KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 020

December 2019

한국선급 활동 #1

현대 LNG 해운과 선박 사이버보안 공동연구 협약 체결

한국선급(KR, 회장 이정기)과 현대LNG해운(주)(HLS, 사장 이규봉)은 2일 현대LNG해운 부산 사무소에서 양사 관계자가 참석한 가운데「선박 사이버보안 규칙 적용, 검증 및 발전을 위한 공동연구」양해각서(MOU)를 체결했다고 밝혔다.

협약으로 양사는 신조 선박에 적용 가능한 사이버보안 솔루션을 공동으로 검증하게 된다. 한국선급이 세계적으로 인정을 받고 있는 '해상 사이버보안 인증 분야'의 역량과 현대LNG해운의 '사이버보안 기술력'이 시너지를 발휘할 것으로 기대된다.

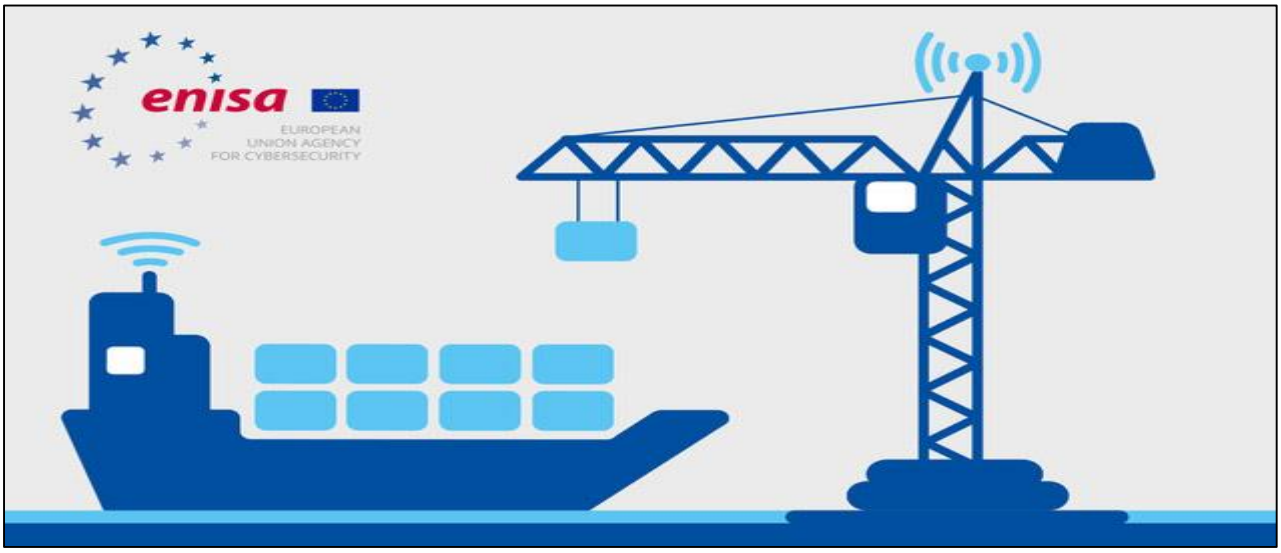
또한 2017년 6월 국제해사기구(IMO)에서 해사안전위원회 98차에서 결의한 '안전관리시스템에서의 사이버리스크관리'에 의해 오는 2021년 사이버보안 리스크 관리가 강화될 것으로 예상됨에 따라 사이버보안 시스템의 리스크 분석 및 설계 안전성 평가 부문에 대해서도 협력해 나갈 예정이다.

한국선급은 지난해 해상사이버보안 관리 시스템 인증 체계를 구축하고, 회사 및 선박에 대한 사이버보안 인증 서비스는 물론 선박의 네트워크 및 자동화 시스템 등에 대해 사이버보안 형식승인 서비스를 제공하고 있다. 현대LNG해운은 국내 최초로 LNG 수송을 시작했으며, 현재 국내 도입 LNG FOB(Free On Board) 물량의 28%를 수송하고 있는 국내 최고의 LNG 전문 선사이다. 25년 이상의 LNG 운반선 운항·관리 경험으로 LNG, 기타액화화물수송, FSRU 등 LNG 연관 사업을 통해 해외시장 진출을 추진, 실행하고 있다.

유럽연합(EU) 항만 사이버보안 가이드라인 발표

유럽연합(EU) 항만 사이버보안 가이드라인 발표

유럽의 사이버보안 대응기구인 ENISA는 최근 항만 사이버보안 가이드라인을 발표하였다. 항만에 랜섬웨어 공격과 같은 사이버보안 사고는 경제적 손실이 상당하고, 항구는 안전, 보안 및 상업적 경쟁력을 보장해야 하기 때문에 항만의 디지털화를 위해 사이버 보안을 최우선 과제로 다루어야 한다고 밝혔다. ENISA의 가이드라인은 항만의 디지털화가 가속화됨에 따라 새로운 사이버 보안 위협을 해결하기 위한 실천을 강조하고 있다. 특히, SMART PORT 개념의 도입은 항만 시스템의 위험노출을 가속화 시키기 때문에 새로운 사이버보안 과제를 불러온다. 항만은 전통적으로 물리적 보안과 안전에 관심을 가지고 있었지만 이제는 글로벌 전략에 사이버 보안을 통합해야 한다고 밝혔다.



ENISA 항만 사이버보안 가이드라인 : Key Point

· 항만 운영에 관련된 모든 이해 관계자는 항만 사이버 보안에 대한 명확한 거버넌스 정의
· 네트워크 분리, 업데이트 관리, 암호 강화, 권한 분리 등과 같은 기술적 사이버 보안 이행
· 항만의 수많은 시스템에서 설계단계에서 사이버 보안 적용
· 항만에서 탐지 및 복구 기능을 이행하여 사이버 공격이 항만운용에 영향을 미치기 전에 신속한 대응체계 마련

출처 : https://www.helpnetsecurity.com/2019/11/27/port-cybersecurity/

영국 해양 서비스 제공업체, 사이버 공격피해

James Fisher & Sons, 사이버 공격으로 인한 피해사례

지난 11월, 영국의 해양 서비스 제공업체인 James Fisher & Sons (JFS)[1] 는 해커로부터 사이버 공격을 받아 영향을 받은 모든 컴퓨터 시스템을 오프라인 상태로 만들었고 공격의 원인과 범위를 파악하기 위한 법의학 수사 및 시스템을 복구하기 위해 외부 사이버보안 전문기관에 의뢰한 것으로 확인되었다. JFS 관계자는 이번 공격이 파일 접근을 차단하는 랜섬웨어 변종이라고 밝혔으며, 이로 인해 회사의 주가가 7% 하락한 것으로 나타났다.

최근 연구에 따르면 해양 부문은 사이버 공격에 매우 취약한 것으로 나타났다. 주로 유조선, 컨테이너 선, 요트 및 유람선의 시스템 운영자는 여전히 Windows XP와 같은 오래된 운영 체제를 사용하고 있다. 따라서 해상 비즈니스에 종사하는 회사는 사이버 공격에 주의를 기울이고 모든 범위의 사이버 위협을 사전에 방지하거나 방지하기 위해 필요한 조치를 취해야 한다.

출처 : https://www.cybersecurity-insiders.com/cyber-attack-on-james-fisher-and-sons/

이미지출처 : https://safety4sea.com/mexican-oil-company-refuses-to-pay-ransom-to-hackers/

1) James Fisher and Sons는 1847 년 설립 된 회사이며 현재 항만청, 신 재생 에너지 서비스, 해양 석유 서비스, 해운 및 해저 설계 및 건설과 같은 기타 기술 사업과 같은 비즈니스를 수행하고 있다.

선박의 사이버 보안 취약점 및 대응방안

선박의 사이버 보안 취약점 6가지

선박 운영자 및 선원은 항해, 통신, 화물, 밸러스트, 안전, 제어 및 기타 목적으로 컴퓨터와 사이버 기술을 사용한다. 보안 감시, 화재 탐지 및 경보와 같은 비상 시스템은 점점 더 사이버 기술에 의존하고 있으며 보안에 취약한 네트워크 설계, 통제되지 않은 액세스, 장비 제조업체 혹은 알 수 없는 원격 접근 등은 선박의 취약점이 될 수 있다. 따라서, 기업은 육상 및 선박에서 식별된 취약성을 신속하고 적절하게 해결하는 것이 필수적이다. 선박에서 예상할 수 있는 사이버 취약점은 다음과 같다.

1. 더 이상 지원되지 않는 운영 체제

2. 오래되거나 누락된 바이러스 백신 소프트웨어 및 맬웨어 방지 프로그램

3. 비효율적인 네트워크 관리, 기본 관리자 계정 또는 암호 사용

4. 선박 컴퓨터 네트워크, 경계 보호 조치 및 네트워크 분할 누락

5. 안전에 중요한 장비 또는 시스템을 항상 육상과 연결

6. 계약자 및 서비스 제공 업체를 포함한 제 3 자에 대한 부적절한 액세스 제어

출처: https://safety4sea.com/cm-6-common-cyber-risks-affecting-maritime-industry/

절차적 통제 및 심층방어 접근 방식

선박의 사이버보안을 강화하기 위해서는 SAFETY4SEA에서 제공하는 아래의 절차적 통제와 더불어, 관리적/기술적 통제가 필요하며 심층방어 접근 방식에 따라 SSP에 따른 선박의 물리적 보안, 네트워크 보호, 침입 탐지, 소프트웨어 화이트리스트, 액세스 및 사용자 제어, 이동식 미디어 및 비밀번호 정책의 사용에 관한 적절한 절차 및 직원의 인식 제고가 필요하다.

절차적 통제	상세 내용
#1 교육 및 인식	▪ 내부 사이버 위협은 상당하며 과소 평가해서는 안되며, 직원이라도 부주의 할 수 있으므로 데이터가 잘못 처리 될 수 있다. ▪ 훈련 및 인식은 선박의 관리 및 운영을 지원하는 선장, 임원, 선원 및 해안 직원을 포함하여 선내 인원에 적합한 수준으로 조정되어야한다.
# 2 업그레이드 및 소프트웨어 유지 관리	▪ 생산자나 소프트웨어 개발자가 더 이상 지원하지 않는 하드웨어나 소프트웨어는 잠재적인 취약점을 해결하기 위한 업데이트가 불가능하다.이러한 이유로 더 이상 지원되지 않는 하드웨어 및 소프트웨어의 사용은 사이버 리스크 평가의 일부로 회사에서 신중하게 평가해야한다. * 참고 : 선박 유형, 인터넷 연결 속도, 해상 시간 등을 고려하여 소프트웨어를 적시에 업데이트하는 절차가 필요함
# 3 안티 바이러스 및 안티 멀웨어 도구 업데이트	▪ 소프트웨어 도구를 이용하여 맬웨어를 감지하고 처리하려면 지속적인 업데이트가 필요하다. 업데이트가 적시에 선박에 배포되고 선박의 모든 관련 컴퓨터가 업데이트 되도록 절차적으로 설정해야한다.
# 5 관리자 권한 사용	▪ 관리자 권한은 시스템 구성 설정 및 모든 데이터에 대한 전체 액세스 권한을 허용하며 해당 권한을 사용하여 시스템에 로그인하는 적절한 교육을 받은 직원에게만 제공해야한다. ▪ 사용자 계정은 더 이상 사용하지 않을 때는 제거해야 하며 일반 사용자 이름을 사용하여 한 사용자에서 다음 사용자에게 전달해서는 안 된다.
# 6 물리적 및 이동식 미디어 컨트롤	▪ 이동식 미디어 장치 사용에 대한 명확한 정책이 필수적이다. 미디어 장치는 일반적으로 제어되지 않는 시스템과 제어되는 시스템간에 정보를 전송하는데 사용되지 않아야한다. 소프트웨어 유지 보수 등의 매체 장치를 사용할 수없는 경우, 이동식 매체에 맬웨어가 있는지 검사해야하는 절차가 있어어야 한다.
# 7 데이터 폐기를 포함한 장비 폐기	▪ 더 이상 사용되지 않는 장비에는 상업적으로 민감한 기밀 데이터가 포함될 수 있다. 이 회사는 사용되지 않는 장비에 있는 데이터 폐기를 제대로하여 중요한 정보를 검색 할 수 없도록 장비를 폐기하는 절차를 가져야한다
# 8 해안 및 비상 계획으로부터 지원 받기	▪ 사이버 공격 시 선박은 기술 지원을 받을 수 있어야 한다. 이 지원 및 관련 절차는 선박에서 이용 가능해야 한다.

[기획시리즈] ⑤

선박의 스마트화를 위한 5G 표준 참조모델

본 기획시리즈는 4차산업혁명과 관련한 핵심 통신인프라인 5G가 해양산업에 미칠 긍정적 파급효과와 이에 따른 사이버 위협에 대해 다뤄보고자 한다. 따라서 본 뉴스레터 2019년 12월호에서는 ***'선박의 스마트화를 위한 5G표준 참조모델'***에 대해 소개한다.

기획시리즈 순서

① 5G란 무엇인가?

② 5G의 네트워크 구조와 네트워크 슬라이싱(Network Slicing) 기술, 그리고 해양산업 변화

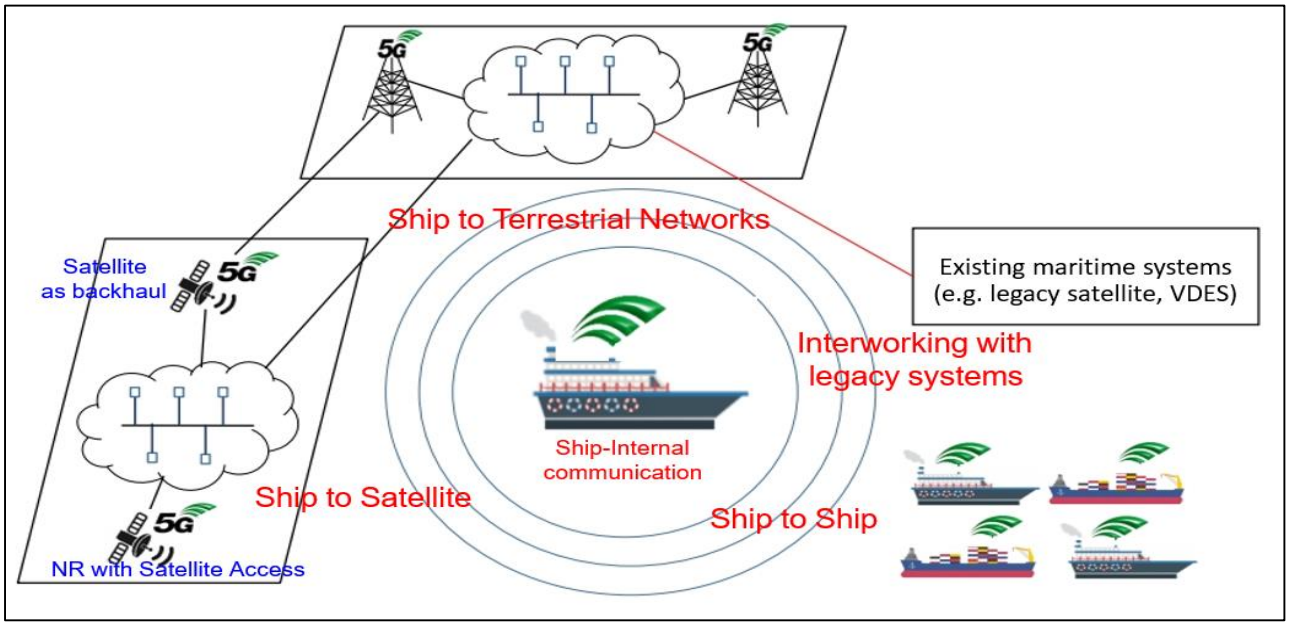
③ LTE의 중앙집중형 네트워크와 5G의 분산형 네트워크의 비교

④ 5G 표준에서 위성의 역할과 해양산업에 미치는 영향

⑤ **선박의 스마트화를 위한 5G 표준 참조모델**

선박의 스마트화를 위한 5G 표준 적용방안

해상의 통신환경은 Reflection, scattering 등으로 인해 육상의 통신환경과 근본적으로 차이가 있다. LTE, 5G와 같은 이동통신 기술도 육상의 통신환경을 기반으로 한 통신기술 이기 때문에 이를 곧바로 해상환경에 적용하기에는 한계가 명확하다. 반면, 해상 사용자는 스마트 항만, 자율운항선박 등 의 해양수산 산업의 디지털화 위해 5G를 선박을 비롯한 해상환경에 적용하기를 원한다. 그렇다면 5G를 해상환경에 맞게 적용하기 위해서는 어떻게 적용해야 하고, 어떤 부분에 대한 추가 연구와 3GPP 표준화 작업이 필요한지에 대해 알아보고자 한다.

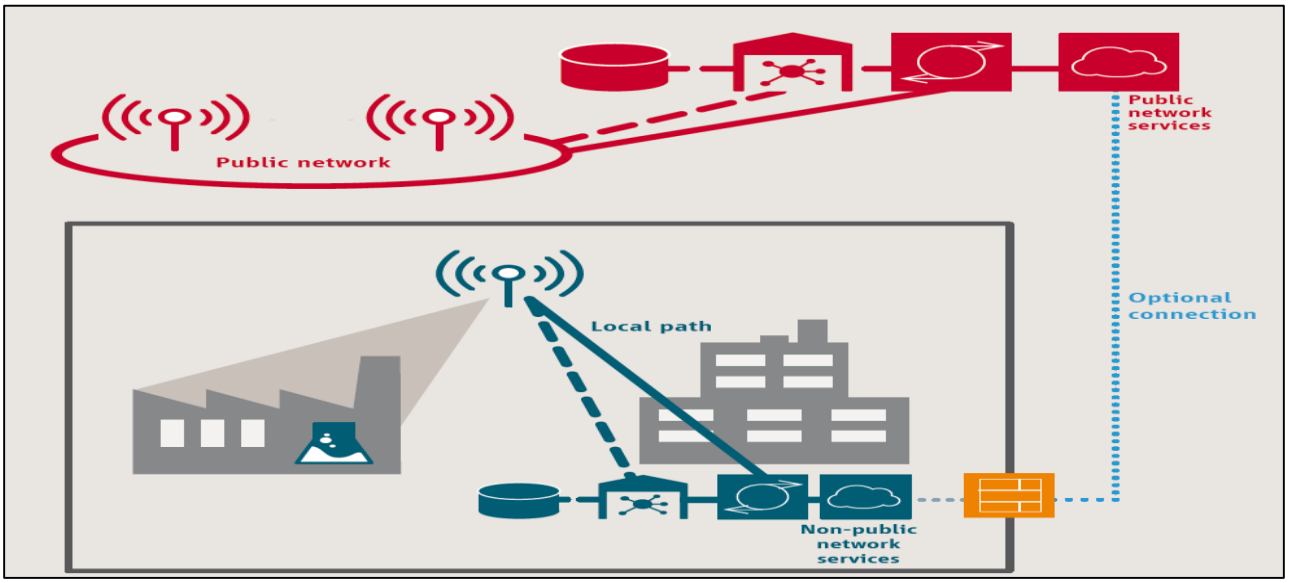


출처 : KR, 싱크테크노, APMC 2019-Update of 5G standardization in 3GPP

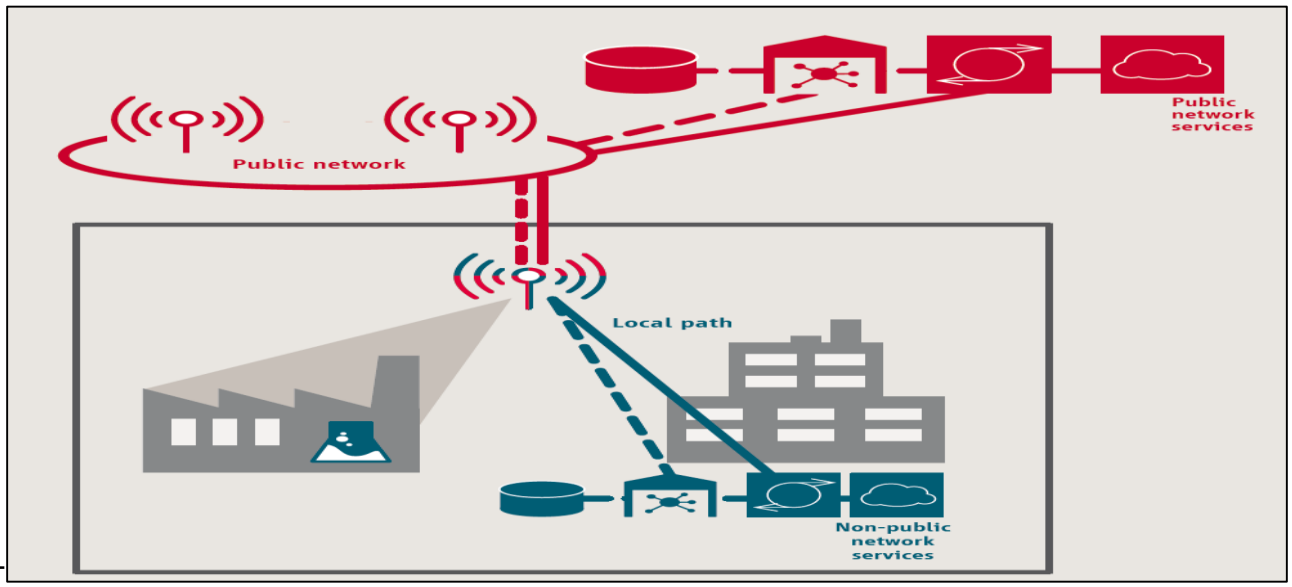
선박 내부 네트워크에 5G Private Network 도입을 위한 참조모델

선박의 스마트화를 위해서는 선박 내부 네트워크는 개선이 필요하다. 특히, 자율운항선박과 같이 선박 내 OT 장비들을 제어하기 위해서는 기존 5G 표준의 스마트공장 분야에서 Private Network 개념을 참조해 볼만 하다. 5G 표준은 Data 교환을 위한 User Plane과 스위치, 라우터 제어하기 위한 Control Plane으로 분리되어 있다. 선박에서 OT 장비들을 제어하기 위해서는 지연속도와 신뢰성, 안정성과 같은 성능이 중요하고, 선내의 상황을 육상에서 CCTV 등으로 모니터링하기 위해서는 통신의 용량과 같은 성능이 중요하다. 따라서, 선박 내에서 각각의 서비스 시나리오에 따라 효율적인 통신성능이 제공되어야 하는데, 이러한 개념이 자율운항선박과 같은 선박의 스마트화를 위한 참조모델이 될 수 있을 것이다.

<외부와 단절된 네트워크에서의 공장 자동화 서비스 시나리오>



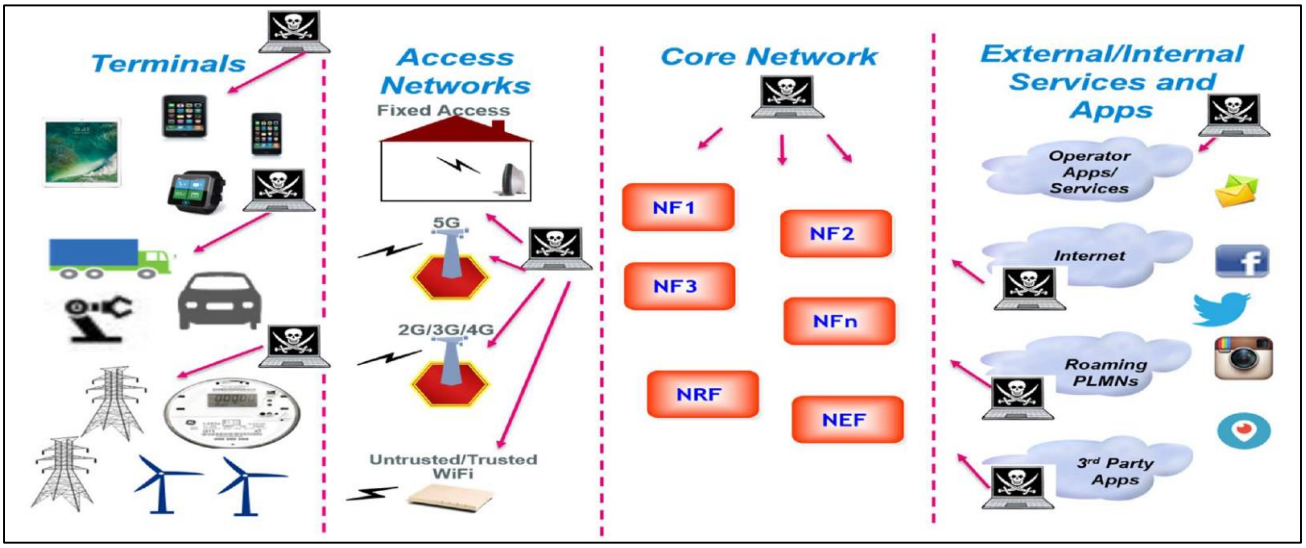
<원격 제어 및 모니터링을 위한 공장 자동화 서비스 시나리오>



출처 : 5G ACIA, 5G Non-Public Networks for Industrial Scenarios

5G 표준의 사이버 위협요소

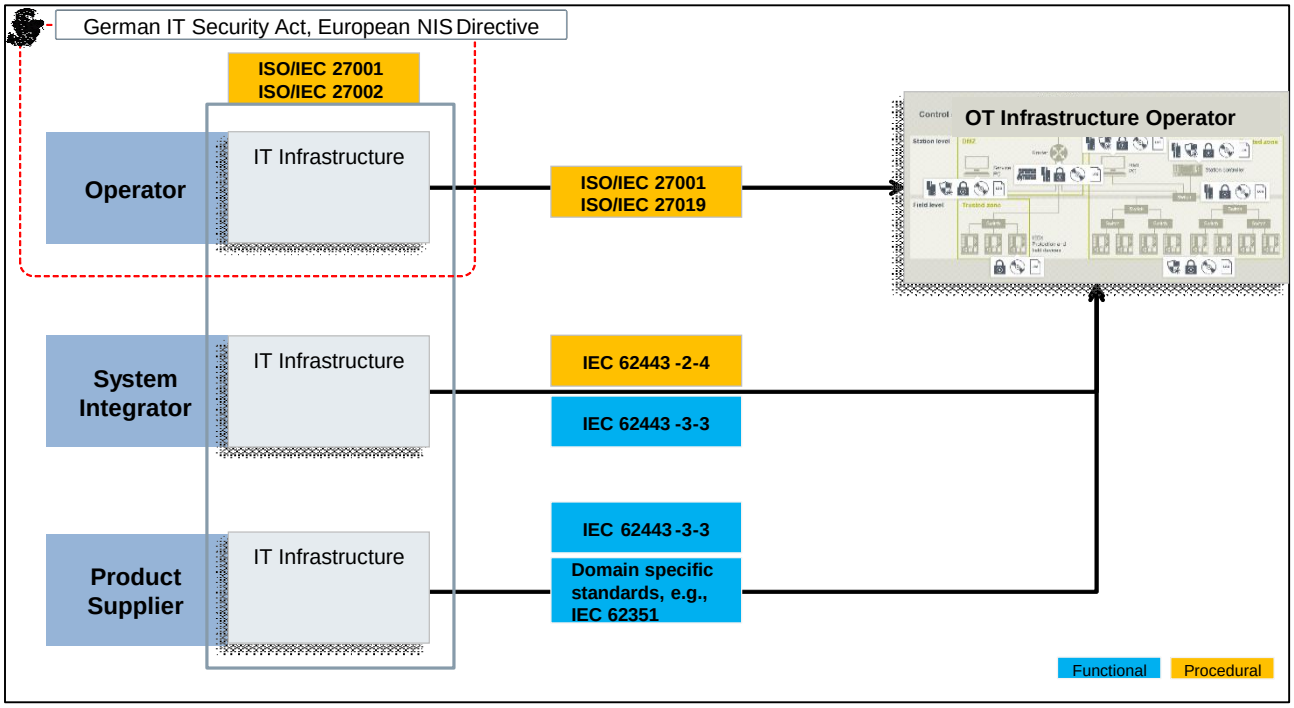
5G 표준은 사이버 위협을 줄이기 위해서는 전체 네트워크의 단말기, 무선망, 유선망, 운영자 호스트 또는 응용 프로그램 및 서비스와 같은 다양한 5G의 요소와 세그먼트들에 대한 리스크 분석을 통해 사이버 위협을 완화시켜 나가고 있다. 아래 그림은 5G 위협에 대한 상위수준의 Landscape를 보여주고 있다.



출처 : The Evolution of Security in 5G, 5G America white paper, July 2019

5G 공장자동화 표준에 적용된 사이버보안 프레임워크

5G의 공장 자동화 관련 표준에는 IEC 62443 표준의 프레임워크를 사용하고 있다. IEC 62443 표준은 OT 시스템에 널리 사용되는 프레임워크이다.



출처 : 3GPP TR 22.804 V.2.0.0(2018-5)

KR 해상 사이버보안 형식승인 가이드라인

사이버보안 형식승인 지침 이해하기

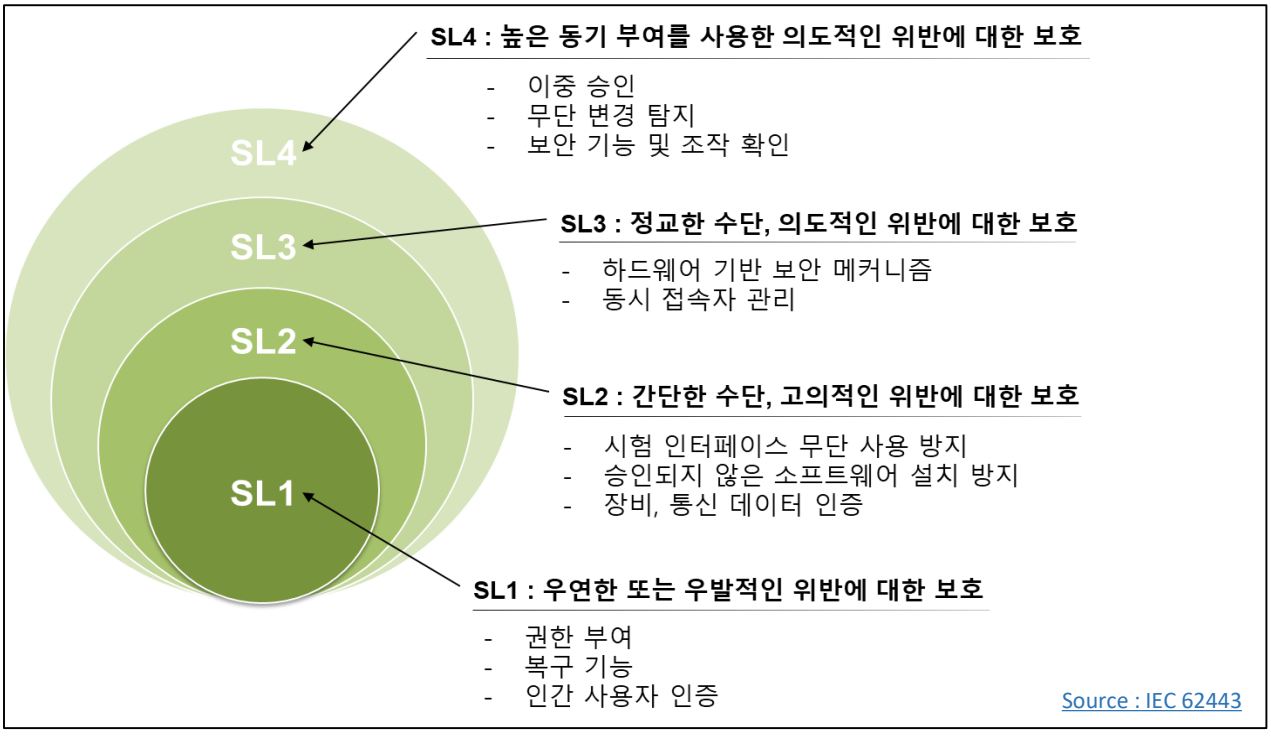
형식승인이란, 선박에 설치하기 전에 제품의 각 형식마다 미리 자료심사 및 승인시험을 하고 만족할 경우 제품이 규정에 적합하다는 것을 제조자에 대해서 증명하는 것을 의미한다. 사이버보안 형식승인은 ISA 62443 4-2, IEC 61162-460과 같은 국제표준을 기반으로 개발되었으며 선박에 탑재되는 원격 접속 장비, 통합 제어 및 모니터링 시스템 등을 포함하는 사이버 시스템의 사이버보안 수준 및 그 수준에 해당하는 요건을 12개의 범주 및 총 124개 항목의 요구 사항에 대한 검증을 통해 보안 기능과 그 수준을 확인한다.

<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



Source : IEC 62443

한국선급 해상 사이버보안 형식인증 검사항목

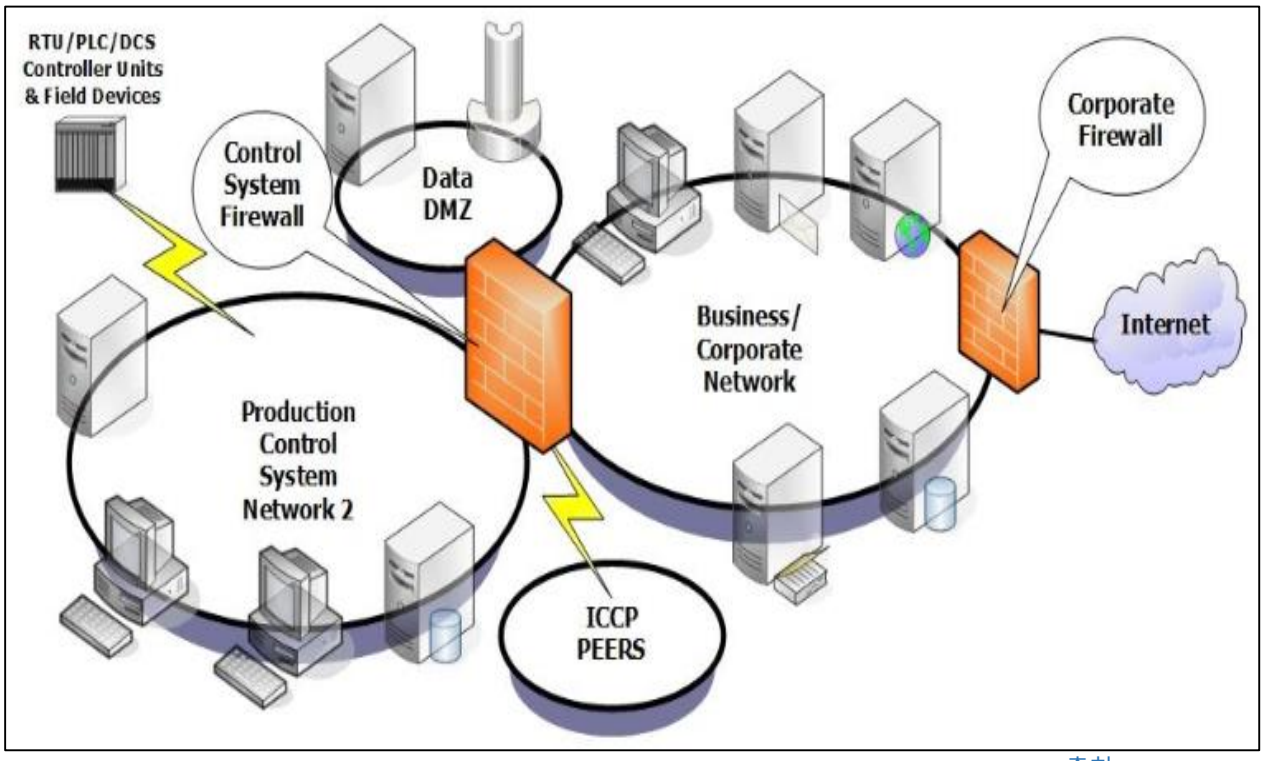
네트워크 분할 (601)

구성품은 논리적 세분화 및 중요도에 기반한 광범위한 네트워크 아키텍처를 지원하기 위해 분할된 네트워크를 지원하여야 한다. (SL1,2,3,4)

네트워크 분할을 위한 가이드라인

선박의 OT 시스템은 IT 시스템과 망분리가 되어야 하며, 이는 물리적 혹은 논리적 방법으로 가능하다. 물리적으로 외부 시스템과 연결되지 않은 독립 시스템(Stand alone system)의 경우 물리적인 망분리가 되어있으므로 네트워크를 통한 외부의 침입으로 부터 안전하다고 볼 수 있다. 하지만 육상으로 부터의 원격 접속을 통한 모니터링, 유지보수 등의 기능이 지원되는 스마트 선박이 점차 늘어 나는 추세이며, 이 경우 논리적인 망분리를 통해 네트워크 분할 기능을 구현할 수 있다. OT 시스템의 내부 망에서도 단일 네트워크로 이루어지지 않고 그 구조에 따라 서브넷을 구성하여야 한다. 서브넷(Subnet)은 말 그대로 네트워크 상에서 하위의 네트워크를 만드는 것이라고 보면 이해하기 쉽다. 물리적으로는 하나의 스위치에 모두 연결되어있는 것으로 보이지만 서브넷 구성을 통해 논리적인 여러 개의 네트워크가 존재하게 되는 것이다. 서브넷 구성에 추가로 방화벽 혹은 스위치의 설정을 통해 접근 통제 정책을 설정하여야 한다. IP 주소 기반의 허용 정책 혹은 통신 포트의 정책 설정을 통해 네트워크 간 데이터의 송수신 여부를 제한하고 보다 안전한 네트워크를 구성할 수 있다.

<제어망과 업무망의 중간지점(DMZ)를 고려한 네트워크 구성예시>



출처 : us-cert.gov

용어 설명

랜섬웨어

랜섬웨어(Ransomeware)는 이용자의 데이터(시스템파일, 문서, 이미지, 동영상 등)을 암호화하고 복구를 위한 금전을 요구하는 악성코드를 말한다. 몸값(Ransom)과 소프트웨어(Software)의 합성어로 시스템을 사용 불가능한 상태로 변경하거나 데이터를 암호화해 사용할 수 없도록 하고 이를 인질로 금전을 요구하는 악성 프로그램 이다.

출처 : https://www.krcert.or.kr/data/guideView.do?bulletin_writing_sequence=27048

유럽연합사이버보안국(ENISA)

유럽연합사이버보안국(European Network and Information Security Agency)은 2004년 EU의 사이버 정보보호를 위해 창설된 기구로서, 각국의 컴퓨터 바이러스와 해킹 실태파악 등을 통해 각국 정보, 기업, 일반인에게 위험성을 알리는 역할을 하고 있다.