KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 026

June 2020

한국선급 활동

- 한국선급-삼성중공업, 선박 사이버보안 협약 체결
- 신조선(LPG Carrier, 84,600 CBM) 사이버 리스크평가 워크샵 수행

와이파이 6에 적용된 차세대 보안기술

사이버 위협의 이해(OWASP Top 10 Internet of Things)

KR 해상 사이버보안 형식승인 지침의 이해

용어 설명

한국선급-삼성중공업, 선박 사이버보안 협약 체결

한국선급(KR, 회장 이형철)과 삼성중공업(삼성중공업, 남준우 대표이사)는 지난 22일 삼성중공업 선박해양연구센터에서 양사 관계자가 참석한 가운데 '선박 사이버보안 네트워크 구축 및 설계 안전성 평가에 관한 공동연구' 양해각서(MOU)를 체결했다.

이번 협약에 따라 양사는 한국선급의 해상 사이버보안 인증 역량과 삼성중공업의 선박 건조 기술역량을 바탕으로 신조선에 적용 가능한 사이버보안 네트워크 구축 및 설계 안전성을 평가하고 선박 사이버보안 취약성 진단 및 테스트를 하게 된다. 또한 국제해사기구(IMO)의 MSC.428(98) 결의안에 따라 2021년부터 사이버보안 리스크 관리에 대한 요구가 강화될 것으로 예상되므로 선박 사이버보안 규칙 적용 및 검증 부문에서도 협력해 나갈 예정이다.

김대헌 한국선급 디지털기술원장은 "삼성중공업과의 공동 연구를 통해 한국선급의 선박 사이버보안 인증 및 기술 서비스 역량을 한층 강화해 나갈 것"이라고 하며 "앞으로 세계 해사업계에서 사이버보안 인증 기술 리더십을 더욱 공고히 할 수 있을 것으로 기대한다."고 말했다.

삼성중공업은 독자 개발한 스마트 선박 솔루션인 에스베슬(SVESSEL)을 기반으로 주요 메이저 선급의 사이버보안 인증 획득을 통해 선박 사이버보안에 대한 기술력을 인정받았다. 이러한 기술을 바탕으로 현재 선박해양연구센터에 구축된 사이버보안 테스트베드를 이용하여, 한국선급과 선박에 대한 다양한 사이버 위협에 대응할 수 있는 기술에 대해서 공동연구를 진행할 예정이다.

심용래 삼성중공업 조선해양연구소장은 "선박 사이버보안 인증 및 기술 서비스를 갖춘 한국 선급과의 공동 연구를 통해 스마트 선박이 갖추어야 하는 보안 역량을 더욱 확고히 할 것"이라고 하며 "다가오는 자율운항 선박 시대에 글로벌 최고 수준의 사이버보안 기능을 갖춘 선박을 고객에게 인도할 것으로 기대한다."고 말했다.

신조선(LPG Carrier, 84,600 CBM) 사이버 리스크평가 워크샵 수행

한국선급은 지난 5월 14일, 현대중공업(HHI) 및 한국조선해양(KSOE) 임직원들과 현대중공업에서 건조중인 현대LNG해운 선사 신조선(LPG Carrier, 84,600 CBM) IT/OT 시스템을 대상으로 사이버 리스크 평가 워크샵(1차)을 수행하였다.

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 식별할 수 있다. 이번 워크샵에서는 ISO / IEC 27005, NIST 800-39 사이버 리스크평가 방법론을 적용하였으며, 산업계 사이버보안 표준인 IEC 62443(산업 자동화 및 제어 시스템에 대한 보안인증)의 Zone & Conduit 개념 또한 적용하였다. 표준에 기반하여 선박의 네트워크를 Remote Zone, Control System Zone, Crew LAN Zone, Bridge Zone, Wireless Zone으로 세분화하여 경계 보호 장비(예 : 프록시, 게이트웨이, 라우터, 방화벽, 단방향 게이트웨이, 가드 및 암호화 된 터널)의 사이버보안 적절성을 평가하였다.

향후 한국선급은 현대중공업(HHI), 한국조선해양(KSOE) 뿐 아니라 선주사(현대 LNG 해운) 및 관련 제조사를 초빙하여 2차 사이버리스크평가 워크샵을 수행할 예정이다. 이를 통해 선박의 기술적 보안 영역 뿐 아니라 선주사의 관리적, 절차적 보안 영역까지 분석할 예정이다.

와이파이 6에 적용된 차세대 보안기술

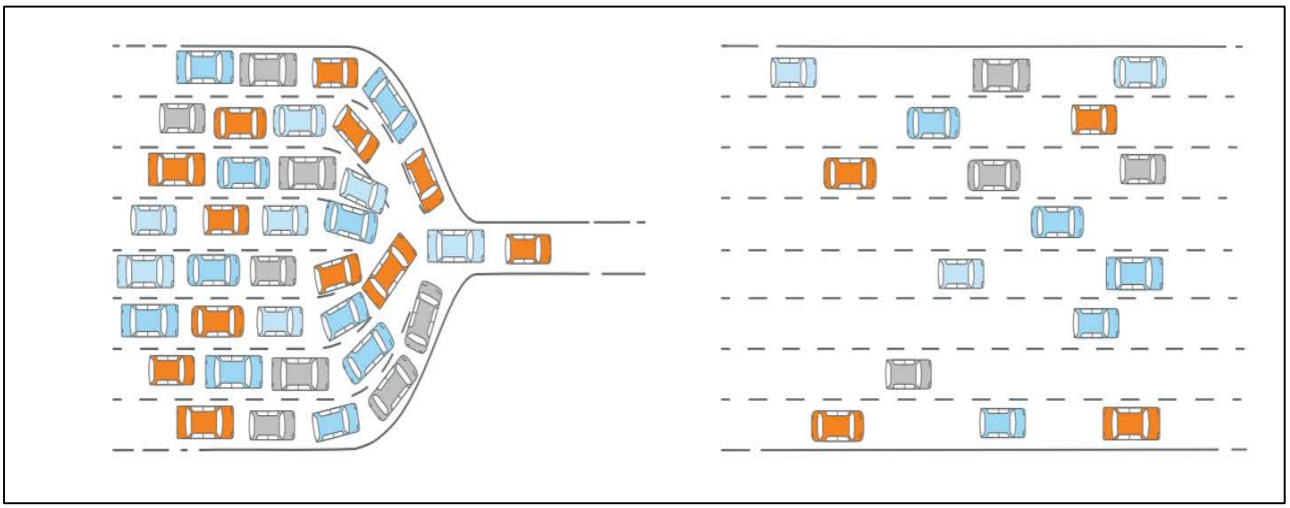
본 기획시리즈는 일상생활과 회사, 선박 등에서 널리 사용되는 무선네트워크의 종류와 통신원리에 대해 알아보고, 무선 네트워크의 취약점과 대응방안을 소개하고자 한다. 따라서 본 뉴스레터 2020년 6월호에서는 ***'무선랜의 새로운 기술과 강화된 보안성'***에 대해 소개한다.

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 **무선랜(WIFI)의 새로운 기술과 강화된 보안성**
⑤ 기타 무선네트워크(Bluetooth, Zigbee 등)의 기술적 보안 취약점과 대응방안
⑥ 해상무선통신의 종류와 기술적 보안 취약점과 보안성 강화방안

새로운 무선랜 기술인 와이파이 6란?

IEEE에서 2018년 말에 공개한 802.11ax 기술을 와이파이 연합(Wi-Fi Alliance)에서 와이파이 6라고 명명하였다. 이 와이파이 6는 기존 기술(802.11ac) 대비 데이터 속도가 4배 늘어났고, 2.4GHz와 5GHz 대역을 모두 사용할 수 있다. 또한, 기존 와이파이 기술은 OFDM 기술로 한 번에 1개의 데이터만 전송 가능하지만, 와이파이 6에 적용된 OFDMA 기술은 동시에 여러 개의 데이터를 전송할 수 있다. 이 기능은 스트리밍되는 HD 비디오 같은 대규모 패킷을 보다 효율적으로 처리할 수 있으며, IoT 디바이스 및 음성 트래픽의 패킷같이 상대적으로 짧은 패킷은 OFDMA를 사용하여 더 효과적으로 처리 될 수 있다.



출처 : 802.11ax(WI-FI 6) 소개, (https://www.arubanetworks.com/ko/products/networking/802-11ax)

와이파이 6에 적용된 WPA3(Wi-Fi Protected Access 3) 기술

앞선 뉴스레터(2월호~4월호)에서 무선랜의 암호화 기술과 취약점에 대해 알아보았다. 와이파이 6에 적용된 WPA3 기술은 기존 WPA2의 취약성을 일부 개선하였으며, 암호화 방식, 키 관리 기술을 개선하였으며, 공항 등 공공장소에서 주로사용되는 개방형 무선네트워크에서도 보안성이 향상되었다. 다음표는 Wi-Fi의 보안기술의 진화과정을 보여주는 표이다.

구분	WEP	WPA	WPA2	WPA3
암호화	RC4	TKIP+RC4	CCMP/AES	GCMP-256
인증	WEP-Open WEB-Shared	WPA-PSK /Enterprise	WPA2-Personal /Enterprise	WPA3-Personal /Enterprise
키 관리	none	4 way-Handshake	4 way-Handshake	ECDH / ECDSA

<Wi-Fi 보안기술의 진화과정>

WPA3의 기능적 보안기술 요소를 좀더 살펴보면, WPA2의 가장 잘 알려진 취약점인 KRACK 공격(키 재설정 공격)을 보완하였다. KRACK 공격이란 암호화 키 자체가 노출되지는 않지만, WIFI 네트워크 망에 인위적으로 암호화 키 재설정을 반복 유도하여 암호화에 사용하는 초기 벡터(Initial Vector)를 알아내어 데이터 복호, 위,변조 가능하도록 하는 공격을 말한다. 아래 표와 같이 WPA3의 보안기술 요소를 요약할 수 있다.

구분	기술 요소	세부 기술 / 설명
WPA3 기능	192bit Security Suite	192bit 타원곡선 암호화
	SAE / 4 Way-Handshake	동일성 동시 인증, KRACK 대응
	Easy Connect	페어링 프로세스 간소화
	Wi-Fi CERTIFIED Enhanced Open	OWE기반 개방형 네트워크 암호화
WPA3 모드	WPA3-Personal Mode	– 개인 사용자 위한 모드 – 자연 암호 사용 – Forward Security – 암호 노출 시 트래픽 보호
	WPA3-Enterprise Mode	– 기업 사용자 위한 모드 – GCMP-256 암호화 – HMAC-SHA384 키 유도 – 384bit ECDH, ECDSA 키 인증 – BIP-GMAC-256 프레임 보호

<WPA3의 보안기술 소개>

사이버 위협의 이해(OWASP Top 10-사물인터넷)

사이버 위협 이해하기

사이버 위협이란, 조직 운영, 조직 자산, 개인, 기타 조직 또는 국가에 대해 사이버 시스템을 통한 무단 액세스, 파괴, 공개, 정보 수정 또는 서비스 거부와 같은 잠재적으로 악영향을 미칠 수 있는 상황이나 사건을 의미한다. (출처 : NIST SP : 800-128)

사이버위협은 ICT 기술이 발전함에 따라 자산에 미치는 영향이 변화하므로 자산의 취약점을 파악하기 위해 주기적으로 목록화 할 필요가 있다.

한국선급 해상 사이버보안 시스템 인증 검사항목(CS1)

204.1 위험관리 : 내부 정보기술 및 운영기술 환경에 의한 영향을 미치는 외부 환경 요인을 위협으로 식별하고 목록화하여야 한다.

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.

Top Ten	2014 IoT Top Ten	2018 IoT Top Ten
I1	Insecure Web Interface	Weak Guessable, or Hardcoded Passwords
I2	Insufficient Authentication/Authorization	Insecure Network Services
I3	Insecure Network Services	Insecure Ecosystem Interfaces
I4	Lack of Transport Encryption	Lack of Secure Update Mechanism
I5	Privacy Concerns	Use of Insecure or Outdated Components (NEW)
I6	Insecure Cloud Interface	Insufficient Privacy Protection
I7	Insecure Mobile Interface	Insecure Data Transfer and Storage
I8	Insufficient Security Configurability	Lack of Device Management
I9	Insecure Software/Firmware	Insecure Default Settings (NEW)
I10	Lack of Physical Hardening	Poor Physical Security

보안 업데이트 매커니즘 부족(Lack of Secure Update Mechanism)

인가되지 않은 소프트웨어나 펌웨어 업데이트는 IoT 사이버 공격의 주요 위협 벡터이다. IOT 위반은 데이터 손실을 초래하는 물리적 결과를 초래할 수 있으며 상당한 법적 책임과 평판을 해칠수 있다.다음 표는 ENISA에서 권고하는 "보안 업데이트 매커니즘 부족"에 대한 보안조치의 예시이다.

도메인	보안조치	참조 표준
IT 보안 관리 IT 보안 아키텍처 식별 및 접근 관리 IT 보안 유지 보수	장치 소프트웨어/펌웨어, 해당 구성 및 애플리케이션이 OTA(Over-The-Air)로 업데이트할 수 있는지, 업데이트 서버가 보안이 되는지, 업데이트 파일이 보안 연결을 통해 전송되는지, 민감한 데이터(예: 하드 코딩된 자격 증명)을 담고 있지 않은지, 인증된 신뢰 기관과 암호화 기관이 서명했는지, 업데이트 패키지가 전자서명, 서명 인증서 및 서명 인증서 체인이 있는지, 업데이트 프로세스가 시작되기 전 장치에 의해 검증되는지 확인하라. OTA 업데이트 기능을 구축하지 못하면 장치가 전체 수명주기 동안 위협 및 취약성에 노출될 수 있다.	・ISO27001 A12. Operations security ・NIST SP 800-53 - SI-7 Software, Firmware, And Information Integrity ・NIST Framework for Improving Critical Infrastructure Cybersecurity ・OWASP I9. Internet of Things Top Ten ・U.S. Department of Homeland Security - Strategic Principles For Securing The Internet Of Things (IoT) ・Cloud Security Alliance (CSA) - Future-proofing the Connected World: 13 Steps to DevelopingSecure IoT Products ・IoT Security Foundation (IoTSF) ・GSM Association (GSMA) ・IoT Security Guidelines- Atlantic Council (Brent Scowcroft Center On International Security) - Smart Homes and the Internet of Things- Online Trust Alliance (OTA) ・IoT Trust Framework and Trust Framework Resource Guide ・BITAG (Broadband Internet Technical Advisory Group) ・Internet of Things (IoT) Security andPrivacy Recommendations Technical Working Group Report ・ARMOUR (Large-Scale Experiments of IoT Security Trust) ・AT&T Cybersecurity Insights ・Exploring IoT Security Volume 2 ・Symantec - An Internet of Things Reference Architecture ・- Symantec - Internet Security Threat Report (ISTR) ・Microsoft - Cybersecurity Policy For The Internet Of Things Etc.
IT 보안 아키텍처	자동 펌웨어 업데이트 매커니즘을 제공하라. 장치는 수시로 펌웨어 업데이트가 있는지 확인하도록 구성되어야 한다. 자동 펌웨어 업데이트는 기본적으로 활성화되어야 한다. 장치는 자동 펌웨어 업데이트를 비활성화할 수 있는 기능을 제공하여야 하고 이를 위해 인증을 요구해야 한다.	
IT 보안 아키텍처	펌웨어 업데이트의 이전 버전과의 호환성. 자동 펌웨어 업데이트는 이전 버전과 호환되지 않는 어떤 방법으로도 네트워크 프로토콜 인터페이스를 변경해서는 안 된다. 업데이트 및 패치는 사용자 통보 없이 사용자 구성 기본 설정, 보안 및/또는 개인 정보 설정을 수정해서는 안 된다. 사용자는 업데이트를 승인, 허가 또는 거부할 수 있는 능력이 있어야 한다.	

출처 : ENISA, Baseline Security Recommendations for IoT, NOVEMBER 2017

KR 해상 사이버보안 형식승인 가이드라인

사이버보안 형식승인 지침 이해하기

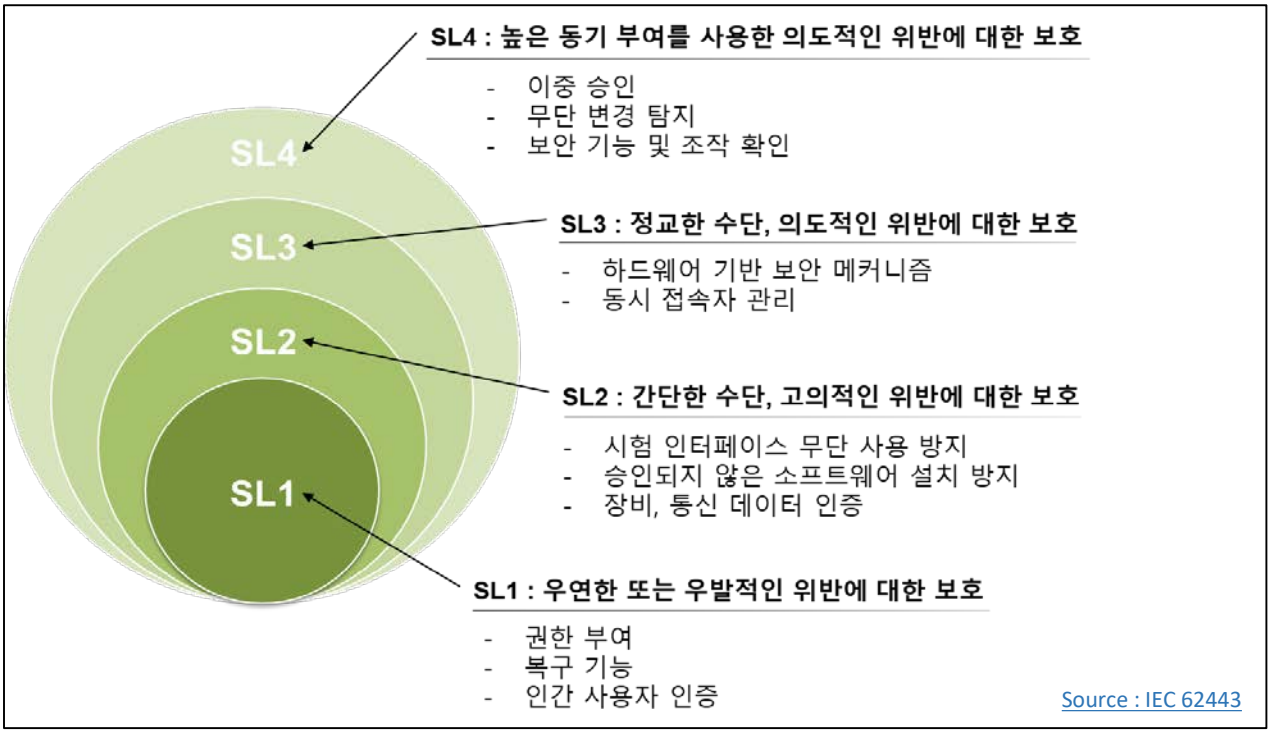
형식승인이란, 선박에 설치하기 전에 제품의 각 형식마다 미리 자료심사 및 승인시험을 하고 만족할 경우 제품이 규정에 적합하다는 것을 제조자에 대해서 증명하는 것을 의미한다. 사이버보안 형식승인은 ISA 62443 4-2, IEC 61162-460과 같은 국제표준을 기반으로 개발되었으며 선박에 탑재되는 원격 접속 장비, 통합 제어 및 모니터링 시스템 등을 포함하는 사이버 시스템의 사이버보안 수준 및 그 수준에 해당하는 요건을 12개의 범주 및 총 124개 항목의 요구 사항에 대한 검증을 통해 보안 기능과 그 수준을 확인한다.

<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

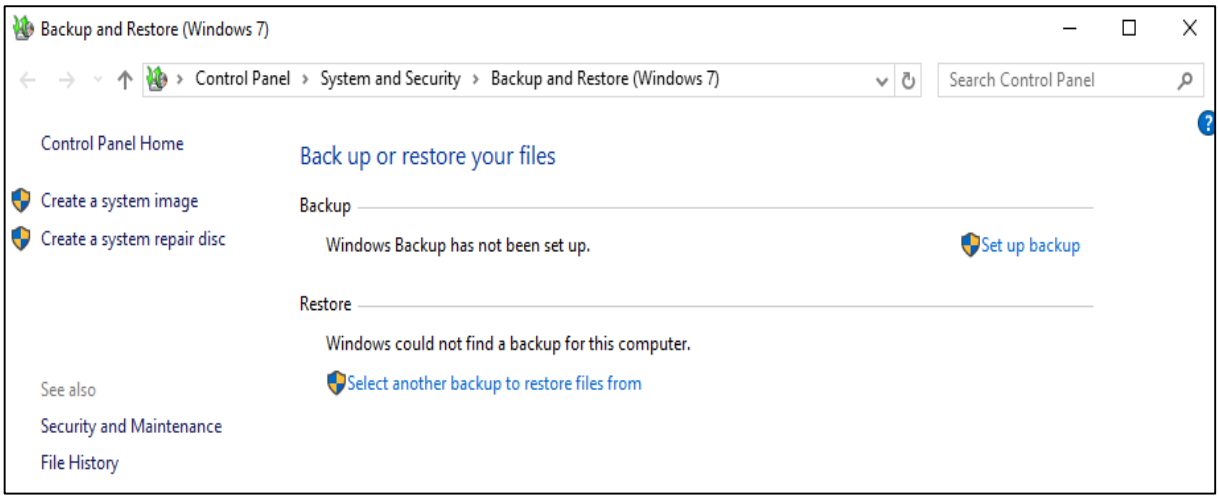
한국선급 해상 사이버보안 형식인증 검사항목

시스템 백업 (803)

1. 사용자 및 시스템 수준 정보를 보호하기 위하여 백업 기능을 제공하여야 하며 백업 프로세스가 정상적인 작동에 영향을 미치지 않아야 한다.(SL 1)
2. 복원을 시작하기 전에 백업된 정보의 무결성을 확인할 수 있는 기능을 제공하여야 한다. (SL 2,3,4)

백업 요구 사항

백업은 필요한 경우 복구를 용이하게 하기 위해 만든 파일 및 프로그램의 복사본을 의미하며(출처 NIST SP 800-34r1) 시스템의 장애 또는 잘못된 구성에서의 복구를 위해 필수적으로 요구되는 기능이다. SL1 등급을 만족하기 위해서는 백업기능의 제공되어야 하며, 백업 수행시에 정상적인 프로세스의 작동에 영향을 미치지 않아야 한다. 가용성이 중요시 되는 OT 시스템에 있어 백업 수행동안 장비를 사용할 수 없다고 한다면 이는 문제가 될 수있기 때문이다. 시스템에서 이러한 기능을 구현하기 어려운 경우 물리적인 이중화를 통해 해당 요건을 만족할 수도 있다. SL 2, 3, 4 등급을 만족하기 위해서는 백업된 정보의 무결성을 확인할 수 있는 기능을 제공하여야 한다. 무결성은 정확성과 완전성을 보호하는 성질을 의미하며 이를 위해 백업파일의 무결성이 깨어진 경우 즉, 백업 파일이 위변조가 되거나 혹은 훼손되어 정상적인 복구가 불가능한 경우 이를 사용자가 알 수 있도록 해야 한다. 위변조가 되거나 혹은 훼손된 파일을 통해 시스템 복구가 진행된 경우 시스템이 해킹에 악용되거나 혹은 시스템을 사용하지 못하게 되어 심각한 문제를 일으킬 수 있기 때문이다.



<백업 기능의 예시>

용어 설명

OFDMA(Orthogonal Frequency Division Multiplexing Access)

- 상호 직교성을 갖는 다수 반송파를 이용하여 신호를 변조하여 다중화하는 전송 방식으로, 고속의 데이터를 서로 직교하는 다수의 부반송파(subcarrier)로 나누어 병렬로 전송하기 때문에 심볼 주기가 부반송파의 수만큼 확장시킬 수 있어 심볼 간 간섭(ISI)을 줄일 수 있다. 그럼에도 불구하고 고스트가 심하면 심볼 사이에 반사파의 최고 주기보다 긴 가드 인터벌(guard interval)을 두어 간섭을 제거한다. 따라서 OFDM은 고스트가 많은 채널 환경에서 고속 데이터 전송이 가능하고, 가드 인터벌 사용으로 단일 주파수 망(SFN) 구성이 가능하며, 다중 입력 다중 출력(MIMO)이나 적응 변조 및 코딩(AMC) 기술 적용이 용이하다. 다만, 상대적으로 큰 PAR(Peak to Average Ratio) 때문에 전력 효율이 떨어지는 단점이 있다. [TTA]

OTA(Over-the-air programming)

- 새로운 소프트웨어, 펌웨어, 설정, 암호화 키 업데이트를 휴대전화, 셋톱박스 등의 장치에 무선으로 배포하기 위한 방식이다. OTA를 통해 새로운 방식의 악의적 공격을 방어 및 예방하고, SW 업데이트를 위해 방문 수리, USB 배송 없이 SW를 업데이트할 수 있어 비용을 절감할 수 있으며, 스마트폰처럼 운영체제나 SW를 업데이트해 장치의 생명주기에 걸쳐 신기능과 기술을 쉽게 적용할 수 있다. [슈어소프트]