# KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 031

November 2020

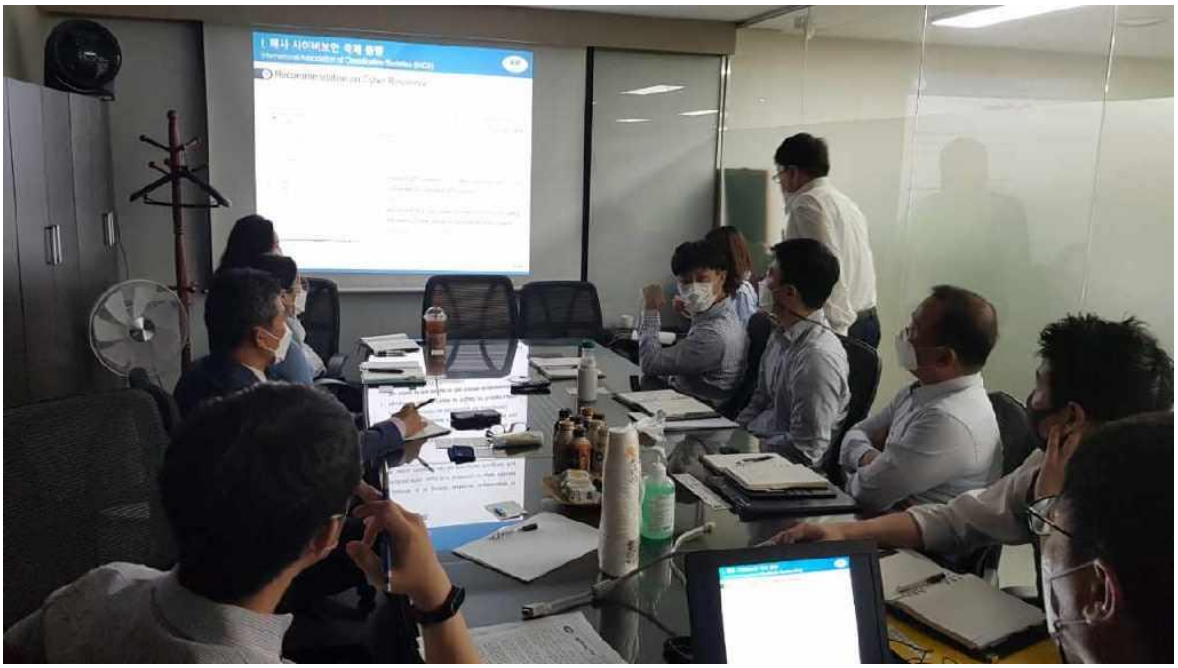
## ISM Code 내 사이버 리스크 관리 대응 교육 수행

한국선급은 지난 10월 20일, 장금상선과 싱크로해운을 방문하여 37명의 선박 감독관을 대상으로 ISM Code 내 사이버 리스크 관리 대응에 대한 교육을 수행하였다.이 교육은 선박 감독관들에게 해사 사이버보안의 국제 동향과 사이버보안 시스템의 구축 사례 등을 포함한 사이버보안에 대한 인식 제고와 함께 2021년 1월 1일 이후 도래하는 첫 DOC 연차심사 시까지 회사의 안전관리 시스템 상에 사이버 리스크 관리가 반영되는 것을 주관청이 확인하도록 권장하는 IMO Resolution MSC.428(98)에 대응할 수 있는 가이드라인을 제공하였다.

한국선급은 지난 1월 2일 IMO Resolution MSC.428(98)에 따라 사이버리스크 관리를 효과적으로 구현하기 위한 참고서로서 DOC 및 SOC 체크리스크를 발간한 바 있다. 이 체크리스트에는 사이버 리스크 관리를 위한 점검 항목과 점검 항목에 대한 해설이 포함되어 있다. 이 체크리스트는 한국선급 홈페이지/정부대행검사및심사/심사/ISM Code/자료실에서 다운로드 받을 수 있다.

https://www.krs.co.kr/sub/kor_board_read.aspx?no=11421&s_code=0204030311&b_code=004019000

한국선급은 지속적으로 선사를 대상으로 사이버보안에 대한 인식 제고 및 IMO Resolution MSC.428(98)에 대응하기 위한 사이버보안 맞춤형 교육 서비스를 강화해 나갈 방침이다.



# CMA CGM 선사 사이버 공격 피해 사례

## 전 세계 주요 4대 컨테이너 선사, CMA CGM의 라그나로커 랜섬웨어 피해사례

세계 4대 해운선사인 CMA CGM는 지난 2020년 9월 29일, 랜섬웨어 공격을 받은 것으로 알려졌다. CMA CGM은 중국 상하이, 선전, 광저우 소재 지사에서 '라그나로커' 랜섬웨어 공격을 받고 컨테이너 예약 시스템이 마비된 것으로 알려졌다. 이번 사건으로 인해 전 세계 주요 4대 선사가 모두 사이버 공격을 받았다는 것을 의미한다.


< 사진출처 : The Maritime Executive >

**< 해운선사에 대한 사이버 공격사례 >**

| 일 시 | 해운선사 | 공격대상 | 공격 형태 |
|---|---|---|---|
| 2017년 | APM-Maesk | 육상 IT 시스템 | NotPetya 랜섬웨어 공격 |
| 2018년 7월 | COSCO | 육상 IT 시스템 | 알려지지 않은 랜섬웨어 공격 |
| 2020년 4월 | MSC | 육상 IT 시스템 | 알려지지 않은 랜섬웨어 공격 |
| 2020년 9월 | CMA CGM | 육상 IT 시스템 | 라그나로커 랜섬웨어 공격 |

특정 업종의 주요 4대 기업이 사이버공격 피해를 입는 경우는 드문 사례이며, 이는 해운업계가 사이버 공격자의 표적으로 노출되었음을 알 수 있다. 이들 사례로 볼 때, 공격자의 주요 타겟은 선사의 육상 IT 시스템인 것으로 유추 할 수 있다. 선사의 육상 IT시스템은 선박관리, 선원관리, 화물관리 등의 시스템 일 수 있고, 이는 선박 목록, 컨테이너 ID 번호 및 선박 항로를 찾는 사이버 공격자들에게 해킹되어 선박 내 보석, 전자제품 등과 같은 고가 제품을 운반하는 컨테이너 화물을 훔치는데 악용될 우려가 있다.

이들 육상 IT 시스템들은 다른 산업분야의 다른 IT 시스템과 비교하여 특별히 다른 점이 없기 때문에, 공격자들에게는 쉬운 공격 대상이 될 수 있다. 따라서 해운업계는 기존 다른 산업계의 사이버 보안 시스템을 벤치마킹하여 해운 물류시스템에 대한 사이버 방어체계를 구축할 필요가 있다.

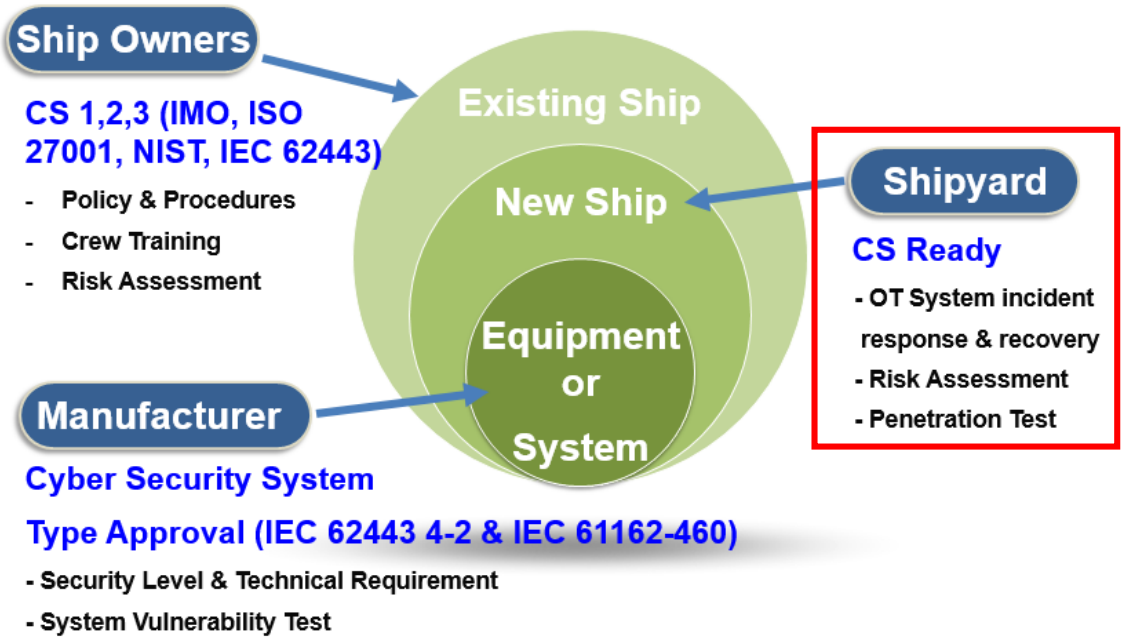
Source : https://zdnet.co.kr/view/?no=20200929103828

# KR 신조선 사이버보안 부기부호(CS Ready)의 이해

## 한국선급 사이버보안 인증 체계

**한국선급 해상 사이버보안 인증**은 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)**

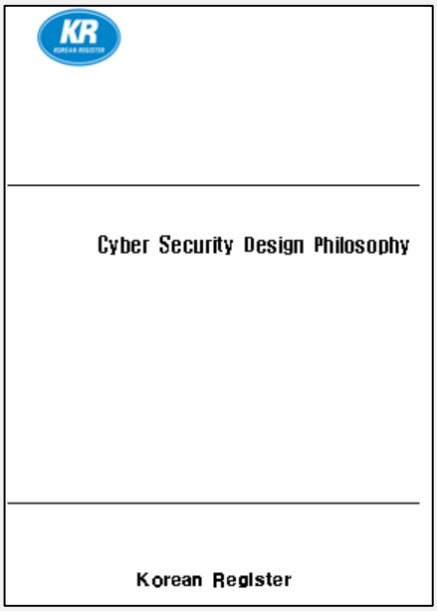



## 신조선 사이버보안 부기부호[CS Ready]의 필요성

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 : #3 시스템 기능 요구사항 명세서

선박 통합 사이버보안 체계 구축을 위해서는 주요 시스템을 대상으로 사이버보안 네트워크를 구축하고 보안 위협에 대한 리스크 평가, 취약성 진단 및 조치하는 일련의 프로세스가 필요하며, 이를 총체적으로 기술한 문서가 **Cyber Security Design Philosophy**다. 시스템 기능 요구사항 명세서란, 시스템 또는 소프트웨어, 외부 인터페이스의 필수 요구 사항(기능, 성능, 설계 제약 및 속성)이 기술되어 있는 문서이며 Design Philosophy에 포함할 수 있다.






**[Cyber Security Design Philosophy 문서 목차 ]**

| 항목 | 설명 | 기타 |
|---|---|---|
| 외부 인터페이스 요구사항 (External Interface Requirement) | ▪ 모든 소프트웨어 시스템으로의 입력과 출력에 대한 요구사항을 상세히 기술<br>▪ 사용자 인터페이스, 하드웨어 인터페이스, 소프트웨어 인터페이스, 통신 인터페이스 등으로 분류할 수 있음 | - 목적 상세 설명<br>- 유효 범위, 정확도, 오차<br>- 측정 단위 / 시간<br>- 입력/출력 관계<br>- 데이터 형식<br>- 명령 형식<br>- 종료 메시지 |
| 기능 요구사항 (Functional Requirement) | ▪ 소프트웨어 입력 처리와 출력을 생성하는 처리 과정에서 발생할 수 있는 기본적인 동작에 대하여 기술 | - 입력의 유효성 확인<br>- 동작의 정확한 흐름<br>- 비정상 상황에 대한 동작<br>- 파라미터의 영향 |
| 성능 요구사항 (Performance Requirement) | ▪ 소프트웨어 전체적으로 사람과의 상호작용 혹은 소프트웨어에서 확인할 수 있는 정적/동적 수치 요구사항 기술 | - 정적 수치 요구사항<br>- 동적 수치 요구사항 |
| 설계 제약사항 (Design Constraint) | ▪ 다른 표준이나 하드웨어적 제한으로 인해 적용되는 설계적 제한사항에 대하여 기술 | - |

**[소프트웨어 명세서 요구사항]**

Source : IEEE Standard 830 - Recommended Practice for Software Requirements Specifications

## [CS Ready] 제출문서 이해하기 : #4 자산 취약성 진단 결과

취약점이란 사이버시스템이나 소프트웨어 상에 존재하는 보안상의 약점을 의미한다. 선박에 탑재되는 IT/OT 시스템을 대상으로 해킹이나 서비스 장애, 데이터 유출/변조/삭제 등이 일어난 경우, 이러한 시스템 상의 취약점을 악용하여 피해가 발생한다. 취약점은 CCE, CVE, CWE로 분류할 수 있으며, 선박 IT/OT 자산을 대상으로 취약성을 진단(자동화 진단도구 활용)하고 조치한 결과를 제출해야 한다.

| 취약점 | 설명 | 대응책 | 관련 URL |
|---|---|---|---|
| 설정 취약점 (CCE) | ▪ Common Configuration Enumeration<br>▪ OS, 서버, PC, 네트워크 장비, 보안장비, DBMS 등 인프라의 설정 상에서 악용 가능한 취약점<br>예) 초기 암호 사용, 서비스 기본 포트 개방 등 | ▪ 설정 변경 | https://nvd.nist.gov/config/cce/index |
| 알려진 취약점 (CVE) | ▪ Common Vulnerability Enumeration<br>▪ 악용가능함이 공개적으로 밝혀진 취약점<br>예) CVE-2020-4163 (시스템 명령어 실행 취약점) | ▪ 패치 | https://cve.mitre.org/<br>https://www.krcert.or.kr/data/secInfoList.do |
| 알려진 약점 (CWE) | ▪ Common Weakness Enumeration<br>▪ 소프트웨어 언어 및 아키텍처, 소스 코딩 등 개발 단계에서 발생가능한 약점<br>예) CWE-20 (부적절한 입력 검증) | ▪ 시큐어코딩 | https://cwe.mitre.org/ |

| Name | STIG | Version | I Pass | I Fail | I Man | II Pass | II Fail | II Man | III Pass | III Fail | III Man |
|---|---|---|---|---|---|---|---|---|---|---|---|
| FG60E_ConFW | Firewall Security Technical Implementation Guide | 8 Release 25 () | 5 | 0 | 6 | 6 | 7 | 34 | 5 | 2 | 8 |

*Table 2: DISA STIG device compliance summary*

Diagram 3: STIG CAT I Findings

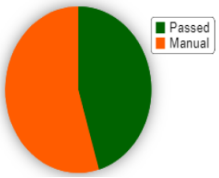



Diagram 4: STIG CAT II Findings

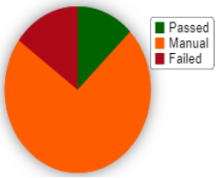
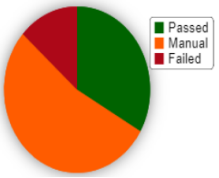



Diagram 5: STIG CAT III Findings




| Group | STIG | Title | Responsibility | IA Controls | Severity | State |
|---|---|---|---|---|---|---|
| V-3000 | NET1020 | Interface ACL deny statements are not logged. | Information Assurance Officer | | CAT III | ✓ |
| V-3008 | NET1800 | IPSec VPN is not configured as a tunnel type VPN. | Information Assurance Officer | | CAT II | ✎ |
| V-3012 | NET0230 | Network element is not password protected. | Information Assurance Officer | | CAT I | ✓ |
| V-3013 | NET0340 | Login banner is non-existent or not DOD-approved. | Information Assurance Officer | | CAT II | ✎ |
| V-3014 | NET1639 | Management connection does not timeout. | Information Assurance Officer | | CAT II | ✗ |
| V-3020 | NET0820 | DNS servers must be defined for client resolver. | Information Assurance Officer | | CAT III | ✓ |
| V-3021 | NET0890 | SNMP access is not restricted by IP address. | Information Assurance Officer | | CAT II | ✓ |
| V-3043 | NET1675 | SNMP privileged and non-privileged access. | Information Assurance Officer | | CAT II | ✓ |
| V-3054 | NET0377 | Firewall has unnecessary services enabled. | | | CAT II | ✎ |
| V-3056 | NET0460 | Group accounts are defined. | Information Assurance Officer | | CAT I | ✎ |
| V-3057 | NET0465 | Accounts assigned least privileges necessary to perform duties. | Information Assurance Officer | | CAT II | ✎ |
| V-3058 | NET0470 | Unauthorized accounts are configured to access device. | Information Assurance Officer | | CAT II | ✎ |

**[자동화 진단도구(Nipper Studio)를 활용한 Firewall 설정 점검]**

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

# KR 해상 사이버보안 형식승인 가이드라인

## 사이버보안 형식승인 지침 이해하기

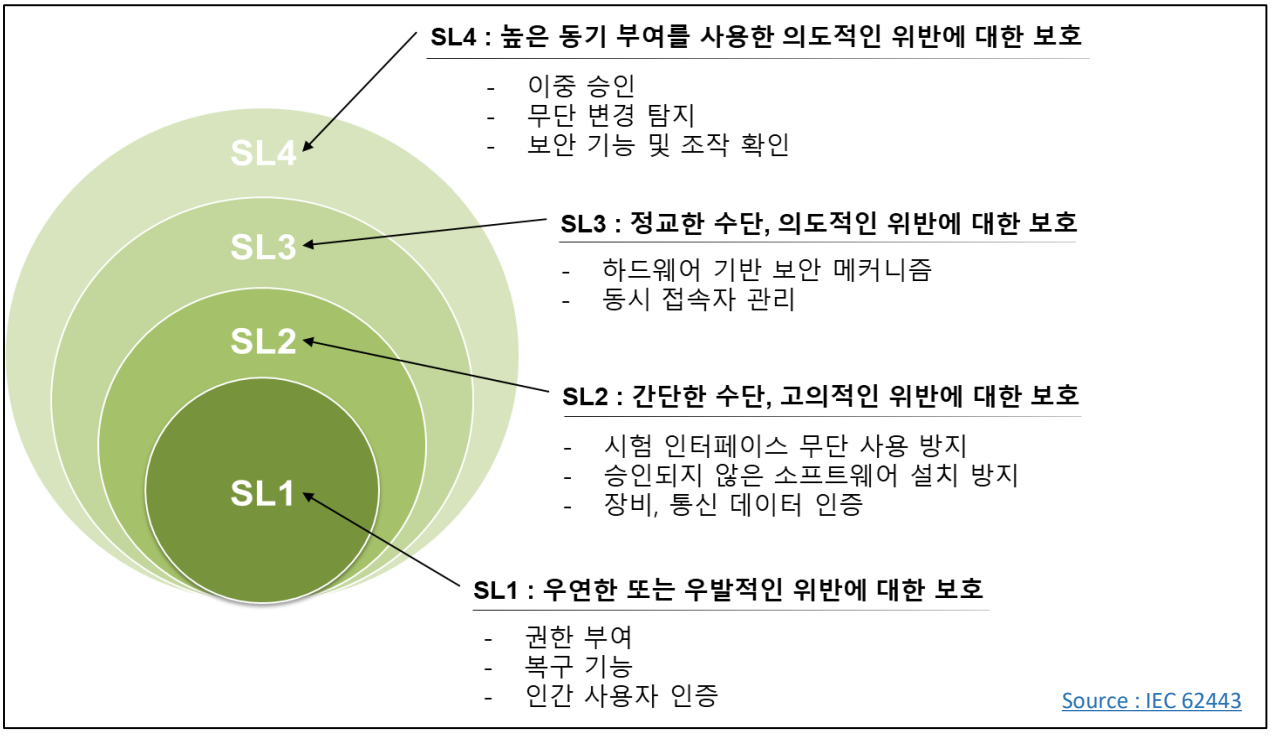
형식승인이란, 선박에 설치하기 전에 제품의 각 형식마다 미리 자료심사 및 승인시험을 하고 만족할 경우 제품이 규정에 적합하다는 것을 제조자에 대해서 증명하는 것을 의미한다. 사이버보안 형식승인은 ISA 62443 4-2, IEC 61162-460과 같은 국제표준을 기반으로 개발되었으며 선박에 탑재되는 원격 접속 장비, 통합 제어 및 모니터링 시스템 등을 포함하는 사이버 시스템의 사이버보안 수준 및 그 수준에 해당하는 요건을 12개의 범주 및 총 124개 항목의 요구 사항에 대한 검증을 통해 보안 기능과 그 수준을 확인한다.

**<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




Source : IEC 62443

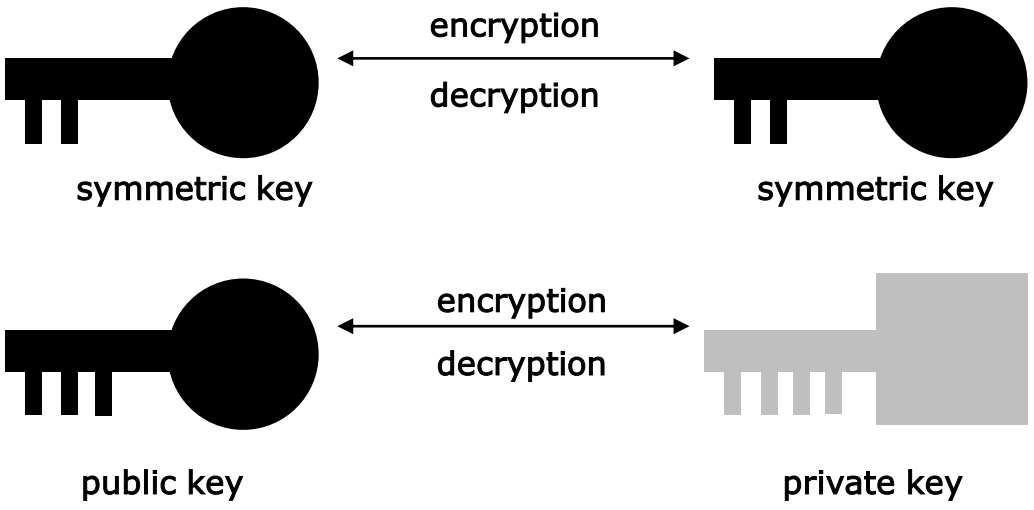
## 한국선급 해상 사이버보안 형식인증 검사항목

**공개 키 인프라 인증 (207)**

1. 공개 키 기반 구조 (PKI)를 사용할 경우, 구성품은 ISA 62443-4-2 CR1.8에 따라 공개 키 기반 구조의 영역 내에서 상호작용하고 작동할 수 있는 기능을 제공하거나 기능을 제공하는 시스템으로 통합되어야 한다. (SL 2,3,4)

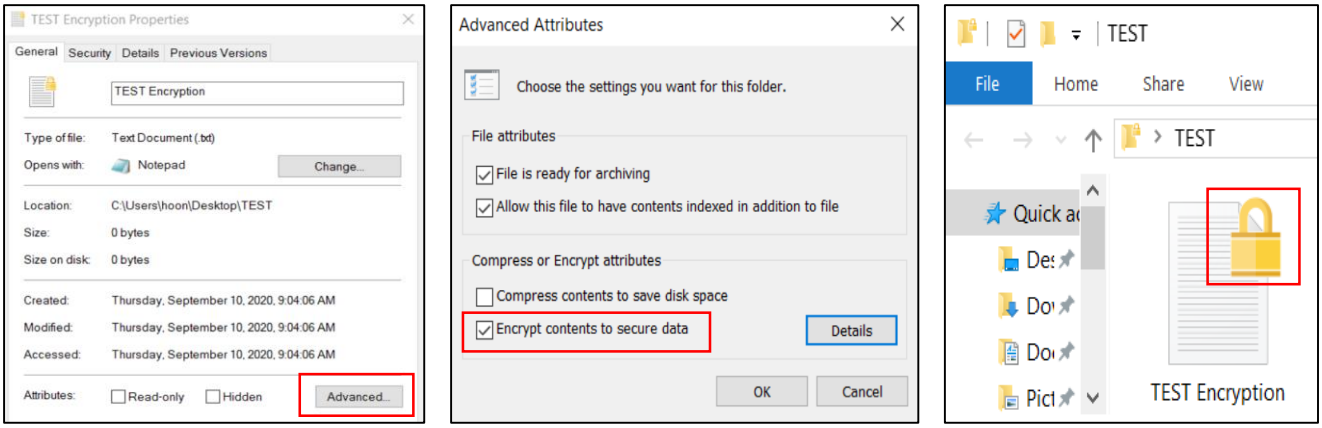
## 암호화 및 복호화 알고리즘

암호화는 암호화 알고리즘 및 키를 사용하여 일반 텍스트를 암호 텍스트로 변경하는 프로세스를 의미한다(source : NIST SP 800-57).



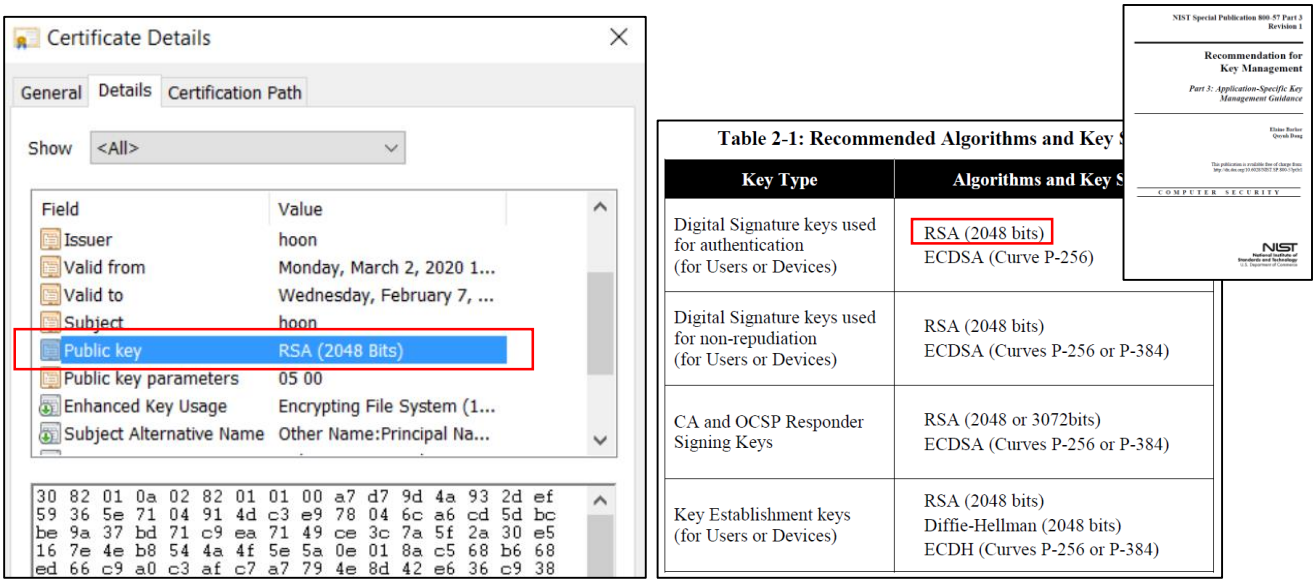

<암호화에 사용되는 키의 종류 - 대칭키/비대칭키>

암호화에는 다양한 알고리즘이 사용되며 크게 두가지 분류로 나누어 볼 수 있다. 암호화 및 복호화에 동일한 키를 사용하는 대칭키 방식(Symmetric key algorithm)이 있고 서로 다른 키를 사용하는 비대칭키 방식(Asymmetric key algorithm)이 있다. 비대칭키 방식은 공개키 방식의 암호화 알고리즘(Public-key cryptographic algorithm)이라고도 하며 공인인증서와 같이 주변에서 볼 수 있는 많은 암호화 기법들에 공개키 방식이 사용된다. 기밀성 보호를 위해 시스템에서 자체적인 암호화 기능을 제공할 수도 있으며, OS 등에서 이미 제공하고 있는 암호화 기능을 사용할 수도 있다. 암호화를 사용함에 있어 대칭키, 비대칭키 방식 중 어느것을 사용하여도 무방하나 취약한 것으로 식별된 알고리즘을 사용하여서는 안된다. 대칭키 방식의 암호화 알고리즘의 예시로는 SEED, DES, ARIA, AES 등이 있으며 공개키 방식의 암호화 알고리즘의 예시로는 RSA, ECC, DAS, TPM 등이 있다.




<윈도우 OS에서 제공하는 파일 및 폴더 암호화 기능의 예시>

윈도우 OS에서는 폴더 및 파일 단위의 암호화 기능을 제공한다. 파일을 우클릭하여 설정화면에서 암호화에 체크함으로써 간단히 파일을 암호화 할 수 있다. 또한 상세정보 확인시 암호화에 사용되는 알고리즘 또한 확인이 가능하다.




<윈도우 OS 암호화 알고리즘 및 NIST 권고안 비교>

위 그림은 윈도우 OS에서 제공하는 암호화 알고리즘의 확인 사진으로써 대칭키인 RSA 알고리즘 사용시 Key 길이를 2048 bit 이상을 사용하도록 하는 NIST SP 800-57 권고안을 준수함을 알 수 있다. 시스템에서 자체적으로 암호화 기능을 제공하고 공개키 알고리즘을 사용하는 경우 윈도우 OS에서 제공하는 기능과 같이 공개키 기반 구조의 영역 내에서 상호작용하고 작동할 수 있는 기능을 제공하거나 혹은 이러한 시스템에 통합될 수 있도록 하여야 한다.

# 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.

## 보안등급 (Security Level)

보안등급(Security Level)은 구역(Zone) 또는 통신경로(conduit)의 위험 평가를 기반으로 구역(zone) 또는 통신경로(conduit)의 장치 및 시스템의 고유 보안과 필수 보안대책의 집합에 대응하는 등급을 의미한다 (source : IEC 62443 4-2).

| Security Level | Definition |
|---|---|
| SL1 | ▪ 우연한 또는 우발적인 위반에 대한 보호 |
| SL2 | ▪ 간단한 수단, 고의적인 위반에 대한 보호 |
| SL3 | ▪ 정교한 수단, 의도적인 위반에 대한 보호 |
| SL4 | ▪ 높은 동기 부여를 사용한 의도적인 위반에 대한 보호 |

<보안등급의 정의> (Source : IEC 62443-3-3)

IEC 62443에서는 보안등급을 SL1 부터 SL4까지 총 4가지로 구분하고 있으며 모든 시스템에 대해 일괄적인 보안 요구사항을  적용하는 것이 아닌, 리스크 평가를 기반으로 각 구역별 보안등급 적용을 권고한다. 보안에 대한 고려는 필수적이나 비즈니스 영속성을 위협을 주는 수준이어서는 안된다. 이를 테면 가정집의 보안을 위해 핵발전소 수준의 보안조치를 적용하는 것은 비용적인 문제를 발생시키게 되어 오히려 부정적인 영향을 미치는 것과 같다.  리스크 평가 단계에서는 허용 가능한 위협을 포함하여 이러한 부분을 고려하여 구역별 보안등급을 결정하여야 한다.

## 기본 요구사항(FR)별 보안등급

IEC 62443에서는 기본 요구사항(FR-Foundational Requirement)별로 보안등급 목적을 설명하고 있다. 7개로 나누어진 기본 요구사항은 이전 호를 참고 할 수 있으며, 첫번째 기본 요구사항인 FR1 식별 및 인증을 예로 보면 보안등급의 목적을 좀 더 상세하게 설명하고 있음을 알 수 있다.

| Security Level | Definition |
|---|---|
| SL1 | ▪ 인증 받지 않은 개체의 일상적인 또는 우연한 접근에 대응하는 보호 메커니즘으로 모든 사용자(사람, 소프트웨어 프로세스 및 장치)를 식별하고 인증한다. |
| SL2 | ▪ 의도적으로 인증 받지 않은 개체가 적은 자원, 일반적인 기술 및 낮은 동기의 단순한 수단을 사용하여 시도하는 접근에 대응하는 보호 메커니즘으로, 모든 사용자(사람, 소프트웨어 프로세스 및 장치)를 식별하고 인증한다. |
| SL3 | ▪ 의도적으로 인증 받지 않은 개체가 중간 규모의 자원, IACS 특화 기술 및 적당한 동기의 정교한 수단을 사용하여 시도하는 접근에 대응하는 보호 메커니즘으로, 모든 사용자(사람, 소프트웨어 프로세스 및 장치)를 식별하고 인증한다. |
| SL4 | ▪ 의도적으로 인증 받지 않은 개체가 대규모의 자원, IACS 특화 기술 및 높은 동기의 정교한 수단을 사용하여 시도하는 접근에 대응하는 보호 메커니즘으로 모든 사용자(사람, 소프트웨어 프로세스 및 장치)를 식별하고 인증한다. |

<보안등급의 정의 – FR1 식별 및 인증>

마지막으로 IEC 62443 4-2에서는 보안등급에 따른 세부적이고 구체적인 요구사항인 CR(Component Requirement)을 제시한다. 앞의 요구사항이 개념적인 것이었다면, CR에서는 구체적이고 기술적인 보안 요구사항들이 명시되어있다.

| Security Level | Definition |
|---|---|
| SL1 | ▪ 사용자를 식별하고 인증할 수 있는 기능을 제공하여야 한다. |
| SL2 | ▪ 모든 인간 사용자를 식별하고 인증할 수 있는 기능을 제공하여야 한다. |
| SL3,4 | ▪ 다중요소 인증을 사용할 수 있는 기능을 제공하여야 한다. |

<CR 요구사항 – CR1.1 인간 사용자 식별 및 인증>

선주, 조선소의 입장에서는 상위 수준에서 부터 보안등급을 고려하여 최종적으로 구역별 보안등급을 결정할 수 있고, 제조사에서는 CR에 대한 분석 및 기술적인 기능 구현을 통해 현재 제공 가능한 보안등급의 정보를 제공할 수 있고 추가로 보완 혹은 개발이 필요한 보안 기능을 식별할 수 있다.

# 용어 설명

## DMZ(비무장지대)

내부 네트워크와 외부 네트워크 사이에 위치하는 네트워크 영역(소속 네트워크)이다. DMZ의 요점은 내부 및 외부 네트워크에서 DMZ로의 연결이 허용되는 반면, DMZ에서 외부 네트워크로의 연결은 외부 네트워크에만 허용된다는 것이다. 즉, DMZ의 호스트는 내부 네트워크에 연결되지 않을 수 있다. 이를 통해 DMZ의 호스트는 외부 네트워크에 서비스를 제공하는 동시에 침입자가 DMZ의 호스트를 손상시킬 경우에 대비하여 내부 네트워크를 보호할 수 있다. 내부 네트워크에 불법적으로 연결하려는 외부 네트워크 누군가에게 DMZ는 막다른 골목이다.

Source : CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

## 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

## SIEM(보안 정보 및 이벤트 관리)

SIEM 소프트웨어는 보안 정보 관리와 보안 이벤트 관리가 결함된 것으로 애플리케이션과 네트워크 하드웨어에 의해 생성된 보안 경고의 실시간 분석을 제공한다. 사이버 위협과 책임이 확대됨에 따라 SIEM의 역할은 분석가가 보유한 가장 큰 자산의 하나가 되었으며, 보안 분석가는 사용자 및 행동 분석, 실시간 모니터링, 데이터 및 애플리케이션 모니터링 등 고급 분석을 위하여 SIEM을 사용한다.

Source : McAfee

# 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.