

# 자율운항선박 운영을 고려한 VTS 관제시스템의 사이버보안 만족도 조사: 부산항 VTSO 사례연구

유윤자\* · † 박한선 · 박상원\*\*

\*한국해양수산개발원 해사안전연구실 전문연구원, † 한국해양수산개발원 해사안전연구실 연구위원, \*\*한국해양수산개발원 해사안전연구실 연구원

**요약** : 우리나라는 국제해사기구에서 제시한 자율수준 3단계의 자율운항선박 기술개발 사업을 추진 중에 있으며, 자율운항선박 및 원격 운항센터의 사이버보안에 관한 기술개발이 핵심과제로 포함되어 있다. 국제해사기구는 현존선의 대한 사이버 위협에 대한 조치로 제98차 해사안전위원회에서 ‘해상 사이버 위험관리 지침(Guidelines on maritime cyber risk management)’을 채택 및 승인하였다. 자율운항선박이 디지털 센서의 거대시스템임을 고려할 때 기술개발 완료시 해상에서 기존 선박과 자율운항선박의 공동 운항을 고려하여 해상교통관제체계(VTS)에 대한 사이버보안 측면을 고려 할 필요가 있다. 이 논문에서는 부산항 VTS 관제사(VTSO)를 대상으로 하여 자율운항선박 운영을 고려한 VTS 관제시스템의 사이버보안 만족도를 조사하였다. VTSO를 대상으로 한 사이버보안 만족도 조사 및 분석방법은 IPA(Importance Performance Analysis) 매트릭스를 적용하였다.

**핵심용어** : 자율운항선박, 사이버보안, VTS, VTSO, IPA 분석기법

**Backgrounds**

- MSC 98<sup>th</sup> Session approved *Guidelines on maritime cyber risk management* in 2017(Source: Res. MSC.428(98)).  
**ENCOURAGES** Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 Jan. 2021.
- Urgent need to raise awareness on *Cyber risk threats and vulnerabilities*** to support safe and secure shipping, which is operationally resilient to cyber risks.  
**RECOGNIZING** that Administrations, classification societies, ship-owners and ship operators ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities.

⇒ How to strengthen cybersecurity (KMI)

KINPR 2019 2/22

**Backgrounds**

자료: Global Maritime Forum(2018), Global Maritime Issue Monitor, p.7.

⇒ How to strengthen cybersecurity (KMI)

KINPR 2019 3/22

**What is the cyber risk ?**

- Types of Cyber attack**  
**MALWARE** Malicious software which is designed to access or damage a computer without the knowledge of the owner. There are various types of malware including *trojans, ransomware, spyware, viruses, and worms*(Source: The guidelines on cyber security onboard ships, BIMCO 2017).  
**PHISHING** Sending emails to a large number of potential targets asking for particular pieces of sensitive or confidential information.  
**WATER HOLING** Establishing a fake website of compromising a genuine website to exploit visitors.  
**SCANNING** Attacking large portions of the internet at random.  
**SOCIAL ENGINEERING** A non-technical technique used by potential cyber attackers to manipulate insider individuals into breaking security procedures, normally, but not exclusively, through interaction via social media.

KINPR 2019 4/22

**What is the cyber risk ?**

- Types of Cyber attack**  
**BRUTE FORCE** An attack trying many passwords with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords until the correct one is found(Source: The guidelines on cyber security onboard ships, BIMCO 2017).  
**DENIAL OF SERVICE(DoS)** Prevents legitimate and authorised users from accessing information, usually by flooding a network with data. A Distributed Denial of Service(DDoS) attack takes control of multiple computers and/or servers to implement a DoS attack.  
**SPEAR PHISHING** Like phishing but the individuals are targeted with personal emails, often containing malicious software or links that automatically download malicious software.  
**SUBVERTING THE SUPPLY CHAIN** Attacking a company or ship by compromising equipment, software or supporting services being delivered to the company or ship.

KINPR 2019 5/22

† 교신저자 : 종신회원, hspark@kmi.re.kr  
 \* 종신회원, yjyoohsy@kmi.re.kr

### What is the cyber security ?

- Cybersecurity can be defined as** the collection of *tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies* that can be used to protect the cyber environment and organisation and user's assets(Source: Overview of cybersecurity, ITU-T X.1205, 2008).
  - USER'S ASSETS** Include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.
- Cyber-Security and Cyber-Safety risks**
  - CYBERSECURITY RISKS** Potential for *intentional disruption* compromise, or exploitation of a computer network or control system by non-authorized personnel(Source: Guidelines for addressing cyber risks at maritime transportation security act(MTSA) regulated facilities, USCG 2016).
  - CYBERSAFETY RISKS** Potential for *accidental disruption* of a computer network of control system by an owner, operator, other actor, or as an unintended consequence of a mishap within a connected cyber system.

KINPR 2019

6/22

### What is the cyber security ?

- Cybersecurity attributes**
  - AVAILABILITY** Ensuring that the asset information, systems, and associated processes are consistently accessible and usable in an appropriate and timely fashion(Source: Code of practice – Cyber security for ships, UK Department for Transport 2017).
  - UTILITY** That asset information and systems remain usable and useful across the lifecycle of the ship asset. An example of loss of utility would be a situation where a ship system has been changed or upgraded and the file format of historic data is no longer intelligible to the system.
  - SAFETY** The design, implementation, operation and maintenance of ship systems and related processes so as to prevent the creation of harmful states which may lead to injury or loss of life, or unintentional physical or environmental damage. A safety issue could arise through malware causing a failure or display or communication ship systems alarm states.
  - RESILIENCE** The ability of the asset information and systems to transform, renew and recover in a timely way in response to adverse events. In the event that an outage occurs, it should be possible to recover a normal operating state, or acceptable business continuity state, in a timely manner.

KINPR 2019

8/22

### Cybersecurity related standards & guidance

- BIMCO guidelines** Cyber risk management approach as set out in the guidelines(Source: The guidelines on cyber security onboard ships, BIMCO 2017).



KINPR 2019

16/22

### How to assess importance & satisfaction ?

□ **가치 지수**는 IMAC(중요성지수)과 만족 지수 VPM(만족지수)의 차이를 의미하며, 가치 지수의 차이는 중요도나 만족도에 따라 달라진다. 양의 값은 중요도가 높고, 음의 값은 중요도가 낮고, 0은 중요도와 만족도가 같음을 의미한다.

영역	중요성지수	만족지수	가치지수	
관리적 보안	인사관리 교육	3.0	3.0	0.0
	정보 접근성 관리	3.0	3.0	0.0
	정보 접근성 관리	3.0	3.0	0.0
	정보 접근성 관리	3.0	3.0	0.0
기술적 보안	정보 접근성 관리	3.0	3.0	0.0
	정보 접근성 관리	3.0	3.0	0.0
	정보 접근성 관리	3.0	3.0	0.0
	정보 접근성 관리	3.0	3.0	0.0
물리적 보안	정보 접근성 관리	3.0	3.0	0.0
	정보 접근성 관리	3.0	3.0	0.0
	정보 접근성 관리	3.0	3.0	0.0
	정보 접근성 관리	3.0	3.0	0.0

□ **중요성지수** (평가 기준: 1-5)

□ **만족지수** (평가 기준: 1-5)

□ **가치지수** (평가 기준: 1-5)

### What is the cyber security ?

- Cybersecurity attributes**
  - CONFIDENTIALITY** The control of access and prevention of unauthorised access to ship data, which might be sensitive in isolation or in aggregate(Source: Code of practice – Cyber security for ships, UK Department for Transport 2017).
  - POSSESSION & CONTROL** The design, implementation, operation and maintenance of ship systems and associated processes so as to prevent unauthorised control, manipulation or interference.
  - INTEGRITY** Maintaining the consistency, coherence and configuration of information and systems, and preventing unauthorised changes to them. A loss of system integrity could occur through physical changes to a system, such as the unauthorised connection of a Wi-Fi access point to a secure network, or through a fault such as the corruption of a database or file due to media storage errors.
  - AUTHENTICITY** Ensuring that inputs to, and outputs from, ship systems, the state of the systems and any associated processes and ship data, are genuine and have not been tampered with or modified. Authenticity issues could relate to data such as a forged security certificate or to hardware such as a cloned device.

KINPR 2019

7/22

### Cybersecurity related standards & guidance



KINPR 2019

15/22

### How to Identify vulnerability & Assess risk ?

업무영역	영역(사양)	비율
장계	15	11.8%
해운	20	15.7%
해사	33	26.0%
정보통신	24	19.3%
보안관리	6	4.7%
기타	29	22.9%
합계	127	100%



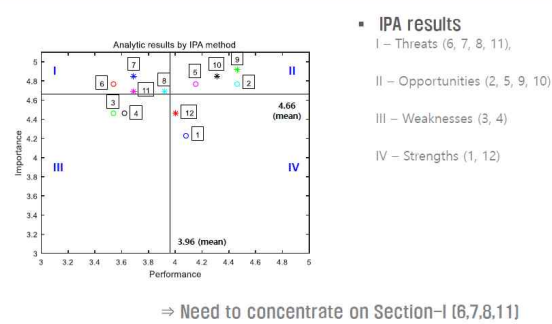
〈표 3-29〉 상대적 중요도 평가항목

대항목 (가중치)	구분	내용	점수 (%)	순위 (Rank)
A (36.3%)	관리적 보안 (Administrative Security)	A-1. 인사제고 및 교육	12.8	1
		A-2. 이동 미디어(USB 등) 통제	9.6	4
		A-3. H/W 및 S/W 접근제어	8.1	6
		A-4. 이상계획 수립	4.9	11
B (37.7%)	기술적 보안 (Technical Security)	B-1. 네트워크 접근제어	12.2	2
		B-2. 사이버 공격 탐지 및 차단	12.0	3
		B-3. 원격/무선 접근제어	6.6	10
		B-4. 데이터 백업 및 복구	6.9	9
C (28.1%)	물리적 보안 (Physical Security)	C-1. 보안구역 통제	8.8	5
		C-2. 정보 및 S/W 백업/복구	7.0	7
		C-3. 장비의 가용성/무결성 보장	6.9	8
		C-4. 데이터 및 라선스스 해킹	4.2	12

KINPR 2019

20/22

### Analytic results of importance & satisfaction by IPA method



KINPR 2019

22/22