디지털산업정보학회 논문지 제18권 제4호-2022년 12월
http://dx.doi.org/10.17662/ksdim.2022.18.4.041

VDI 적용을 통한 자율운항선박의 C.I.A 확보 방안 연구*

최 영 렬** · 백 남 균***

Securing C.I.A for Autonomous Vessels through the Application of VDI

Choi Youngryul · Baik Namkyun

〈Abstract〉

In the fourth industrial era, when various technologies are fused and combined, new and advanced technologies from other industries are used extensively in the maritime industry field. New security threats are also increasing along with the development of new technologies.

In addition, in incorporating convergence technologies into the maritime industry, various problems, such as communication definitions and procedures between technologies and customer-customized delays, occur. In this paper, for the problems mentioned above, research results on the network configuration of safer autonomous vessels by supplementing and fusing existing solutions rather than developing new technologies are proposed. In conclusion, the entire network consists of VDI and presents additional configurations to ensure confidentiality, integrity, and availability, which are the three security elements. According to the composition of such a convergence network, it is intended to help prepare countermeasures to protect internal data from external threats.

Key Words : Automous Ship, Virtual Desktop Infrastructure, Confidentiality, Integrity, Availability

Ⅰ. 서론

현대 사회는 4차 산업혁명이 확산되며 다양한 분야에 대한 혁신이 일어나고 있다. 또한 Convergence 환경 도입과 더불어 AI, Big Data, IoT 제품 등의 융합 기술들이 산업현장에서 활용되고 있다. 진보된 타 산업의 융합 기술들이 개발 적용됨에 따라 새로운 보안 위협 또한 발생하게 되며 이에 대처 가능한 기술 적용이 강구된다.

해사환경에서는 이러한 환경 변화에 대응하기 위한 여러 가지 방안을 발표하고 있다. 그 중 국제해사기구 (International Maritime Organization, IMO)에서는 융합 관련 기술에 대한 무인선박, 원격조종선박, 자율운항선박 등 다양한 용어로 사용되어온 무인선박을 자율운항선박(Maritime Autonomous Surface Ship, MASS)로 부르기로 결정하며 정의를 규정하였

* 이 논문은 2022년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임(P0008703, 2022년 산업혁신인재성장지원사업)
** 부산외국어대학교 스마트융합보안대학원 석사과정(제1저자)
*** 부산외국어대학교 스마트융합보안학과 교수(교신저자)

다[1]. 그 뿐만 아닌 우리나라 '해양수산부'에서는 혁신을 위한 해상 관련 구축전략을 수립하며 현재 한국형 E-내비게이션이라는 사업을 진행 중에 있다[2]. 현재 선박에 대한 사고 원인은 사람의 과실에 의한 비중이 매우 높게 형성되어 있으며 이는 경제적 손실을 가지고 올 뿐만 아닌 인명사고 위험이 존재한다. 이에 자율운항선박은 선원에게 의존하는 것이 아닌 인공지능을 활용하여 자율적으로 운행을 한다는 점에서 인명피해와 더불어 해양사고를 줄여 경제적인 피해를 막을 수 있다는 것에 큰 기대를 불러일으키고 있다[3].

하지만 이러한 인공지능 활용 또한 해킹에 대한 위협이 사라진다고 보기 힘들다. 선박에 대한 보호자산의 전환에 따라 시스템 공격이 주를 이룰 것으로 보이며 원격을 통한 실제 해킹 대상이 증가할 것으로 판단되어 경제적 손실은 여전히 존재할 것으로 판단된다[4]. 또한 이러한 경우 인공지능 활용에 따라 사람의 관여가 없기에 사고 발생에 따른 책임소재 파악이 힘들어 지며 피해 규모 또한 커질 수 있다. 이러한 보안 위협 및 문제들에 대한 대응을 위해서는 보안의 3대 요소인 기밀성, 무결성, 가용성에 대한 방안이 필요하게 된다.

본 논문에서는 여러 보안 기법 방안 중 가상 데스크톱 환경을 활용하여 선박 네트워크 구성을 제안한다. 더불어 보안 3대 요소 확보를 위한 각각의 방안을 추가 제안한다.

논문 구성은 다음과 같다. 2장에서 현재 선박기구에서 내려오는 지침과 가상 데스크톱 환경의 기술적 특성에 대해 서술하며 3장에서는 안전한 자율운항선박의 구성 방안 제시 및 전체적 네트워크 구성으로 인한 보안 효과들을 서술하며 마지막 결론으로 마무리 된다.

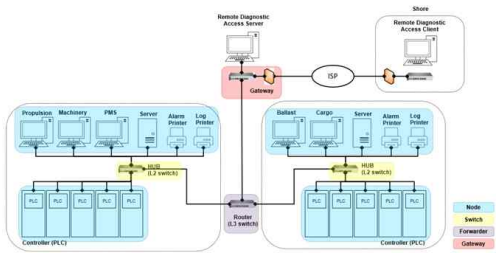
II. 관련연구

2.1 한국선급(KR)의 규정 지침

한국선급(KR)에서는 선급에 대한 지침 및 가이드라인인 해상 사이버보안 시스템 지침을 개발 배포하였다. 자율운항선박에 대한 'MASS'정의에 따른 IMO와 해사산업계 및 주요 선급에서는 관련 가이드라인 개발 및 국제규제 채택 등 많은 노력을 기하고 있다. 그 중에서도 한국 선급에서는 사이버보안의 기본요소인 무결성, 가용성, 기밀성 관점에서 인증해 주는 서비스인 KR 사이버보안 형식승인 지침 문서를 배포하였다. 또한 다음 <그림1>과 같이 네트워크 구성도에 대한 규정을 제시하고 있다.

하지만 이 그림에서 보듯 보안 3요소에 기반한 네트워크 구성으로 보기 어려우며 그림에 대한 설명이 자세히 나와 있지 않아 확인이 어렵다.

본 논문에서는 KR에서 규제하는 보안 3요소에 벗어나지 않고 안전한 선박 네트워크 구성을 제안하고자 한다.



<그림 1> KR 사이버보안 형식승인 [5]

2.2 VDI 기술적 특성

가상 데스크톱 환경(Virtual Desktop Infrastructure, VDI)은 클라이언트 단말기를 통해서 사용자에게 메인서버에 연결하여 가상 데스크톱 환경에 접속하여 가상 머신을 사용할 수 있도록 지원하는 가상화 기술

이다[6]. 해당 사용자는 위치에 구애받지 않고 모든 어플리케이션 및 자료가 저장된 중앙 서버와 스토리지에 접속하여 저장소를 활용할 수 있어 언제 어디서나 개인 데스크톱과 같은 가상환경에 접속이 가능하다.

또한 VDI는 CPU, 메모리, 저장 공간을 효율적으로 할당할 수 있어 하드웨어 자원에 대해 관리가 용이해지며 데이터에 있어 최종 클라이언트가 아닌 서버에 저장이 된다. 따라서 최종단말 기기가 도난당하거나 손상되는 경우에도 데이터의 보호가 가능해진다. 마지막으로 중앙집중식 관리를 통해 모든 데스크탑 환경을 손쉽게 패치하고 업데이트가 가능하며 PMS 역할에 대한 대처가 가능해진다.

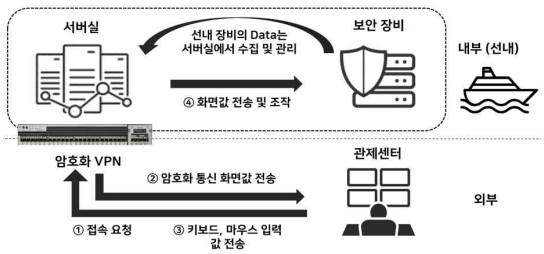
Ⅲ. 보안 3대 요소 확보를 위한 조치 방안

본 논문에서는 기본적인 네트워크 구성에 대해 VDI로 구성을 진행하며 거기에 있어 추가로 보안성 강화를 위한 보안 3요소에 기반하여 추가 방안을 제시하고자 한다.

3.1 암호화 전송 프로토콜을 활용한 기밀성 확보 방안

기본적 VDI 특성에 따른 문서들은 각각의 최종단말가 아닌 문서 중앙화를 통한 서버에 데이터가 저장이 되어진다. 또한 서버의 데이터를 가상 화면에 띄우기 위해서는 인증 서버를 통해 인가된 사용자에게만 자산에 접근할 수 있게 하는 기본적 기밀성에 기반하고 있다 볼 수 있다.

하지만 이 환경 또한 해커들의 침해에 있어 안전하다 볼 수 없다. 특히 자율운항선박의 경우 침해에 따라 선박의 GPS 조작으로 인한 선박 충돌 및 운행 경로 변경으로 선박이 다른 나라에 불법 침범 등과 같이 피해 규모가 상당히 크다. 본 절에서는 이러한 위험사고에 대응하기 위하여 기밀성 강화 확보 조치를 다음 <그림2>와 같이 암호화 전송 프로토콜을 추가 구성한다. 내부와 외부의 네트워크 연결에 있어 트래픽 등에 대한 Data 노출 방지를 위해서는 반드시 전송 프로토콜에 대해 암호화가 되어 사용이 되어야한다. 이로써 외부 비인가자에 대한 침입 허용시에도 암호화된 통신값을 통해 자료 노출에 대응이 가능해지며 안정성을 확보하는 방안을 마련한다.

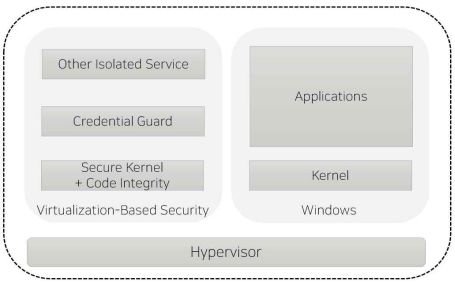


<그림 2> 암호화 VPN을 통한 전송 방식

3.2 VBS/HVCI를 통한 무결성 강화

현재 다양한 OS들이 개발되어 시장에 나와 운영되고 있다. 그중에서도 Windows 운영체제 사용률이 가장 높은 형세를 보인다. 제안하는 방안 역시 선박에 대한 가상 머신 OS를 Windows 기반으로 사용시에 활용될 수 있다.이에 본 논문에서는 가상화 기반 보안(Virtualization - Based Security, VBS)을 활용하며 추가로 하이퍼바이저 보호 코드 무결성(Hypervisor Enforced Code Integrity, HVCI)을 통해 정보를 담고 있는 시스템을 대상으로 무결성에 대한 강화방안을 제안한다. 가상화 OS에 대한 내부도식은 <그림3>과 같다. 기본적으로 이 기능은 Windows의 위협 모델 개선 및 Windows의 커널을 악용하려는 Malware에 대한 보호방안 중 하나이다. 적용방안으로는 Windows 하이퍼바이저를 활용하여 격리된 가상 공간을 새롭게 추가 생성하게 된다. 이어 가상 공간 위에 HVCI

인 커널 모드에 대한 코드 무결성을 추가하여 가상 머신을 실행하면 시스템을 위협하는데 사용할 수 있는 메모리의 할당량을 점검하여 제한할 수 있다. 또한 드라이브 서명 등을 활용하여 시스템의 업로드 전 인증과정을 통해 허용된 서비스만이 가상머신의 시스템 상에 업로드가 가능하도록 한다. 이를 통해 외부 환경에서의 사용자는 OS 조작에 대한 무결성을 점검하고 해당 가상머신을 신뢰된 루트로 활용할 수 있다. 동시에 가상 머신 내에 기록된 데이터 및 활용하는 시스템에 대해서도 신뢰성 확보가 가능하다.



<그림 3> OS 가상화 내부 도식화

3.3 가용성 확보를 위한 관리서버 이중화 방식

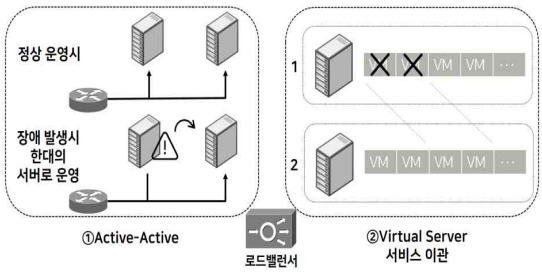
이번 절은 VDI 방식이 가지는 단점과 기존의 운영서버를 운영함에 있어 사용되는 StandAlone 방식에 대한 대응이자 가용성 확보를 위한 방안이다. 수많은 가상머신의 운영에 있어 하나의 리소스에 오류가 발생하면 다른 가상머신 전체에 영향을 준다는 문제점을 가지고 있다.

특히 선박의 경우 원해에 운항중인 선박에 대해 원격 조정 및 관제 서비스가 중단될 경우 큰 사고로 이어질 수 있다. 이로 인해 서버 장애시에도 서비스 영향을 주지 않는 구성은 필수적이게 된다. 그에 따라 가상데스크톱 운영에 있어 필요한 모든 관리서버에 대해 이중화 구성을 제안하고 기능에 대해 서술한다.

이중화구성에 앞서 전 서버의 앞단에 위치한 로드 밸런싱 기능을 탑재한 스위치를 활용한다. 스위치를 통해 기능 또는 성격에 따라 적절한 서버에 데이터를 부하 분산시켜 1차적으로 서버의 과부하에 대응을 한다. 또한, 그림4의 ① - 관리서버에 대한 구성은 Active-Active로 동작하게 구성된다. 운영함에 있어 한 대의 서버에 이상 발생시에도 물리적으로 위치한 다른 한 대의 서버로 이전하여 대응운영이 가능하도록 구성한다.

그림4의 ② 하나의 운영서버에 존재하는 여러 가상머신들 중 error 발생한 해당 가상머신을 다른 운영서버로 서비스를 이관시켜 무중단 서비스를 제공한다.

이로써 운항중 선박의 서비스에 발생 할 수 있는 문제에 대해 즉각 대처 및 원활한 서비스의 성능 보장이 가능하다.



<그림 4> 이중화 구성을 통한 가용성 확보 방안

3.4 제안하는 융합적 네트워크 구성

<그림5>는 본 논문에서 제안하는 자율운항선박에 대한 전체적인 네트워크 구성도이다. 제안하는 구성에 따라 선박의 동작 구성은 다음과 같다. 자율운항선박 내에 운영되는 장비들에 대해 가상 데스크톱 환경으로 구성한다. 즉 가상 데스크톱 환경의 운영서버에 선내 장비인 GPS, 레이더 등 조종이 필요한 모든 장비들에 대해 각각의 가상 머신으로 구축하고 이를 관제센터에서 원격접속 하게 된다. 관제센터에서는

서버에 구성된 가상 머신에 접속하여 선박을 원격 운항하며 관제를 진행하게 된다. 또한 가상 데스크톱 구성에 따라 발생할 수 있는 애로사항 및 원격함에 있어 발생하는 문제점과 운영되는 가상 머신들에 대한 안전성 확보 방안을 추가하여 네트워크 구성도를 제안한다. <그림5>와 같은 네트워크 구성에 따라 발생하는 긍정적 효과는 다음과 같다.

첫째, 해상과 육상간의 통신함에 있어 암호 프로토콜 통신을 구성하여 외부로부터의 네트워크 해킹 등 보안위협에 대해 기밀성을 강화시켜주는 방안으로 활용된다.

둘째, 가상 머신에 대한 가상화 메모리 영역 생성 및 무결성 검증 코드로 인해 가상 머신에 대한 OS 해킹 및 변조 등의 무결성 검증이 가능해 지며 이를 통해 내부 시스템에 대한 신뢰성 확보가 가능해진다.

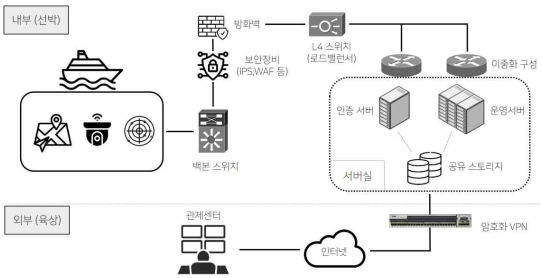
셋째, 운항중인 선박과 관제센터간의 원격 조정 및 관제를 함에 있어 관리서버 오류 발생시에도 이중화 구성을 통해 서비스 이관 및 무중단 서비스 제공을 통해 보안사고에 대응하며 가용성을 강화할 수 있는 수단이 된다.

넷째, Endpoint 단에 악의적인 해킹 시도로 접속을 허용하게되어도 내부 스토리지에 저장되어 있는 정보에 대해서 자료를 복사하거나 혹은 가져가기 등의 행위가 불가능하여 원천적 해킹 시도에 대비가 가능해진다.

이를 통해 자율운항선박은 기밀성, 무결성, 가용성을 갖춘 네트워크 구성을 가지게 되며 외부로부터 접근하는 위협에 대해 자산을 보호하며 보다 효율적인 관리를 통해 선박이 야기하는 문제점들에 대해 대응이 가능하다.

IV. 결론

현재 사회는 Convergence 환경에 들어서며 타산업



<그림 5> 전체적인 네트워크 구성도

의 융합 기술들이 적용되고 있다. 융합기술의 발전에 따라 보안위협은 여전히 존재할 뿐 아닌 고도화된 APT 등의 새로운 보안위협들이 추가 발생하는 상황에 있다. 해사환경 또한 이러한 문제점들에 대해 공통적으로 발생하기에 보안 대응방안들이 필요하다.

하지만 해사 선박에 관련된 네트워크 구성도는 KR 한국선급 규정 외에 뚜렷한 자료를 찾아보기 힘든 상황이며 해사선박의 네트워크 구성 및 보안에 대한 논문 자료 또한 찾기 힘든 상황에 있다. 보안 요소의 강화를 위해서 다양한 회사의 솔루션들의 연구 및 개발이 이루어지고 있으나 새롭게 개발되는 여러 보안 솔루션을 선박에 접목시키는 것에 있어 기술간 통신 프로토콜 정의・절차 및 고객맞춤 지연 등의 커스터마이징에 관련된 이슈가 발생할 수 있다. 그에 따라 본 논문에서는 새로이 기술을 개발하여 제안하는 것이 아닌 VDI를 통한 전체적 네트워크 구성과 추가적인 보안요소 강화를 위해 보안 3대 요소에 기반하여 자율운항선박에 대한 융합적 네트워크 구성을 제안하고 있다. 기존 모델들의 적절한 융합을 통해서도 충분한 선박 네트워크 구성이 되며 외부의 위협으로부터 안정성 확보가 충분히 가능할 것이라 판단된다. 또한 저자가 제안하는 방안과 같이 현재 기술들을 좀 더 발전시키고 적절한 융합을 갖춘다면 보다 빠른 시일 내에 자율운항선박의 개발이 이루어질 것이며 이로 인해 해사 환경에서의 대응방안 마련에 도움이 되고자 한다.

참고문헌

[1] 장유락, "자율운항선박 인공지능의 윤리문제에 대한 소고 - 사고 알고리즘을 중심으로 -," 한국해사법학회, 해사법연구, 제33권, 제1호, 2021, pp.143-171.

[2] 해양수산부 지능형 해상교통정보서비스, https://e-navigation.mof.go.kr/mainHome.do

[3] 한성훈·송영조, "자율운항선박을 둘러싼 현황과 법적과제 -자율운항선박의 운항 중 사고에 대한 형사책임을 중심으로-," 한국법정책학회, 법과정책연구, 제22권, 통권 65호, 2022, pp.99-115

[4] 박한선·박혜리·허성례·이혜진·김보람, "자율운항선박, 침체된 해운산업 및 조선 산업의 새로운 성장 동력," 한국해양수산개발원, KMI 동향분석, 제72권, 통권 72호, 2018, p. 1-19.

[5] Korean Register, https://www.krs.co.kr/kor/Content/CF_View.aspx?MRID=155&URID=153

[6] Park Ung-Kyu, "The Technology Trends and Future Prospects of Cloud Computing," Journal of Science & Culture, Vol.6, No.1, 2009, pp.51-60.

■ 저자소개 ■

최 영 렬
(Choi, Young Ryul)

2021년 8월~현재
부산외국어대학교
스마트융합보안학과(공학석사)
2021년 2월 부산외국어대학교 정보보호학과
(공학사)

관심분야 : 네트워크, 정보보안컨설팅, 모의해킹
E-mail : dudfuf261@naver.com

백 남 균
(Baik, Nam Kyun)

2019년 3월~현재
부산외국어대학교 정보보호학과
2000년 ~ 2017년
한국인터넷진흥원 수석연구원
2011년 2월 숭실대학교 전자공학과(공학박사)
2001년 2월 숭실대학교 전자공학과(공학석사)
1998년 2월 숭실대학교 전자공학과(공학사)

관심분야 : 스마트융합보안, 정보보안컨설팅
E-mail : white-knight@daum.net

논문접수일 : 2022년 9월 13일
수 정 일 : 2022년 9월 21일
게재확정일 : 2022년 10월 11일