검사된 장비는 재사용 불가, 검사의 목적 상실

[출처 : 국방보안연구소]



파괴적 검사 방법 예

[출처 : Bloomberg : “The Big Hack”]

임베디드 시스템 보안을 위한
Power Fingerprint

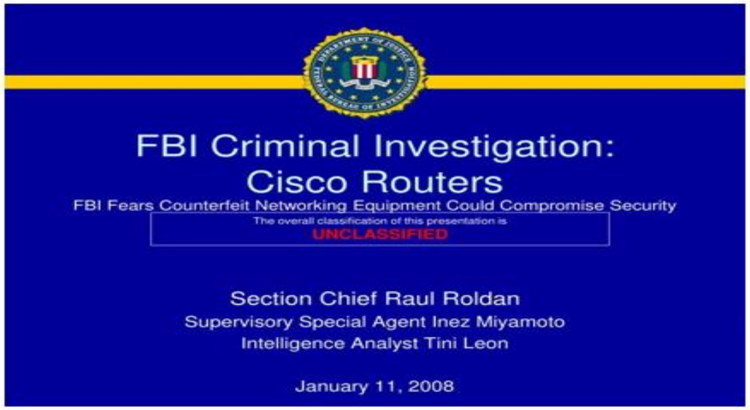
HANCOM
한컴MDS

미국의 위변조 사이버 공격에 의한 사고 사례

- **미 해군의 위조된 네트워크 장비 사용**

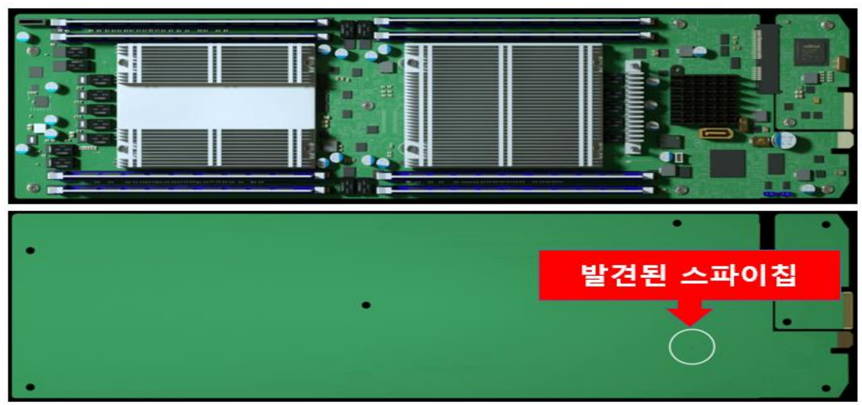
  중국에 의해 위조된 것으로 추정되는 CISCO 장비 사용

  미국 정부 네트워크가 18개월간 무방비 상태로 노출되었던 사건



- **미국의 정부와 주요 기업에 납품되는 서버용 보드**

  중국에서 제작 및 공급되는 과정에 스파이 칩으로 의심되는 부품이 설치되어 제공



HANCOM 한컴MDS

미 국방부의 Power Fingerprint를 활용하는 개발 프로젝트 소개

- **미국방부 DARPA의 LADS(Leveraging the Analog Domain for Security) 프로그램의 목적**

  EMSD(Embedded Mission Specific Device)의 보안 위협을 모니터링할 수 있는 새로운 방안 개발

  일반 PC나 서버와 같은 시스템에 보안 향상을 위해 적용되고 있는 Cybersecurity Defense in Depth 전략을 임베디드 시스템에도 적용할 수 있는 기술 검토

  기존 보안 환경을 유지하면서 임베디드 시스템에 추가로 보안 성능을 향상 시킬 수 있는 방안으로 Power Fingerprint를 활용한 보안 솔루션 개발

- **LADS 프로그램의 보호 대상**

  군용/산업제어시스템/SCADA/IoT 등에 사용되는 저전력 및 리소스가 작은 임베디드 시스템

- **위협 측정 방법**

  어떠한 특정 신호(음성, 전력, 전자파 기타 등등)의 제한 없으며,

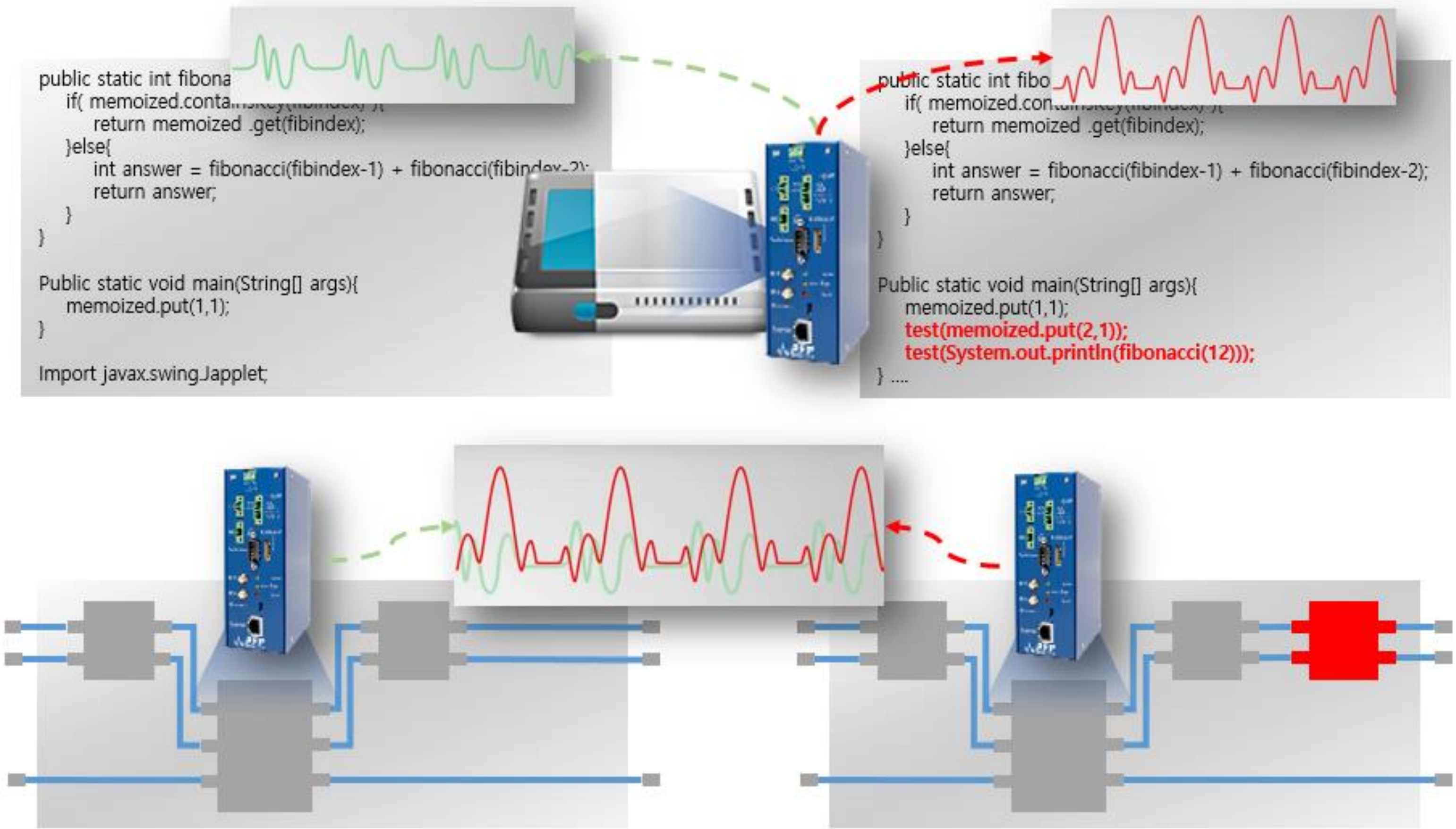
  디바이스가 동작하는 과정에 출력할 수 있는 비자발적 아날로그 신호를 측정하여 이상 동작 감지

- **전체 투자 비용**

  $36M (한화 약 400억원)

임베디드 시스템 보안 향상을 위한 기술 – Power Fingerprint 소개

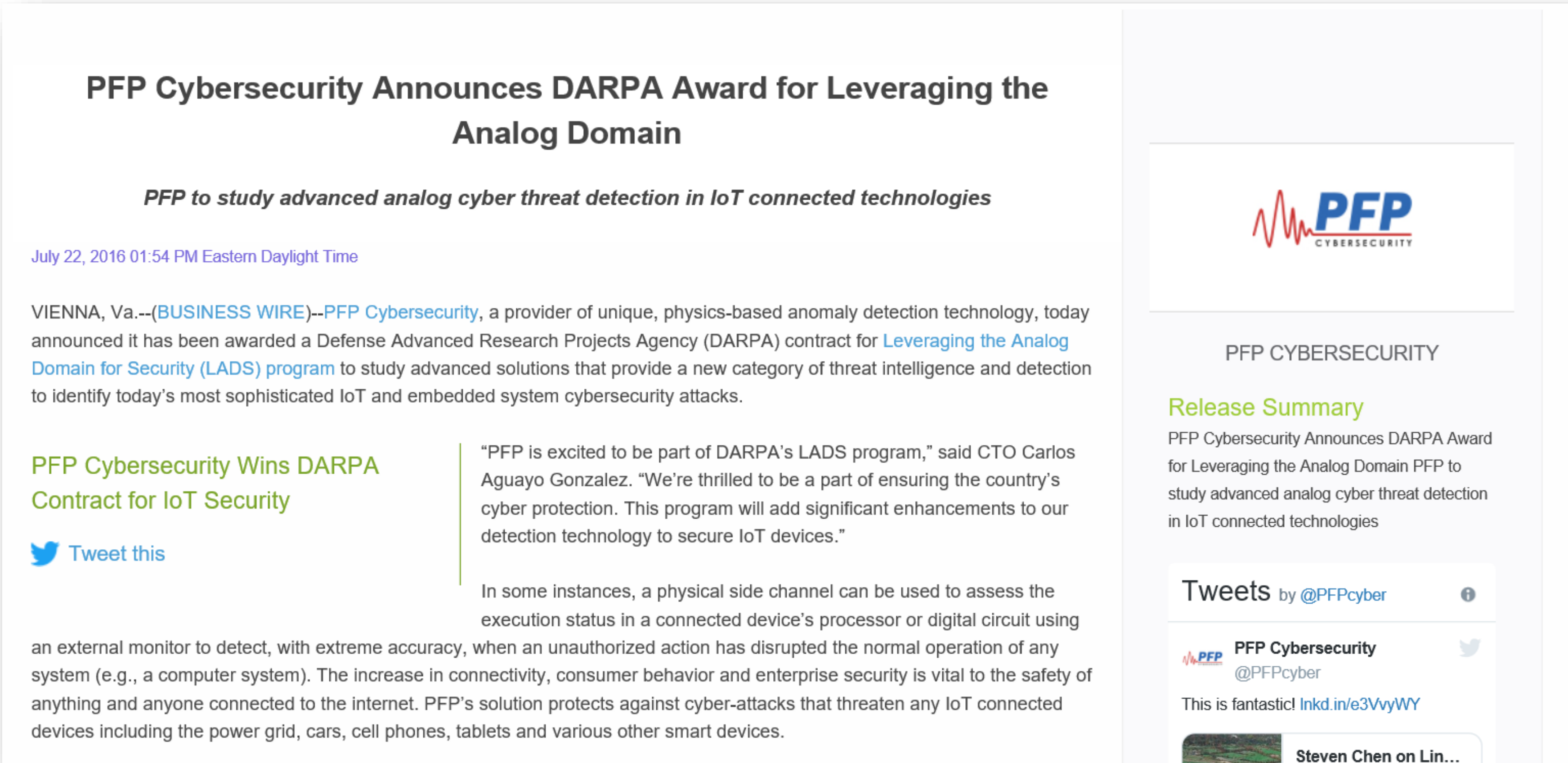
- **Power Fingerprint**
  - 장치의 HW/SW 조합을 구분할 수 있는 신호
  - HW 구성이 달라지거나 SW 로직이 변경되면 다른 형태의 신호 패턴이 발생
  - Power Fingerprint를 이용하여 사이버 공격에 의해서 발생 가능한 HW/SW의 모든 이상 동작 탐지 가능



세계 최초 Power Fingerprint를 이용한 보안 솔루션 개발사 PFP Cybersecurity

- **DARPA에서 LADS 프로그램에 활용하는 도구로 PFP Cybersecurity사의 제품을 선정**

  총 3곳에 투자하여 현재 유일하게 PFP Cybersecurity사가 Power Fingerprint를 이용한 보안 솔루션을 실용화



PFP Cybersecurity Announces DARPA Award for Leveraging the Analog Domain

PFP to study advanced analog cyber threat detection in IoT connected technologies

July 22, 2016 01:54 PM Eastern Daylight Time

VIENNA, Va.--(BUSINESS WIRE)--PFP Cybersecurity, a provider of unique, physics-based anomaly detection technology, today announced it has been awarded a Defense Advanced Research Projects Agency (DARPA) contract for Leveraging the Analog Domain for Security (LADS) program to study advanced solutions that provide a new category of threat intelligence and detection to identify today's most sophisticated IoT and embedded system cybersecurity attacks.

PFP Cybersecurity Wins DARPA Contract for IoT Security

Tweet this

"PFP is excited to be part of DARPA's LADS program," said CTO Carlos Aguayo Gonzalez. "We're thrilled to be a part of ensuring the country's cyber protection. This program will add significant enhancements to our detection technology to secure IoT devices."

In some instances, a physical side channel can be used to assess the execution status in a connected device's processor or digital circuit using an external monitor to detect, with extreme accuracy, when an unauthorized action has disrupted the normal operation of any system (e.g., a computer system). The increase in connectivity, consumer behavior and enterprise security is vital to the safety of anything and anyone connected to the internet. PFP's solution protects against cyber-attacks that threaten any IoT connected devices including the power grid, cars, cell phones, tablets and various other smart devices.

PFP CYBERSECURITY

Release Summary

PFP Cybersecurity Announces DARPA Award for Leveraging the Analog Domain PFP to study advanced analog cyber threat detection in IoT connected technologies

Tweets by @PFPcyber

PFP Cybersecurity
@PFPcyber

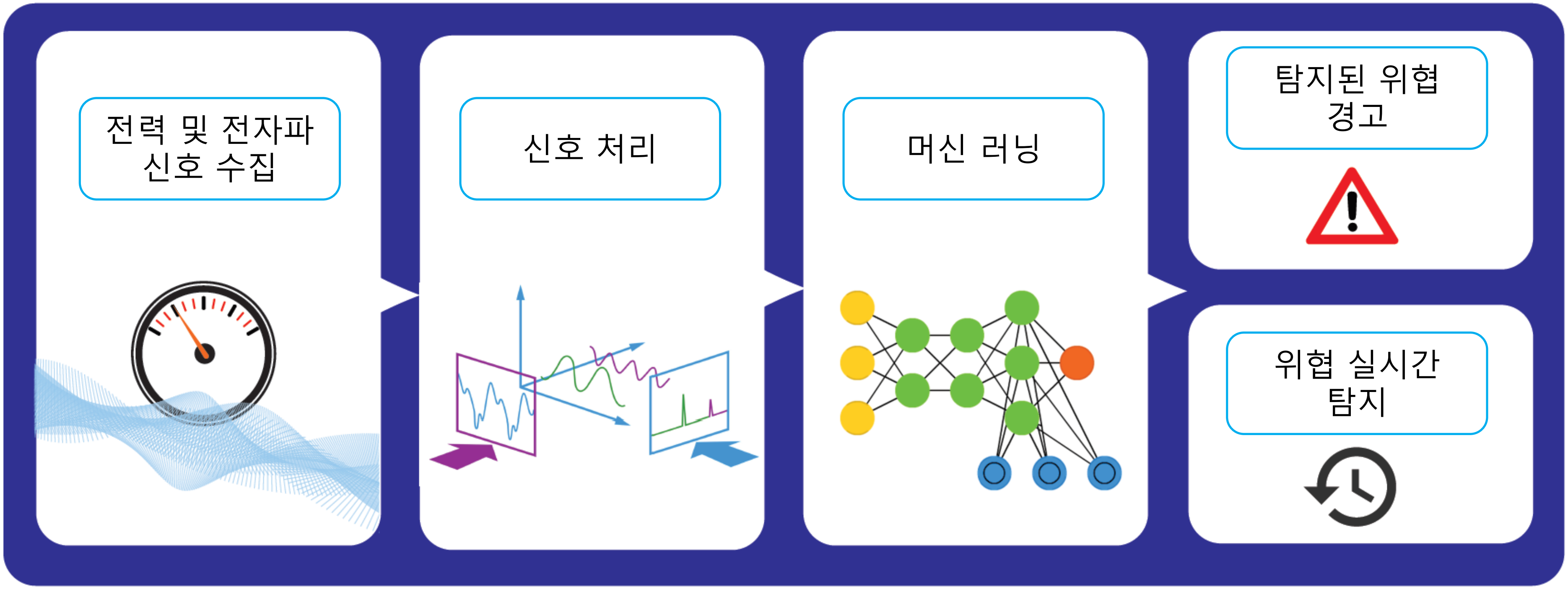
This is fantastic! lnkd.in/e3VvyWY

Steven Chen on Lin...

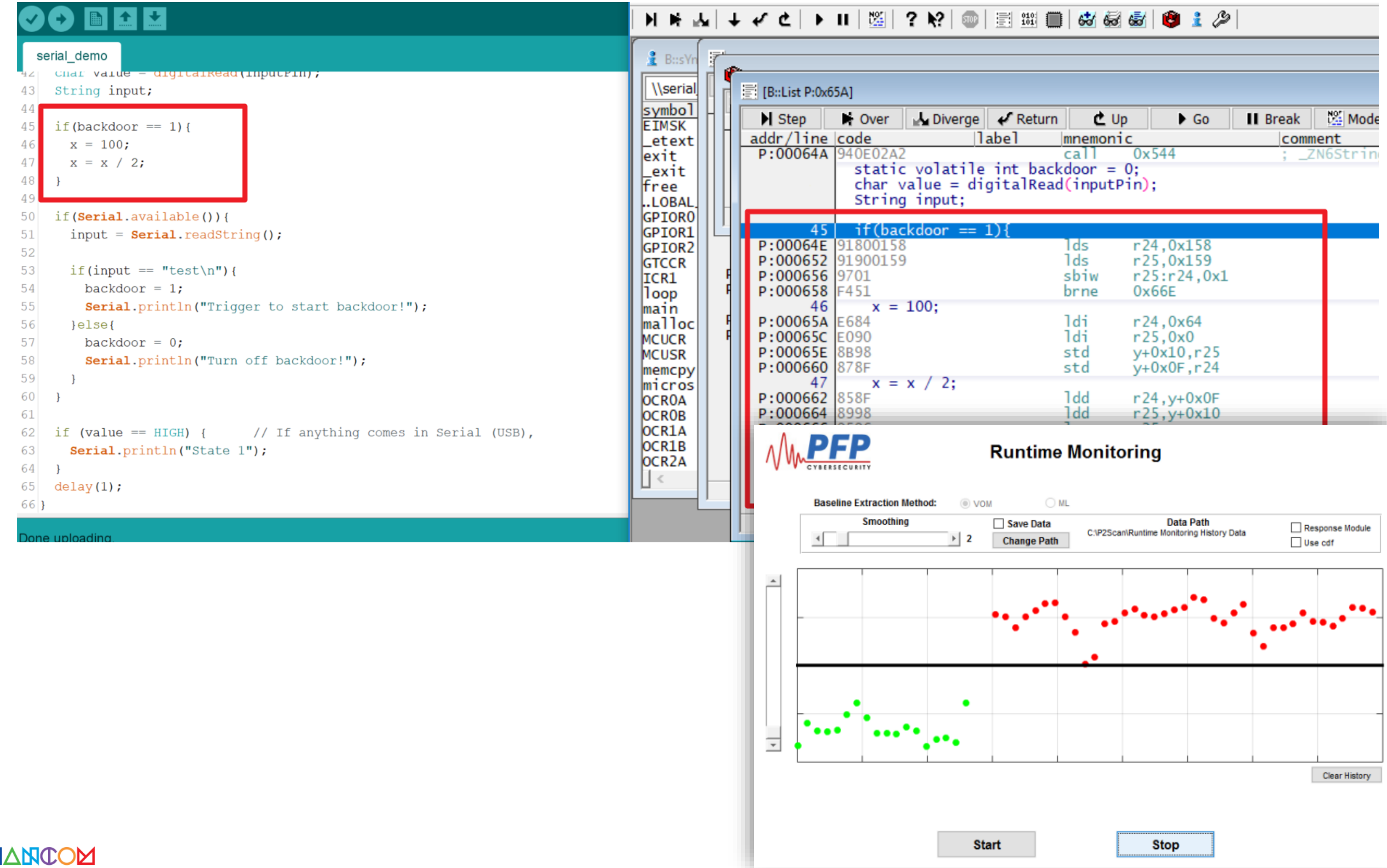
*** 출처 : Business Wire, https://www.businesswire.com/news/home/20160722005760/en/PFP-Cybersecurity-Announces-DARPA-Award-Leveraging-Analog**

파워 핑거프린트 신호 분석 과정

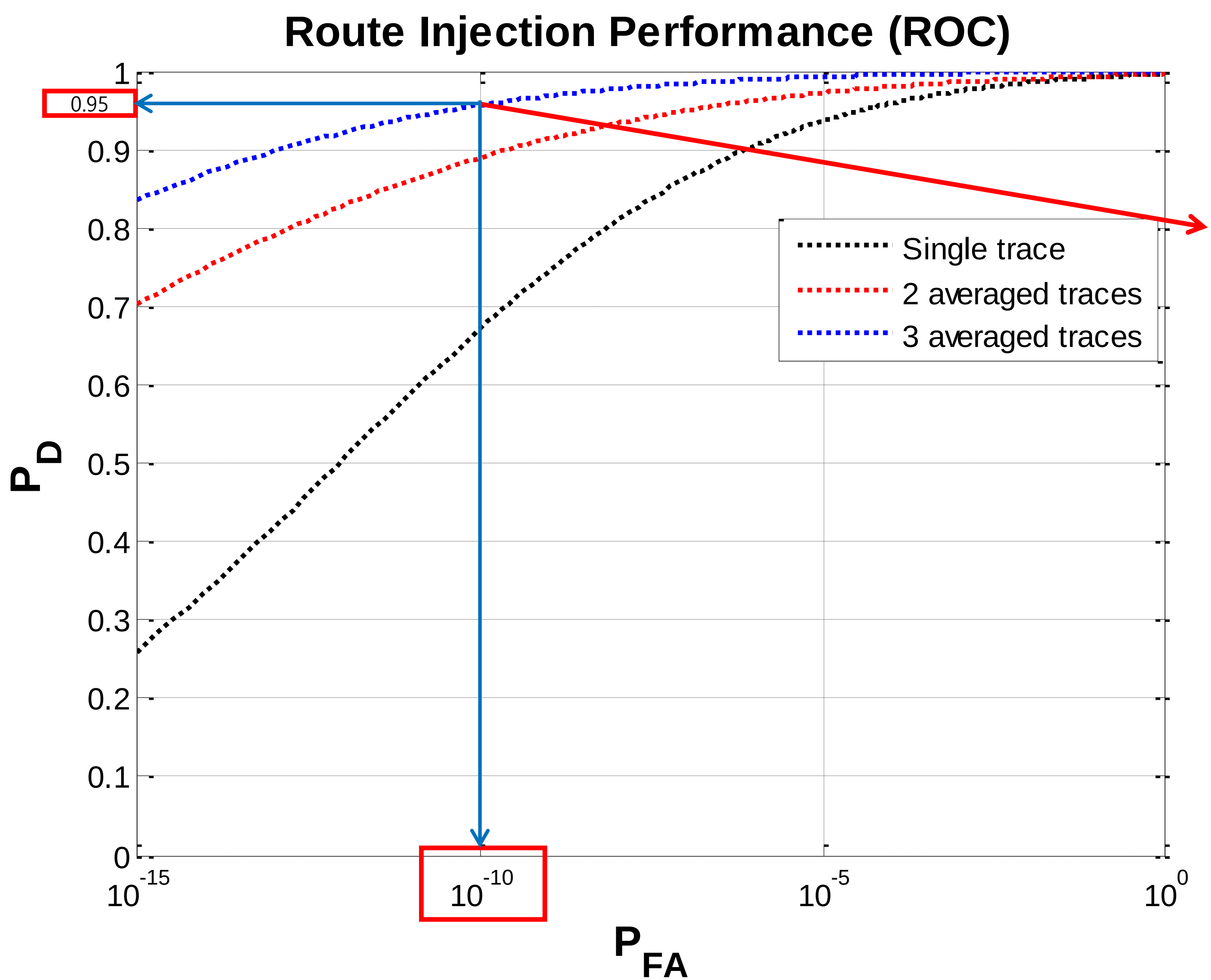
- **수집된 신호를 머신 러닝을 통해 임베디드 장치를 특정하는 신호(Signature) 추출**
- **Signature와 다른 형태로 동작하는 신호 검출 시 위협으로 판단하고 경고**



미세 변화에 대한 탐지 결과



위협 탐지능력



3회 학습했을 경우

검출율: 95%
오검출율: 10^{-10}
(복권 1등 당첨 보다 낮은 확률)

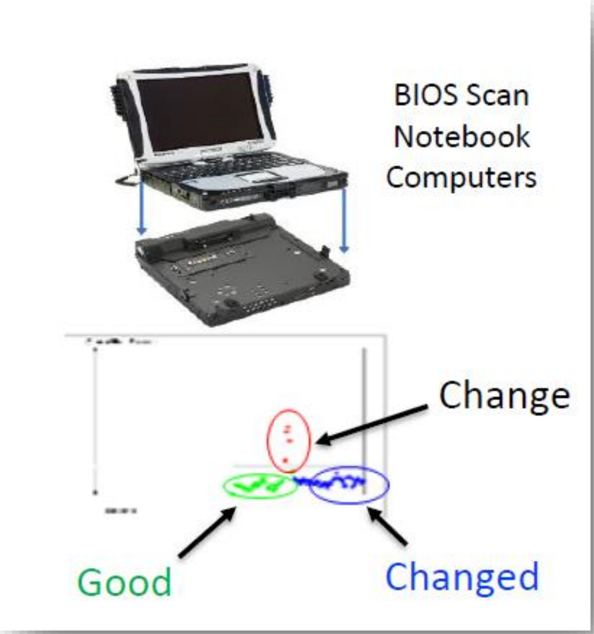
참조: 美방위고등연구기획국(DARPA)의 분석자료(Route Injection Monitoring Performance)

HANCOM 한컴MDS

적용 사례

미국방부의 위협 탐지를 위한 활용 사례

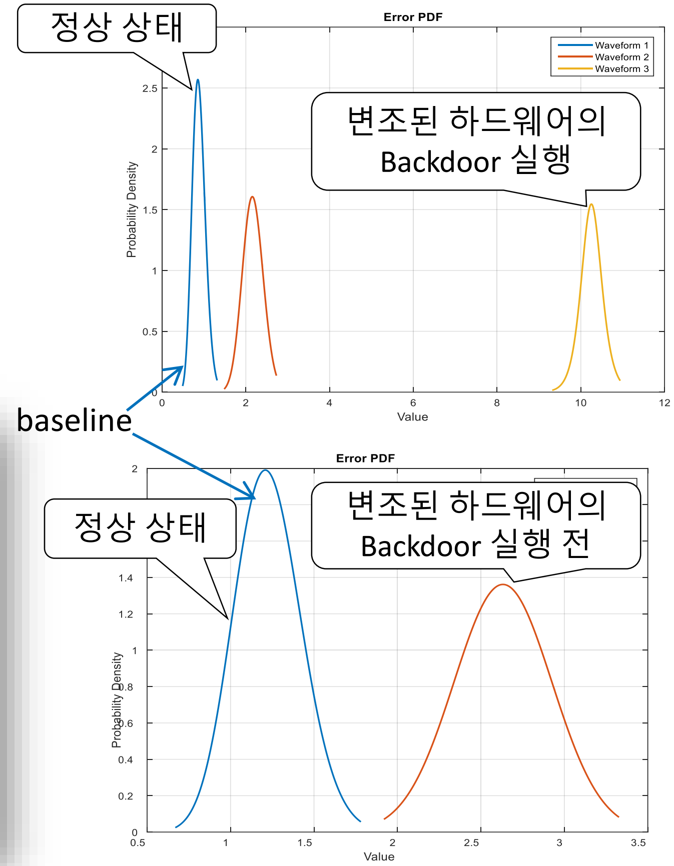
- **군 보안 위협 탐지를 위해 다양한 목적으로 적용**
  - ➔ LADS 프로그램에 미국방부 전환 배치 진행 중
  - ➔ 미 육군 RCCTO(the Army Rapid Capabilities and Critical Technologies Office)는 데이터 센터, 네트워크 인프라, 산업제어시스템 및 무기 시스템에 적용
  - ➔ 미 공군 납품 장비 위조/변조 여부 검사
  - ➔ 미 해군의 한 부대에서 운영 방안 작성



DoD 납품용 노트북 변조 여부 검사

미공군 VME 모듈 변조 여부 검사

- **반도체의 백도어 또는 킬 스위치와 관련된 변조(tampering) 탐지**



Cond_1: False
활성화

Kill switch Activated

Cond_1: True
비활성화

Kill switch loaded

인텔 모든 코어 프로세서에 스포일러(SPOILER) 보안 취약점 발견

인텔 CPU에서 새로운 보안 취약점이 발견되었다

스포일러(Spoiler)로 명명된 이번 보안 취약점은 독일 뤼벡(Lübeck) 대학과 우스터 폴리테크닉 연구소(Worcester Polytechnic Institut)의 공동로 밝혀진 것으로, 연구진은 해당 취약점이 모든 인텔 코어 프로세서를 위협한다고 전했다.

스포일러는 지난해 초 공개된 스펙터/ 멜트다운과 달리 AMD CPU에는 영향이 없는 인텔 CPU만의 보안 취약점으로, OS와는 상관없이 인텔 CPU의 투기적 실행 과 가상 머신, 샌드박스 환경에도 영향을 미친다.

연구진에 따르면 특정 메모리 워크드로에서 인텔의 투기적 실행을 위해서는 메모리의 정보를 알 수 있는 전체 실제 주소 비트가 필요하며, 이를 통해 사용자 공간에서 전체 주소를 사용할 수 있게되므로 권한 상승을 포함한 기타 마이크로아키텍처 공격이 가능하다.

이번에 발견된 보안 취약점은 스펙터/ 멜트다운과 달리 소프트웨어를 통한 완화 조치가 불가능한 실리콘 수준의 문제이며, 때문에 차세대 CPU에서 구조적 대응이 필요하다.

* 출처 : 보드나라, https://www.bodnara.co.kr/bbs/article.html?num=153230

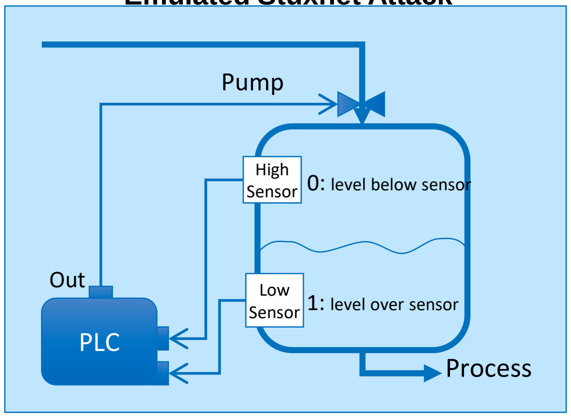
SW를 통해 취약점 제거 또는 완화가 불가능한 약점에 의한 공격 탐지

임베디드시스템 펌웨어 변조 공격 탐지

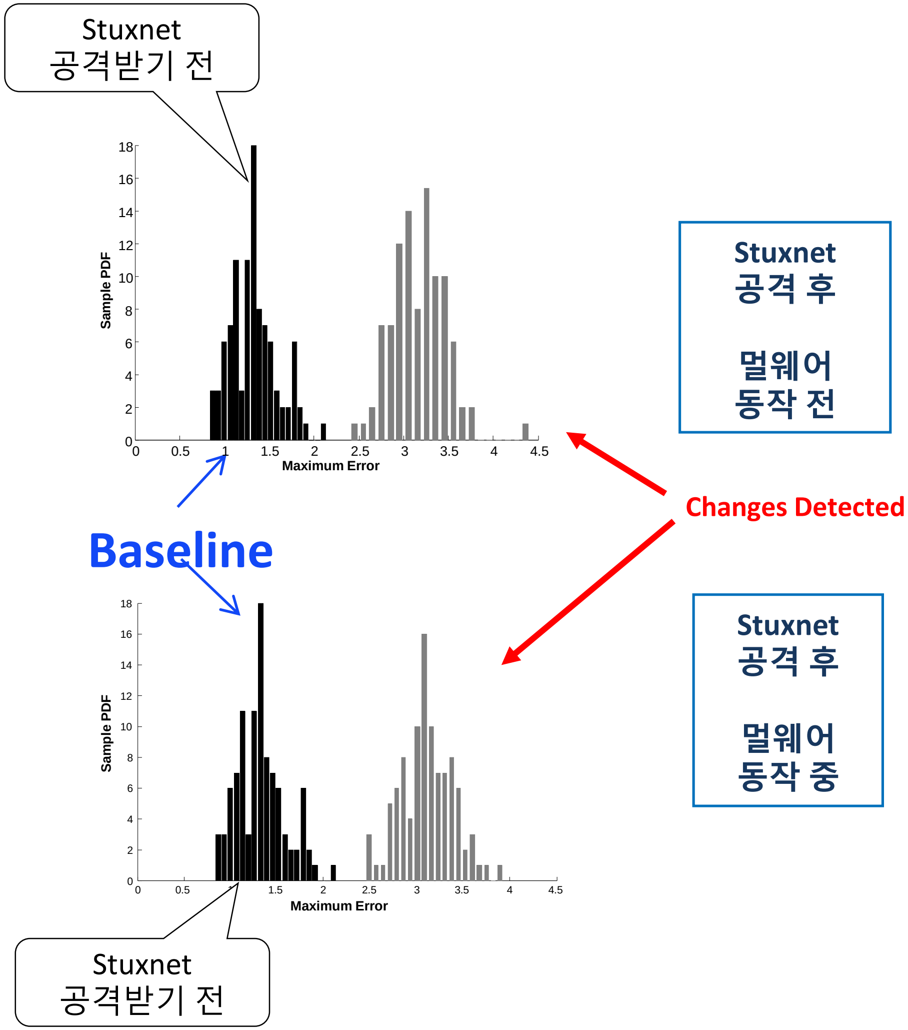
- **Siemens PLC (Stuxnet) – 잠재된 공격**

  이란 핵시설에서 사용하는 지멘스 PLC에 대한 공격 탐지

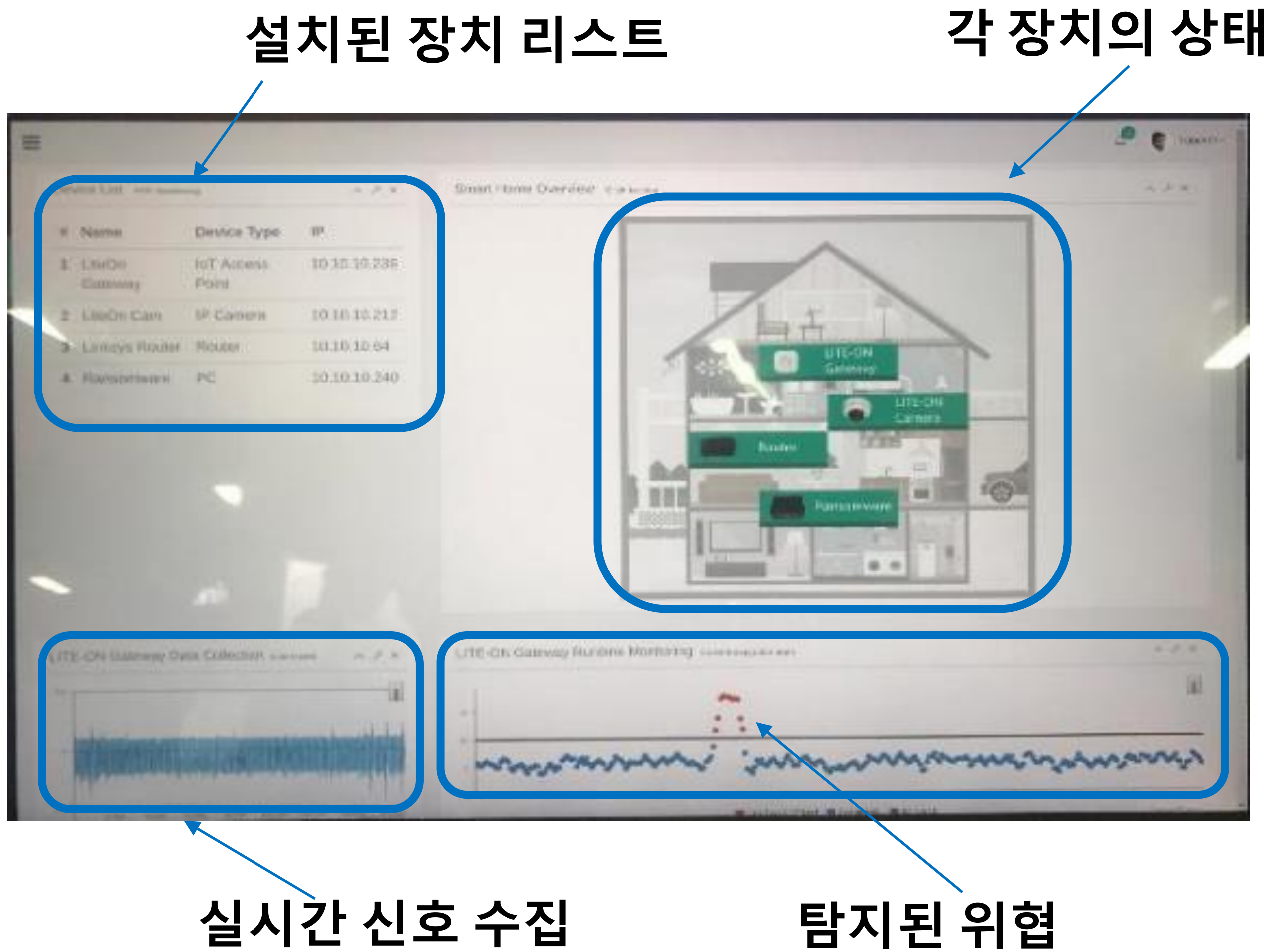
Emulated Stuxnet Attack



Siemens PLC
(SIMATIC S7-1200)

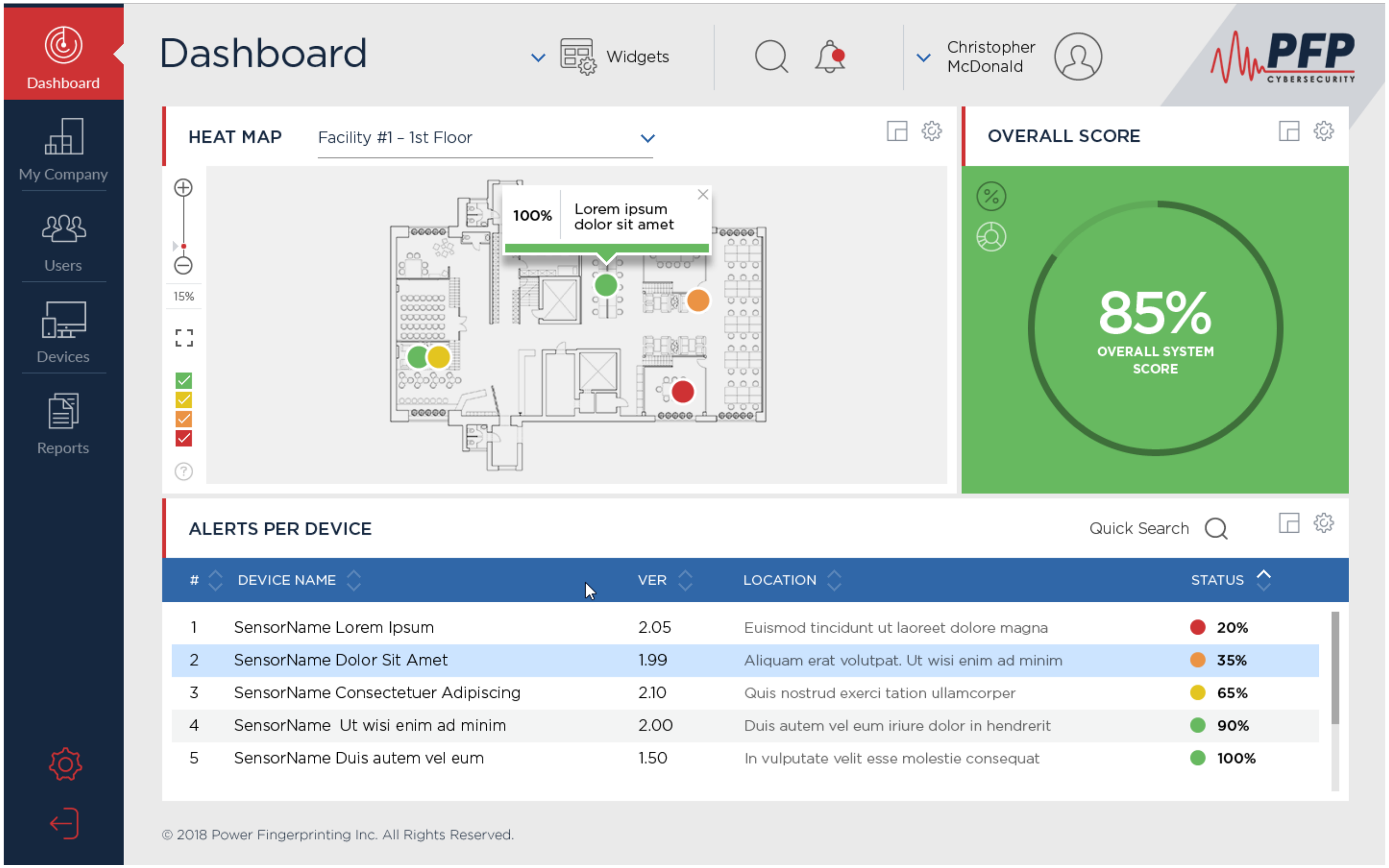


스마트홈 IoT 적용 사례



PFPdhk 빅데이터 솔루션과 연동한 사례로 공격 탐지 뿐만 아니라 추적도 가능

생산 라인 관리를 위한 적용 사례



보안 위협 모니터링 및 HW고장 사전 경보

PFP 적용 효과

- **효과적으로 위변조 장비 탐지 가능**
  - 모든 장비에 대해서 위변조 여부 시험이 가능
  - 자동화를 통해 시험 기간 단축

- **임베디드 장비에 대한 SW 보안 위협 차단**
  - 보안이 가장 취약한 제어 장치에 대한 보안성 확보
  - 오래된 장치에도 즉시 적용하여 보안 허점 완벽히 제거

- **정상 상태 모델 기반의 위협 추론을 수행하므로 Zero-Day Attack도 탐지하여 대응 가능**
  - 모든 위협을 사전 예측하여 경고하여 완벽한 보안 환경 구축

- **장비 노후화나 고장으로 인한 사고 발생 최소화하기 위한 예지 진단**
  - 위조 부품 또는 재활용 부품에 의한 고장 발생 사전 방지
  - 노후 장비의 고장 발생 가능성 사전 예측

Q & A

Thank you

성명준 부장 | myungjun@hancommds.com 031-627-3022

데이터 분석 · 보안 사업부

㈜한컴MDS www.hancommds.com

본사 13493 경기도 성남시 분당구 대왕판교로 644번길 49 한컴타워 3,4층 031-627-3000
연구소 13487 경기도 성남시 분당구 판교로 228번길 17 판교세븐벤처밸리 2단지 1동 9층 031-600-5000