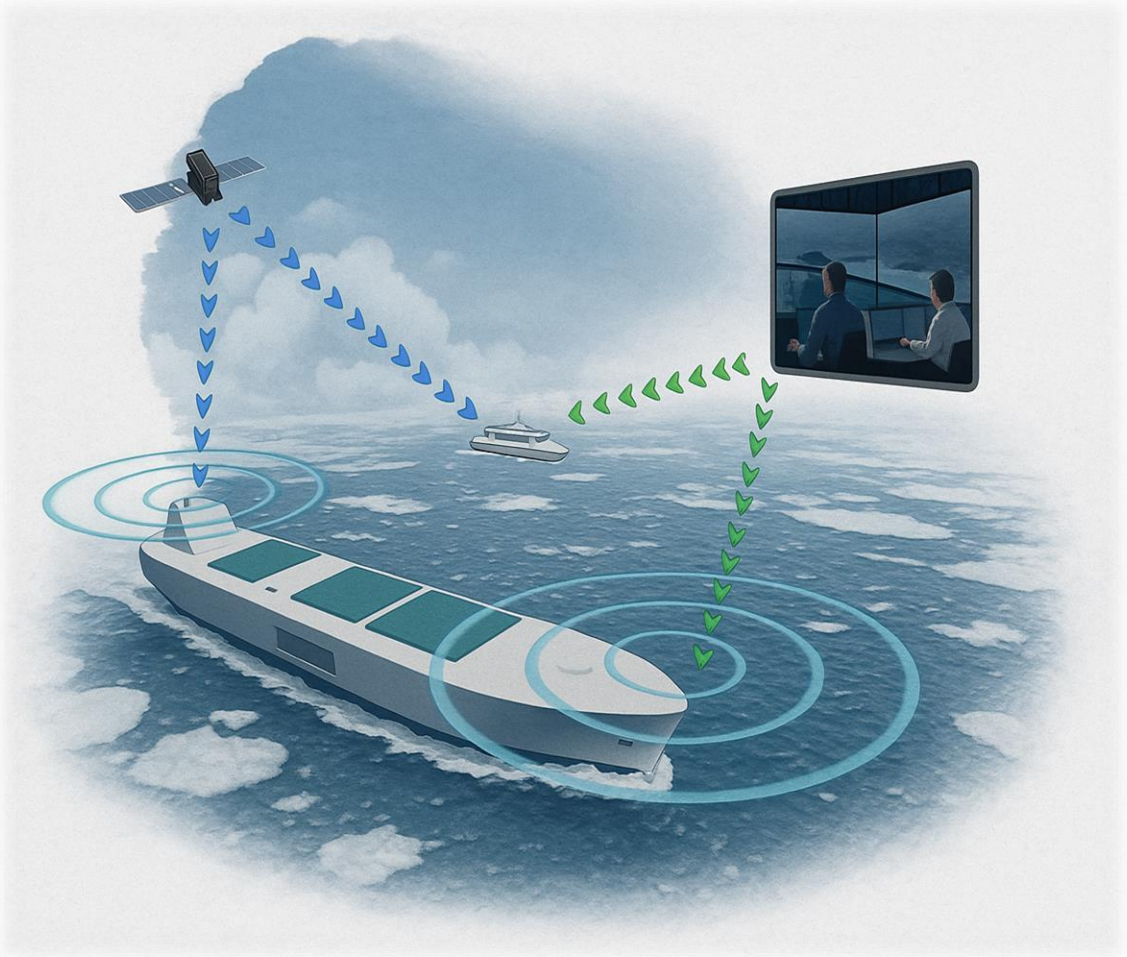
A SysML-Based Hazard Analysis: A Case Study of Autonomous Navigation Systems in Winter Conditions

SEMSS Group, Aalto University

Raheleh Farokhi

Sunil Basnet

Osiris A. Valdez Banda



Komarec 2025
29-30 October, Kotka, Finland

Aalto University
School of Engineering

Contents

Introduction & objectives

- Rapid advancements in MASS are increasing system complexity.
- More complexity related to navigation of MASS in winter conditions.

Challenge: Ensuring safety in complex, high-risk, and dynamic maritime environments

Complex Interactions
- Software ↔ Hardware ↔ Human ↔ Environment
- Timing-critical control actions
- Vulnerability to unsafe interactions or missed responses

Maritime autonomous surface ships (MASS)

Winter Navigation Conditions

Introduction & objectives

STPA
(System Theoretic Process Analysis)

offers interaction-focused hazard identification

SysML
(Systems modelling language)

Supports structured, model-based systems design

Goal of this study:

To integrate SysML and STPA for more Scalable, traceable, and dynamic hazard Analysis in ANS

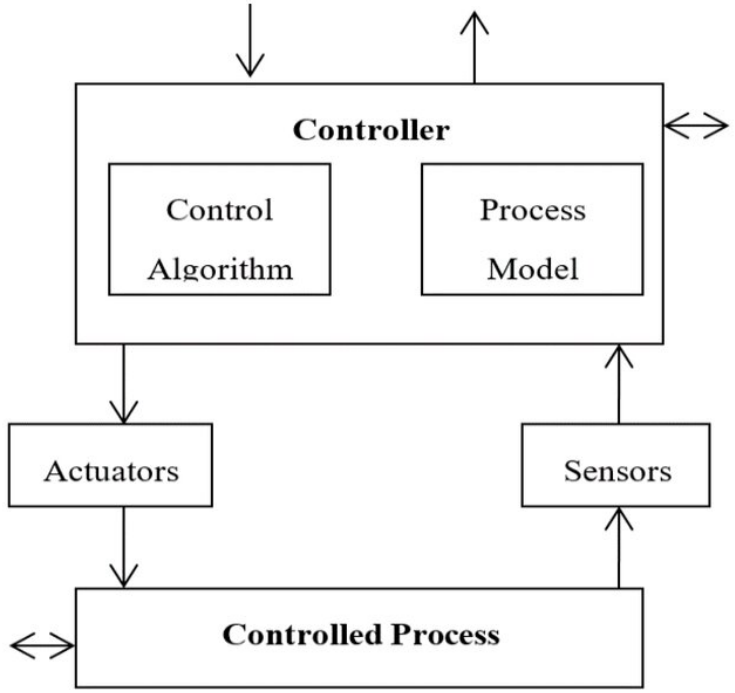
Introduction & objectives

STPA

STPA

A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident/loss

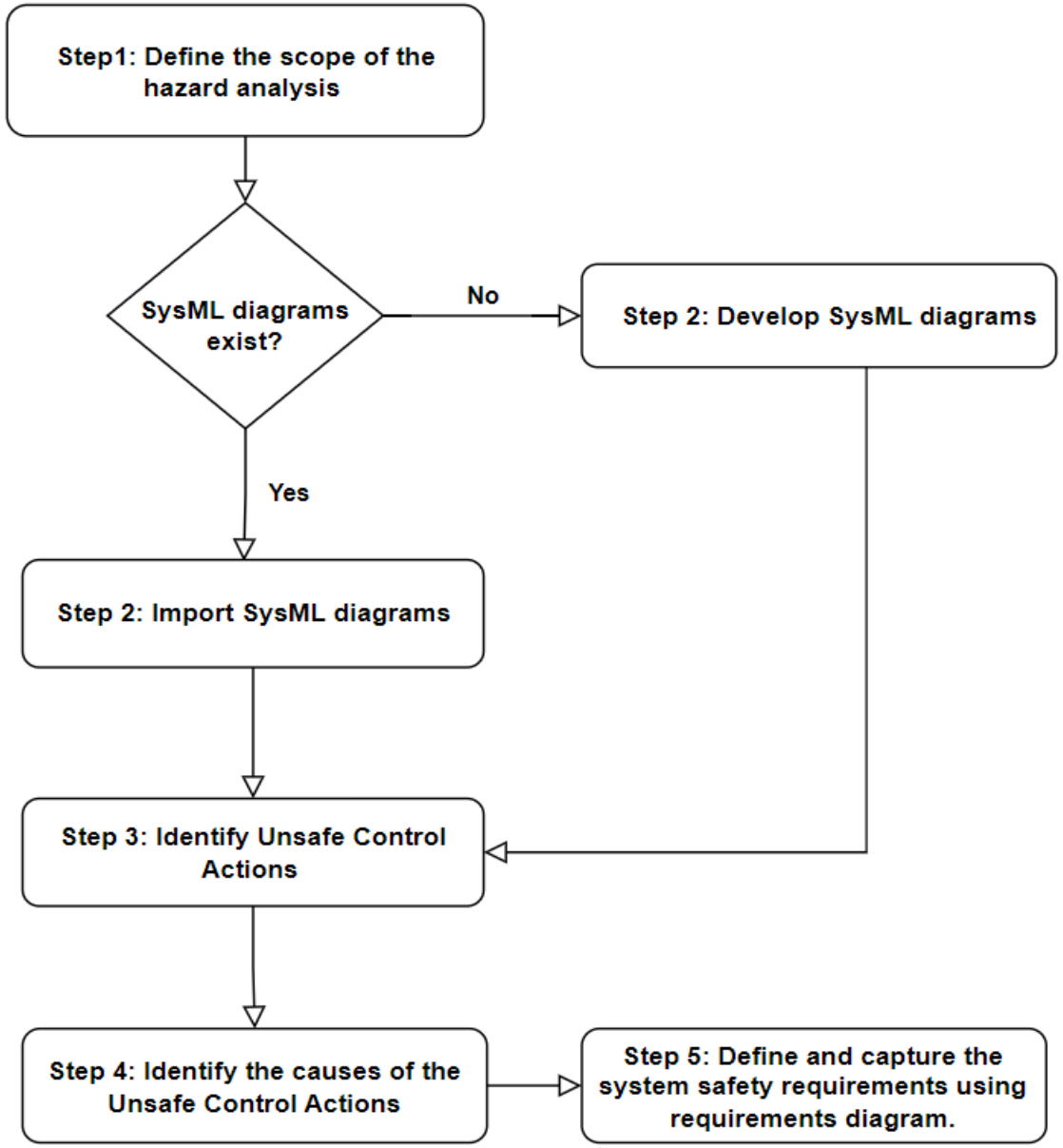
Hazards can emerge from the actions of different controllers in a system as well as the interaction of the different parts of the system.



Control Loop Overview
(Karatzas and Chassiakos 2020)

SysML-based STPA process

The overall framework for SysML-based STPA hazard analysis.



Results

Step 1

Scope definition

Table 1: The losses related to ANS

ID	Losses
L1	Loss of life
L2	Injury to people
L3	Loss of ship
L4	Damage to ship
L5	Loss of mission
L6	Loss of cargo

Table 2: System-level hazards leading to losses

ID	System-level hazards	Related losses
H1	Ship fails to detect and respond to environmental obstacles in time.	L1, L2, L3, L4, L5, L6
H2	Ship is unable to adapt or perform accurate route adjustments	L3, L4, L5, L6

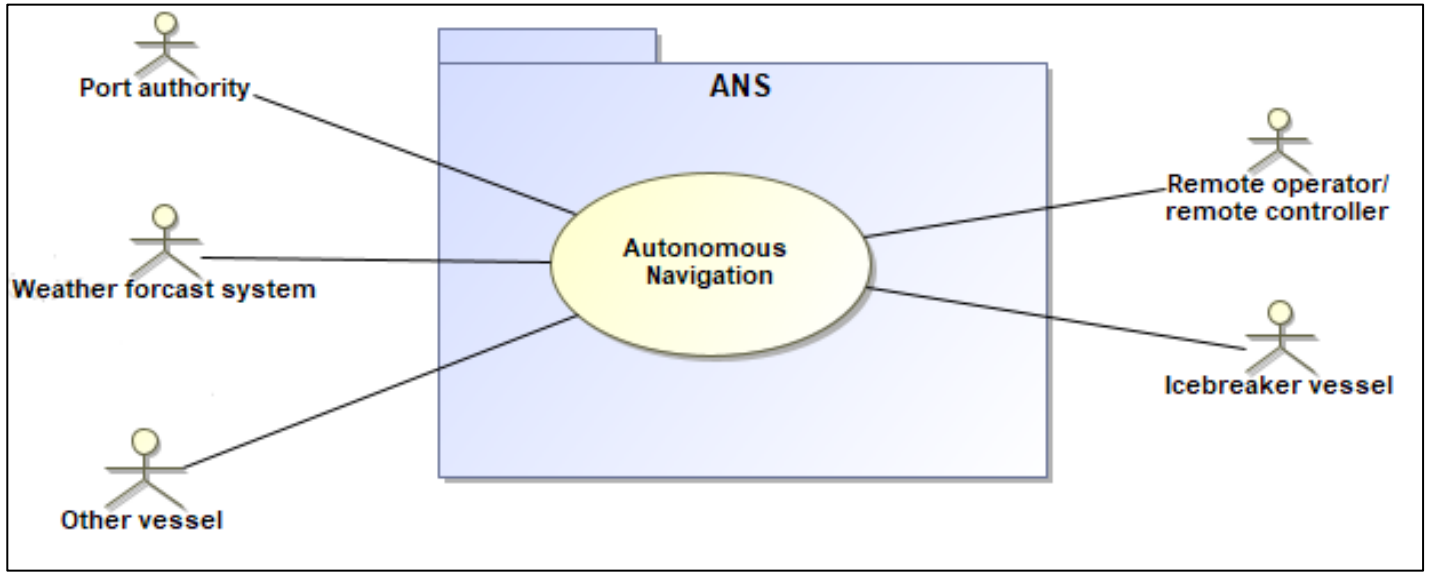
Table 3: Safety constraints for preventing system-level hazards

ID	Safety constraints	Related hazards
SC1	The ship must ensure continuous detection and timely response to environmental obstacles.	H1
SC2	The system must provide accurate and real-time route adjustments.	H2

Results

Step 2

Develop/Import SysML diagrams of the system



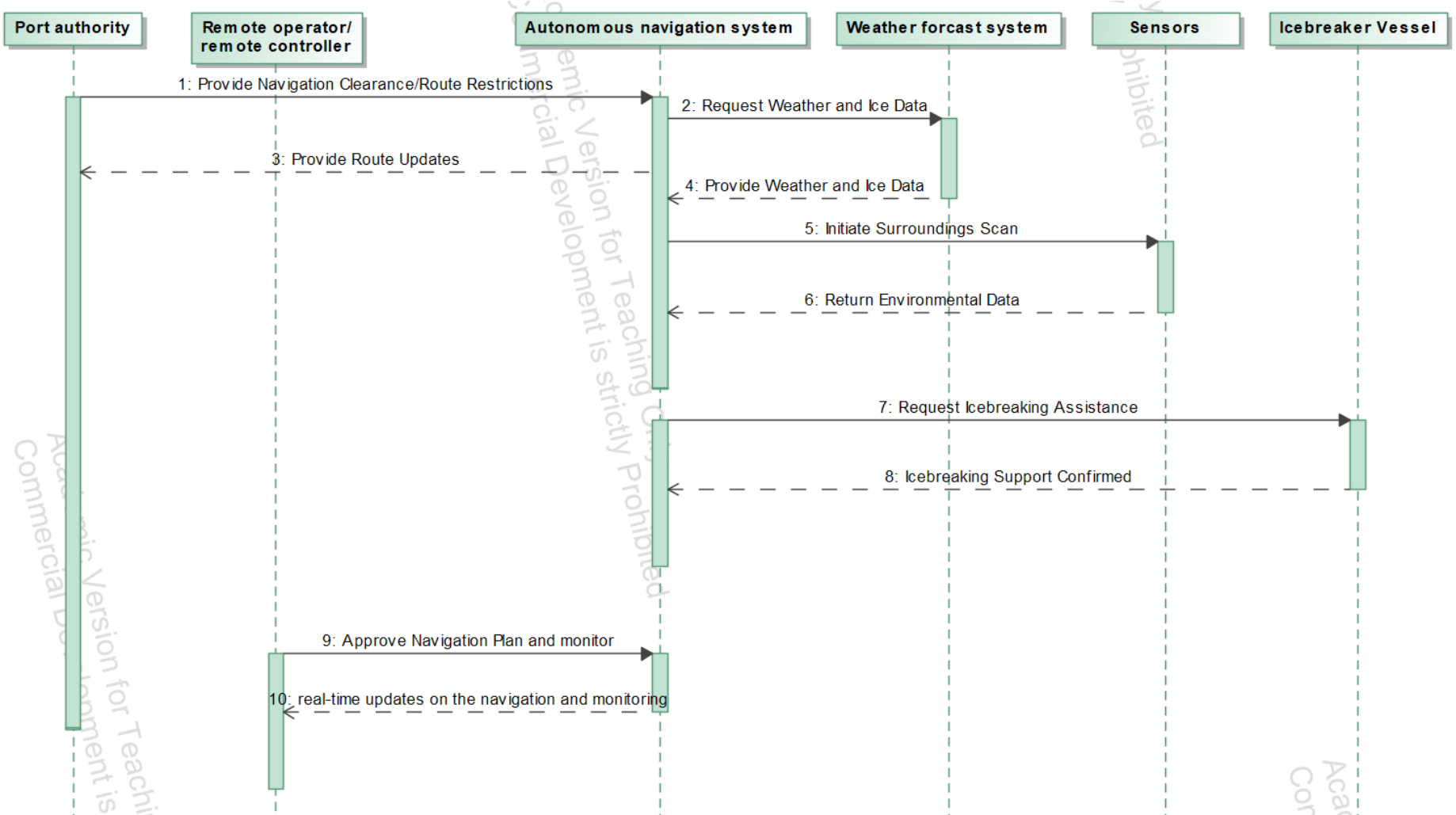
SysML use case diagram for autonomous navigation in winter conditions

Results

Step 2

Develop/Import SysML diagrams of the system

SysML sequence diagram to show control actions and feedback in STPA



Results

Step 3 Identifying Unsafe Control Actions (UCAs)

Table 4: UCAs and related consequences

Controller	**ANS**
Control actions	Initiate surrounding scan
UCAs	
Not providing	UCA-1: ANS fails to request the sensors to scan for data
Providing causing hazards	UCA-2: ANS requests the sensors to scan for data during inappropriate conditions
Providing too early, late, out of order	UCA-3: ANS requests the sensors to scan for data too late or in the wrong order
Stopped too soon, applied too long	UCA-4: NA

Table 5: Scenarios leading to UCA-1

Scenario ID	**Scenarios leading to UCA-1**
SC1	ANS fails to request for the sensors to scan for data due to software errors.
SC2	ANS fails to request for the sensors to scan for data due to control logic errors.
SC3	ANS fails to request to scan for data due to a Power supply failure in the sensors.

Results

Step 4 Identifying the causes (i.e., loss scenarios) of the UCAs

Table 5: Scenarios leading to UCA-1

Scenario ID	Scenarios leading to UCA-1
SC1	ANS fails to request for the sensors to scan for data due to software errors.
SC2	ANS fails to request for the sensors to scan for data due to control logic errors.
SC3	ANS fails to request to scan for data due to a Power supply failure in the sensors.

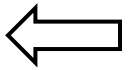


Table 6: Causal factors

Scenario ID	Causal factors
SC1	Software errors
SC2	Control logic errors
SC3	Power supply failure

Results

Step 5 Define the system safety requirements

Table 4: UCAs and related consequences

Controller	**ANS**
Control actions	Initiate surrounding scan
UCAs	
Not providing	UCA-1: ANS fails to request the sensors to scan for data
Providing causing hazards	UCA-2: ANS requests the sensors to scan for data during inappropriate conditions
Providing too early, late, out of order	UCA-3: ANS requests the sensors to scan for data too late or in the wrong order
Stopped too soon, applied too long	UCA-4: NA

Table 7: Safety Requirements to Mitigate UCA-1 to UCA-4

ID	**Safety requirements**
SR1	ANS must verify that sensors are operational before requesting scans.
SR2	ANS must request scans only under suitable environmental conditions.
SR3	ANS must trigger scans in the correct sequence and timing.
SR4	ANS must adjust scanning based on real-time feedback.

Table 8: STPA vs. SysML-STPA: Key Differences

Aspect	Traditional STPA	SysML-STPA (This Study)
System Representation	Single control structure diagram	Multiple SysML diagrams (Sequence, Requirements)
Interaction Modeling	Static	Dynamic (Sequence diagrams capture timing and order)
Traceability	Limited	High-loss scenarios and UCAs linked across diagrams
Clarity in Complex Systems	Hard to manage	Modular and scalable for complex architectures
Timing & Feedback Analysis	Implicit or missed	Explicit (shown clearly in sequence diagrams)
Requirement Integration	External to the process	Captured directly in SysML requirements diagrams
Support for Targeted Safety Interventions	General	Precise (shows the exact point of failure or delay)

Thank you!

Any questions?

Aalto University
School of Engineering