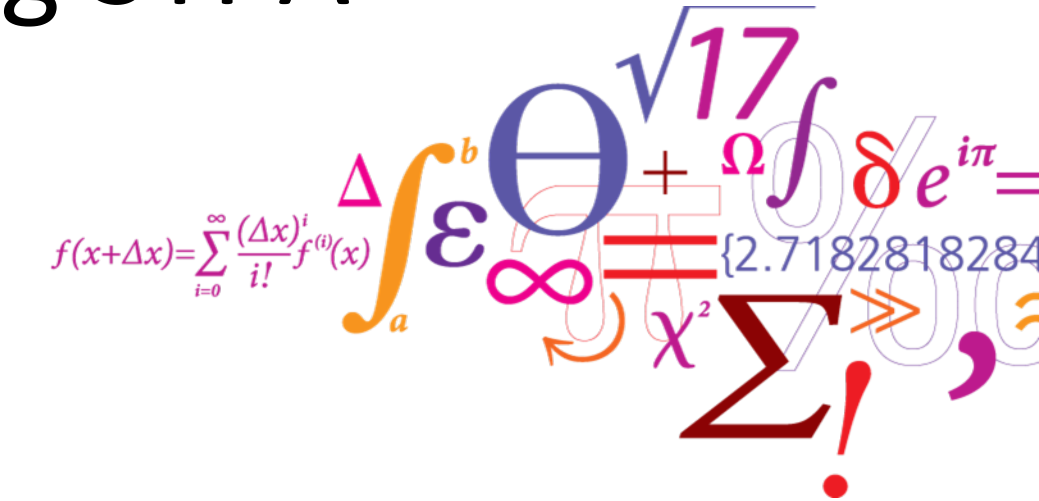
2019 STAMP Workshop

DTU Project CyberShip

Cyber-risk analysis of ship systems using STPA

Rishikesh Sahay, PhD
Daniel A. Sepulveda, PhD

25-28 March, 2019



DTU Management Engineering
Department of Management Engineering

DTU Compute
Department of Applied Mathematics and
Computer Science

Agenda

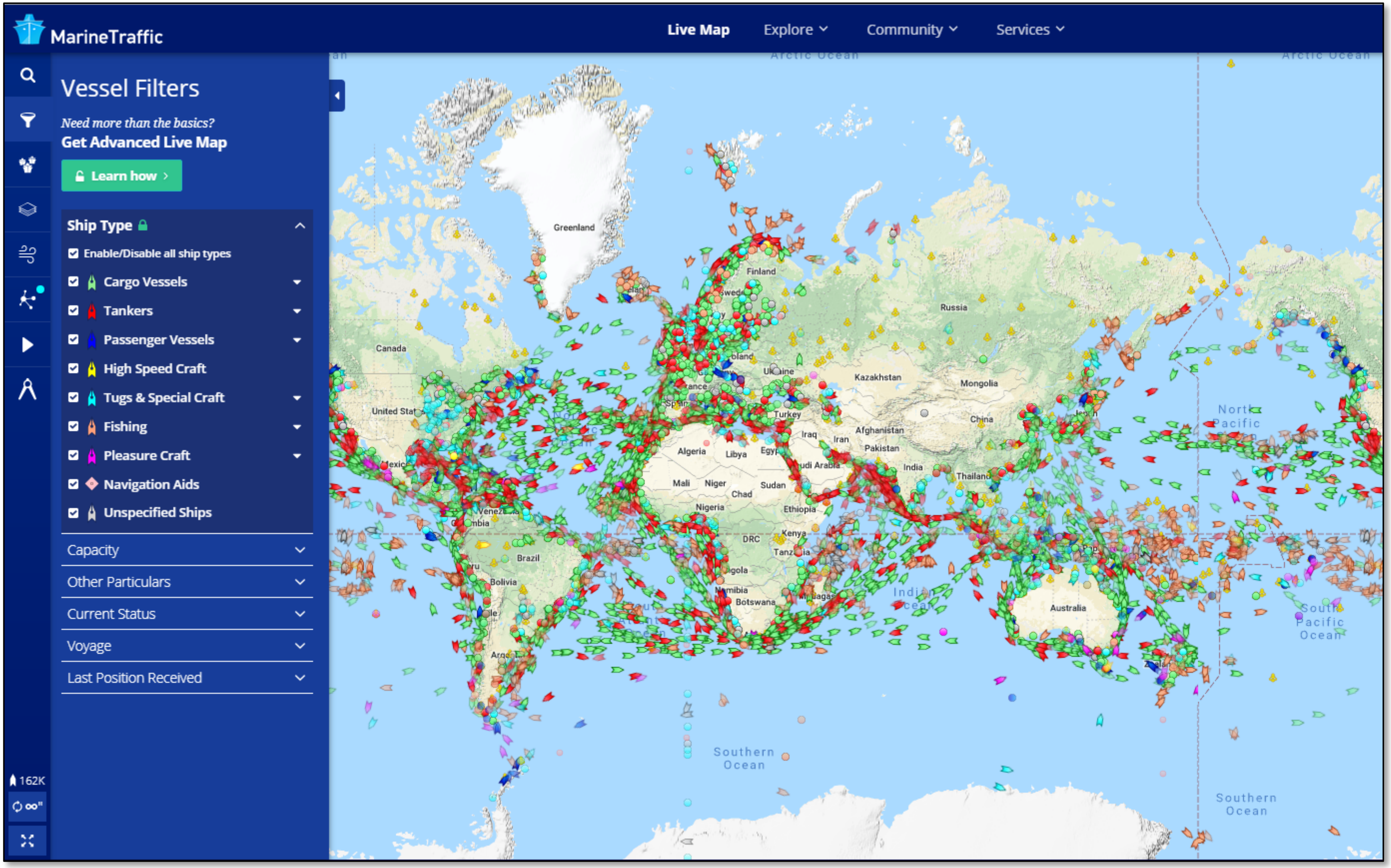
DTU Project CyberShip

- CyberShip problem
- Project Description
- CyberShip Framework
- STPA Process Application
- Next Steps

Project Description

Shipping Operations in the economy

Shipping Operations in the economy



Vessel Filters

Need more than the basics?

Get Advanced Live Map

Learn how ›

Ship Type

☑ Enable/Disable all ship types
☑ Cargo Vessels
☑ Tankers
☑ Passenger Vessels
☑ High Speed Craft
☑ Tugs & Special Craft
☑ Fishing
☑ Pleasure Craft
☑ Navigation Aids
☑ Unspecified Ships

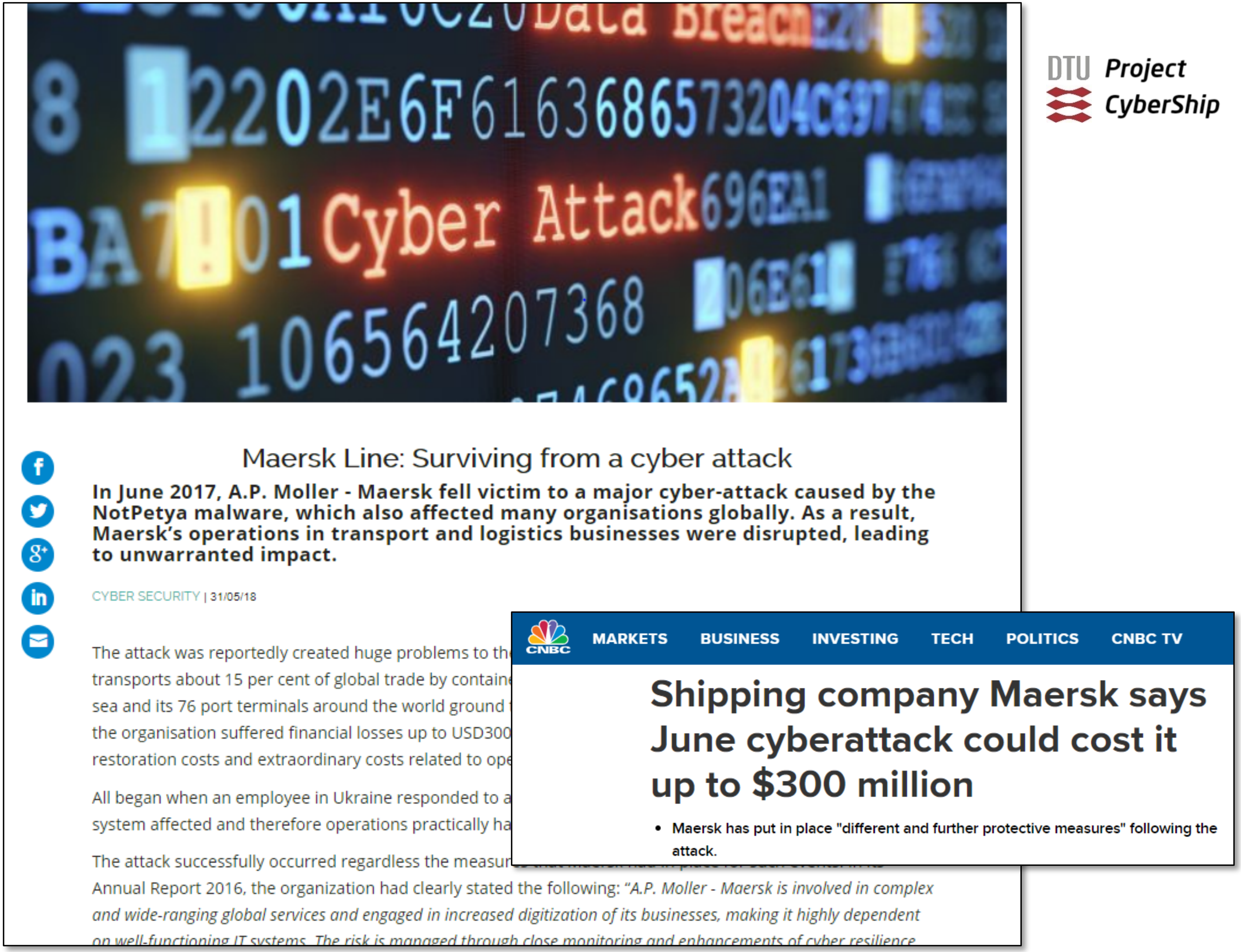
Capacity

Other Particulars

Current Status

Voyage

Last Position Received



Maersk Line: Surviving from a cyber attack

In June 2017, A.P. Moller - Maersk fell victim to a major cyber-attack caused by the NotPetya malware, which also affected many organisations globally. As a result, Maersk's operations in transport and logistics businesses were disrupted, leading to unwarranted impact.

CYBER SECURITY | 31/05/18

The attack was reportedly created huge problems to th
transports about 15 per cent of global trade by containe
sea and its 76 port terminals around the world ground
the organisation suffered financial losses up to USD300
restoration costs and extraordinary costs related to ope

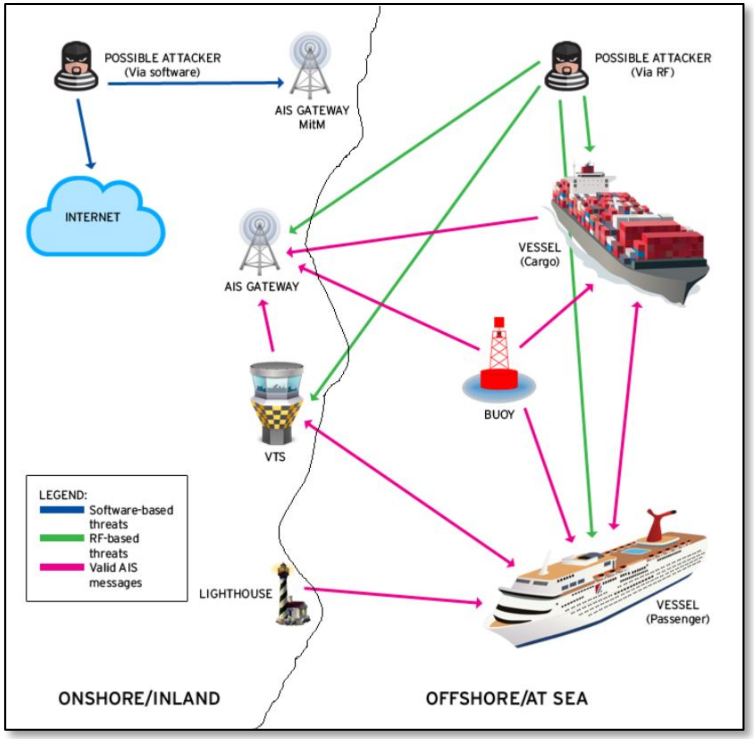
All began when an employee in Ukraine responded to a
system affected and therefore operations practically ha

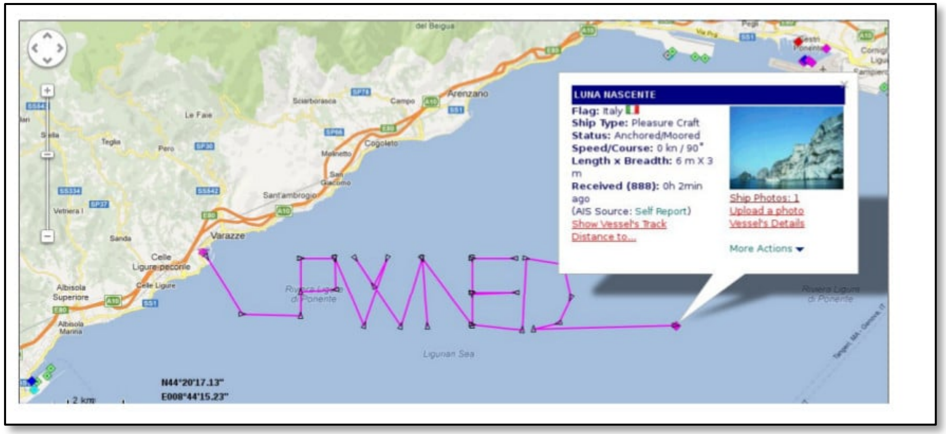
The attack successfully occurred regardless the measur
Annual Report 2016, the organization had clearly stated the following: *"A.P. Moller - Maersk is involved in complex and wide-ranging global services and engaged in increased digitization of its businesses, making it highly dependent on well-functioning IT systems. The risk is managed through close monitoring and enhancements of cyber resilience*

Shipping company Maersk says June cyberattack could cost it up to $300 million

- Maersk has put in place "different and further protective measures" following the attack.

Cyber Attacks




LUNA NASCENTE
Flag: Italy
Ship Type: Pleasure Craft
Status: Anchored/Moored
Speed/Course: 0 kn / 90°
Length x Breadth: 6 m X 3 m
Received (888): 0h 2min ago
(AIS Source: Self Report)
Show Vessel's Track
Distance to...
Ship Photos: 1
Upload a photo
Vessel's Details
More Actions

Project purpose

”Propose a **framework** for improving the **resilience** in the shipping industry to **cyber risks**, with the ship being its main focus”

BIMCO MAERSK NORDEN UltraShip DanishShipping Danish Maritime OMT

DTU Management Engineering
Department of Management Engineering

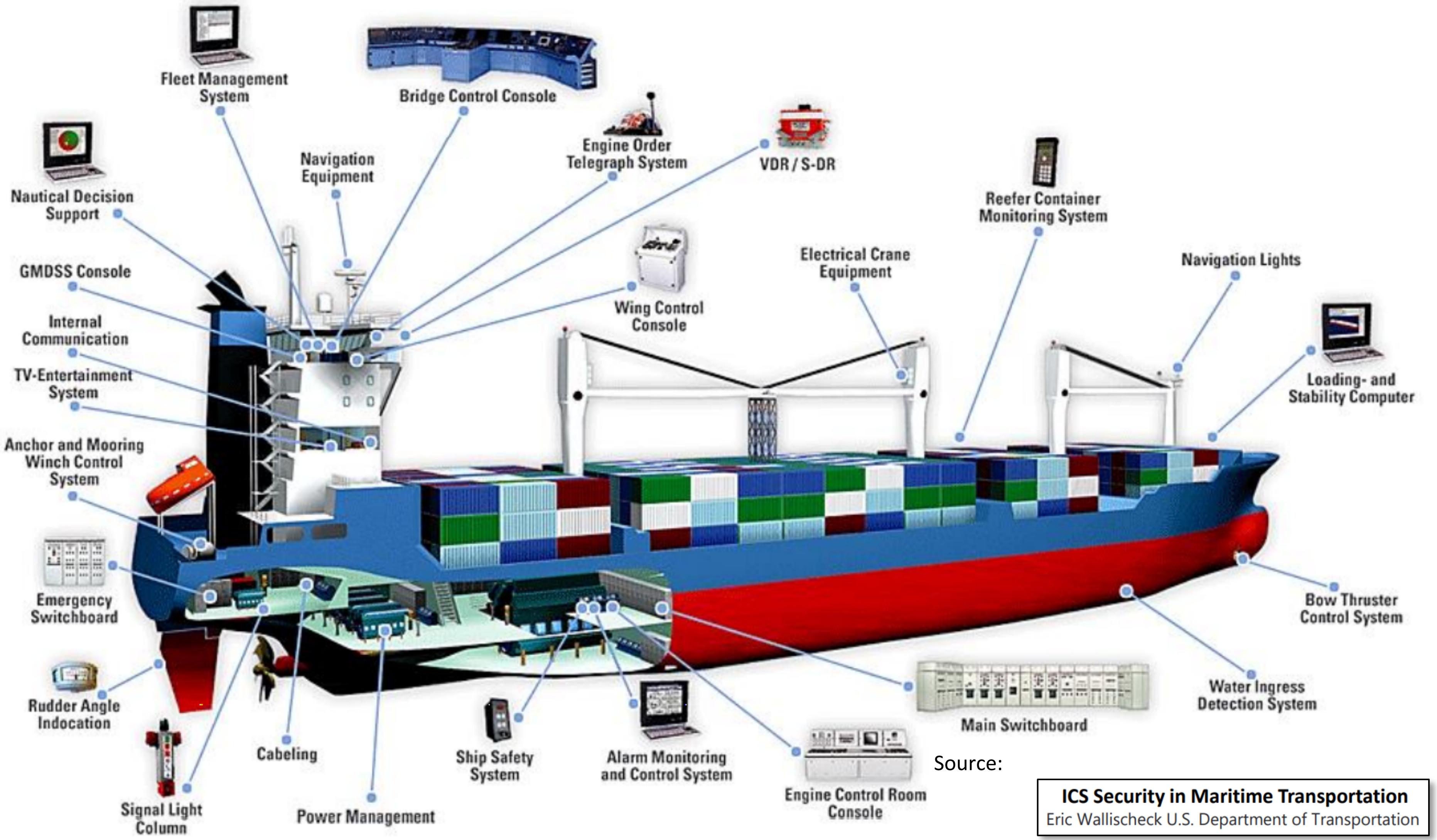
DTU Compute
Department of Applied Mathematics and Computer Science

Basic Definitions

CyberShip Model

Ship Systems

DTU Project CyberShip



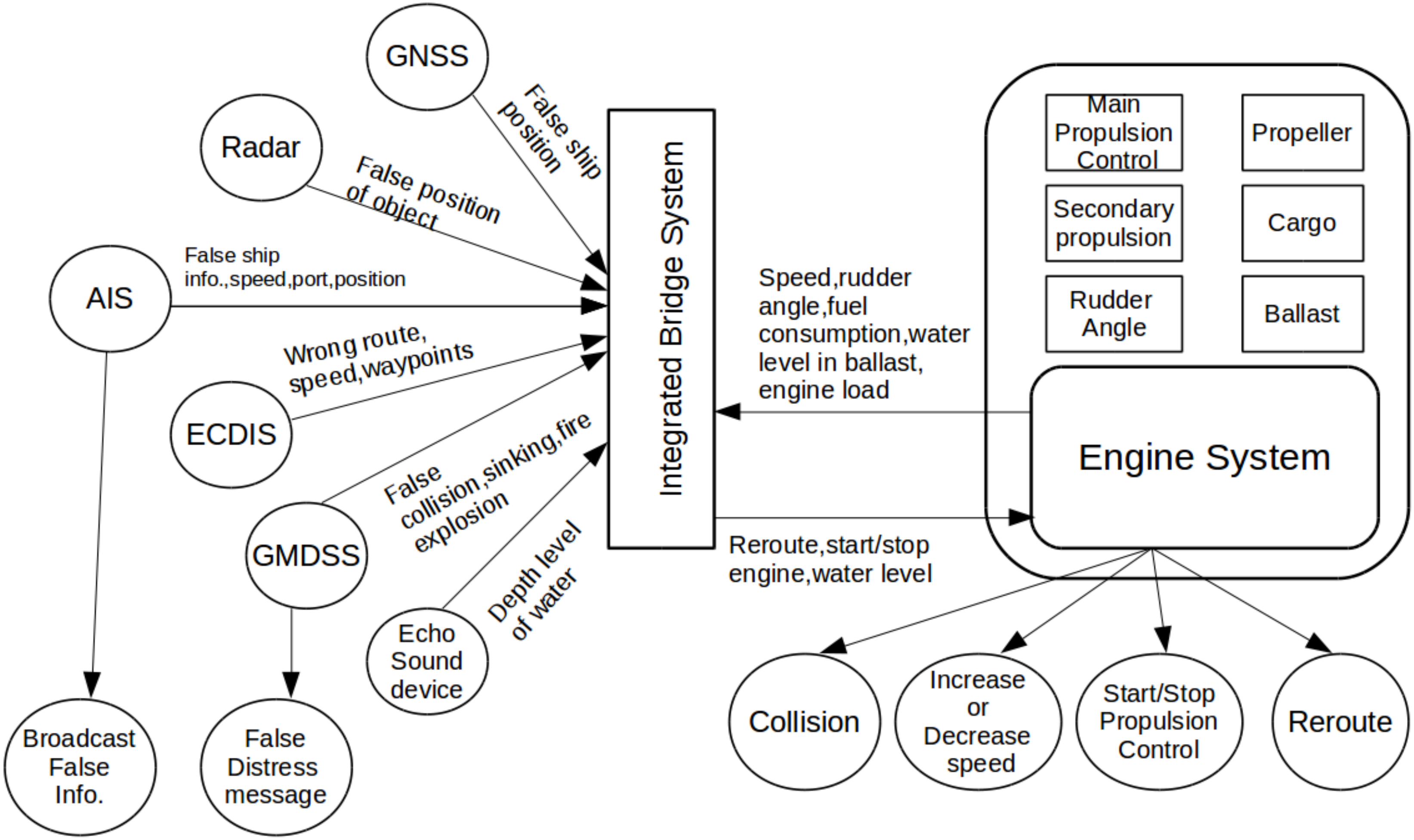
Fleet Management System
Bridge Control Console
Navigation Equipment
Engine Order Telegraph System
VDR / S-DR
Nautical Decision Support
Reefer Container Monitoring System
GMDSS Console
Electrical Crane Equipment
Navigation Lights
Wing Control Console
Internal Communication
TV-Entertainment System
Loading- and Stability Computer
Anchor and Mooring Winch Control System
Emergency Switchboard
Bow Thruster Control System
Water Ingress Detection System
Main Switchboard
Rudder Angle Indocation
Cabeling
Ship Safety System
Alarm Monitoring and Control System
Engine Control Room Console
Signal Light Column
Power Management

Source:

ICS Security in Maritime Transportation
Eric Wallischeck U.S. Department of Transportation

Impact of Attack Traffic

DTU Project CyberShip



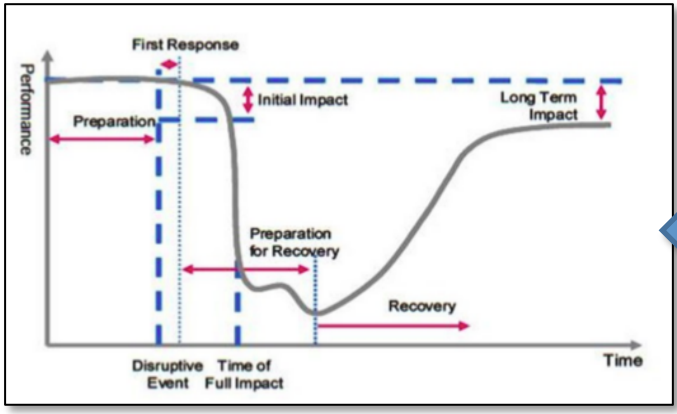
Sahay, R., & Sepúlveda Estay, D. A. (2018). **Work Package 2 Report - Cyber resilience for the shipping industry**.

DTU Project CyberShip

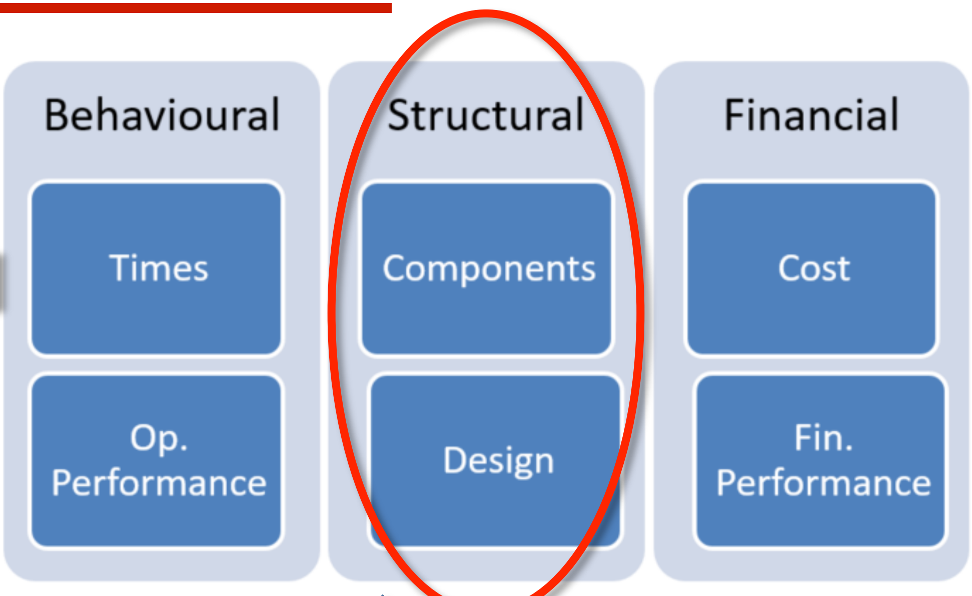
Basic Definitions

Key performance Indicators

Key Performance Indicators



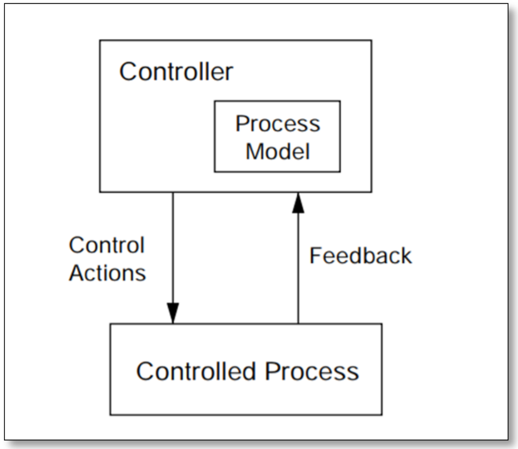
(1)



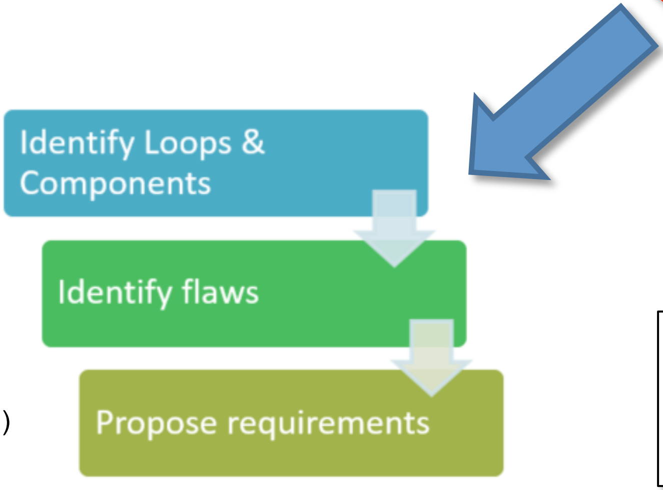
Behavioural
- Times
- Op. Performance

Structural
- Components
- Design

Financial
- Cost
- Fin. Performance



(2)



Identify Loops & Components

Identify flaws

Propose requirements

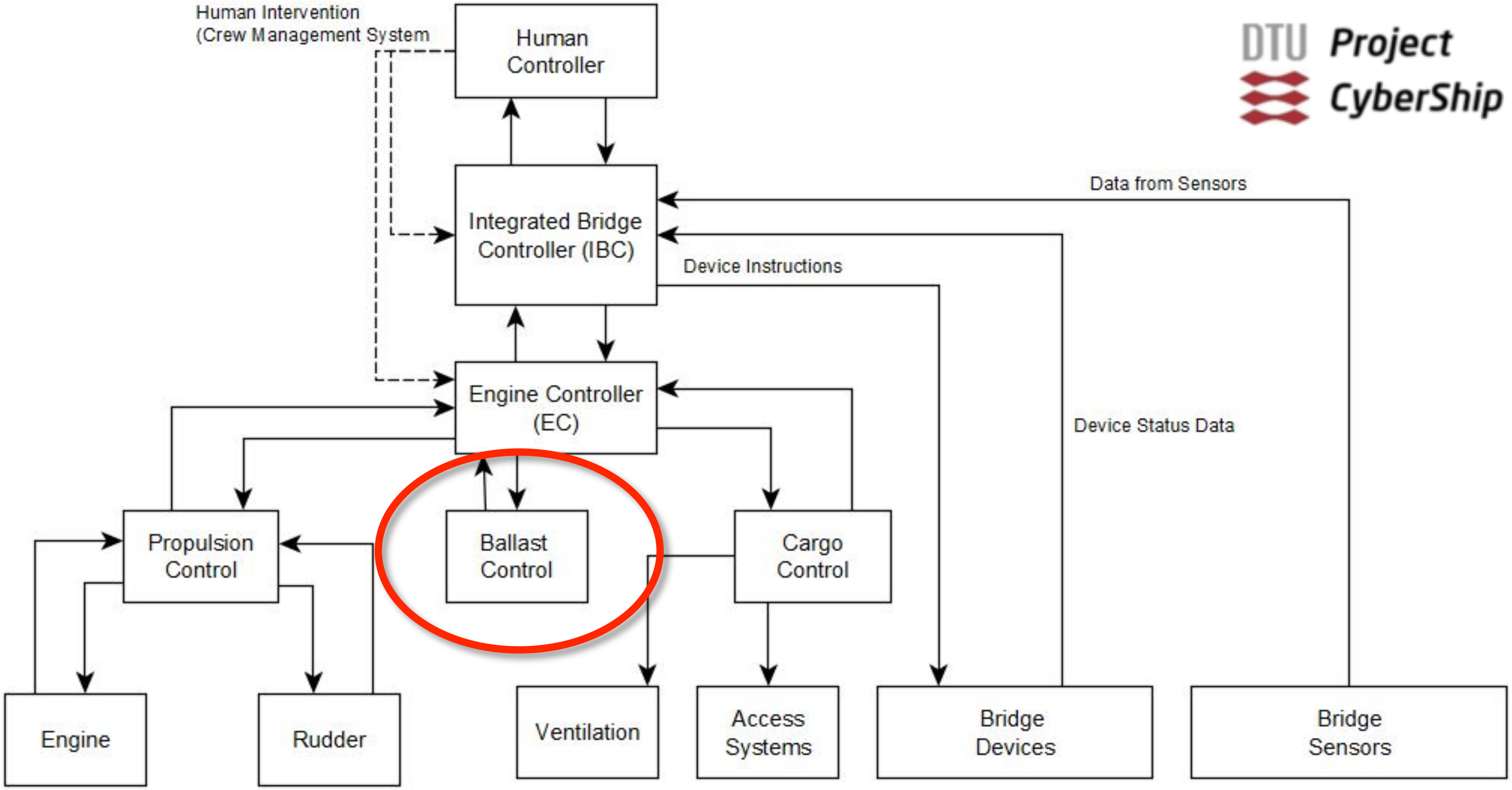
(1) Sheffi, Y., & Rice Jr, J. B. (2005). **A supply chain view of the resilient enterprise**. MIT Sloan management review, 47(1), 41-49.

(2) Leveson, N. (2011). **Engineering a safer world: Systems thinking applied to safety**. MIT press.

DTU Project CyberShip

STPA application

Analysis of a Shipping system



Human Intervention
(Crew Management System

Human Controller

Integrated Bridge Controller (IBC)

Data from Sensors

Device Instructions

Engine Controller (EC)

Device Status Data

Propulsion Control

Ballast Control

Cargo Control

Engine

Rudder

Ventilation

Access Systems

Bridge Devices

Bridge Sensors

Automatic Identification System (AIS)

Electronic Chart Display and Information System (ECDIS)

Global Maritime Distress System (GMDSS)

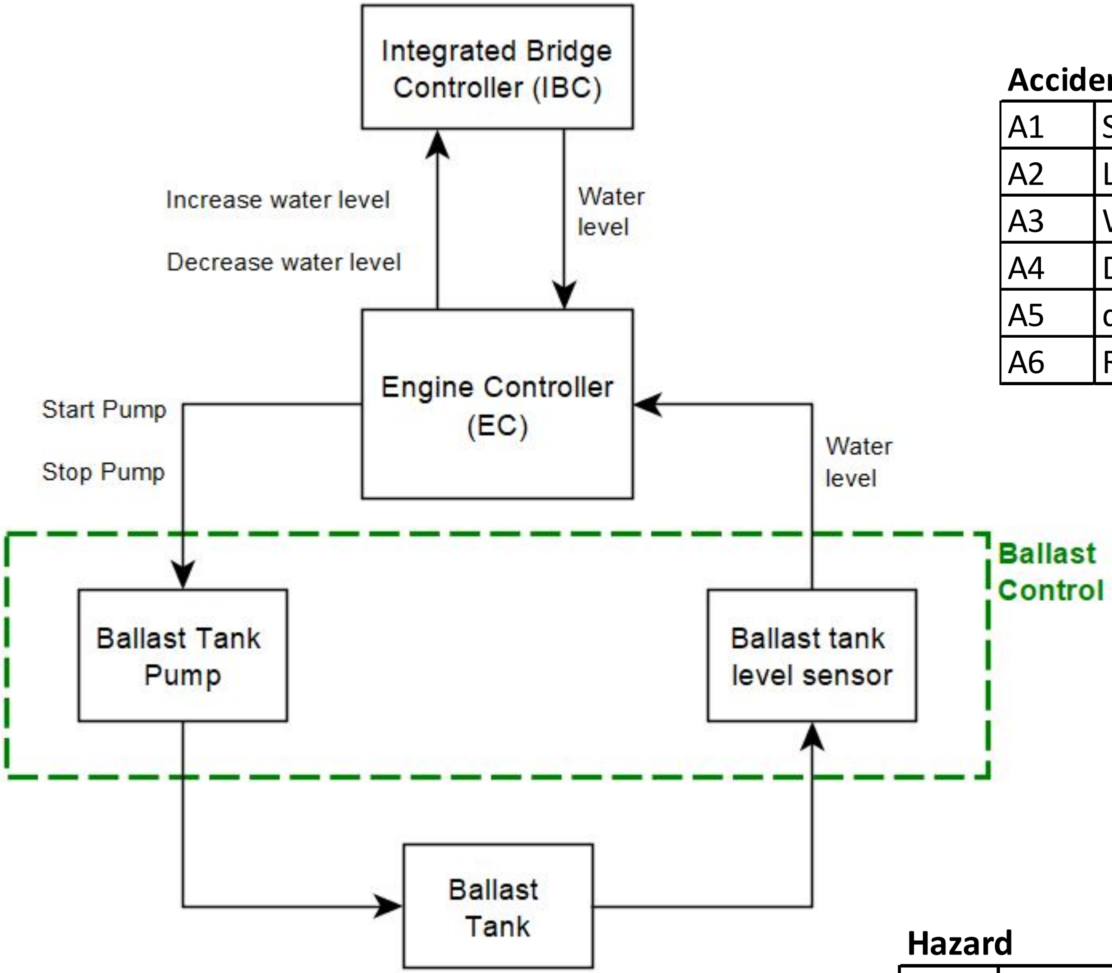
Radar

Echo Sounding Device

Global NAvigation Satellite System (GNSS)

Global Positioning System (GPS)

DTU Project CyberShip



Integrated Bridge Controller (IBC)

Increase water level

Decrease water level

Water level

Engine Controller (EC)

Start Pump

Stop Pump

Water level

Ballast Control

Ballast Tank Pump

Ballast tank level sensor

Ballast Tank

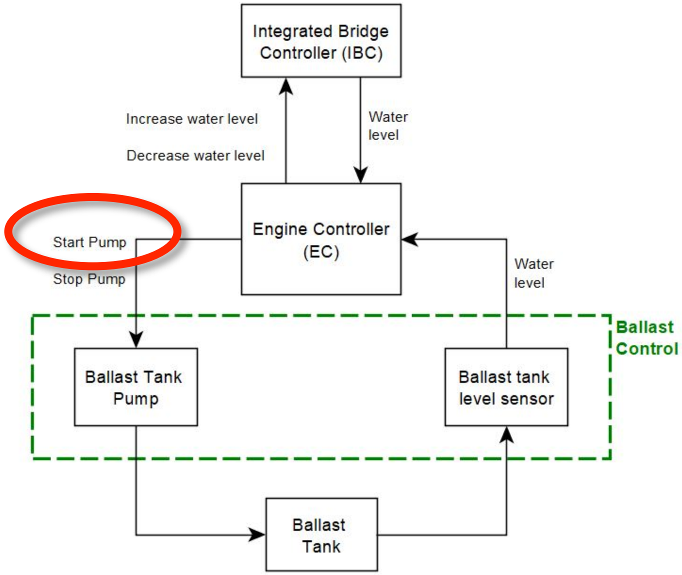
Accidents

A1	Shipment late or non arriving
A2	Loss/Harm to life of passengers /crew
A3	Wrong or non delivery to customers
A4	Damage to the Ship
A5	damage to the cargo
A6	Reputational loss

Hazard

H1	Uncontrolled manouvering of the ship
H2	Unidentified cargo items /wrong cargo data
H3	Incorrect functioning of ship components
H4	Uncontrolled transmission of data
H5	Uncontrolled data being transmitted

Analysis Example



			UCA			
Source	Destination	Control Action	Performed with Hazard	Not Performed with Hazard	Performed too long too short with hazard	Performed too early too late with hazard
EC	Ballast tank Pump	Start Pump	when EC has provided wrong parameter (Velocity, Level) to Pump.	when EC is compromised because of human in the loop	when the requirement was for a shorter period and the pump acted for too long	when there are communication channel congestion
			when EC receives the wrong parameters (Velocity, Level) from IBC	when EC has been compromised because of component failure	when the requirement was for a longer period and the pump acted for too short	when there is a feedback delay between Actuator to Ballast tank
			when Ballast tank Pump is not functioning	when EC has been compromised because of external hacker		when a programmed EC action was performed too early or too late.
			When there is network failure and the control action is not received by Ballast tank	when EC did not receive command from IBC		
			when EC is compromised because of human in the loop			
			when EC has been compromised because of component failure			
			when EC has been compromised because of external hacker			
			when it was not required			

Analysis Results

Scenarios identified in UCA Analysis

a.- Component Failure / Cascading effects

b.- Mis-interaction

- ➢ Network Failure
- ➢ Network Congestion (resulting delay)

c.- Controllers Compromised by hackers

d.- Human Mistakes (Intentional or unintentional)

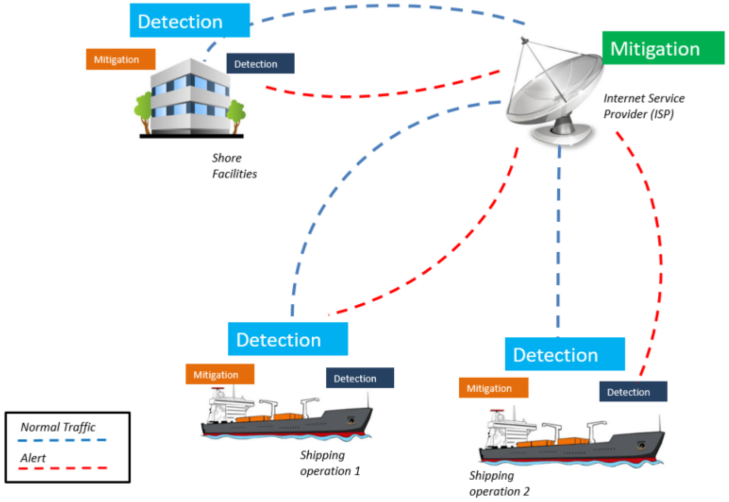
e.- Incomplete or no feedback provided for decision making

Method Advantages

STPA Method Advantages

- Explicit representation of the shipping IT system
    - Mapping of functions
    - Review of design considerations
- Identification of design requirements
    - Infrastructure requirements
    - Design of communications
- Identification of crucial systems
    - Highest #UCA detected per Hazard
    - Highest #UCA detected per Accident
- Design of a resilience plan
    - Redundancy systems
    - Flexible response design

Research Next Steps

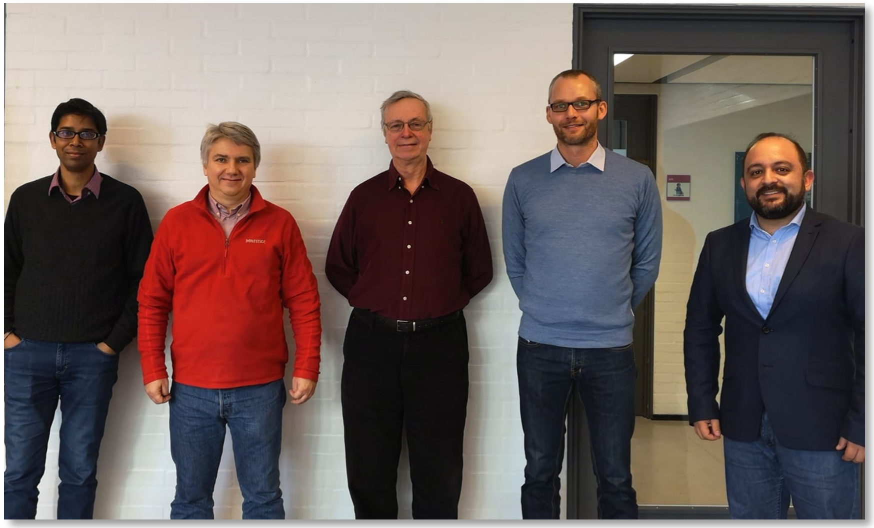


- Comparison of STPA results with
  - Attack fault tree analysis
  - Asset–based risk
- Extending analysis to the whole ship
- Identification of design requirements (CyberShip Project)
- Analysis of an extended shipping system (shore center and several ships)
- Training requirements for cyber-attack response

DTU Project CyberShip

Thanks for your attention

Rishikesh Sahay, PhD, risa@dtu.dk
Daniel Sepulveda, PhD, dasep@dtu.dk



CyberShip Core team
From Left to right:

- Rishikesh Sahay, PhD
- Prof. Christian D. Jensen
- Prof. Harilaos Psaraftis
- Prof. Michael B. Barfod
- Daniel Sepulveda, PhD.

Research Site
http://orbit.dtu.dk/en/projects/cyber-resilience-for-the-shipping-industry-cybership(666b8477-992f-4bd7-82d3-e89fddb4c87d).html