정 보 보 호 학 회 지
제 33 권 제6호, 2023. 12

해양선박 대상 사이버 복원력 연구 동향

고 아 름*, 최 희 원**, 전 승 호***, 서 정 택***

요 약

현대 해양선박은 PLC 등 기존의 OT 시스템과 선박자동식별시스템 등 IT 시스템의 접목으로 스마트 선박, 자율운항 선박으로 진화되고 있다. 하지만 이러한 기술 통합은 공격이 가능한 접점이 늘어나며, 이는 사이버보안 위협을 증가시키고 있다. 선박은 대부분 항만으로부터 고립된 환경에서 운영되기 때문에 사이버공격이 발생 시 외부의 기술 지원이나 긴급 대응이 어려워진다. 이러한 배경으로 해양선박을 대상으로 하는 사이버 복원력은 해양선박 환경에서 중요한 개념으로 자리 잡고 있다. 본 논문은 해양선박 환경 표준 통신 네트워크인 SAN을 분석하고, 사이버 복원력을 소개한 후, NIST의 사이버 복원력 모델을 기반으로 해양선박 대상 사이버 복원력 연구를 분석한다.

Ⅰ. 서 론

최근 해양선박 기술은 첨단 ICT(Information and Communication Technology) 기술을 도입하여 기존 선박에 정보통신, 센서, 스마트 기술 등을 융합하여 시스템이 선박을 제어하는 스마트 선박을 넘어 자체 진단 및 관리를 수행하며 최소한의 에너지로 안전하게 자율적으로 항해할 수 있는 자율운항 선박으로 진화하고 있다. 하지만, 해양선박 시스템에서 운항 제어를 맡는 OT(Operational Technology) 영역과 자율운항 기능을 위해 외부 네트워크와 연결되는 IT(Information Technology) 영역의 융합으로 외부 네트워크 접점이 증가함에 따라 사이버공격에 노출될 위험이 커졌다[1].

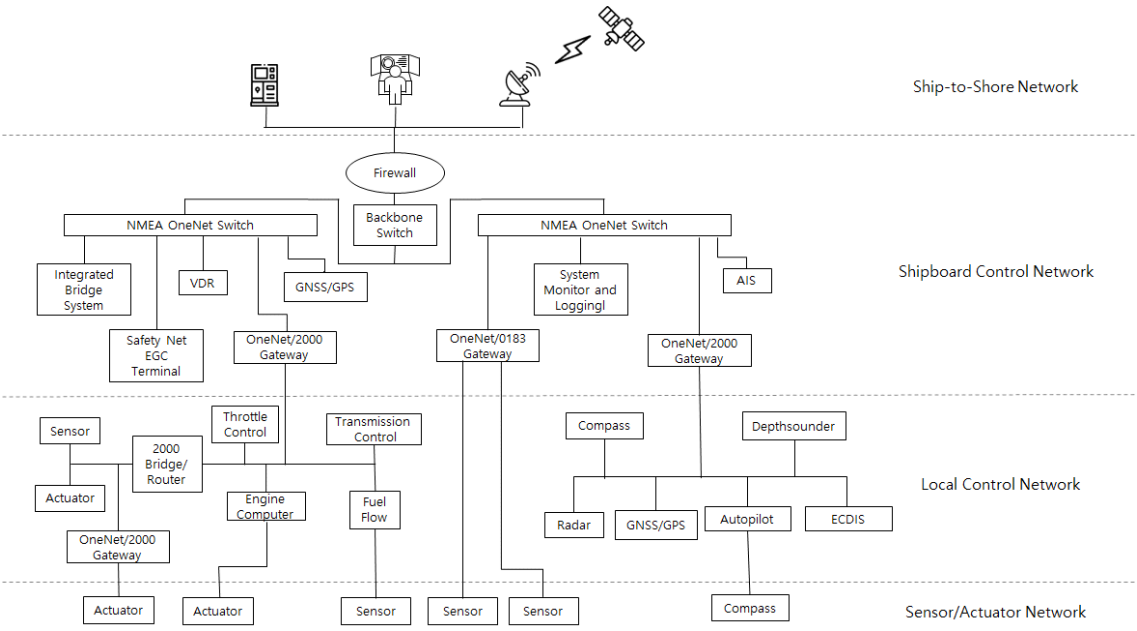
사이버공격이나 기술적 장애 발생 시, 시스템 복구 시간을 단축하고 피해를 최소화하기 위해 실시간 대응은 필수적이다[2]. 그러나 선박은 운항 시간의 대부분을 항만과 멀리 떨어진 고립된 환경에서 운항하기 때문에 사이버공격 발생 시 외부의 기술 지원이나 긴급 대응이 어려울 수 있다. 이는 사이버공격이나 기술적 장애가 발생했을 때 즉각적인 대응을 제한하여 선박의 안전과 운영 효율성에 위험을 초래할 수 있다.

이러한 배경을 바탕으로 해양선박 대상 사이버 복원력은 해양선박 환경에서 중요한 개념으로 자리 잡고 있다. 사이버 복원력(Cyber Resilience)이란 사이버 자원을 사용하거나 이에 의존하는 시스템에서 발생하는 사이버공격 또는 침해에 대해 예측하여 사이버공격으로부터의 피해를 최소화하고 적응하며, 손상된 자산을 회복하는 능력을 일컫는다[3]. 해양선박의 안전과 보안에 대한 글로벌 표준 설정 기관인 국제 해사 기구(IMO, International Maritime Organization)는 2021년 1월 1일부터 발효된 IMO 결의안 MSC.428(98)을 통해 해운 산업에서 사이버 위험에 대한 운영상 복원력의 중요성을 강조하였으며[4], 국제선급협회 IACS[5], 국제 해운 협회 BIMCO[6], 노르웨이 선급 협회 DNV[7]에서도 해양 사이버보안 및 복원력의 중요성을 강조하였다. 하지만 현재로서 해양선박을 대상으로 하는 사이버 복원력 연구가 부족한 실정이다.

이에 따라 본 논문은 해양선박 대상 사이버 복원력 연구들의 동향을 분석한다. 4개의 연구를 분석하였으며 사이버 복원력의 대상이 되는 선내 시스템별로 분석하였다.

본 논문의 구성은 다음과 같다. 2장에서 해양선박의 표준 통신 네트워크 구조에 대해 분석하고, 3장에서 사이버 복원력의 개념을 소개한다. 4장에서는 해양선박을 대상으로 하는 사이버 복원력 연구 동향을 제시하고 5장에서는 결론을 제시한다.

이 논문은 2023년도 정부(과학기술정보통신 부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (RS-2023-00241376, 해양 선박 공공 서비스·인프라의 암호화 사이버위협에 대한 네트워크 행위기반 보안관제 기술 개발)
* 가천대학교 정보보호학과 (학부생, ko6103@gachon.ac.kr)
** 가천대학교 컴퓨터공학과 (대학원생, chw1226@gachon.ac.kr)
*** 가천대학교 컴퓨터공학부 (교수, shjeon90@gachon.ac.kr, seojt@gachon.ac.kr)



〔그림 1〕 SAN 네트워크 구조도

Ⅱ. SAN(Ship Area Network)

본 장에서는 해양선박의 표준 통신 네트워크 구조인 SAN(Ship Area Network)에 대하여 분석한다. SAN은 ETRI(Electronics and Telecommunications Research Institute)와 현대 중공업이 공동으로 개발한 표준으로, IEC 61120-450 표준에 채택되었며, 선박 내에 구축되어 제어 명령, 상태 정보, 문서 및 도면 정보 등을 교환할 수 있도록 제공되는 백본 네트워크를 의미한다[8]. 선박 네트워크는 선박 내 기계장치 제어를 중앙에서 자동으로 가능하게 하므로 선박 자동화에 반드시 필요한 요소이다. SAN을 포함한 전체 네트워크 인프라는 소규모 현장 네트워크부터 전 세계 네트워크까지 계층적 아키텍처를 가지고 있다. 해당 아키텍처는 선박 대 지상 네트워크 (Ship-Shore Network), 선박 제어 네트워크(Shipboard Control Network), 로컬 제어 네트워크(Local Control Network), 센서/액추에이터 네트워크(Sensor/Actuator Network)로 구성된다. [그림 1]은 SAN 네트워크의 구조도를 나타낸다.

2.1. 선박 대 지상 네트워크(Ship-to-Shore Network)

선박 대 지상 네트워크는 최상위 네트워크로 선박 영역 네트워크, 위성 모뎀 및 안테나, 위성 공간 및 사용자 세그먼트, 원격 유지보수 서버 및 클라이언트를 포함한 원격 유지보수 서비스를 제공한다[9]. 해당 네트워크에서는 Inmarset, Irdium 및 Very Small Aperture Terminal(VSAT)과 같은 위성 통신이 일반적으로 통신 수단으로 활용된다[10]. 따라서 위성 통신의 취약점을 통한 선박에 대한 원격 접근 및 시스템 원격 제어와 같은 사이버공격이 발생할 수 있다. 2017년 2월, 해커가 오래된 펌웨어 사용 및 기본 암호를 사용하는 해상 위성통신의 취약점을 활용하여 키프로스에 지부티로 향하던 독일 소유 8.250TEU 컨테이너의 화물 네트워크 컨트롤 시스템을 장악했던 사이버공격 사례가 있다[11].

2.2. 선박 제어 네트워크(Shipboard Control Network)

NMEA(National Marine Electronics Association) 및 이더넷(Ethernet)을 기반으로 한 게이트웨이와 로컬 제어 네트워크의 융합한 형태로, 선박 내의 네트워크 통신은 IEC 611621-450 표준 프로토콜을 준수하며 UDP(User Datagram Protocol) 멀티캐스트를 활용함으로써 효율적이고 실시간성의 특징을 갖는 전송 모드를 제공한다[9]. 해당 네트워크는 시스템 모니터링, AIS(Automatic Identification System), GNSS(Global

Navigation Satellite System) 등을 포함하며 하위 레벨의 네트워크 내 시스템에 대한 모니터링을 수행한다[12]. C4ADS(Center for Advanced Defense Studies)는 2016년 2월 이후 2019년 초까지 러시아 영해 외부에 위치한 선박이 GNSS 스푸핑공격의 희생양이 된 사례를 최소 7,910건 감지했으며 잠재적으로 해상 항해 안전에 위험을 초래할 수 있다고 발표하였다[13]. 라타키아시 남동쪽에 위치한 Khmeimim 공군기지에서 GPS 스푸핑 송신기가 발견되었다.

2.3. 로컬 제어 네트워크(Local Control Network)

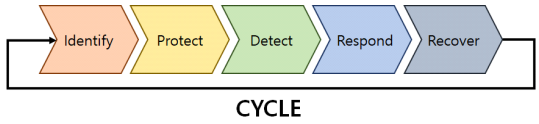
컨트롤러, I/O 모듈 및 기기로 구성된 로컬 네트워크로, 경보 모니터링 시스템, 브릿지 조종 시스템, 항해 데이터 레코드 및 통합 브릿지 시스템과 같은 단일 목적을 이루는 네트워크이다[9]. 네트워크 내부의 통신은 Ethernet 또는 Profifbus 및 CANopen과 같은 필드 버스 기술을 활용하며, 선박 자동화 시스템의 로컬 제어 네트워크는 IEC 61162-450 인터페이스를 지원하지 않는 시스템이나 로컬 네트워크에 대한 게이트웨이 역할을 한다. 해당 네트워크는 GPS 수신기, 자동조종 장치, 수심 측심기, 항법 계측기 및 항해 차트 플로터 등의 통신을 수행한다[14]. 2022년 3월에는 Borholmslinjen (Borholms 노선)의 페리가 전파 방해 사고로 인해 2시간 동안 지연되었다[15]. 페리에 탑승한 두 대의 동유럽 트럭에는 전파 방해 장비가 포함되어 페리의 GPS 시스템이 오작동한 것으로 알려졌다.

2.4. 센서/액추에이터 네트워크(Sensor/Actuator Network)

센서와 액추에이터를 포함하는 현장 네트워크로 로컬 제어 네트워크 및 선박 제어 네트워크와 PLC(Programmable Logic Controller), HMI(Human Machine Interface)와 같은 현장 장치의 제어 및 모니터링 정보를 송수신한다[9]. SIS(Ship Information System)은 센서/엑추에이터 네트워크를 통해 센서 및 엑추에이터와 명령 및 제어 통신을 이룬다[16]. 2021년 이슬람 혁명수비대(IRGC)는 평형수 관리 시스템(BWMS, Ballast Water System)에 대한 사이버공격을 통해 선박을 침몰시키는 공격 시나리오가 유출되었다[17]. 해당 공격 시나리오는 위성통신 취약점을 통해 원격으로 선박 내부의 HMI에 접근하여 선박 내부의 현장 장치인 평형수 관리 시스템을 조작하는 것을 계획하였다.

Ⅲ. 사이버 복원력

사이버 복원력 개념은 2012년 다보스에서 개체 된 세계경제포럼(WEF:World Economic Forum)에서 처음 논의 되었다[18]. 사이버 복원력은 비즈니스 연속성, 정보 시스템 보안 및 조직 복원력을 통합한 개념이다[19]. 이는 사이버공격에 대한 대응 전략뿐만 아니라, 발생 가능한 피해를 최소화하기 위해 조기에 대비하고 회복하는 시스템을 의미한다[20]. 시스템의 지속성과 견고성은 조직이 경쟁에서 우위를 차지하기 위한 중요한 평가 요소로 간주되며, 두 가지 기능은 예측 가능한 공격에 대응하여 안전한 상태를 유지할 수 있어야 한다. 따라서 조직은 사이버공격 및 자연재해와 같은 이례적인 상황에서도 빠르게 적응하고 복원 및 보안 위험 완화 기능을 제공할 수 있어야 한다[21]. NIST(National Institute of Standards and Technology)에서 발표한 사이버 복원력 모델은 [그림 2]와 같이 5단계로 구성되며, 순환구조이다.



〔그림 2〕 사이버 복원력 모델〔22〕

- 1 단계: 식별(Identify)
  조직 내의 물리적인 자산과 데이터 자산을 정기적으로 식별하고 기록하는 데이터 인벤토리를 유지한다. 식별된 데이터 자산은 적용 가능한 보안대책과 매핑한다. 이를 통해 조직은 보유하고 있는 자산을 효과적으로 관리하고 보안 규제에 대한 요구사항을 충족시킬 수 있다.
- 2 단계: 보호(Protect)
  조직 내의 일원이 보안대책에 대해 명확히 이해함으로써 관리 대상 자산을 사이버공격으로부터 보호할 수 있도록 한다. 이를 통해 사이버 내구성을 유지하고 사이버공격을 방지할 수 있다.
- 3 단계: 탐지(Detect)
  자산 간의 네트워크에 사이버공격 탐지 도구 등을

통해 사이버공격을 탐지 및 분석한다. 이를 통해 조직은 다양한 보안 공격에 대해 대비할 수 있다.

- 4 단계: 대응(Respond)
  사이버공격이 탐지되었을 경우, 신속하고 효과적으로 대응한다. 이를 통해 사이버공격으로 인해 발생하는 피해를 최소화할 수 있다.
- 5 단계: 복구(Recover)
  공격 대상 자산을 초기 상태로 되돌리고 이미 발생한 사이버공격이 재발할 가능성을 고려하여 해당 자산을 보완한다. 이를 통해 차후에 발생할 사이버공격에 대해 미리 예방할 수 있다.

Ⅳ. 해양선박 대상 사이버 복원력 연구 동향

본 장에서는 2019년부터 2023년까지 나온 해양선박을 대상으로 한 사이버 복원력 연구를 2장에서 소개한 NIST의 사이버 복원력 모델을 기반으로 분석한다. [표 1]은 조사한 연구들의 목록이며, [표 2]는 NIST의 사이버 복원력 모델을 기반으로 분석하여 요약한 표이다.

〔표 1〕 선박 대상 사이버 복원력 연구 목록

연구	대상	요약
〔23〕	All-Round	온톨로지 기반 선박 대상 사이버 복원력 프레임워크 개발
〔24〕	GNSS	Likelihood Field 접근 방식을 통한 보조 GNSS 독립적 위치 확인 시스템과 GLRT를 기반으로 한 통계적 변화 탐지기 제안
〔25〕	SIS	선박 정보 시스템(SIS) 대상 사이버 복원력 프레임워크 및 동형 암호화 기술과 몬테카를로 알고리즘을 결합한 검색 엔진 개발
〔26〕	PLCs	소프트웨어 다양화와 하드웨어 중복성을 결합한 쿼드 중복 PLC 아키텍처 제안

4.1. All-Round

Helmar 외 3인[23]은 온톨로지 기반으로 해양선박 대상 사이버 복원력 프레임워크를 제안하였다. 해당 연구에서 제안된 프레임워크는 사이버공격을 탐지하는 보안 정보 및 관리 시스템(SIEM, Security Information and Event Management Systems)을 온톨로지 및 추론기(Inference System)와 결합하여 사이버공격에 즉각적으로 대응하고 시스템을 복구한다. 해당 연구에서 제시한 프레임워크는 PCS(Port Community Systems) 환경에 적용하여 검증되었다. PCS는 터미널 운영자, 선주, 항만 IT 운영자 등 다양한 이해관계자가 서로 네트워크를 형성하는 분산 시스템의 중심 부분이다.

- 식별(Identify)
  선박 내 IT 자산의 물리적인 위치 정보, 초기 접근 자산 정보, IT 자산 간의 물리적 연결 정보, 보안 대책이 적용 가능한 IT 자산 간의 구간 정보를 포함하는 온톨로지를 개발한다.
- 보호(Protect)
  추론기를 활용하여 개발된 온톨로지를 기반으로 주어진 사이버공격 상황에 대한 대응 전략을 도출하여 시스템을 보호한다.
- 탐지(Detect)
  SIEM을 활용하여 보안 툴로부터 수신받은 정보를 기반으로 하드웨어 및 소프트웨어를 포함한 IT 자산의 이상 동작을 탐지하고, 탐지된 이상 동작이 사이버공격으로 인한 이상 동작인지의 여부를 판별한다.
- 대응(Respond)
  손상된 IT 자산의 구성 요소에 대한 정보를 온톨로지에 전달하고, 추론기를 활용하여 사이버공격으로 인한 시스템 전체의 파급력 예측 및 추가적인 사이버공격으로 인한 위협과 공격 대상이 될 IT 자산을 식별한다. 식별된 IT 자산에 적용 가능한 보안대책을 평가하여 가장 효과적인 보안대책을 도출한다.
- 복구(Recover)
  추론기를 통해 사이버공격에 대한 대응이 효과적으로 되었는지를 확인하고, 대응이 효과적으로 수행되었다면 이를 SIEM에게 전달한다. 대응 이후에도 사이버공격이 지속되는 경우, 사이버공격으로 인한 위협이 완전히 제거될 때까지 Respond 단계를 반복한다.

4.2. GNSS

위성 항법 시스템(GNSS)은 내비게이션 및 위치 측정에 사용되는 시간과 궤도 정보를 방송하는 위성 네트워크이다[27]. 해당 시스템은 선박의 위치, 속도 및 정확한 시간을 제공하며, 이를 통해 항해자는 선박의 정확한 위치를 파악하여 안전한 항로를 결정하고, 다른

선박과의 충돌 위험을 감소시킬 수 있다.

Dagdilelis 외 3인[24]은 GNSS 신호의 정확성과 신뢰성을 지속적으로 감시하고 검증하는 통계적 검정 방법인 GLRT(Generalized Likelihood Ratio Test)기반 통계적 변화 탐지기와 보조 GNSS 독립적 위치 확인 시스템을 제안하였다. 해당 연구는 덴마크 남부 푸텔 군도에서의 해상 시험 중 수집된 실제 항해 데이터를 기반으로 한 스푸핑 공격을 시행함으로써 제안된 시스템이 선박의 위치를 정확하게 추정하고 공격을 효과적으로 탐지하였다. 통계적 변화 탐지기는 NIST 사이버 복원력 단계의 탐지와 대응에 해당될 수 있으며, 보조 GNSS 독립적 위치 확인 시스템은 복구에 해당될 수 있다.

- 탐지(Detect)
  통계적 변화 탐지기는 확률 분포인 가우스 모델과 연속 확률 밀도 함수를 추정하는 비모수적 방법인 KDE(Kernel Density Estimation)에 따른 변화분석을 통해 GNSS 측정 위치와 추정 위치 간의 차이를 모니터링함으로써 사이버공격을 탐지한다.
- 대응(Respond)
  사이버공격이 탐지되면, 해당 GNSS 신호는 격리되고 위치 정보에서 제외된다. 이는 잘못된 GNSS 데이터로 인한 추가적인 오류를 방지하고, 시스템의 정확성을 유지하는데 중요한 역할을 한다.
- 복구(Recover)
  보조 GNSS 독립적 위치 확인 시스템은 두 단계로 이루어지며, 첫 번째 단계에서는 레이더 이미지에서 검출된 해안선 특징과 전자 항해 차트 (ENC, Electronic navigation Chart)에서 추출한 해안선 특징을 확률적으로 매칭하여 대략적인 위치를 추정한다. 두 번째 단계에서는 레이더로 감지된 부표나 위치 정보를 전달하는 장치인 비콘과 같은 항법 표시를 ENC의 동일한 객체와 연관시킨다. 이후 삼각 측량을 통해 한 지점에서 다른 지점까지의 방향을 각도로 나타내는 베어링 정보를 기반으로 하여 선박의 위치를 추정하고, 삼변측량을 통해 부표나 비콘까지의 거리 정보를 사용하여 위치를 결정한 후 선박의 위치를 복구하였다.

4.3. 선박 정보 시스템(SIS)

선박 정보 시스템(SIS)은 해양 분야(해사, 항만, 해양선박)에서 항해, 안전 및 운영에 필수적인 데이터 등을 집약하고 관리하는 복합적인 시스템이다. 다양한 해양선박이 서로 다른 SIS 기능을 가지고 있지만, Liu 외 3인[28]에 따르면 일반적인 SIS는 센서 네트워크, 디스플레이 네트워크 등 독립적인 다양한 서브넷과 전체 해양선박 통신 네트워크로 구성되어 있으며, 해당 네트워크들은 참조 입력, 제어 입력, 센서 정보 등의 정보를 서브넷과 시스템 간에 교환할 수 있다.

Onishchenko 외 4인[25]은 SIS 내의 기밀 데이터가 암호화되지 않아 사이버공격으로 인한 유출 취약성을 시사하고, 이에 따라 사이버 복원력 프레임워크를 구축하였다. 본 연구에서 제안한 SIS 대상 사이버 복원력 프레임워크는 동형 암호화 기술과 몬테카를로 알고리즘을 결합한 검색 엔진을 활용하여, 암호화된 데이터를 복호화하지 않고 해당 데이터를 분석하여 효율적으로 사이버공격을 탐지 및 대응할 수 있다. 해당 검색 엔진은 실험을 통해 데이터의 보안성이 검증되었으며, 데이터의 양에 따른 검색 속도 변화를 관찰하여 시스템의 효율성 또한 검증하였다.

- 식별(Identify)
  사이버 위협 대응 프로세스를 정의하기 위해 현대 사이버공격 유형을 분석한다. 분석 결과, 사이버공격에서 가장 높은 비율을 차지하는 공격 유형은 악성 코드 주입이었으며, 그 뒤로 디렉토리 이탈, XSS 공격으로 분석되었다. 뿐만 아니라, 선박 정보 시스템 내의 기밀 데이터는 암호화가 되지 않고 사용되고 있어 사이버공격에 대한 취약성이 분석되었다.
- 보호(Protect)
  앞서 식별된 사이버공격 유형을 기반으로 대응전략을 설계한다. 이를 위해 사이버 위협 및 자산의 취약성을 분석하고, 사이버공격에 대한 위험도를 중요 자산의 수준을 기반으로 하여 정량적으로 평가한다.
- 탐지(Detect)
  동형 암호화 기술과 몬테카를로 알고리즘을 결합하여 서버로부터 암호화된 데이터를 수신한다. 이후 순차적으로 사이버공격과 연관된 특정 키워드를 추출하는 검색 알고리즘을 기반으로 사이버공격을 탐지한다.

- 대응(Respond)
  사이버공격으로 인해 손상된 자산을 격리한 후, 발생한 사이버 사건에 대해 명확히 문서화하도록 한다.
- 복구(Recover)
  문서화된 사이버 사건을 기반으로 손상된 자산을 개선함으로써 차후에 일어날 사이버공격에 대비한다.

4.4. PLC

PLC는 산업 장비와 자동화 시스템을 제어할 수 있는 컴퓨터 기반의 단일 프로세서 장치이다[29]. PLC는 일반적으로 산업제어시스템(ICS, Industrial Control System) 환경에서 입력 및 출력을 통해 개별 기계 또는 복잡한 프로세스를 모니터링하고 제어하는 데 사용된다. 해양 선박 환경에서는 엔진 관리, HVAC(Heating, Ventilation, Air Conditioning), 항해 시스템 등 선박의 중요한 기능을 모니터링하고 제어한다[30].

Luo 외 7인[26]은 산업 제어 시스템에 대한 사이버 공격에 대응하여 복원력을 강화하기 위한 새로운 쿼드 중복 PLC 아키텍처를 제안하였다. 해당 아키텍처는 두 개의 PLC 세트로 구성되며, 각 세트는 병렬로 작동하는 두 개의 PLC로 이루어져 있다. 각 PLC는 서로 다른 제어 소프트웨어를 실행하여, 사이버공격이 발생할 경우 모든 PLC에 동일한 영향을 미치지 않도록 한다. 하나의 PLC 세트는 기본 PLC 세트로 사용되고, 다른 하나의 PLC 세트는 보조 PLC 세트로 사용된다. 해당 연구에서는 냉각수 시스템을 제어하는 Siemens S7-1500 개방형 컨트롤러 PLC에 메모리 손상 공격을 시행 함으로써 제안된 아키텍처가 일반적인 제어 주기보다 빠르게 사이버공격으로부터 복구할 수 있음을 검증하였다.

- 탐지(Detect)
  기본 PLC 세트의 두 PLC가 동시에 동일한 입력을 받아 처리하고, 결과를 비교하는 중복 실행 개념을 적용하여, 두 PLC의 출력이 서로 일치하지 않을 경우, 사이버공격이 발생하였다고 간주한다.
- 대응(Respond)
  사이버공격이 탐지되면, 보조 PLC 세트는 사이버공격을 당한 기본 PLC 세트의 메모리 파티션을 덮어쓴다. 이 과정에서 사이버공격이 보조 PLC 세트로 전파되는 것을 방지하기 위해 지연 버퍼가 활성화되며, 보조 PLC 세트는 새로운 기본 PLC 세트가 된다.
- 복구(Recover)
  사이버공격을 받은 기본 PLC 세트는 다양화된 바이너리의 사전 컴파일러 된 라이브러리에서 새로운 메모리 주소 공간을 선택하여 보조 PLC 세트로 자동 재생성된다.

〔표 2〕 NIST 사이버 복원력 모델 기반 연구 분석

Ref	식별(Identify)	보호(Protect)	탐지(Detect)	대응(Respond)	복구(Recover)
〔21〕	IT 자산에 대한 자산 정보를 저장하고 있는 온톨로지 개발	추론기를 활용한 온톨로지 기반 사이버공격 대응 전략 도출	SIEM을 활용한 IT 자산 이상 동작 탐지 및 판별	추론기를 활용한 사이버공격 파급력 예측 및 예상되는 공격 대상 IT 자산 식별 및 보안 대책 도출	반복적인 사이버공격 모니터링 및 대응
〔22〕	-	-	GLRT 기반, 가우스 모델과 KDE에 따른 변화분석	GNSS 격리 후 위치 정보에서 해당 신호 제외	삼각측량 및 삼변측량을 통한 위치 수정
〔23〕	현대 사이버공격 유형 식별 및 선박 정보 시스템 취약성 도출	중요 자산에 따른 사이버공격 위험도 평가 및 대응전략 설계	동형 암호화 기술 및 몬테카를로 알고리즘 결합을 통한 데이터 보호 및 사이버공격 탐지	손상된 자산 격리 및 사이버사건 문서화	문서화된 사이버사건을 활용한 차후 사이버공격 대비 및 손상된 자산 개선
〔24〕	-	-	동시 중복 실행 개념 기반 출력 간 불일치 탐지	보조 PLC 세트로 전환	다양화된 바이너리와 새로운 메모리 주소를 통한 재생성

Ⅴ. 결 론

본 논문은 해양선박 환경에서의 사이버 복원력에 관한 연구들을 조사하였다. 사이버 복원력의 개념을 정립한 후, 선내 시스템별로 사이버 복원력 연구를 분류하였다. 각 연구들은 NIST의 사이버 복원력 모델을 기반으로 분석되었으며, GNSS와 PLC를 대상으로 하는 사이버 복원력 연구는 NIST 사이버 복원력 모델의 탐지, 대응, 복구 단계를 통해 사이버공격으로 손상된 시스템을 복구할 수 있는 기술을 제안하였다. SIS와 모든 시스템에 적용 가능한 사이버 복원력 연구는 NIST 사이버 복원력 모델 내의 모든 단계를 거쳐 사이버공격으로 손상된 시스템을 복구할 수 있는 프레임워크를 제안하였다.

해양선박 기술이 첨단 ICT 기술과 융합되면서, 해양선박에 대한 보안 위협이 증가할 것으로 예상된다. 하지만, 나날이 증가하는 보안 위협에 비해 현재까지 이루어지고 있는 해양선박 대상 사이버 복원력 연구는 현저히 부족한 실정이다. 이에 따라 해양선박을 대상으로 하는 지속적인 사이버 복원력 연구가 필요할 것으로 판단된다.

참 고 문 헌

[1] 주간기술동향, “해양 선박 사이버보안 동향”, https://m.koita.or.kr/m/mobile/mem_knowledge/ktip_read.aspx?no=49158&page=14, Accessed on November 2023.

[2] Choi, S. H., Youn, J., Kim, K., Lee, S., Kwon, O. J., & Shin, D. "Cyber-Resilience Evaluation Methods Focusing on Response Time to Cyber Infringement.", *Sustainability,* 15(18), pp. 13404, September. 2023.

[3] NIST, “cyber resiliency”, https://csrc.nist.gov/glossary/term/cyber_resiliency, Accessed on November 2023.

[4] International Maritime Organization, “Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems”, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx, Accessed on November 2023.

[5] IACS, “Rec 166 - Recommendation on Cyber Resilience”, https://iacs.org.uk/resolutions/recommendations/161-180/rec-166-new-corr2-cln, Accessed on November 2023.

[6] Bimco, Clia, ICS, Intercargo, Intermanager, Intertanko, IUMI, OCIMF and World Shipping Council, “The Guidelines on Cyber Security onboard Ships-Version 4”, *BIMCO*, 2020

[7] DNV, “Cyber security resilience management for ships and mobile offshore units in operation”, https://www.dnv.com/cybersecurity/recommended-practices/index.html, Accessed on November 2023.

[8] 이광일, 송문섭, 장병태, "E-navigation과 사물인터넷(IoT)의 국제 표준 및 기술동향", *ETRI*, 2014.

[9] Kang, Jonggu, Daekeun Moon, and Junghan Kim. "Building communication interface in ship area network for merchant marine: A practical approach." *2013 13th International Conference on Control, Automation and Systems (ICCAS 2013). IEEE*, 2013.

[10] CCDCOE, “Cybersecurity Considerations in Autonomous Ships”, https://ccdcoe.org/uploads/2022/09/Cybersecurity_Considerations_in_Autonomous_Ships.pdf, Accessed on November 2023.

[11] 김창훈, “미래 해양 산업의 주요 이슈와 사이버보안 기술”, *대구대학교*, 2022.

[12] Sahay, R., Meng, W., Estay, D. S., Jensen, C. D., & Barfod, M. B., “CyberShip-IoT: A dynamic and adaptive SDN-based security policy enforcement framework for ships”, *Future Generation Computer Systems*, 100, pp.736-750, November. 2019.

[13] WIRED, “To protect Putin, Russia in spoofing GPS signals on a massive scale”, https://www.wired.co.uk/article/russia-gps-spoofing, Accessed on November 2023.

[14] ENDIGE BOATING, “NMEA 2000 PGN’s deciphered”, https://endige.com/2050/nmea-2000-pgns-deciphered/, Accessed on November 2023.

[15] Bornholms Tidende, “Never seen before: The ferry’s GPS system with triple backup went down”, https:

//tidende.dk/trafik/aldrig-set-foer-faergens-gps-system-med-tredobbelt-backup-gik-ned/119685, Accessed on November 2023.

[16] Xing, B., Liu, S., Chen, X., & Zhi, P., “Design of sensor data flow for ship information system”, *Journal of ship production and design*, 33(04), pp.310-316, November. 2017.

[17] Jo, Y., Choi, O., You, J., Cha, Y., & Lee, D. H., “Cyberattack models for ship equipment based on the MITRE ATT&CK framework”, *Sensors*, 22(5), pp.1860, February. 2022.

[18] 고영현. "ICT 공급망 사이버 레질리언스 대책 개발에 관한 연구:(A) study on developing cyber resilient ICT supply chain controls.", *중앙대학교 석사 학위 논문*, February. 2021.

[19] IBM, “What is cyber resilience”, https://www.ibm.com/topics/cyber-resilience, Accessed on November 2023.

[20] KT Enterprise, “진화하는 사이버 보안 위협에서 살아나는 법”, https://enterprise.kt.com/bt/dxstory/1886.do, Accessed on November 2023.

[21] Annarelli, A., Nonino, F., & Palombi, G., “Understanding the management of cyber resilient systems”, *Computers & industrial engineering*, 149, pp. 106829, November. 2020.

[22] NIST, “Framework for Improving Critical Infrastructure Cybersecurity”, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, Accessed on November 2023.

[23] Hutschenreuter, H., Çakmakçi, S. D., Maeder, C., & Kemmerich, T., “Ontology-based Cybersecurity and Resilience Framework”. *ICISSP,* pp. 458-466, 2021.

[24] Onishchenko, O., Shumilova, K., Volyanskyy, S., Volyanskaya, Y., & Volianskyi, Y., "Ensuring cyber resilience of ship information systems.", *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation,* 16(1), pp. 43-50, March. 2022.

[25] Dagdilelis, D., Blanke, M., Andersen, R. H., & Galeazzi, R., “Cyber-resilience for marine navigation by information fusion and change detection”, *Ocean Engineering*, 266(3), pp. 112605, December. 2022.

[26] Luo, J., Kang, M., Bisse, E., Veldink, M., Okunev, D., Kolb, S., Joseph, G., & Canedo, A., "A Quad-Redundant PLC Architecture for Cyber-Resilient Industrial Control Systems", *IEEE Embedded Systems Letters*, 13(4), pp. 218-221, December. 2021.

[27] HEXAGON, “What are Global Navigation Satellite Systems?”, https://novatel.com/tech-talk/an-introduction-to-gnss/what-are-global-navigation-satellite-systems-gnss, Accessed on November 2023.

[28] Liu, S., Xing, B., Li, B., & Gu, M. "Ship information system: overview and research trends.", *International Journal of Naval Architecture and Ocean Engineering,* 6(3), pp 670-684, September. 2014.

[29] Alphonsus, E. R., & Abdullah, M. O., “A review on the applications of programmable logic controllers (PLCs)”, *Renewable and Sustainable Energy Reviews*, 60, pp. 1185-1205, July. 2016.

[30] Marine Electrical, “What Are PLCs and Why Are They Important?”, https://www.finelinemarineelectric.com/blog/what-are-plcs-and-why-are-they-important/, Accessed on November 2023.

〈저자소개〉

고아름 (Areum Ko)

2021년 3월~현재 : 가천대학교 컴퓨터공학과 학사 과정

<관심분야> CPS 보안, 선박 보안

최 희 원 (HeeWon Choi)

2023년 8월 : 가천대학교 글로벌경영학과 졸업
2023년 9월~현재 : 가천대학교 정보보호학과 석사과정
<관심분야> CPS 보안, 정보보호 평가

전 승 호 (Seungho Jeon)

2018년 2월 : 고려대학교 정보보호학과 석사 졸업
2022년 8월 : 고려대학교 정보보호학과 박사 졸업
2023년 1월~현재 : 가천대학교 컴퓨터공학부 스마트보안 전공 연구교수
<관심분야> 딥러닝, 시스템 보안

서 정 택 (Jung Taek Seo)

종신회원

1999년 2월 : 한국교통대학교 컴퓨터공학과 학사 졸업
2001년 2월 : 아주대학교 컴퓨터공학과 석사 졸업
2006년 2월 : 고려대학교 정보보호공학 박사 졸업
2016년 3월~2021년 2월 : 순천향대학교 정보보호학과 부교수
2021년 3월~현재 : 가천대학교 컴퓨터공학부 부교수
2000년 11월~2016년 2월 : 국가보안기술연구소 책임연구원/연구부장
2014년 6월~2015년 6월 : University of Florida 초빙연구원
2009년 12월~2013년 5월 : 제주 스마트그리드 실증단지 보안센터 센터장
2013년, 2018년 : 한국철도공사 정보화자문단 자문위원
2016년 1월~2016년 12월 : ㈜ SR 철도안전자문단 자문위원
2017년 1월~현재 : 한국정보보호학회 CPS보안연구회 위원장
2017년 2월~현재 : 한국남동발전 사이버보안자문단 자문위원
2017년 11월~현재 : 인천국제공항공사 사이버보안 자문위원회 자문위원
2018년 12월~현재 : 한국서부발전 사이버보안 자문위원
2020년 6월~현재 : 한국전력공사 보안위원회 자문위원
<관심분야> CPS보안, 제어시스템 보안, 스마트그리드 보안, 원자력 발전 사이버보안, 스마트팩토리 보안, 스마트시티 보안, 자율주행인프라 보안, 해양선박 보안, 항공우주 보안