Risk Based Assessment Tool for MASS (RBAT)

5th International Ship Autonomy and Sustainability Summit

EMSA
European Maritime Safety Agency

Nicolas Charalambous

Department 2: Safety, Security & Surveillance / Unit 2.1

2 September 2024,

Hamburg

RISK METHODOLOGIES

Failure Mode Effects Analysis (FMEA)

HAZOP

Bow Tie

1940 1950 1960 1970 1980 1990 2000

Fault Tree Analysis (FTA)

Software

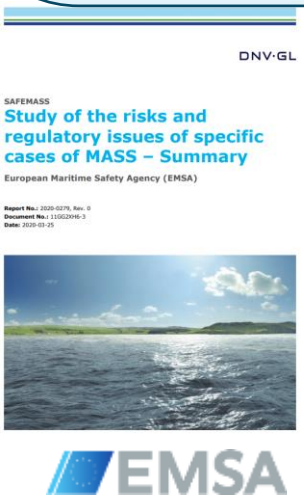
EMSA

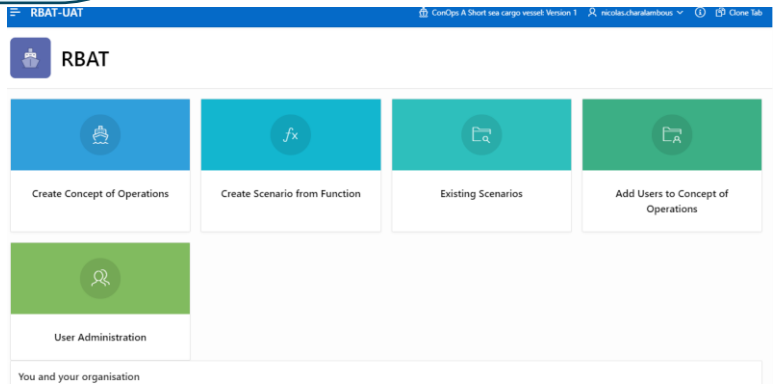
- New automation systems
- Increased interdependency between systems.
- Changes in the Human Machine Interface and the Role of the user.

- Tailored for autonomous and remotely operated vessels.
- Functions being automated or remotely controlled.
- Addresses risks from transferring control.

What is RBAT?

- Function-based and flexible.
- Adaptable to different technology stages.
- Focus on systematic failures and human errors.





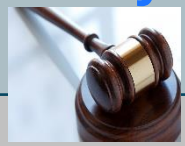
1. Tailored for Automation

2. Flexibility and adaptability

Why RBAT ?

3. Systematic Hazard Analysis

4. Could support regulatory Compliance



Tool Objective

1. Mature the Concept
2. Design Requirement Generation
3. Transparency and Traceability

Human Factors

1. Human Role in Automation
2. Error Mitigation
3. Human Machine Interaction

EMSA

Overcome historical data

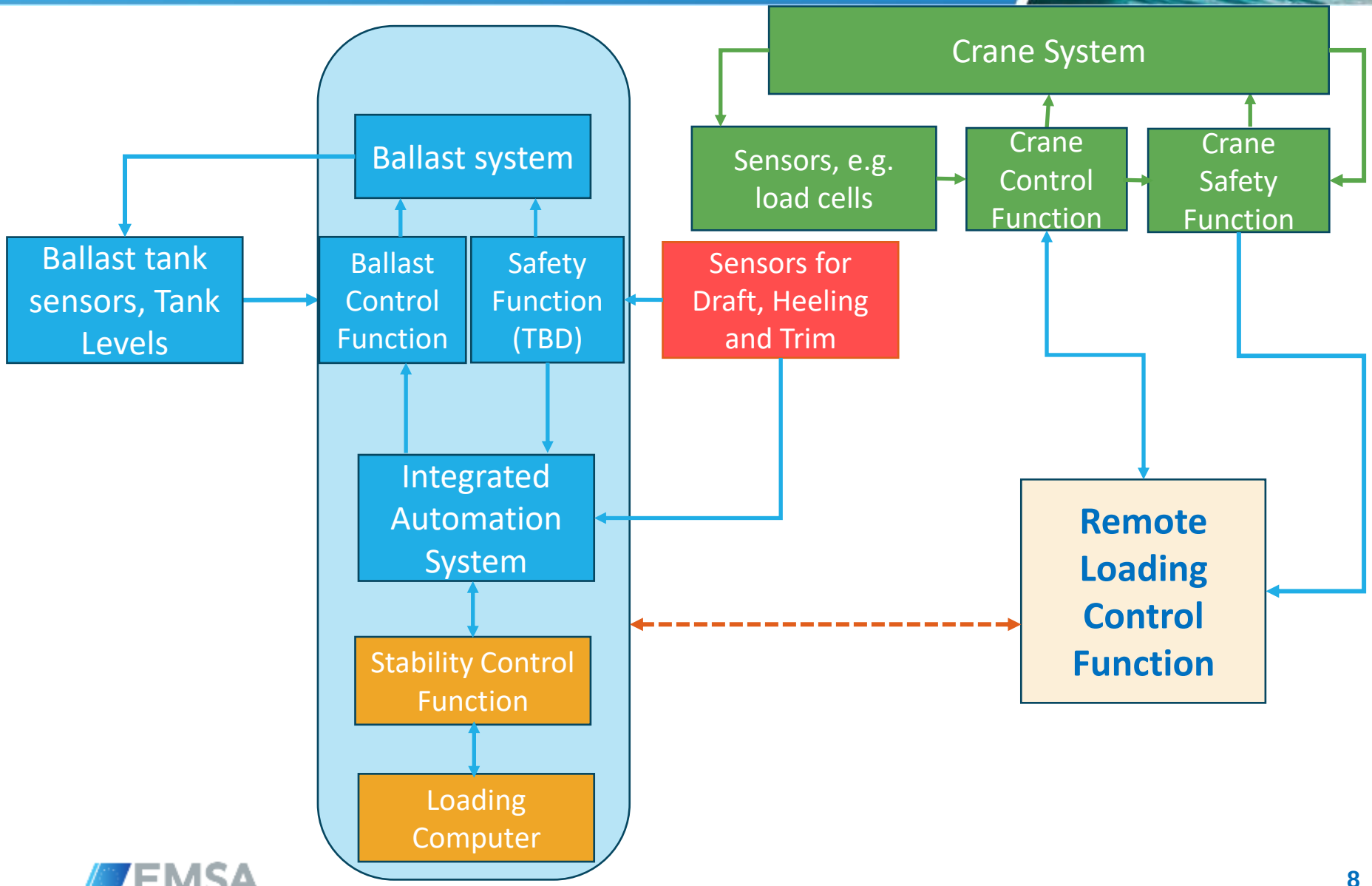
Function Based Approach

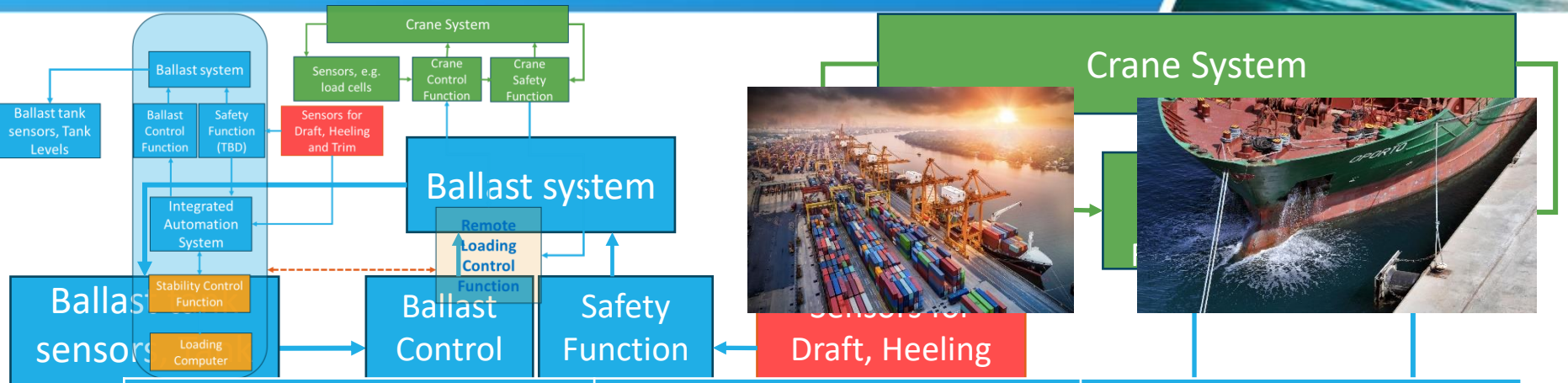
Identifies risk in control transfer

Systematic Risk Management

Missions and operations

Mission phase	Activities in port
Functions	**Handle and monitor cargo** - Plan and prepare cargo handling - Un secure/secure and unload/load cargo **Perform ballasting and trim/list** - Calculate and verify trim/list and stability - Operate ballast pumps **Maintain communication** - Communication between vessel and dock crane operator
Supervision	Active Supervision


Crane System
Ballast system
Sensors, e.g. load cells
Crane Control Function
Crane Safety Function
Ballast tank sensors, Tank Levels
Ballast Control Function
Safety Function (TBD)
Sensors for Draft, Heeling and Trim
Integrated Automation System
Remote Loading Control Function
Stability Control Function
Loading Computer



Functions	Subfunction/Control action	Performing Agent
Loading and unloading of Cargo	Provide and Control loading sequence	Remote Loading Control System
	Load / Unload Containers	Crane Control System
Performing ballasting	Calculate and verify trim & stability	Loading Computer
	Control Stability	Stability Control System
	Operate ballast pumps and valves	Ballast Control System

Supervisory Control Agents	Supervising	What can trigger supervisor action
Stability Control System	Operate ballast pumps and valves	Alarms from Ballast Control Function
	Control Unloading and loading sequence	Measured heeling draft or trim outside limits
Remote Loading Control System	Control stability	Alarm from the Stability Control Function
	Load/Unload containers	Alarms from Crane control Function
	Load/Unload containers	Communication problems or unexpected feedback from the Crane Function

Hazard Analysis (Part 2)

Guidewords	Unsafe condition	Causal factors	Worst case outcome	Incident category
Too early/late or in wrong order	Loading Sequence not executed as planned	Random hardware failure or systematic failure or systemic failure in the remote loading control function 	The sequence and weight of containers being loaded/unloaded in combination with the way ballast is shifted leads to too much heeling and/or wrong trim, of the vessel. Could lead to capsizing at quay or during transit	Capsize/listing 
Too early/late or in wrong of order	Loading Sequence not fit for purpose	Loading plan not appropriate	Container stacked in the wrong order	Capsize/listing

Hazard Analysis (Part 2)

Worst case outcome	Effect on Health Safety and Environment	Enabling Conditions	Exposure to enabling conditions	Operational restrictions	Classification of Health Safety Environment
Containers stacked in the wrong order and the point of gravity is too high	Significant	Large waves	High	None	Significant
Combination of loading with the way ballast is shifted, leads to too much heeling and/or wrong trim	Catastrophic	Large waves	High	None	Catastrophic

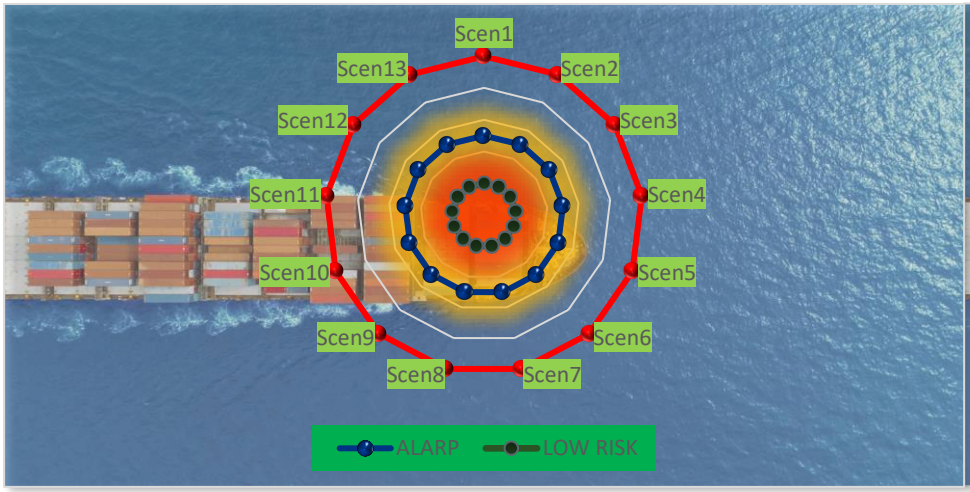
Mitigation Analysis (Part 3)

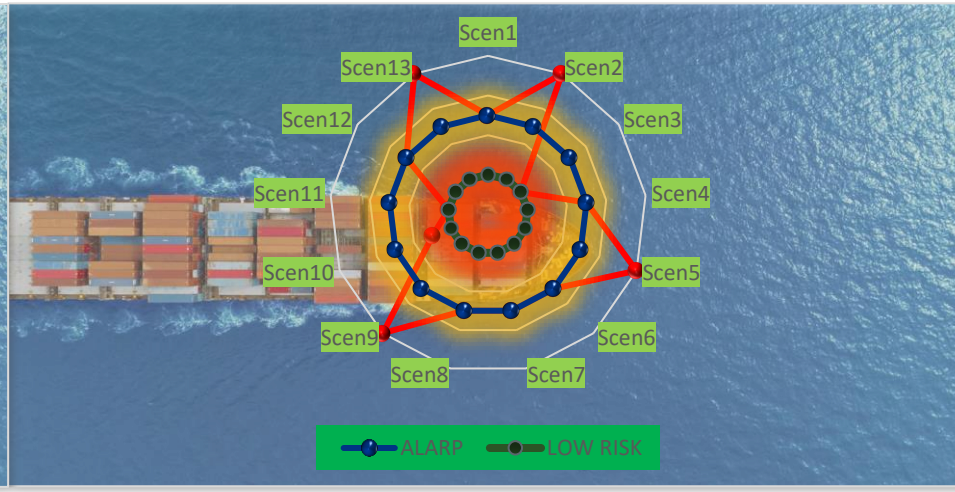
Mitigation name	Agent responsible for the activation	Mission phases	Events to which the mitigation is planned	Systems that must function	How humans are involved in executing the mitigation layer
Cargo operator actively supervising start of loading and unloading, can aboard operation	Cargo Operator	Loading/Unloading Cargo	Activation of unloading, ballasting or both.	ROC independent emergency stop 	Active Human Supervision

Risk Analysis and Risk Evaluation(Part 4)

Effectiveness of risk mitigations	Ship & Uptime related Severity					
	None	Negligible	Minor	Significant	Severe	Catastrophic
Low	Low	Low	Medium	High	High	High
Moderate	Low	Low	Low	Medium	High	High
Medium	Low	Low	Low	Medium	Medium	High
High	Low	Low	Low	Low	Medium	High
Very High	Low	Low	Low	Low	Low	Medium
Extremely High	Low	Low	Low	Low	Low	Low

- Classification of the worst case outcomes
- Prediction of the effectiveness of the mitigations
- Consider the operational restrictions and other limitations
- Consider the effectiveness of the embedded fault detection isolation and recovery capacity
- Consider the effectiveness of the various mitigations layer that were added to the systems

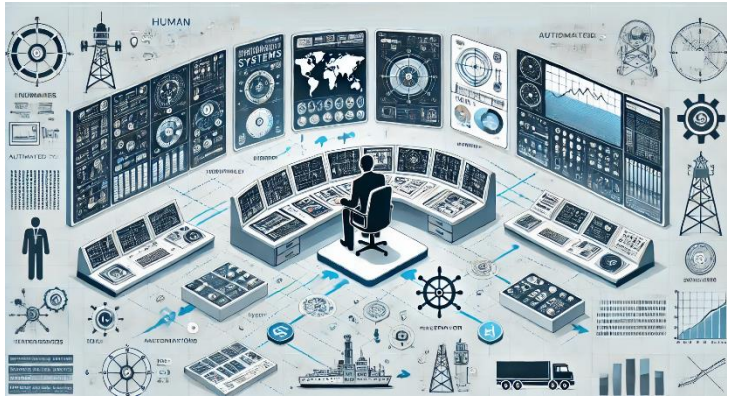


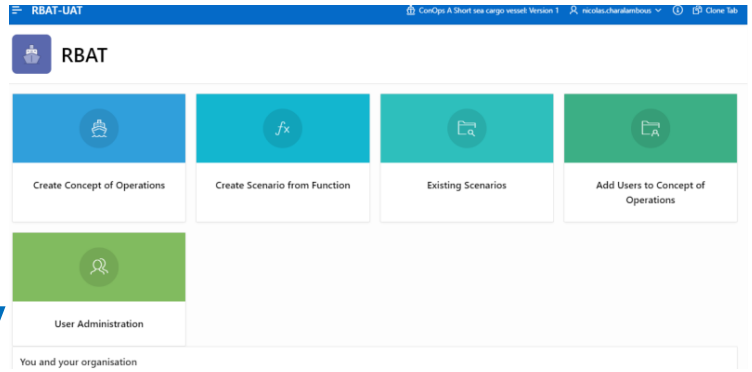


Mitigation Layers efficiency

Operational Restrictions

- Function-Based Approach;
- Novelty in Risk Management;
- Hazard Cause Analysis;
- Human Integration;
- Lack of Historical Data;
- Fallback Functions/States Identification;
- Mitigation Evaluation;
- Critical System Identification;
- Project Alignment;
- Transparency and Traceability





emsa.europa.eu

- twitter.com/emsa_lisbon
- facebook.com/emsa.lisbon

EMSA
European Maritime Safety Agency