This presentation shows transformations of slides from the traditional to the assertion-evidence design

Before

Aalto University
Marine and Arctic Technology
Marine Risk and Safety Group

Autonomous ship safety and future of seafaring

Author: Meriam Chaal
Co-Authors: Osiris Valdez Banda, Sunil Basnet, Spyros Hirdaris and Pentti Kujala

Aalto University
School of Engineering

After

An initial risk assessment of autonomous ships

Meriam Chaal
Prof. Osiris V Banda

Aalto University, Marine Risk and Safety Group

01 April 2020

Aalto University
School of Engineering

Aalto-yliopisto
Aalto-universitetet
Aalto University

Content

- Introduction
- Methods for autonomous ship safety
- Results of the initial steps of STPA applied to the concept of autonomous ship
- Recommendations related to capacity building for autonomous ships
- Conclusion

This talk focuses on the risk assessment and what its results recommend for the operators of autonomous ships

Risk assessment methods

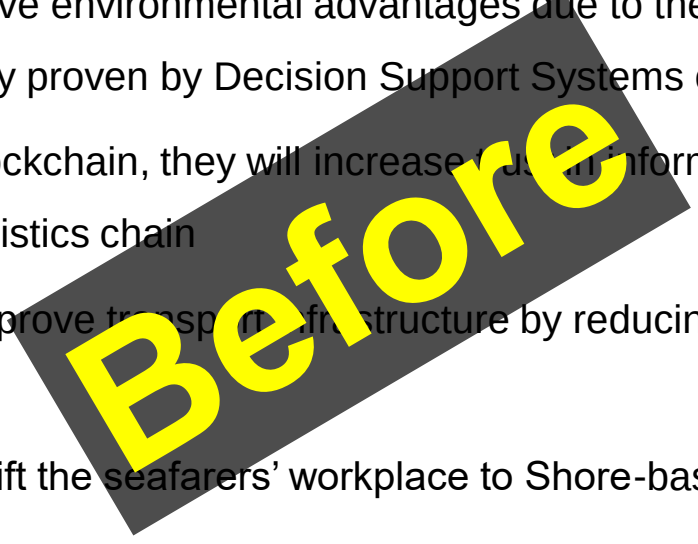
Applied to autonomous ships

Recommendations for capacity building

Introduction

Why Autonomous Ships?

- They will have environmental advantages due to the fuel savings, which were already proven by Decision Support Systems onboard current ships.
- With the Blockchain, they will increase trust in information sharing and optimize logistics chain
- They will improve transport infrastructure by reducing the density of land traffic
- They will shift the seafarers' workplace to Shore-based Control Centres
- **They will enhance safety both at ports and at sea**



Why autonomous ships?

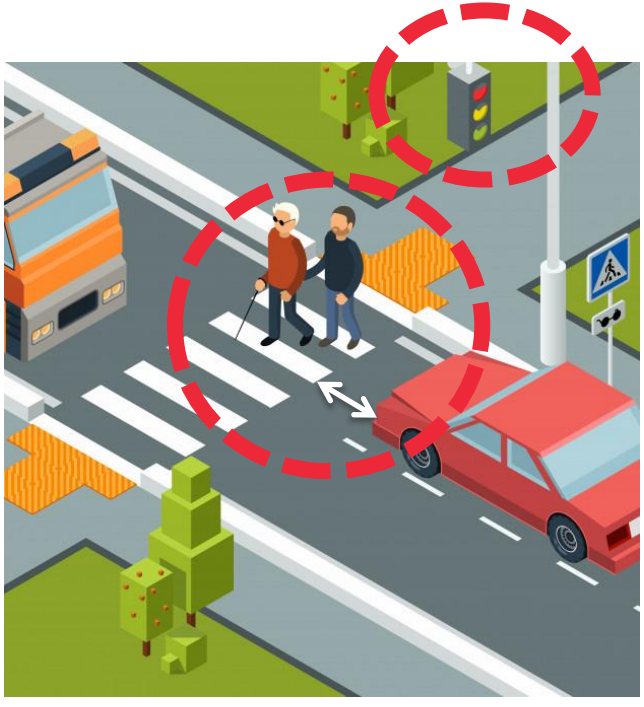
https://www.morethanshipping.com/blockchain-technology-friend-foe/

http://www.imo.org/en/MediaCentre/PressBriefings/Pages/08-MSC-99-MASS-scoping.aspx

https://www.shutterstock.com/search/trucks+business?orientation=horizontal&image_type=photo&safe=true&search_source=base_related_searches

Why do we need risk assessment?

Safety
=
Freedom of Risk



https://www.freepik.com/premium-vector/care-person-crossing-street-urban-city-crosswalk-disabilities-man-with-helper-isometric_6214620.htm

Risk assessment is the possibility of undesired events and the associated uncertainties

Can cause losses

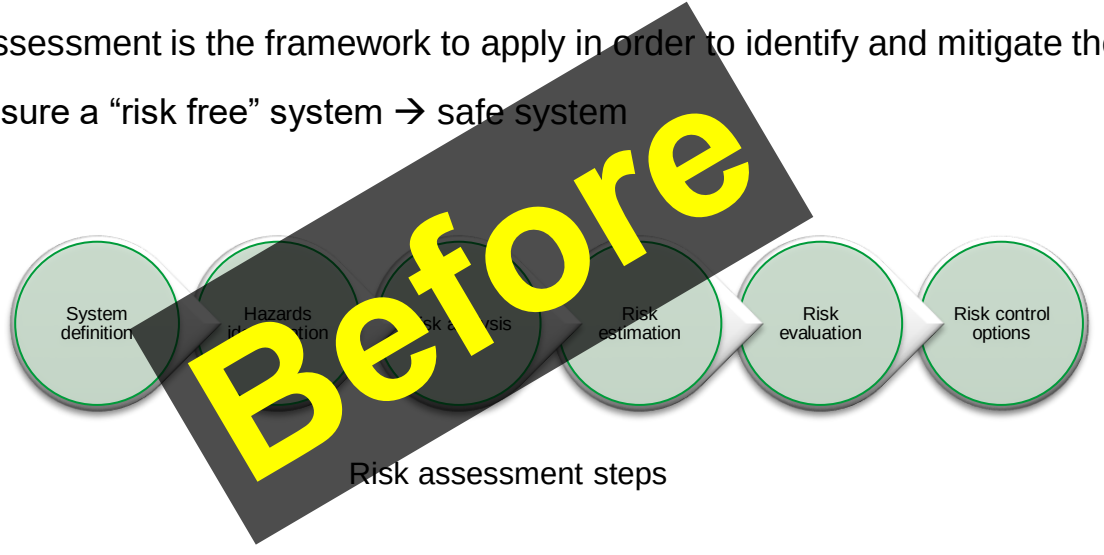
http://marasinews.com/ar/node/6595

Uncertainties about the event
Possibility and Consequences

https://ocean.si.edu/conservation/pollution/animals-and-oil-spill-what-can-you-do

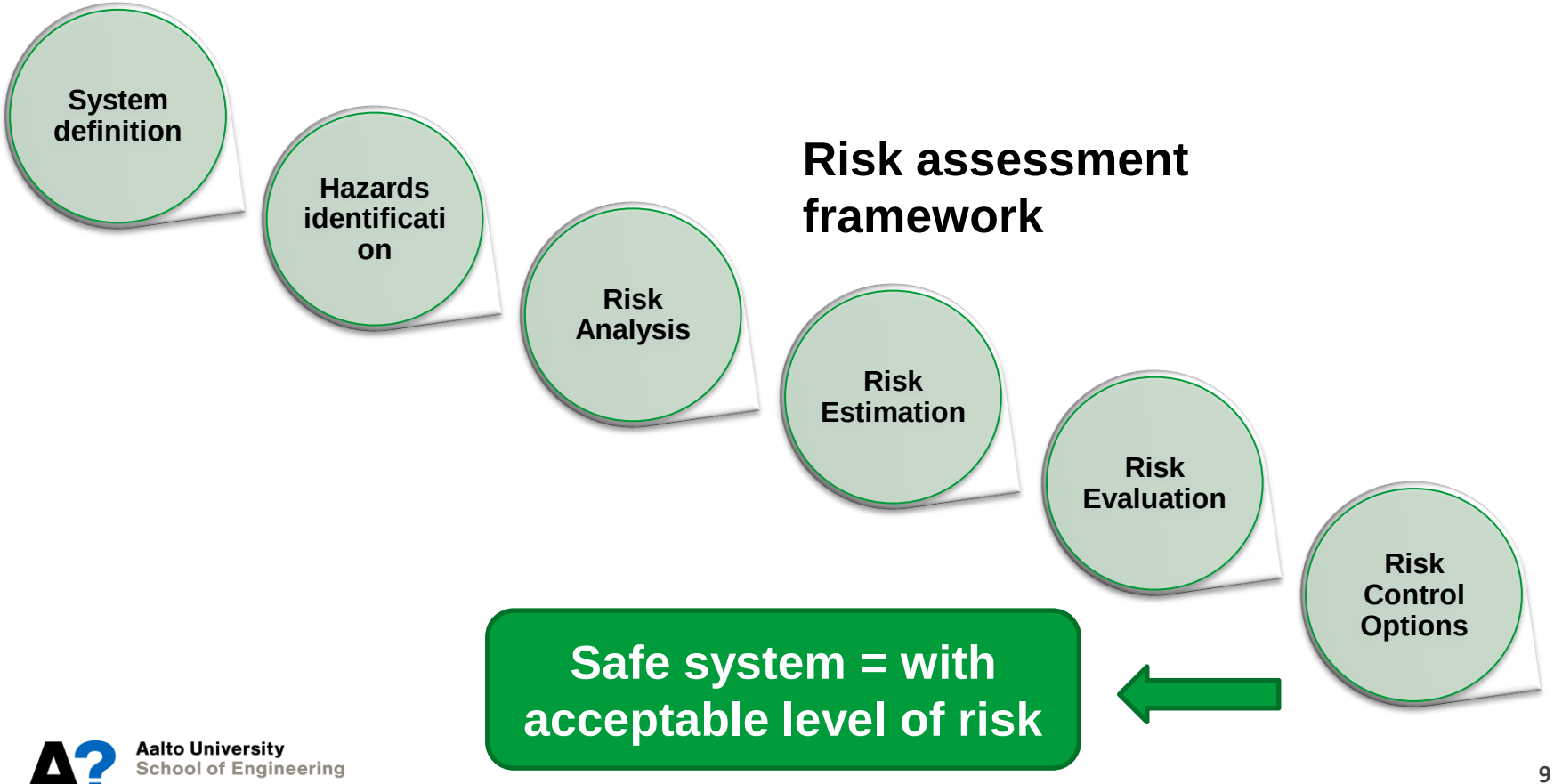
Safety and Risk

- Safety is the freedom of risks
- Risk is the possibility of an undesired event and the associated uncertainties
- Risk assessment is the framework to apply in order to identify and mitigate the risks and ensure a “risk free” system → safe system



Risk assessment steps

A risk assessment framework is necessary to develop safe systems



Risk assessment methods

- **Traditional methods: FTA, ETA, FMEA, HAZOP**

-They have been applied since ages , when systems were mostly electro-mechanical

-They focus on the failures of the system components and their frequencies (probabilities).

-The safety of the system is highly related to its reliability (low frequencies of failures) R=P*C

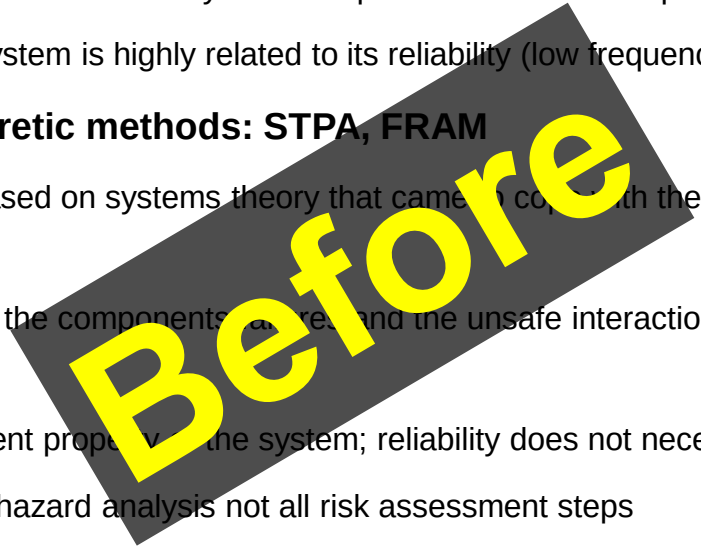
- **System-theoretic methods: STPA, FRAM**

-Recent methods based on systems theory that came in co[illegible]th the complexity of modern systems

-They focus on both the components [illegible]re[illegible] and the unsafe interactions between the system components

-Safety is an emergent prope[illegible]y [illegible] the system; reliability does not necessarily result on safety

-They are limited to hazard analysis not all risk assessment steps



Traditional risk assessment methods have limitations

-Since 1930's

-Focus on system reliability f/t

https://www.dreamstime.com/stock-illustration-gear-system-simple-mechanical-wheels-isolated-white-background-image53996472

Risk = P*C

→Reliability implies safety

Probability	Consequence: Very Low 1	Low 10	Medium 100	High 500	Very High 1,000
Probable 1	1	10	100	500	1,000
Credible 0.1	0.1	1	10	50	100
Remote 0.01	0.01	0.1	1	5	10
Improbable 0.001	0.001	0.01	0.1	0.5	1
Unlikely 0.0001	0.0001	0.001	0.01	0.05	0.1

https://www.ge.com/digital/documentation/meridium/Help/V43050/Default/Subsystems/Operations/Content/AboutBaselineRiskMatrixRecords.htm

Examples: FTA, ETA, FMEA, HAZOP

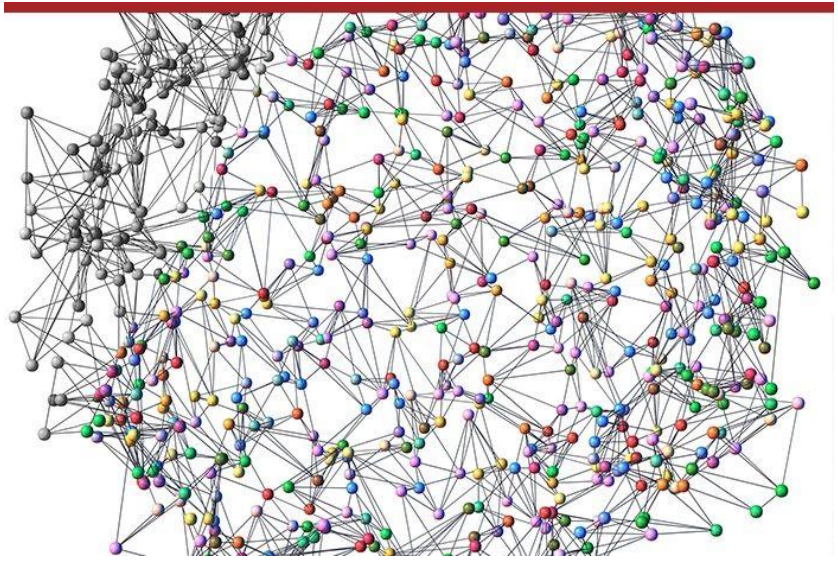
Methods for Autonomous ship safety

- The autonomous ship is a complex software-intensive system with many interacting sub-systems→ **System-theoretic methods are suitable**
- **STPA** is better than FRAM for the software-intensive systems such as autonomous ships
- STPA is an iterative process suitable for **new design**
- STPA started from the space engineering systems and is currently applied to the modern systems of different transportation industries
- The maritime industry is slow in applying STPA. For autonomous ships few applications to isolated systems (such as Dynamic Positioning system)

Before

System-theoretic methods are suitable for modern systems

- Recently based on systems theory for complexity
- Proactive
- Focus > on component interactions
- Safety > reliability
- Safety > an emergent property



https://bigzinbigapple.com/f/can-complex-systems-collapse

Examples: STPA, FRAM

Recommendations related to capacity building for autonomous ships

The traditional safety measures of the maritime industry are inadequate for autonomous ships

- Formal Safety Assessment (FSA) for new design
- FSA adopted in 2002

https://www.imo.org

STPA is the most suitable method for Autonomous ships

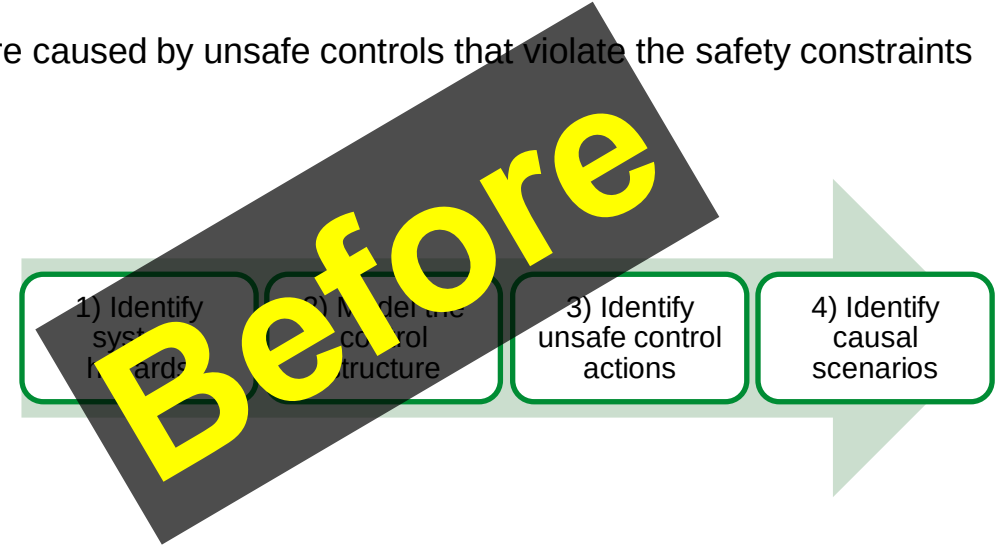
- New design
- Complex
- Software-intensive
- Transportation system

http://emergence.libs.uga.edu/?q=node/11

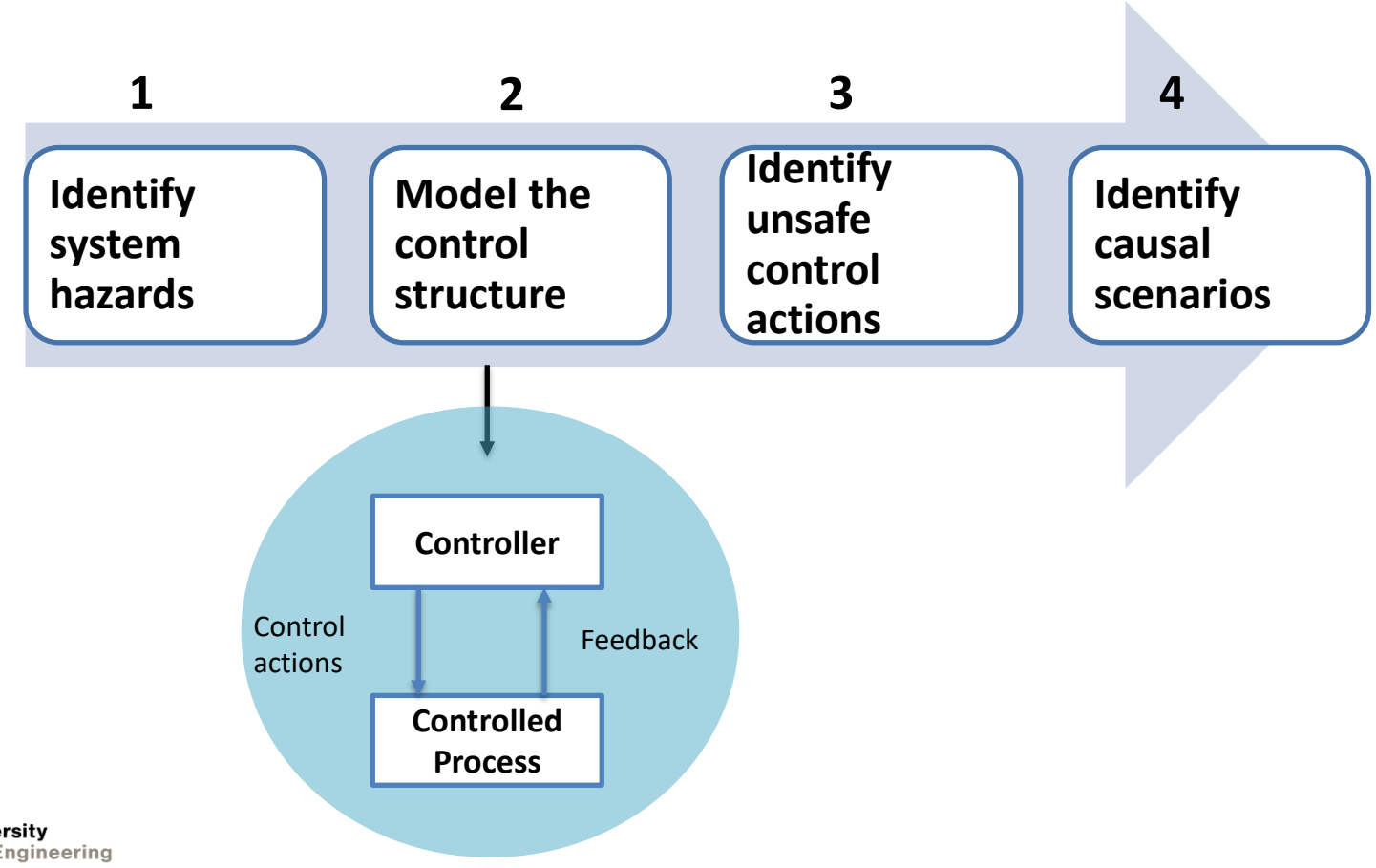
STPA process

- A system should be modelled as hierarchical control loops, where every controller enforces the safety constraints on the controlled process behavior
- A system model is a functional model that does not focus on the technical design
- Accidents are caused by unsafe controls that violate the safety constraints

STPA hazard analysis steps (Leveson, 2011)

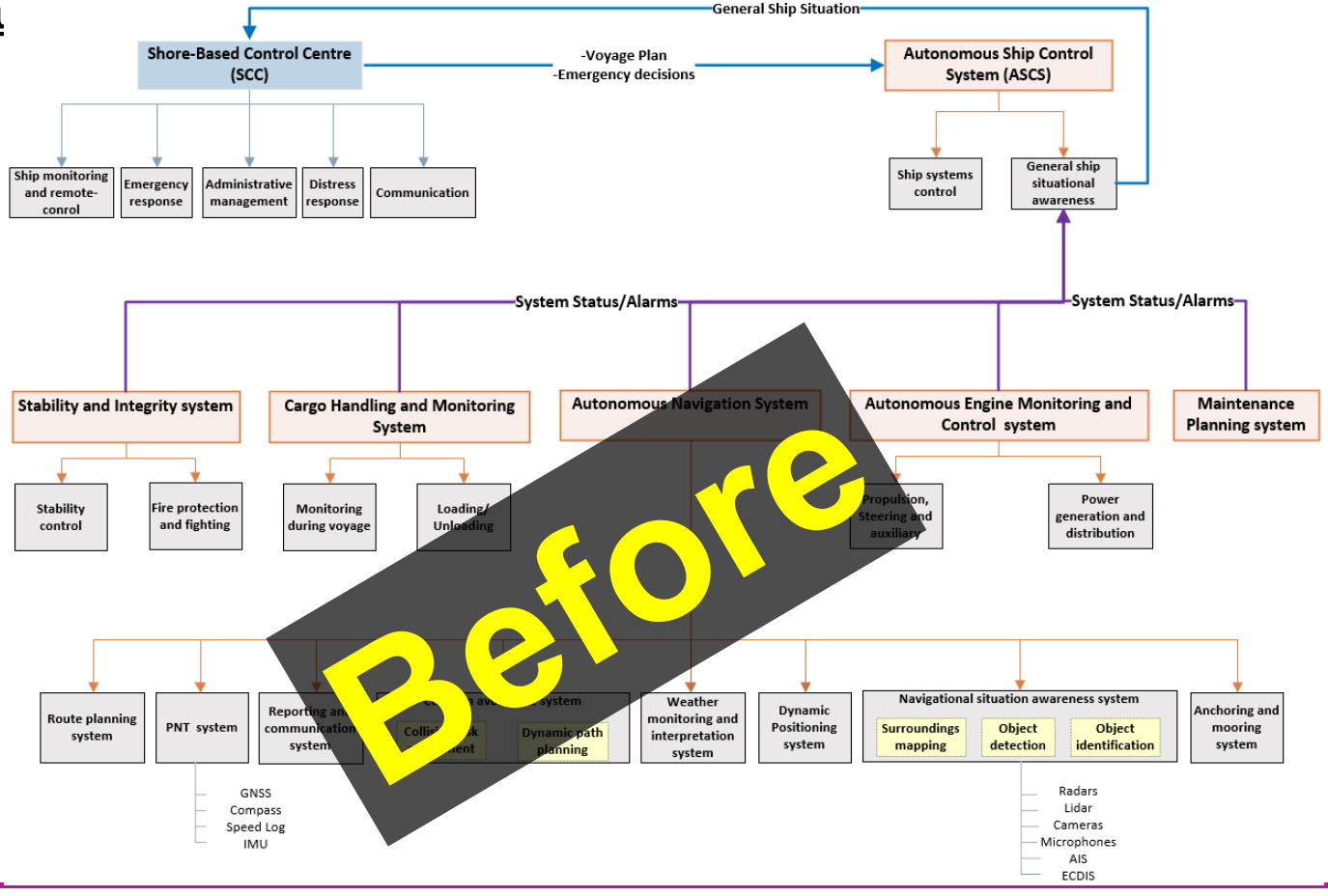


STPA consists of applying four main steps

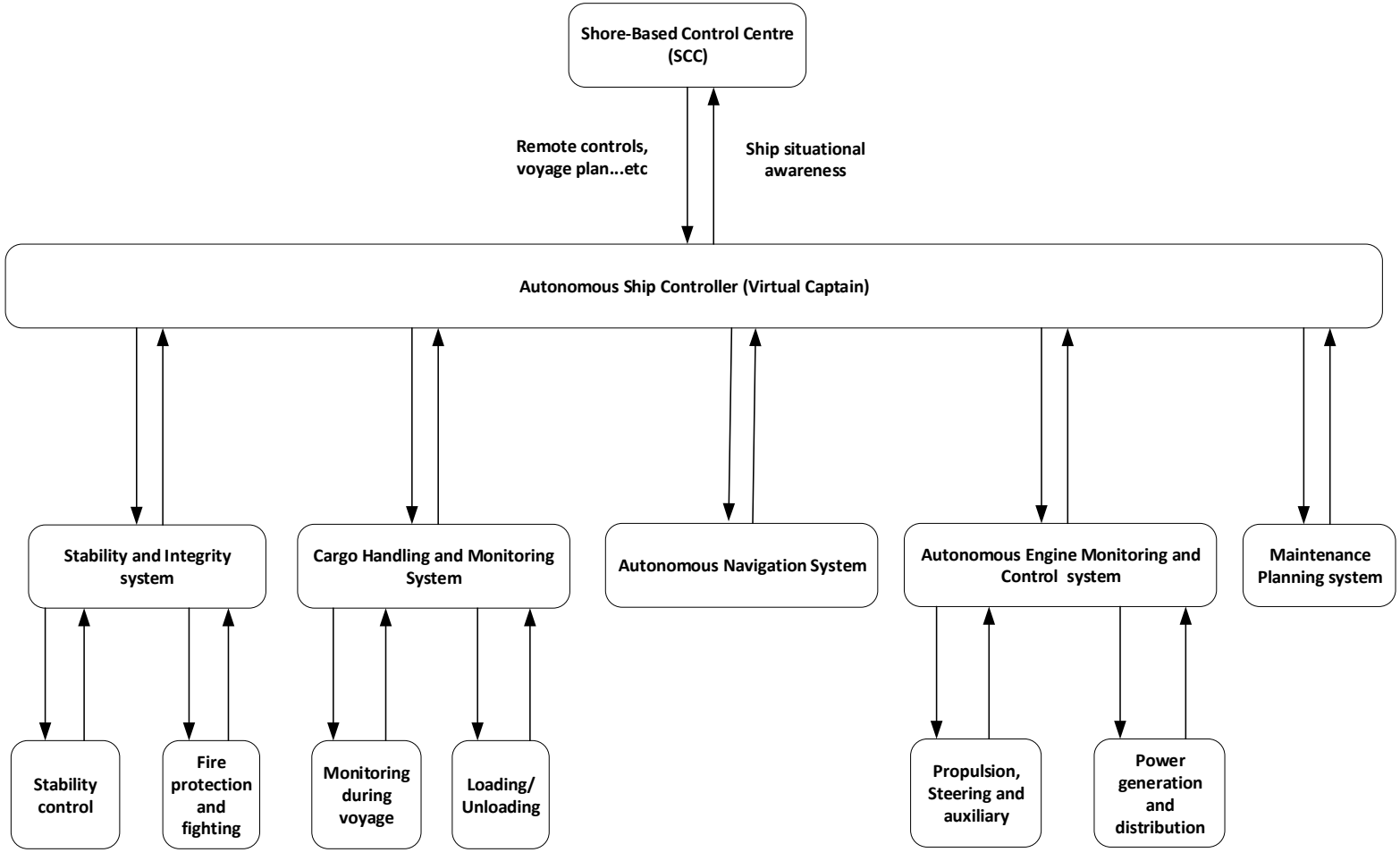


Safety control

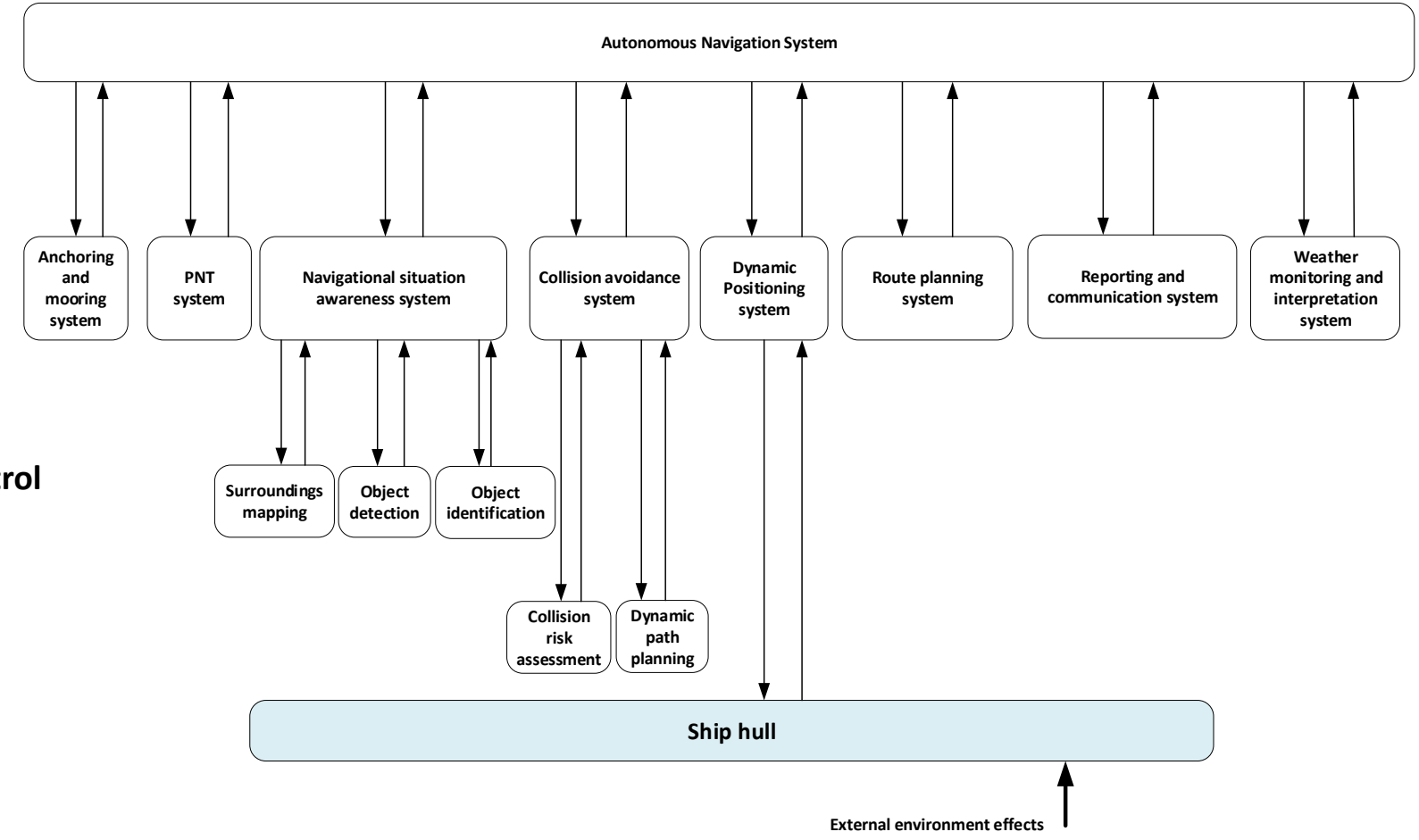
stru



Safety control structure (Level1)



Safety control structure (Level2)

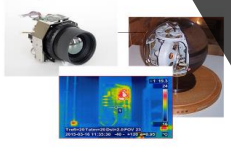


Many data for Situational Awareness

Shore-Based Control Centre

Global Navigation Satellite System (GNSS) for Positionnig Navigation and Timing, INMARSAT for satellite communication and distress messages

Before

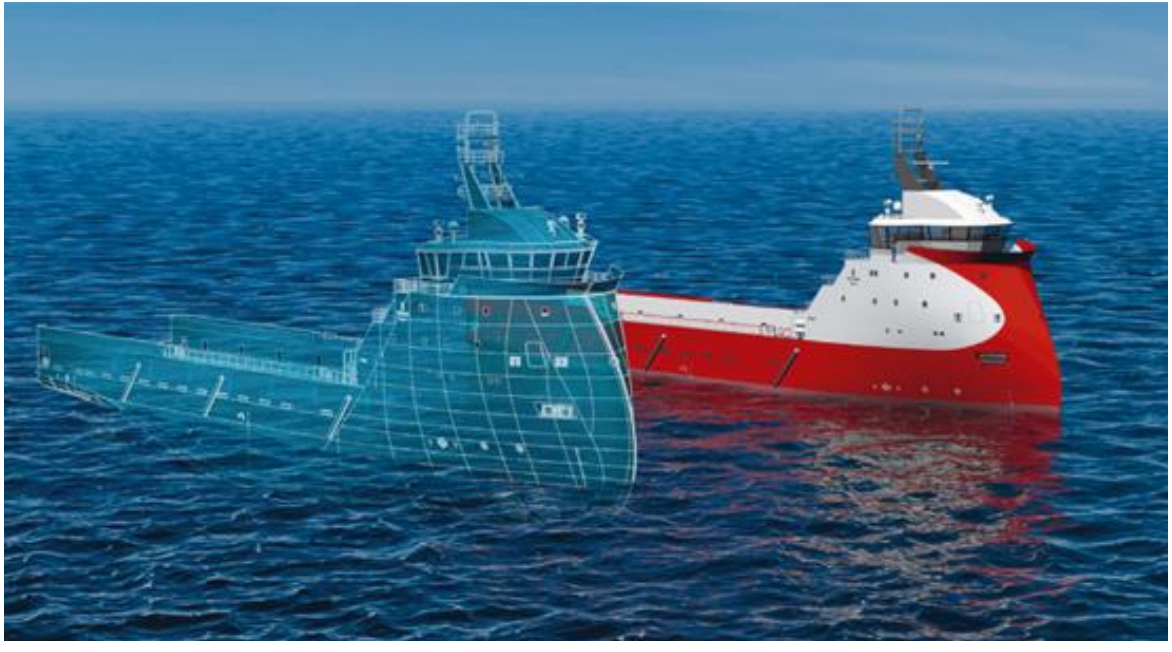


Navig n Systems (IN sual Aiding tem (Infrared Camera, Thermal Camera, Optical Camera), Sound Aiding System, LIght Detection And Ranging (LIDAR), Radar, AIS data...

Radio communication, 5G mobile communication

The operators must analyze the ship data to assess the inner capabilities for decision-making

Digital twin for the ship data



https://www.dnvgl.com/expert-story/maritime-impact/Digital-twins-and-sensor-monitoring.html

Ship operators must analyze huge external data for situational awareness

Radio communication and INMARSAT

GNSS and AIS

https://marpoint.gr/rolls-royce-spearheads-study-autonomous-ships/

Electronic Charts and weather station

Most of the unsafe control actions are related to data analysis

https://safety4sea.com/rolls-royce-reveals-future-shore-control-centre/

Many ships at a time

Human-machine interface

Short time for response