How to qualify safety of MASS technology?

Safety Assessment of Maritime Autonomous Surface Ships: A Scenario-Based Approach

Georg Hake
German Aerospace Center (DLR)

Day 1
11:20 - 11:40
Hamburg

in cooperation with:

NFAS INAS
International Network for Autonomous Ships

MASS Technology

ICMASS2025
International Conference on Maritime Autonomous Surface Ships

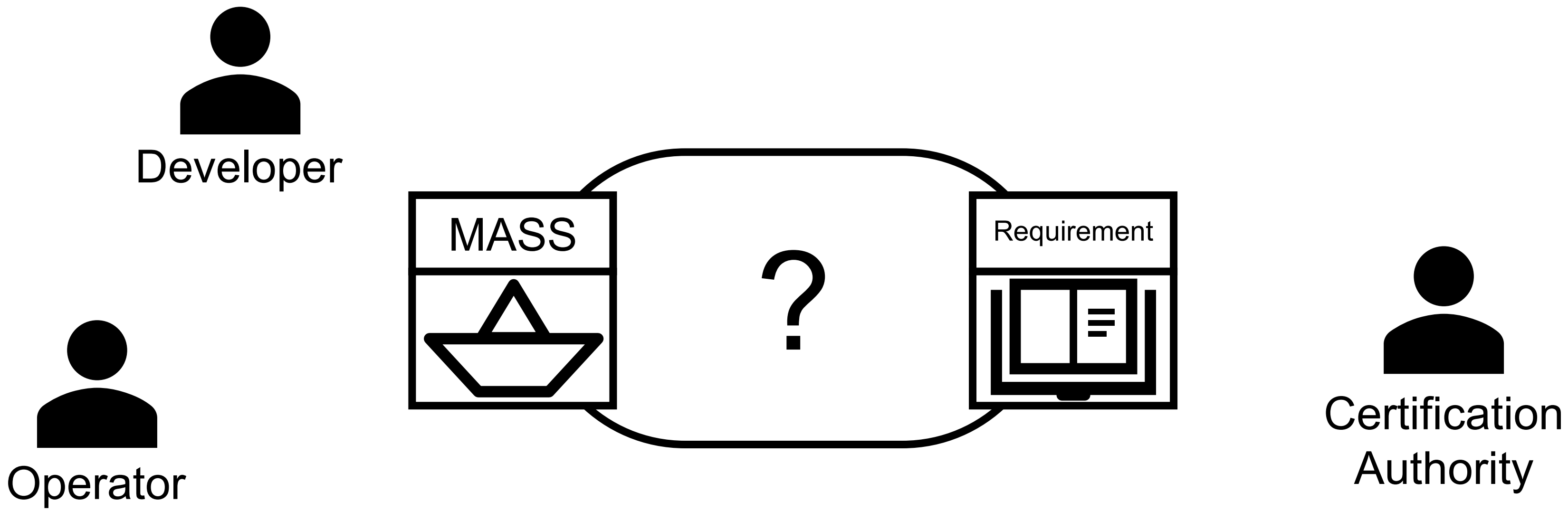
SAFETY ASSESSMENT OF MARITIME AUTONOMOUS SURFACE SHIPS:
A SCENARIO-BASED APPROACH

Authors: Georg Hake, Anna Austel, Jan Steffen Becker, Lina Putze, Nina Wetzig

Presented by: Georg Hake

Motivation

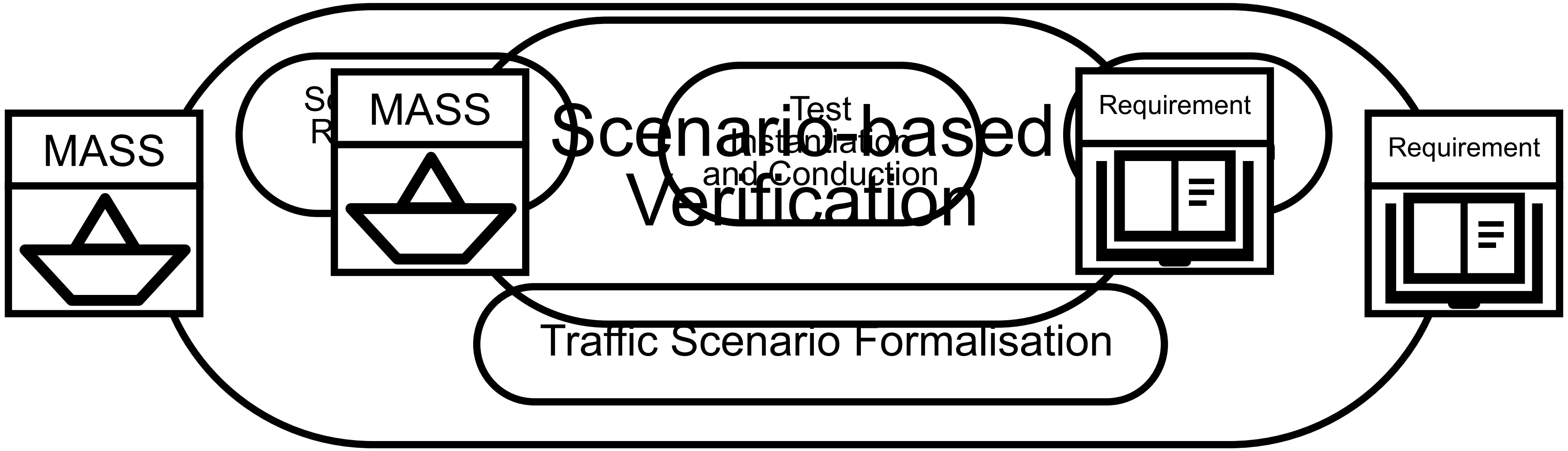
- For development, certification and operation of MASS it has to be ensured that they are sufficiently safe
- In particular a reliable and traceable safety argument is needed, showing that they adhere to rules and requirements



Scenario-based Verification

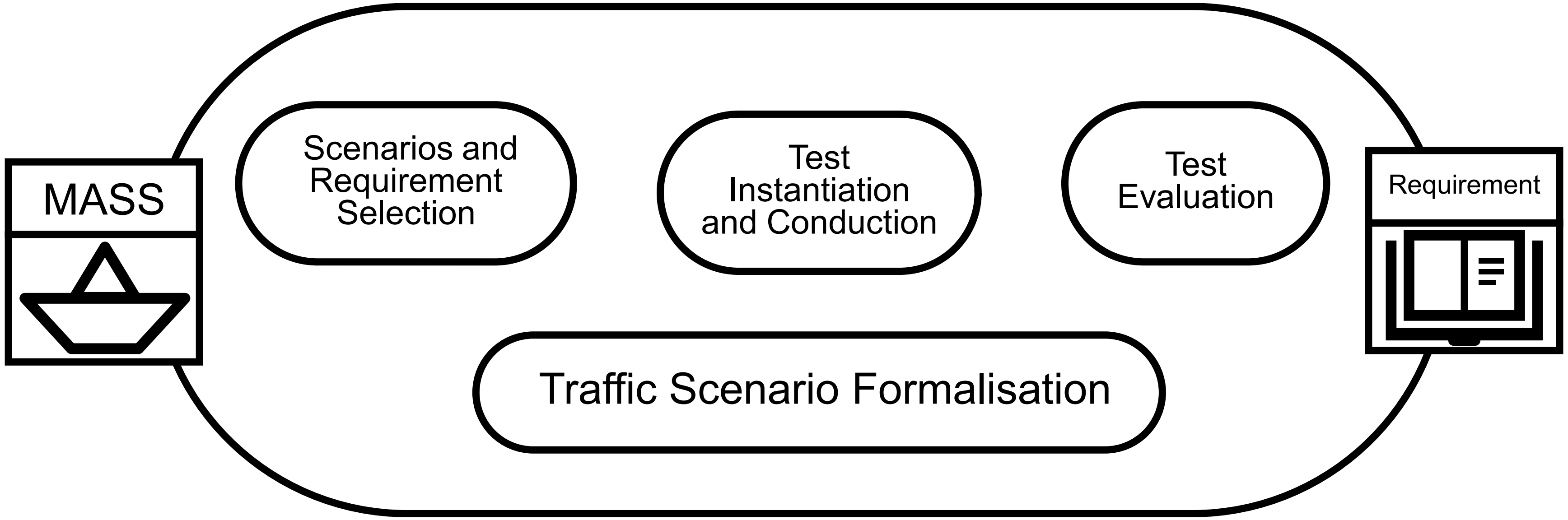
- Approach for safety argumentation from the automotive domain
- Based on testing vehicles in carefully selected operating scenarios
- Important steps include
    - ➢ Selection of relevant test scenarios and derivation of corresponding requirements
    - ➢ Generation of concrete test scenarios and test conduction
    - ➢ Evaluation of test runs for satisfaction or violation of requirements

➢All of these necessitate formal specification of traffic scenarios

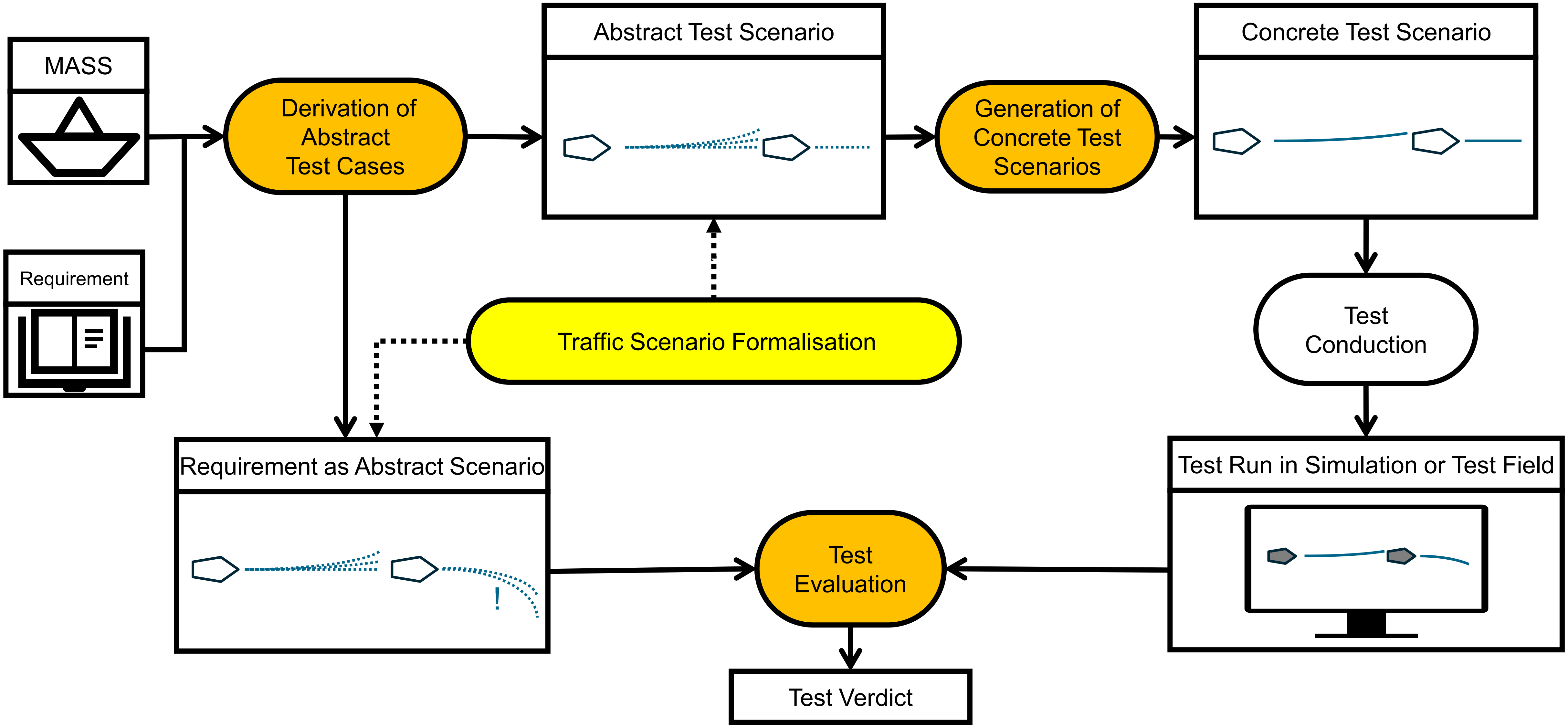

MASS
Sc
R
MASS
Scenario-based Verification
Test Instantiation and Conduction
Requirement
Requirement
Traffic Scenario Formalisation

Contribution

Transfer important steps of scenario-based verification to the maritime domain:

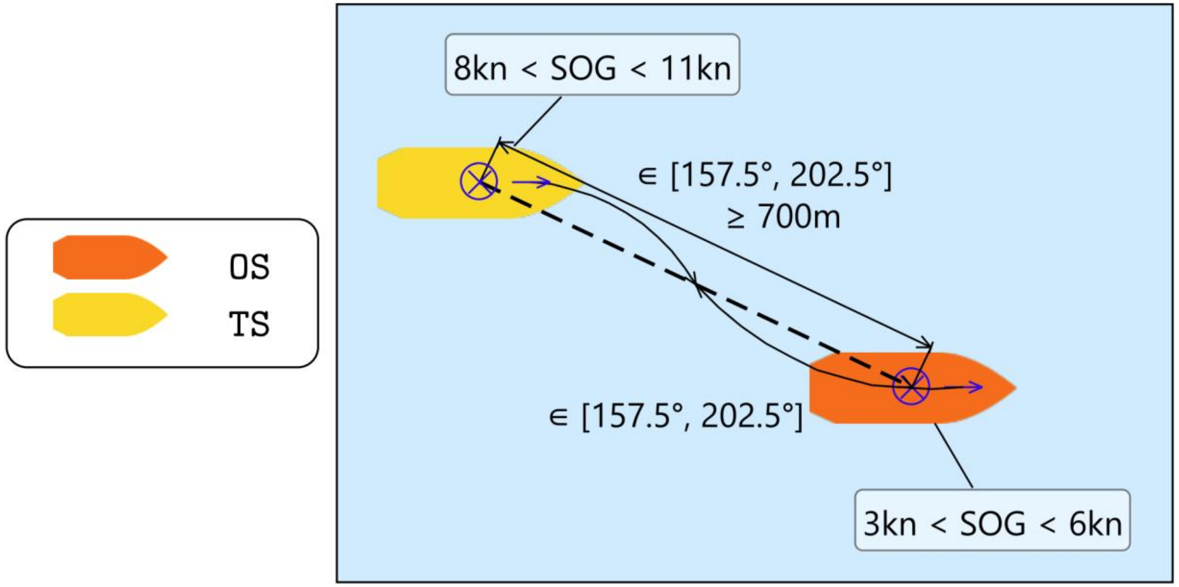

MASS
Scenarios and Requirement Selection
Test Instantiation and Conduction
Test Evaluation
Requirement
Traffic Scenario Formalisation

Scenario-based Testing – Simplified Example


MASS
Requirement
Derivation of Abstract Test Cases
Abstract Test Scenario
Generation of Concrete Test Scenarios
Concrete Test Scenario
Traffic Scenario Formalisation
Test Conduction
Requirement as Abstract Scenario
!
Test Evaluation
Test Run in Simulation or Test Field
Test Verdict

Traffic Scenario Formalisation
Traffic Sequence Charts

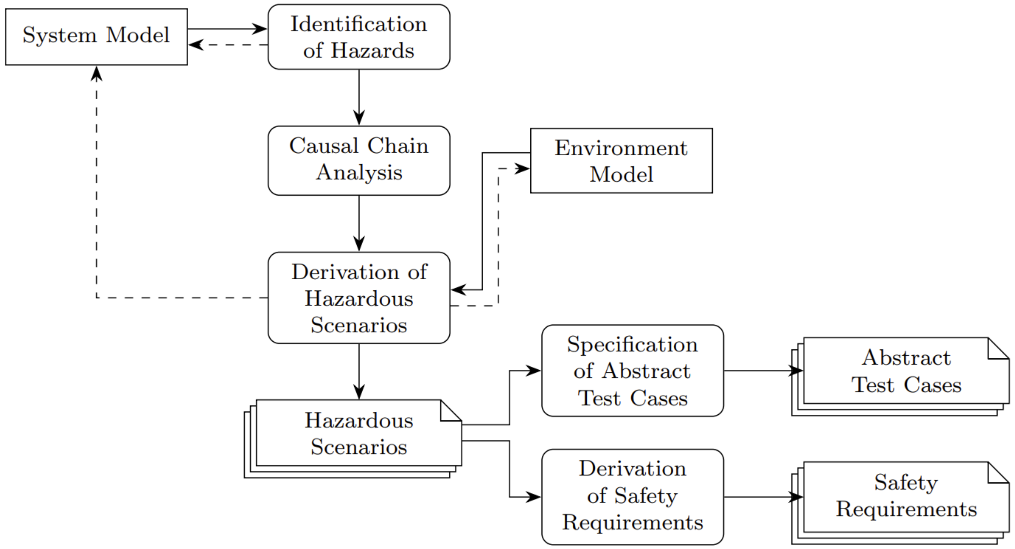
- Formal visual language for abstract traffic scenarios
  - Machine and Human readable
- Focus on graphical specification of spatio-temporal properties



Derivation of Abstract Test Cases

Identification of Hazard

Idea: Scenarios associated with an increased risk are considered to be particularly relevant for scenario-based testing

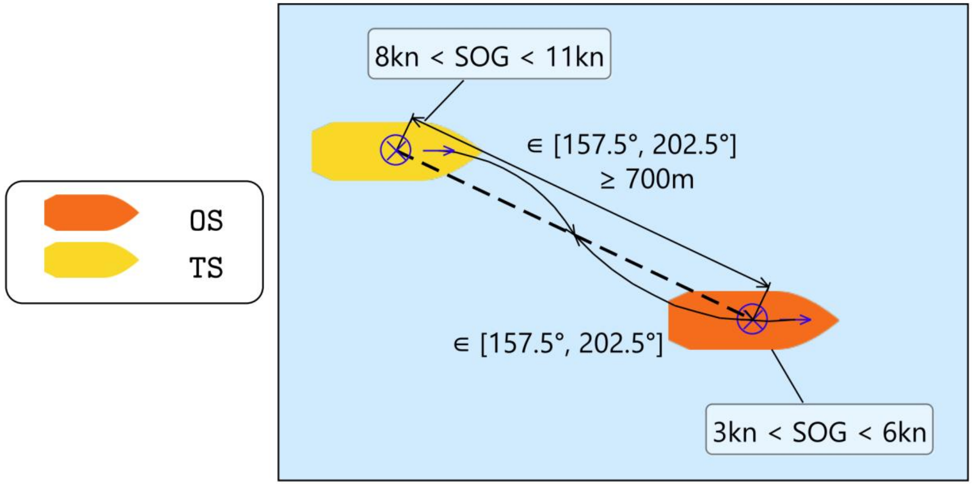


System Model
Identification of Hazards
Causal Chain Analysis
Environment Model
Derivation of Hazardous Scenarios
Hazardous Scenarios
Specification of Abstract Test Cases
Abstract Test Cases
Derivation of Safety Requirements
Safety Requirements

Definition of Basic Scenarios

Starting Point: Set of basic scenarios that covers the target operational domain

- Vary and refine basic scenarios to identify hazardous scenarios

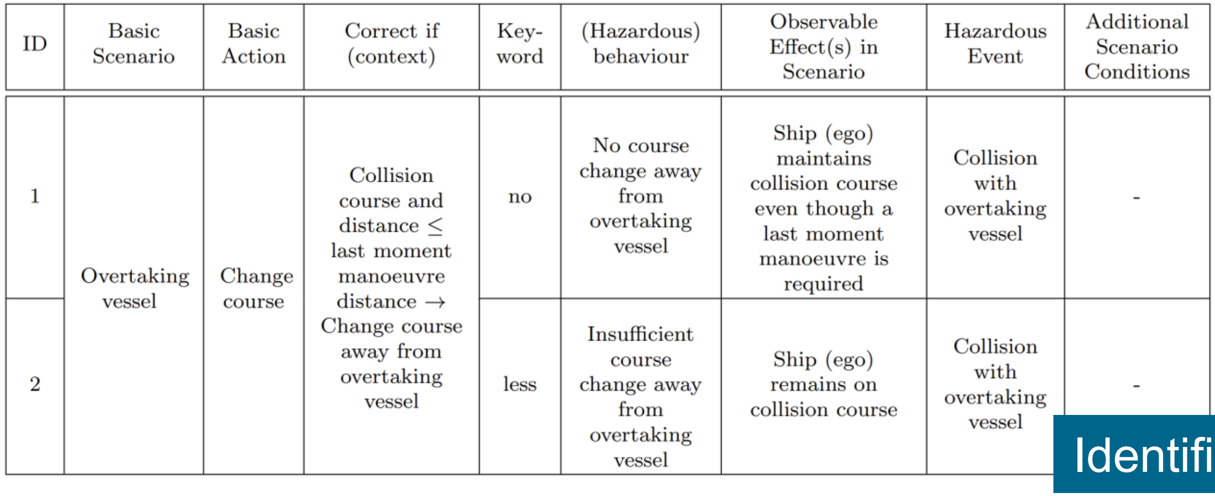


Derivation of Abstract Test Cases

Identification of Hazards

Identification of hazardous behaviour on vehicle level

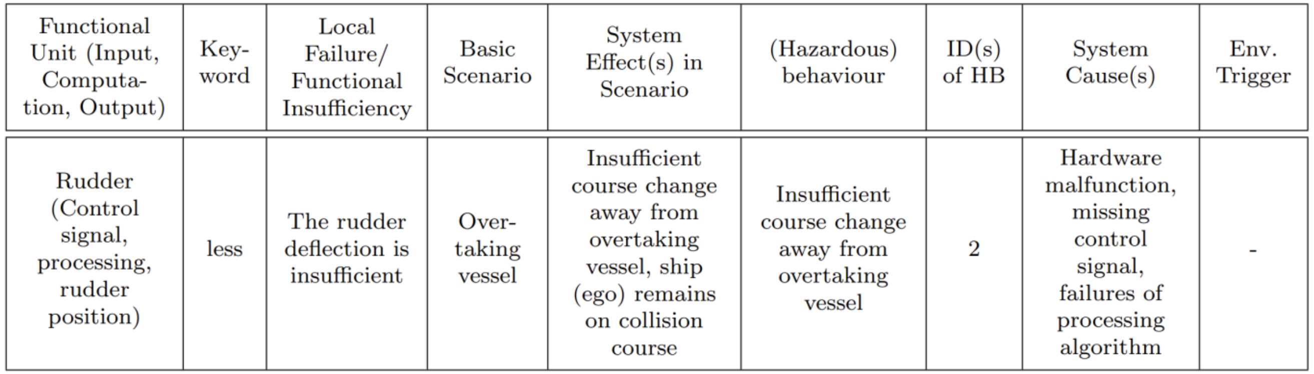
Keyword-based brainstorming approach →Top-down analysis



ID	Basic Scenario	Basic Action	Correct if (context)	Key-word	(Hazardous) behaviour	Observable Effect(s) in Scenario	Hazardous Event	Additional Scenario Conditions
1	Overtaking vessel	Change course	Collision course and distance $\leq$ last moment manoeuvre distance → Change course away from overtaking vessel	no	No course change away from overtaking vessel	Ship (ego) maintains collision course even though a last moment manoeuvre is required	Collision with overtaking vessel	-
2				less	Insufficient course change away from overtaking vessel	Ship (ego) remains on collision course	Collision with overtaking vessel	-

Identification of local failures and functional insufficiencies

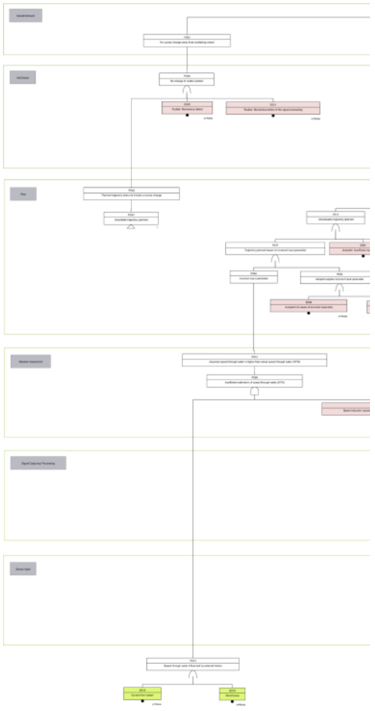
Keyword-based brainstorming approach → Bottom-up analysis

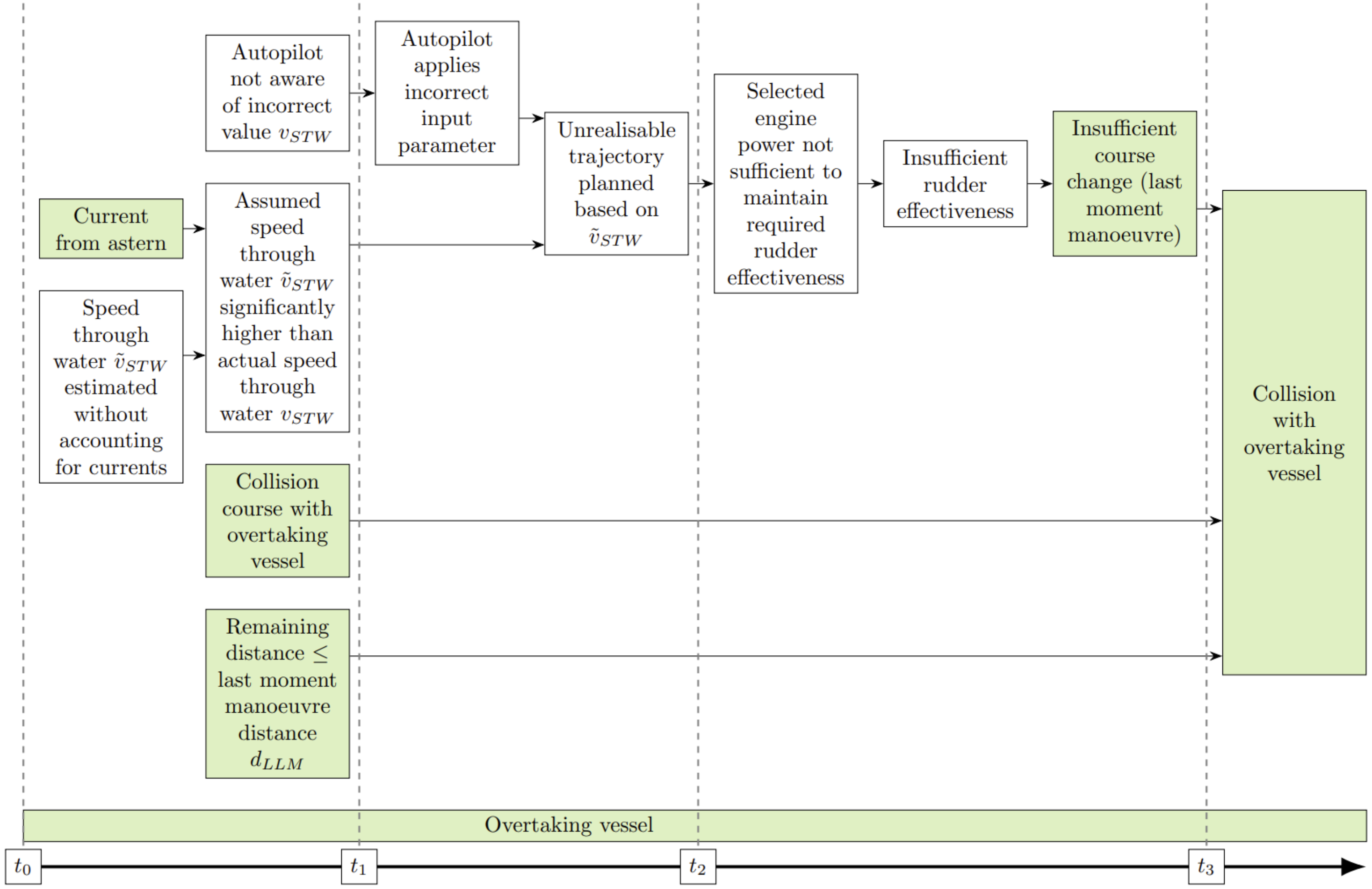


Functional Unit (Input, Computation, Output)	Key-word	Local Failure/ Functional Insufficiency	Basic Scenario	System Effect(s) in Scenario	(Hazardous) behaviour	ID(s) of HB	System Cause(s)	Env. Trigger
Rudder (Control signal, processing, rudder position)	less	The rudder deflection is insufficient	Overtaking vessel	Insufficient course change away from overtaking vessel, ship (ego) remains on collision course	Insufficient course change away from overtaking vessel	2	Hardware malfunction, missing control signal, failures of processing algorithm	-

Derivation of Abstract Test Cases
Causal Chain Analysis

- Environmental fault tree analysis
- Analysis of minimal branch sets of the environmental fault trees
- Assignment of discrete time steps





Autopilot not aware of incorrect value v_{STW}

Autopilot applies incorrect input parameter

Current from astern

Assumed speed through water $\tilde{v}_{STW}$ significantly higher than actual speed through water v_{STW}

Speed through water $\tilde{v}_{STW}$ estimated without accounting for currents

Unrealisable trajectory planned based on $\tilde{v}_{STW}$

Selected engine power not sufficient to maintain required rudder effectiveness

Insufficient rudder effectiveness

Insufficient course change (last moment manoeuvre)

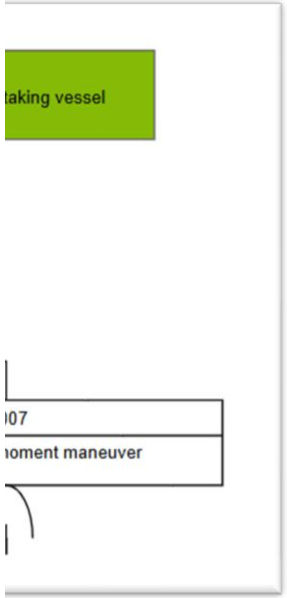
Collision course with overtaking vessel

Remaining distance $\leq$ last moment manoeuvre distance d_{LLM}

Collision with overtaking vessel

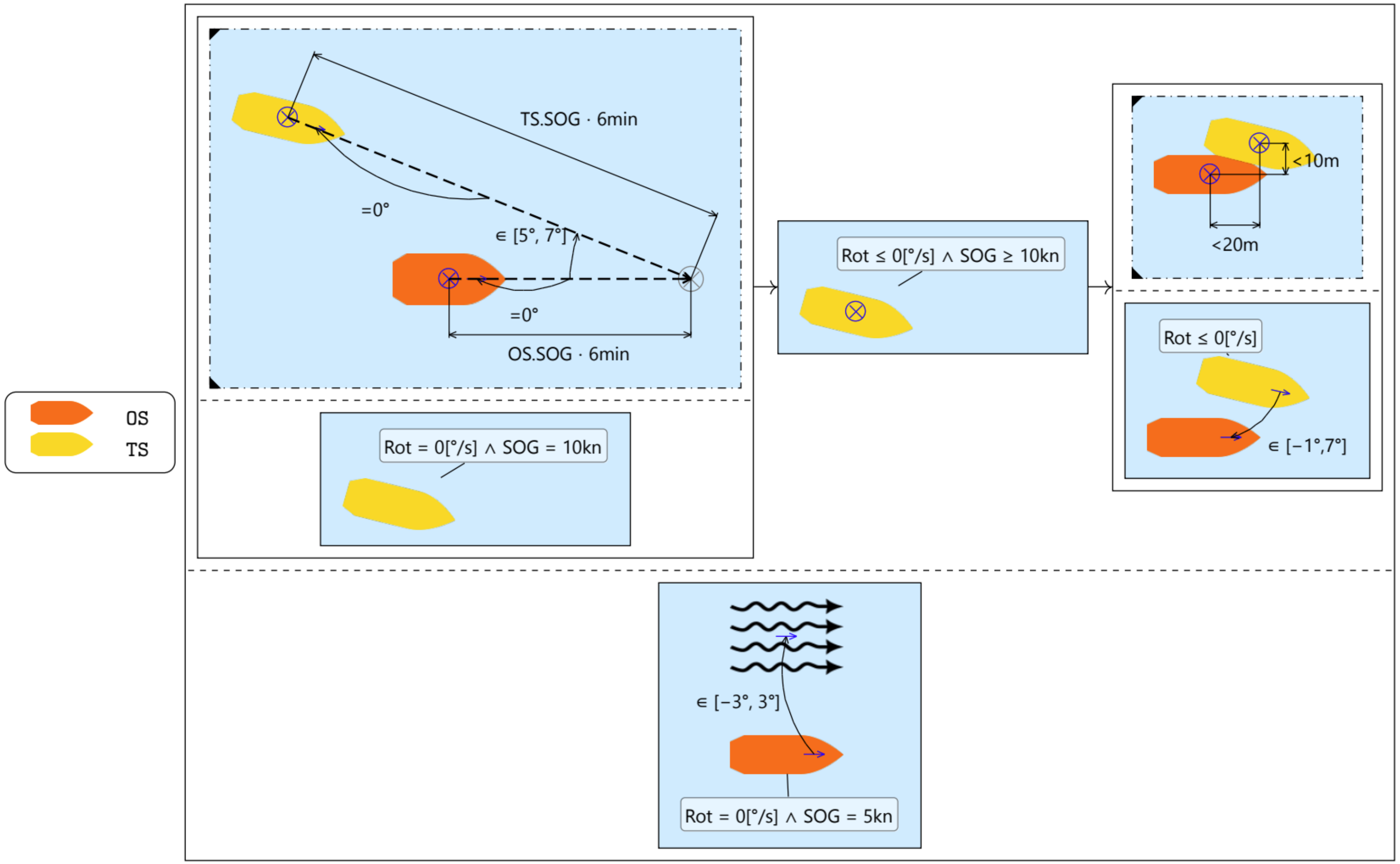
Overtaking vessel

t_0 t_1 t_2 t_3



Derivation of Abstract Test Cases

Specification of Abstract Test Cases and Safety Requirements



+

Requirements

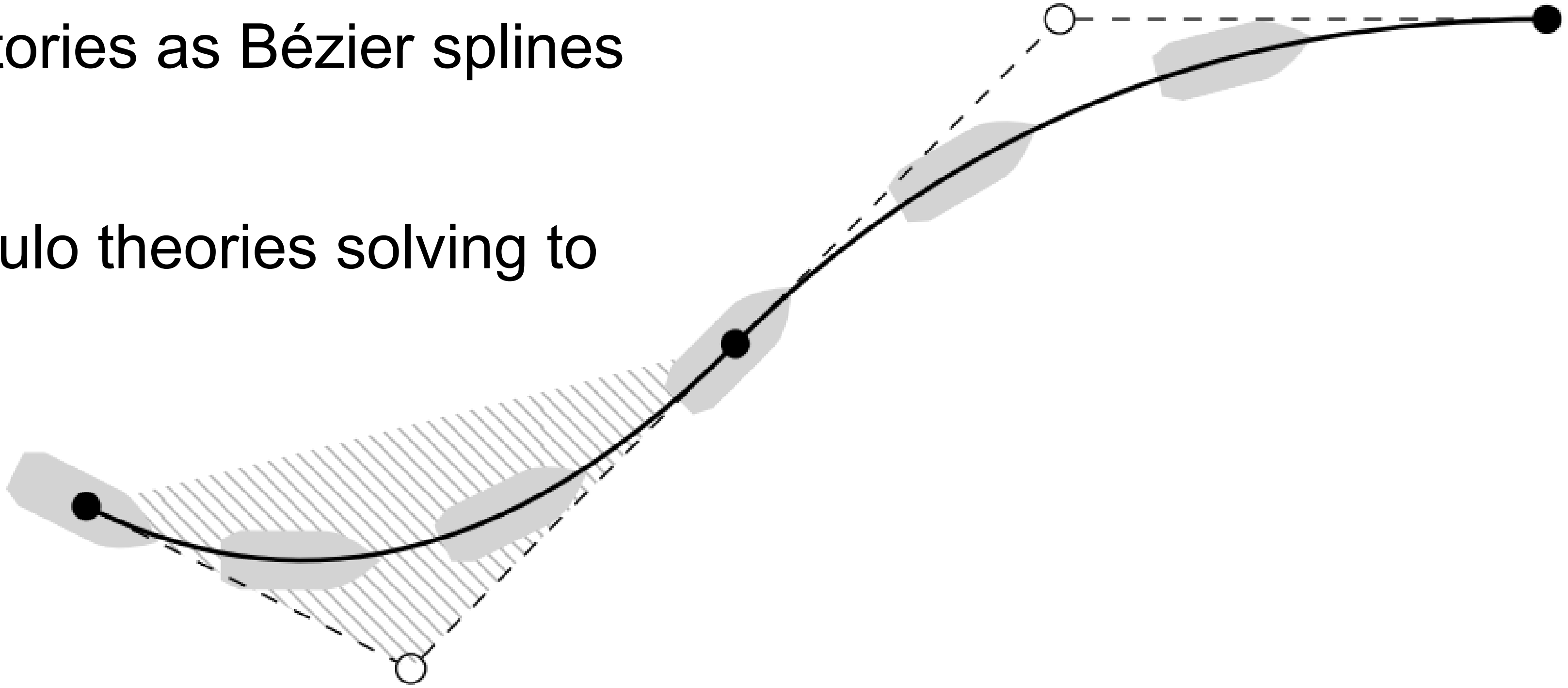
1. The vessel must avoid a collision and adhere to the COLREG rules in the process.
2. …

Generation of Concrete Test Scenarios

Using MTSCs

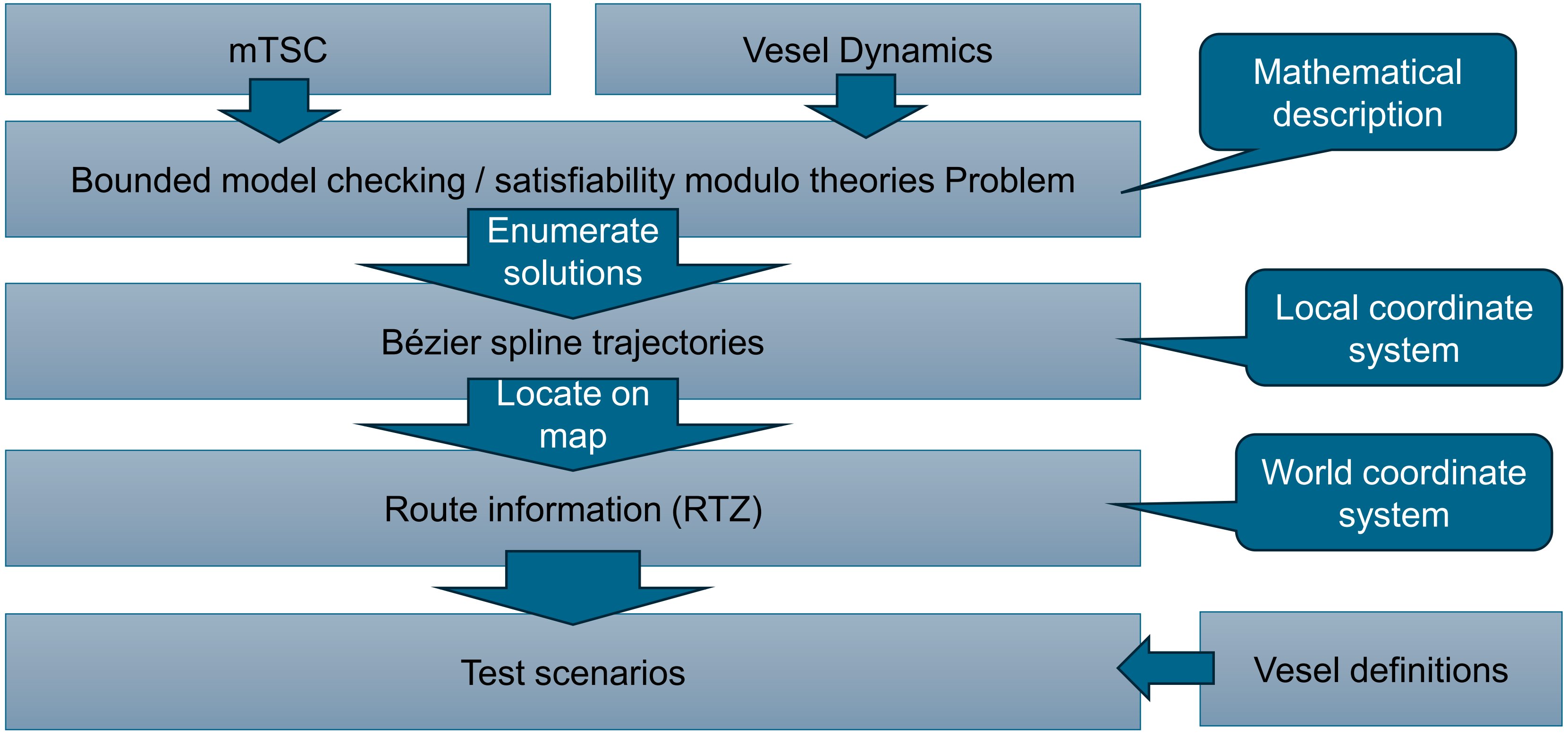
Idea: Encode mTSCs as linear equations and solve them

- Exploit mathematical semantics of mTSCs
- Simplify vessel dynamics
- Encode vessel trajectories as Bézier splines
- Discretize directions
- Use satisfiability modulo theories solving to enumerate solutions



Generation of Concrete Test Scenarios

Solution for our Example



mTSC

Vesel Dynamics

Bounded model checking / satisfiability modulo theories Problem

Mathematical description

Enumerate solutions

Bézier spline trajectories

Local coordinate system

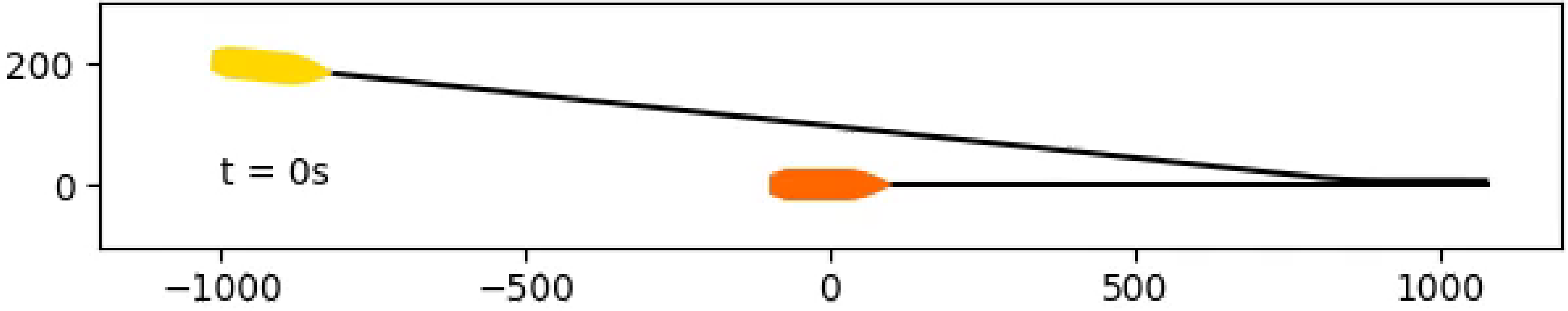
Locate on map

Route information (RTZ)

World coordinate system

Test scenarios

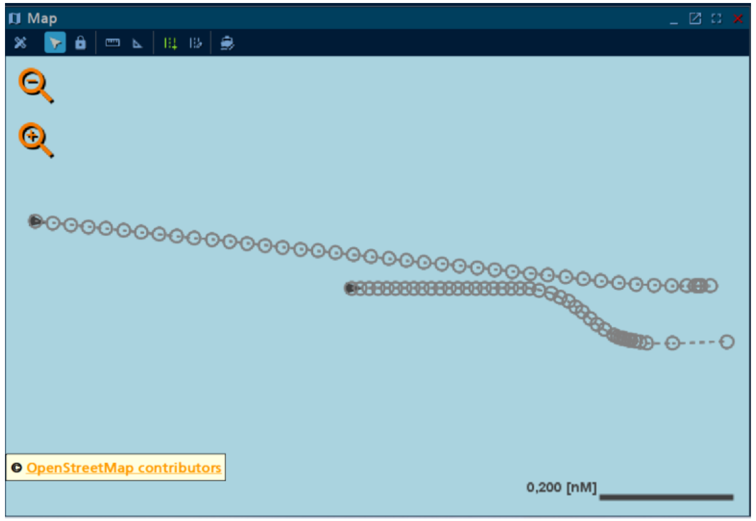
Vesel definitions



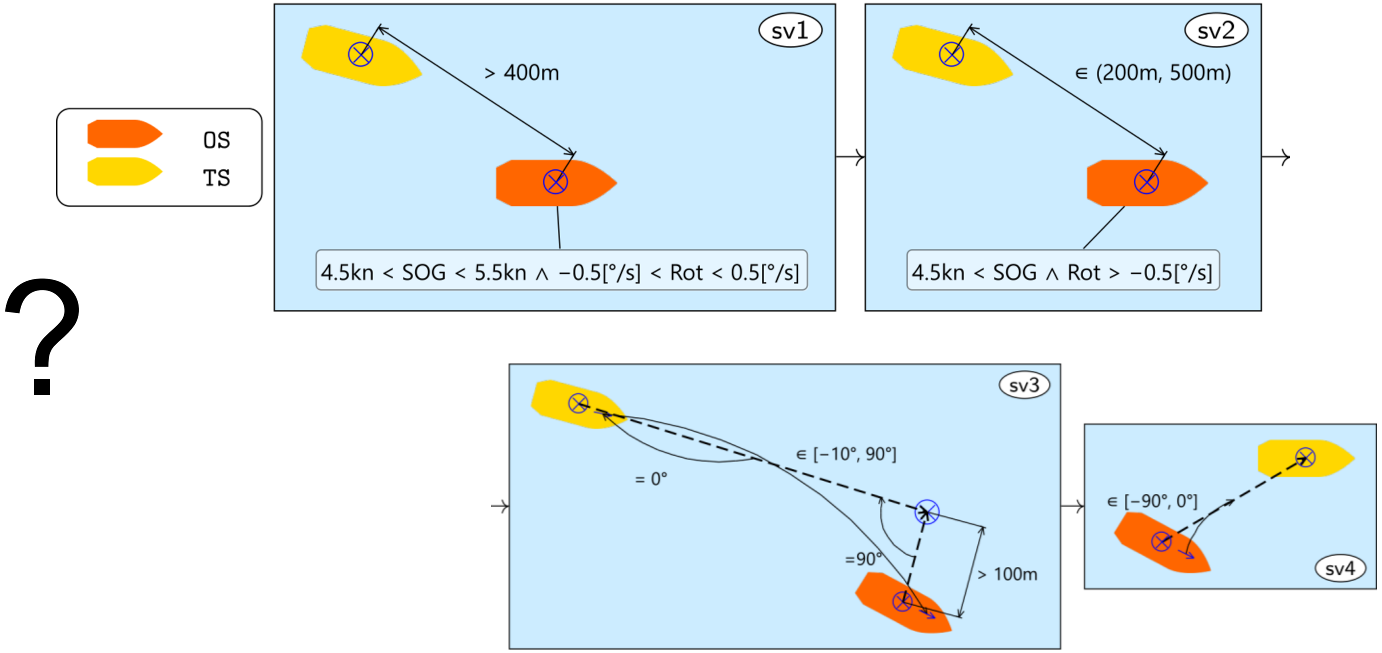
Test Evaluation

Given a test run we need to evaluate pass or fail

➢Determine whether it adheres to corresponding requirements



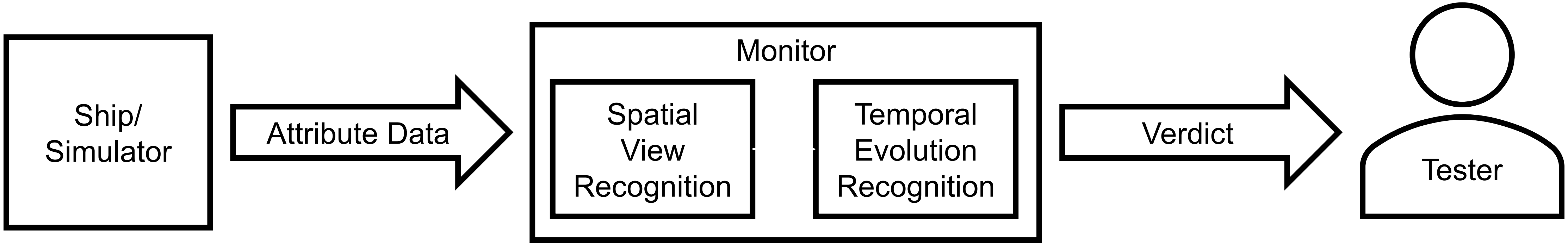
?


OS
TS
sv1
> 400m
4.5kn < SOG < 5.5kn ∧ −0.5[°/s] < Rot < 0.5[°/s]
sv2
∈ (200m, 500m)
4.5kn < SOG ∧ Rot > −0.5[°/s]
sv3
∈ [−10°, 90°]
= 0°
=90°
> 100m
sv4
∈ [−90°, 0°]

Test Evaluation
TSC Monitoring

We employ TSC monitoring:

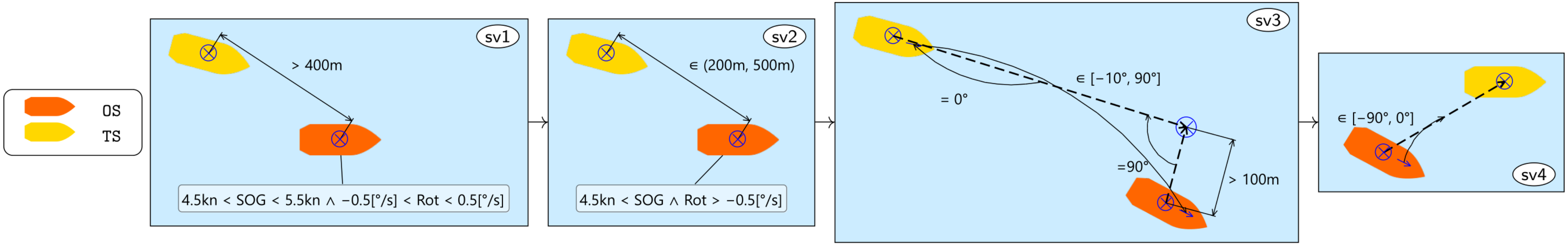
- Formalize requirement as a TSC
- Construct an online monitor
  - ➢ During test drive, decide whether it satisfies or violates the TSC



Test Evaluation

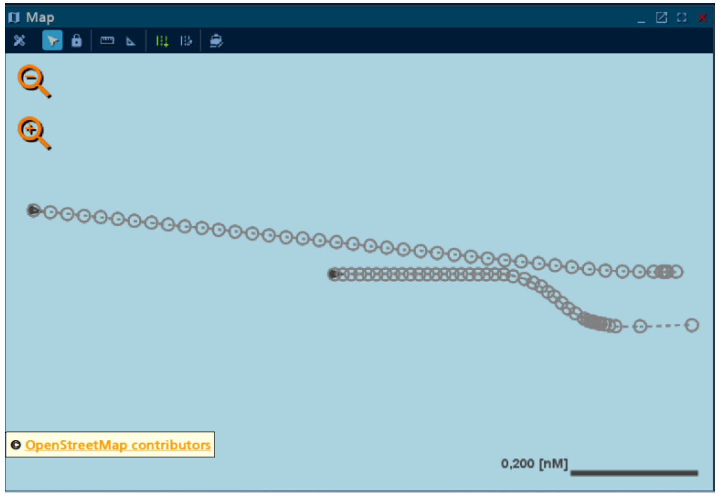
Example

Requirement (following COLREG) formalized as a TSC:

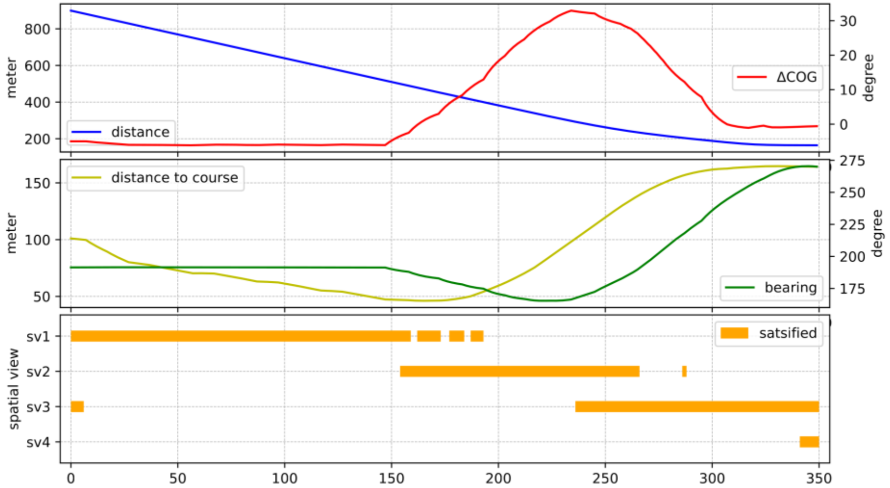


OS
TS
sv1
> 400m
4.5kn < SOG < 5.5kn ∧ −0.5[°/s] < Rot < 0.5[°/s]
sv2
∈ (200m, 500m)
4.5kn < SOG ∧ Rot > −0.5[°/s]
sv3
∈ [−10°, 90°]
= 0°
=90°
> 100m
sv4
∈ [−90°, 0°]

Test Run:



Monitor output:



Conclusion

We transfer important steps of scenario-based verification
to the maritime domain:

- ➢Formal specification of abstract traffic scenarios
- ➢Selection of relevant test scenarios and derivation of corresponding requirements
- ➢Generation of concrete test scenarios
- ➢Evaluation of test runs for satisfaction or violation of requirements