NTNU

Norwegian University of Science and Technology

Prioritizing the Results from STPA - A Case study for a Car Ferry with a Novel Battery Power Supply System

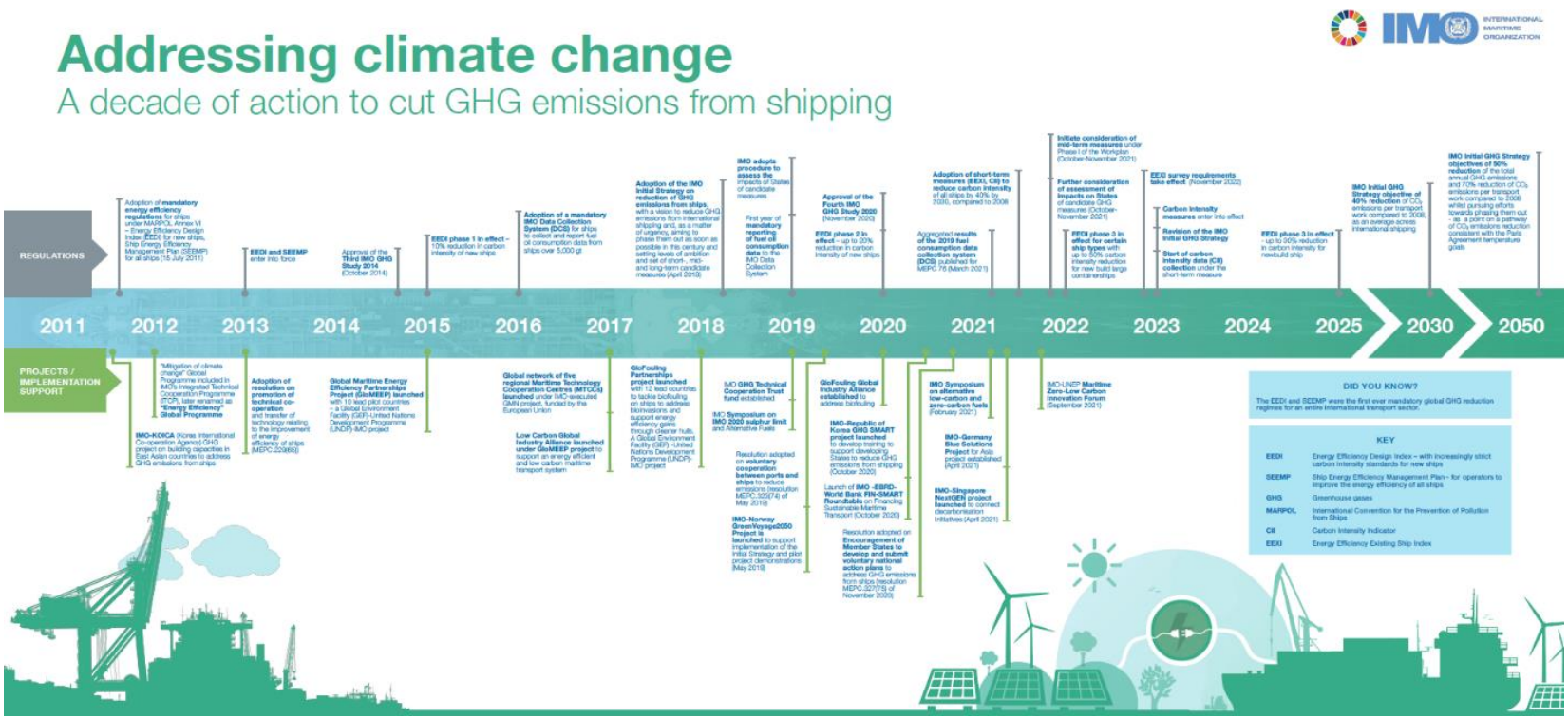
08.06.2023
Associate Professor Hyungju Kim (NTNU)
Dr. Young-Shik Kim (KRISO)
Ms. Kwiyeon Koo (USN)

Contents

NTNU

Introduction

GHG Reduction in Maritime Industry



GHG Reduction in Maritime Industry

PORT OF OSLO

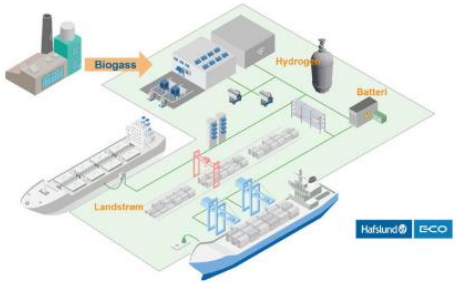
World's first emissions-free port

Port of Oslo's vision is to become the world's most environmentally friendly urban port. The plan for a zero-emissions port was established and approved by Oslo City Council in 2018.

By 2030, Oslo will eliminate 95% of greenhouse gas emissions. Port of Oslo will reduce emissions by 85% in the same period, and become emissions-free over the long term.

Zero-emissions urban port: Oslo is well on its way to developing a zero-emissions port. Illustration: Municipality of Oslo

ELECTRIC LOCAL FERRY. Several million people travel emissions-free between Oslo and Nesodden each year. Ferries charge batteries at the pier in front of the town hall. Photo: Geir Anders Rybakken Ørslien



ENERGY EFFICIENT. Port of Oslo invests in increased energy efficiency through electric transport and terminal infrastructure, shore power, and renewable fuels for ships, shore power, hydrogen and battery. Illustration: Hafslund Eco

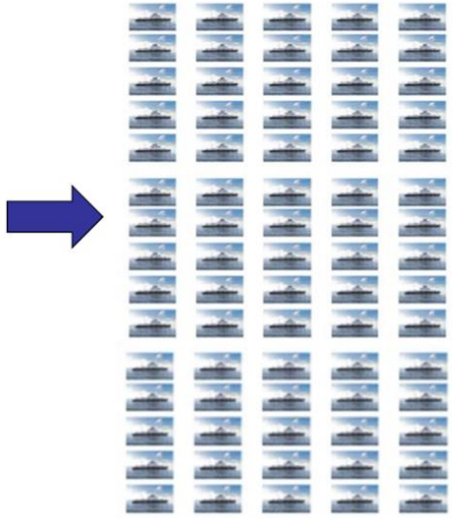
https://www.oslohavn.no/en/menu/klima-og-miljo-i-oslo-by-og-havn/zero-emissions-port/

Battery Powered Ships in Norway

NORLED

2015: The first el-ferry "Ampere" is launched

2022: About 80 el-ferries in Norway



Source: NORLED

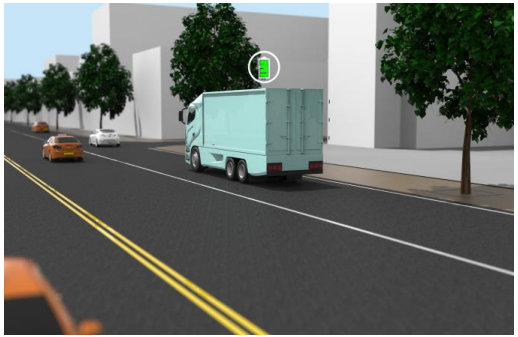
Battery Powered Ships in South Korea

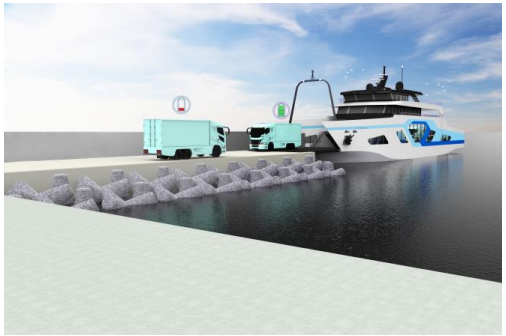
Charging facilities in Norway and Finland

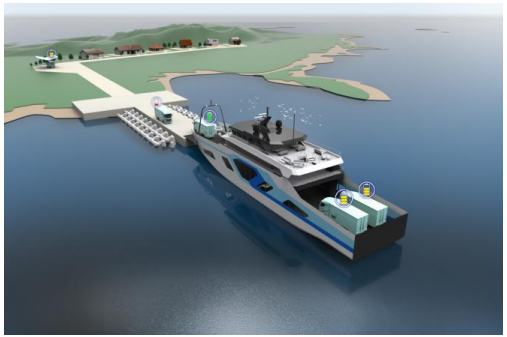
Different weather condition in South Korea

A Novel Battery Power Supply System

A Novel Battery Power Supply System







https://www.youtube.com/watch?v=_ikCgYrHj6Q

A Novel Battery Power Supply System

Launched on March 2022

- Gross Tonnage : 460 ton
- Length Overall All : 60m
- Capacity : 120 persons + 20 cars
- Power Supply : 2 x 800kW battery trailers

A Novel Battery Power Supply System

Car-ferry at the quay

Car deck (front)

Car deck (rear)

Bridge

Propulsion motors

Propulsion motor test w/ battery

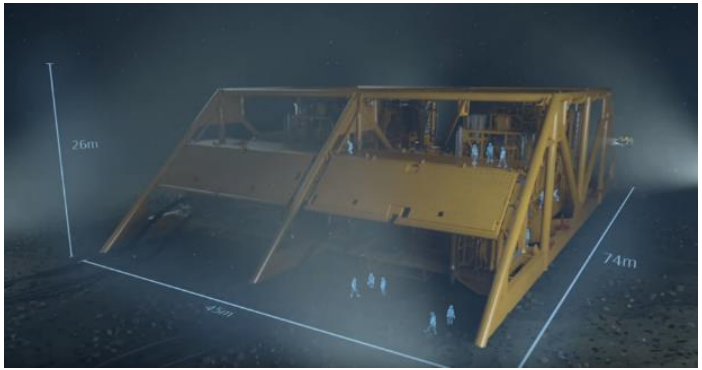
Power distribution panels

Fixed battery

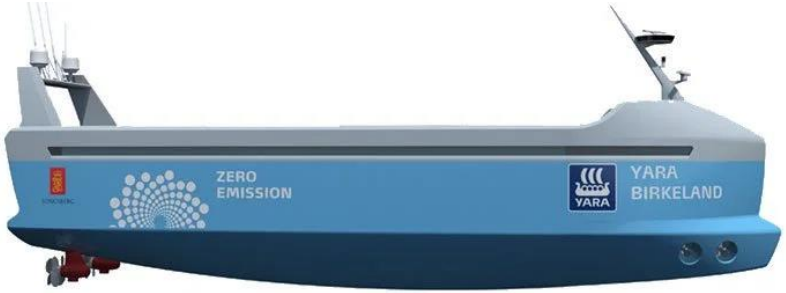
Objective

Analyze safety of the car ferry with a novel battery power supply system

Too Many UCAs and Loss Scenarios

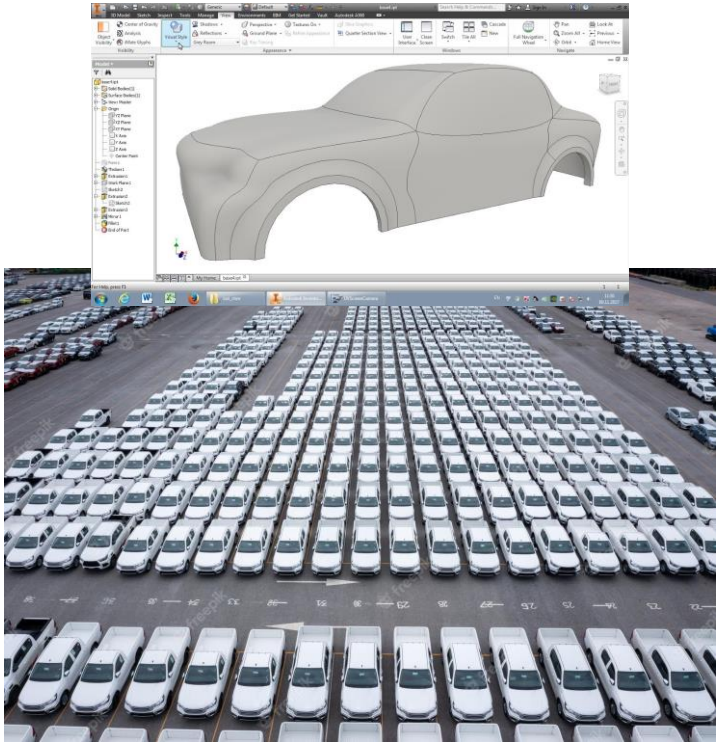


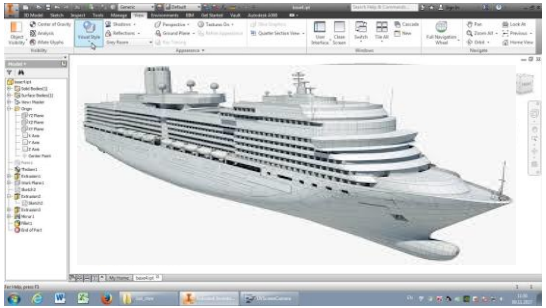
130 UCAs and
976 Loss Scenarios



81-155 UCAs and
256-766 Loss Scenarios

Too Many?



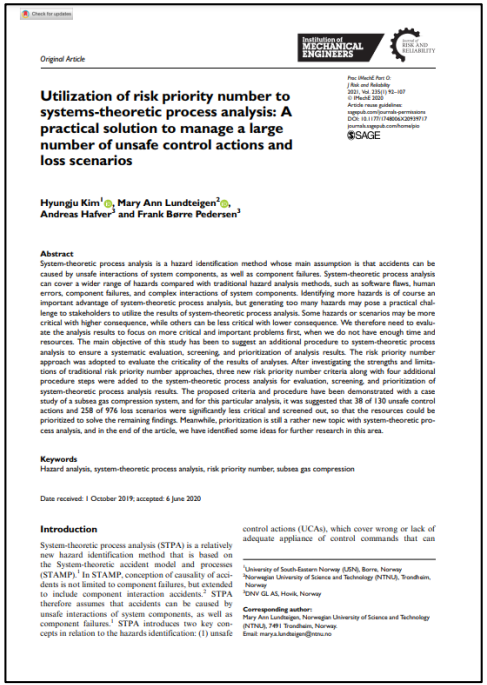


NTNU

Method

Prioritizing the Results from STPA

Prioritizing the Results from STPA



Original Article

Utilization of risk priority number to systems-theoretic process analysis: A practical solution to manage a large number of unsafe control actions and loss scenarios

Hyungju Kim[1], Mary Ann Lundteigen[2], Andreas Hafver[3] and Frank Børre Pedersen[1]

Abstract

System-theoretic process analysis is a hazard identification method whose main assumption is that accidents can be caused by unsafe interactions of system components, as well as component failures. System-theoretic process analysis can cover a wider range of hazards compared with traditional hazard analysis methods, such as software flaws, human errors, component failures, and complex interactions of system components. Identifying more hazards is of course an important advantage of system-theoretic process analysis, but generating too many hazards may pose a practical challenge to stakeholders to utilize the results of system-theoretic process analysis. Some hazards or scenarios may be more critical with higher consequence, while others can be less critical with lower consequence. We therefore need to evaluate the analysis results to focus on more critical and important problems first, when we do not have enough time and resources. The main objective of this study has been to suggest an additional procedure to system-theoretic process analysis to ensure a systematic evaluation, screening, and prioritization of analysis results. The risk priority number approach was adopted to evaluate the criticality of the results of analyses. After investigating the strengths and limitations of traditional risk priority number approaches, three new risk priority number criteria along with four additional procedure steps were added to the system-theoretic process analysis for evaluation, screening, and prioritization of system-theoretic process analysis results. The proposed criteria and procedure have been demonstrated with a case study of a subsea gas compression system, and for this particular analysis, it was suggested that 38 of 130 unsafe control actions and 258 of 976 loss scenarios were significantly less critical and screened out, so that the resources could be prioritized to solve the remaining findings. Meanwhile, prioritization is still a rather new topic with system-theoretic process analysis, and in the end of the article, we have identified some ideas for further research in this area.

Keywords

Hazard analysis, system-theoretic process analysis, risk priority number, subsea gas compression

Date received: 1 October 2019; accepted: 6 June 2020

Introduction

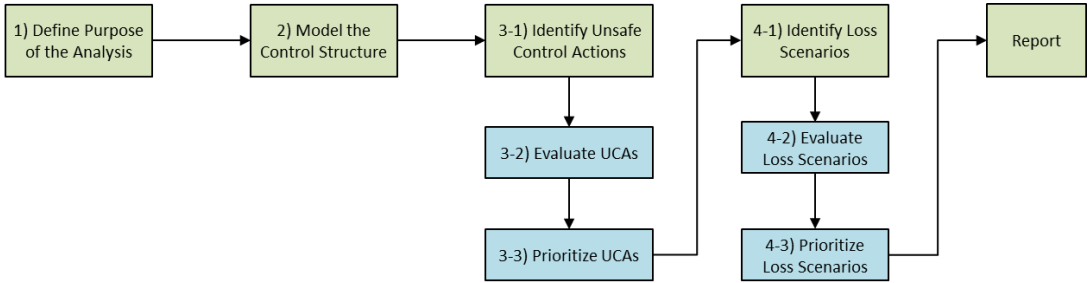
System-theoretic process analysis (STPA) is a relatively new hazard identification method that is based on the System-theoretic accident model and processes (STAMP).[1] In STAMP, conception of causality of accidents is not limited to component failures, but extended to include component interaction accidents.[2] STPA therefore assumes that accidents can be caused by unsafe interactions of system components, as well as component failures.[1] STPA introduces two key concepts in relation to the hazards identification: (1) unsafe control actions (UCAs), which cover wrong or lack of adequate appliance of control commands that can

[1]University of South-Eastern Norway (USN), Borre, Norway
[2]Norwegian University of Science and Technology (NTNU), Trondheim, Norway
[3]DNV GL AS, Høvik, Norway

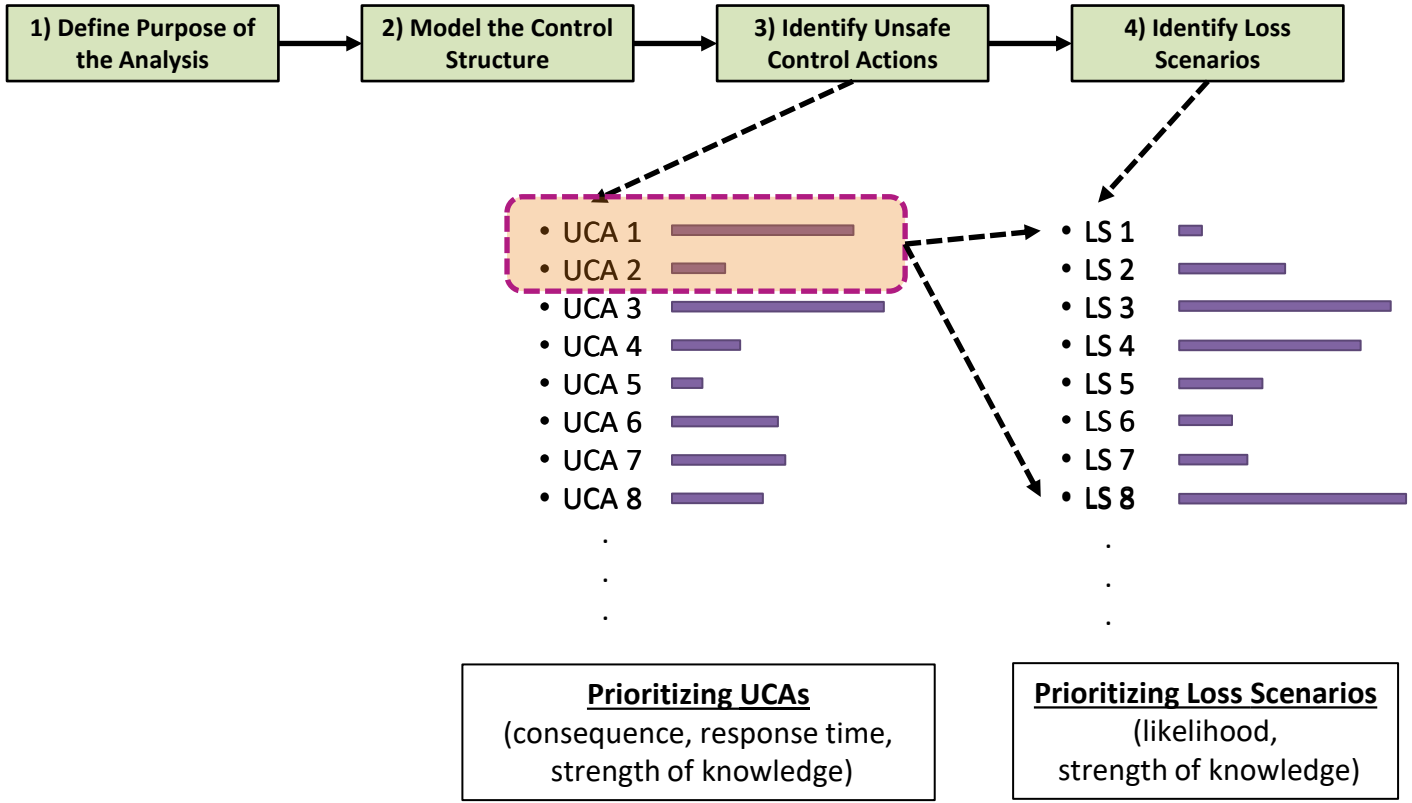
Corresponding author:
Mary Ann Lundteigen, Norwegian University of Science and Technology (NTNU), 7491 Trondheim, Norway.
Email: mary.a.lundteigen@ntnu.no

https://doi.org/10.1177/1748006X2093971

Additional sub-steps for evaluation and prioritization



Prioritizing the Results from STPA



Evaluation Criteria

Table 3. Evaluation criteria for UCAs.

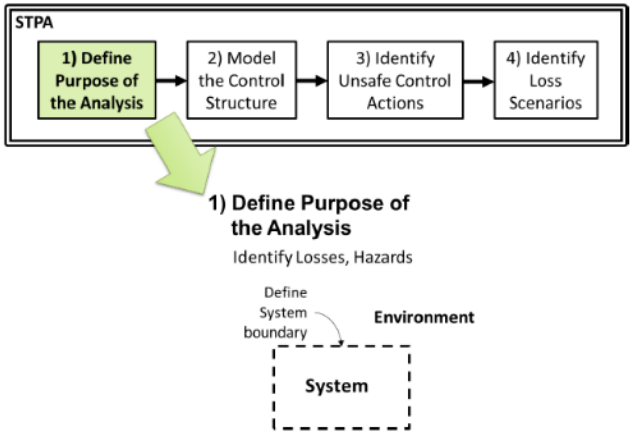
Criteria	Category and description
Severity[a] (SV)	5. Catastrophic loss to human, environment, and/or property. 4. Severe loss to human, environment, and/or property. 3. Major damage to human, environment, and/or property. 2. Damage to human, environment, and/or property. 1. Minor damage to human, environment, and/or property.
Available time to respond (ATR)	5. Not possible to prevent occurrence of accident after UCA. 4. Accident can be prevented or mitigated, only if required action is provided instantly. 3. Accident can be prevented or mitigated, if required action is provided in time. 2. UCA causes accident rather slowly, so we have some time to respond to UCA and prevent or mitigate accident. 1. UCA causes accident very slowly, so we have far enough time to respond to UCA and prevent or occurrence of accident.
Strength of knowledge on UCA (SOK)	5. Complex control action with no or little experience. 4. Complex control action with a small number of experiences. 3. Complex control action with a large number of experiences. 2. Straightforward control action with a small number of experiences. 1. Straightforward control action with a large number of experiences.

Table 4. Evaluation criteria for loss scenarios.

Criteria	Category and description
Likelihood[a] (LH)	5. Event that is expected to occur frequently. 4. Event that happens now and then and will normally be experienced by the personnel. 3. Rare event, but will possibly be experienced by the personnel. 2. Very rare event that will not necessarily be experienced in any similar plant. 1. Extremely rare event.
Strength of knowledge on loss scenario (SOK)	5. Complex scenario with no or few experience. 4. Complex scenario with a small number of experiences. 3. Complex scenario with a large number of experiences. 2. Straightforward scenario with a small number of experiences. 1. Straightforward scenario with a large number of experiences.

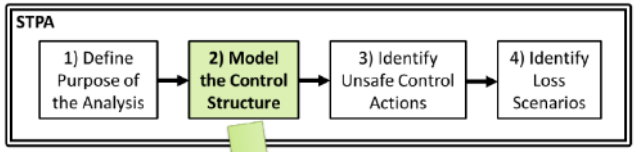
NTNU

Results

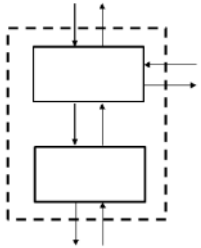


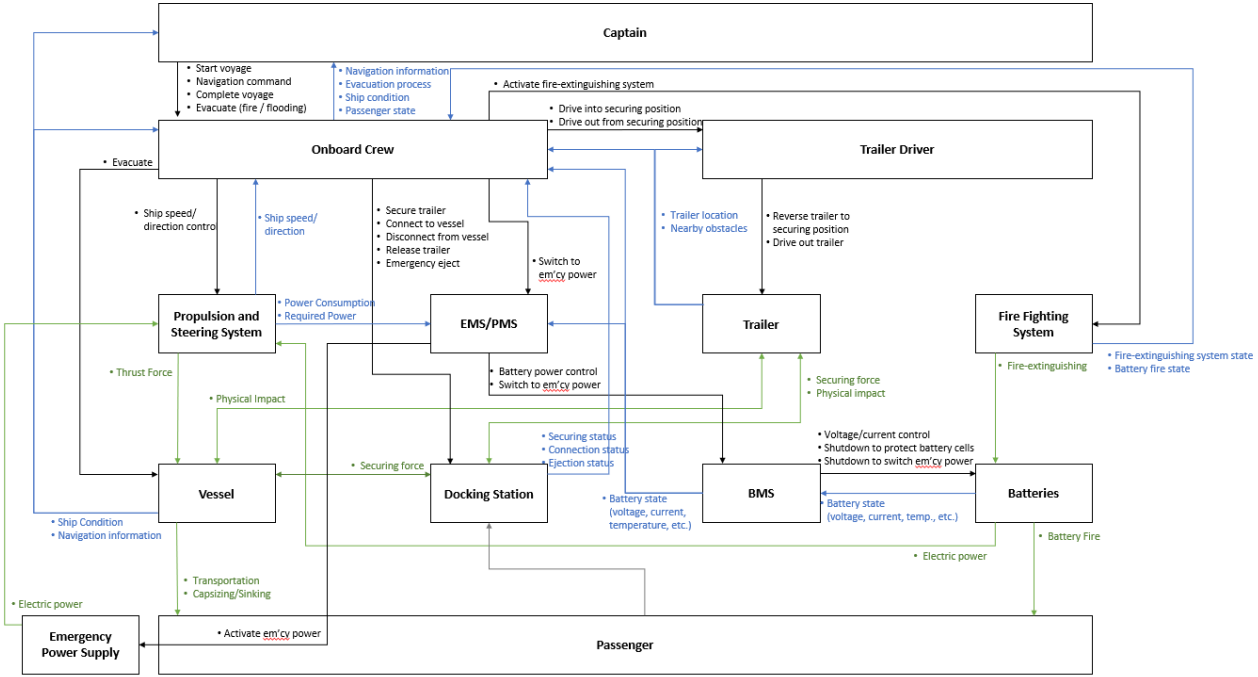
No	Loss
L1	Loss of human life/injury
L2	Asset damage (ship, battery trailer)
L3	Loss of time (inefficient operation)

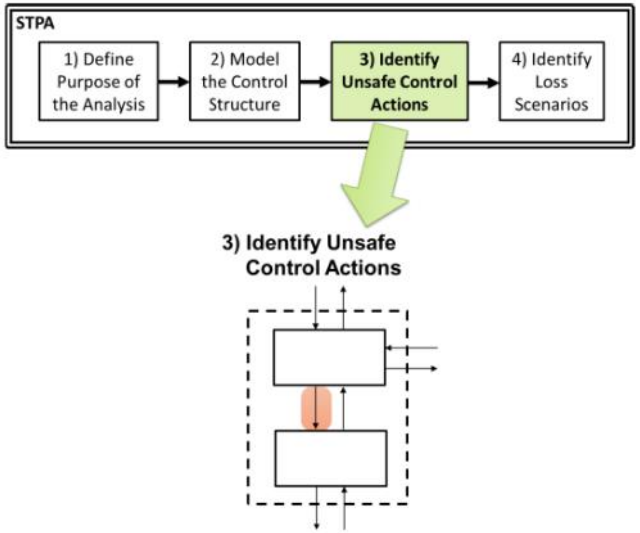
No	Hazard
H1	Vessel related hazards
H1.1	Collision, contact, grounding [L1, L2]
H1.2	Uncontrollable fire occurs [L1, L2]
H1.3	Delayed vessel operation [L3]
H2	Passenger related hazards
H2.1	Passengers fail to evacuate when emergency [L1]
H2.2	Passengers evacuate when no emergency [L3]
H3	Battery trailer related hazards
H3.1	Trailer crashes into human, ship structure, other obstacles [L1, L2]
H3.2	Delayed trailer operation

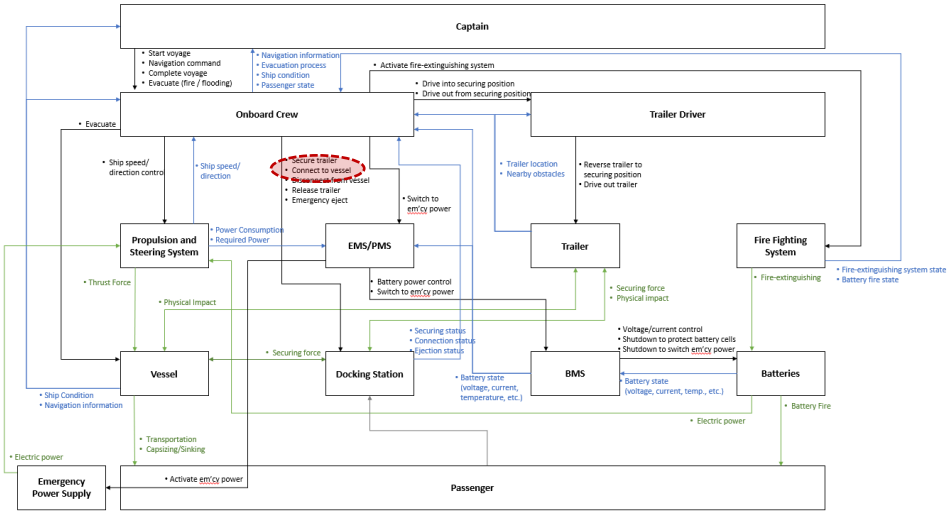


2) Model the Control Structure

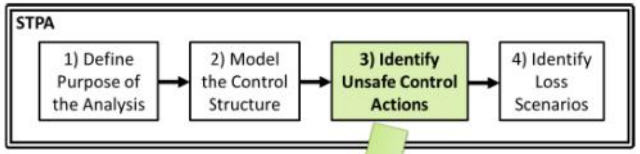


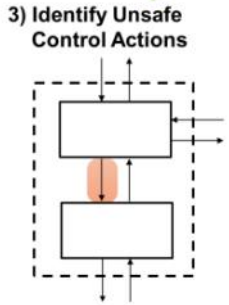




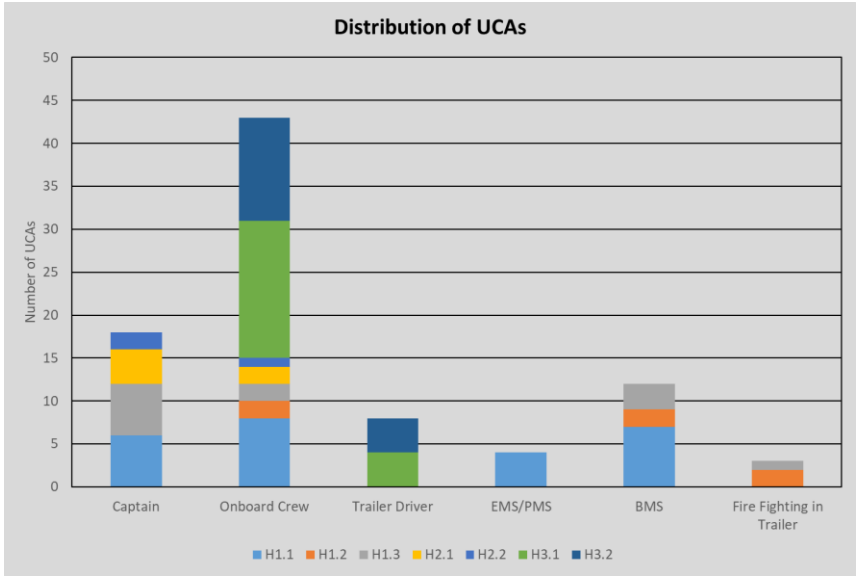


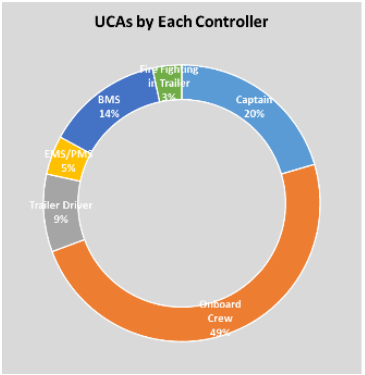
Controller: Onboard crew									
ID	Control Action	Condition		Unsafe Control Actions?					
		Battery trailer is properly secured	Vessel is ready to be connected	Not provided	Provided	Too early	Too late	Too short	Too long
CA.OC.003	Connect battery trailer to vessel	Yes	Yes	Unsafe [H3.2]	Safe	Unsafe [H3.1]	Unsafe [H3.2]	N/A	N/A
		Yes	No	Safe	Unsafe [H3.1]	N/A	N/A	N/A	N/A
		No	Yes	Safe	Unsafe [H3.1]	N/A	N/A	N/A	N/A
		No	No	Safe	Unsafe [H3.1]	N/A	N/A	N/A	N/A

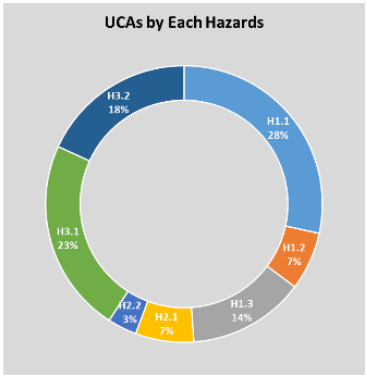


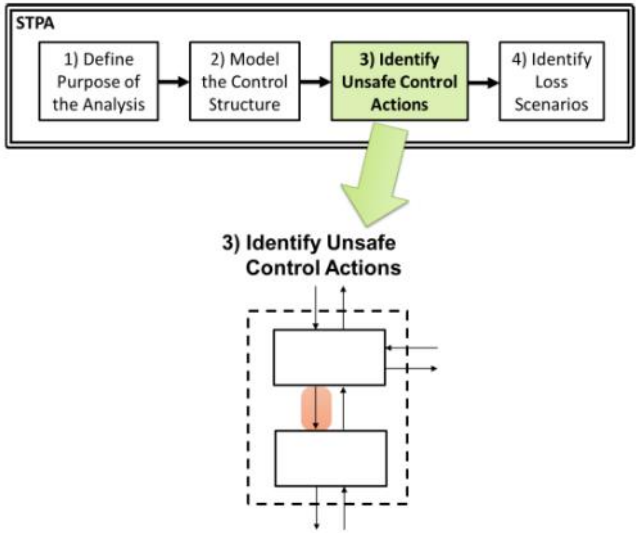


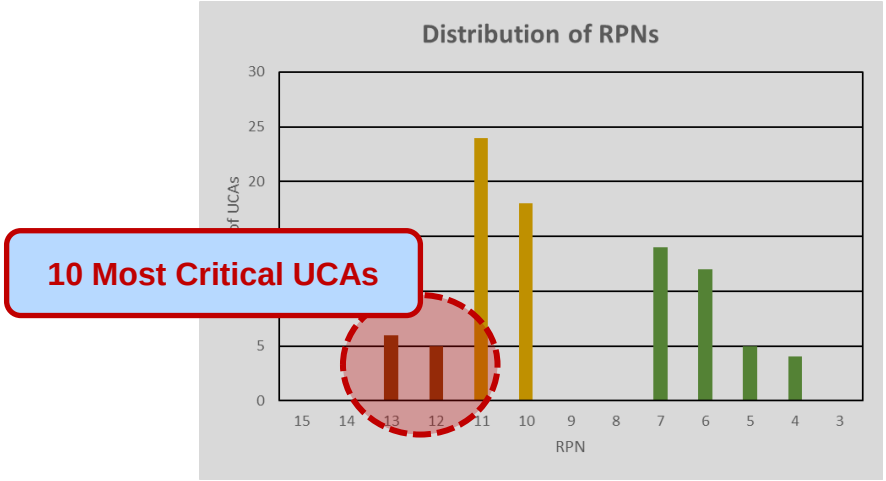
88 Unsafe Control Actions (UCAs)





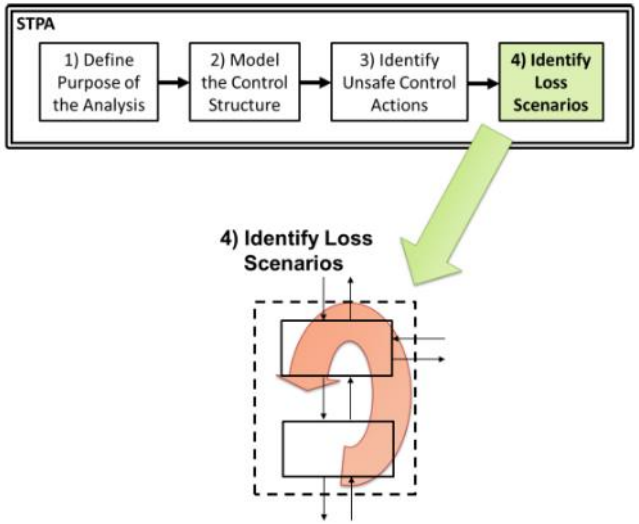




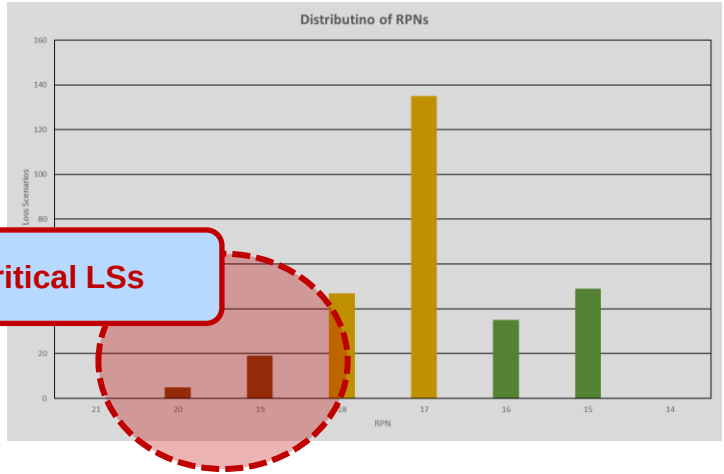


Prioritizing UCAs

Controller	No.	UCA	SV	ATR	SKU	RPN
Onboard Crew	UCA.OC.001	Onboard Crew does not provide Guide Battery Trailer to Securing Position command when the securing position is clear [H3.2]	1	2	3	6
	UCA.OC.002	Onboard Crew provides Guide Battery Trailer to Securing Position command too early before the securing position is clear [H3.1]	4	4	3	11
	UCA.OC.003	Onboard Crew provides Guide Battery Trailer to Securing Position command too late after the securing position is clear [H3.2]	1	2	3	6
	UCA.OC.004	Onboard Crew provides Guide Battery Trailer to Securing Position command when the securing position is not clear [H3.1]	4	4	3	11
	UCA.OC.005	Onboard Crew does not provide Secure Battery Trailer command when the battery trailer is parked on correct securing position [H3.2]	1	2	4	7
	UCA.OC.006	Onboard Crew provides Secure Battery Trailer command too early before the battery trailer is parked on correct securing position [H3.1]	2	4	4	10
	UCA.OC.007	Onboard Crew provide Secure Battery Trailer command too late after the battery trailer is parked on correct securing position [H3.2]	1	2	4	7
	UCA.OC.008	Onboard Crew provide Secure Battery Trailer command when the battery trailer is not parked on correct securing position [H3.1]	2	4	4	10
	UCA.OC.009	Onboard Crew does not provide Connect Battery Trailer to Vessel command when the battery trailer is properly secured and the vessel is ready to be connected [H3.2]	1	2	4	7
	UCA.OC.010	Onboard Crew provides Connect Battery Trailer to Vessel command too early when the battery trailer is properly secured but the vessel is not ready to be connected [H3.1]	3	4	4	11



290 Loss Scenarios (LSs) from 10 critical UCAs



Controller	LS No	Loss Scenario	Risk Reducing Measures
Onboard Crew	LS.OC.033.009	Onboard Crew does not receive the information that the ejection is required, so Onboard Crew does not provide Eject Battery Trailer to the Sea command when uncontrollable fire occurs from the battery trailer	- Apply a back-up communication with Onboard Crew - Install separate alarm system for ejection situation
Onboard Crew	LS.OC.028.008	Onboard Crew provides Guide Battery Trailer from Securing Position command too early when the battery trailer is released from securing position but the route is not clear, because Onboard Crew misunderstands that the route is clear or ignore checking the route before guide the trailer	- Install automatic alarm system to warn occupied trailer route - Allocate additional crew to support trailer guide - Apply fully autonomous trailer - Provide periodic training of guiding trailer to Onboard Crew

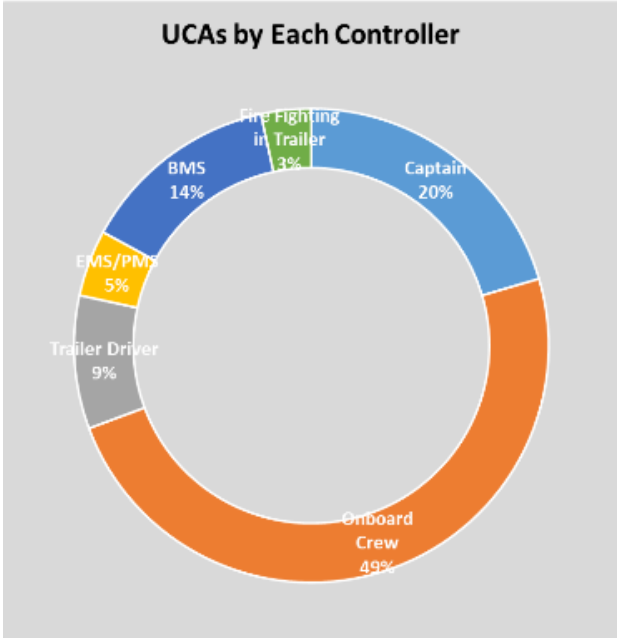
NTNU

Discussion

Discussion

1) Main Findings by STPA

- Additional important roles for onboard crew members : guiding, connecting, securing battery trailers
- Regular safety training, backup communication, separate alarm system, additional crew, etc.



Discussion

2) Evaluation Criteria

Table 3. Evaluation criteria for UCAs.

Criteria	Category and description
Severity[a] (SV)	5. Catastrophic loss to human, environment, and/or property. 4. Severe loss to human, environment, and/or property. 3. Major damage to human, environment, and/or property. 2. Damage to human, environment, and/or property. 1. Minor damage to human, environment, and/or property.
Available time to respond (ATR)	5. Not possible to prevent occurrence of accident after UCA. 4. Accident can be prevented or mitigated, only if required action is provided instantly. 3. Accident can be prevented or mitigated, if required action is provided in time. 2. UCA causes accident rather slowly, so we have some time to respond to UCA and prevent or mitigate accident. 1. UCA causes accident very slowly, so we have far enough time to respond to UCA and prevent or occurrence of accident.
Strength of knowledge on UCA (SOK)	5. Complex control action with no or little experience. 4. Complex control action with a small number of experiences. 3. Complex control action with a large number of experiences. 2. Straightforward control action with a small number of experiences. 1. Straightforward control action with a large number of experiences.

Table 4. Evaluation criteria for loss scenarios.

Criteria	Category and description
Likelihood[a] (LH)	5. Event that is expected to occur frequently. 4. Event that happens now and then and will normally be experienced by the personnel. 3. Rare event, but will possibly be experienced by the personnel. 2. Very rare event that will not necessarily be experienced in any similar plant. 1. Extremely rare event.
Strength of knowledge on loss scenario (SOK)	5. Complex scenario with no or few experience. 4. Complex scenario with a small number of experiences. 3. Complex scenario with a large number of experiences. 2. Straightforward scenario with a small number of experiences. 1. Straightforward scenario with a large number of experiences.

STPA HANDBOOK

NANCY G. LEVESON
JOHN P. THOMAS

MARCH 2018

This handbook is intended for those interested in using STPA on real systems. It is not meant to introduce the theoretical foundation, which is described elsewhere. Here our goal is to provide direction for those starting out with STPA on a real project or to supplement other materials in a class teaching STPA.

hyung-ju.kim@ntnu.no