WHEN TRUST MATTERS

Risk-based Assessment Tool for MASS concepts

NFAS

Remi Brensdal Pedersen

31 May 2022

European Maritime Safety Agency

RBAT purpose

Risk assess whether increased or new ways of using automation and remote operation is as safe or safer than conventional shipping.

RBAT framework and tool

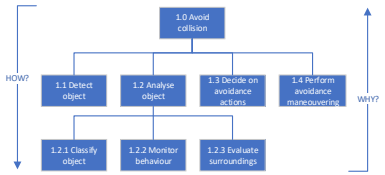
RBAT

Framework

Tool

What is automated (and why)?

Multi-level function map



- Operational modes and context
- Ship type

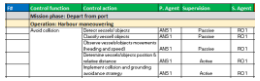
How is it automated (and why)?

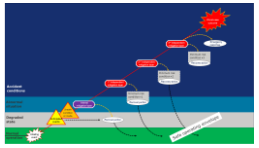
Use of automation

- Human involvement
- Automation mode
- Operator location
- Etc.

How can it *fail* (and be mitigated)?

Risk model

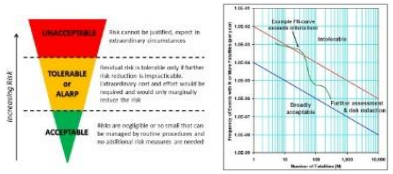




Is it safe (enough)?

HAZID/ Risk acceptance criteria

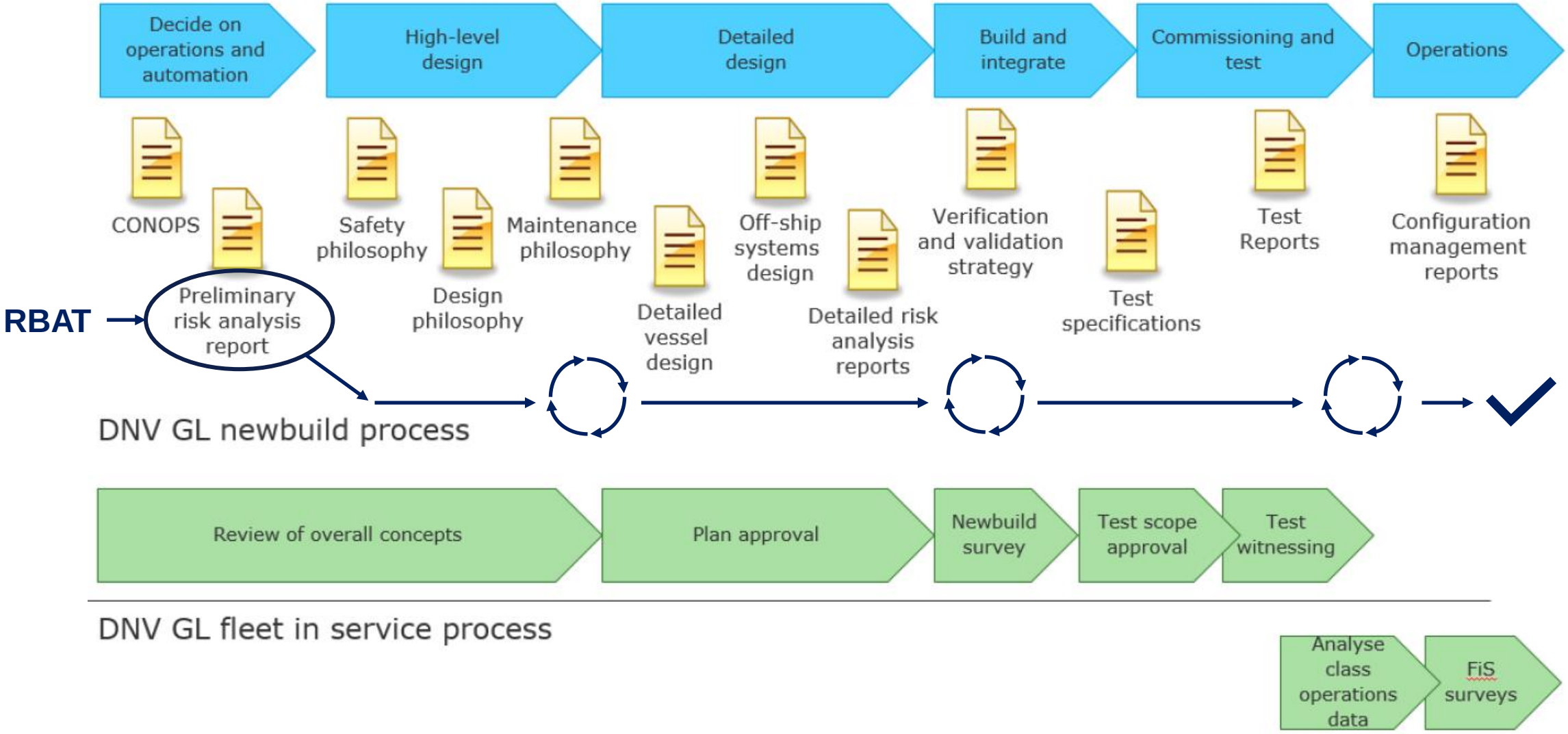
Effectiveness of risk mitigation layers	Severity					
	No effect	Negligible	Minor	Significant	Severe	Catastrophic
Low	Low	Medium	High	High	High	High
Moderate	Low	Low	Medium	High	High	High
Medium	Low	Low	Medium	Medium	High	High
High	Low	Low	Low	Medium	Medium	High
Very high	Low	Low	Low	Low	Medium	Medium
Extremely high	Low	Low	Low	Low	Low	Medium



Concept of Operations
- Functions
  - Sub-functions

→ Auto-remote solution → Hazard and mitigation analysis → Risk evaluation/ ALARP → Equivalent safety?

Submitter's activities



Proposed usage by EMSA

Ref. Ares(2022)645065 - 27/01/2022

EMSA
European Maritime Safety Agency

Lisbon, 27 January 2022

Subject: The RBAT (Risk Based Assessment Tool) in the approval process of MASS projects

Dear Sir/Madam,

During the discussions at the MASS workshop which took place on 25/06/2021, it became obvious that the way the RBAT can be used in the approval process was not clear to the participants. As a result, it was agreed that EMSA would prepare a proposal for a flowchart to clarify the possible use of RBAT.

The Annex of this document is describing a proposed usage by different parties of the RBAT once it has been finalised. EMSA would appreciate any input or comments to the proposed utilisation of the tool, especially since this structure will influence its structure and settings

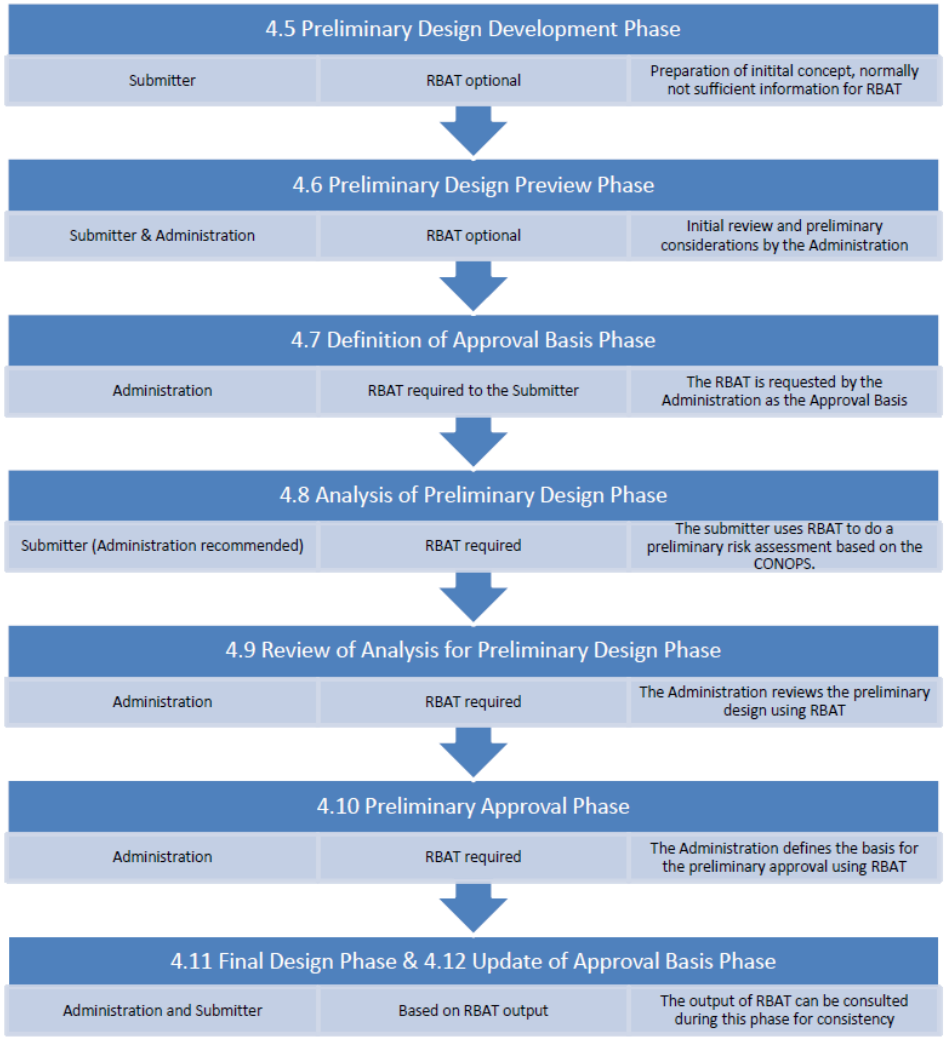
I would appreciate if you could send your comments to: Sifis.Papageorgiou@emsa.europa.eu.

Yours sincerely,

Leendert Bal
Head of Department
Safety, Security and Surveillance

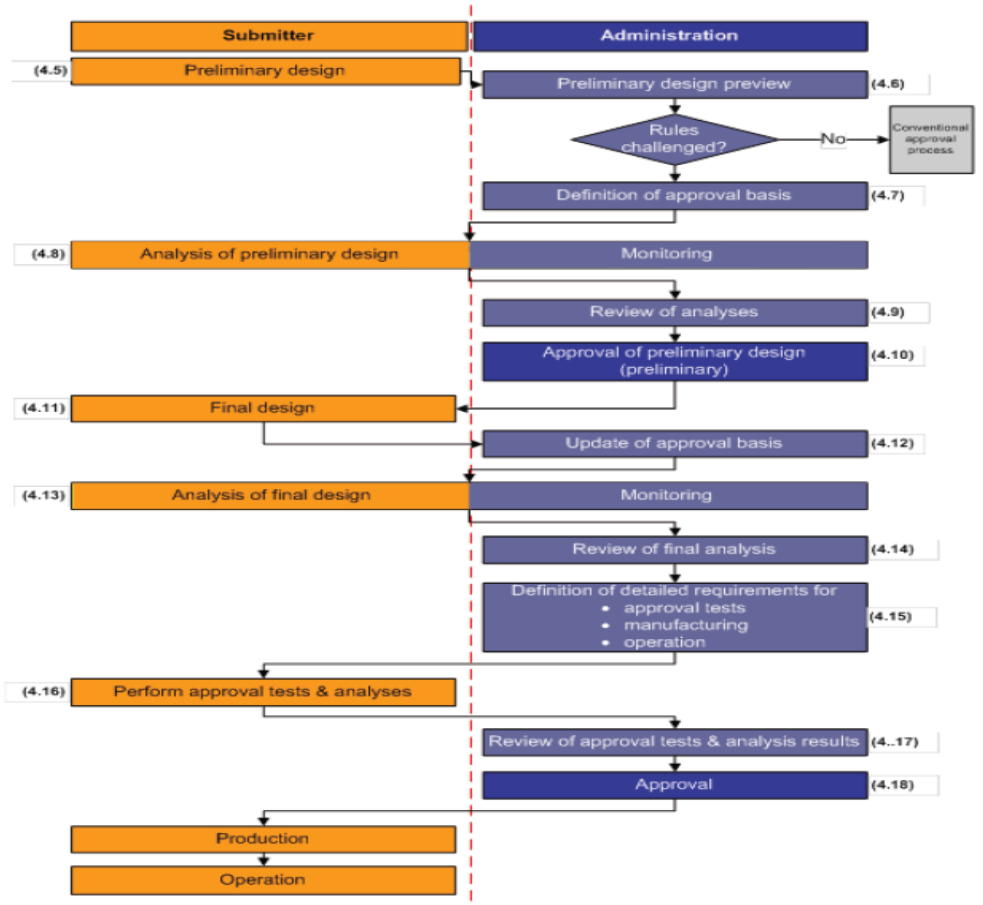
Page 1 of 6

Leendert.Bal@emsa.europa.eu
EMSA, Praça Europa 4, 1249-206 Lisbon, Portugal
emsa.europa.eu



What does the guidelines say?

IMO MSC.1/Circ.1455 Alternative Design



NMA circular

		MSC.1/Circ. 1455	*RSV 2020/12*
1. Foreløpig design (Preliminary Design)		4.5	
	1.1 Concept of operation - CONOPS	4.5	7.1
	1.2 Pre-HAZID		7.2
	1.3 Sikkerhetsfilosofi		7.3
	1.4 Designfilosofi		7.4
	1.5 Drift- og vedlikeholdsfilosofi		7.5
2. Analyse av foreløpig design (Analysis of preliminary design)		4.8	
	2.1 Oppdatert Pre-HAZID med tilhørende		7.2
	2.2 risikoanalyser/vurderinger		7.2
	2.2.Gap-analyse		7.6
	2.3 HAZID og risikovurderinger		7.9
3. Analyse av endelig design (Analysis of final design)		4.1	
	3.1 HAZID og risikovurderinger		7.9
4. Performance approval tests & analyses		4.1	
	4.1 Failure Mode and Effect Analysis (FMEA)		7.10
	Testkrav		9

7.2 Pre-HAZID

Basert på CONOPS skal det gjennomføres en pre-HAZID, hvor hele operasjonen gjennomgås og hvor det settes fokus på hvilke farer som foreligger på de ulike delene av operasjonen. Det skal gjøres risikoanalyser/vurderinger knyttet til identifiserte farer i HAZID. HAZID skal som et minimum dekke følgende:

d) Kommunikasjon
e) Navigasjon og farled
f) Fartøyets funksjoner
g) Fjernstyring
h) Evakuering/beredskap

7.9 Risikovurderinger og HAZID

Når endelig design og løsninger er utredet, skal det fremlegges en overordnet risikoanalyse med tilhørende HAZID. Risikoanalysen skal belyse områder som avviker fra gjeldende regelverk.

Risikoanalyser skal utføres av personer som har dokumentert kunnskap om den relevante metodikken som benyttes, samt innehar den nødvendige kunnskapen om systemene som skal vurderes. Roller og kompetanse skal kunne dokumenteres. Generelt skal risikovurderinger inneholde følgende:

a) Oppnåelse av definerte akseptkriterier for prosjektet
b) Overordnede risikoanalyser skal inneholde en pålitelighetsanalyse/sårbarhetsanalyse fra hver leverandør/produsent av sikkehetskritiske driftssystem. Denne skal identifisere konsekvensene av eventuelle enkeltfeil. Produsentens operasjons- og konstruksjonsbegrensninger for systemet må tas hensyn til i analysen.
c) Risikoanalyser skal ta hensyn til innføring av ny teknologi, og/eller ny anvendelse av eksisterende teknologi.
d) Sikkerkritiske systemer for operasjon og drift skal identifiseres.
e) Risiko vedrørende menneske-maskin-grensesnitt (HMI).

Bureau Veritas

Topic	Plans and documents to be submitted
Classification	Plans and documents to be submitted according to Society Rules in the scope of the classification of the ship and relevant to the service notation applied for
Additional class notations	Plans and documents to be submitted according to Society Rules in the scope of the additional class notations as specified in this Guidance Note, see Sec 3, [2.3.1], Sec 3, [4.3.1], Sec 3, [5.3.1] and Sec 4, [7.1.1]
Operational limitations	Details of parameters to which the crew or operators must refer for the control of the ship, see [2.3]
Identification	Details of provisions for identification, see [2.4]
Interactions	Details of provisions for interactions, see [2.5]
Automation systems	Detailed specification of all automation systems, including: • Specification of the Navigation system, see Sec 3, [2] • Specification of the Communication network and system, see Sec 3, [3] • Specification of the Machinery system, see Sec 3, [4] • Specification of the Cargo management system, see Sec 3, [5] • Specification of the Passenger management system, see Sec 3, [6] • Specification of the Remote Control Centre, see Sec 3, [7] These specifications should clearly specify for each function the distribution of roles and responsibilities between the human and the system, see [2.6] and [1.8.2]
Risk assessment	Detailed risk assessment report including: • Groups of functions considered, see Sec 2, [2.2] • List of hazards considered, see Sec 2, [2.3] • Risk analysis outcome, see Sec 2, [2.4] • Risk Control Options considered, see Sec 2, [2.6]
Technology assessment	Detailed technology assessment report, if applicable, see Sec 2, [3]
Reliability	Details of provisions for improving the reliability of systems including: • General system design, see Sec 4, [2] • Human machine interface, see Sec 4, [3] • Network and communication, see Sec 4, [4] • Software quality assurance, see Sec 4, [5] • Data quality assurance, see Sec 4, [6] • Cybersecurity, see Sec 4, [7]
Testing	Detailed tests specifications and reports, including: • Software tests, see Sec 4, [8.1] • Simulation tests, see Sec 4, [8.2] • Full scale tests, see Sec 4, [8.3] All tests reports should include the targeted objective, the followed procedure, the expected results and the outcome achieved

American Bureau of Shipping

Concept of Operations Document

Goal

The goals of the Concept of Operations Document (

i) provide a clear vision of the intended use ar

ii) facilitate a clear understanding of the syster

iii) present information related to the ba requirements of the autonomous and remot and utilized by all stakeholders

iv) highlight differences between current / conv

v) provide the basis for system validation

To meet these goals, a Concept of Operations Docur

i) describe the desired function features and c

ii) provide a description of the operational env

iii) describe how the function will be used

iv) facilitate understanding of the overall funct

v) form an overall basis for long-range operati subsequent system definition documents su

Content

The list below provides a guidance on the list of content required for the CONOPS.

i) General	*a)*	Objectives of the proposed function
	b)	Scope of the proposed function
	c)	Description and overview of the proposed function
	d)	Expected reliability requirements of the proposed function
ii) Functional integration	*a)*	Operational policies and constraint
	b)	Performance and reliability characteristics
	c)	Capabilities, functions/services and features
	d)	Limitations and boundaries of function
	e)	Integration with related onboard functions
	f)	Major system elements and the interconnection among those elements
iii) Operational environment & scenarios	*a)*	Operational Envelope - Intended Area of Operations and Details/ Limitations/Restrictions
	b)	Defined Planned Voyage and Operation Phases with supportive Methods of Control
	c)	Characteristics of operational environment
	d)	Modes of operation
	e)	Major elements and the interconnection among those elements
	f)	Interfaces to external systems or procedures
	g)	Interface with other stakeholders in the environment for example other vessels/units, port State and coastal State.
	h)	Operational risk factors
	i)	Provisions for safety, security, integrity and continuity of operations in emergencies
	j)	Logistics requirements

2.3.1 Concept of operation

The first step is for the submitter to decide on which of the operational tasks that traditionally have been performed by crew that will be performed either by remote-control and/or automatically.

In some cases, the project's goal is to reduce or remove crew from the vessel (compared with conventional ship operations). In other cases, the goal is not to reduce the crew, but to increase the safety or efficiency of the operations with the current crew.

The concept of operations should clearly describe all the operational tasks that the vessel will undertake that will be either fully or partly automated.

Each operational task should be further broken down into sub-tasks to a level that enables a clear distinction between tasks where a human is in charge of decision making and tasks where a system is in charge of decision making.

When a human is in charge of decision making, the location of the decision maker should be clearly described. Typically, this will be either:

- on-board
- from a remote control centre (RCC)
- a combination of persons on-board and persons in a RCC.

Whenever human intervention is expected or required by the system(s), special attention should be placed on the timing aspects, and the ability of the human to establish sufficient situational awareness so that correct actions can be taken within reasonable time (this is sometimes referred to as the command latency).

Other aspects of the planned characteristics and operations should also be described, including, but not limited to:

- operational area(s)
- vessel characteristics
- jurisdictions and regulations
- safety and availability targets
- weather and sea-state limitations
- presence of crew or other personnel on board the vessel
- roles and responsibilities of involved personnel
- minimum risk conditions for the vessel
- remote control centre characteristics
- communication-link characteristics (including coverage analysis of wireless communications)
- preliminary performance requirements for the key autoremote functions and systems (e.g. safe speed, vessel not under command, position keeping, object detection ranges, object identification, etc).

Such description of operational aspects should be contained in the document concept of operation (CONOPS). To aid customers in creating good CONOPS documents, DNV GL provides a CONOPS template as well as lists of possible modes, operations and tasks typically relevant for commercial vessels, and may be subject to automation and remote-control. These documents can be obtained upon request to the DNV GL.

Multi-level function map

Automation

- Parasuraman and Riley (1997, p. 231) defines automation as;
  - *"the execution by a machine agent (usually a computer) of a **function** that was previously carried out by a human".*

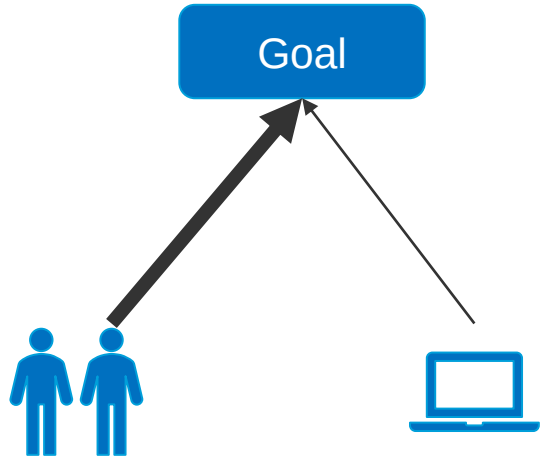
- The term function can be defined as;
  - *Specific purpose or objective [i.e. **goal**] to be accomplished, that can be specified or described without reference to the physical means of achieving it* (IEC, 2020).

  or
  - *A purpose [i.e. **goal**] for which something is designed or exists* (DNV GL, 2019).

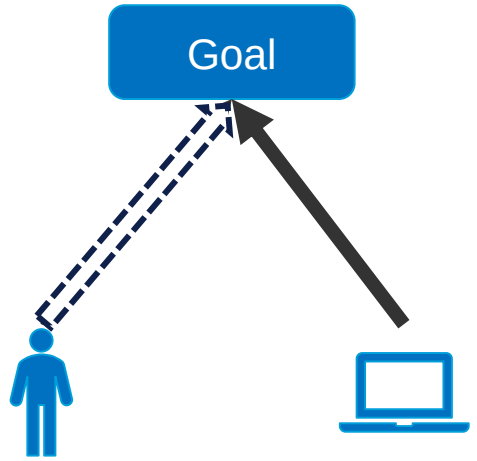
- In principle, the terms "goal" and "function" are interchangeable (IEC, 2000).

Similar **goals**, different allocation of functions (between humans and technology) – implies a **hierarchy** of goals

Low "degree" of automation



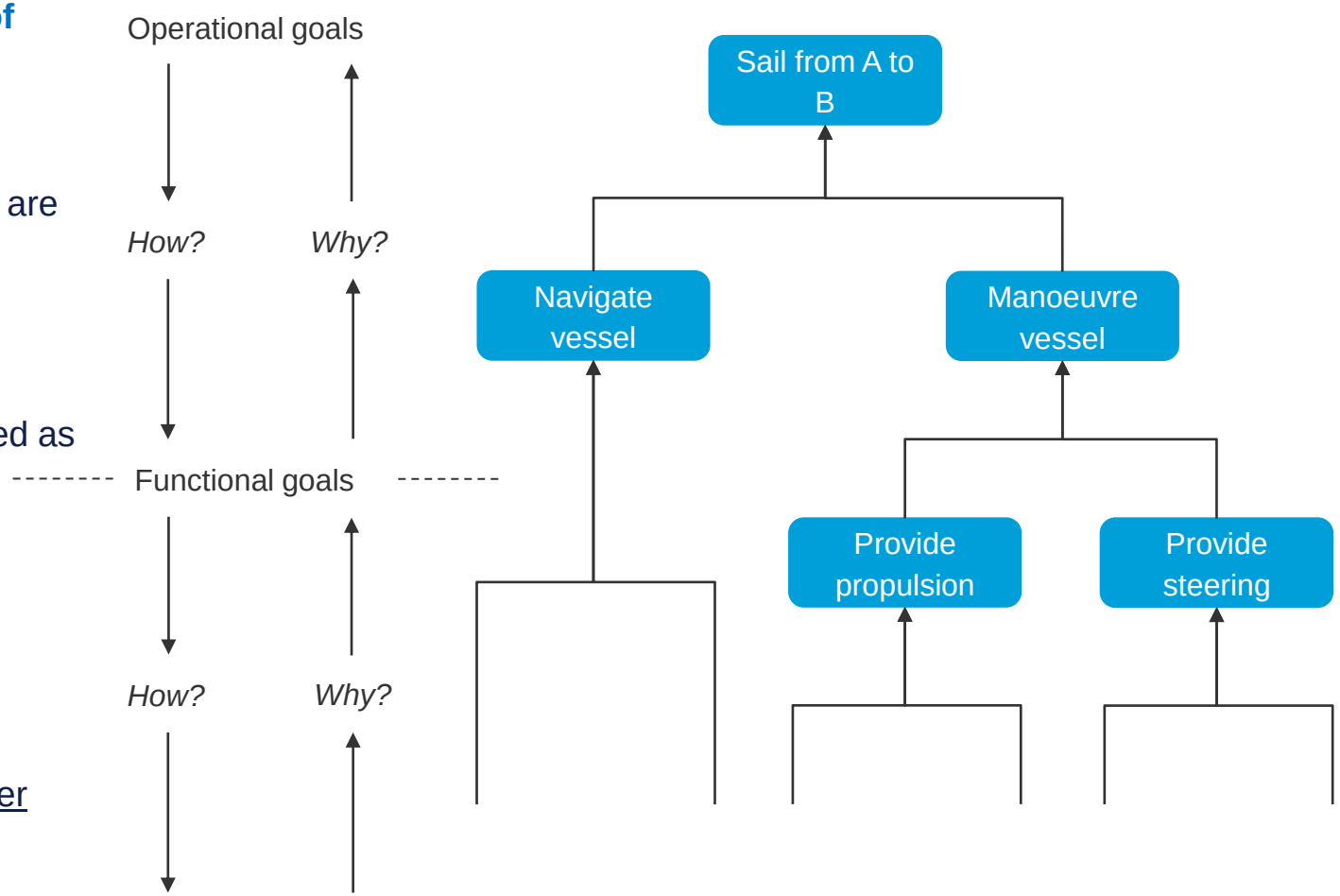
High "degree" of automation



…but more (complex) supervision.

Hierarchical goal structure

- Functions (i.e. goals) can be considered at various **levels of abstraction**.
- When modelling complex systems, these abstraction levels are often expressed as **goal hierarchies**.
- Higher level functions are often expressed as abstract **operational goals**, while lower level functions are expressed as **functional goals**.
  - Operational goals-> purpose of performing operation(s)
  - Functional goals-> purpose of using technology
- An inherent property of goal hierarchies is that <u>different lower level goals may serve the same higher level goals</u>.



RBAT Methodology

RBAT methodology

DNV has developed a risk assessment methodology specifically for systems involving remote control and advanced use of automation.

The method consists of five steps:

- Step 1: Define Use of Automation
- Step 2: Hazard analysis
- Step 3: Mitigation analysis
- Step 4: Perform risk evaluation
- Step 5: Address risk control

USE OF AUTOMATION/ REMOTE CONTROL					
Control function	**Control action**	**Performing agent**	**Supervision category**	**Supervising agent**	**Other systems and roles involved (onboard, onshore)**
Mission phase: Arrival in port					
Operation: Perform port/harbour manoeuvering					
Perform manoeuvring	Approach dock at low speed	Onboard autonomy system	Active supervision	Onboard safety operator	Thrusters, thruster control system
...	...	...	...	...	...

HAZARD ANALYSIS					
Unsafe condition/ mode	**Guideword**	**Causal factor(s)**	**Worst-case outcome**	**Event category**	**Severity**
Vessel fails to reduce speed.	Needed but missing/ Not provided when needed	Control system failure	Impact with quay in transit speed	Contact with shore object	Significant - Single serious or multiple injuries
	...	...	...	...	...

MITIGATION ANALYSIS					
Internal mitigation layer (self-recovery capacities)	**1st independent mitigation layer**	**2nd independent mitigation layer**	**3rd independent mitigation layer**	**Mitigation effectiveness**	**Criticality**
Yes	Emergency stop (MRC2)	Drop of emergency anchor (MRC3)	None	High	Medium
...	...	...	...	...	...

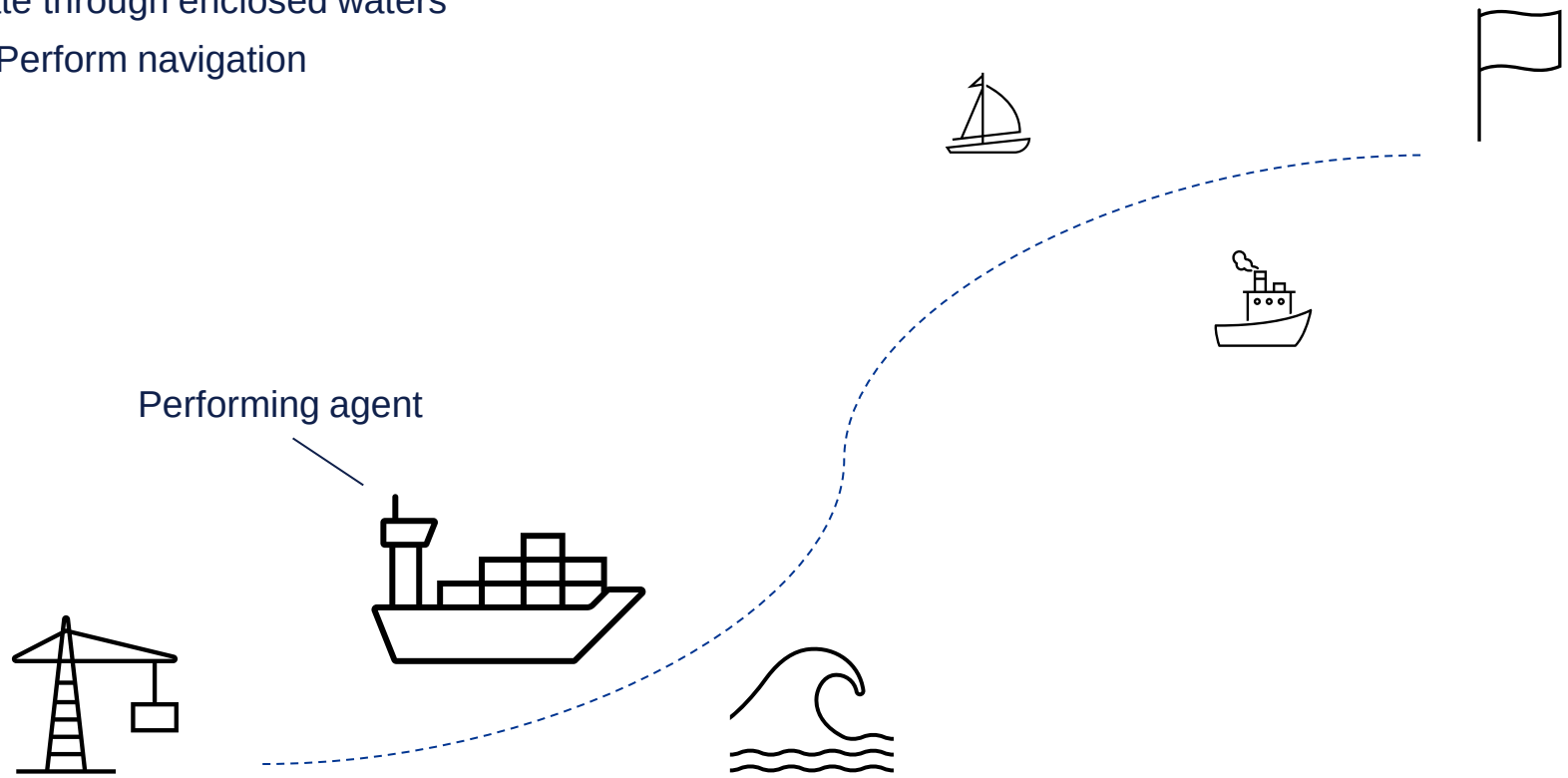
RISK CONTROL	
Comments (incl. Assumptions)	**Actions**
Dropping the emergency anchor requires manual actions.	Verify that there will be enough time available for the onboard safety operator to drop anchor.
...	...

Step 1: Use of automation

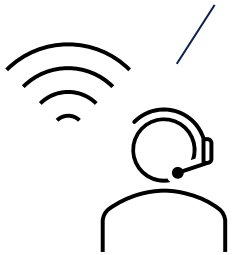
Mission phase: Transit to location

Operation: Navigate through enclosed waters

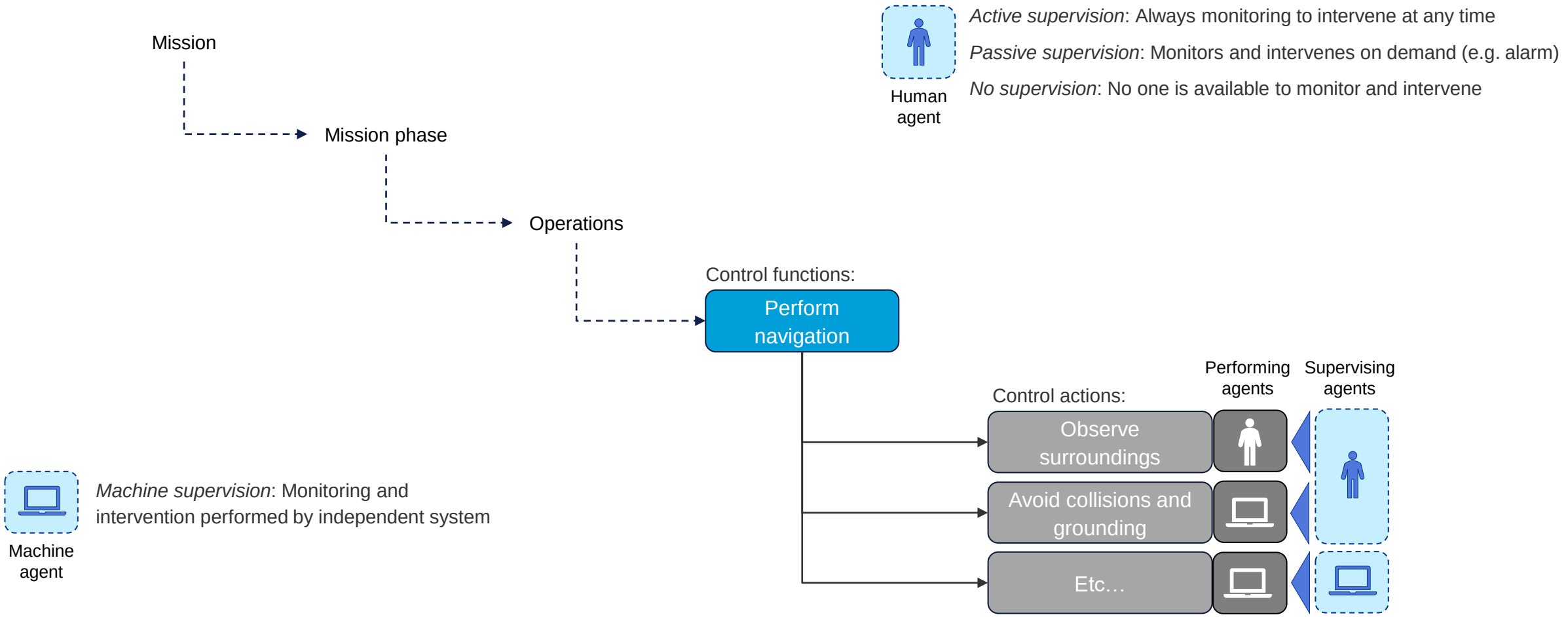
Control Function: Perform navigation



Active Supervising agent



Allocation of functions



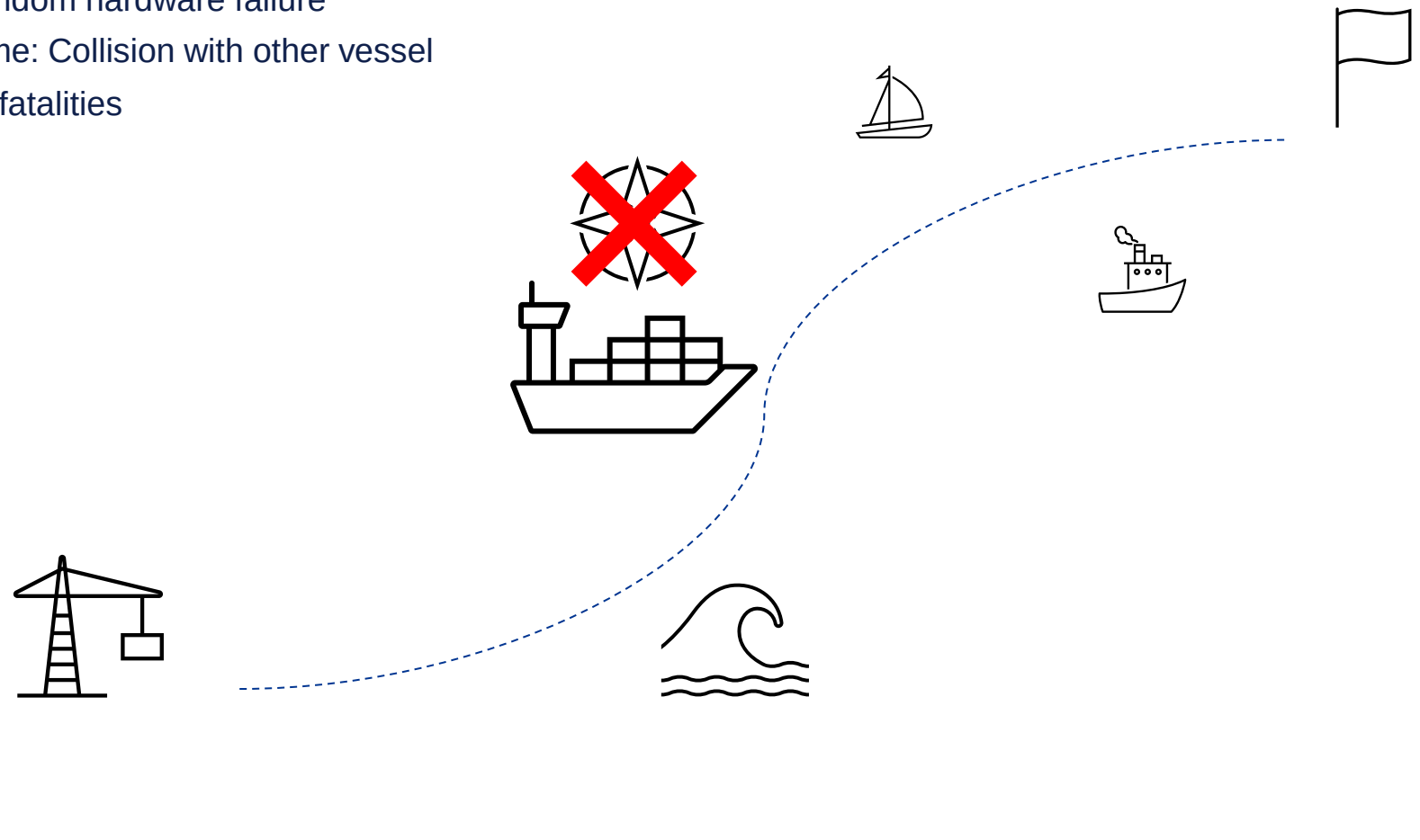
Step 2: Hazard analysis

Unsafe condition: Navigation is not provided

Causal factor: Random hardware failure

Wost-case outcome: Collision with other vessel

Severity: Multiple fatalities



Hazard identification

Unsafe conditions

- Not provided
- Provided when not required
- Incapable/not fit for purpose
- Control parameters out of range
- Control parameters are within range but incorrect
- Too early/late or in wrong order
- Stops too soon
- Applied to long
- Not followed/rejected

+

Causal factors

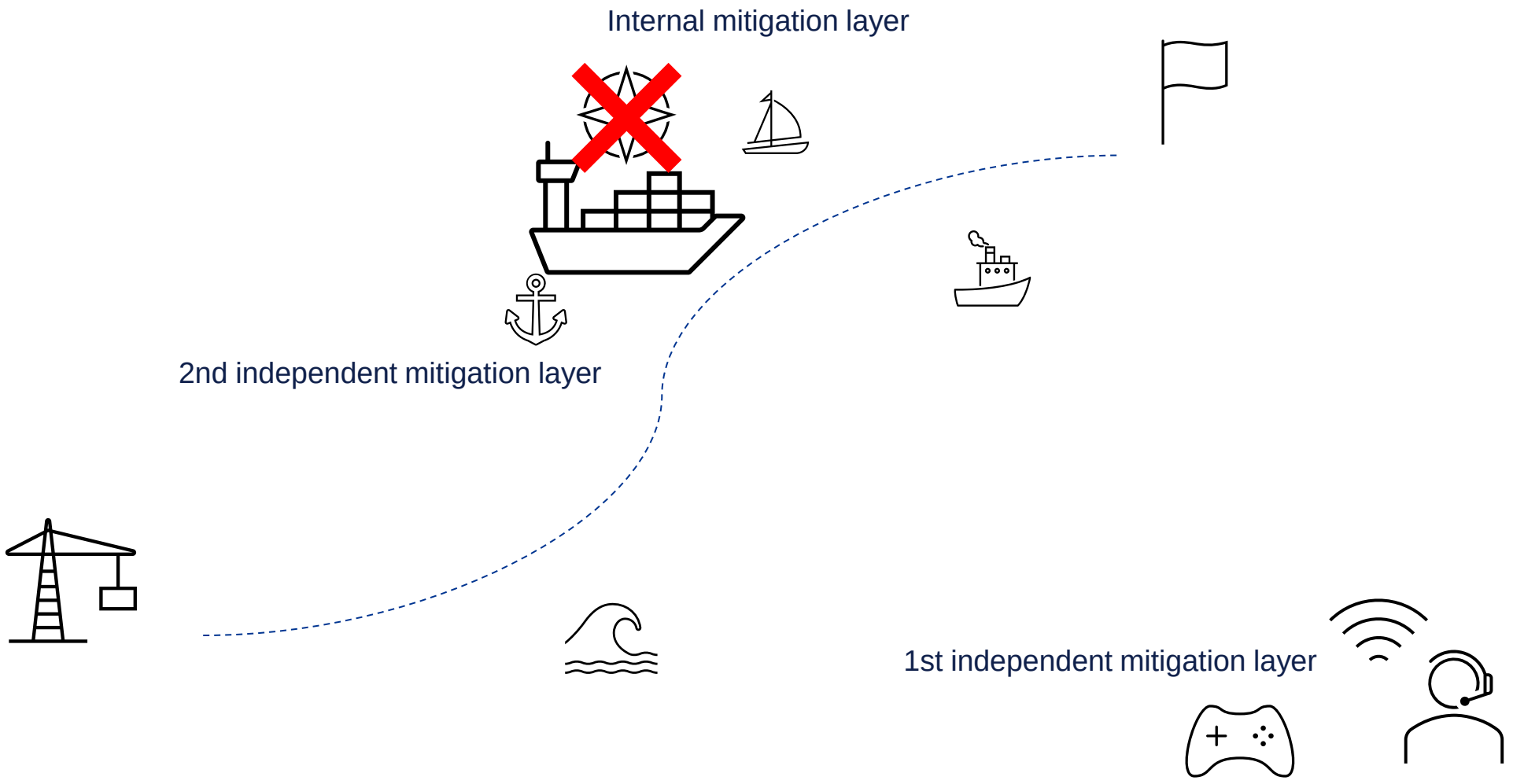
- Random hardware failures
- Systematic failures
- Systemic failures
- Operator failures
- Failures due to environmental conditions
- Failures due to deliberate actions

=

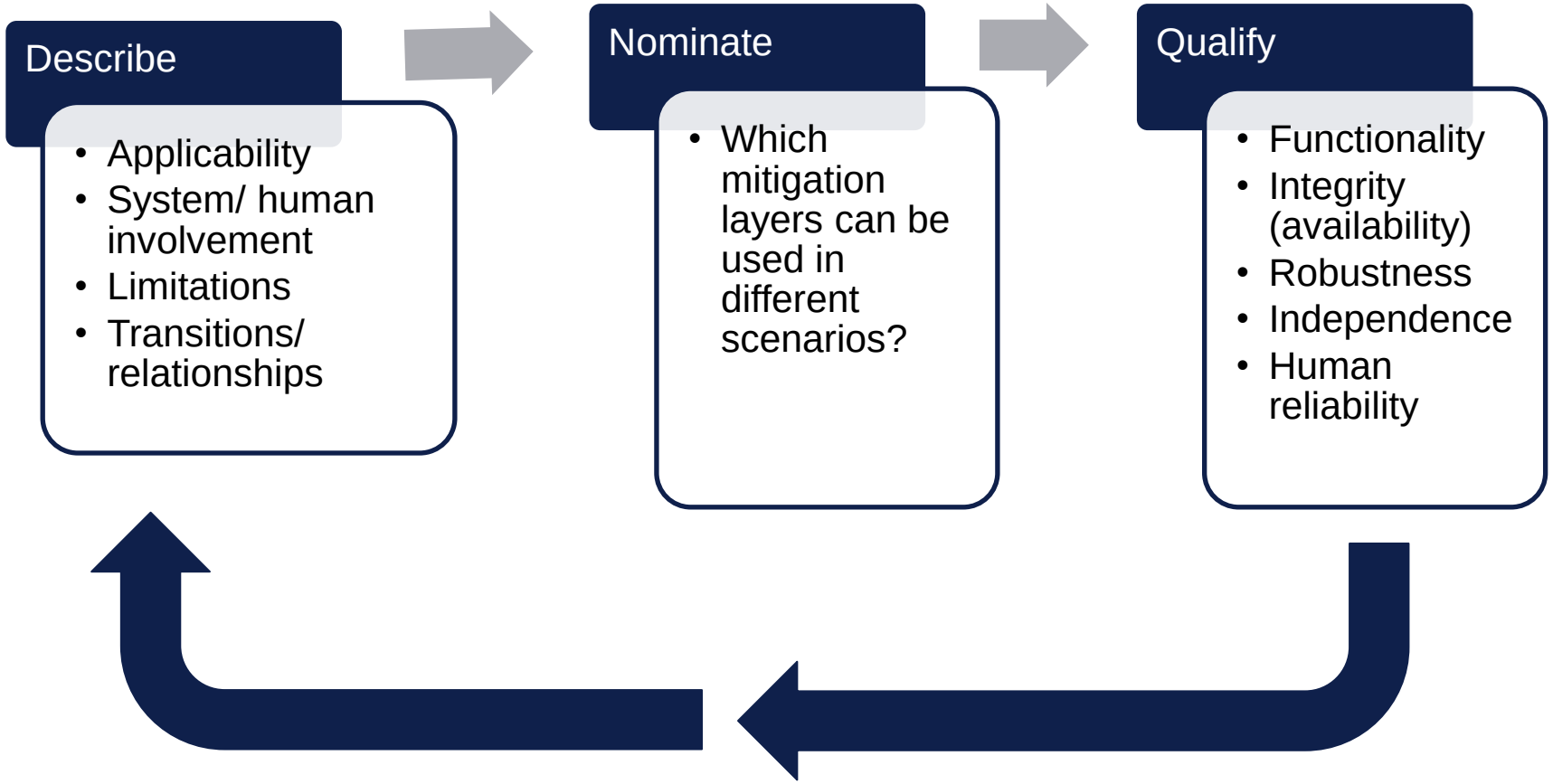
Accidents with losses

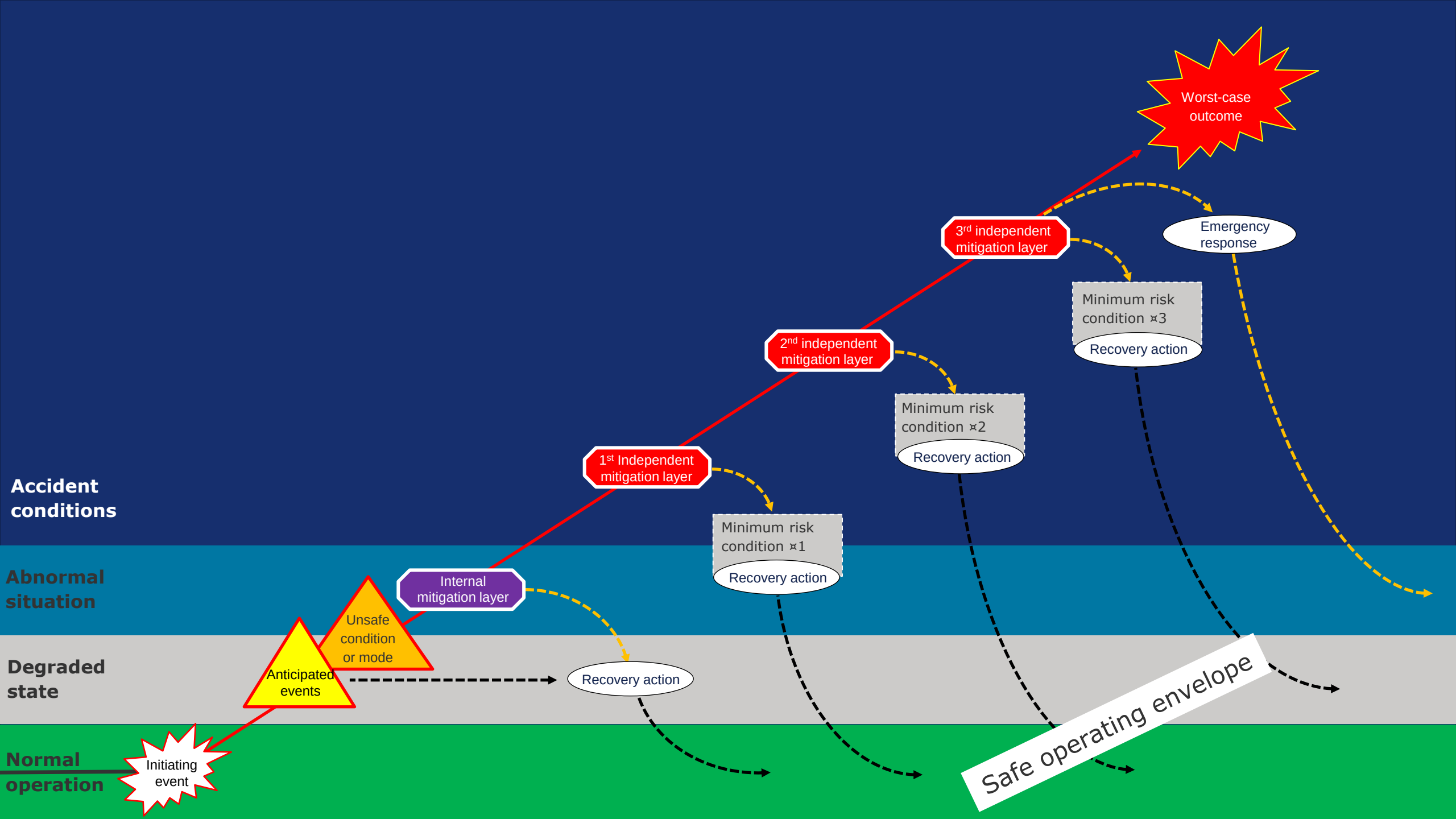
- Collision
- Contact
- Grounding/stranding
- Fire/explosion
- Capsize/listing
- Flooding/foundering
- Damage to ship equip.
- Hull failure
- Non-accidental event
- Missing
- Loss of control

Step 3: Mitigation analysis



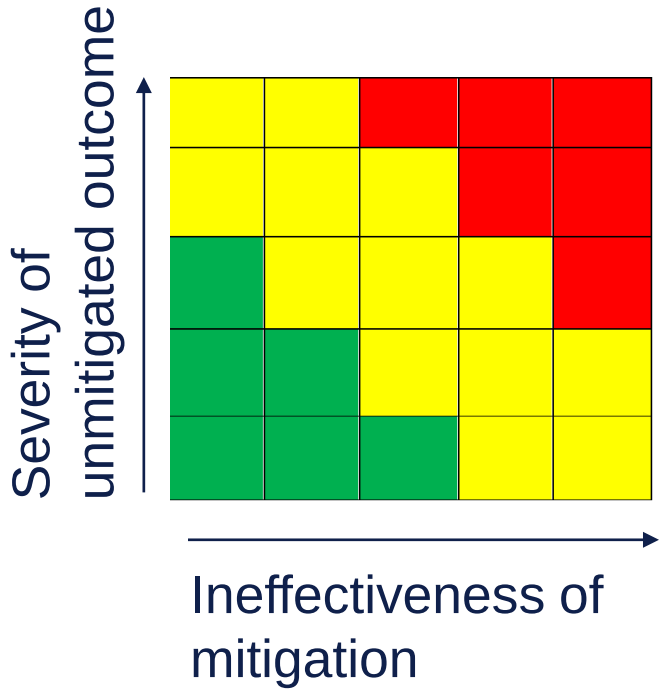
Focus on mitigations




Worst-case outcome
3rd independent mitigation layer
Emergency response
Minimum risk condition ¤3
Recovery action
2nd independent mitigation layer
Minimum risk condition ¤2
Recovery action
1st Independent mitigation layer
Minimum risk condition ¤1
Recovery action
Internal mitigation layer
Unsafe condition or mode
Anticipated events
Recovery action
Initiating event
Safe operating envelope
Accident conditions
Abnormal situation
Degraded state
Normal operation

Step 4: Risk evaluation in RBAT – alternative approach

- There is a trend towards qualitative techniques, both in research and industry standards
- Frequency of initiating (software related) events is not considered
- Instead the focus is to assess whether failures/hazards are associated with severe outcomes
- If this is the case, it must be ensured that the mitigation (recovery, response) is adequate, compared relatively to the severity
  - Criticality=severity of outcome*effect of mitigation
- If mitigation itself cannot reduce the risk sufficiently, the integrity of the control function must be assured (development, testing etc.) and the residual risk must be accepted by stakeholders



Severity	Effects on human safety
No effect	No injuries
Negligible	Superficial injury
Minor	Single injury or multiple minor injures
Significant	Single serious or multiple injuries
Severe	Single fatality or multiple serious injuries
Catastrophic	Multiple fatalities (more than one)

Effectiveness	Description
Very high	At least three effective *independent* mitigation layers that for the assessed scenario can prevent losses regardless failure cause.
High	At least two effective *independent* mitigation layers that for the assessed scenario can prevent losses regardless failure cause.
Medium	At least one effective *independent* mitigation layer that for the assessed scenario can prevent losses regardless failure cause.
Moderate	At least one *internal* mitigation layer that can prevent losses from random *hardware* failures. The control function has additional capacities for self-recovery from other types of failures, however, for the assessed scenario these are not effective regardless failure cause.
Low	The control function has some capacities for self-recovery, however for the assessed scenario these are expected to have a limited effect.

Step 4: Risk evaluation in RBAT – alternative approach

Effectiveness of risk mitigation layers	Severity					
	No effect	Negligible	Minor	Significant	Severe	Catastrophic
Low	Low	Medium	High	High	High	High
Moderate	Low	Low	Medium	High	High	High
Medium	Low	Low	Medium	Medium	High	High
High	Low	Low	Low	Medium	Medium	High ✕
Very high	Low	Low	Low	Low	Medium	Medium
Extremely high	Low	Low	Low	Low	Low	Medium

Step 5: Risk control

Operational restrictions/ reduced hazard exposure

Effectiveness of risk mitigation layers	Severity					
	No effect	Negligible	Minor	Significant	Severe	Catastrophic
Low	Low	Medium	High	High	High	High
Moderate	Low	Low	Medium	High	High	High
Medium	Low	Low	Medium	Medium	High	High
High	Low	Low	Low	Medium	Medium	High
Very high	Low	Low	Low	Low	Medium	Medium
Extremely high	Low	Low	Low	Low	Low	Medium

Improved/ additional mitigations

Summary

Benefits

- Tool and framework facilitates a systematic and structured approach tailored to address risks introduced by automation and remote ops
  →Provides confidence (assurance) that the most relevant hazards have been considered
- Goal-based approach, i.e. can be adapted according to a large variety of concepts and maturity levels
- Assess use of automation across various contexts (mission phases and operations)
- Combines assessment of operator performance (human element), technical failures and external conditions

Limitations

- RBAT is a *functional approach* – this implies that unless functions required to manage hazards have not been identified, risk associated with functional failures will not be assessed
  → For example, if batteries have not been identified as a hazard, the function “ventilate explosive gases” may not have been included in the assessment
  → A coarse “pre-HAZID” can be performed to address this gap
- Functions not considered to be affected by automation and remote control not part of scope → assumed to be covered by existing rules and regulations

Thank you!

- Contact information:

  - Remi Brensdal Pedersen
  - Email: remi.brensdal.pedersen@dnv.com
  - Phone: 90553439