KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 032

December 2020

한국선급 활동

- SC Shipmanagement 회사 사이버보안 적합성 인증 획득

사이버 해적, 일주일 만에 두번째 공격을 받은 해운업

KR 신조선 사이버보안 부기부호(CS Ready)의 이해

KR 해상 사이버보안 형식승인 가이드라인

IEC 62443 4-2의 이해

용어 설명

해사 사이버보안 교육 소개

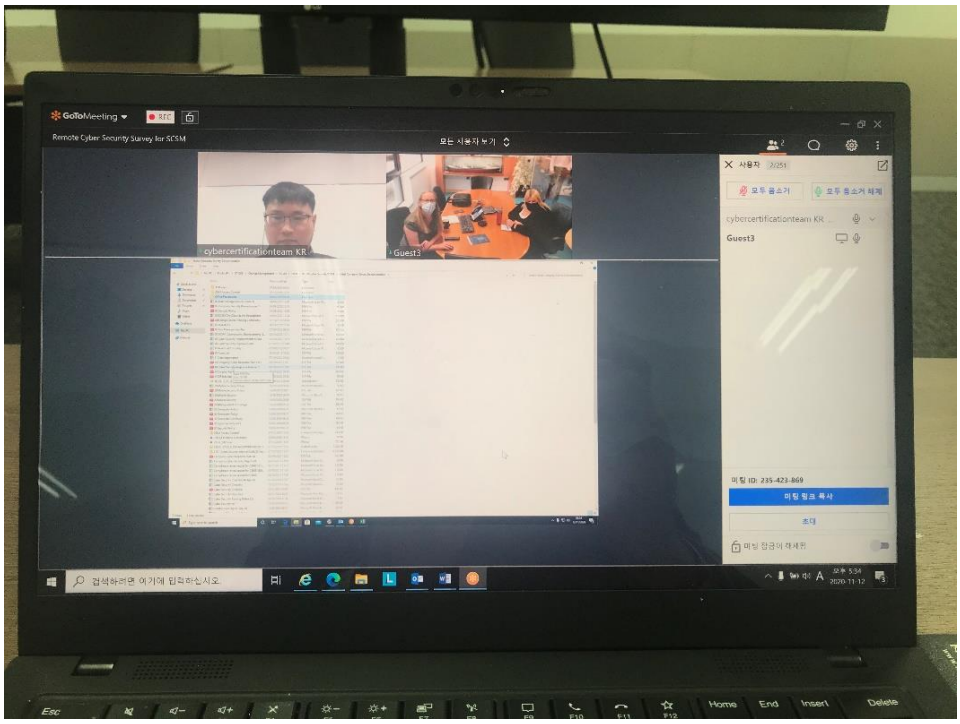
SC Shipmanagement 회사 사이버보안 적합성 인증 획득

한국선급(KR, 회장 이형철)은 영국의 컨테이너선사인 SC Shipmanagement 사의 사이버보안 시스템에 대한 회사 사이버보안 적합성 증서를 발급하였다고 30일 밝혔다.

한국선급은 SC Shipmanagement 사의 본사 내 사이버보안 관리 시스템에 대해 관리적, 기술적, 물리적 측면에서 사이버보안 역량을 검증하였다. 특히 코로나 19로 인하여 사이버보안 검사원의 현장 검사가 어려워짐에 따라 SC Shipmanagement 사에 대한 사이버보안 적합성 인증을 위한 현장 검사를 원격사이버보안 검사로 대체하여 진행하였다.

원격사이버보안 검사는 검사원이 회사나 선박에 직접 입회하여 검사하는 대신 회사나 선박 소유자가 제출한 전자파일 형태(사진, 비디오, 문서 사본 등)의 자료를 검토하고, 필요한 경우 실시간 영상으로 해당 회사 또는 선박과 통신하여 수행하는 검사를 말한다. 코로나19(COVID-19)로 인해 전 세계적으로 비대면 활동이 중요해지고 있는 가운데, 이러한 원격사이버보안 검사는 최첨단 디지털 기술을 검사에 활용하여 효율성을 개선함으로써 전통적인 현장검사 역량을 강화할 것으로 예상된다.

한국선급은 2021년 SC Shipmanagement 사 컨테이너선 5척의 사이버보안 시스템에 대한 문서검토 및 원격사이버보안 검사를 통해 사이버보안 역량을 검증할 계획이다.



사이버 해적, 일주일 만에 두번째 공격을 받은 해운업

IMO의 IT 시스템이 정교한 사이버 공격을 받음.

전 세계 해운업계가 일주일 만에 두 번의 사이버 공격을 받아, 이는 성수기 상품들을 이동시키기 위해 이미 무리하고 있는 공급망 붕괴에 대한 우려를 낳고 있다. 국제해사기구(IMO)는 27일 성명을 통해 “IMO의 IT 시스템에 대한 정교한 사이버 공격을 받았다"고 밝혔다. 현재 다수의 IMO 웹 기반 서비스를 이용할 수 없으며 이 공격이 공용 웹사이트와 내부 시스템에 영향을 미치고 있다고 말했다.

이 공격은 이번 주 초 전세계에서 4 번째로 큰 컨테이너 선사인 CMA CGM SA가 IT 시스템이 손상되었다는 공개 이후 공개되었습니다. 프랑스에 본사를 둔 Marseille는 30일 점차 네트워크에 다시 연결되고 있어 예약 및 문서 처리 시간이 향상되고 있다고 밝혔다. 또한 "우리는 데이터 유출을 의심하고 있으며 그것의 잠재적인 양과 종류를 파악하기 위해 가능한 모든 것을 하고 있다"고 이 회사는 이메일로 보낸 성명서에서 말했다.

최근 몇 년 동안 일련의 사이버 사건들이 해운업계를 괴롭혔는데, 그 중 가장 큰 것은 2017년 코펜하겐에 본사를 둔 A.P. Moller-Maersk A/S에 약 3억 달러의 손실을 입힌 침입이었다. 해운산업에 종사하는 고객들을 가지고 있는 사이버보안 업체인 Pen Test Partners의 보안 전문가인 Ken Munro는 "머스크 사건은 해운업계가 매우 노출되어 있음을 깨달은 사기꾼과 사이버 범죄자들의 관심을 분명히 끌었다"고 말했다. " 육상 시스템이 컨테이너를 예약할 수 없다면, 선박은 적재할 수 없고 수익을 창출할 수 없다. 따라서 선박에 대한 표적형 공격은 랜섬웨어 운영자들에게 이익이 된다.“

최근의 공격이 세계 무역에 잠깐의 자극제가 될 것인지 아니면 더 넓은 피해의 방아쇠가 될 것인지를 말하기는 너무 이르지만Bloomberg Intelligence의 Lee Klaskow와 같은 물류 전문가들은 사이버 위협은 "확실히 단기 역풍과 두통"이라고 말한다. 최근의 사이버 해적 행위들의 시기는 특히 계절적 주기가 회복되는 것을 여전히 기다리고 있는 선박들에게 좋지 않다.

소비자들은 집에서 일하고 온라인에서 필수품을 구입해야 했기 때문에, 이 대유행은 종이 수건과 마스크에서부터 트램폴린과 컴퓨터 모니터에 이르기까지 모든 것에 대한 공급망을 혼란에 빠뜨렸다. Covid-19의 폐쇄로 인한 심각한 침체를 예상하여 초기에 용량을 줄였던 화주 수요는 실제로 줄어들지 않았다. 전자상거래 구매가 강세를 유지하고 있고 회사들이 재고를 재충전하고 있기 때문이다. 이에 따라 태평양을 가로지르는 화물 컨테이너를 옮기는 데 드는 벤치마크 비용이 연초 이후 3배로 늘었다.

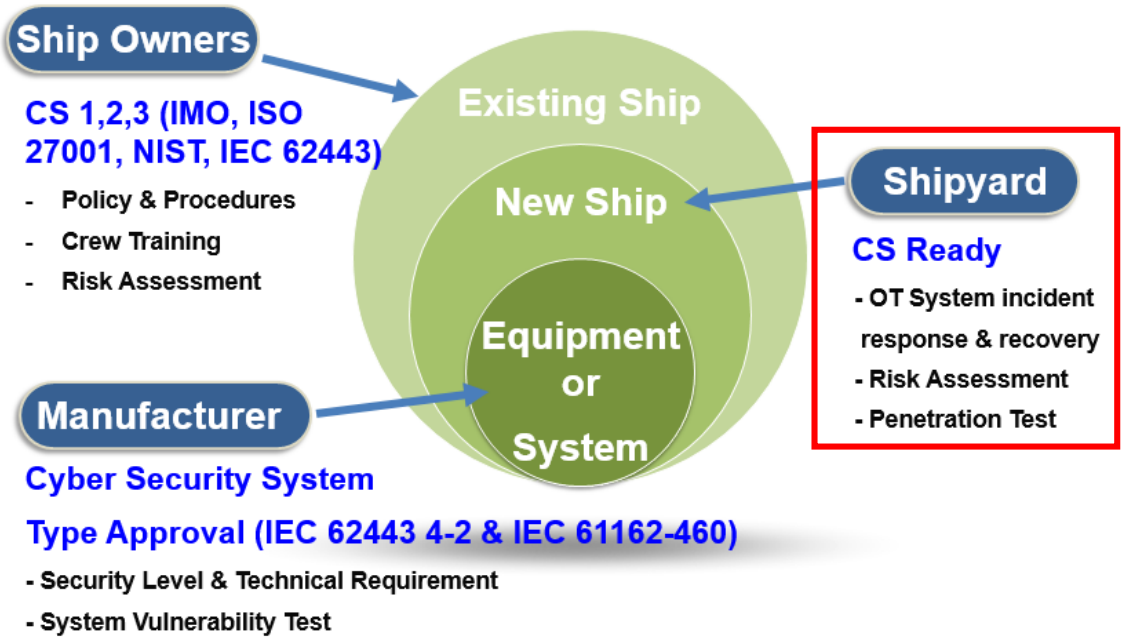
Source : BLOOMBERG, Oct. 2020.

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)**

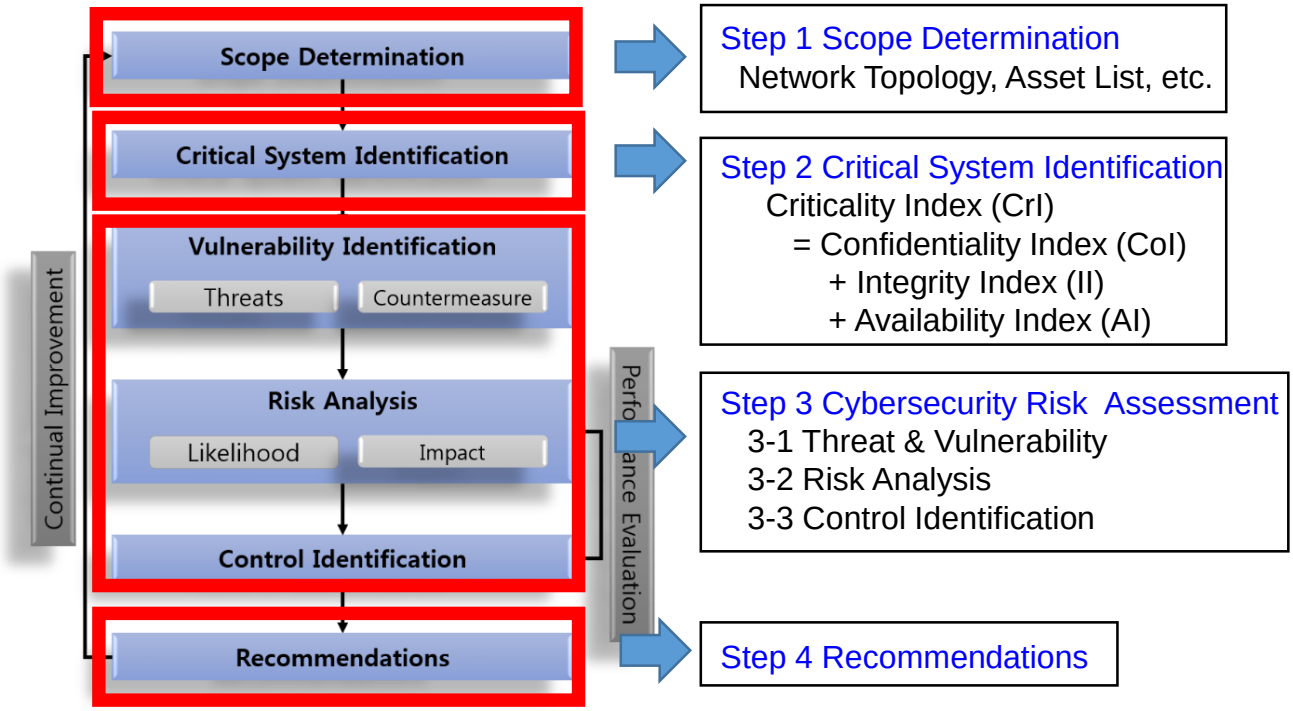


신조선 사이버보안 부기부호[CS Ready]의 필요성

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] 제출문서 이해하기 : #5 사이버 리스크평가 보고서

선박 사이버 리스크평가(Cyber Risk Assessment)는 선박 IT/OT 시스템의 사이버보안 설계 타당성을 검증하는 필수적인 요소이다. 선박 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 및 데이터 암호화 등)을 워크샵을 통해 식별하여 사이버 리스크평가 보고서를 승인 문서로 제출해야 한다. 한국선급은 ISO / IEC 27005, NIST 800-39 기반 4단계로 구성된 독자적인 사이버 리스크평가 프로세스를 지난 5월 신조선에 적용(현대 LNG해운, 현대중공업, 한국조선해양, 현대글로벌서비스, 콩스버그코리아 참여)하였으며 본 뉴스레터에서는 각 상세 단계에 대해서 설명하고자 한다.



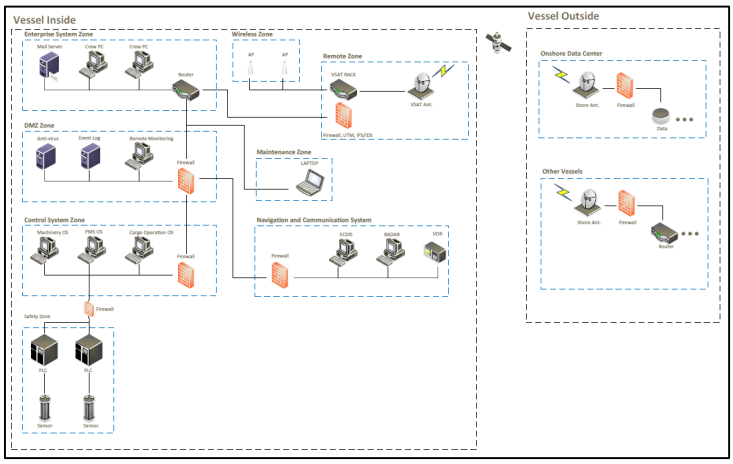
STEP 1 : SCOPE DETERMINITATION

목적 : 필요한 정보를 수집하여 **리스크 평가 목적 및 범위를 명확하게 이해**하는 것
준비사항 : 네트워크 도면, 자산 목록, 리스크 허용 기준, 취약성 진단 결과 등

.

#1 네트워크 도면

- Zone 및 Conduit 표기(IEC 62443)
- 경계보호장치(게이트웨이, 라우터, 방화벽, VPN) 표기
- 대상 시스템 및 장비 표기
  - AMS(Alarm Monitoring System)



#2 자산목록

- 대상 시스템을 구성하는 모든 장비
  - 운영체제(OS) / 펌웨어, 소프트웨어 및 버전 정보
  - 물리적 위치
  - 하드웨어 모델 및 버전
  - VLAN 및 IP / MAC 주소

Zone	Asset	Manufacturer	Software	OS	Port	Location	PIC
Enterprise System	Mail Server	HP	PMS	Windows Server 2016	USB : 3 LAN : 2	Accomm.	2nd officer
	PCs	HP	PMS	Window 10	USB : 3 LAN : 2	Accomm.	2nd officer
	Printers	HP	-	-	USB : 2 LAN : 2	Accomm.	2nd officer
	Router	CISCO	CISCO	-	USB : 1 LAN : 20	Accomm.	2nd officer
DMZ	Firewall	CISCO	CISCO	-	USB : 1 LAN : 20	W/H	2nd officer
	Event Log	Advantech	-	Windows Server 2016	USB : 4 LAN : 2	W/H	2nd officer
	Anti-virus	HP	-	Windows Server 2016	USB : 4 LAN : 2	W/H	2nd officer
Control System	No.1 O/S	HP	KC 600	Windows Embedded	USB : 5 LAN : 3	ECR	1st engineer
	No.2 O/S	HP	KC 600	Windows Embedded	USB : 5 LAN : 3	ECR	1st engineer
	OS Switch	Moxa	Phoenex	-	-	ECR	1st engineer
	Firewall	Fortinet	Forti	-	USB : 1 LAN : 20	ECR	1st engineer
Wireless	A.P.	CISCO	CISCO		USB : 1 LAN : 4	W/H	2nd officer
Remote System	Vsat Rack	Intellian	-	-	USB : 3 LAN : 10	W/H	2nd officer
	Router	CISCO	CISCO	-	USB : 1 LAN : 20	W/H	2nd officer
	Firewall	CISCO	CISCO	-	USB : 1 LAN : 20	W/H	2nd officer
Navigation and Communication System	No.1/2 ECDIS	JRC	-	Windows Embedded	USB : 3 LAN : 4	W/H	2nd officer
	No.1/2 Radar	JRC	-	Windows Embedded	USB : 3 LAN : 4	W/H	2nd officer
	Firewall	Fortinet	Forti	-	USB : 1 LAN : 20	W/H	2nd officer

#3 리스크 허용 기준

- 리스크 매트릭스 산정(3x3 또는 5x5)
- 리스크 산정식 결정
- 리스크 허용기준 산정
  - Intolerable Risk : 15 ~ 25
  - ALARP Risk : 5 ~ 12
  - Negligible Risk : 1 ~ 4

Impact	5	5 Significant	10 Significant	15 Major	20 Major	25 Major
	4	4 Low	8 Significant	12 Significant	16 Major	20 Major
	3	3 Low	6 Significant	9 Significant	12 Significant	15 Major
	2	2 Low	4 Low	6 Significant	8 Significant	10 Significant
	1	1 Low	2 Low	3 Low	4 Low	5 Significant
Index		1	2	3	4	5
		Probability				

Ref. : IEC 62443, ISO 2705 : 2011, API STD 780

STEP 2 : CRITICAL SYSTEM IDENTIFICATION

목적 : 자산(결과) 평가를 통해 **주요 시스템 식별**
준비사항 : CIA(기밀성, 무결성, 가용성)를 통한 자산평가

.

● **자산평가를 통한 Criticality Index 산정**

No.	Category	Assets	Model	Software / Application	Manufacturer	Interlocking or Related Equipment	Location	Redundancy / Substitute	Value			Criticality Index
									C	I	A	
1	SNS	VSAT network switch	-				Bridge		4	3	4	4
2	SNS	Wireless AP (Wireless access point)	-				Bridge		2	2	2	2
9	SNS	ECR PC	-	Windows 8.1	LG		ECR		3	3	3	3
10	SNS	Ship's Office PC	-	Windows 8.1	LG		Ship's Office		3	3	3	3
11	SNS	C/E ENG. Day Room PC	-	Windows 10	Samsung		C/E Day Room		3	3	3	3
12	SNS	Cap't Day Room PC	-	Windows 10	Samsung		Cap't Day Room		3	3	3	3
13	SNS	Server	R740	Windows Server 2012	Dell		ECR		2	2	2	2

Criticality Index : CrI = CoI + II+ AI

Three(3) factors are considered : **Confidentiality (C), Integrity (I), Availability (A)**

Sum of Asset Criticality Value	Category	(CrI)
13 ≤ Asset Criticality ≤ 15	Definite	5
10 ≤ Asset Criticality ≤ 12	Probable	4
7 ≤ Asset Criticality ≤ 9	Occasional	3
5 ≤ Asset Criticality ≤ 6	Remote	2
3 ≤ Asset Criticality ≤ 4	Improbable	1

● **기밀성(Confidentiality) 평가 기준**

기밀성은 인가된 사용자만 자산에 접근할 수 있도록 하는 것으로써 비인가자의 자산 사용 및 정보에의 접근으로 인한 비즈니스 피해 영향도를 고려하여 등급을 구분

Confidentiality Index	Descriptor	Definition
5	Critical	Unauthorized disclosure could result in significant risk to human, asset, environment Critical financial loss, Very long-term business interruption/expense, Possibility of fatalities
4	Significant	Significant financial loss, Long-term business interruption/expense, Permanent physical injuries
3	Moderate	Unauthorized disclosure could result in moderate risk to human, asset, environment Moderate financial loss, Medium-term business interruption/expense, Short-term injury
2	Minor	Minor financial loss, Short-term business interruption/expense, First-aid case injury
1	Negligible	Unauthorized disclosure could not pose a risk to human, asset, environment Negligible financial loss, Very short-term business interruption/expense

STEP 2 : CRITICAL SYSTEM IDENTIFICATION

목적 : 자산(결과) 평가를 통해 **주요 시스템 식별**
준비사항 : CIA(기밀성, 무결성, 가용성)를 통한 자산평가

.

● 무결성(Integrity) 평가 기준

무결성은 인가되지 않은 자에 의한 위·변조를 방지하는 것으로써 자산 혹은 정보의 정확성/신뢰성이 손실되었을 경우의 비즈니스 피해 영향도를 고려하여 등급을 구분

Integrity Index	Descriptor	Definition
5	Critical	Unauthorized modification could result in significant risk to human, asset, environment Critical financial loss, Very long-term business interruption/expense, Possibility of fatalities
4	Significant	Significant financial loss, Long-term business interruption/expense, Permanent physical injuries
3	Moderate	Unauthorized modification could result in moderate risk to human, asset, environment Moderate financial loss, Medium-term business interruption/expense, Short-term injury
2	Minor	Minor financial loss, Short-term business interruption/expense, First-aid case injury
1	Negligible	Unauthorized modification could not pose a risk to human, asset, environment Negligible financial loss, Very short-term business interruption/expense

● 가용성(Availability) 평가 기준

가용성은 적시에 자산 혹은 정보에 접근 및 사용이 보장되는 성질로써 필요시 해당 자산의 사용 혹은 정보에의 접근이 어려운 경우의 비즈니스 피해 영향도를 고려하여 등급을 구분

Availability Index	Descriptor	Definition
5	Critical	Unavailability could result in significant risk to human, asset, environment Critical financial loss, Very long-term business interruption/expense, Possibility of fatalities
4	Significant	Significant financial loss, Long-term business interruption/expense, Permanent physical injuries
3	Moderate	Unavailability could result in moderate risk to human, asset, environment Moderate financial loss, Medium-term business interruption/expense, Short-term injury
2	Minor	Minor financial loss, Short-term business interruption/expense, First-aid case injury
1	Negligible	Unavailability could not pose a risk to human, asset, environment Negligible financial loss, Very short-term business interruption/expense

STEP 3 : CYBER SECURITY RISK ASSESSMENT

목적 : **워크샵**을 통해 주요 시스템에 대한 **위협을 식별**, **사이버 공격 시나리오 식별 및 리스크 분석**, 리스크를 줄이기 위한 **개선사항 도출**

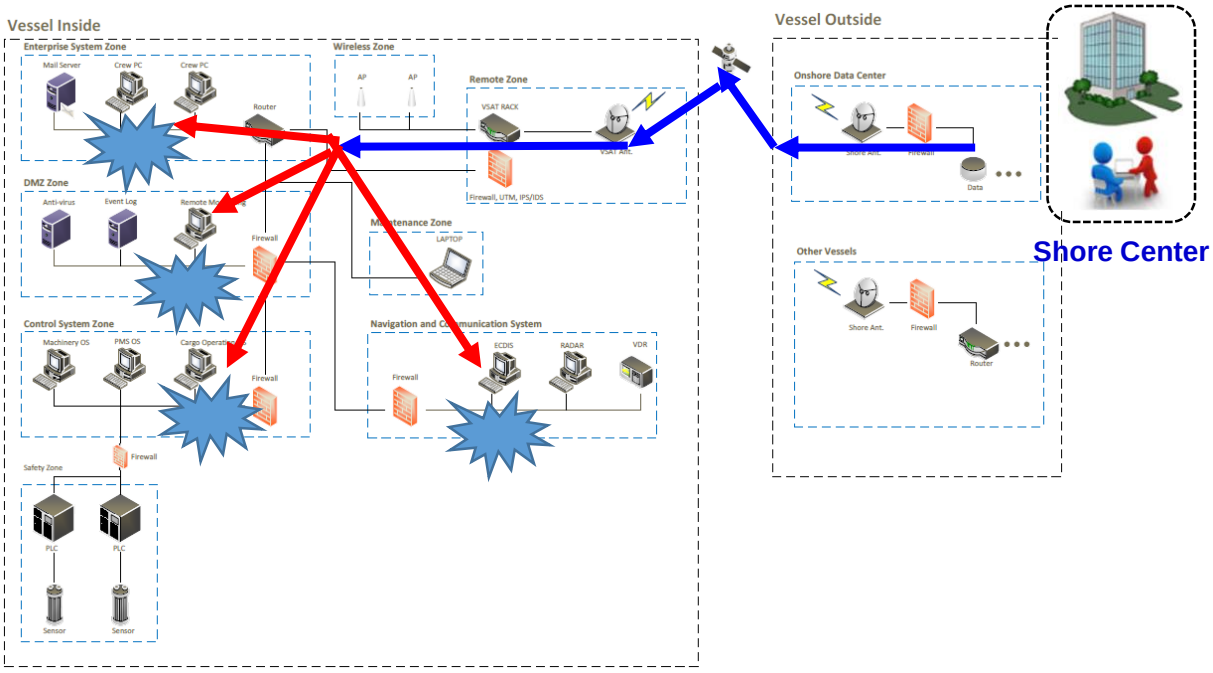
● (3-1) OT 시스템 위협 식별

No. (old No.)	Top 10 2016	Top 10 2014
1 (3)	Social Engineering and Phishing†	Malware Infection via Internet and Intranet
2 (2)	Infiltration of Malware via Removable Media and External Hardware	Infiltration of Malware via Removable Media and External Hardware
3 (1)	Malware Infection via Internet and Intranet	Social Engineering
4 (5)	Intrusion via Remote Access	Human Error and Sabotage
5 (4)	Human Error and Sabotage	Intrusion via Remote Access
6 (6)	Control Components Connected to the Internet	Control Components Connected to the Internet
7 (7)	Technical Malfunctions and Force Majeure	Technical Malfunctions and Force Majeure
8 (9)	Compromising of Extranet and Cloud Components	Compromising of Smartphones in the Production Environment
9 (10)	(D)DoS Attacks	Compromising of Extranet and Cloud Components
10 (8)	Compromising of Smartphones in the Production Environment	(D)DoS Attacks

Ref. : BSI Industrial Control System Security – Top 10 Threats and Countermeasures 2016

● (3-1) 사이버 공격 시나리오 식별

Threat	Cause	Agent	Consequence
Malware	Remote update and maintenance	External	System malfunction / network infection



STEP 3 : CYBER SECURITY RISK ASSESSMENT

목적 : **워크샵**을 통해 주요 시스템에 대한 **위협을 식별**, **사이버 공격 시나리오 식별 및 리스크 분석**, 리스크를 줄이기 위한 **개선사항 도출**

● (3-2) 리스크 분석

- 각 사이버공격 시나리오의 **리스크(Risk Index)**를 분석함
- **리스크(Risk Index)**는 Probability Factor인 **Threat Index(TI)**, **Vulnerability Index(VI)**와 Step 2**의 Criticality Index(CrI)**를 고려하여 산정됨

- **Threat Index (TI)** : probability that an attack occurs to the asset
- **Vulnerability Index (VI) :** probability that the attack succeeds when the cyber-attack occurs

Impact	5	5 Significant	10 Significant	15 Major	20 Major	25 Major
	4	4 Low	8 Significant	12 Significant	16 Major	20 Major
	3	3 Low	6 Significant	9 Significant	12 Significant	15 Major
	2	2 Low	4 Low	6 Significant	8 Significant	10 Significant
	1	1 Low	2 Low	3 Low	4 Low	5 Significant
Index		1	2	3	4	5
		Probability				

Cyber Security Risk Index(RI) = Threat Index(TI) x Vulnerability Index(VI) x Criticality Index(CrI)

● (3-3) 개선사항 도출

Asset	Threats	Threat Agents / Motivation	* Potential Cause (Hazards)	Potential Consequenc	Existing Controls	VI	TI	CrI	RI	Proposed Controls (Responsibility)	Res Risk VI	Res Risk TI	Res Risk CrI	Res Risk RI
No.1 & 2 ECDIS	Careless use of external storage media	Crew, external party / accidental or intentional	* Malicious use of USB * External storage device	Asset damage, loss of functionality, data deletion, virus, collision, grounding	1) USB scanning 2) Anti virus vaccine for ships PCs	4	4	4	16	1) Strenthen USB policy (USB scanning polity) 2) Cyber security Training for existing and new crew 3) Dedicated USB only for ECDIS update	2	4	4	8
	Computer virus	Crew, third party / accidental or intentional	* Chart update with infected external storage media	Asset damage, loss of functionality, data deletion, virus, collision, grounding	1) Anti virus vaccine for ships PCs 2) Recovery plan (backup disk) 3) Redundancy (two marine ECDIS systems) 4) Paper chart (emergency folio only) 5) Service technicians available world wide	4	4	4	16	Recommendation 1) Restricted use of USB drive 2) Use of encrypted USB drive) ECDIS update with CD provided by ender (use portable CD-rom drive)	2	4	4	8

Existing Control만 적용할 경우 RI는 16, Proposed Control까지 적용할 경우 RI는 8로 감소

STEP 4 : RECOMMENDATION

목적 : 조치를 위해 **사이버보안 리스크평가 결과**(사이버보안 리스크 수준, 리스크 감소를 위한 개선조치, 책임자)를 **문서화**

- **Cyber Risk Control Log 문서화**
  - 목적 : 리스크 관리
  - 범위 : ALARP & Intolerable Risk
  - 포함 사항 : Cause / Consequence / Existing Safeguards / Action / Due Date / Responsible Party 등

CYBER RISK CONTROL LOG — Sheet No. (1) of (20)

PROJECT	XXX Cyber Security Risk Assessment
TASK	Cyber security Risk Assessment (XXX)
DOCUMENT	CS Risk Assessment Report (XXX)
TARGET YSTEM	Cyber Assets of XXX

Scenario ID	Asset	Threats	Risk Index	Risk Level
S1-NCS-1d	ECDIS	Careless use of external media	27	Intolerable
S1-NCS-1e	ECDIS	Computer virus	27	Intolerable
S1-NCS-4a	Radar system (ARPA)	Computer virus	27	Intolerable
Cause	Duty officer's error (connecting USB that infected with malware, etc.), ECDIS (chart) update using the affected external storage device, Virus infection via USB (when chart update files are received by E-mail), ARPA is failed caused by virus infected ECDIS			
Potential Consequence	Malicious code infection, ECDIS cannot be used, ARPA radar cannot be used			
Existing Safeguards	ECDIS update using the CD (read only storage device) supplied by ECDIS Maker/Manufacturer Scan virus before using the USB for ECDIS chart update			

[√] Course of Action (Compulsory):
A. Strengthen security policy (related to the use of external storage media, etc.)
B. Strengthen security education policy

[√] Recommendation (Advisory) or Remarks:
C. When update software, check the compatibility of the system and security issues
D. Use secure USB drives

Written by: Workshop facilitator Date: 21/12/2017 (dd/mm/yyyy)

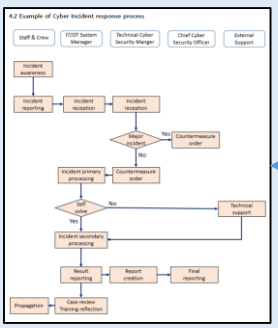
Response:

Control ID	Remarks	Will be applied within		
S1-NCS-1d-A, B		3 month	6 month	1 year
S1-NCS-1e-A, B		3 month	6 month	1 year
S1-NCS-4a-A, B		3 month	6 month	1 year
		3 month	6 month	1 year

Written by: Signed: Date: (dd/mm/yyyy)
Close out:
Written by: Signed: Date: (dd/mm/yyyy)

Awareness Training

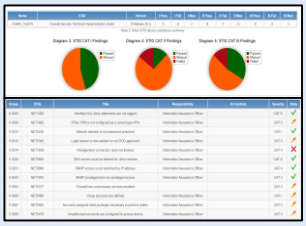
Malware Protection System



Incident Response Procedures

Cyber Risk Mitigation

USB Blocker



Vulnerability Scanning

Penetration Testing

KR 해상 사이버보안 형식승인 가이드라인

사이버보안 형식승인 지침 이해하기

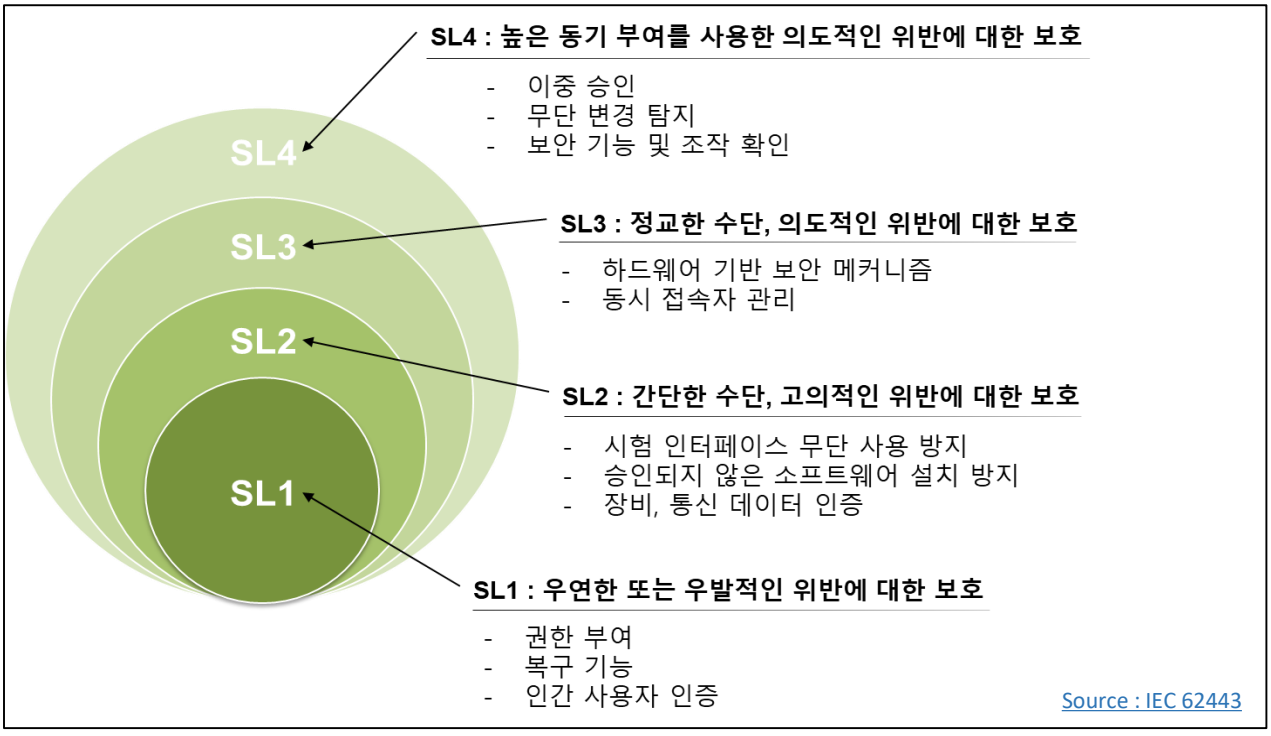
형식승인이란, 선박에 설치하기 전에 제품의 각 형식마다 미리 자료심사 및 승인시험을 하고 만족할 경우 제품이 규정에 적합하다는 것을 제조자에 대해서 증명하는 것을 의미한다. 사이버보안 형식승인은 ISA 62443 4-2, IEC 61162-460과 같은 국제표준을 기반으로 개발되었으며 선박에 탑재되는 원격 접속 장비, 통합 제어 및 모니터링 시스템 등을 포함하는 사이버 시스템의 사이버보안 수준 및 그 수준에 해당하는 요건을 12개의 범주 및 총 124개 항목의 요구 사항에 대한 검증을 통해 보안 기능과 그 수준을 확인한다.

<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

비밀번호 기반 인증 강화 (206)

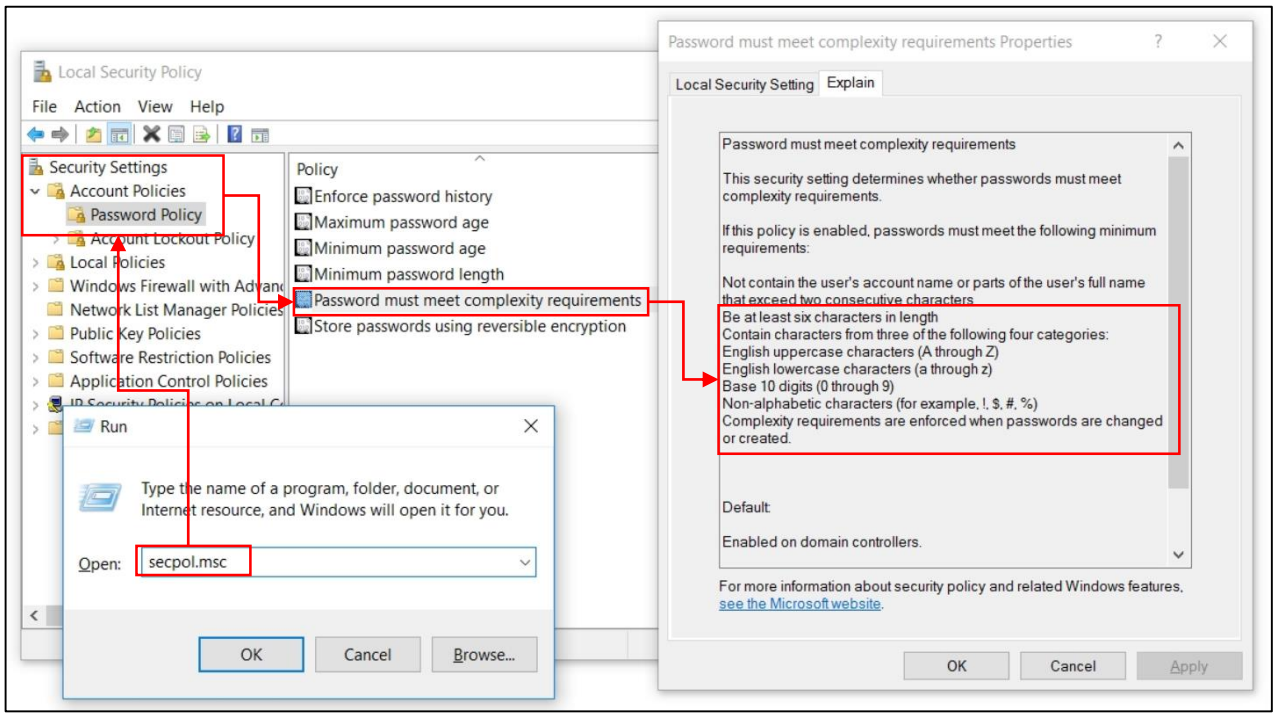
1. 비밀번호 기반 인증을 사용하는 구성품의 경우, 이러한 구성품은 최소 길이 및 다양한 문자 유형을 기반으로 구성 가능한 비밀번호 강도를 적용할 수 있는 기능을 제공하거나, 이 기능을 제공하는 시스템에 통합되어야 한다. (SL 1,2)
2. 구성품은 모든 사용자들에게 암호의 최소 및 최대 수명 제한을 적용할 수 있는 기능을 제공하거나 기능을 제공하는 시스템으로 통합되어야 한다. (SL 1,2)
3. 구성품은 구성 가능한 수의 암호를 재사용하는 것으로부터 인간 사용자 계정을 보호하는 기능을 제공하거나 기능을 제공하는 시스템으로 통합되어야 한다. (SL 3)
4. 구성품은 사용자에게 만료 전 구성 가능한 시간에 비밀번호를 변경하도록 요청하는 기능을 제공하여야 한다. (SL 4)

비밀번호 방식의 인증자 사용

인증자는 개체의 신원을 확인하는데 사용되는 수단을 의미한다(source : IEC 62443 4-2). 인증자는 비밀번호, 토큰, OTP 등 다양한 종류가 존재하며 이번 호에는 가장 대표적인 인증자의 하나인 비밀번호에 대한 보안 요구사항을 살펴보도록 하겠다.

<비밀번호 복잡성 설정 기능의 예시>

비밀번호 복잡성(Password Complexity)은 비밀번호 생성 혹은 변경 시에 숫자, 문자, 특수 문자 등의 조합을 사용하도록 강제하는 기능으로 SL1 혹은 SL2를 만족하기 위해서는 이러한 기능이 제공되어야 한다.



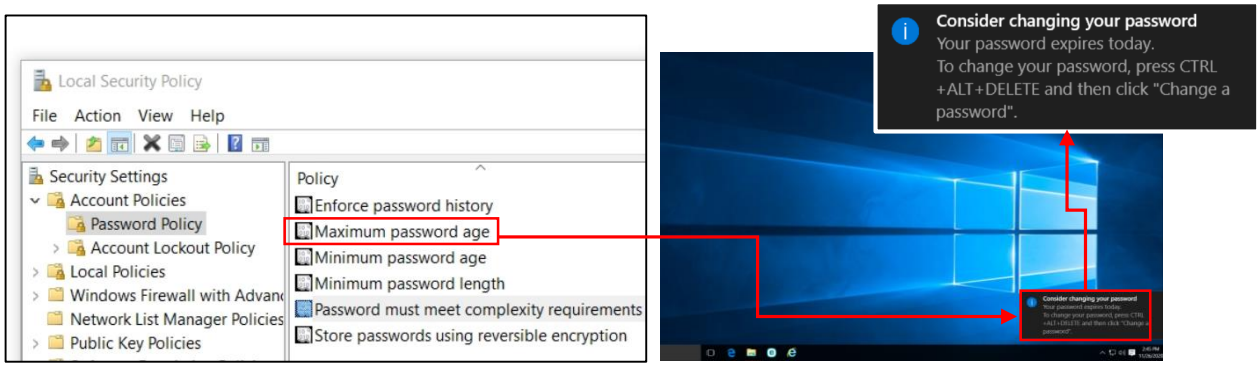
<윈도우 OS에서 제공하는 비밀번호 복잡성 기능의 예시>

윈도우 OS에서 제공하는 비밀번호 복잡성 설정 기능은 다음과 같다.

비밀번호의 길이는 최소 6자 이상이되 다음의 범주 4가지 중 3가지를 포함하여야 함

- 영문 대문자 사용, 영문 소문자 사용, 숫자 사용, 특수 문자 사용

비밀번호 최대 수명 및 최소 수명 제한 기능 또한 제공되어야 한다. 최대 수명은 비밀번호를 설정한 후 사용 가능한 날짜를 의미 하며 해당 기간이 지난 후에는 비밀번호 변경 후 사용이 가능하다. 최소 수명은 비밀번호 변경 후 다시 이전의 비밀번호로 변경하여 결과적으로 비밀번호 변경이 이루어 지지 않는 상황을 막기 위한 것으로 유사한 기능으로는 이전에 사용되었던 비밀번호를 기억하는 기능 등이 있다. 마지막으로 SL4를 만족하기 위해서는 비밀번호 만료 전 알림 기능이 제공되어야 한다.



<비밀번호 만료전 알림 기능의 예시>

IEC 62443 4-2의 이해

IEC 62443 이해하기

한국선급은 사이버보안 서비스를 위해 ISO 27001, IEC 62443 3-3 & 4-2, IEC 61162-460을 채택/적용하고 있다. 특히, IEC 62443 4-2는 사이버보안의 기술적 요건으로 사이버보안 형식승인 서비스에서 대다수가 적용되고 있다. 이에 폭넓은 이해 증진을 위해 IEC 62443의 개념 그리고 IEC 62443 4-2의 요건에 대해 기고하고자 한다.

장치 분류 (Device categories)

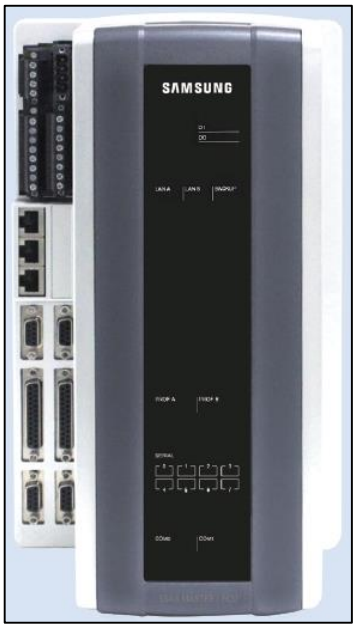
IEC 62443 4-2는 시스템을 구성하는 장치들을 총 4가지로 구분한다.

Device Category	Definition
소프트웨어 애플리케이션	▪ 제어시스템 자체나 프로세스와 인터페이스 하는데 사용되는 하나 이상의 소프트웨어 프로그램과 부속 프로그램
임베디드 장치	▪ 산업 공정을 직접 감시하거나 제어하도록 설계된 특수 목적 장치
호스트 장치	▪ 하나 이상의 공급 업체로부터 하나 이상의 소프트웨어 애플리케이션, 데이터 저장소 또는 기능을 호스팅할 수 있는 운영 체제를 실행하는 범용 장치
네트워크 장치	▪ 장치 간의 데이터 흐름을 가능하게 하거나 데이터 흐름을 제한하지만, 제어 공정과 직접 상호작용하지 않는 장치

<IEC 62443 4-2의 장치 분류> (Source : IEC 62443-4-2)

단말 장치인 노드와 네트워크 장치로 구분하고 네트워크 장치의 역할에 따라 스위치, 포워더 그리고 게이트웨이로 구분하는 IEC 61162-460과는 달리, IEC 62443 4-2에서는 단말기를 임베디드 장치와 호스트 장치로 구분하고 이에 활용되는 소프트웨어 어플리케이션을 별도로 구분한다. 요구 사항 중 각 장치 별로 그 적용 방식이 달라야 하는 경우에는 해당 요건을 별도로 명시하고 각 장치 별로 요구사항을 명시하였다. 각 요구 사항은 SAR(Software application requirement), EDR(Embedded device requirement), HDR(Host device requirement), NDR(Network device requirement)로 그룹화 되어있다. 예를 들어 악성코드에 대한 요구 사항인 CR 3.2의 경우 SAR 3.2, EDR 3.2, HDR 3.2, NDR 3.2로 구분하여 각각 다른 요구 사항을 제시한다. 악성코드 보호를 위한 가장 가까운 예시로는 악성코드 보호 프로그램을 구매하여 설치하는 것이다. 악성코드 보호 프로그램은 일반적으로 PC에 설치되므로 IEC 62443 4-2의 장치 분류에 따른

호스트 장치가 이에 해당한다. 호스트 장치 요구사항인 HDR 3.2는 악성코드 보호 프로그램을 설치할 것을 요구한다. 소프트웨어 어플리케이션 요구사항인 SAR 3.2에서는 이러한 내용을 문서화 할 것을 요구한다. 소프트웨어 어플리케이션 자체에서 악성코드 보호 기능을 개발할 필요는 없는 것이다. 네트워크 장치 요구사항인 NDR 3.2와 임베디드 장치 요구사항인 EDR 3.2에서는 보완 통제가 제공된다면 해당 장치에는 직접적으로 악성코드 보호 프로그램을 설치하지 않아도 됨을 명시하고 있다.



<임베디드 장치 예시 – PLC>
(Source : www.snsys.net)

소프트웨어 어플리케이션은 제어시스템 자체나 프로세스와 인터페이스 하는데 사용되는 하나 이상의 소프트웨어 프로그램과 부속 프로그램을 의미하며 시스템을 구동하기 위한 다양한 소프트웨어들이 이에 해당한다. 선박에 탑재되는 다수의 OT 장비들은 제조사 자체적으로 개발한 소프트웨어 어플리케이션을 해당 장비에 설치 및 운용하고 있으며 SAR의 요구사항을 만족할 수 있도록 개발하여야 한다. 임베디드 장치는 산업 공정을 직접 감시하거나 제어하도록 설계된 특수 목적 장치를 의미하며, 프로그래머블 로직 컨트롤러(PLC)가 이에 해당한다. 호스트 장치는 하나 이상의 공급 업체로부터 하나 이상의 소프트웨어 애플리케이션, 데이터 저장소 또는 기능을 호스팅할 수 있는 운영 체제를 실행하는 범용 장치로써 OT 장비의 HMI(Human-Machin Interface) 기능을 제공하는 오퍼레이터 워크스테이션, 데이터 저장 등의 업무를 수행하는 서버 등이 이에 해당한다. 마지막으로 네트워크 장치는 장치 간의 데이터 흐름을 가능하게 하거나 데이터 흐름을 제한하지만, 제어 공정과 직접 상호작용하지 않는 장치로써 우리 주변에서 흔히 볼 수 있는 허브, 라우터 등이 이에 해당한다. 또한 네트워크 구현을 위해 필수적이지는 않지만 보안의 관점에서 중요하게 요구되는 방화벽, 침입 탐지 시스템, 침입 차단 시스템 등도 네트워크 장치의 영역에 포함된다.


<호스트 장치 예시 – HMI>
(Source : www.kisa.or.kr)

용어 설명

VLAN(가상네트워크망)

하나 이상의 기존 LAN에서 생성된 사용자 지정 네트워크. 여러 네트워크(유선 또는 무선 모두)의 기기 그룹을 하나의 논리적 네트워크로 결합할 수 있게 한다. 그 결과는 물리적 근거리 통신망처럼 관리할 수 있다.

Source : TechTerms

ALARP

합리적으로 실행 가능한 한 낮음. 위험을 통제하는데 필요한 돈, 시간 및 노력에 대한 위험을 계산하는 것을 포함함. 작업장 내에서 위험이 통제될 것으로 예상되는 수준을 설명하며, 안전성이 수반되는 시스템의 관리 및 규제에 자주 사용됨.

Source : CREATIVE Safety supply

VPN(가상사설망)

VPN은 장치에서 네트워크로의 인터넷을 통한 암호화된 연결이다. 암호화된 연결은 민감한 데이터가 안전하게 전송되도록 하는 데 도움이 된다. 허가받지 않은 사람이 트래픽을 엿보지 못하게 하고 사용자가 원격으로 작업을 할 수 있게 한다.

Source : CISCO

해사 사이버보안 교육 소개

KR 사이버보안 교육

국제해사기구(IMO)의 '안전관리시스템에서의 해사 사이버 리스크 관리 결의(Resolution MSC.428(98)'에 따라 싱가포르, 마샬 아일랜드 등 기국에서는 국제안전경영코드(ISM code) 대상 기업들에게 2021년 1월 1일 이후 첫 연차 심사 전까지 안전관리시스템에서의 사이버리스크 관리를 요구하고 있다. 이에 해사 사이버보안에 대해 이해하고 적절한 사이버보안 시스템을 구축하기 위한 해사 사이버보안 교육에 대한 수요가 증가하였다.

한국선급은 2015년부터 국내외 선사, 조선소, 기자재업체, 서비스공급업체를 대상으로 사이버보안 교육을 제공하고 있다. 특히 지난 3월에는 싱가포르 MPA에 해사 사이버보안의 이해 과정에 대해 승인을 받아 해양 클러스터 기금을 통해 싱가포르 선사들에 사이버보안 교육을 제공하였다.

한국선급은 코로나19로 인해 집체교육이 어려운 고객들을 위하여 사이버보안 컨설팅 전문회사인 ㈜오렌지씨큐리티와 협력하여 지난 10월부터 해사 사이버보안 이러닝 과정을 제공하였고 교육은 수료한 국내외 교육생들에게 교육 수료 후 수료증을 발급하였다. 해사 사이버보안 이러닝 과정은 '해사 사이버보안의 이해', '해사 사이버보안의 관리 실무' 과정으로 구성되어 있다. '해사 사이버보안의 이해' 는 전체 직원의 사이버 보안 인식 제고를 목적으로 해사 사이버보안의 개요, 사이버 사고 사례 등으로 구성되어 있으며, '해사 사이버보안의 관리 실무' 는 실무자를 위한 내용으로 사이버 리스크 관리 수행 방법 등으로 구성되어 있다. 해사 사이버보안 이러닝 과정은 ㈜오렌지씨큐리티의 사이버보안 이러닝 아카데미 (https://edu.orangecq.com/)를 통해 신청할 수 있다.

교육 과정 샘플은 유튜브에서 '해사 사이버보안의 이해(https://youtu.be/fSIDLMj4gho)' 와 '해사 사이버보안의 관리 실 무(https://youtu.be/67t0ckrNtiA)'이 확인 가능하다.

한국선급은 지속적으로 교육 콘텐츠를 개발하여 고객들에게 제공함으로써 사이버보안 이러닝 교육을 강화해 나갈 계획이다.