SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Maritime Cybersecurity: Guidelines and Testbeds

Prof. Jianying Zhou

Singapore University of Technology and Design

SMI Forum 2022

iTrust @ SUTD

iTrust
Centre for Research in Cyber Security

DeST-SCI National Satellite of Excellence
Design Science and Technology for Secure Critical Infrastructure

MISSION

Advance the state of the art and practice in the DESIGN of SECURE complex interconnected critical infrastructure

VISION

To be Singapore's one-stop centre for (a) research, training, and analysis and (b) Cyber defence of Critical Infrastructure.

To be the world's leading centre for applied research in Cyber Security in the context of Critical Infrastructure.

https://itrust.sutd.edu.sg

World-Class OT Testbeds

01 Training & Education

02 R&D

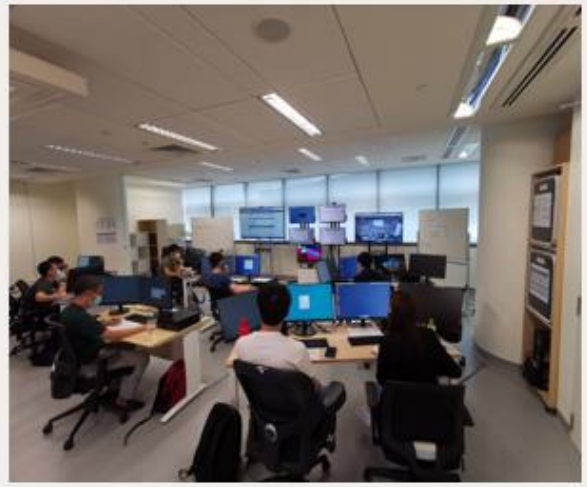
03 Tech Validation

04 Cyber Exercise

Secure Water Treatment (SWaT); 2015

Water Distribution (WADI); 2016

Electric Power & Intelligent Control (EPIC); 2017



CyberX & Internet of Things (IoT); 2016

https://itrust.sutd.edu.sg/itrust-labs_overview

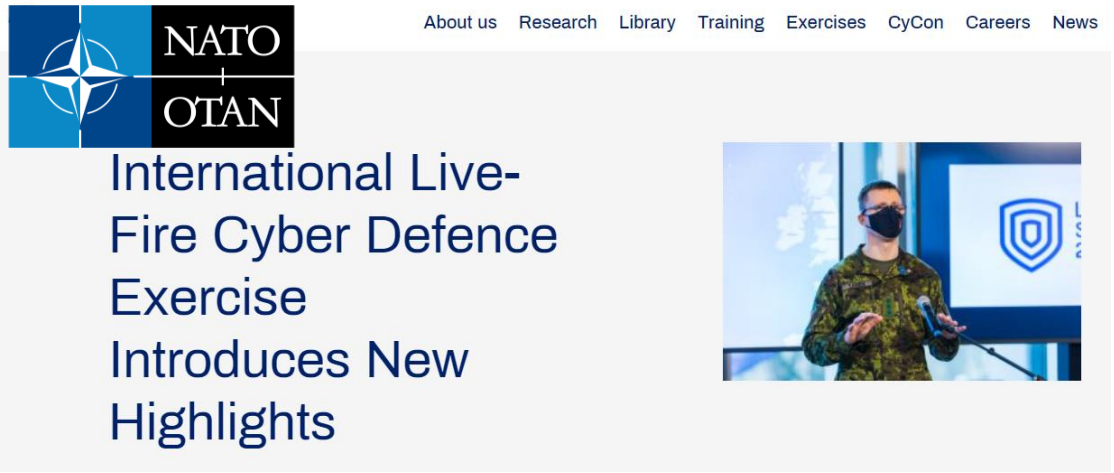
International Cyber Exercises

01 Tactics, Techniques, Procedures

02 Tech Validation

03 Tech Evaluation

Red Teaming | Blue Teaming
2016, 2017, 2019 – 2022



Crossed Swords | Locked Shields
2020 – 2022

https://itrust.sutd.edu.sg/ciss-2022

Maritime Cybersecurity

marine insight

You are here: Home › Shipping News › Maritime Cyber Attacks Increase By 900% In Three Years

Maritime Cyber Attacks Increase By 900% In Three Years

By MI News Network | In: Shipping News | Last Updated on July 20, 2020

Twitter Facebook LinkedIn Pinterest Buffer

Cyber-attacks on the maritime industry's operational technology (OT) systems have increased by 900% over the last three years with the number of reported incidents set to reach record volumes by year end.

https://www.marineinsight.com/shipping-news/maritime-cyber-attacks-increase-by-900-in-three-years/

GOV.UK Topics Government activity

Home > Government > Cyber security > Cyber security breaches survey 2022

Department for Digital, Culture, Media & Sport

Official Statistics

Cyber Security Breaches Survey 2022

Published 30 March 2022

https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

Cyberstar About us Solutions Blog

03/15/2022

How Bad Was Maritime Cyber Security in 2021? Consider These 8 Incidents

https://www.zkcyberstar.com/2022/03/15/how-bad-was-maritime-cyber-security-in-2021-consider-these-8-incidents/

Cyber Risk Management

- Increasing adoption of ICT in the maritime industry with enhanced monitoring and communication capabilities.
- However, increased connectivity introduces cyber risks.
  - *Shipboard OT systems subject to cyber attacks;*
  - *Disrupt safe operations of a vessel and cause catastrophic consequences.*
- Need to establish a guideline for cyber risk management on shipboard OT systems.
  - *Ship owners can use it as the recommended best practices for adoption;*
  - *Maritime authorities can use it to perform vessel inspections.*
- Many regulations and industry guidelines on maritime cyber risk mitigation strategies from various sources (e.g. IMO, ABS, BIMCO, DNV, ENISA, …).
  - *The target audience of the existing guidelines are those at the management/decision-making level and operator level.*

Singapore lacks its own guideline that can be easily referred to and adopted by maritime authorities and ship owners.

New Guidelines

One-year Study on Cyber Risks of Shipboard Operational Technology (OT) Systems

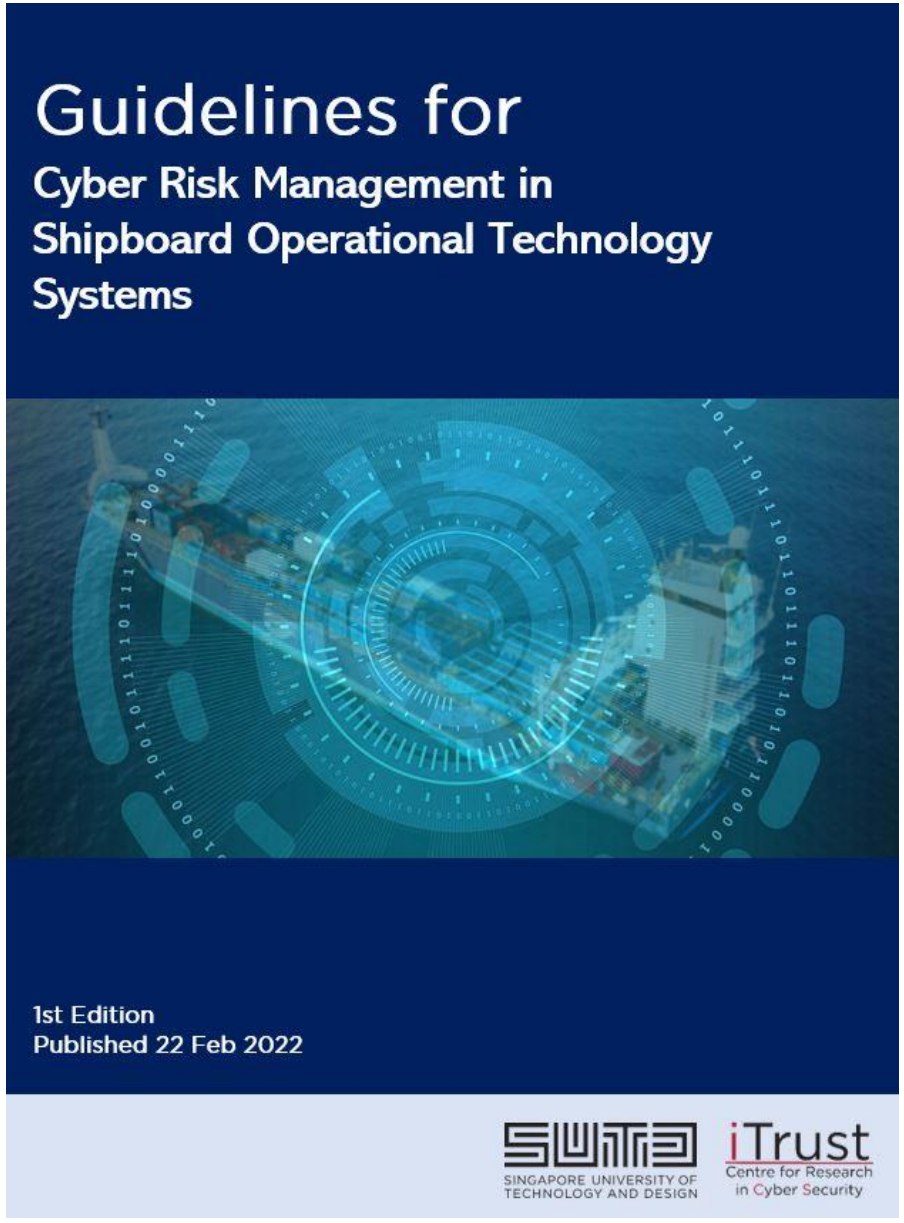
Deliverables

- **New guidelines** on cyber risk management
- **Checklist** for authorities and shipowners to conduct **cyber risk assessment**

Outcomes

- **Supported** MPA's efforts in **developing cyber notation for SRS (Nov 21)**
- **Info paper** in the 105th IMO/MSC meeting, Apr 2022

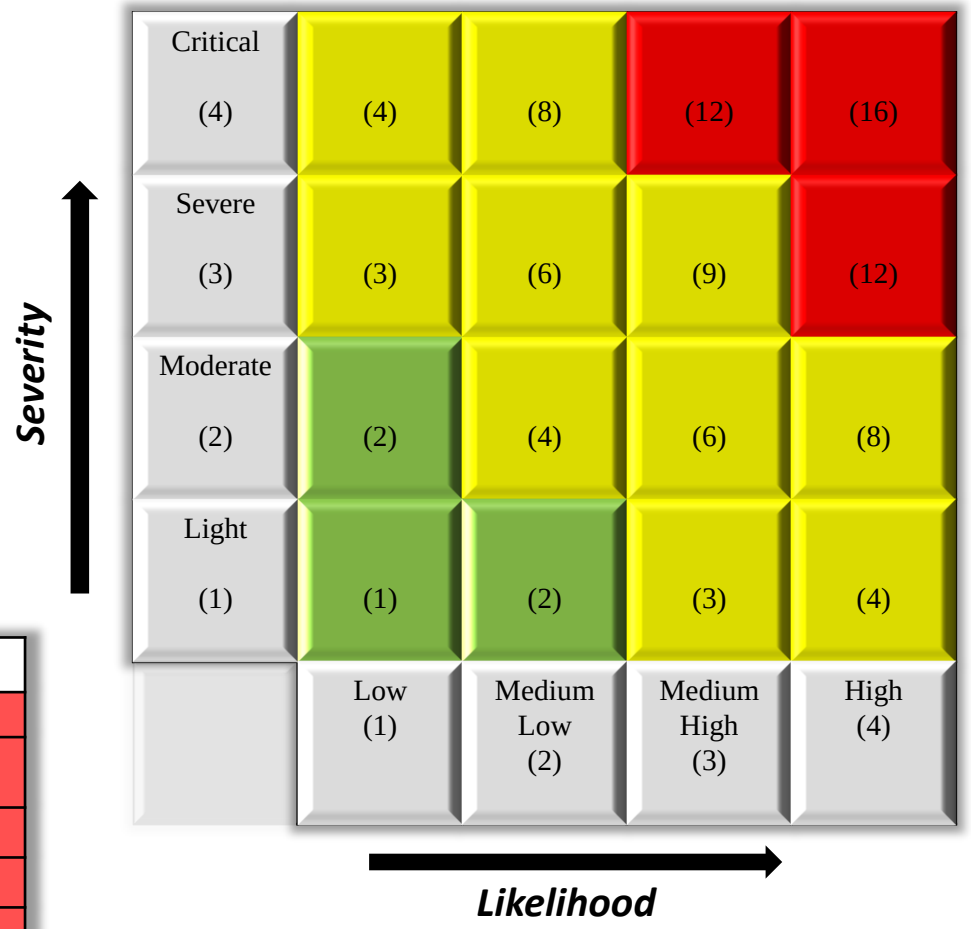
https://itrust.sutd.edu.sg/news-events/news/guidelines-for-cyber-risk-management-in-shipboard-ot-systems



New Guidelines: Cyber Risk Assessment

- Better understanding of impact of cyber risks.
- Calculate risk score for each of OT sub-systems using a 4-by-4 risk score matrix.
  - **Likelihood:** The possibility a cyber incident will occur.
  - **Severity:** The impact caused by the occurrence of the cyber incident.
  - **Risk score** = *Severity Score* x *Likelihood Score*

High risk systems	*Attack surface*	*Cyber attack*
ECDIS	USB ports, NMEA	DoS attack, virus, spoofing
SATCOM, ICS	VSAT modem/system	Phishing emails, unauthorised admin access, FTP access, command-line access
AIS	AIS messages	Spoofing
DPS	GNSS Receiver	DoS attack
GPS	GPS receiver	Spoofing
RADAR	Local ethernet switch	Malware intrusion
CCR	Malicious emails, USB ports	Ransomware, Malware
BWS	Malicious emails, USB ports	Phishing, Malware intrusion
Propulsion, Machinery & Power Control Systems	USB ports	Malware attack



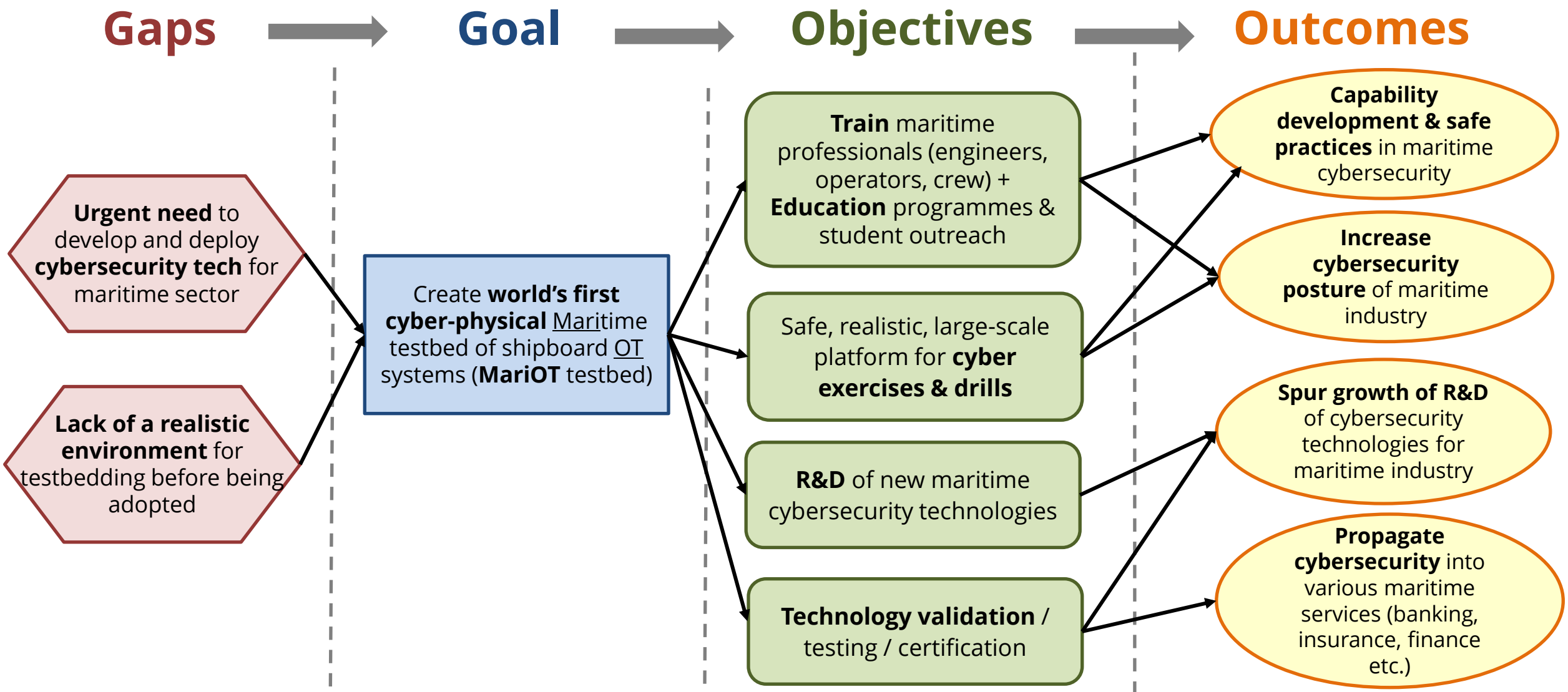
Risk Level	*Risk Score*
High	**12-16**
Medium	**3-9**
Low	**1-2**

New Guidelines: Check List

- Help to do cyber risk assessment.
- Provide actionable list of measures.
- **Tier Security:** the urgency of cyber risks of a ship to be managed.
  - **Tier -1 (Risk Score = 12–16): must have** for high risks that are most vulnerable and easy to exploit
  - **Tier -2 (Risk Score = 3–9): should have** for medium risks that are possible for an attacker to exploit
  - **Tier -3 (Risk Score = 1–2): good to have** for low risks that have less chances being exploited by an attacker

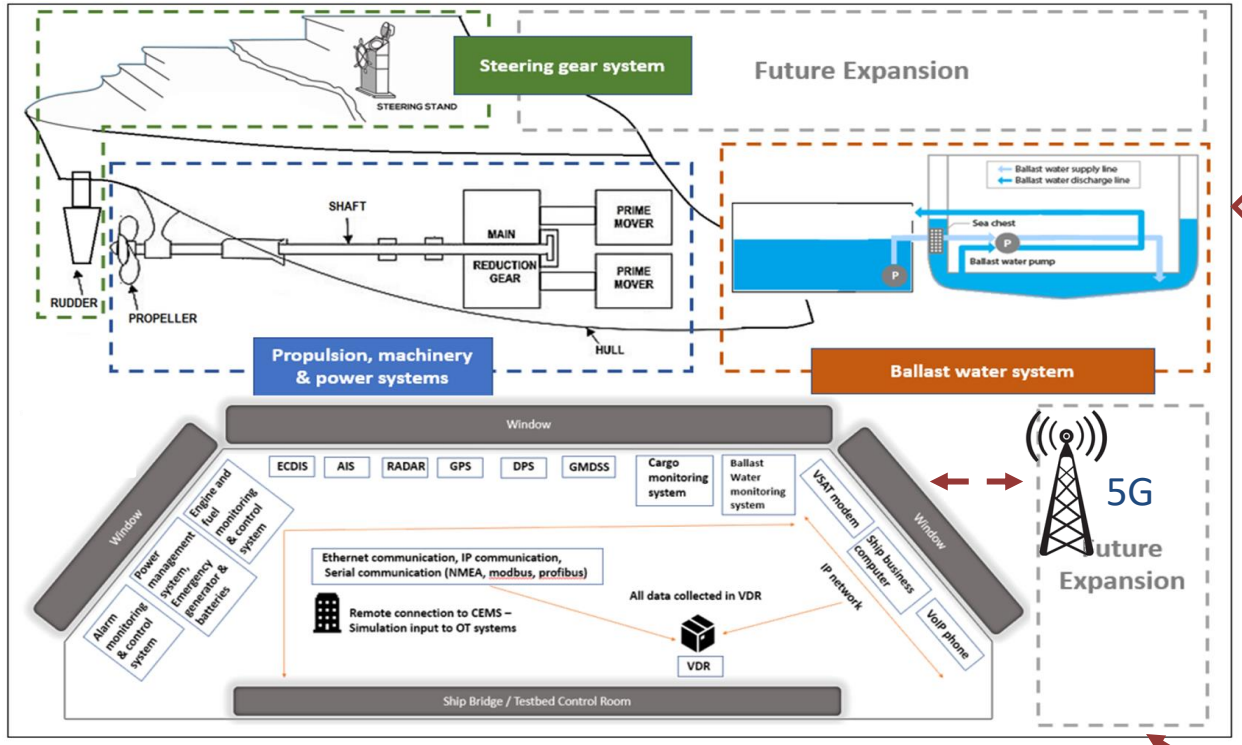
OT sub-system(s)	*Cyber risk checklist*	*Mitigation checklist*	*Security tier*
Satellite Communication System (SATCOM)	❑ Phishing email attempt	❒ **T1-13** Antivirus software is installed in the business computer. ❒ **T1-14** Files and email attachments downloaded from emails are scanned with antivirus software before opening it. ❒ **T1-15** Crew awareness is established on the following: ○ The crew can distinguish phishing emails from the real ones ○ The crew is aware that emails from unknown sources should be viewed carefully, and suspicious emails should not be opened ○ The crew is aware that they must not click on unknown URLs ❒ **T1-16** Email security is implemented in Outlook/Gmail – For example, S/MIME (Secure Multipurpose Internet *Mail* Extension) can be implemented to encrypt the email and ensure authenticity & integrity of the email.	1

Maritime Cybersecurity Testbed



New Testbed: MariOT

Physical testbed (iTrust)

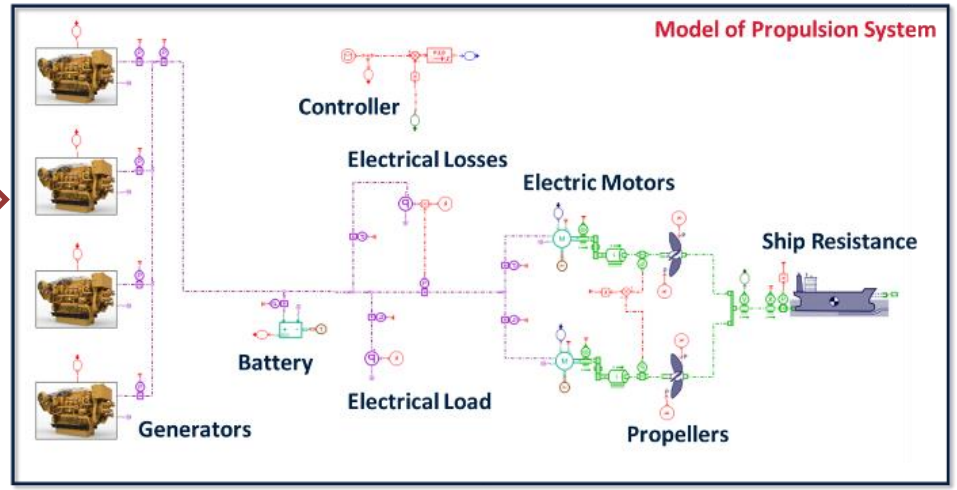


- **Flexible hybrid platform** for multi-scenario simulation
- **Common industry protocols** + open framework to connect & configure different components
- Interfaces for launching attacks and **validating new technologies**
- **Virtual models** and open cyber-physical interface to overcome physical limitations
- Connection to SUTD's **5G testbed for ship-shore comms security**

Open Interface

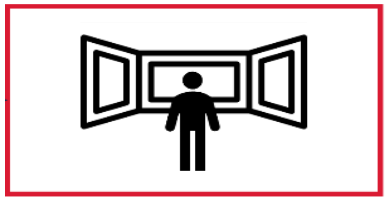
- Allows **connection to 3rd party** systems

Virtual models (ABS)



- **Simulate & incorporate** hardware due to space/hardware limitations
- Allow for **advanced/future technologies**
- **Future proof** testbed

Remote link



- **Cyber attack scenarios from MariOT** piped to simulator in crew training

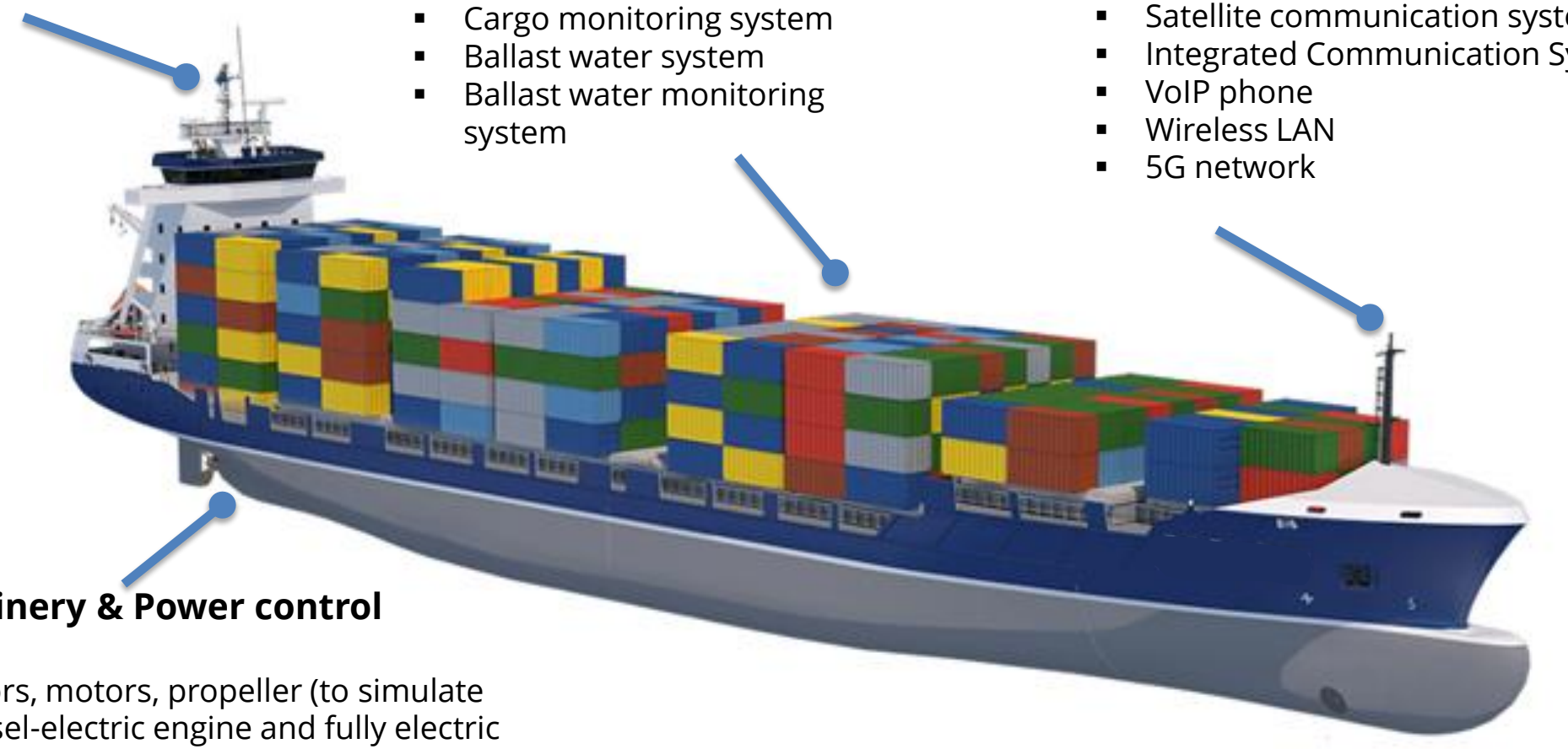
Navigation Simulator @ CEMS, Singapore Polytechnic

New Testbed: Components of MariOT

Navigation Systems
- ECDIS
- RADAR
- BNWAS
- AIS
- GPS
- DPS
- GMDSS
- VDR
- Steering gear system with Rudder

Cargo Management Systems
- Cargo monitoring system
- Ballast water system
- Ballast water monitoring system

Communication Systems
- Satellite communication system
- Integrated Communication System
- VoIP phone
- Wireless LAN
- 5G network



Propulsion, Machinery & Power control Systems
- Series of generators, motors, propeller (to simulate diesel engine, diesel-electric engine and fully electric engine)
- Engine and fuel monitoring & control system
- Alarm monitoring and control system
- Power management system
- Fire detection and monitoring system

Maritime Cybersecurity Roadmap

Proposed SUTD roadmap for R&D capability development	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033
1. **Guidelines** for Cyber Risk Management in Shipboard OT Systems		Completed													
2. **MariOT testbed:** Design and construction of maritime testbed				Develop-ment phase		Operational phase (10 years)									
3. A Digital Twin of Shipboard OT Systems and Security Testing			Cyber Attack Simulation (Shipboard) (Cyber Range / Lab)												
4. Vulnerability Discovery and Security Assessment of Shipboard OT Systems*							Risk Profiling & Assessment of Vessels								
5. New Security Solutions for Shipboard OT Systems*			Protection of Maritime Information Infrastructure (CII)^					Protection of Maritime Information Infrastructure (Non-CII^)				Secure Offline Backup			

***** Research topics under National Satellite of Excellence (NSoE) Phase II proposal, pending approval by the Cyber Security Agency of Singapore (CSA)

^ Critical Information Infrastructure

Key thrusts under SMI R&D 2030 roadmap for Maritime Cybersecurity

Thank You

Prof. Jianying Zhou

http://jianying.space/

jianying_zhou@sutd.edu.sg