KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 027

July 2020

한국선급 활동

㈜썬컴 Ship@TAMS 제품에 KR 사이버보안 형식승인 증서 수여

COVID-19로 인해 해상 사이버공격 400% 증가

해상무선통신 종류와 AIS의 보안 취약점

사이버 위협의 이해(OWASP Top 10 Internet of Things)

KR 해상 사이버보안 형식승인 지침의 이해

㈜썬컴 Ship@TAMS 제품에 KR 사이버보안 형식승인 증서 수여

한국선급(KR, 회장 이형철)은 최근 ㈜썬컴이 개발한 'Ship@TAMS' 제품에 대해 사이버보안 승인 증서를 수여했다고 24일 밝혔다. 최근 디지털 기술이 선박에 본격적으로 적용됨에 따라 편의성이 증대되었다. 그러나 사이버 위험 노출도 증가하여 사이버보안 인증 서비스에 대한 수요가 증가하고 있다. 이에 한국선급은 국제표준(IEC 62443 4-2, IEC 61162-460)을 기반으로 자체 개발한 사이버보안 승인 서비스를 시행하고 있다. ICT 기자재에 대한 사이버보안 승인 서비스는 선박에 탑재되는 사이버 시스템에 대해 보안의 기본 요건인 기밀성, 무결성, 가용성에 대한 기술적 검토, 사고 발생 시 대응을 위한 감시기능과 백업 및 복구 기능에 대한 검사를 포함하고 있다. 이번에 승인을 받은 'Shp@TAMS'는 조선·해양 IT 전문기업인 ㈜썬컴이 직접 개발한 선내 설치 장비로 육상의 서버와 선박 내 PC와 연동되어 백신에 대해 통합 관리기능을 제공한다. 또 전자해도표시장치(ECDIS)와 같은 운영기술(OT) 장비에 대해 USB를 사용할 경우에도 Ship@TAMS 자체에서 제공하는 USB 보안 검사 기능을 통해 바이러스 감염을 막을 수 있도록 설계된 것이 특징이다. ㈜썬컴의 고태훈 대표는 "세계적으로 우수한 인증역량을 보유한 한국선급으로부터 승인 증서를 받게 되어 뜻깊게 생각한다"며, "앞으로도 선박 사이버보안과 관련된 기술을 선제적으로 개발하여 우수한 강소기업으로 성장해 나가겠다"고 소감을 밝혔다. 한국선급의 박개명 사이버인증팀장은 "해사업계에서 사이버보안 활동은 이제 필수가 되었다"고 강조하며, "이번 승인을 받은 ㈜썬컴과 같이 국내 조선·해양 IT 중소기업들이 해외수출 발판을 마련하고 기술력을 인정받을 수 있도록 선제적인 사이버보안 활동을 적극 지원하겠다."고 말했다.

COVID-19로 인해 해상 사이버공격 400% 증가

해상 사이버공격 400% 증가에 대한 보고

사이버보안 자문회사인 Naval Dome에 따르면 2020년 2월 이후 사이버공격 시도가 400배 증가하였다. 주요 원인은 COVID-19 대유행을 이용한 악성코드, 랜섬웨어, 피싱 이메일의 증가지만, Naval Dome은 해외 여행 제한, 사회적 거리 두기 , 경기 침체 등이 기업들의 자기 방어 능력을 약화시키기 시작했다고 말했다.

게다가, OEM 기술자들은 선박과 시추선 시스템에 서비스를 제공하기 위한 이동에 어려움을 겪고 있어, 운영자들이 보안 조치들을 우회해야 하는 "원격" 서비스 호출을 점점 더 많이 하고 있어 사이버 공격의 기회가 증가하고 있다.

Naval Dome CEO인 Itai Sela는 "COVID-19로 인한 사회적 제한과 국경 폐쇄로 OEM, 기술자, 벤더들은 서비스를 위하여 시스템을 인터넷에 연결해야만 했다. 예산이 삭감되고 서비스 엔지니어의 부재로 인하여 우리는 OEM의 요청으로 OT 시스템을 해안 네크워크에 연결하는 선박 및 연안 장비 직원들이 진단을 수행하고 소프트웨어 업데이트와 패치를 직접 업로드 하는 것을 마주하고 있다."고 말했다.

"이는 IT 시스템과 OT 시스템이 더 이상 분리되지 않으며, 개별 엔드포인트, 중요 시스템 및 구성요소가 취약할 수 있음을 의미한다."고 Naval Dome은 경고했다. 이들 중 일부는 보안 업데이트 패치가 없고 사이버 공격에 더욱 취약한 레거시 시스템이다. Sela는 "잘 보호되지 않는 홈 네트워크와 개인용 PC에서 원격으로 일하는 OEM 인력의 증가가 문제를 가중시킨다." 라고 말했다.

2020년 첫 3개월 동안, 자택 근무자들을 대상으로 한 공격이 10배나 증가했다. 보안 소프트웨어 업체 맥아피는 1월부터 4월까지 모든 기업에 대한 클라우드 기반 사이버 공격이 630% 증가했다고 보고했다.

Sela는 "우리의 철학은 모든 시스템이 위험 순위 결정에 따라 보호되어야 한다는 것이다. 그렇다면 전체 플랫폼은 내외부 공격 벡터로부터 보호된다. 네트워크만 보호된다면 망에 들어가는 모둔 것들이(예: 인가된 인력의 의도치 않은 공격) 연결된 모든 시스템을 감염시킬 것" 이라고 말했다.

Naval Dome 사업개발 담당 부사장인 Ido Ben-Moshe는 원격 작업과 원격 제어 방식의 자율 기술 도입이 코로나바이러스 이후 세계에서 더 빠른 속도로 이루어질 가능성이 높다고 말한다. 그는 "이를 통해 기업들이 적절한 보호 조치를 이행하지 못할 경우 새로운 사이버 보안 문제에 직면하게 될 것"이라고 말했다.

출처 : The Maritime Executive, JULY 01, 2020

해상무선통신 종류와 AIS의 보안 취약점

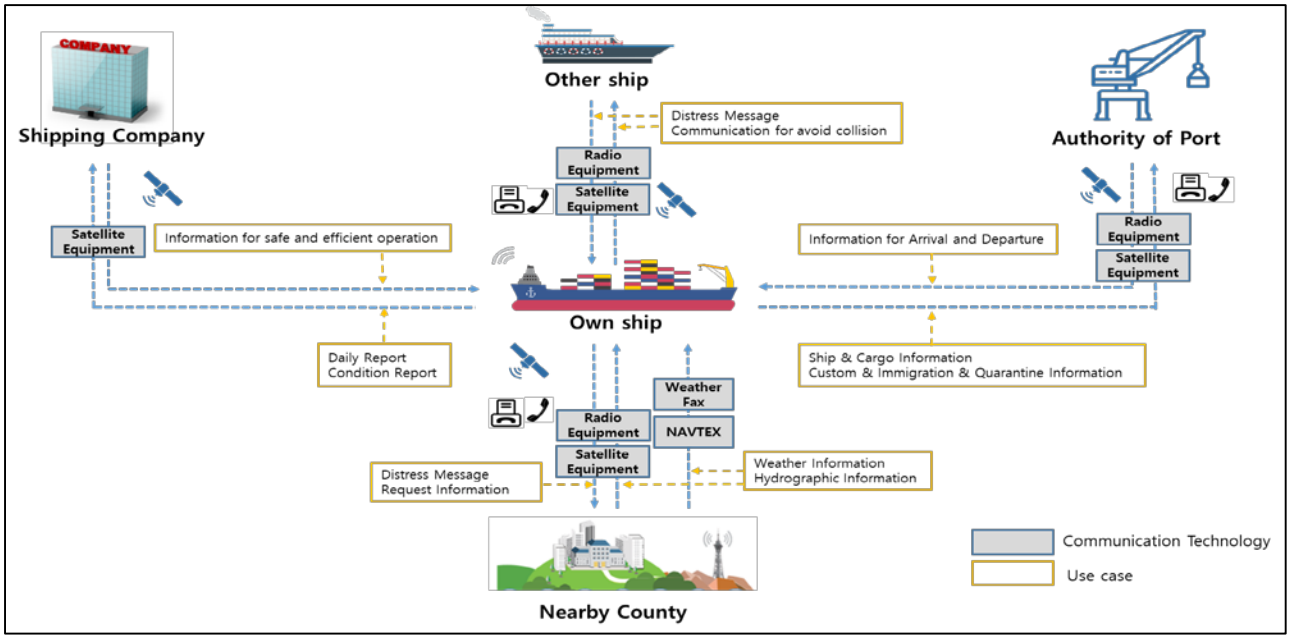
본 기획시리즈는 일상생활과 회사, 선박 등에서 널리 사용되는 무선네트워크의 종류와 통신 원리에 대해 알아보고, 무선 네트워크의 취약점과 대응방안을 소개하고자 한다. 따라서 본 뉴스레터 2020년 7월호에서는 ***'해상 무선통신 종류와 AIS의 보안 취약점'***에 대해 소개한다.

기획시리즈 순서

① 무선 네트워크의 종류와 통신원리
② 무선랜(WIFI)의 기술적 보안 취약점과 대응방안-1
③ 무선랜(WIFI)의 기술적 보안 취약점과 대응방안-2
④ 와이파이6에 적용된 차세대 보안기술
⑤ **해상무선통신 종류와 AIS의 보안 취약점**
⑥ 해상위성통신의 보안 취약점과 대응방안

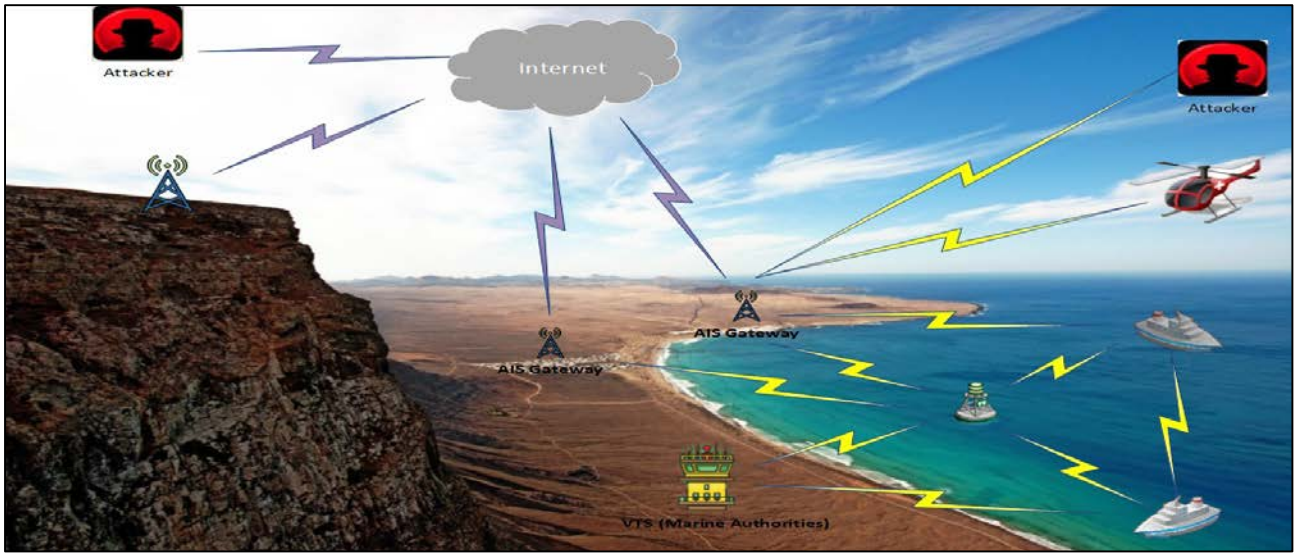
해상무선통신의 종류

현재 선박에 설치된 해상무선통신 장비는 각각 독립적으로 운용되고 있다. 이 중에서 가장 널리 보급되어 있는 디지털 무선통신 장비는 AIS(Automatic Identification System)이다. 다만, AIS의 경우 선박의 위치추적(Tracking for vessels)과 충돌방지(Collision avoidance), 수색구조(Search and rescue), 사고조사(Accident investigation) 등 특정된 서비스를 수행하기 위한 용도로 사용되고 있고, 인터넷을 통한 데이터 교환은 위성통신(VSAT)을 주로 사용하고 있다.



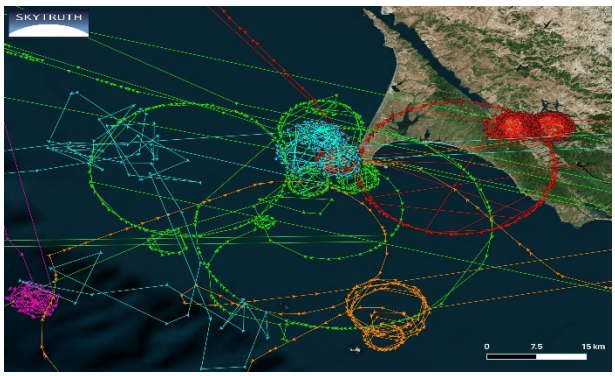
AIS 시스템의 보안 취약성

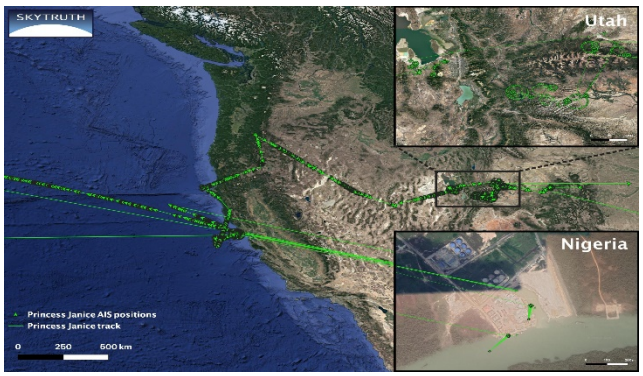
AIS는 2002년 부터 선박에 보급된 해상 무선통신 장비로서, IMO SOLAS 규정에 따라 300톤 이상의 국제항해선박에 설치가 의무화된 통신장비 이다.(내항선, 어선 등의 경우 각 국가별 설치 규정이 다를 수 있음) 전세계적으로 약 100만척 이상의 선박에 설치된 것으로 예상되고 있다. 2014년 유명 해킹 그룹인 블랙햇(Black hat)은 싱가포르 컨퍼런스에서 AIS 시스템의 보안취약성에 대한 소개를 진행한 바 있다.



출처 : Blackhat Asia 2014, AIS Exposed understanding Vulnerabilities & Attacks 2.0

이 자료에 따르면, AIS는 기계간 인증(Authentication), 무결성 체크 (Integrity check) 기능이 설계되어 있지 않기 때문에 무선 스푸핑(RF spoofing), 하이재킹(Hijacking), GPS 스푸핑 등의 다양한 사이버 위협에 노출되어 있음을 알 수 있다. 특히, 2016년 4월 북한의 GPS 재밍 공격으로 동해지역에서 약 290척의 선박 GPS 시스템이 무력화된 사건이 있었다. 또한, 최근 미국의 민간 연구소 skytruth에 따르면, AIS 표시장치에서 선박이 실제위치와는 다르게 허위로 돌고 있는 선박이 표시되는 현상을 발견했다고 한다. 이 선박을 추적해본 결과, 수천 마일 떨어진 곳에서 항해하는 선박이 허위로 나타나는 것이다. 선원 입장에서는 이러한 가짜 AIS 신호로 인해 선박의 항로를 결정하는데 있어 혼란을 초래할 수 있다.





출처 : https://skytruth.org/blog/

사이버 위협의 이해(OWASP Top 10-IoT)

OWASP Top 10-사물인터넷 편

OWASP(Open Web Application Security Project)에 따르면 OWASP 사물 인터넷 프로젝트의 목표는 제조업체, 개발자, 소비자가 사물인터넷과 관련된 보안 문제를 더 정확히 이해하고 사용자가 IoT 기술을 구축, 배포 또는 평가할 때 보안 측면에서 더 현명한 의사 결정을 내리는데 도움을 제공하기 위함이다. 2020년 사이버보안 뉴스레터에서는 OWASP에서 선정한 사물인터넷(IoT)의 사이버 위협 Top 10과 대응방안을 살펴보고자 한다.

안전하지 않거나 오래된 구성요소의 사용

오래된 소프트웨어 구성요소를 사용하거나 코드에서 안전하지 않은 라이브러리를 참조하면 제품의 전반적인 보안이 저하될 수 있다. 따라서 IoT 장비 개발자 또는 제조자는 아래의 규정을 만족하여야 한다.

1. IoT 장비의 모든 소프트웨어 구성요소를 안전하게 업데이트할 수 있어야 한다.
2. 소프트웨어가 업데이트가 필요한 경우, 제조자 또는 서비스 공급자는 사용자에게 알려야 한다.
3. 소프트웨어 구성요소를 업데이트할 수 있는 경우, 업데이트는 시기적절해야 한다.
4. 소프트웨어 구성요소를 업데이트할 수 있는 경우, 장비가 소프트웨어 업데이트를 받을 수 있는 최소 기간과 지원 기간의 이유를 명시된 수명 종료 정책을 발표하여야 한다.
5. 소프트웨어 구성요소를 업데이트할 수 있는 경우, 각 업데이트의 필요성을 소비자에게 명확히 하고 업데이트를 구현하기 쉬워야 한다.
6. 소프트웨어 구성요소를 업데이트할 수 있는 경우, 업데이트는 가능한 경우 장치의 기본 기능을 유지하여야 하고 업데이트 중에 사용 가능한 상태로 유지하는 것이 중요하다.
7. 소프트웨어 구성요소를 업데이트할 수 있는 경우 소프트웨어 업데이트의 입증 여부를 보장하고 보안 패치를 보안 채널을 통해 제공해야 한다.
8. 소프트웨어를 업데이트할 수 없도록 제한된 장비의 경우 제품을 분리하고 하드웨어를 교체할 수 있어야 한다.
9. 소프트웨어를 업데이트할 수 없는 제한된 장치의 경우, 소프트웨어 업데이트의 부재에 대한 근거, 하드웨어 교체 지원 기간 및 수명 만료 정책은 소비자가 명확하고 투명하게 접근할 수 있는 방법으로 공표해야 한다.

출처 : ETSI TS 103 645 v1.1.1

KR 해상 사이버보안 형식승인 가이드라인

사이버보안 형식승인 지침 이해하기

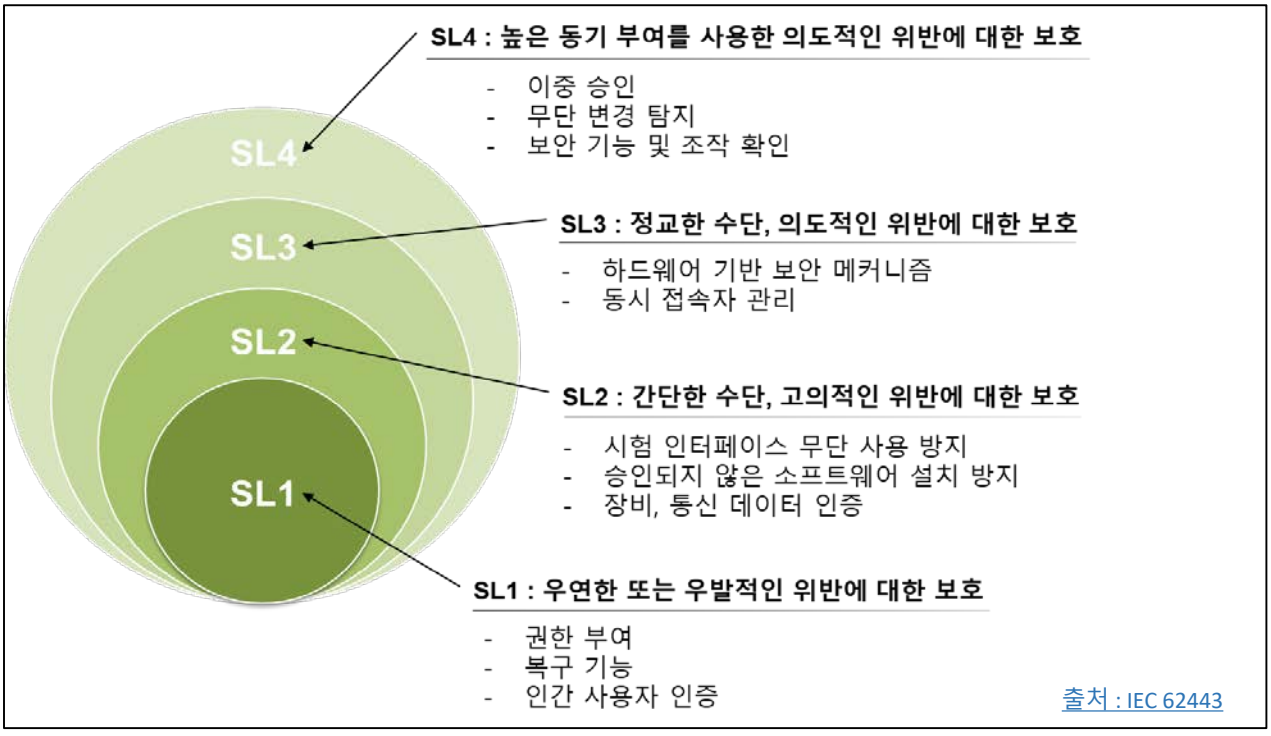
형식승인이란, 선박에 설치하기 전에 제품의 각 형식마다 미리 자료심사 및 승인시험을 하고 만족할 경우 제품이 규정에 적합하다는 것을 제조자에 대해서 증명하는 것을 의미한다. 사이버보안 형식승인은 ISA 62443 4-2, IEC 61162-460과 같은 국제표준을 기반으로 개발되었으며 선박에 탑재되는 원격 접속 장비, 통합 제어 및 모니터링 시스템 등을 포함하는 사이버 시스템의 사이버보안 수준 및 그 수준에 해당하는 요건을 12개의 범주 및 총 124개 항목의 요구 사항에 대한 검증을 통해 보안 기능과 그 수준을 확인한다.

<KR 사이버보안 형식승인 지침의 구성>

제1절 : 일반사항	제5절 : 데이터 기밀성	제9절 : SW 애플리케이션 요건
제2절 : 식별 및 인증	제6절 : 제한된 데이터 흐름	제10절 : 임베디드 장비 요건
제3절 : 사용 제어	제7절 : 사고에 대한 적시 대응	제11절 : 호스트 장비 요건
제4절 : 시스템 무결성	제8절 : 리소스 가용성	제12절 : 네트워크 장비 요건

출처 : http://www.krs.co.kr/KRRules/KRRules2019/data/data_other/ENGLISH/gc31e000.pdf

보안등급(SL, Security Level)의 이해



출처 : IEC 62443

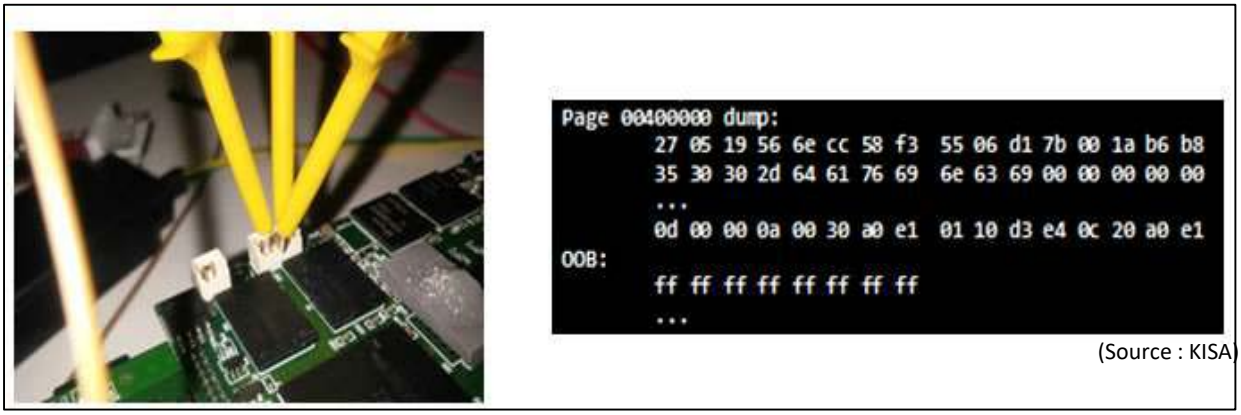
한국선급 해상 사이버보안 형식인증 검사항목

임베디드 장비 요건 - 물리적 진단 및 시험 인터페이스 사용 (1002)

1. 물리적 공장 진단 및 시험 인터페이스(예: JTAG 디버깅)에 대한 무단 사용을 방지하여야 한다. (SL2)
2. 기기의 진단 및 시험 인터페이스에 대한 능동 모니터링을 제공하고 이러한 인터페이스에 접속하려는 시도가 감지될 때 감사 로그 기록을 생성하여야 한다. (SL 3,4)

진단 및 시험 인터페이스의 보안

PLC와 같은 임베디드 장비의 경우 시스템 유지보수 혹은 펌웨어 업데이트 등을 위해 별도의 물리적 PORT가 사용될 수 있다. 이에 대한 예시로 JTAG(Joint Test Action Group) Port가 있으며 이러한 물리적인 Port는 외부 공격에 악용될 수 있다.



<노출된 Port에 대한 물리적 공격의 예시>

사이버보안 형식승인의 SL2 등급을 만족하기 위해서는 이러한 공격의 대상이 될 수 있는 물리적인 Port에 대한 무단 사용 방지가 제공되어야 한다. 물리적 공장 진단 및 시험 인터페이스에 대한 무단 사용 방지의 예시로는 우선 개발 단계에서만 해당 Port를 사용하고 제품 출시 이후에는 해당 Port의 제거하는 방법이 있다. 이는 가장 완벽한 방법이지만 제품의 특성에 따라 출시 이후 해당 Port의 사용이 필수적으로 요구될 수도 있으므로 이러한 경우 접근 제한 기능을 제공함으로써 해당 요건을 만족 할 수도 있다. JTAG Port의 경우 칩 제조사에서 제공하는 프로그램 도구를 이용하여 접근 제한 기능을 구현할 수 있다. SL 3, 4 등급을 만족하기 위해서는 진단 및 시험 인터페이스에 대한 능동 모니터링을 제공하고 접근 시도가 감지될 경우 이를 기록으로 남길 것을 요구하고 있다. 무단 사용 방지를 위해 Port 제거가 아닌 접근 제한 기능을 구현하는 경우 이에 대한 접근 기록을 로그 등에 남김으로써 해당 요건을 만족할 수 있다.