자율운항 선박의 사이버 보안 리스크 전망

조용현, 강준모*
고려대학교 정보보호대학원 연구원
고려대학교 정보보호대학원 박사과정 *

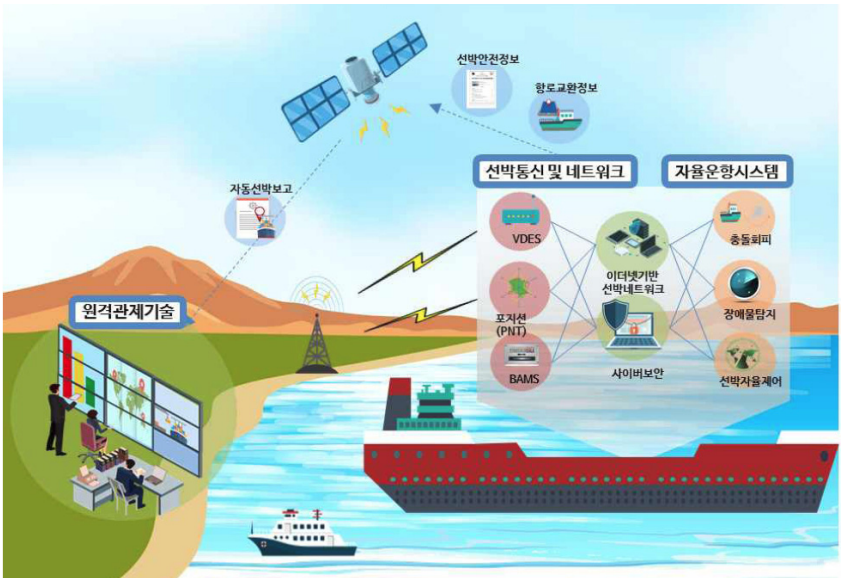
I. 서론

조선해양 산업과 ICT가 융합되는 환경이 본격화됨에 따라 선박 시스템은 새로운 ICT 플랫폼 기반에서 동작하게 되었다. 이 플랫폼은 IoT(사물인터넷), 빅데이터, AI(인공지능), 센서와 센싱 네트워크, 사이버 물리시스템(CPS), 선박과 이해관계자(정부기관과 선주 및 화주, 선박운영사 등)와 연결되며 4차 산업혁명의 기술 변화와 추이를 같이 하고 있다. 2010년 초반부터 선박 위성통신 장비와 기술이 보편화되면서 ICT 플랫폼을 통해 육상에서 수천 km 떨어진 선박의 운항관리, 선체관리 및 모니터링, 원격 유지보수와 성능분석이 가능한 Smart Ship 기술이 적용되기 시작했다. 조선산업과 ICT 융합을 통해 차세대 선박운항시스템인 e-Navigation 기반기술 및 장비표준 개발이 이루어지고 있어 조선 내 ICT 융합 장비의 비중은 선가 대비 약 6~15% 이상으로 증가하고 글로벌 시장규모는 2020년에 약 220억 달러, 국내 시장규모는 약 9.7억 달러로 전망되고 있다[1].

우리나라에서는 4차 산업혁명위원회에서 Smart Ship 보다 한 단계 진보된 자율운항 선박을 “혁신성장을 위한 사람 중심의 4차 산업혁명 대응계획”에 포함하여 2022년에 최초운항을 실현한다는 방침이다[2]. 자율운항 선박은 [그림 1]과 같이 정보통신기술(ICT)을 기반으로 하는 선박으로, 자율운항 제어시스템(Autonomous Navigation System: ANS), 선박 자동식별 장치(Automatic Identification System: AIS), 위성통신망 선박 원격제어 기술(Integrated Maritime Information Technology: IMIT)과 같은 최첨단 정보 기술을 조선 기술에 접목하여 자율 운항, 경제적 운항, 안전 운항이 가능한 차세대 디지털 선박으로 정의된다[3].

일본에서는 2018년 5월 국토교통성 자율운항 선박 실증실험을 공고하고 테스트를 추진하

* 본 내용은 조용현 연구원(☎ 02-3290-4250, yhjo13@korea.ac.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.



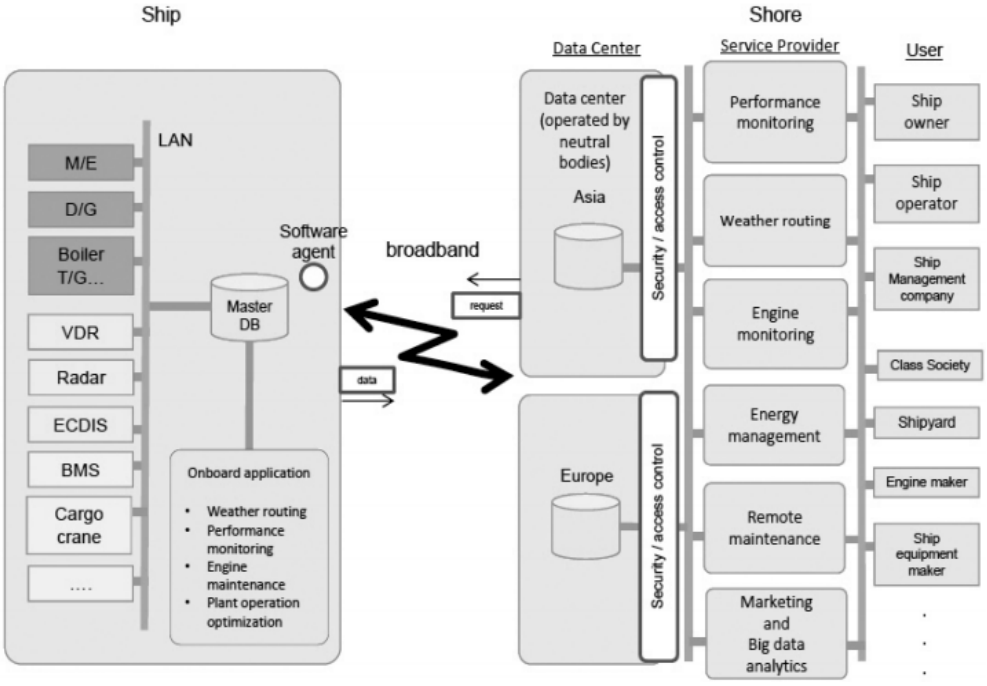
<자료> ICT 표준화전략맵 Ver. 2018.

[그림 1] 자율운항선박 기술의 개요도

고 있으며 AI기반의 원격조작, 선박지원, 모니터링, 고장감지, 운항 및 제어기술의 안전성을 제고할 방안을 연구하고 있다[4].

이러한 첨단 선박에서 사용되는 하드웨어 및 소프트웨어, 육상과 선박 간의 통신 프로토콜과 선체 내 유무선 네트워크인 SAN(Ship Area Network)의 보안 문제는 [그림 2]와 같이 Smart Ship과 이해관계에 있는 Ship owner, operator, management, Shipyard, Ship equipment maker, shipper의 새로운 비즈니스 리스크로 대두되고 있다. 이러한 리스크는 조선해양산업 이해관계자 외에도 보험산업 측면에서는 조선해양산업에서의 주요 리스크 관리 전략인 해상보험(적하보험, 선박보험, 운임보험)에까지 영향을 끼칠 수 있다는 점이 제시되고 있다. 전통적인 조선해양 리스크는 총기로 무장하고 선박 또는 선원, 화물을 납치, 탈취하는 해적 활동이나 해양안전사고로 인한 환경오염 등이었으나 ICT 적용이 증가함에 따라 그 양상이 변화하고 있다.

Smart Ship은 ICT를 통해 새로운 플랫폼 기반의 자동화된 프로세스를 기반으로 인간의 항해기술과 관리능력에 의존하는 체계이나 현재 유럽 주도로 개발중인 자율운항 선박은 각 단계별로 인간의 개입을 최소화하는 선박을 일컫는다. 국내에서는 현대중공업이 2011년 3월 세계 최초로 자율운항 선박의 전단계인 Smart Ship을 개발하여 관련기술을 축적하고 있으며, 삼성중공업은 육상에서 선박 시스템을 실시간 모니터링 체계(Vessel Portal Service: VPS)를 통해



<자료> Sea Japan 2014 Environmental Technology Seminar

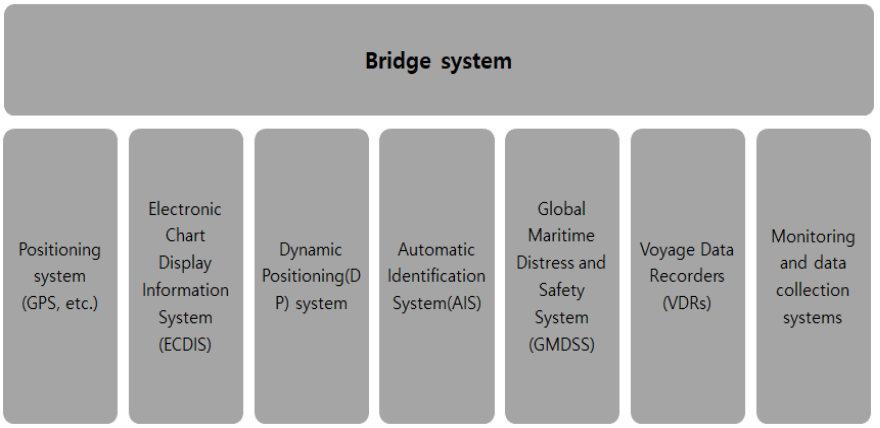
[그림 2] 선박, 데이터, 사용자 관계도

고장 여부를 진단하고 필요한 조치가 가능하도록 구현하고 있으며, 대우조선해양은 선박 모니터링 장치와 선박 설비관리 시스템 등 관련 기술을 이미 보유하고 있어 자율운항 선박에 응용할 것으로 예상하고 있다[5]. 미국, 노르웨이, 일본, 영국, 중국은 Smart Ship과 자율운항 선박을 개발하기 위해 조선해양 산업계와 ICT 기업, 정부가 협력을 공고히 하고 있다.

그러나 이러한 조선과 ICT 융합 기술들은 보안성이 확보되지 않을 경우 선박과 그 이해관계자에게 손실이 예상된다. 본 고에서는 조선해양 산업에서의 보안위협을 선박 시스템의 취약성과 사고사례를 바탕으로 살펴보고 보안 강화 동향에 대해 살펴보고자 한다.

Ⅱ. 선박 시스템의 취약성

해운과 조선에 관한 국제적인 문제들을 다루기 위해 설립된 국제기구인 IMO(International Maritime Organization)에서 발간한 “cyber security risk management guideline”에서는 선박의 취약한 시스템으로 선박 운항 및 화물관리, 승객 관리, 엔진 및 통신 시스템인 [그림 3]의



<자료> 고려대학교 정보보호대학원 자체작성

[그림 3] 선체 내 Bridge system과 연결된 주요 시스템의 구성

Bridge system을 중심으로 [표 1]과 같이 Cargo handling and management system, Propulsion and machinery management and power control systems, Access control systems, Passenger servicing and management systems, Passenger facing public networks, Administrative and crew welfare systems, Communication systems 등을 제시하고 있으나 취약한 시스템은 이에 제한되지 않는다고 명시하고 있다.

선박의 취약성 증가는 선박 내부에 ICT 시스템과 전자 장비가 증가하고 있기 때문이다. 이 가이드라인에서는 식별-보호-탐지-대응-복구 5단계의 기능으로 효율적인 cyber risk 관리 프레임워크를 제시하고 있다. 또한, IMO MSC(Maritime Safety Committee) 98차 회의(2017년 6월 20일)를 통해 사이버 보안에 대한 가이드라인을 규정하고 2021년 1월 1일부터 안전관리시스템에 사이버보안 관리 분야(Maritime Cyber Risk Management)를 포함하는 것을 권고[6]하였으며, 이 지침은 업계의 모든 조직을 대상으로 적용될 예정이다. 이 지침에서는 BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF와 UMI에서 제시하고 있는 선박의 제조 및 지원을 위한 사이버보안 가이드라인과 ISO(International Organization for Standardization)/IEC(International Electrotechnical Commission) 27001, NIST Framework을 통해 효율적인 보안관리 체계를 마련하도록 규정하고 있다.

그리고 Smart Ship, 자율운항 선박의 특성상 CPS(Cyber Physical System)로 구성되는 환경이므로 상기에서 제시된 디지털 장치와 네트워크에 대한 보호조치뿐 아니라, 원격 또는 AI기반 디지털 영상 감시체계를 통한 안전관리 체계도 요구된다.

[표 1] Target systems, equipment and technologies

시스템	상세장비
Communication systems	- integrated communication systems - satellite communication equipment - Voice Over Internet Protocols(VOIP) equipment - wireless networks(WLANs) - public address and general alarm systems
Bridge systems	- integrated navigation system - positioning systems(GPS, etc.) - Electronic Chart Display Information System(ECDIS) - Dynamic Positioning(DP) systems - systems that interface with electronic navigation systems and propulsion/manoeuvring systems - Automatic Identification System(AIS) - Global Maritime Distress and Safety System(GMDSS) - radar equipment - Voyage Data Recorders(VDRs) - other monitoring and data collection systems
Propulsion and machinery management and power control systems	- engine governor - power management - integrated control system - alarm system - emergency response system
Access control systems	- surveillance systems such as CCTV network - Bridge Navigational Watch Alarm System(BNWAS) - Shipboard Security Alarm Systems(SSAS) - electronic “personnel-on-board” systems
Cargo management systems	- Cargo Control Room(CCR) and its equipment - level indication system - valve remote control system - ballast water systems - water ingress alarm system
Passenger servicing and management systems	- Property Management System(PMS) - electronic health records - financial related systems - ship passenger/seafarer boarding access systems - infrastructure support systems like domain naming system (DNS) and user authentication/authorisation systems
Passenger-facing networks	- passenger Wi-Fi or LAN internet access - guest entertainment systems - passenger Wi-Fi or Local Area Network(LAN) internet access, for example where onboard personnel can connect their own devices - guest entertainment systems

시스템	상세장비
Core infrastructure systems	- security gateways - routers - switches - firewalls - Virtual Private Network(s)(VPN) - Virtual LAN(s)(VLAN) - intrusion prevention systems - security event logging systems
Administrative and crew welfare systems	- administrative systems - crew Wi-Fi or LAN internet access, for example where onboard personnel can connect their own devices

<자료> BIMCO

BIMCO(Baltic and international maritime conference)는 2016년 2월 1.1버전의 THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS[7]에 이어 2017년 6월에 2.0 버전을 발표하였다. 이 가이드라인에서는 선박의 ICT 환경이 고려되었으며 해사기구 및 해운회사 등의 관련 조직이 참여하였다.

Cyber security and safety management에서는 사이버보안과 안전관리를 다루고 있으며 해양 사이버보안은 탑승한 인원(승객 및 선원), 선박과 화물에 대한 무단 접속과 조작/중단, 데이터의 유실로부터 보호한다고 정의하고 있다. 주요 우려사항으로 선박의 전자차트 디스플레이

[표 2] GUIDELINES ON CYBER SECURITY ONBOARD SHIPS 주요 내용

카테고리	주요 내용
Cyber security and safety management	사이버 보안과 안전 관리를 위한 계획 수립과 절차, 범위를 설명하고 있으며 심층 방어 방법을 권장하고 있다.
Identify threats	위협의 종류를 목적과 동기로 분류하고 그룹화하여 선박과 회사에 끼칠 수 있는 영향을 설명하고 있다.
Identify vulnerabilities	선박을 구성하는 주요 시스템인 Bridge system, 화물관리 시스템, 접근제어 시스템 등의 취약성에 대해 설명하고 있다.
Assess risk exposure	위험 평가를 함에 있어서 다양한 이해 관계자를 식별하고 이에 대한 평가 방법을 설명하고 있다.
Develop protection and detection measures	발견된 위험을 보호하기 위한 기술적 보안 대책을 제시하고 있다.
Establish contingency plans	CIA 모델을 기반으로 한 비상 계획 개발에 대해 제시하고 있다.
Respond to and recover from cyber security incidents	침해사고에 대한 복구계획 수립에 대해 설명하고 있다.

<자료> BIMCO

및 정보시스템(ECDIS)의 데이터 무결성 훼손, 선박용 소프트웨어의 유지관리 및 패칭 과정에서 발생할 수 있는 장애, 선박의 운용에 중요한 센서 데이터의 손실 또는 조작을 열거하고 있다.

Identify threats에서는 해양 사이버보안의 위협을 회사, 선박, 운영과 거래(trade)로 식별하고 있으며, 금융기관, 공공기관 등 다른 비즈니스 섹터에서의 경험이 조선산업에서의 사이버공격에 대한 성공적인 경감 사례가 될 수 있음을 제시하고 있다.

Identify vulnerabilities에서는 선박에서 취약점에 노출될 수 있는 시스템을 식별하고 있다. 다만 선박과 육상(항만 또는 선박 운영회사, 해운 회사 등)과의 통신이 이루어지는 시스템인 엔진 성능 모니터링 시스템, 선박 유지관리 시스템, 화물과 승선원 관리시스템, 항해 관리시스템 등 육상에서 선박의 운항을 점검하고 관리하기 위해 통신하는 시스템을 추가로 식별하고 있다.

위험 평가에 관한 Assess risk exposure에서는 K-ISMS, ISO27001 등에서 제시하고 있는 위험평가 가이드 및 통제항목과 동일하게 위험평가의 책임은 고위 경영진에 있음을 명시하고 있다. 영향 평가는 CIA Model을 통해 평가하나 해양 산업과 선박의 환경을 고려해야 한다. 예를 들면, 민감한 정보에는 선박 위치, 시스템의 상태 및 판독 값, 화물의 세부사항, 권한, 인증서 등을 포함하도록 하고 있다. 선박의 전력관리시스템은 SCADA 시스템을 포함하고 있고 선박 전체의 전력 분배와 제어를 담당하는데, 이 시스템은 선박의 통신시스템과 연결되어 육상의 회사에서 모니터링 하도록 구성되어 있다.

보호대책에 관한 Develop protection and detection measures에서는 위험 평가 결과가 나타난 위험에 대해 고위경영진의 책임 하에 보호대책을 이행해야 한다. 보호 조치는 절차와 지침으로 구성하고 기술적인 수단과 관리적인 수단을 제시하고 있다. 특히, 보호대책으로 선박이 위성 및 무선 통신을 이용할 때 위성통신시스템과 사양을 고려하고, 운항 선박에 대한 불법적인 접속을 방지하는 방법을 고려해야 한다. 제어 소프트웨어와의 관리 인터페이스는 주로 웹 기반 사용자 인터페이스의 형태로 제공되는데 그러한 인터페이스의 보호는 선박에 설치될 때부터 고려해야 한다.

업무연속성 계획에 관한 Establish contingency plans에서는 선박의 경우 전자 항법 장비의 가용성 또는 탐색의 무결성 데이터 손실, 글로벌항법위성시스템(GNSS)의 가용성 또는 무결성 손실, 해안과의 필수적인 통신의 손실, 세계 해상조난안전시스템(GMDSS) 통신 두절, 선박의 추진시스템, 보조시스템 및 산업제어시스템을 포함한 산업제어시스템의 가용성 손실, 기타 데이터 관리 및 제어 시스템의 무결성 손실, 랜섬웨어 또는 서비스 거부공격(DoS)에 대한 손실

등을 고려해야 한다.

사고대응 계획에 관한 Respond to and recover from cyber security incidents에서는 예를 들면 전자해도시스템(ECDIS)가 악성코드에 감염되었을 때 원상 복구하는 복구계획, 사고대응 계획, 조사 계획 등을 수립해야 한다.

Ⅲ. 조선해양 산업의 사이버보안 사고사례

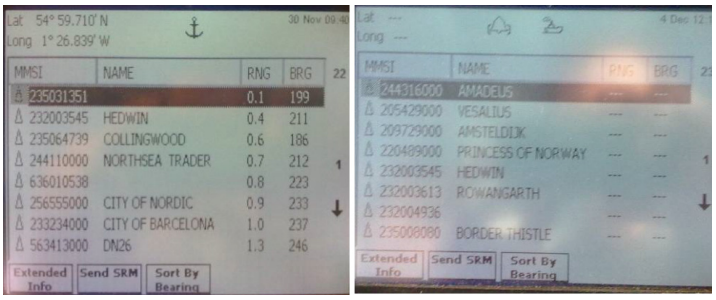
2018년 4월, 기존에 서아프리카 해역을 대상으로 선박과 선원을 납치하던 나이지리아 범죄조직이 해킹그룹과 연계하여 한국, 일본, 노르웨이 등의 해운회사의 임직원 개인정보(User ID, password)를 탈취하여 비즈니스 스캠(Business SCAM)을 시도하는 사례가 발생하였는데 이는 전통적인 해적이 사이버 공격 기술을 활용하였다는 데 의미가 있다.

2018년 3월 네덜란드 해운회사의 e-메일 시스템이 자동전달 기능을 통해 외부 공격자에게 최소 11개월 동안 포워딩되어 호주 국적 임직원 개인정보 500여건의 민감정보가 유출된 것으로 확인되었다.

2017년 12월 영국과 싱가포르의 글로벌 해운회사들이 해킹으로 인해 데이터가 유출되거나 시스템이 다운된 사고가 발생하였다. 특히, 영국의 선박회사의 경우, 제3자의 불법적인 접근이 1년 가까이 지속되었으며, 그 영향으로 회사가 저장하고 있던 개인식별정보 및 민감정보가 유출되어 해커가 이를 빌미로 회사를 협박한 사고로 이어졌다.

2017년 12월 선박에서 이용되는 위성통신장치시스템에서 심각한 취약점이 발견되었으며, 해당 취약점을 이용하여 공격자가 해상에서 운항중인 선박의 위성통신시스템과 내부 엔진장치, 운항장치 등에 침투할 수 있음이 밝혀졌다. 그러나 이 시스템은 2017년 6월부로 EoS(End Of Services)되어 취약한 시스템을 탑재한 선박은 패치 전까지 위협을 내재하고 있었으나 선박시스템의 경우 수명 연한이 20~30년 이상으로 폐기 전까지는 내부 시스템을 업그레이드 하거나 패치하기 어려운 문제점을 내포하고 있었다. 선원을 대상으로 한 설문조사에 따르면 응답자 중 43%가 선박시스템의 악성코드 감염을 경험했다고 응답하였는데, 패치되지 않은 시스템에서의 악성코드 위험도는 육상에서 운영중인 정보시스템의 악성코드 보안대책보다 더 강화되어야 할 것이다.

2017년 8월 미 해군함정이 싱가포르 해협에서 유조선과 충돌하여 승조원 10명이 사망한 사건이 발생하였는데, 이후 언론에서는 사이버공격에 의한 개연성을 제기하였고, 이 함정이



<자료> Alan Grant, The Potential effects of GPS Jamming on Marine Navigation, 2013. 8.

[그림 4] Normal AIS(좌), GPS Jamming Attack AIS(우)

속한 미해군 7함대에서는 앞선 6월에 이지스함이 필리핀 선적 컨테이너선과 충돌사고가 발생한 바가 있는 등 최첨단 군용선박의 연이은 사고가 문제가 되었다.

2017년 8월 알리안츠의 선박 안전과 위험 보고서에 따르면, 2016년 3월 북한의 사이버공격으로 한국 선박의 GPS 시스템이 무력화된 사건을 계기로 선박 안전에 사이버보안 영향이 증대할 것으로 예상하였다[8]. 2015년 개최된 Defcon에서 GPS spoofing 취약점을 이용하여 선박 또는 드론, 자동차, 네비게이션에 잘못된 위치정보를 MITM(Man in The Middle) attack으로 전송하는 기술을 발표하였다. 또한, 2017년에 발생한 GPS 보안 사건의 경우, 한 선박이 러시아 Novorossiysk 항만으로 GPS 정보를 입력하고 항해중에 목적지가 32km 떨어진 Gelendzhik으로 설정된 것으로 최초의 GPS misdirection으로 보고되고 있다.

2017년 6월 세계 최대의 해운회사인 머스크 라인의 우크라이나 지점에서 사용 중인 회계소프트웨어의 취약점을 통해 감염된 NotPetya 랜섬웨어가 전세계 지점과 항만 등에 전이되어, 이로 인한 추가 피해 방지를 위해 전체 IT시스템을 강제 다운시키고 시스템 복원을 위해 3개월간에 걸쳐 45,000대의 PC, 2,500개의 애플리케이션을 재설치한 사건이 발생하였다. 이 때문에 머스크 라인의 총 피해 추산액은 약 3,000억으로 집계되었다. 감염 및 전파 증상이 발견된 초기에 신속한 판단을 내려 추가 피해 방지를 위해 IT시스템을 강제 다운하고 트위터 등을 통해 피해 및 복구활동 조치 사항을 전파함으로써 고객 이탈을 방지하였다.

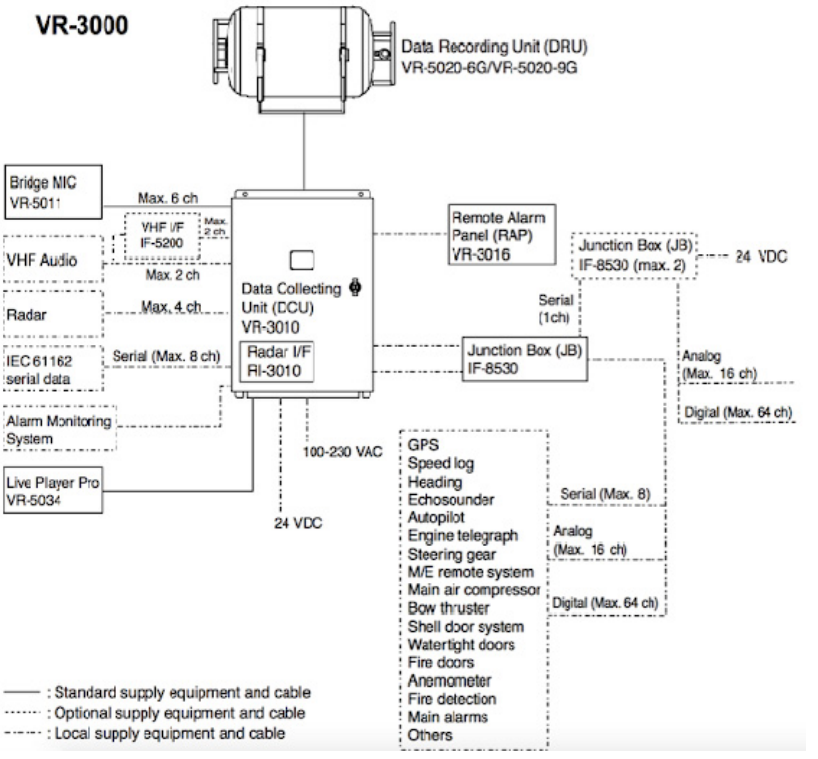
2017년 2월 독일 소유의 컨테이너선(8,250 TEU급)이 해킹되어 10시간 동안 선박의 통제권을 잃어버리는 사건이 발생하였는데 이를 원상 복구하기 위해서 선박은 운항을 중단하고 IT시스템 복구 작업을 실시하였다[9]. 이 사건은 선박의 Navigation System을 원격으로 공격한 해커에 의해 실행되었으며 경로와 방법은 알려지지 않았다. 컨테이너선의 경우 대량의 화물을 운송하고 있어 화물운송 지연 및 선박 연료비의 증가 등으로 인한 경제적 손실이 발생할 수 있는

사건이었다.

2016년 8월 미국 및 전 세계 13개 항만에서 사용중인 미국의 Cargotec 주식회사의 선박 Navis 웹 기반 시스템에서 Zeroday 취약점인 sql-injection(CVE-2016-5817)이 발견되어 공개되었으며, 이로 인해 해양 시스템의 패치 관리에 대한 이슈가 제기되었다[2]. 이 취약점을 이용한 exploit code가 유통되고 있어 패치되지 않은 해당 시스템은 여전히 위험에 노출되어 있을 것으로 보인다.

2016년 프랑스 방산 회사에서 스텔스 기술 등 해군 잠수함 관련 자료 22,400페이지가 전직 해군 장교에 의해 유출되었다. 이 사건이 시사하는 것은 조선해양 관련 특수기술은 사이버보안의 문제뿐만 아니라 영업비밀보호의 측면도 고려해야 한다는 것이다.

2016년 3월 해적이 글로벌 해운사의 선박을 납치한 후 특정화물이 적재된 컨테이너만을 탈취하고 이탈한 사건이 발생하였다. 이후 해당 회사는 선적화물 관리시스템과 선하 증권 관리 시스템을 조사한 결과 시스템에서 악성코드가 발견되었다. 해적이 해커를 고용하여 해운회



<자료> https://ioactive.com/maritime-security-hacking-into-a-voyage-data-recorder-vdr/, 2013. 8.

[그림 5] VDR architecture

사 시스템에 침입하여 선적화물에 대한 데이터베이스를 감시해온 것으로 추정되고 있다. 이는 해양 사이버보안은 선박뿐만 아니라 선박의 운항과 화물을 관리하는 시스템까지 광의적으로 포함해야 함을 의미하고 있다.

2015년에 발견된 선박에서의 BlackBox 역할을 하는 VDR(Voyage Data Recorder) 시스템에서 취약점이 발견되어 원격에서 VDR에 기록된 데이터의 삭제 및 변조가 가능하다고 발표되었다. [그림 5]의 VDR architecture를 살펴보면 GPS, Speed log, Heading 등의 중요한 운항 정보가 Serial, Analog, Digital로 DCU(Data Collecting Unit)에 수집된다. 이에 따라 선박 사고 조사 시 해당 취약점의 패치 여부와 해당 취약점에 의한 원격에서의 VDR 데이터 위변조 여부를 확인해야 디지털 증거의 무결성이 증명될 것으로 판단된다.

2014년 10월에 선박 등에 연료를 공급하는 해상급유 주요 기업인 WFS(World Fuel Services)가 Email SCAM으로 1,800만 달러의 사기 피해를 입었으며, 이후에도 Business SCAM이 꾸준히 지속되었고 2018년 4월에는 해운사를 타깃으로 한 집중공격이 발생하였다[10].

2013년 10월 마약 밀매업자들이 해커를 고용하여 벨기에 Belgian port of Antwerp 항만 제어 시스템에 침입하여 코카인과 헤로인을 선적한 컨테이너를 확인하고 합법적 화물주가 도착하기 전에 반출하였다. 해커는 Trojans 첨부파일 이메일을 통해 관련 PC를 감염시키고, 사무실에 침입하여 비밀번호를 탈취하는 USB를 설치하였는데, 해커는 이메일을 통한 공격 방법과 직접 사무실에 침입하여 [그림 6]과 같은 소프트웨어에 접근하기 위해 PC에 키로거를 꽂는 방법을 활용한 것이다[11].

<자료> BBC의 경찰 인터뷰 방송 내용 캡처

[그림 6] 해커가 공격한 선박 화물관리 소프트웨어

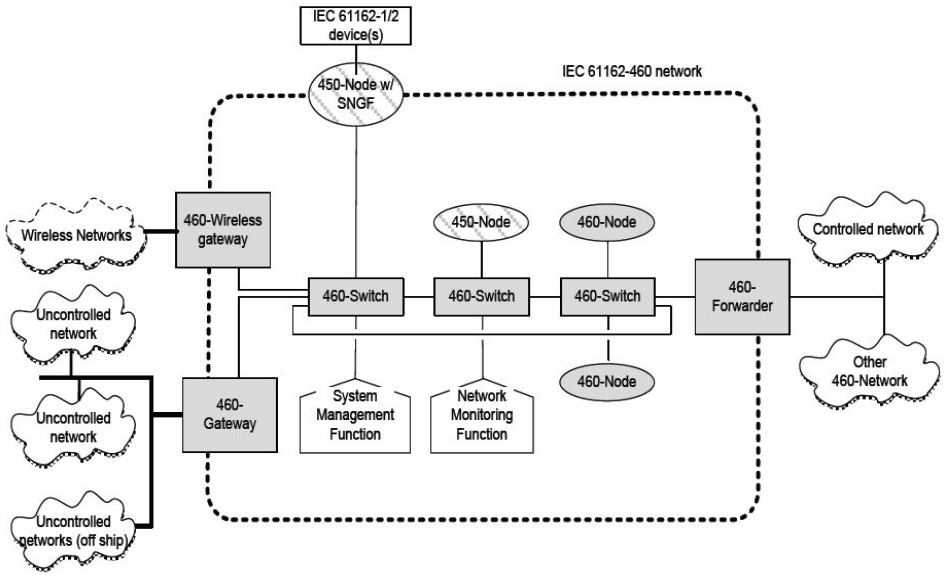
2012년 범죄조직에서 고용한 해커가 호주 세관과 Cargo System에 침입하여 세관 당국이 의심하는 선적 컨테이너(선적화물) 정보를 파악하는 사건이 발생하였다[12].

2011년 8월 Iranian Shipping Line 서버에 해커가 침입하여 요금, 적재화물, 화물번호, 운송날짜와 장소 데이터를 손상시켰다[13].

Ⅳ. 선박 보안 강화를 위한 동향

ENISA에서는 2011년 해양 산업 부분의 사이버 보안 리스크를 분석하고 관련 연구[14]를 통해 문제점을 파악하고 단기, 중기, 장기적인 관점에서 활발한 연구를 추진하여 왔다. 당시까지만 해도 IMO 등 관련 국제기구에서 사이버 보안에 대한 가이드라인 등이 없었고, 선박의 위성 네트워킹도 제한적이었으며, 선박 시스템에 ICT가 이용되는 것은 극히 제한적이었다. 현재와 같이 자율운항 선박의 건조를 준비하고 있는 환경에서는 이 같은 기초 데이터를 바탕으로 안전한 항해를 위한 체계 마련이 요구될 것이다.

선박과 관련된 해양 산업 전반에 걸친 사이버 보안 이슈로 인해 선박 장치와 내부 및 외부 시스템으로부터의 보안 위협으로부터 장비들을 보호하기 위한 선박 장치, 선박 네트워크, 선박 게이트웨이의 보안 구조와 기능 요구사항을 2015년 8월에 [그림 7]과 같이 국제표준 IEC 61162-460으로 정의하였다.



<자료> IEC(International Electrotechnical Commission)

[그림 7] IEC 61162-460 구조도

TTA에서는 해양 및 선박 관련 표준안을 설계하였는데 선박 장치 및 시스템들에 안전하고 신뢰성 있는 보안 기능을 제공하기 위한 요구사항으로 선박 보안 이더넷 인터페이스 규격을 정의[15]하였고, 선상에서의 사이버 시스템의 보안을 유지하고 필요한 절차 및 조치에 관한 사

항을 선주와 운영자에게 제공하기 위한 선박 사이버보안 관리에 관한 지침을 제정하였다[16].

한국선급은 선박의 사이버 보안 검사를 위한 선급기술규칙으로 해상 사이버보안 관리시스템(Cybersecurity Management System)을 3가지 유형으로 분류하여 선급부호를 부여하고 있으며, 각 레벨별로 요구하는 통제항목은 상이하고 문서검토와 현장검사를 진행하게 된다. 레벨 1은 기본적인 사이버보안 관리 시스템을 갖춘 선박이며, 레벨 2는 검사항목을 만족하는 강화된 사이버보안 관리 시스템을 갖춘 선박이며, Level 3는 고도의 사이버보안 관리 시스템을 갖춘 선박을 말한다. 이외에도 미국 선급협회(ABS), 영국 로이드(LR) 등도 사이버보안 기술 표준안과 인증제도를 시행하고 있다.

V. 결론

4차 산업혁명 시대에서 자율주행자동차와 AI 등 다양한 키워드가 각광받고 있는 가운데, 조선해양 산업에서도 Smart Ship을 바탕으로 한 자율운항 선박 분야가 새로운 패러다임으로 떠오르고 있다. 특히, 자율운항 선박을 포함하여 ICT 기술과 결합된 조선해양 분야에서는 정보보호 측면에서 충분히 고려가 이루어져야 한다. 기존의 정보보호 기술이 적용되기 위해서는 선박과 육상 간의 네트워킹이 가능한 해양 위성통신시스템에 대한 보호대책과 선박의 위치정보가 위변조되지 않도록 보호대책이 요구된다.

최근 조선해양 산업에서의 사이버보안 사고사례를 살펴보면 선박-육상 이해관계자 시스템의 보안 취약점을 이용한 공격에 의해 해운물류 시스템 또는 항만 시스템이 피해를 입는 사례가 관찰되고 있고, 선박 자체의 정상 운항을 방해하는 행위도 발생하였다.

기존에는 선박의 보안위협으로는 해적, 화재, 화물분실 등의 물리적인 위해요인이었으나 ICT와의 융합을 통해 위협의 범위가 넓어졌다. 자율운항 선박은 정교한 시스템으로 선박 자체에 사이버 방어체계와 물리적 보호체계가 동시에 갖추어져야 할 필요성이 있다. 예를 들면, 선박에 접근할 수 있는 경로에는 위성통신망을 통한 원격 접근, 내부 시스템을 이용한 로컬 접근, 선박 내 시스템으로의 접근 등이 있으며, 이러한 정보시스템을 통한 원격/로컬 접근에 대한 대책 외에도 선박에 직접 침입하여 시스템을 파괴하는 것에 대비하기 위한 접근통제 대책 등이 요구된다.

K-ISMS, ISO27001 통제항목에서의 물리적 보호대책이 조선해양 분야 특히 본 고에서 언급하고 있는 자율운항 선박의 보호대책에서도 요구되며, 조선해양 산업의 특수한 환경을 고려

한 보호대책이 연구/발전되어야 한다. 특히, 선체 내 ICT를 보호하는 사이버 공간과 선체와 인명, 화물을 보호하는 물리적 환경을 고려한 융합보안과 CPS(Cyber Physical System) 보안체계가 구성되어야 한다. 선박 건조단계에서는 ECDIS 및 각종 선박 제어시스템과 IoT 장비들의 보안취약성에 대한 보호대책을 강구해야 하며 자율운항을 위한 센서 네트워크가 안전하게 보호되는 환경이 필요하다.

우리나라는 조선해양 분야에서 세계 최고의 기술력과 경쟁력을 보유하고 전 세계 바다를 지배하여 왔다. 비록 최근 어려운 상황에 직면하고 있지만 4차 산업혁명 시대를 맞이하여 자율운항 선박이 다시 한번 조선해양 강국으로 발돋움할 원동력이 되기를 기대하며, 이를 위해 무엇보다도 중요한 해양안전관리 측면에서 사이버보안, 정보보호 분야가 뒷받침되길 바란다.

[참고문헌]

[1] 해양수산부 홈페이지, “차세대 선박운항장비 개발”, 2014. 11. 13.
[2] 4차산업혁명위원회, “혁신성장을 위한 사람 중심의 4차 산업혁명 대응계획”, 2017. 11. 30.
[3] 한국정보통신기술협회(TTA) 정보통신용어사전
[4] 한국과학기술기획평가원, “22년 자율운항선박 상용화 행보 가속”, 2018. 6. 11.
[5] KB금융지주, “자율운항선박의 현재와 미래”, 2018. 1. 17.
[6] IMO, MSC-FAL.1/Circ.3 “GUIDELINES ON MARITIME CYBER RISK MANAGEMENT,” 2017. 7. 5.
[7] BIMCO, “THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS,” 2017. 7.
[8] Allianz Global Corporate & Specialty, “Safety and Shipping Review 2017,” Aug, 2017.
[9] IHS Markit, “Hackers took ‘full control’ of container ship’s navigation systems for 10 hours,” 2017. https://goo.gl/xtkCTr
[10] Ship&Bunker, “WFS In Court Over $18M Bunker Scam Claim,” 2014. https://goo.gl/2PdZmQ
[11] VICE, “To Move Drugs, Traffickers Are Hacking Shipping Containers”, 2013, https://goo.gl/YqZ4ne
[12] KASPERSKY LAB., “Maritime industry is easy meat for cyber criminals,” 2015. https://goo.gl/C28PUo
[13] CSOonline, “Defeating 21st Century pirates: the maritime industry and cyberattacks,” 2018. https://goo.gl/w7df2s
[14] ENISA, “ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARITIME SECTOR,” 2011. 11.
[15] 한국정보통신기술협회, “선박 보안 이더넷 연결 인터페이스 -제1부: 일반 요구사항(ttak.ko-11.0203-Part1)”, 2015. 12. 16.
[16] 한국정보통신기술협회, “선박 사이버보안 관리지침(기술보고서)”, 2017. 11. 1.