Norwegian University of
Science and Technology

Safety Verification for Autonomous Ships

ESWC2018

02.11.2018

Børge Rokseth, Odd Ivar Haugen & Ingrid Bouwer Utne

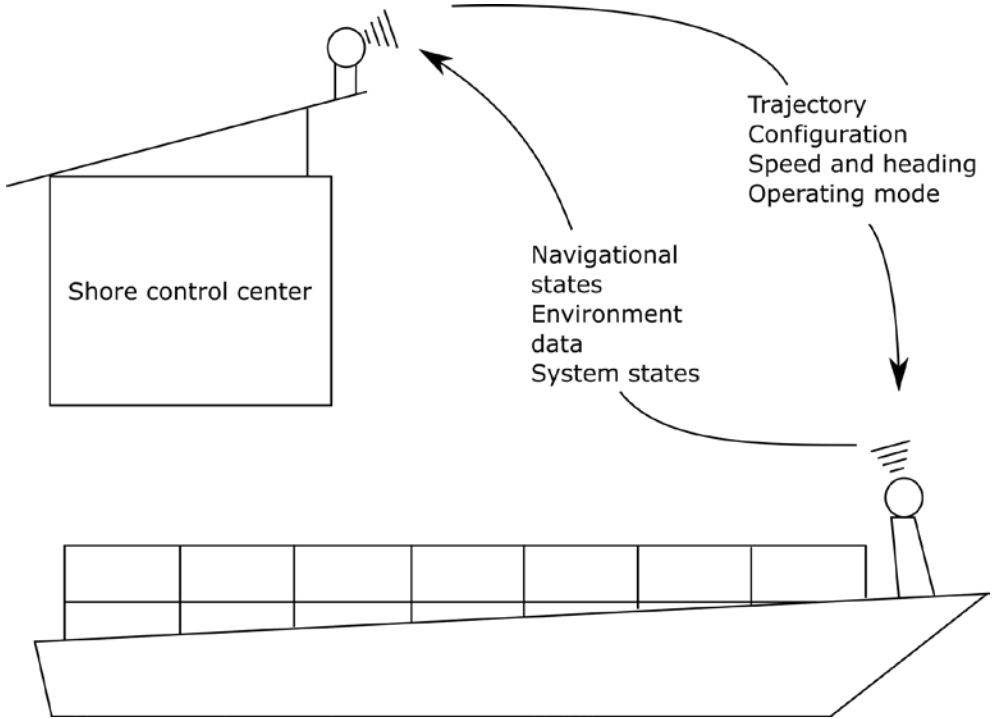
Objectives of the presented work

Exploring the possibility of using STPA as a foundation for safety verification

Identifying design requirements and necessary functionality for safety for autonomous ships at an early stage in the concept development

Gaining insight into how autonomous ship functionality should be designed to make it possible to gain sufficient levels of confidence

What are autonomous ships?



What are autonomous ships?

Plan journey
- Make tentative trajectory
- Determine system settings for each leg

Update plan to accommodate changing conditions and real-time data
- Change, or deviate from, trajectory
- Reconfigure power and propulsion
- Deviate from planned operating modes

SCC

ASS

Remote control control mode

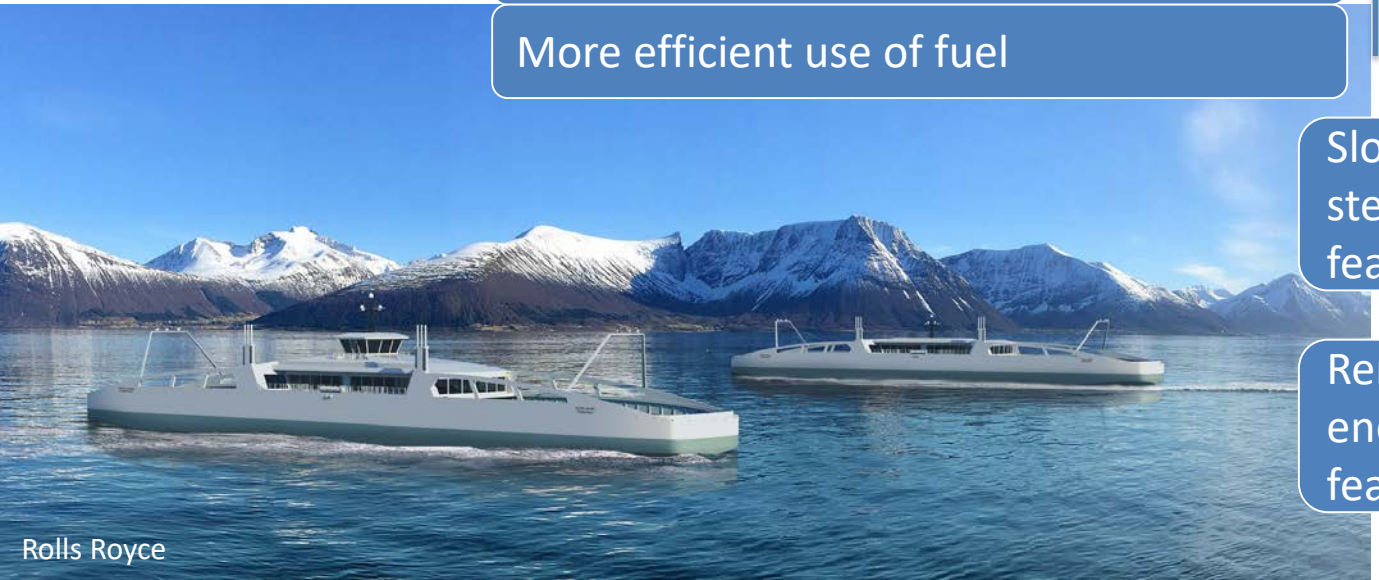
Indirect remote control mode

Autonomous control mode

Why autonomous ships?

Potential benefits

- More efficient use of space in ship design
- More efficient use of crew and their skill
- More efficient use of fuel



Rolls Royce

- Slow steaming feasible?
  - Renewable energy feasible?
- Many smaller ferries?
  - Less waiting

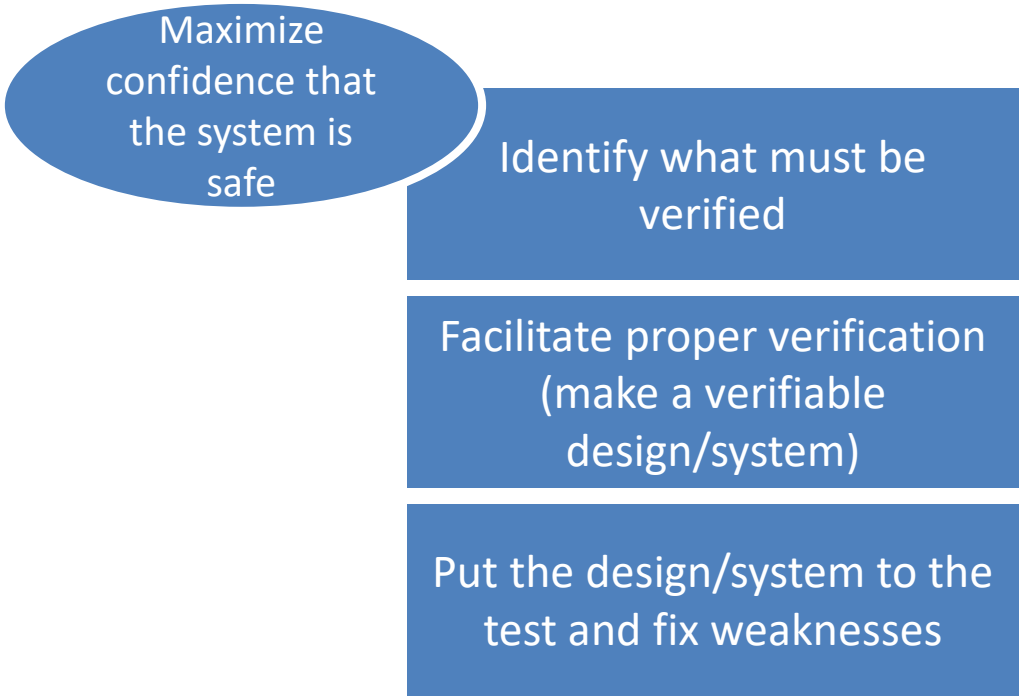
The verification challenge

The safety verification challenge:

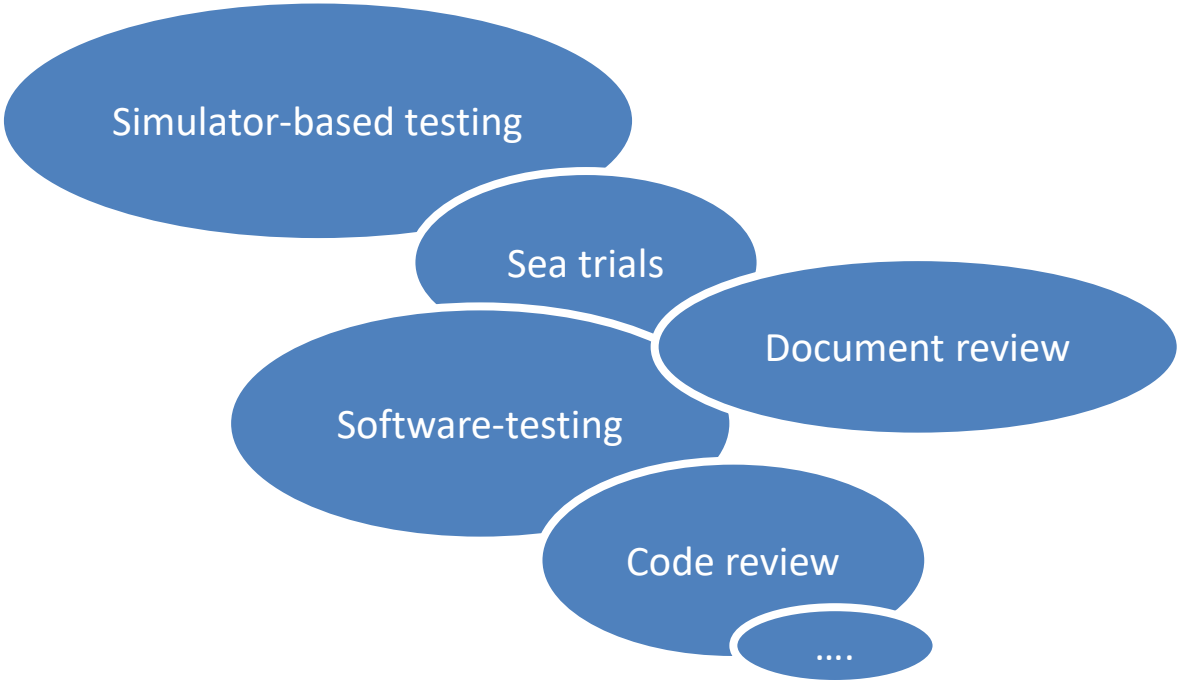
Think of all potential hazardous scenarios

Test how the system handles them

Safety Verification



Verification activities



Using STPA to develop a verification program

Step 1: Conduct STPA to find:
- Hazardous scenarios
- Safety constraints

Step 2: For each scenario, identify:
- Key variables
- Verification objectives (aims)
- Acceptance criteria

Step 3: For each verification objective determine suitable means (verification activities for verification)

Step 4: Describe setup, execution, and concrete acceptance criteria for each activity

Case study

Autonomous ships

Step 1: STPA

- Accidents:
  - A-1: The ship collides with a moving obstacle
  - A-2: The ship collides with a stationary obstacle

- Hazards:
  - H-1: The ship violates a specified minimum separation distance to an obstacle
  - H-2: Ship violates COLREG or rules for sensible behavior on the sea (A-1)

Step 1: STPA

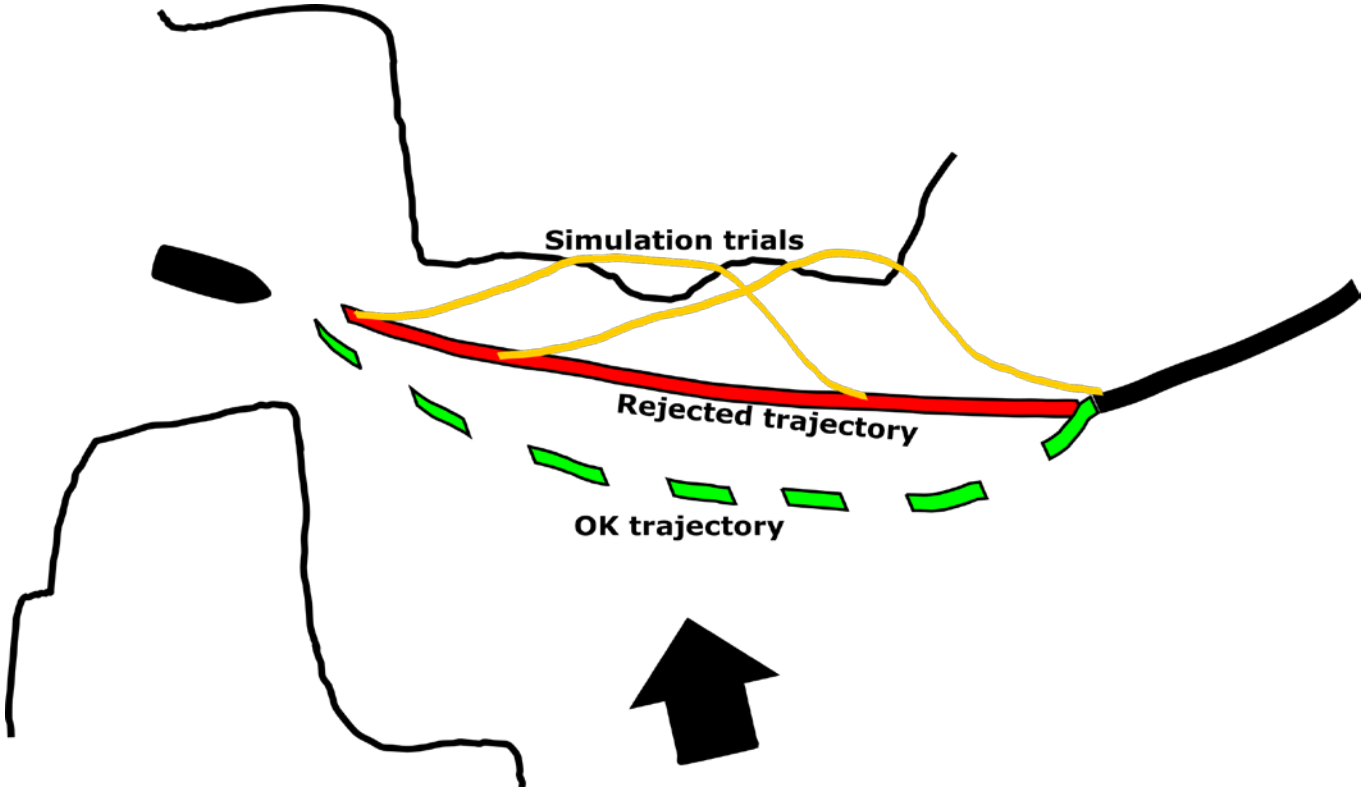
Control action	Not provided	Provided
Update trajectory (SCC)	**UCA-1**: The trajectory is not updated by SCC to avoid obstacles or ensure COLREG compliance when the ship is under indirect remote control (H-1,2)	**UCA-2**: A trajectory which is such that loss of maneuverability will result in violation of minimum specified separation distance to an obstacle, is provided (H-1,2)

Step 1: STPA

UCA-2: A trajectory which is such that loss of maneuverability will result in violation of minimum specified separation distance to an obstacle, is provided

- **SC**: There are two options to avoid this:
  - Ensure that loss of maneuverability will not occur
  - Update the trajectory such that loss of maneuverability will not result in violation
- **Scenario**: The remote operator incorrectly believes that the maneuverability will remain sufficient to avoid violation following any WCSF
  - **SC:** The autonomous ship must include a function to online assess whether nominal trajectory will result in violation in the event of any single failure

Online consequence analysis



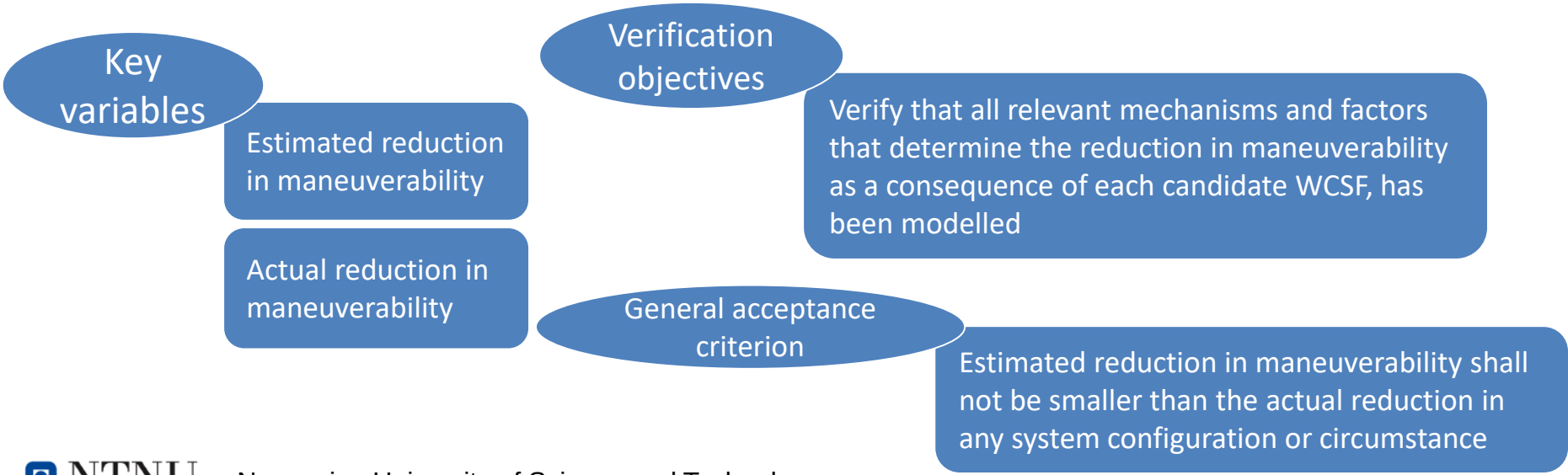
Step 1: Refined STPA

Refined STPA of “Online Consequence Analysis (OCA) function”:

- **UCA**: OCA incorrectly provides “an affirmative” for the nominal trajectory
  - **SC:** Potential outcome of each candidate WCSF must be correctly estimated online for the given system configuration and set of circumstances
    - **Scenario**: The OCA underestimates the consequences of a WCSF candidate because the embedded logics are based on an analysis that disregards relevant mechanisms or factors

Step 2: Key variables, verification objectives and acceptance criteria

Scenario: The OCA underestimates the consequences of a WCSF candidate because the embedded logics are based on analyses that disregards relevant mechanisms or factors



Step 3: Verification activities

Verification objective: Verify that all relevant mechanisms and factors that determine the reduction in maneuverability as a consequence of each candidate WCSF, has been modelled

Check whether OCA will under-estimate maneuvering capacity remaining after any WCSF candidate

Simulator based testing

Check assumptions. Has all relevant factors been accounted for by the model

Review model documentation

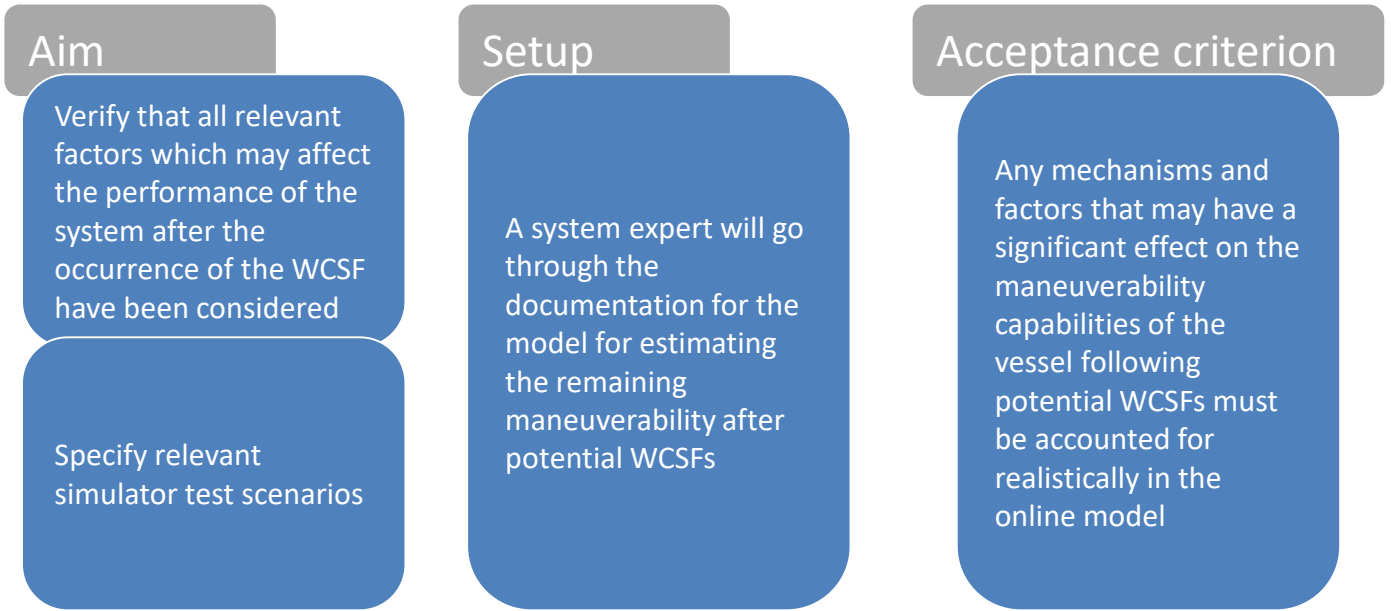
Specify simulator test scenarios by identifying questionable assumptions to test

Verify simulation-based tests

Practical trials

Step 4: Setup and execution

Review model documentation



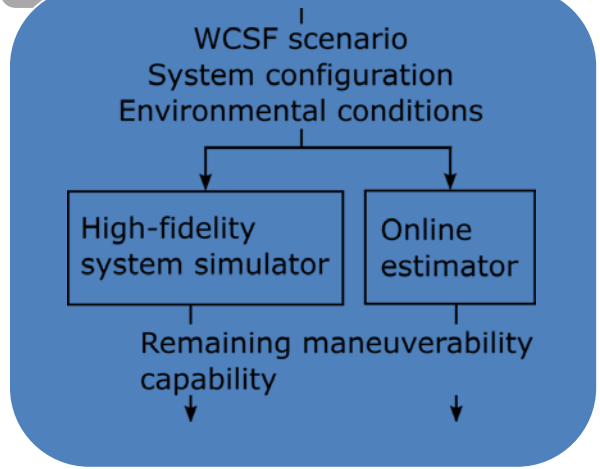
Step 4: Setup and execution

Simulator-based testing

Aim

Compare online model for estimating remaining maneuverability after WCSF to results from high-fidelity simulator model for all candidate WCSFs in a wide selection of system configurations and environmental circumstances

Setup



Acceptance criterion

The losses in maneuverability estimated by the online estimator must be at least as severe as those estimated by the high fidelity simulator

Conclusion

- Enables development/outlining of safety verification program in early concept development phase
- Integrates design and verification management
- Further work will focus on conducting a more comprehensive case study for autonomous ships in cooperation with industry partners