KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 028

August 2020

MacNet 전략웹비나 사이버보안 발표

(사)해양산업클러스터(MacNet, 회장 이형철 한국선급 회장)가 지난 15일 온라인을 통해 'MacNet 2020 전략세미나"를 개최하였다.

MacNet이 주최하고 부산시가 후원한 이번 전략세미나는 '지속 가능한 해운항만산업 발전을 위한 탈탄소화 규제와 사이버보안의 전략적 대응'이라는 주제로 개최되었다. 그 중 제2세션에서 '디지털 산업환경 변화에 따른 해사 사이버보안 현황 및 대응'을 주제로 펜타시큐리티 심상규 상무가 '자율운항 선박의 사이버보안', 고려대학교 차영균 교수가 'Cybersecurity in the Digitalization'에 대해 발표하였고, 한국선급의 박개명 팀장이 토론에 참여하였다.

심상규 상무는 자율주행자동차의 사이버보안 기술을 바탕으로 선박의 외부 통신 보안과 내부 시스템 보안에 어떻게 사이버보안을 적용할 것인가에 대해 발표하였다. 차영균 교수는 ICT 기술 도입으로 인한 해사 산업계의 변화와 관련한 사이버보안에 대해 설명하였다.

현재 해상 비즈니스 환경이 블록체인, 인공지능(AI), 빅데이터, 디지털 플랫폼, 사물인터넷 등 정보통신기술(ICT)의 도입으로 사이버 상의 위협과 리스크가 한창 높아지는 추세이다. 이러한 상황에서 '해운 항만의 사이버보안 문제 대응 ' 에 대한 심도 있는 논의가 진행되었다고 MacNet 관계자는 전했다.

해상 사이버 공격 3년 만에 900% 증가

해사 산업계 운영 기술(OT) 시스템에 대한 사이버 공격 지난 3년간 900% 증가

지난 주 항만 보안 세미나 및 엑스포 온라인 포럼에서 항만과 터미널 운영자들을 언급하면서 보스턴에 위치한 Naval Dome의 북미 본부 책임자인 Robert Rizika는 2017년에 50 건의 중대한 OT 해킹이 보고되었으며, 2018년에는 120건, 작년에는 310건 이상으로 증가했다고 말했다. 그는 올해 500건 이상의 주요 사이버보안 사고가 발생할 것으로 보이지만, 실질적으로는 모두 보고되지는 않을 것이라고 말했다.

Rizika는 Maersk 선사에 미화 3억 달러의 손실을 초래한 NotPetya 이후 해사 산업계에 대한 사이버 공격이 놀라운 속도로 증가하고 있으며, 올해 미국에 본사를 둔 가스 파이프 라인 운영사 및 MSC 선사가 악성 코드에 의해 타격을 받았으며, 그 중 후자의 사건은 5 일 동안 제네바 본사가 폐쇄되었다고 말했다.

지난 달 이란의 샤히드 라지 항구의 OT 시스템이 해킹되어 수십 척의 화물선과 유조선이 하역을 기다리고 있으며, 항구 입구에 긴 트럭이 형성되었다고 Naval Dome은 전했다. 이 공격에 대한 보고는 사이버 위협이 전 세계 항구에 미치는 잠재적 영향에 대한 대중의 인식을 높이는 데 어느 정도 사용되었다.

또한 Rizika는 런던 로이드가 발표한 보고서에서 15개의 아시아 항구가 해킹을 당하면 재정적 손실이 1,100억 달러 이상이 될 것이며, OT 시스템 해킹이 보험 적용되지 않는 것처럼 상당한 금액이 보험 정책을 통해 회복되지 않을 것이라고 밝혔다.

RTG, STS 크레인, 교통 관제 및 선박 정박 시스템, 화물 처리 및 안전 및 보안 시스템 등 OT 시스템의 어느 부분이 위협을 받고 있는지 설명하면서, Rizika는 모두 위협을 받고 있다고 말했다.

“IT 인프라와 달리 운영자가 모든 연결된 시스템의 상태를 확인할 수 있는 OT 네트워크 ‘대시보드’가 없다. 운영자는 공격이 발생했는지, 시스템 오류, 시스템 실패 또는 재부팅이 필요한 예외사항이 항상 기록되었는지 거의 알지 못한다.”

"흥미로운 것은 많은 사업자가 기존의 사이버 보안으로 보호받고 있다고 생각하지만 IT 시스템을 보호하는 방화벽과 소프트웨어는 OT 네트워크의 개별 시스템을 보호하지 않는다. 또한 바이러스 백신 시스템은 필수적인 것이 아니고, 시스템 성능을 손상 및 저하시킨다는 것이 매우 빨리 판명될 것이다."라고 그는 말했다

OT 네트워크가 보호되는 것으로 생각되는 경우, Rizika는 네트워크와 단절된 영구적인 상태로 운영되거나 RF 무선 통신(Wi-Fi) 또는 심카드를 통한 셀룰러 네트워크를 통해 항만 시스템과 해외 기자재 업체 사무실과 연결되는 종종 불충분하고 산업용 컴퓨터 시스템을 기반을 두고 있다고 말했다.

"해커는 크레인에 접속할 수 있다. 그들은 데이터 저장 시스템에 접속할 수 있다. 그들은 셀룰러 연결, Wi-Fi 및 USB 스틱을 통해 핵심 운영 시스템에 침투할 수 있다. 이러한 시스템에 직접 침투할 수 있다."

Rizika는 해양 산업이 점점 디지털화되고, 네트워크 및 자율 시스템의 사용이 증가하고 더 많은 장비와 기술이 온라인으로 이동함에 따라 더 많은 취약점과 허점이 만들어질 것이라고 말했다.

"시스템이 제대로 보호되지 않으면 사람들이 공격할 수 있는 새로운 사이버보안 통로가 생길 것이다."

"이 세심하게 관리되는 작업의 한 조각이 무너지면 전례 없는 적체를 만들고 글로벌 무역에 영향을 미쳐 몇 달이 아니면 몇 주 동안 운영 및 인프라를 방해하여 수천만 달러의 손실을 초래할 것이다. "

Naval Dome은 또한 사이버 범죄자, 테러리스트 및 불량 국가가 언젠가 이러한 환경을 인질로 잡고 몸값을 요구하기 시작할 것이라고 예측한다. "우리가 주요 문제가 될 것으로 생각하는 영역은 사이버로 인한 환경 오염이다. 생각해 보라. 모든 선박이 항구에 있는데 해커가 쉽게 유해 물질, 평형수, 연료 오일 등의 누출 및 폐기를 시작하도록 시스템 및 밸브를 쉽게 중단시킬 수 있다."

항만 운영자가 OT 시스템을 보호하기 위해 취해야 할 첫 번째 단계에 대한 조언을 제공하면서 두 공간의 차이점에 대한 깊은 이해가 중요하다고 말했다.

" IT 보안과 OT 보안 사이에는 단절이 있다. 네트워크 간에는 실제 분리가 없다. 사람들은 OT 측으로 들어와 IT 측에 침투 할 수 있다. 우리는 지금 실제로 이것을 보고 있다. 성공적인 IT 네트워크 해킹은 OT 시스템의 초기 침투에 그 기원을 가지고 있다."

Source : Naval Dome, 2020

해상위성통신의 보안 취약점과 대응방안

본 기획시리즈는 일상생활과 회사, 선박 등에서 널리 사용되는 무선네트워크의 종류와 통신 원리에 대해 알아보고, 무선 네트워크의 취약점과 대응방안을 소개하고자 한다. 따라서 본 뉴스레터 2020년 8월호에서는 **'해상 위성통신의 보안 취약점과 대응방안'**에 대해 소개한다.

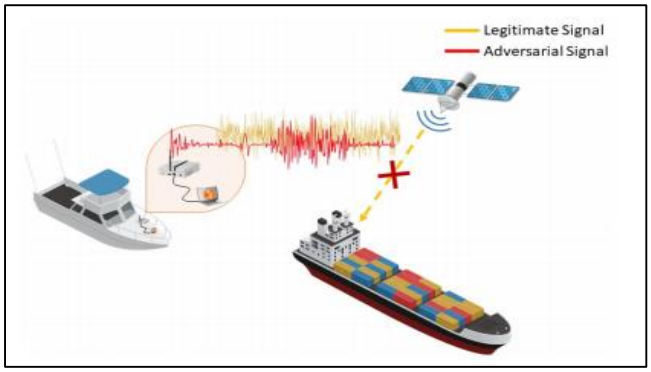
기획시리즈 순서

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

해상위성통신의 주요 보안 취약점

1. Global Navigation Satellites System(GNSS)

국제 항해 선박들은 자신의 정확한 위치를 수신하기 위해 대부분 GNSS 시스템이 대부분 장착되어 있다. GNSS 시스템은 위성에서 발생하는 신호를 이용하여 선박의 위치를 예측할 수 있는 시스템을 말한다. GNSS 시스템을 사이버보안 관점에서 바라보면, 가용성을 높이기 위해 기밀성, 인증 메커니즘을 사용하지 않도록 설계되어 있다. 이로 인해 공격자들은 손쉽게 스푸핑 공격이 가능하다. 실제로, 2017년 6월 흑해지역에서는 최소 20척의 선박이 이 GNSS 스푸핑 공격으로 인해, 수동 항법 시스템으로 전환한 사례가 알려지고 있다. 또한, GNSS 시스템은 재밍 공격에도 매우 민감하다. GNSS 주파수에서 노이즈를 방출하여 GNSS의 가용성을 무너뜨릴 수 있다.



<그림1 선박 재밍과 스푸핑 공격의 로직>

기술	기밀성	인증	가용성
GNSS	X	X	X
AIS	X	X	X
SATCOM	X	O	O
CAN-BUS	X	X	O

<표1 선박 통신의 사이버보안 속성>

출처 :arXiv:2003.01991v1, Vessels Cybersecurity: Issues, Challenges, and the Road Ahead, 4 Mar 2020

2. Satellite Communication

위성통신의 보안 수준은 운용사에 따라 달라질 수 있으나, 최근 한 연구결과에 따르면, VSAT 안테나와 게이트웨이 사이의 암호화되지 않은 연결이 발견되었다고 한다. 따라서, 안전하지 않은 서비스(예시, POP3 전자 메일 또는 HTTP 브라우징)를 사용하면 개인정보 유출 문제가 발생할 수 있다. 또한, 잘 알려진 보안취약점인 CVE(Common Vulnerabilities and Exposures)의 리스트를 살펴보면, GMDSS 서비스 중에도 보안 취약점들이 발견되고 있다. 취약점의 근본적인 원인은 SAILOR 6000 통신 제품군 내의 독점 솔루션인 ThraneLINK 프로토콜에서 발견되었다. 특히 인증되지 않은 펌웨어 업데이트 및 악성 소프트웨어를 설치할 수 있는 백도어도 발견되었다. 또한, Mini-C INMARSAT 터미널에서 추가적인 프로토콜 수준 취약점을 알고 있는 공격자는 선박에서 불법 복제 및 테러 시도를 신호로 보내는 선박 보안 경보 시스템(SSAS)을 비활성화 할 수 있다. 도한, VSAT 안테나의 방향을 간단히 수정하여 추가 물리적 공격이 가능하므로 안정적인 위성통신 링크를 거부 할 수도 있다.

보안대책

보안 이슈	보안 대책
GNSS Spoofing	Cross-Technology Location Estimation (GNSS, SATCOM)
Electronic Warfare	Anti-jamming Protocols
Non-Standardized SATCOM Protocols	Standardization Efforts
AIS Spoofing	Software Security Frameworks
Bridge System Assessment	Standardized Security Assessment Procedures
Malware Attacks	Containerization
Automatic Safety Systems	Wireless Sensing and ML
Wired Communication Protocols Security	Physical Security Strategies, Access Control

<표2 선박 무선통신의 주요 보안 이슈와 보안대책>

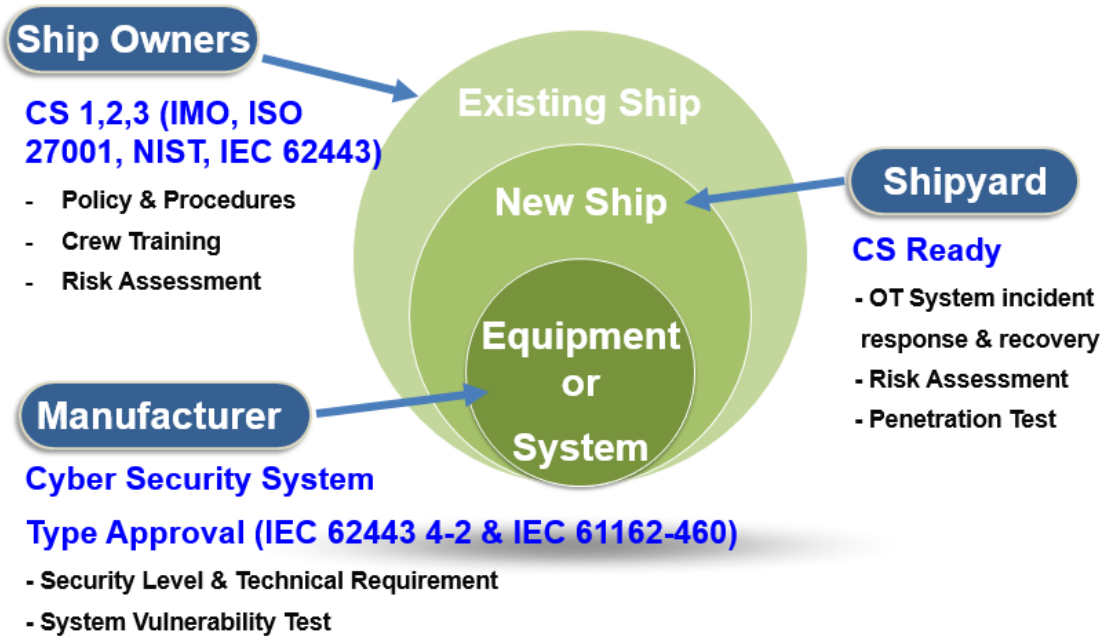
선박에서 무선통신과 관련된 주요 보안 이슈와 이에 따른 보안 대책은 위 표와 같이 요약할 수 있다. 하지만, 이러한 보안 대책은 근본적인 보안대책이기는 어렵지만, 가장 효과적인 방법일 수 있다. 해상무선통신 기술도 점점 더 기술의 발전이 빨라지고 있으므로 새로운 통신기술에는 사이버보안을 고려한 설계가 매우 중요할 것이다.

KR 신조선 사이버보안 부기부호(CS Ready)의 이해

한국선급 사이버보안 인증 체계

한국선급 해상 사이버보안 인증은 사이버보안 관리 시스템을 갖춘 회사 또는 선박에 적용되며, 인증심사(문서검사, 현장검사)를 통과하면 회사/현존선은 적합성 인증서, 신조선은 [CS Ready] 부기부호가 부여된다. 회사/현존선은 사이버보안 성숙도에 따라 3단계 [CS1, CS2, CS3]로 구분되며, 36개 검사 영역, 144개 검사 항목으로 구성되어 있다.

- **CS1, CS2, CS3** : 현존선 운영을 위한 사이버보안 요구사항**(선사 주관)**
- **CS Ready** : 신조선 통합 사이버보안 시스템 구축을 위한 요구사항**(조선소 주관)**
- **CS 형식승인** : 기자재 시스템의 사이버보안 기능에 대한 요구사항**(제조업체 주관)**

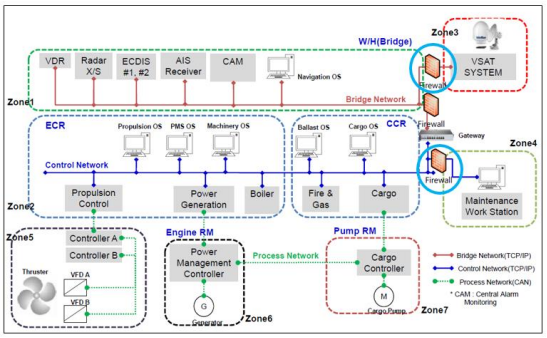


신조선 사이버보안 부기부호[CS Ready]의 필요성

해상 비즈니스 환경의 변화로 인해 고도화된 자동화 · 통합 제어시스템이 선박에 탑재되고 있으며 육상에서 선박 내 시스템 원격 접속 및 제어, 유지보수 등이 가능해짐에 따라 선박 사이버리스크는 점점 더 증가하고 있다. 따라서 사이버사고를 예방하고 대응할 수 있는 통합 시스템을 선박 건조단계에서부터 구축 · 검증하는 것은 해사 안전을 위해 매우 중요하다. 한국선급에서는 사이버보안 시스템을 갖춘 신조선에는 [CS Ready] 부기부호를 부여하고 있으며, 본 뉴스레터를 통해 각 검사 요건에 대해 소개하고자 한다.

[CS Ready] 주요 Activity : 문서검사(선박 네트워크 등)

선박 네트워크 구성도, 자산 목록, 시스템 기능요구사항 명세서, 사고 대응 및 복구 매뉴얼 등에 대한 문서검사를 통해 선박 사이버보안 설계 유효성(Validation)을 검토하는 단계이다. 제출 문서목록 및 상세 사항은 다음 페이지에서 확인할 수 있다.



[선박 네트워크 구성도]

[CS Ready] 주요 Activity : 사이버 리스크평가

사이버 리스크평가는 선박 IT/OT시스템의 사이버 보안 설계 타당성을 검증하는 필수적인 요소이다. 주요 시스템에 대한 사이버 위협과 취약점을 식별하여 가능한 사이버 공격 시나리오 및 사이버 리스크 수준을 확인하고, 리스크를 저감하기 위한 기술적 보안 대책(방화벽, IPS/IDS, VPN, Anti-virus, 통신 · 데이터 암호화 등)을 식별할 수 있다.

[사이버리스크평가 워크샵]

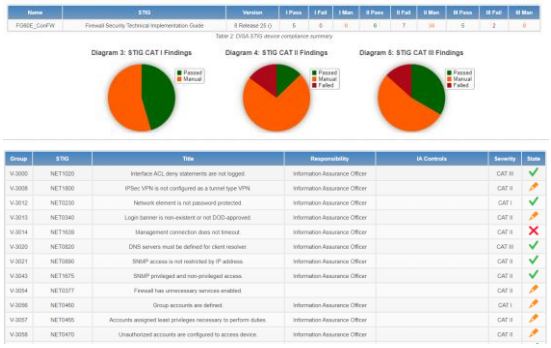
[CS Ready] 주요 Activity : 현장검사 (Factory Acceptance Test & Onboard Test)

선박 사이버보안 시스템의 보안 기능이 적절하게 구현되었는지 현장검사를 통해 확인할 수 있다. 개별 시스템의 사이버보안은 Factory Acceptance Test(FAT)를 통해 검증하며, 육상에서의 선박 원격 접근, 외부 통신 인터페이스 제어 등 통합 시스템의 사이버보안은 Onboard Test를 통해 검증한다.

[사이버보안 FAT]

[CS Ready] 주요 Activity : 취약성 진단 및 침투테스트

문서검사를 통해 확인된 사이버보안 기능을 현장에서 검증하는 방법으로 취약성 진단 혹은 침투테스트를 활용할 수 있다. 다양한 자동화 Tool을 사용하여 PC, 서버, DBMS, 네트워크, 웹 및 애플리케이션, 악성코드, 암호화 통신 방식 등의 보안 취약성을 손쉽게 진단 및 조치할 수 있다.



[네트워크 취약성 진단]

CS Ready 제출 문서 목록[해상 사이버보안 시스템 지침 2장,3절 참조)

CS Ready 부기부호를 받고자하는 신조선은 문서검토를 위해 아래의 자료를 제출하여야 한다.

항목	상세 내용
자산목록	▪ **시스템을 구성하는 모든 장비 List-up** - 운영체제(OS) / 펌웨어, 소프트웨어 및 버전 정보 - 하드웨어 모델 및 버전 - 포트정보 (USB, LAN, WiFi, Serial 등) - 물리적 위치 - VLAN 및 IP / MAC 주소 - Anti-Virus 프로그램
네트워크 구성도	▪ **선박 전체 시스템 아키텍처 도면(논리적, 물리적)** - 자산 및 구역 정의(IEC 62443 3-3 Zone & Conduit 기반) - 경계보호장치(게이트웨이, 라우터, 방화벽, VPN) - 데이터 흐름(단방향, 양방향)
시스템 기능 요구사항 명세서 및 사용자 매뉴얼	▪ **Security Design Philosophy** - 사이버 시스템 / 사이버보안 장비 구성 및 기능 - 보안구성, 기능 및 설정(방화벽, DMZ 등) - 네트워크 장비(스위치 등) 기능 및 설정 - 사이버 사고 탐지 기능(IPS, IDS, SIEM) 등 - 원격・무선연결에 대한 보안 정책 - 통신・데이터 암호화 정책 - 소프트웨어 유지보수 정책 - 사이버 사고 복구 정책 - 패스워드 관리, 악성코드 탐지(백신) 등 ▪ **소프트웨어 기능 설명서 / 사양 / 사용자 매뉴얼** ▪ **타 시스템 간의 인터페이스 방식 / 매커니즘** - I/O List (Control / Monitoring) - 프로토콜 정보
자산 취약성 진단 결과	▪ **기술 취약성 진단결과** - 서버, 보안장비, 네트워크장비, PC, DBMS 등
사이버 리스크평가 보고서	▪ **사이버 위협 목록 문서화** - 스푸핑, 스니핑, 무작위 대입 공격, 기타 등 ▪ **사이버 자산평가(기밀성, 무결성, 가용성)** ▪ **사이버 리스크 수용 기준 문서화** ▪ **사이버 리스크 식별 및 조치계획 관리** - Safeguard 식별 및 조치 - Inherent Risk 및 Residual Risk 식별
소프트웨어 레지스트리 및 품질 계획서	▪ **소프트웨어 품질 관리 계획서** ▪ **소프트웨어 인벤토리 관리 (변경관리 포함)** - 소프트웨어 이름 및 게시자 - 설치 날짜, 버전 번호 - 유지 보수 유형 (로컬 / 원격) - 계정 유형 (일반 / 전용) - 읽기, 쓰기, 실행 권한이 있는 액세스 제어 목록 - IP / 포트 대상 - 라이센스 번호.
사고대응 및 복구 매뉴얼	▪ **사이버 사고대응 및 복구 매뉴얼** - 사이버 사고 목록 - 사이버 사고 감지 표시 및 경보, 영향 - 사이버 사고대응 및 복구 정책 / 순서도 - 자동 및 수동 복구
사이버보안 시험 절차서	▪ **Factory Test Procedure** : 개별 시스템 보안 검증을 위한 테스트 절차 ▪ **Onboard Test Procedure** : 선박 통합 시스템 보안 검증을 위한 테스트 절차

KR 해상 사이버보안 형식승인 가이드라인

사이버보안 형식승인 지침 이해하기

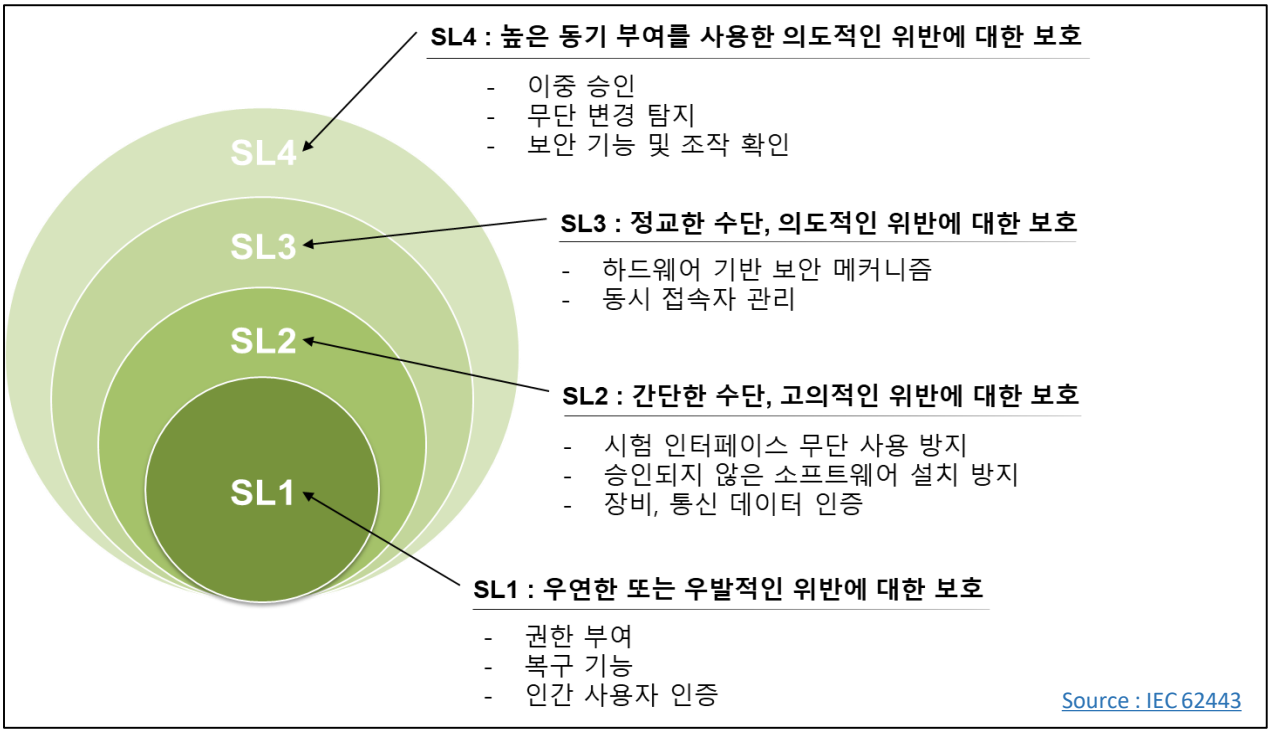
형식승인이란, 선박에 설치하기 전에 제품의 각 형식마다 미리 자료심사 및 승인시험을 하고 만족할 경우 제품이 규정에 적합하다는 것을 제조자에 대해서 증명하는 것을 의미한다. 사이버보안 형식승인은 ISA 62443 4-2, IEC 61162-460과 같은 국제표준을 기반으로 개발되었으며 선박에 탑재되는 원격 접속 장비, 통합 제어 및 모니터링 시스템 등을 포함하는 사이버 시스템의 사이버보안 수준 및 그 수준에 해당하는 요건을 12개의 범주 및 총 124개 항목의 요구 사항에 대한 검증을 통해 보안 기능과 그 수준을 확인한다.

<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

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

보안등급(SL, Security Level)의 이해



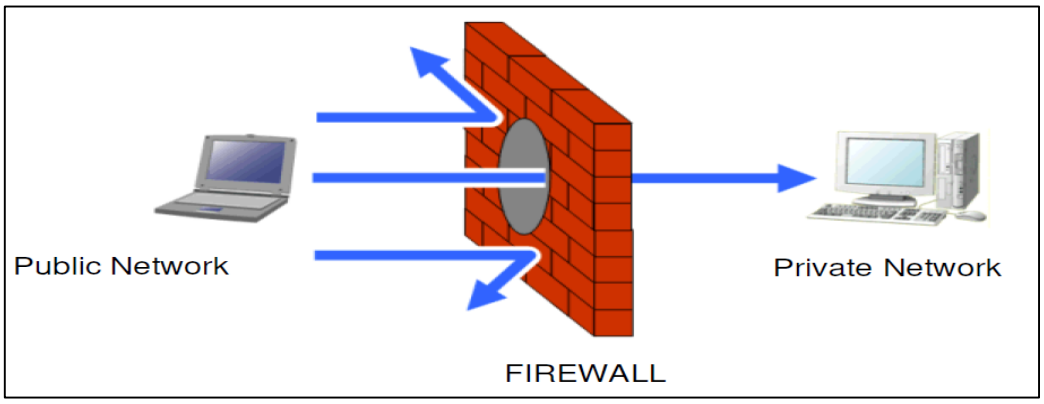
한국선급 해상 사이버보안 형식인증 검사항목

네트워크 장비 요건 - 구역 경계 보호 (1211)

1. 구역 경계의 통신을 모니터링하고 제어하는 기능을 제공하여야 한다. (SL1)
2. 기본적으로 네트워크 트래픽을 거부할 수 있는 기능을 제공하여야 하며 예외로 네트워크 트래픽을 허용하여야 한다. (SL2)
3. 시스템 경계를 통한 통신으로부터 보호할 수 있는 기능을 제공하여야 한다.
4. 작동 실패 시 시스템 경계를 통과하는 통신으로부터 보호할 수 있는 기능을 제공하여야 한다. (SL3,4)

구역 경계 보호를 위한 기능

복잡하게 구성되어 있는 네트워크의 효율적인 보안을 위해 구역(Zone)을 분할하여 각 구역 내부 별로 보안을 유지하고 구역의 경계(Conduit)를 보호하여 전체적인 보안을 유지하는 방법이 사용된다. 이를 위해 구역 및 이에 대한 전달자(Zone & Conduit) 개념을 통해 각 구역을 나누고 경계를 보호하는 기능이 제공되어야 한다.



<방화벽을 이용한 구역 경계 보호>

방화벽을 이용한 구역 경계 보호기능이 대표적인 예시가 될 수 있다. 방화벽의 기본적인 개념은 우리가 살고 있는 집의 문과 같다. 열쇠가 있는 사람(허용된 IP)은 출입이 허용되며, 그 외의 사람(허용되지 않은 IP)은 출입이 불가능하다. 구역 외부의 접근을 사전에 등록된 IP, 프로토콜 등에 대해서만 허용하여 외부로부터의 접근을 최소화 하여 보안을 유지할 수 있으며 허용된 IP(eg. 내부자)로 부터의 공격에 대비하여 추가로 침입탐지 시스템(IDS-Intrusion Detection System) 혹은 침입차단 시스템(IPS-Intrusion Prevention System) 등을 병행하여 더욱 높은 수준의 보안을 유지할 수 있다.

용어 설명

해양통합클러스터 (맥넷)

2015년 11월 맥넷은 해양산업계와 정부, 학계, 연구기관 등이 네트워킹을 통하여 기술과 정보를 공유하고, 상호협력으로 공동 발전하는 생태계를 조성하고자 발족하였다. 그 후 조선·해운·항만·기자재·선급·금융 등 49개 유관기관이 MOU를 체결하여 협의체 형태로 운영되어 왔으며, 2019년 11월 사단법인 해양통합클러스터(맥넷)로 새롭게 출범하였다.

맥넷의 사명은 클러스터의 근본정신인 민간, 정부, 학계 3가지 축의 네트워크를 정교하게 운영함으로써 각 분야 실무자들의 목소리를 잘 아울러 정부 해양산업정책에 반영될 수 있도록 지원하는 것이다.

Source : MacNet

스푸핑 공격

외부 악의적 네트워크 침입자가 임의로 웹사이트를 구성하여 일반 사용자들의 방문을 유도해 인터넷 프로토콜인 TCP/IP의 구조적 결함을 이용하여 사용자의 시스템 권한을 획득한 뒤 정보를 빼가는 해킹 방법이다. 스푸핑 공격의 종류에는 ARP 스푸핑, IP 스푸핑, DNS 스푸핑, 이메일 스푸핑 등이 존재한다.

Source : Naver