Safety innovations through the design and application of cyber resilience in Smartship

Technical Division
Outfitting Design Department
Electric Design Team
2023.10.25

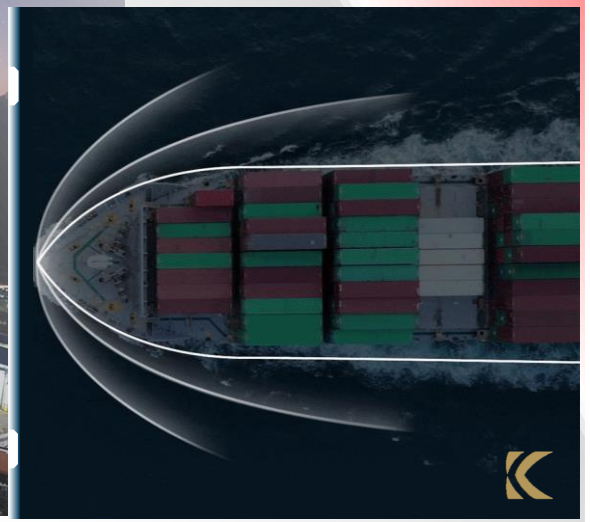
Byung-hoon Lee
Senior Manager

케이조선
K Shipbuilding

CONTENTS

케이조선
K Shipbuilding

New challenge with KHI



케이조선
K Shipbuilding

Vessel by the numbers

Abt.
100,000
meter cable

Abt.
3,300
alarms

Abt.
170
systems

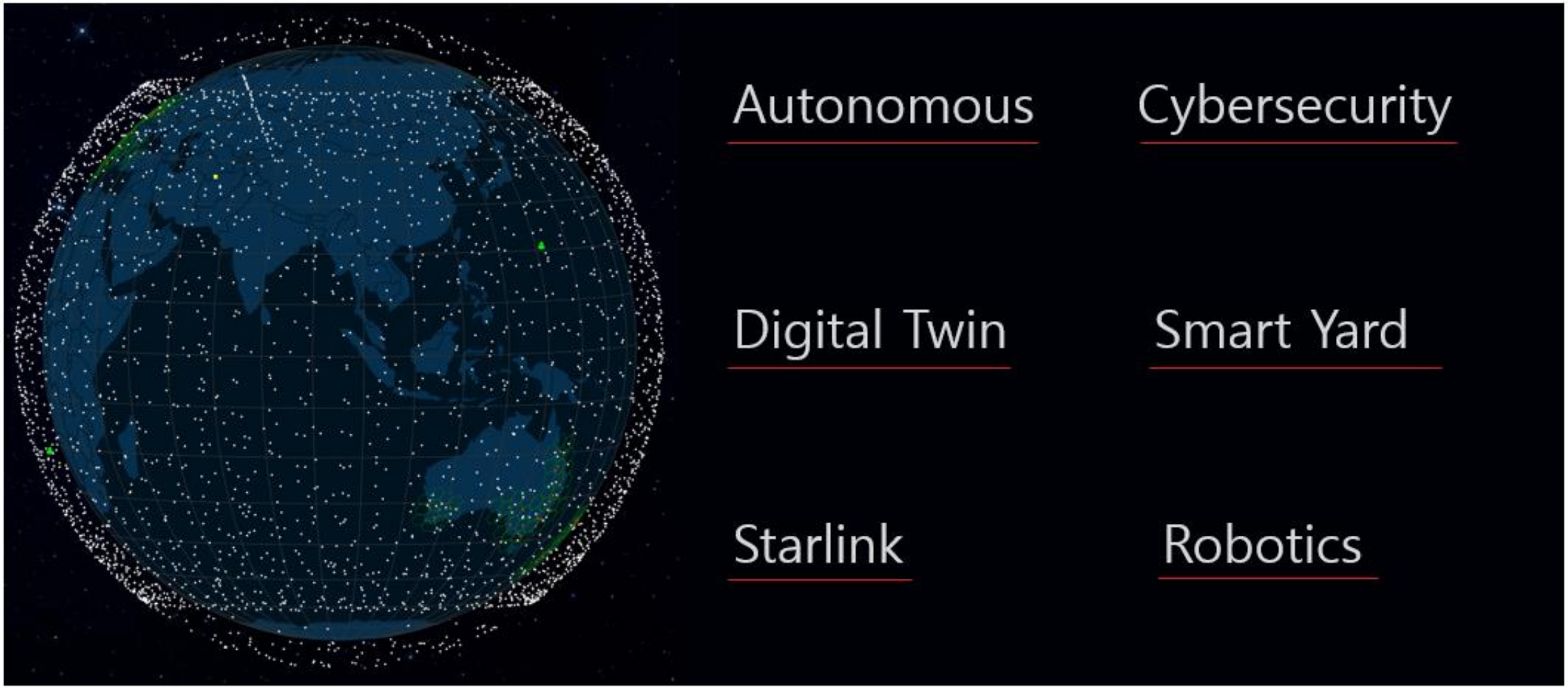
25
persons

24
Antenna

3
Satellite

케이조선
K Shipbuilding

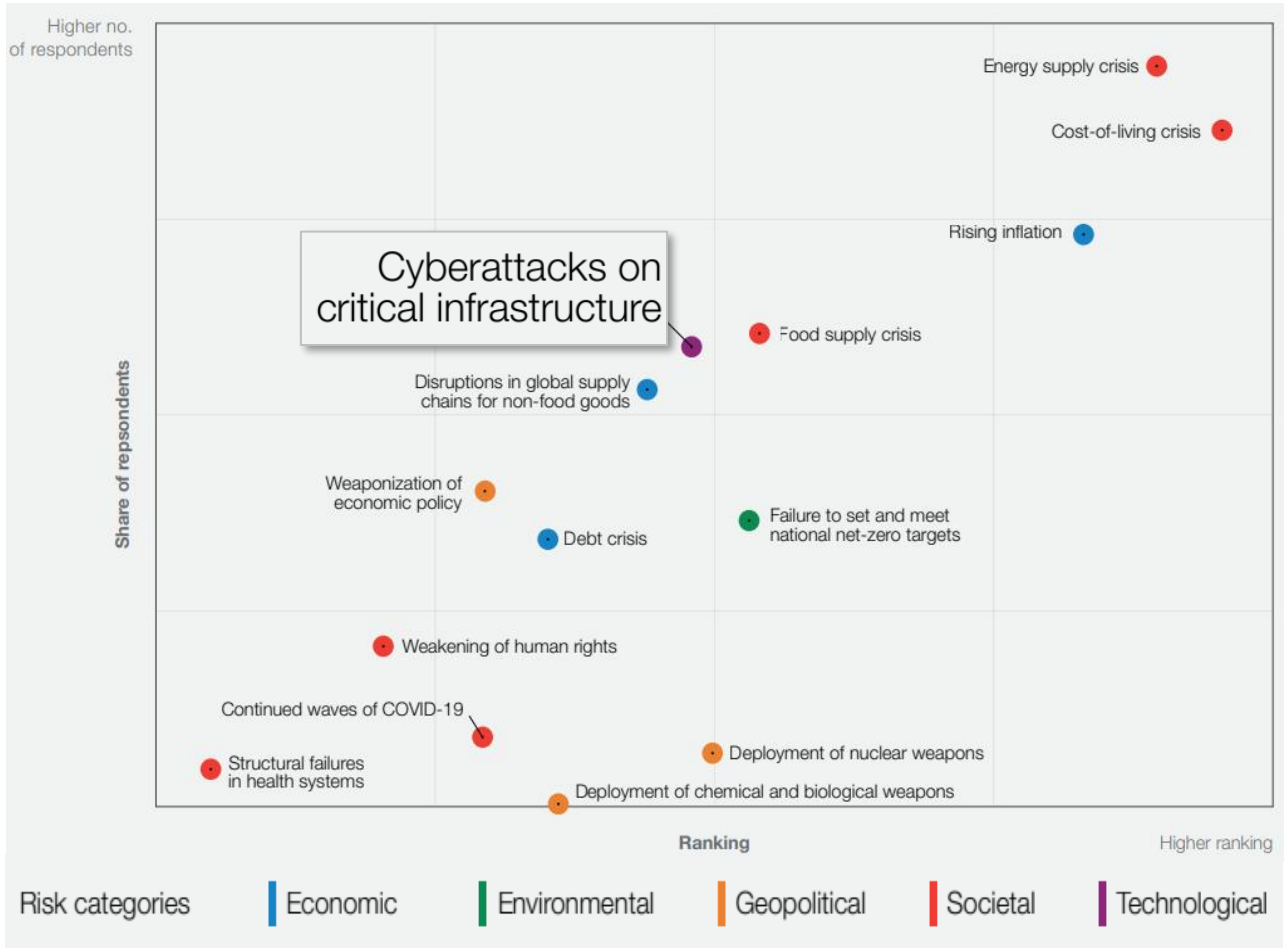
Maritime Digital Transformation by the keywords

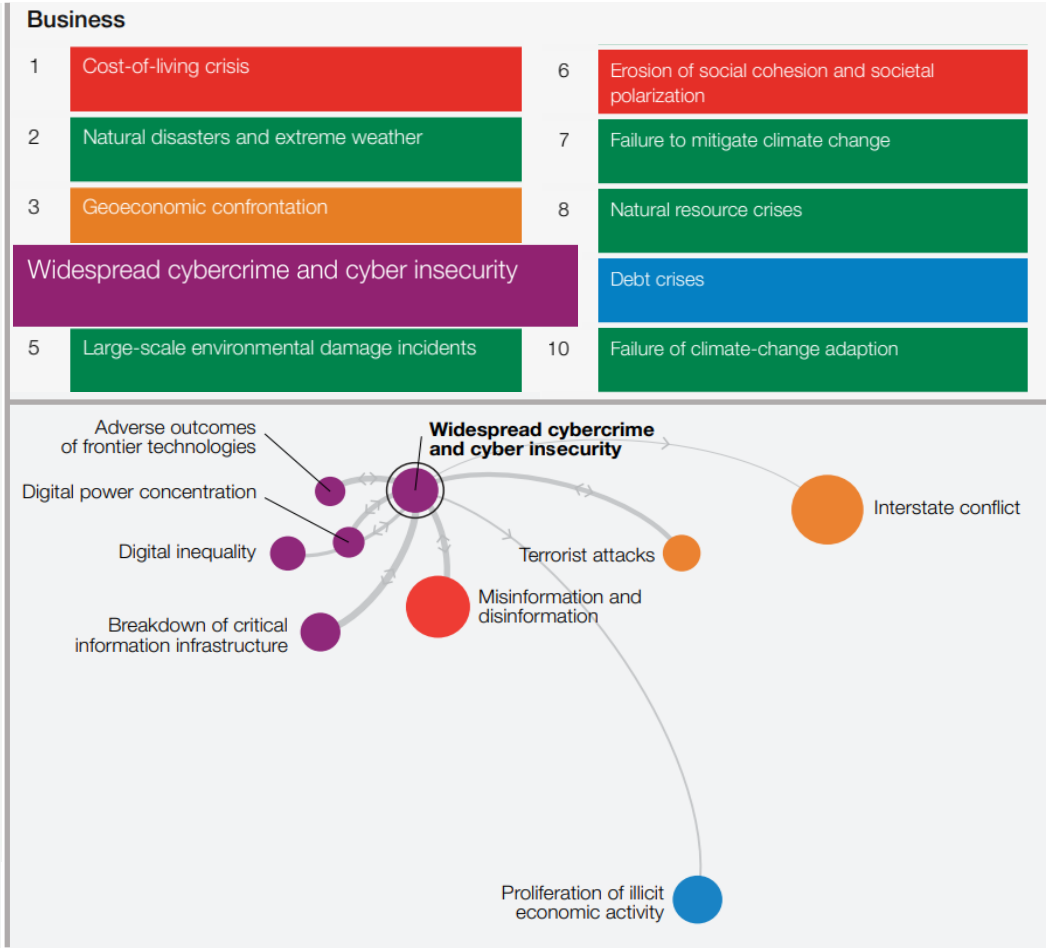


Source) Starlink satellite, https://satellitemap.space/

케이조선 K Shipbuilding

Threat of Cyber attacks





Source) 2023 world economic forum, the global risks reports 2023 [WEF_Global_Risks_Report_2023.pdf (weforum.org)]

Threat of Cyber attack in Maritime Industries

Cyberattack Threatens Release of Port of Lisbon Data

Year	Month
2022	December
Reference number	Impact area
20221201	Shore
Incident location	Incident country
Lisbon	Portugal
Victim country	Victim identity
Portugal	Port of Lisbon

world's largest classification ety hit by somware Attack acting over 0 Ships

Month	
January	
ce number	Impact area
	Shore, Offshore
location	Incident country
	Norway
country	Victim identity
	DNV Classification Society
ety, Shipping	Method Ransomware

company y a n South

Month	
June	
Impact area	
Shore	
Incident country	
South Korea	
Victim identity	
Hyundai Merchant Marine	
Method	
Malware	

- Ferry on the Borholmslinjen (Borholms line) delayed after GPS jamming incident
- Hapag-Lloyd in Hamburg hit by spear-phishing attack using phishing website
- Putin's Yacht "Graceful" hit by hacking/spoofing attack in Kaliningrad, Russia
- Mabanaft GmbH and Oil tanking GmbH Group hit by Ransomware attack in Germany
- Nine Swedish Navy vessels hit by AIS spoofing attack in the Baltic Sea
- Blue Water Shipping hit by a Malware attack in Denmark
- AIDA Cruise Ships hit by ransomware attack in Rostock, Germany
- USS Roosevelt hit by AIS spoofing attack in Polish waters to appear in Russian territorial waters near Kaliningrad
- ThyssenKrupp Marine Systems hit

n Korea
el 'Lucky Star' dark activity in gnim, North Korea
da Shipyard in Vladivostok, ia hit by DoS/GPS spoofing k
da Shipyard in Vladivostok, ia hit by DoS attack
ort of Nagoya, Japan hit by ansomware Attack by Lockbit roup
okyo MOU Port State Control in e Asia-Pacific Region belatedly eports Cyberattack in 2022
hipping line Kawasaki Kisen Kaisha K-Line) hit by data breach in Japan
hipping company K Line hit by alware attack in Japan

Source) The Maritime Cyber Attack Database, https://maritimecybersecurity.nl/

케이조선 K Shipbuilding

Threat of Cybersecurity in Korea

North Korea

Threat actor naming taxonomy: Sleet

We observed an increase in the sophistication of North Korean cyber operations and targeting overlaps among North Korean threat actors.

For more information on threat actor naming, see pages 10-11.

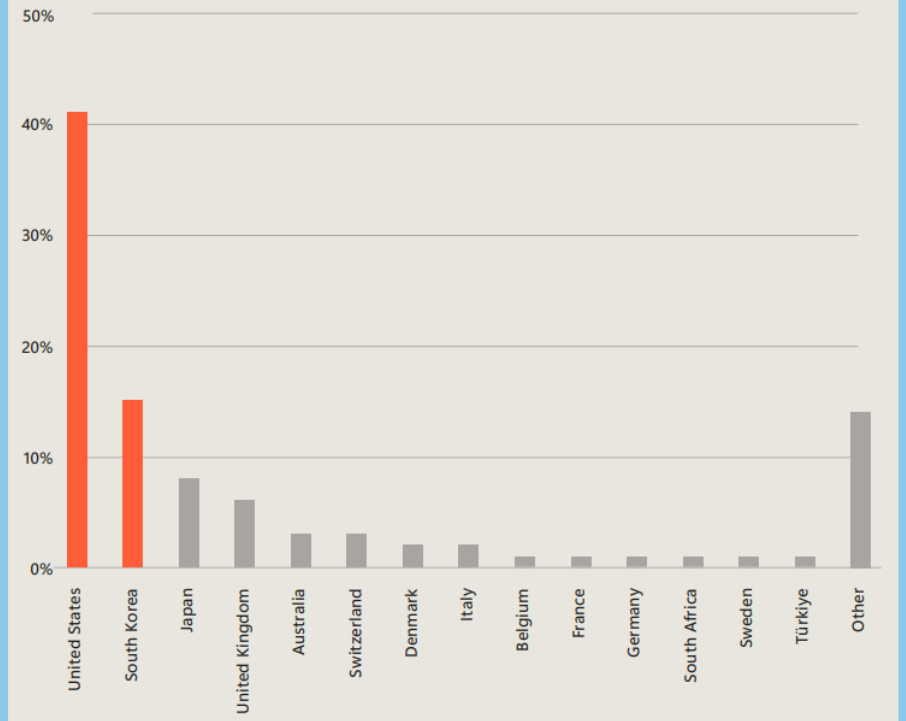
Cyber actors help fund North Korea's nuclear and missile program

North Korean leader Kim Jong Un's main priorities include expanding the country's weapons arsenal and countering the state's perceived adversaries: the United States, South Korea, and Japan.[29] North Korea test-launched a record number of missiles in 2022. As the US government estimates cyber operations now fund approximately half of North Korea's weapons program, that means Pyongyang's hackers are working harder than ever to cover growing military expenditures.[30]

In support of its goals, North Korean cyber threat actors pursue cyber operations to collect intelligence on the policy plans of these adversaries, gather intelligence about other countries' military capabilities to improve their own, and steal cryptocurrency to fund the state.

Countries most targeted by North Korean state-sponsored threat actors

Unsurprisingly, the US and South Korea comprise over 50 percent of North Korea's cyber focus.



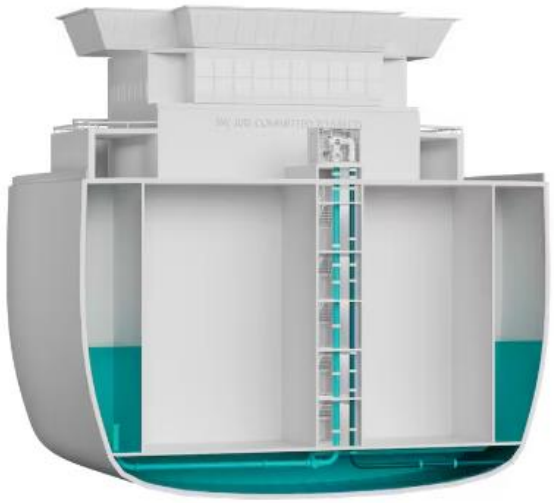
Source: Microsoft Threat Intelligence events data

Source) Microsoft Digital Defense Report 2023

케이조선 K Shipbuilding

Threat Scenarios on ships

BALLAST WATER MANAGEMENT SYSTEM



CAPSIZED

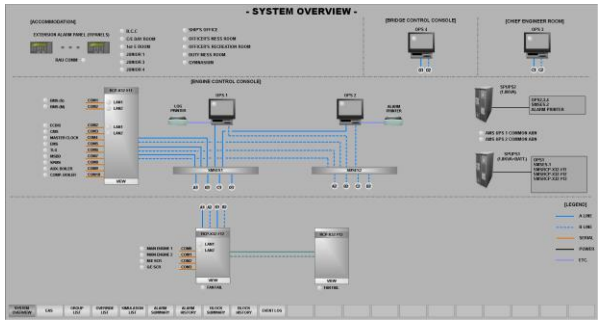
Ref. Image) https://knutsenballastwater.com/

ELECTRONIC CHART DISPLAY & INFORMATION

LOST

Ref. Image) http://marineworks.co.kr//

INTEGRATED AUTOMATION SYSTEM



CRUSH

케이조선
K Shipbuilding

Response to maritime cyber threats

International status of maritime cyber security

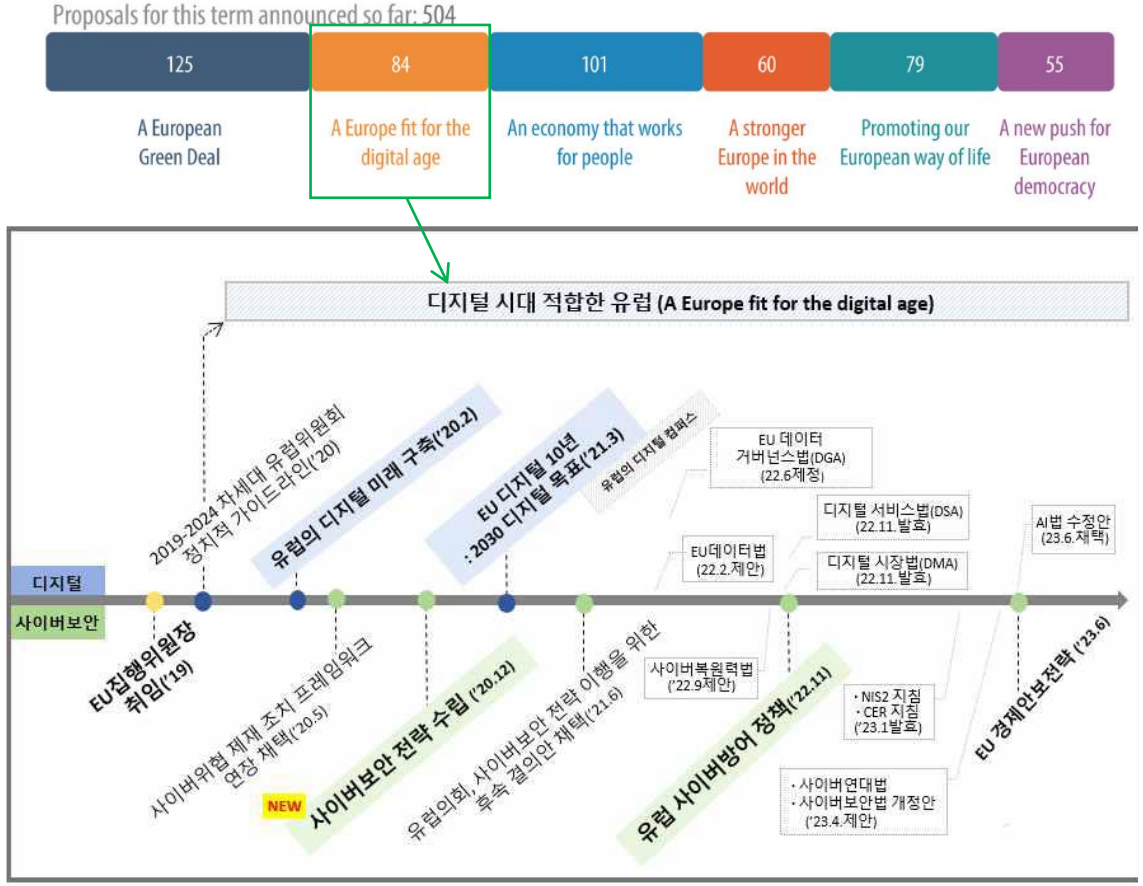
Source) Korean Register, Cyber safety Newsletter

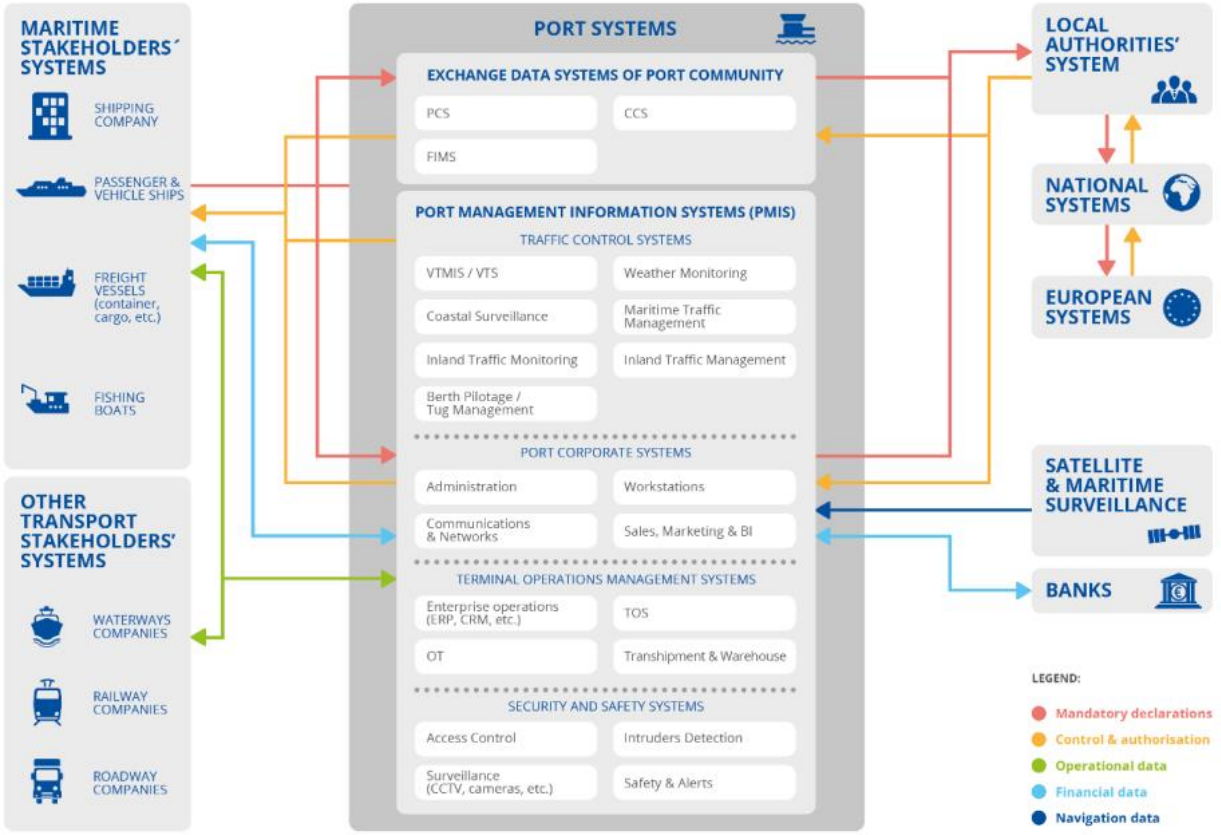
케이조선 K Shipbuilding

Response to maritime cyber threats

European Parliament

The six policy priorities of the 'von der Leyen' Commission.





Source) KISA Insight 2023 Vol.4, EU의 디지털 미래 구축을 위한 사이버보안(Cybersecurity) 방향과 시사점

케이조선 K Shipbuilding

Response to maritime cyber threats

IACS International Association of Classification Societies

ABS · RINA · IRCLASS Indian Register of Shipping · BUREAU VERITAS · CCS China Classification Society 中国船级社 · PRS · DNV · Lloyd's Register · ClassNK · KR Korean Register · CRS

2016	2018	2020	2022
Establishment	Recommendation (Deleted)	Recommendation	Unified Req.
Cyber Systems Panel	Recommendation No. 153~164	Recommendation No. 166	Unified Requirement E26 / E27

Identify	선내시스템, 사람, 자산, 데이터 및 기능에 대한 사이버보안 리스크를 관리하기 위한 조직적 이해를 개발한다.
Protect	사이버 사고로부터 선박을 보호하고 선박 운항의 연속성을 최대화 하기 위한 적절한 보호 장치를 개발 및 구현한다.
Detect	선내 사이버 사고의 발생을 탐지하고 식별하기 위한 적절한 조치를 개발하고 구현한다.
Respond	선내에서 탐지된 사이버 사고에 대한 조치를 취하기 위한 적절한 조치 및 활동을 개발 및 구현한다.
Recovery	사이버 사고로 인해 손상된 선박 운항에 필요한 모든 기능 또는 서비스를 복구하기 위한 적절한 조치 및 활동을 개발하고 구현한다.

Source) Korean Register, Overview of IACS UR E26

케이조선 K Shipbuilding

Response to maritime cyber threats

Joint Development Project

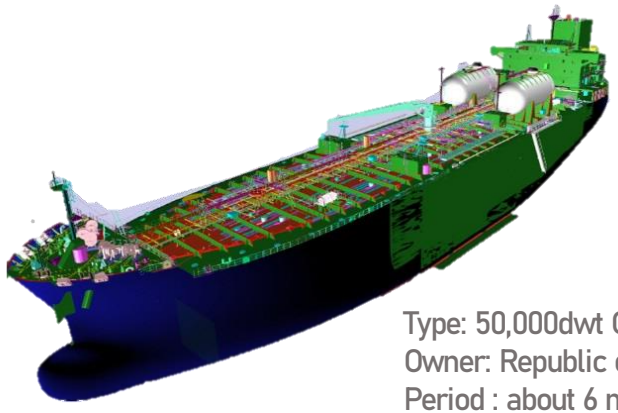
케이조선 K Shipbuilding

KR KOREAN REGISTER

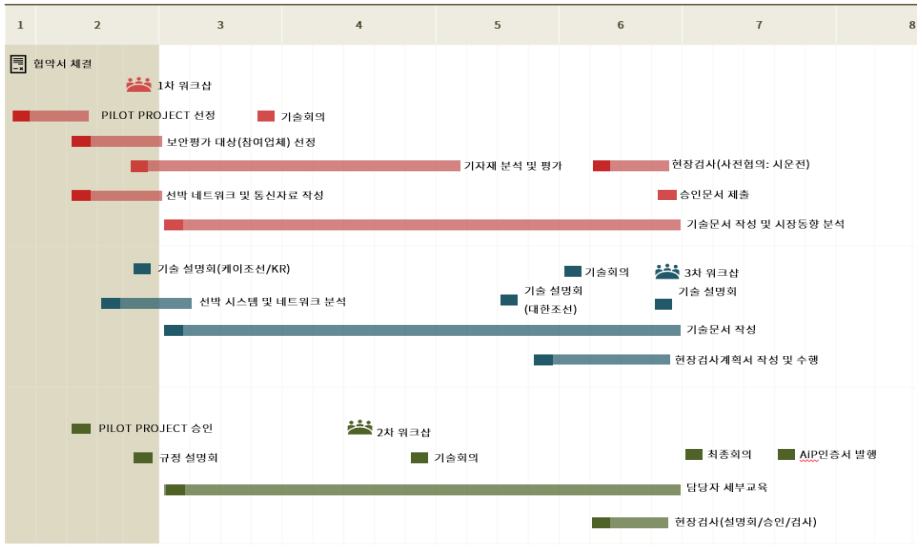
포스텍 ForceTEC

FORTINET

IGLOO



Type: 50,000dwt Oil Tanker
Owner: Republic of Korea
Period : about 6 month



케이조선 K Shipbuilding

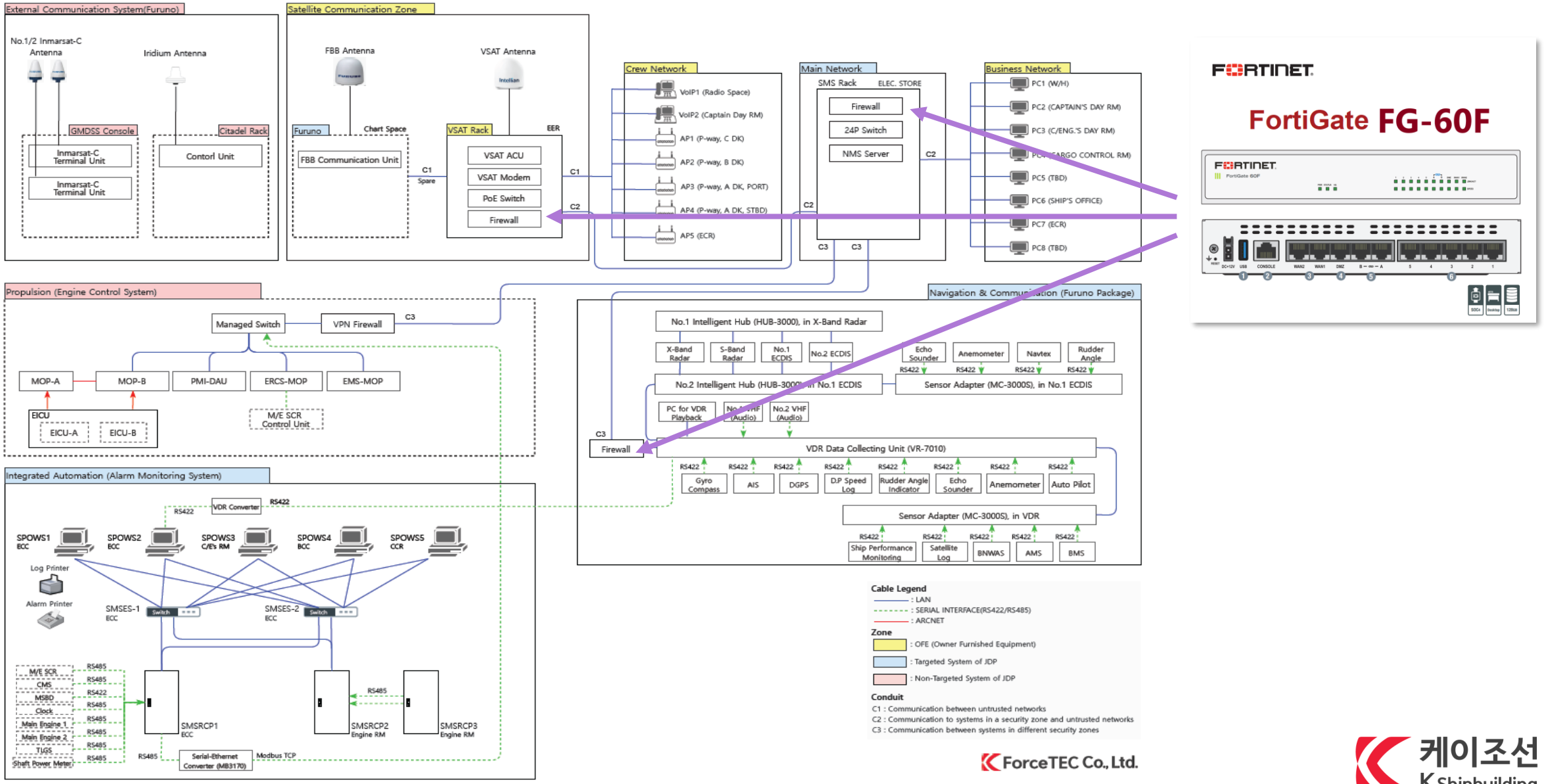
Design of Cybersecurity to onboard vessel

No.	Component Name	IP Address	Subnet Mask	MAC address	Malware Protection Means	Interface to other Systems	Interface Method	OS			Software			Firmware			Access Control Version	Maintenance Method Last update	Scope of E26 Name
								Name	Version	Last update	Name	Version	Last update	Name	Version	Name			
1	No.1 ECDIS	LAN1:XXX.XXX.XXX.XXX LAN1:XXX.XXX.XXX.XXX	XXX.XXX.XXX.XXX XXX.XXX.XXX.XXX		X	X	X	LINUX	N/A	-	BIOS	1.1	2023.X.X	BIOS	1.1	2023.X.X	N/A	-	BIOS
2	No.2 ECDIS																		
3	S-BAND RADAR																		
4	X-BAND RADAR																		
5	AIS																		
6	VDR																		
7	SPEDD LOG																		
8	SPEDD LOG																		
9	ECHO SOUNDER																		
10	No.1 GNSS																		
11	No.2 GNSS																		
12	MF/HF																		
13	No.1 INMARSAT-C																		
14	No.2 INMARSAT-C																		
15	No.1 VHF																		
16	No.2 VHF																		
17	No.3 VHF																		
18	NAVTEX																		
19	FAX																		

Example of Vessel Asset Inventory List, K Shipbuilding CS System

케이조선 K Shipbuilding

Design of Cybersecurity to onboard vessel

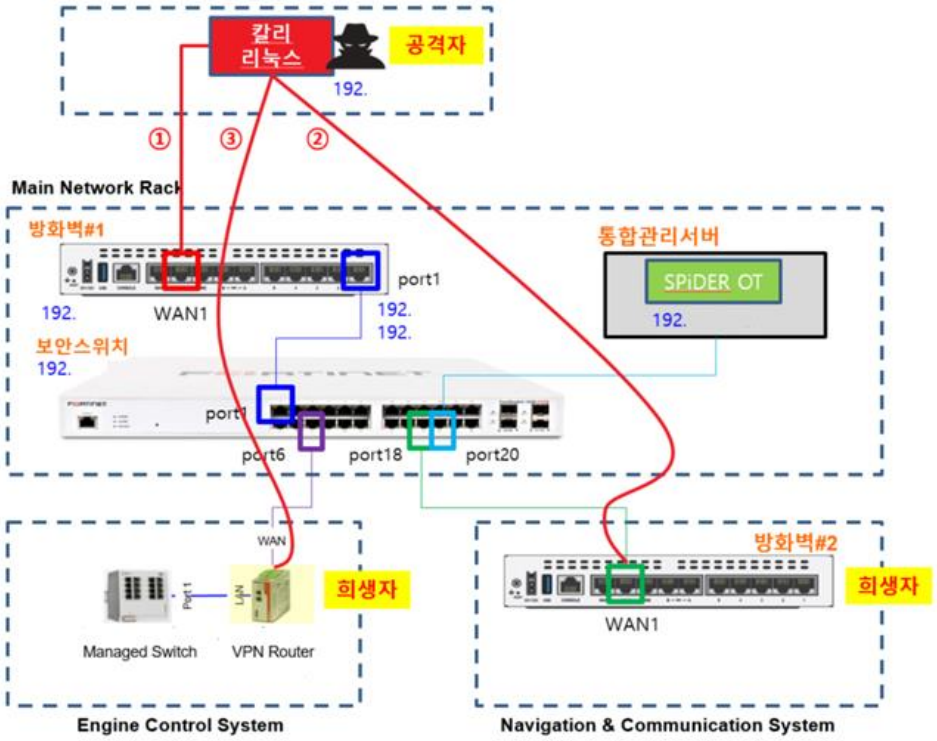


Example of Zone and Conduit Diagram, K Shipbuilding CS System

케이조선 K Shipbuilding

Design of Cybersecurity to onboard vessel

PLAN | DO | RESULT



Example of Test Plan, K Shipbuilding CS System

	Scheme of Onboard Test **Cyber Resilience of Ships**	Page	5 / 29
		Model No.	50KPC10
		Hull No.	S1936

1.5 TEST RESULT FOR 'Security Zones and Network Segmentation'

1) Result of network interface

No.	SYSTEM	EXPECTED RESULTS	RESULT	
			PASS	FAIL
1	Main Network		☐	☐
2	Navigation & Communication		☐	☐
3	Main Engine		☐	☐

2) Result of network scanning

No.	ITEM	IP ADDRESS	EXPECTED RESULTS	RESULT	
				PASS	FAIL
1	Firewall #1			☐	☐
2	FortiSwitch			☐	☐
3	SPiDER OT			☐	☐
4	Firewall #2			☐	☐
5	Intelligent Hub			☐	☐
6	VPN Router			☐	☐

3) Comment

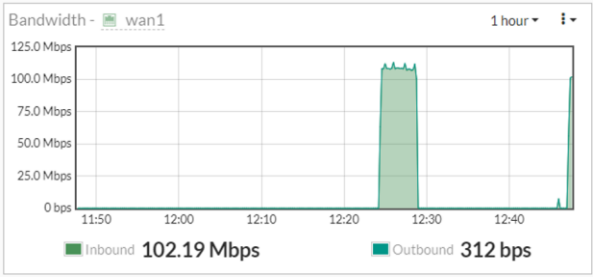
No.	ITEM	COMMENTS	REMARK

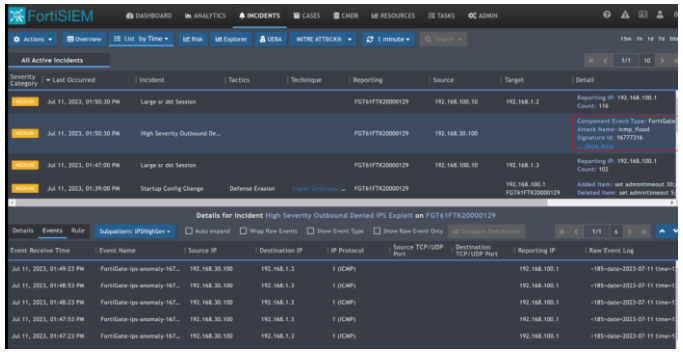
Result:

Witness : Buyer Class Builder

Date:

K Shipbuilding





케이조선 K Shipbuilding

Design of Cybersecurity to onboard vessel

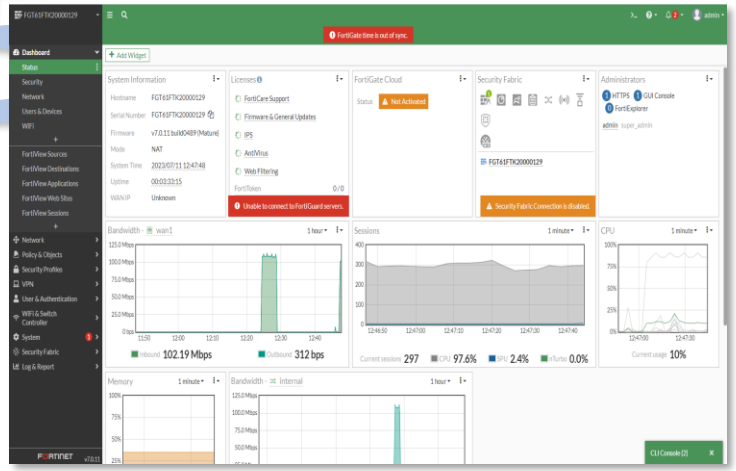
1

2

3

4

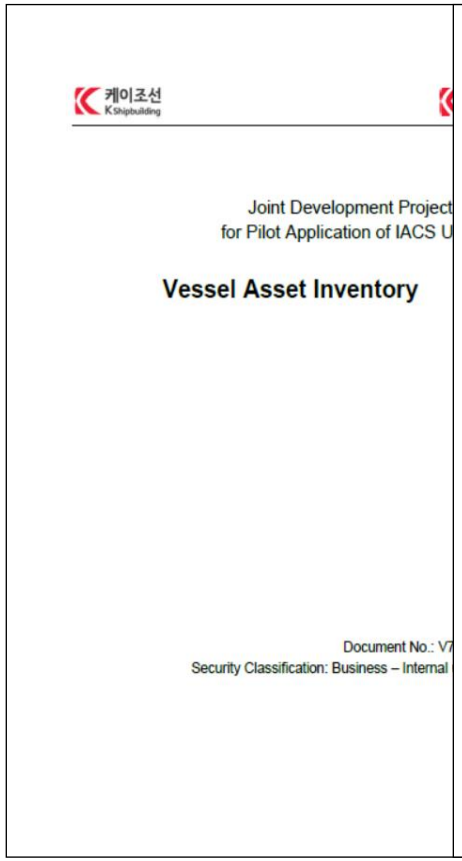
5



6

케이조선
K Shipbuilding

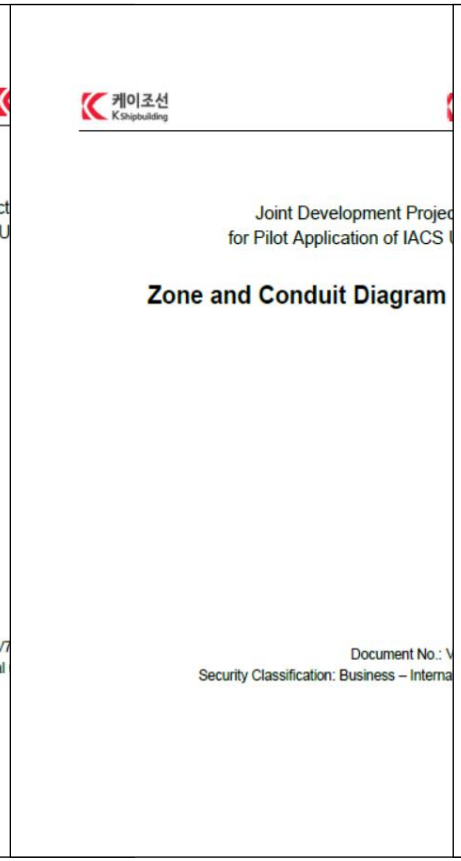
Design of Cybersecurity to onboard vessel


케이조선 K Shipbuilding

Joint Development Project
for Pilot Application of IACS U

Vessel Asset Inventory

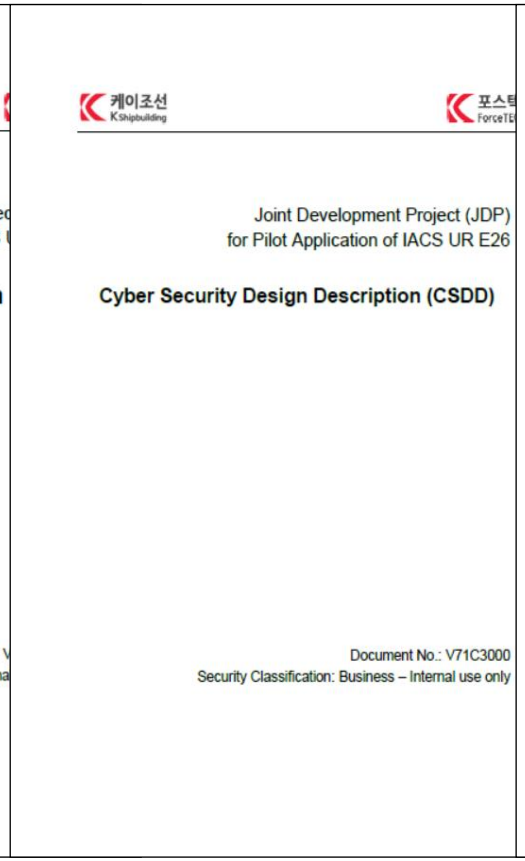
Document No.: V7
Security Classification: Business – Internal


케이조선 K Shipbuilding

Joint Development Projec
for Pilot Application of IACS

Zone and Conduit Diagram

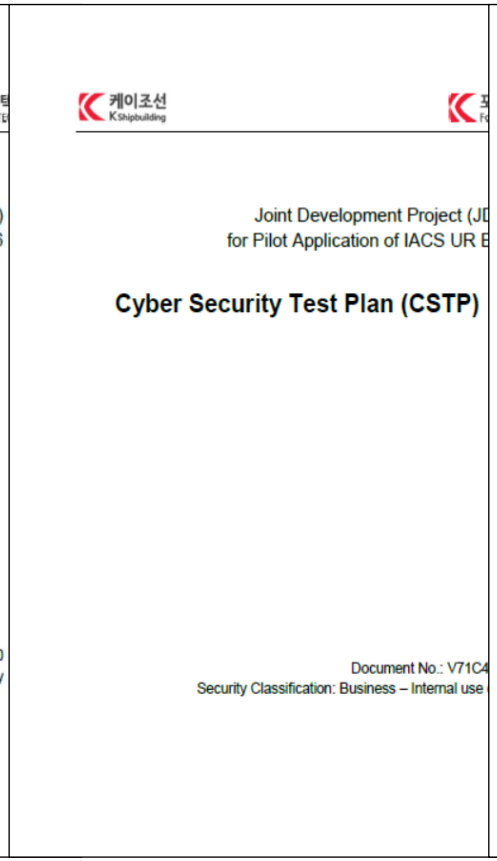
Document No.: V
Security Classification: Business – Interna


케이조선 K Shipbuilding 포스텍 ForceTEC

Joint Development Project (JDP)
for Pilot Application of IACS UR E26

Cyber Security Design Description (CSDD)

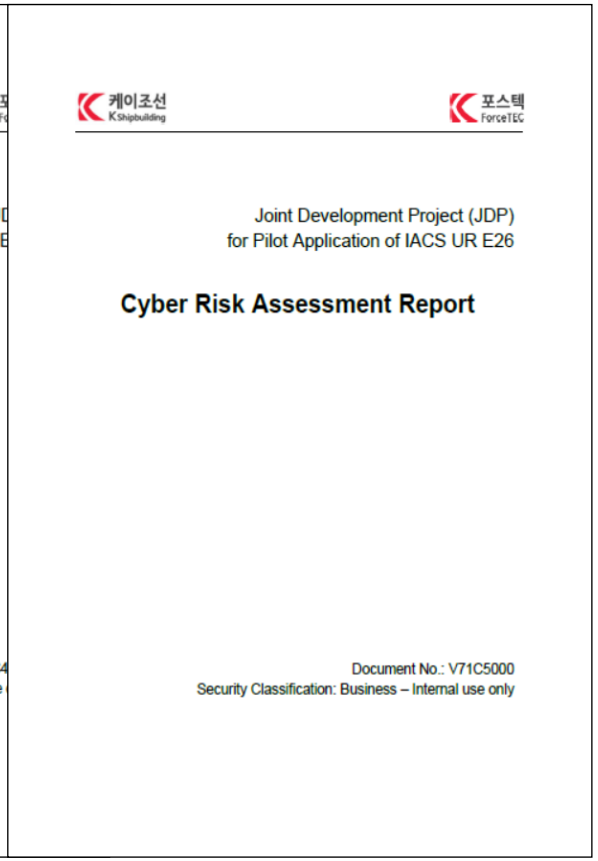
Document No.: V71C3000
Security Classification: Business – Internal use only


케이조선 K Shipbuilding

Joint Development Project (JD
for Pilot Application of IACS UR E

Cyber Security Test Plan (CSTP)

Document No.: V71C4
Security Classification: Business – Internal use


케이조선 K Shipbuilding 포스텍 ForceTEC

Joint Development Project (JDP)
for Pilot Application of IACS UR E26

Cyber Risk Assessment Report

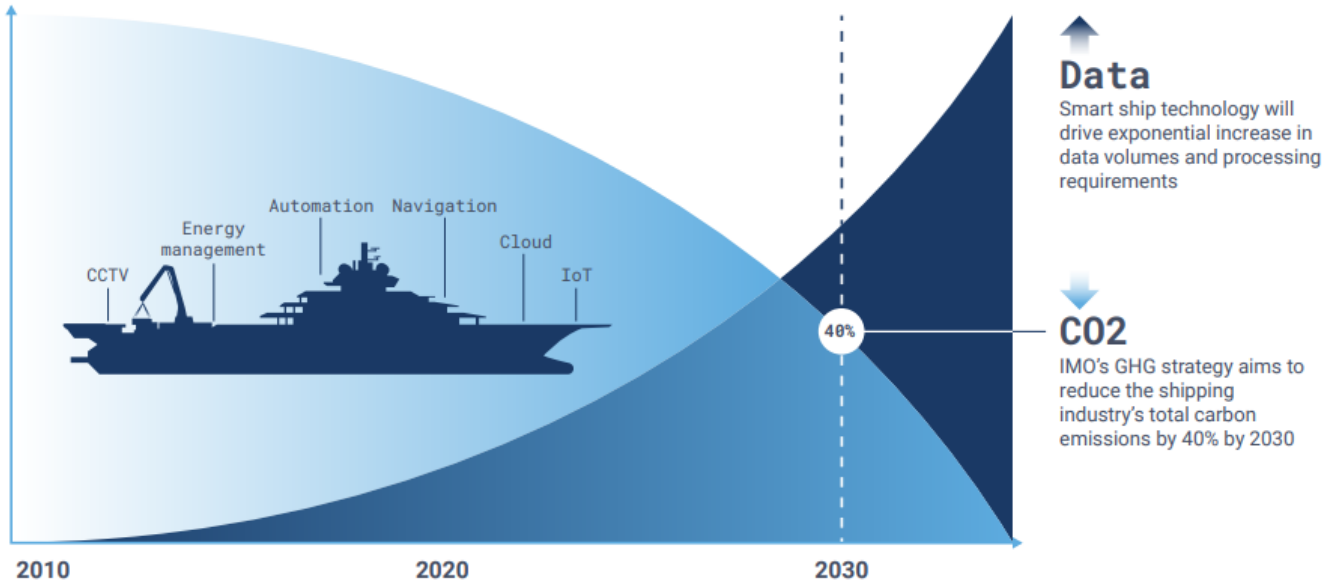
Document No.: V71C5000
Security Classification: Business – Internal use only

APPROVED document for Approval, K Shipbuilding CS System

케이조선 K Shipbuilding

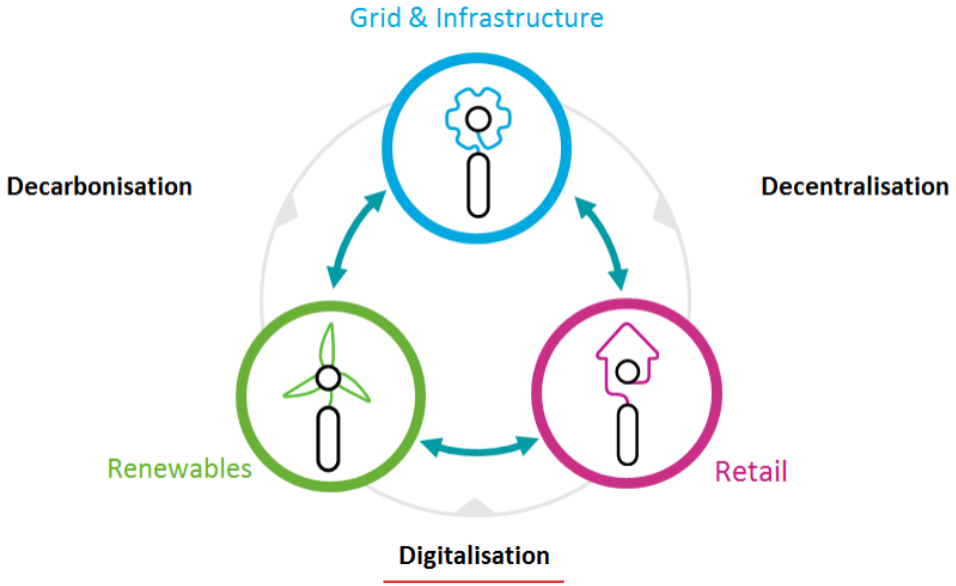
Sustainable maritime cyber security ecosystem

HANDLING THE DATA PROCESSING REQUIREMENTS OF GREEN TECHNOLOGY



Source) IMPLEMENTING SMART SHIP TECHNOLOGY TO REACH IMO 2030/2050 EMISSIONS TARGETS, Hatteland Technology

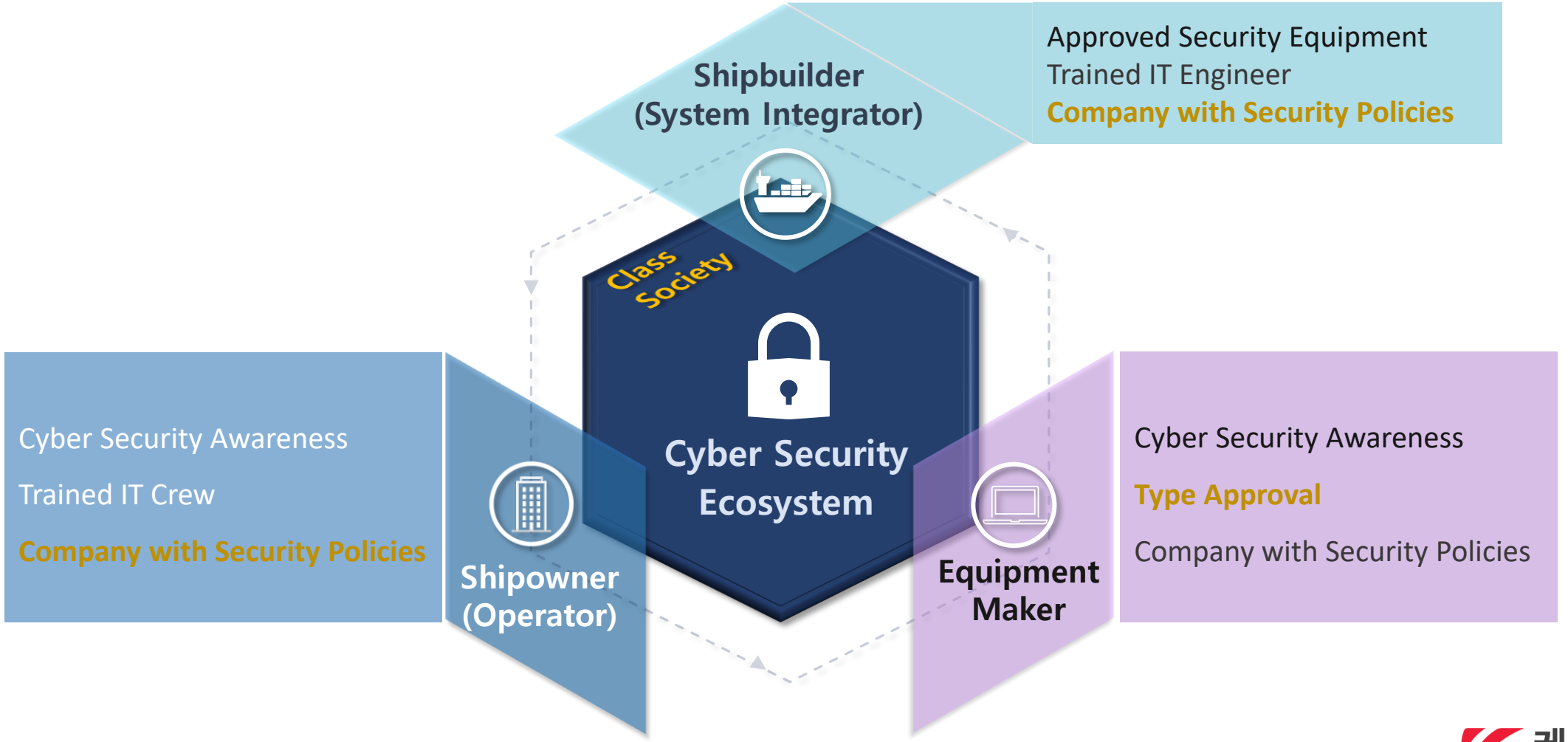
The energy world of tomorrow, 3D energy grid



Source) Digitalization is a key enabler for the energy transition, Martin Herrmann, PEEF 2017

케이조선 K Shipbuilding

Sustainable maritime cyber security ecosystem



케이조선
K Shipbuilding

Sustainable maritime cyber security ecosystem