

## 해양 사이버보안 및 사용자 인증체계

홍승표<sup>○</sup>, 이훈재<sup>\*</sup>, 이영실<sup>\*\*</sup>

<sup>○</sup>동서대학교 일반대학원 컴퓨터공학과,

<sup>\*</sup>동서대학교 정보보안학과,

<sup>\*\*</sup>동서대학교 International College

e-mail: debiii@naver.com<sup>○</sup>, hjlee@dongseo.ac.kr<sup>\*</sup>, lys0113@dongseo.ac.kr<sup>\*\*</sup>

## Maritime Cybersecurity and User Authentication Systems

Seoung-Pyo Hong<sup>○</sup>, Hoon-Jae Lee<sup>\*</sup>, Young-Sil Lee<sup>\*\*</sup>

<sup>○</sup>Dept. of Computer Engineering, Dongseo University,

<sup>\*</sup>Dept. of Information Security, Dongseo University,

<sup>\*\*</sup>Dept. of Computer Engineering English Track, International College, Dongseo University

### ● 요약 ●

정보통신기술이 발전함에 따라 미래 해양산업에는 첨단 ICT 기술을 중심으로 두고 패러다임이 변화하고 있다. 해양 선박 분야에서는 현 단계인 스마트 쉽(Smart Ship), 자율운항선박(MASS) 등 육상과 선박간의 통신기술이 필요한 시점에서 사이버 공격 위협으로부터 자유로울 수 없다. 선박 간의 사용자 인증은 선박의 보안을 강화하고 인가된 사용자 만이 선박 시스템에 접근하고 조작할 수 있도록 하는 중요한 요소이다. 보안 요구 사항과 해당 규정에 따라 설계되고 구현되어야 하며, 또한 중요한 측면은 인증 시스템의 안전성과 안정성을 유지하기 위해 주기적인 업데이트와 강화된 보안 대책을 시행하는 것이다. 본 논문에서는 선박 간의 사용자 인증기술에 대해서 알아보고 다양한 방법에 대하여 제안하였다.

**키워드:** 사용자 인증(user authentication), 사이버 보안(cyber security), 자율운항선박(mass)

### I. Introduction

정보통신기술이 발전함에 따라 미래 해양산업에는 첨단 ICT 기술을 중심으로 두고 패러다임이 변화하고 있다. 해양 선박 분야에서는 현 단계인 스마트 쉽(Smart Ship), 자율운항선박(MASS) 등 육상과 선박 간의 통신 기술이 필요한 사이버 공격 위협으로부터 자유로울 수 없다. 인간의 개입이 필요 없는 무인선박(Fully Autonomous Ship)은 자체적으로 항로를 설정하고 조종할 수 있는 기술을 탑재하고 있다. 인공지능 및 센서 기술의 발전으로 인해 무인선박은 자체적으로 환경을 인식하고 상황에 따라 적절한 조치를 취할 수 있게 되었다. 여러 기술을 종합적으로 갖고 있는 무인선박은 다양한 센서를 사용하여 주변 환경을 감지하게 되는데 GPS, LADAR, Sonar, 비전 시스템 등을 활용하여 장애물 회피, 다른 선박과의 거리 유지, 항로 추적 등을 수행한다.

최근에는 무인선박의 에너지 효율성을 개선하기 위한 기술 개발에도 주력하고 있는데 예를 들어, 태양광 패널, 풍력 발전 시스템 등을 도입하여 전력을 공급하거나 연료 소비를 줄일 수 있는 시스템이 개발되고 있다.

### II. Preliminaries

#### 1. 자율운항선박

국제해사기구(International Maritime Organization, IMO)는 국제연합(United Nations, UN) 산하 전문기구 중의 하나로서 해상에서 발생할 수 있는 인명의 손실과 막대한 환경적 재난 및 재산의 손실을 방지하기 위하여 매년 각 회원 국가의 대표들이 모여 회의를 통해 해상 안전과 선박 설비에 관한 국제적 기준을 제정하고, 조난 및 안전 제도(Global Maritime Distress and Safety System, GMDSS)를 마련하고 그 시행 여부를 감독 및 관리하고 있어 해운, 조선 등 관련 산업에 미치는 영향력은 크다고 볼 수 있다 [1].

자율운항 선박은 국제해사기구(IMO)에서 MASS(Maritime Autonomous Surface Ship)라고 명명하였으며, 자율화시스템을 통해 사람의 개입없이 의사결정을 하고 또는 최소한의 개입으로 선박의 관리 및 제어의 전체 또는 일부를 대신할 수 있는 선박을 의미한다. 자율운항선박은 부분자율운항선박과 완전자율운항선박으로 구분하게 되는데 해사산업에서는 스마트 쉽, 무인선박, 자율운항선박 등 다양한 용어로 혼재되어 사용되고 있다[2].

## 2. 자율 기술 수준(Level of Autonomy)[3]

Table 1. Level of Autonomy

Level	Data acquisition/ Analysis	Decision-making	Action
AL 1	System or operator	Operator	Operator
AL 2	System/remote	Operator(System/remote)(1)	Operator
AL 3	System/remote	System/remote (Operator)(2)	System/remote
AL 4	System	System(3)	System(3)
AL 5	System	System	System

[Remarks]  
 (1) It supports operator decision-making either through the system or remotely, but the final decision is made by the operator.  
 (2) Operator confirmation of decision-making is required.  
 (3) Decision-making and execution are constantly monitored by the operator.

각 자율 기술 수준의 정의는 다음과 같다[4].

- AL 1 : 데이터 수집/분석은 운영자 및 시스템에 의해서 수행될 수 있지만 수집된 정보를 바탕으로 한 의사 결정 및 그 실행은 운영자가 수행한다.
- AL 2 : 시스템 또는 선외의 원격 운영을 통해 데이터가 수집/분석되고 그에 따른 의사 결정 및 실행은 운영자가 수행한다. 시스템은 운영자의 의사 결정에 대하여 운영자를 지원한다. 시스템 또는 선외로부터 원격 운영을 통해서 운영자의 의사 결정을 지원한다.
- AL 3 : 시스템 또는 선외의 원격 운영을 통해서 데이터가 수집/분석되고 그에 따른 의사 결정 및 실행도 시스템 또는 원격 운영에 의해 수행된다. 단, 시스템에 의한 의사 결정에 대한 운영자의 확인이 반드시 요구되며, 운영자 확인이 선행되지 않을 경우 해당 의사결정 사항을 철회한다. 시스템 고장 시 또는 원격운영이 원활하지 않은 경우 운영자의 대응이 필요하다.
- AL 4 : 시스템에 의해서 데이터가 수집/분석되고 그에 따른 의사 결정 및 실행도 시스템에 의해 수행된다. 시스템에 의한 의사 결정 및 그 실행에 대한 정보를 운영자가 항상 모니터링 한다. 비정상 운용 시나리오(시스템고장 등)에 대하여 시스템의 대응이 가능하다.
- AL 5 : 완전한 자율수준으로서 데이터 수집/분석, 의사 결정 및 실행 등 모든 기능이 시스템에 의해 수행되며 운영자는 비상 상황을 모니터링 한다. 비정상 운용 시나리오(시스템 고장 등)에 대하여 시스템의 대응이 가능하다.

## 3. 선박 간의 사용자 인증

선박 간의 사용자 인증은 선박의 보안을 강화하고 인가된 사용자인 이 선박 시스템에 접근하고 조작할 수 있도록 하는 중요한 요소이다. 다양한 방법과 기술이 사용되며 일반적으로 사용되는 방법은 다음과 같다.



Fig. 1. Classification of user authentication recommendations

1) 암호화된 인증 : 사용자 인증에는 암호화된 인증 정보가 사용된다. 일반적으로 사용자는 개인 식별 정보 (예 : 사용자 이름, 비밀번호, PIN)를 입력하여 시스템에 로그인하고 자신을 인증한다. 이 정보는 안전하게 저장되어야 하며, 암호화된 형태로 전송되고 저장되어야 한다[5].

2) 스마트 카드 또는 토큰 : 스마트 카드나 토큰은 사용자 인증에 사용되는 물리적인 장치이다. 선박의 사용자는 개인적인 스마트 카드나 토큰을 소지하고, 이를 선박 시스템에 연결하여 인증할 수 있다. 이러한 장치는 고유한 식별 정보를 가지고 있으며, 카드 패스워드 또는 생체 인식과 같은 추가적인 보안 기능을 사용할 수 있다.

3) 생체 인식 기술 : 생체 인식 기술은 사용자의 생체적인 특징 (예 : 지문, 홍채, 얼굴)을 사용하여 인증하는 방법이다.

4) 이중 인증 : 이중 인증은 두 개 이상의 인증 요소를 동시에 사용하여 사용자를 인증하는 방법이다. IEC 62443-4-2 구성요소 식별 및 인증제어에서 Security Level 4에 해당한다[6]. 예를 들어, 비밀번호와 스마트 카드를 함께 사용하여 인증할 수 있다. 이렇게 함으로써 보안 수준을 높이고 사용자의 신원을 더욱 확실하게 확인할 수 있다.

선박 간의 사용자 인증은 보안 요구 사항과 해당 규정에 따라 설계되고 구현되어야 하며, 또한 중요한 측면은 인증 시스템의 안전성과 인정성을 유지하기 위해 주기적인 업데이트와 강화된 보안 대책을 시행하는 것이다.

## III. Conclusions

해양 산업은 e-Navigation 시스템을 시작으로 체계적인 접근 방식과 다양한 전략을 수행하고 있다. 다양한 해양 서비스를 제공하고 있으며, 서비스 운영에 필수적인 장비 개발 및 스마트 항로표지 서버 구축 등 통합 운영이 가능한 스마트 항만을 목표로 나아가고 있다. 그러나 스마트 항만을 고도로 자동화된 시스템을 구축하고 검증하기 위해 사이버 보안 측면에서는 잠재적으로 발생 가능한 치명적인 위험 요소들을 고려할 필요가 있다. 선박 간의 사용자 인증은 서로 다른 기관 혹은 사용자의 신뢰 관계가 중요하며, 다양한 방법으로 기반한 인증 방식들을 연구하고 있으며 한국 해양산업에서는 IHO S-100과 IEC 63173-2(SECOM) 표준을 기준으로 스마트 항로표지를 위한 테스트베드를 구축하고 있다. 본 논문에서는 인간이 개입하지 않는 자율운항 개발 단계에서 사용자 인증이 더욱더 중요하며 다양한

사용자 인증 방식에 대한 시스템을 제안하였다.

## ACKNOWLEDGEMENT

이 논문은 2023년 해양수산부 재원으로 해양수산과학기술진흥원의 지원을 받아 수행된 연구임 (해양 디지털 항로표지 정보협력시스템 개발 (3/5) (20210650))

## REFERENCES

- [1] Sung-Hwa Hong.(2020).An Efficient Method of Coastal and Offshore Communication for Safe Navigation of Autonomous Ships.Korea Institute of information and Communication Engineering Vol ,24(2),161-162.
- [2] Kim Jin, Jang Hwa-seop.(2019). Technology Trends and Preparation of Autonomous Ship. Bulletin of the Society of Naval architects of Korea, 56(4),4-7
- [3] Park Han-sun. (2022). Recent IMO Trend analysis and regulatory improvement of autonomous ships. Bulletin of the Society of Naval architects of Korea, 59(4),59-61
- [4] Guidelines for Autonomous Shipping.(2022). Korean Register.
- [5] Universal Hydrographic Data Model(S-100). IHO
- [6] Secure Communication between Ship and Shore(SECOM) IEC 63173-2. IEC