University of
South-Eastern Norway

Fire safety of battery powered autonomous ferry: a case study of Sundbåten using System-Theoretic Process Analysis.

Candidate name: Henning Mathias Methlie

University of South-Eastern Norway
Faculty of Technology, Natural Sciences and Maritime Sciences

MASTER THESIS

May 2022

Candidate number: 8022

Abstract

Battery solutions onboard ships is rising in popularity as implementation of green technologies is becoming increasingly important to satisfy environmental aspects and the risk has to be critically assessed. Trial and error is a crucial element in developing technical solutions, but a lack of knowledge and experience can greatly increase the potential for unexpected causal scenarios leading to unacceptable losses. To identify causal factors for complex systems taking various elements into consideration there is a relatively new risk analysis method called System-Theoretic Process Analysis (STPA) designed for modern socio-technical systems. Due to the flexibility of the method, it is capable of analyzing causal factors and the interactivity between the different elements such as software, human elements, physical components and so on. However, there is relatively few studies applying STPA on autonomous ships with battery solutions.

The objective of this thesis is to investigate and add research towards battery fire safety onboard ships. For this purpose, the thesis includes a qualitative analysis of existing research on the topic, investigation of battery fire accidents, and a preliminary risk analysis of the new electric passenger ferry with autonomous capabilities called “Sundbåten” using STPA.

Acknowledgement

I would like to express my deepest gratitude and major thanks to my professor and supervisor Hyungju Kim. Not only for his invaluable guidance for this thesis, but for other subjects as well. I would also like to give him the biggest thank you for his kindness and continuous initiative to share discussions and knowledge.

Table of content

1 Introduction

1.1 Background

Implementing state-of-the-art green and futuristic solutions is essential to continue the evolution of our society from a technical point of view. In an ideal world, accidents would not occur, but that is not the reality. History shows that risk taking is a key component in in the development of technical solutions. For a technical manager it is crucial to ensure the safety of all stages of development from the conceptual design phase to actual operation for any project. State of the art technical systems capabilities can be incredibly intriguing and impressive, but it is crucial not to be blinded by all the benefits. Especially for novel socio-technical systems there are previously unknown risks emerging which can cause major losses. Therefore, it is incredibly important to reduce the risk of unacceptable losses by applying suitable risk analysis methods to increase likelihood of identifying all critical causal factors.

Two incredibly interesting segments within the maritime business that are rising in popularity for many ship owners and maritime organizations are ships with autonomous capabilities and electric solutions. The evolution of both these segments are still at a relatively early stage which from a safety aspect causes a lot of uncertainty. Based on the literature review conducted in the thesis it seems to be a clear lack of academic research regarding the safety of both autonomous ships, battery solutions as well as the human interaction with the emerging socio-technical systems. This thesis will target the safety aspect of battery solutions onboard ships with focus on fire events and human interaction.

This thesis is a preliminary risk analysis on a real vessel called “Sundbåten”. It is a relatively small passenger ferry which is currently being rebuilt into a more modern socio-technical system with autonomous capabilities and batteries. The ferry will be installed with a hybrid power solution using batteries as its main source of power and a diesel generator for emergency scenarios. The ferry will also be equipped with a semi-autonomous control system which means one captain is always onboard during operation. The ferry is specifically designed for short distance voyages inshore in Kristiansund.

There are not only benefits with implementation battery power systems for marine vessels. The development of battery solutions onboard ships is still at a relatively early stage, so it can be argued that there are still a lot of possible fault scenarios that are unknown. Another challenge with implementing the solutions is that in certain cases in can be difficult to undergo proper trial and error phases to identify all unexpected fault scenarios. Referring to the two battery fire accidents that has occurred in Norway in recent years (MF Ytterøyningen and MS Brim), potential worst-case scenarios are easy to imagine. These scenarios are undoubtedly highly critical in terms of human safety, commercial aspects, social- and environmental impact. As for materialistic damage there are obviously various levels of criticality from minor damage to the battery packs to thermal runaways leading to fire and explosion. Since Sundbåten can carry more than hundred passengers at a time, it is crucial for the overall safety to properly analyze how to handle the battery installation. Any major accident would also undoubtedly lead to social and legal complication which would drastically slow down the development and testing of Sundbåten and other similar systems.

Most studies on the topics as of today shows indications that there is a lack of experience with large battery systems onboard. It is fair to say that for many novel technical solutions despite all the benefits, it will also bring new previously unknown causal factors which potentially leads to critical loss scenarios. As the complexity increases in socio-technical systems it also becomes increasingly difficult to analyze the different interactions between all elements such as the human element, all physical components and complex control systems. The human element in autonomous ships can have different roles such as the onboard captain, remote human operator, software developers or even passengers (Ahvenjärvi, 2016). The different human elements have each their interrelations with the technical system which is crucial to define to be able to identify important risks. For this thesis, the focus in the risk analysis procedure will be directed towards the interactivity between the fire safety system and the different human elements that has a goal of detecting, preventing, and controlling fire events inside the battery room.

Analyzing the overall risk and the interaction can be difficult to analyze with traditional risk analysis methods. Therefore, it should be considered essential to adapt to the novel socio-technical system by developing modern risk analysis methods to minimize risk and identify all critical causal factors and avoid unacceptable loss scenarios. To identify responsibilities, unsafe control actions, unacceptable loss scenarios the risk analysis method called System-Theoretic

Process Analysis (STPA) will be used. STPA is a relatively new hazard analysis method based on system theory. The hazard analysis technique is designed to analyze modern systems' increasing complexity, including socio-technical and software intensive systems. Leveson and Thomas (2018) implies that STPA are not only capable of identifying all causal scenarios as possible with traditional methods, but also many more. Due to its flexibility the method has risen in popularity various autonomous systems such as cars and aircrafts. But, referring to the literature review there are still not many studies applying STPA for ferry operation with battery solutions.

1.2 Literature review

For the literature review there are two main points with goal of supplying the academic purpose of the thesis. First point is to research application and suitability of the STPA method to be able to validate the method as a good solution. Since it is fair to say that there is an increasing complexity there is new and previously unknown factors that must be taken into consideration. Therefore, it is considered highly important to ensure that the most suitable risk analysis for modern sociotechnical systems is applied. This is done below by reviewing academic literature on the application of the method itself and the outcomes of the research. There is also a review on procedure itself based the STPA handbook from Leveson and Thomas published on Massachusetts Institute of Technology (MIT) webpages in section 2.2.

The second objective with the literature review is to do in-depth research battery fire onboard ships. This will be done by attempting to answer a few key questions such as what has been researched, what research methods did they use, human interaction with the battery fire safety systems, fire extinguishing- and detection systems and if there are any clear gaps in the academic research. As part of the literature review investigating battery fire there will be a separate battery fire report in section 3 which is based upon other sources such as Norwegian news outlets, online and academic articles.

There is simply just not much research academic research that includes all the main objectives for this thesis. Therefore, some of the literature researched articles will be not directly towards the overall objective, but relevant in some way to supply the overall objective of the thesis. The first subsection is dedicated to reviewing STPA as a suitable method compared to traditional ones as well as results and points from various academic articles. Various STPA procedures will also be investigated to improve this thesis' application of the method. The second subsection will cover a few points regarding the battery fire aspect.

1.2.1 Battery fire research

Already back in 2015 Rao et al. published a very interesting article researching fire tests and safety measures for larger scale lithium-ion batteries for ships and they had some quite interesting findings (Rao et al., 2015). They used a practical approach by conducting various fire tests to analyze not only the behavior of the fire and lithium-ion batteries, but also fire extinguishing agents. More specifically four tests with various conditions, one free burn scenario and three scenarios with different extinguishing agents. In their tests both usage of carbon dioxide and superfine powder they experienced thermal runaway and reignition scenarios. There was also a case of explosion in test 2 which means that the battery was ignited inside a limited space with lack of oxygen. But the key finding was that during testing of heptafluoropropane the batteries did not re-ignite, explode nor experience a thermal runaway event. In their conclusion they point out the fact that it is very different from traditional power fuel ships including the general lead battery room which implies that new considerations should be taken. As a result of the practical findings, they point out five main fire safety measures for lithium-ion battery rooms. First is that heptafluoropropane fie extinguishing systems was undoubtedly the most efficient agent for battery fires and should be included. lithium-ion batteries shall be located in designated rooms with A60 fire walls and doors. These rooms should also be compact to prevent spread of smoke and/or fire and not have other external heat sources inside the room. As for the battery materials they shall have flame resistant qualities. They also point out that the temperature control of the battery and battery room shall be taken very seriously no matter the condition state or operation. Lastly, as a measure against vibration and possible collision scenarios they suggest the installation to be fixed as amidship as possible.

Rosewater and Williams also published an interesting article already back in 2015 analyzing safety in lithium-ion grid energy storage systems. As part of their analysis, they conducted STPA on a lithium-ion based grid energy storage system. They point out some of the advantages of the STPA method to be efficient, less costly and the fact that the method is suitable to identify causal scenarios that other methods does not. A very interesting key point for novel technical system is that they mention that STPA allows them to do a more "more rational assessment of uncertainty (all that is not known) thereby promoting a healthy skepticism of design assumptions" (Rosewater & Williams, 2015). The focus in Rosewater and Williams' research is very specifically the energy management system, actuators, sensors and the controlled processes of the battery system itself. Compared to their PRA procedure they confirm that STPA is more suitable to analyze complex high consequence sociotechnical systems such as lithium-ion installations. A highly relevant point they make which is relevant for this thesis' objective as well is that their focus on the battery itself is only a small part of a much larger safety picture in a battery energy storage system. This is why it should be considered incredibly important to understand the responsibilities and interactions of all elements in order to identify all unacceptable causal and loss scenarios.

To keep in mind to analyze human interactions in the lithium-ion battery fire events Chen et al. made some quite noteworthy findings in their research on fire hazard predictions for lithium-ion batteries (Chen et al., 2018). They basically prove that the heat release rate of primary lithium-ion batteries have an exponential increase relative to the number of batteries. The point being is that with increasing sized battery packs onboard marine vessels also have an increasing damage potential. I.e., this would increase the risk for humans to interact with the battery solutions during fire events.

As for fire monitoring systems Wei et al. recently published an article researching a special STM32 processor which apparently can determine if the vessel's battery system has a fire hazard by analyzing various data such as air pressure, temperature, humidity, flame- and heat radiation and smoke inside the battery box (Wei et al., 2021). This can possibly highly increase the safety during interactions between the human element and the battery system during a possible hazardous event. They claim that the processor can avoid and detect thermal runaway events at an early stage and counteract it which can potentially greatly reduce risk and mitigate worst-case scenarios. They also suggest that this type of system should be part of the foundation for the future development of battery safety systems.

1.2.2 STPA and the human element

The last few decades novel autonomous solution with battery systems has been introduced to the market at a rapid speed. Arguably one of the biggest challenges from a management perspective is to ensure the safety of these systems as they are implemented. Since there are no safety guarantees, it should be considered key to be on the forefront of adapting to the emerging socio-technical systems by continuously develop and improve new risk analysis methods and procedures. With the new state-of-the-art socio-technical system some of the biggest challenges is to identify the unknown and unpredictable causes leading to hazardous events.

It is incredibly important to select a suitable risk analysis method depending on the system which is to be analyzed and the main objective. For decades traditional risk analysis methods such as fault tree analysis (FTA), event tree analysis (ETA), failure modes and effect analysis (FMECA) and hazard and operability analysis (HAZOP) have been regarded for many years as effective methods to determine the safety state and reliability of the equipment in technical solution. Although the methods have their strong sides, they have limitations when applied to novel solutions since they are highly dependent on historical data. Although the methods have clear benefits when analyzing equipment itself, studies suggests that the methods have clear limitations when it comes to emerging systems (Escande et al., 2016). An interesting point regarding this article is that they refer to both Lannoy and Mannan's investigation reporting that there is a drastic increase in frequency of major technological accidents. This can safely be interpreted as a suggestion that novel technical systems bring many new causal factors leading to accidents. As a conclusion to their investigation, Escande et al. suggests that the traditional methods can have difficulties in identifying root causes of accidents for the emerging technical systems and struggles to predict operational scenarios.

To analyze the safety state and identify causal scenarios for the modern technical system for Sundbåten in the best possible manner it is essential to select the most suitable risk analysis method. In a relatively recent study Zhou et al. assessed applicability of a wide range of different common risk analysis methods to analyze which was the most suitable for similar autonomous systems with a system engineering approach with several safety requirements and criteria (Zhou et al., 2020). They researched 29 traditional risk analysis methods in 269 different studies and had some very interesting findings related to assumptions made in the introduction. “The results indicate that STPA can be regarded as the most promising hazard analysis technique for autonomous ships that fulfill all the evaluation criteria” (Zhou et al., 2020). Regarding applicability on these modern types of systems, it was implied that traditional methods were outdated due to its procedures focusing on individual parts of the system and not including the interaction between the different elements. In the article from Zhou et al. they point out in the conclusion that STPA is suitable not only for complex systems in general, but also the very critical aspect of interaction between the different parts. This includes the interaction between the complex control system, hardware components and the different human interactions. This study is considered reliable and is considered a clear indication that STPA should be the most suitable hazard analysis for Sundbåten’s socio-technical system.

The main challenge is to obviously to provide a satisfying risk analysis and successfully answering the research question which is difficult due to various factors. The application of the risk analysis STPA itself is relatively straight forward, but there are challenges. Despite Zhou et al. (2020) after an extensive analysis on application of different methods on autonomous systems pointed out that STPA is the most suitable method, other studies suggests that it is still not perfect. Johansen & Utne implied that this is partly due to the original STPA procedure being heavily qualitative and lacking the qualitative aspect to differentiate the criticality of identified risks (Johansen & Utne, 2020). Glomsrud and Xie shed light on a different issue which is related to the design of the Control Structure Model (CSM) in STPA step 2 (see section 2.2.2) and researched the possibility of extending step 1 with self-defined procedures to simplify and improve the design of CSM (Glomsrud & Xie, 2020). These are only a few examples of challenges with the application of the standard STPA procedure, which must be taken into consideration.

In another research article the STPA method is not applied to an actual system, but a variation of a larger framework designed specifically for autonomous ships is represented (Chaal et al., 2020). The research done is an attempt to develop the method by designing a hierarchical control structure model for maritime automated operation systems designed as a basis for implementation of STPA analysis. The authors imply in the conclusion that organizational structures as they presented are essential due to a lack of it in previous analyses of autonomous ships as of today. "The control structure will then be used as an advanced starting point to apply STPA analysis to enhance the control structure and identify the eventual safety, resilience, and reliability requirements of autonomous ships" (Chaal et al., 2020). To use this information for this thesis, it is important to remember that variations of the control structure model are individual and can have many different variations. A key aspect of the article from Chaal et al. is that the advanced starting point will likely improve the analyst's ability to clarify and define possible interactions between all the different controllers and controlled processes defined in the system.

As mentioned in an article on supervisory risk control of autonomous ships, emerging risks are being evolved from the new technology and that there is a lack of knowledge and operational experience (Utne et al., 2020). They also mention that there is a limited ability to verify operational safety of such systems. And again, the authors refer to STPA as a suitable hazard identification and analysis tool. Utne et al. brings up a very interesting aspect in online risk modelling which might be taken into consideration. One of the benefits of their proposed method is that the online risk model can predict future risk by simulating sailing process using a complex mathematical model of the ship's environment and planned operation.

Maximizing risk mitigation is obviously the ultimate goal of any risk analysis method. Sundbåten is planned to have semi-autonomous capabilities which essentially means that there will always be one operator onboard during any operational modes. Zhou et al. have published an article investigating the safety aspect of the different levels of automation (Zhou et al., 2020). Based on the results the authors suggest in their conclusion that the higher the level of autonomy, there are more possible risk mitigation measures designed to eliminate hazardous events. Referring to Sundbåten's socio-technical system, a very key point that Zhou et al. touches upon is that the risk mitigation from higher levels of autonomy includes less interactions between the human elements and the technical system. So, the question for this thesis is then to what regard does that impact the interaction between the captain and the safety system onboard Sundbåten. Zhou et al. continues to add an incredibly important point about how autonomous technical systems can struggle to identify damage reduction measures after an accident has occurred no matter the autonomy level. Following that point it is very interesting to analyze and see the importance of the interactivity between the human element and the technical system to create an overall optimal safety solution. Also relevant for this thesis Zhou et al. mentions that an interesting extension of their study would be to apply STPA for maritime transport systems where conventional, remote controlled and fully autonomous ships coexist. As a suggestion to future work, they wrote this: "Furthermore, assessing the safety of future autonomous ships should include the human aspect in autonomous operation, for example, as a designer of decisions and of safety constraints for the system" (Zhou et al., 2020).

Human interaction with a socio-technical system is likely something that will be researched and continuously developed for many years to come. It is fair to say that despite a vessel being autonomous, does not mean that the human element is not essential for operational success in terms of the unpredictable safety aspect. Ahvenjärvi had an interesting take in one of his articles regarding the human element relative to the complexity of systems: "Although some types of operator errors will be eliminated, the human element and the human error in different forms have to be taken into account" (Ahvenjärvi, 2016). This can be various roles such as onboard operator, remote control center operator, software developer or for Sundbåten's socio-technical system it can even include passengers. Ahvenjärvi points out another highly interesting point in the paper which is very relevant for this thesis in particular: "The human element is often associated with human errors. The positive side of the human element is the human creativeness and the ability to adapt to unforeseen and surprising situations (Ahvenjärvi, 2016). The author is following up pointing out that the human elements' strength is also the autonomous systems' potential weakness and that resilience built into the control system is essential to make autonomous vessels safe in the future. Now for this thesis, the questions are how should the human element interact with the battery fire safety system onboard Sundbåten? This is obviously something that can be discussed and researched to find the optimal safety solution.

The discussion about the importance of the human element during operation for a MASS vessel's safety are likely to be a discussion for years. In a study from 2016 it is implied that vessels have incidents due to human error that can be avoided with automation, but there are issues solved by human operators which will not be solved by the autonomous control system. An interesting and relevant point Home et al. points out is an issue regarding the control system: "many real world problems are *complex* in the sense that they have an infinite solution space due to many unknown factors and interrelationships" (Hoem et al., 2018). Interestingly the authors continue to that statement by implying that it is basically theoretically impossible to program a solution for all problems. Identifying some of these interrelationships and its unsafe control actions are also considered to be one of the main objectives for this thesis.

Hoem et al.'s research on safety and reliability shows some very notable pointers regarding the safety of the human elements role in autonomous systems. First its mentioned that it is generally accepted that automation has the potential to reduce the risks due to the human variable, but also includes possible downsides (Hoel et al., 2020). Despite this, they point out the fact that automation system can not only reduce risks, but it also has potential of creating causal factors leading to hazardous events. The authors also suggests that automation can reduce workload for human operator which can possibly cause boredom which again can lead to slower assessment and reaction to a risk scenario. This would be critical especially for battery fire scenarios as each second counts to be able to minimize the risk. The finish off their article by recommending that new types and extensive use of human targeted risk analyses. Although Sundbåten is a semi-autonomous vessel it should still be taken into consideration during the analysis of the battery fire safety system.

Regarding the implementation of autonomous control systems for ships another article suggests that due to the autonomous vessels being at a conceptual stage with few prototypes that only technical factors are sufficiently explored (Wróbel et al., 2020). The study suggesting that that human-oriented issues as under-explored is important to note due to the incredibly high possible worst-case scenarios for human interaction in battery fire scenarios onboard ships. The idea behind this thesis is to analyze the battery safety system onboard ships with an extra focus towards human interaction with the different controllers. Building on the point that there is a gap in the research on this topic, Chae et al. wrote the following in their study from 2020 for MASS: "the IMO human element, human reliability assessment (HRA), and operational risk assessment take into account that the human element should be actively researched and developed" (Chae et al., 2020). The same authors also point at communication systems support MASS operations to be an integral part of the safety system, which includes the Shore Control Centre (SCC). This paper also points towards STPA as one of the most suitable for autonomous ships.

A relevant article from Kim et al. researched the application of STPA on different autonomy levels (Kim et al., 2020). Kim et al. had this to say about the interrelation between the human element and the autonomous system: "The main observation from the paper is that the combined reliance on human and autonomous *can* give a rise to more unsafe situations, than if humans are in control or the ship is in full control" (Kim et al., 2020). When it comes to the actual application of STPA the authors emphasize the importance of identifying all loss scenarios and safety constrain to ensure safety. In a study already in 2018 Wróbel et al. applied STPA for an automated merchant vessel (AMV). Also, in this paper they end up according to themselves with a very successful STPA procedure for their objective to improve the safety system (Wróbel et al., 2018).

The hazard analysis method STPA clearly has benefits due to all the positive findings in several studies. Despite those findings, Glomsrud and Xie have a clear opinion about STPA needing to be improved to properly analyse autonomous ships (Glomsrud & Xie, 2020). One of the issues they are implying is that it is not necessarily straight forward to design the Control Structure Model (CSM) in step 2, especially for autonomous systems that are not necessarily clearly defined. The general idea of losses in STPA step 1 is that it includes unacceptable human, material or societal consequences. Glomsrud and Xie's idea is that the standard "high level" losses can limit findings of less severe losses that are still important for the stakeholders. As a solution they have attempted to extend step 1 and create a gap to simplify and improve the design of CSM by identifying less critical losses related to either safety, availability, security or efficiency. This bridge is suggested to convert constraints into requirements. This is something that will be taken into consideration for application of STPA on Sundbåten.

As Johansen and Utne mentions in their article, the standard STPA procedure is basically a qualitative hazard identification method (Johansen & Utne, 2020). Their objective with the paper was to research the possibility of expanding the STPA model to include quantitative aspects. Although they did find seven suitable combinations, they still specify that there is a major challenged to combine the methods and that it must be addressed further. The potential lack of quantitative factors is something that will be considered for this thesis and assessed after procedure findings and results. Dghaym et al. also implies after their findings that one of the limitations with STPA is that it lacks quantitative analysis which then requires a combination with another analysis technique (Dghaym et al., 2021). As a solution, the authors used a structural combination of STPA and a formal modelling to generate critical requirements to ensure the safety and security of an Unmanned Surface Vehicle (USC).

One recent study applied an interesting closed-loop variation of the STPA method called STPA-SynSS (Zhou et al., 2021). Compared to this thesis having an extra focus towards human interaction, the article from Zhou et al. also had an extra objective to analyze the safety and security for ship-ship collision and cyber security incidents. Their overall process is separated into three main steps in hazard identification, hazard evaluation, and a hazard control step. The workflow in this method is based upon the four same steps as in the standard STPA procedure including two additional steps. Step 5 is designed specifically to evaluate hazard components by analyzing each individual hazardous element, initiating mechanism, target and threat. In addition, a partial sub-step in step 5 is determining probability and severity of unacceptable losses which is arguably one of the weaknesses of the standard STPA procedure. From this sub-step is the authors created a control loop back to identifying unacceptable losses in step 1 in order to be reassessed. In other words, this means that an identified unacceptable hazard element in step 5 can be tracked back to the earlier steps in order to be reassessed and removed or mitigated to an acceptable state.

The Norwegian Maritime Authority (NMA) emphasizes that autonomous vessels must hold the same level of safety as conventional ships and will be assessed based on degree of autonomy and ship type (Norwegian Maritime Authority, 2020). There is one highly relevant article from NTNU that conducts a risk analysis of a very similar small harbor passenger ferry project compared to Sundbåten (Kristensen, 2021). Their objective was also to conduct a preliminary hazard analysis in the in an early stage of the development process. Operational conditions are very similar to Sundbåten as they are both relatively small passenger ferries with a fixed route inshore which means they will have similar challenges. The big difference is that NTNU's ferry is planned to be fully autonomous with a remote supervisor. Again, it is pointed out that there is a lack experience with autonomous vessels which complicates the process of analyzing the risk aspect of the system. To analyze their system, they used a PHA method. The big takeaway points from this article are their possible hazardous event findings, consequences and risk mitigation measures which will be similar for Sundbåten.

1.3 Goal of the thesis

The safety of human lives is arguably the most important aspect of any socio-technical system. Based on the background of selecting the thesis together with the literature review conducted there is identified a clear gap in the research related to battery fire safety onboard ships. There is also clearly lacking academic research applying the STPA method on similar systems. For many of the complex novel systems it can be essential to analyze the human elements to really understand the safety aspect. By performing the STPA hazard analysis the goal is to identify and shed light on any critical and unacceptable unsafe control actions, loss scenarios, potential accidents, or other safety issues for the battery fire safety onboard Sundbåten. Below is the two research questions:

- RQ1: What are the main causes of previous battery fire accidents onboard ferries?
- RQ2: What kind of additional hazards should be considered for the battery fire safety system?

By answering these research question in a satisfying manner, the goal is to add as much research value to the main objectives presented below:

- Add additional research to battery fire safety onboard marine vessels
- Add additional research to the application of STPA on modern socio-technical systems
- Investigate potential hazards for the interactivity between the fire safety system onboard a semi-autonomous electric passenger ferry and the human element(s)

1.4 Structure of the Report

The structure of the thesis is based on the IMRAD model. Section 1 is an introduction to the thesis with various subsections. First there will be a short background to selection of the thesis. Following that is the literature review with the purpose of investigating research related to the safety state of battery solutions onboard marine vessels and the application of STPA. Following the review there is a section defining clear goals of the thesis which is based on the background and findings from the literature review. After this there is an own section to shed light on limitations to find the objectives defined and to answer the research question(s) in an ideal manner. Section 2 covers the research methods used in the thesis to gather data and acquire satisfying results. As a method subsection there will be a step by step describing the main procedure of the thesis which is the application of the risk analysis method STPA. Section 3 is a thorough report investigating battery fire onboard ships. That report is based on general battery fire theory as well as two battery fire accidents in the Norwegian vessels MS Brim and MF Ytterøyningen. Section 4 covers the results after applying the STPA procedure on Sundbåten's battery fire safety system with focus on the human element. The next section will cover the overall discussion touching upon various aspects such as existing research related to the main objective, observations and findings from conducting the STPA and aspects related to the research questions. The last section in the main part of the thesis is the conclusion with recommendations for future research related to the topics. In the appendix there will also be an acronym list as well as additional information from the STPA procedure. See the table of contents for an overview.

2 Research Method

Research methods can be viewed as building stones for a thesis. If the thesis topic or research questions is considered the foundation, then the method(s) will be all the tools required to build the house. For any thesis it is incredibly important to have a proper research design suitable for the thesis' objective. Without structured and suitable methods to answer the research question(s), the findings are highly likely to going to be suboptimal.

2.1 General

The research methods for this thesis will be heavily leaning towards qualitative research methods. To best answer the research questions the research design is a combination of literature reviews and the application of the STPA method. The literature reviews together with the application of the hazard analysis STPA together with a literature review will be the basis for the unit of analysis. The hazard analysis STPA will first be researched in the literature review and then applied in a later main section. The goal with this specific combination is that the literature review will supplement and improve the actual application of the STPA for Sundbåten.

The literature review in section 1.3 was purely based upon relevant published research articles retrieved from trustworthy academic databases. The review covers the latest studies on battery fire safety for marine solutions, studies applying STPA on similar technical systems and the STPA handbook from Leveson and Thomas. The battery fire survey in section 3 is a qualitative case study investigating recent battery fires to determine the safety aspect with battery solutions onboard marine vessels. The case study will investigate published documents related to the two accidents onboard the Norwegian ships MS Brim and MF Ytterøyningen. A secondary purpose with the separate battery fire survey is to investigate fire accidents to increase the understanding and supplement the STPA procedure.

The purpose of researching application of the STPA method for similar systems is to improve the quality of the application of the method which improves the validity and reliability of the findings. The STPA analysis will cover a preliminary analysis of Sundbåten's fire safety system including the interactivity with the human elements. One of the biggest strengths of the method is the model which allows the analyst to analyze a complex system. This essentially means that the method considers the interaction between all parts of the systems and not each component individually as various other traditional methods opt into. All steps in the STPA procedure are based upon flexible qualitative analysis which can be seen in the STPA findings. Key empirical data will be acquired and analyzed throughout STPA's four main steps which is described in section 2.2.

Figure 1 below represents the overview tree of the research methods forming the thesis. By combining these research methods, the design is intended to provide a basis to create a proper risk analysis of the system and answer the research questions in a satisfying manner. General data and information collection about the Sundbåten project is retrieved from private sources participating in the project. For this thesis in particular the goal of the selection of method(s) is to contribute to minimize the risk and unexpected events of the new battery solution onboard Sundbåten. That is why STPA is selected as the main research method.

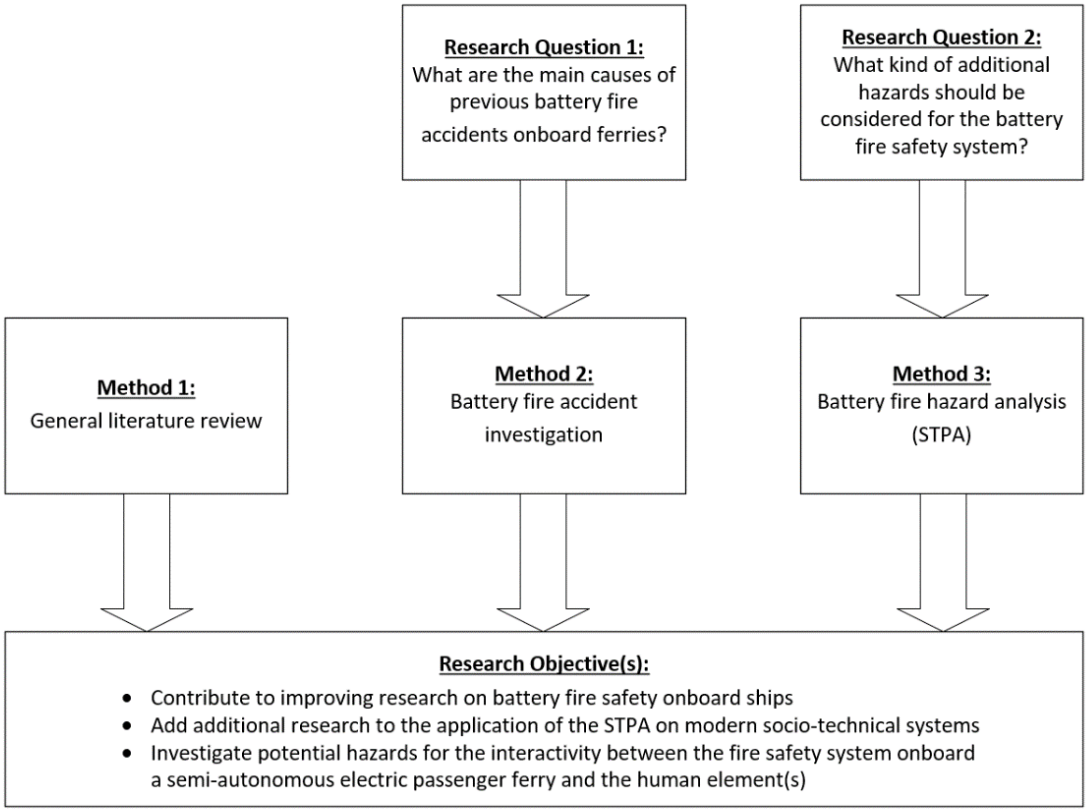

Research Question 1:
What are the main causes of previous battery fire accidents onboard ferries?
Research Question 2:
What kind of additional hazards should be considered for the battery fire safety system?
Method 1:
General literature review
Method 2:
Battery fire accident investigation
Method 3:
Battery fire hazard analysis (STPA)
Research Objective(s):
Contribute to improving research on battery fire safety onboard ships
Add additional research to the application of the STPA on modern socio-technical systems
Investigate potential hazards for the interactivity between the fire safety system onboard a semi-autonomous electric passenger ferry and the human element(s)

Figure 1 - Research Design

2.2 System-Theoretic Process Analysis theory

This section covers a brief overview of the application of hazard analysis method STPA's procedure in general. For this section and the application of the procedure in later section on Sundbåten's technical is highly based upon the procedure from Thomas and Leveson's STPA handbook (2018). Below is a figure representing a high-level overview of the STPA procedure. This is known as the standard procedure which this thesis will be based upon. The method consists of four main steps which will be briefly described in each paragraph below. For the main results of the application of the procedure see section 4 and appendix B for the full procedure.

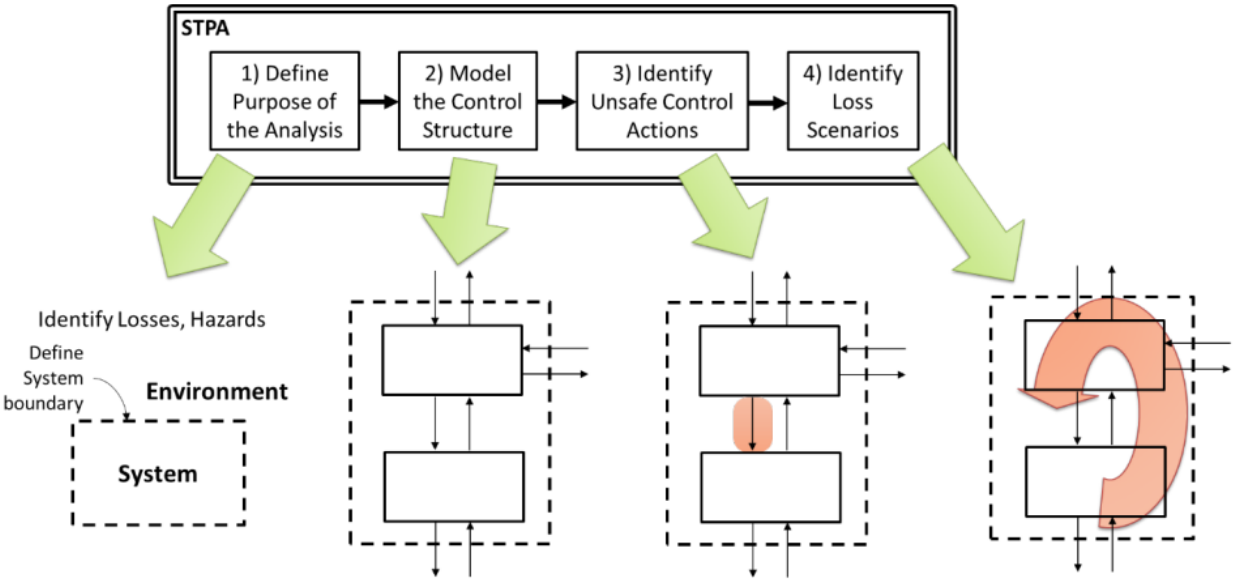

STPA
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios
Identify Losses, Hazards
Define System boundary
Environment
System

Figure 2 - Overview of the basic STPA Method (Leveson and Thomas, 2018)

Without clear system boundaries it can be difficult to really dive into the system as a whole and understand interactions between the different elements. Step 1 in the procedure is vital to define Sundbåten's system boundaries and its environment. The standard procedure includes three sub-steps identifying and defining high-level losses, system-level hazards and system-level constraints that are again related to these losses. To properly do this it is essential to have a clear idea of the scope of the system which is to be analyzed.

In step 2 the basis of the actual system to be analyzed will be defined by developing a model called Control Structure Model (CSM). This is a model representing the overview of the system intended to be analyzed. It is a well-structured CSM gives a great overview of the key interactions between the different controllers, controlled processes or other essential parts of the system. A CSM consists of boxes representing controllers, controlled processes, control actions, feedback and also in- or outputs which is not considered control actions or feedback. The CSM can is defined in the handbook like this: “A hierarchical control structure is a system model that is composed of feedback control loops. An effective control structure will enforce constraints on the behavior of the overall system” (Thomas and Leveson, 2018). The great advantage about visualizing the system with CSM and using control loops is the ability to understand the system as a whole and to anticipate unsafe interactions between the different elements including equipment, complex software, and human interaction. A well-made CSM is considered to be absolutely crucial in order to be able to identify unknown unsafe control actions leading to unacceptable losses. Following the CSM there is a set of tables describing the responsibilities of the control structure entities which is an essential part of defining the last two steps. These entities define the different controllers’ responsibilities at a deeper level to then understand its responsibility relative to the overall system to ensure that all defined system-level constraints are enforced. In other words, the tables include a list of responsibilities with related process models and feedback signals which essentially defines controllers in the CSM.

Step 3 is when the analysis is diving into defining potential unsafe control actions that can be causal factors leading to losses. “An Unsafe Control Action (UCA) is a control action that, in a particular context and worst-case environment, will lead to a hazard” (Thomas and Leveson, 2018). These actions are defined in the procedure and is the basis of the controller behavior that can lead to hazardous events if they are not prevented. First part of this step is creating tables for each key controller from the CSM described above. These tables act as a key tool to define each controller UCA’s. The tables include one critical Control Action for each controller with various situational scenarios to determine it shall be considered unsafe, safe, or not applicable. UCA has their own ID number with a reference to potential hazards defined in step 1.

Step 4 is the final step of the standard procedure. The purpose of this step is to define loss scenarios based on specific UCA's defined in the previous step. A "loss scenario" can be defined a possible causal factor leading to an unsafe control action which then leads to a hazardous event. Figure 3 below is created by Leveson and Thomas visualizes the two different types of loss scenarios that has to be taken into consideration. First is the unsafe controller behaviour which includes failures involving the physical controller, power failure, inadequate control algorithms, unsafe control inputs from other controllers and inadequate process models (Leveson and Thomas, 2018, p. 45). For type 2 it is generally issues related to feedback or information not being received from the controlled process as intended. This includes data from other processes, other controllers, other sources in the system or environment.

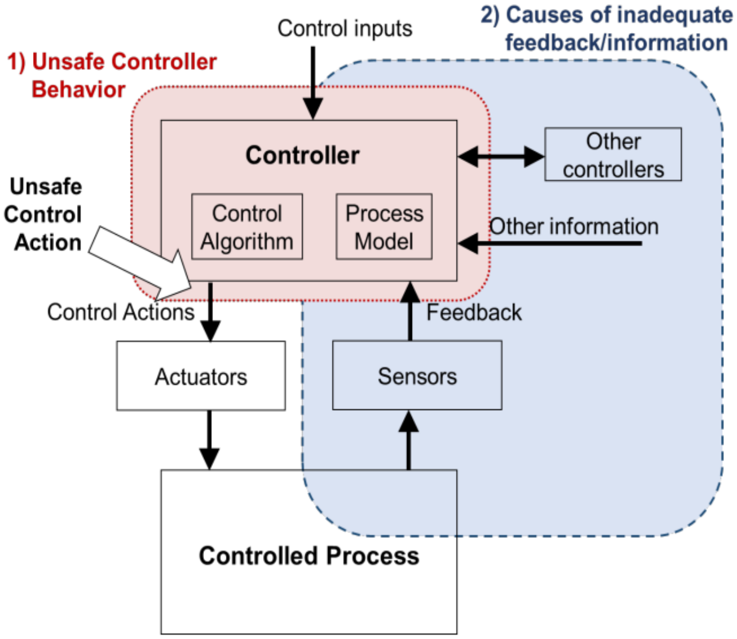


Figure 3 – "Unsafe Control Actions can be caused by (1) unsafe controller behavior and (2) inadequate feedback and other inputs (Leveson and Thomas, 2018, page 44).

The goal after conducting all these four steps is to have successfully identified previously unknown causal factors that could potentially lead to an unacceptable loss scenario. After key loss scenarios are identified and highlighted, they can in the future be based to identify functional requirements, design changes, safety procedures etc. that can help to drastically mitigate or even remove the risk.

3 Battery fire survey for ships

Battery systems is gradually becoming a more and more popular solution as a power source onboard marine vessel. At the same time, it has been an increased awareness of the potential risks due to recent accidents and the potential worst-case scenarios. But based on all the potential benefits of battery solutions it is highly likely here to stay. Most new and advanced technological development has a trial-and-error period before the best possible solution has been invented. Therefore, an important part of the continuing evolution of battery systems is to really take a close look on incidents in order to improve the technical solution and safety systems. It can be easy to be blinded by all the benefits of new state of the art green solutions but it is incredibly important to be realistic in terms of downsides as well. The conclusion is not at all to discredit battery solutions onboard marine vessels, but to raise awareness of the potential risk and safety solutions to counteract it.

This section is an in-depth investigation of lithium-ion battery fire theory and two extremely relevant battery fire accidents onboard the Norwegian vessels MF Ytterøyningen and MS Brim. The safety aspect of batteries onboard ships is at a relatively new stage which makes it absolutely essential to investigate relevant accidents as soon as they occur in order to further understand and develop the safety aspect and identify all critical causal factors. The structure of the report is split into three main parts starting with general theory on lithium-ion battery fire theory in 3.1 before separately analysing each of the two fire accidents in section 3.2 and section 3.3. Most published articles and reports related to the accidents from various sources have been investigated, organized and summarized for each of the accidents. For each of the accidents, there is an own section describing the course of events step-by-step. As a main literature source to recap the two events, a fire evaluation report from the fire departments will be used.

3.1 Lithium-ion battery fire theory

The purpose of the theory section is to gain a basic understanding of how the lithium-ion battery is functioning and potential causal scenarios. The battery will be briefly described before the causal factors and potential loss scenarios from battery heat and fire development is investigated. The theory below is based upon an article interviewing Sissel Forseth which is the leading researcher on power supplies for the Norwegian Defense Research Establishment (FFI). The article includes basic theory as well as essential information on how a fire can occur and how firefighters should handle the battery fire (Falkenberg, 2021). A typical Li-ion battery consists of four main components in cathode, anode, electrolyte and a separator (see figure 4). The separator is a type of plastic film and acts a safety function for the Li-ion battery. The electrolyte is a combustible liquid mix often consisting of various organic carbonates and salts. Since the electrolyte is a liquid, the separator prevents a short circuit between the anode and cathode. The downside with the plastic film is the plastic potentially smelting at high temperature approximately between 130°C and 160°C. At temperatures above 180°C, the cathode releases oxygen which essentially means the battery contains all ingredients to maintain its own internal fire.

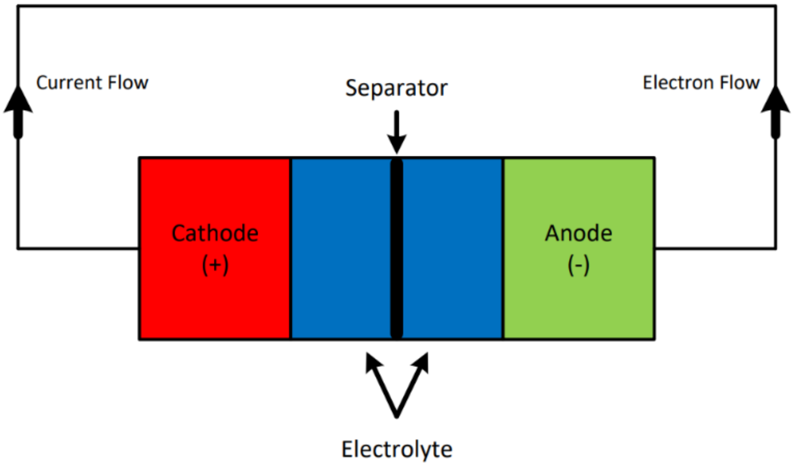


Figure 4 – Simplified figure based on figure on from an article from Zhang et al. on thermal safety for lithium-ion batteries (Zhang et al., 2018).

In the same article as above, Forseth shares interesting theory on how the fire and explosion occurs after being exposed to too much heat. When overheating, the electrolyte inside the battery will transition into gas. If the gas is not released, the continuously increasing pressure will eventually cause the battery to crack. As soon as the battery cracks,

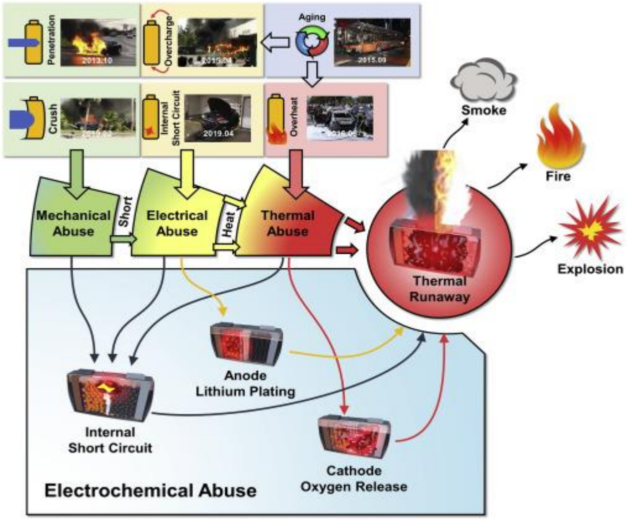


Figure 5 – "Conditions leading to battery failure" Huang et al., 2021. https://doi.org/10.1016/j.xcrp.2020.100285

flammable vapor from the electrolyte is released. If the battery then continues to self-heat, the cathode can then develop oxygen and combustible toxic gases such as methane, ethane, propane, hydrogen, carbon dioxide and hydrofluoric acid. The level of combustible gases that gets released is based on how much (Zhang et al., 2018)the battery is currently charged with in ampere hours (Ah). The potential release of toxic and flammable gases is the main reason to why battery fires are so dangerous inside closed compartments or rooms. This is especially relevant for marine vessels designed with own battery- and engine rooms with not much accessibility and limited ventilation capabilities.

“The flammable electrolyte is a potential hazard and in the last two decades, there have been several reports of fire and explosion related incidents caused by Li-ion battery failure” (Henriksen et al., 2019). There can be many different causes which leads to overheating and fire in a lithium-ion battery. No matter which causes it is, the battery is highly likely to start to continuously self-heat which will eventually leads to a heating snowball effect often referred to as thermal runaway. “The main concern of a battery system is that the temperature will rise to such level that it will go into thermal runaway. Thermal runaway is the exothermic reaction that occurs when a lithium ion battery starts to burn.” (DNV, 2019, p. 68). As DNV points out, these types of fires and heating scenarios is very hard to cool down and get control of. Mechanical abuse, overcharge, heat exposure, over-discharge, external and internal short-circuit are just some of the causes. Potential causes get especially tricky onboard ships where there are different conditions than onshore battery systems. See figure 4 below for an overview of causes and consequences on battery fires provided from DNV. For most of the causes in figure 3, DNV has a short description of each (Referring to document Technical Reference for Li-ion Battery Explosion Risk and Fire Suppression, page 68-70). Figure 6 on the following page is information based on DNV’s own publucation on lithium-ion battery explosion risk.

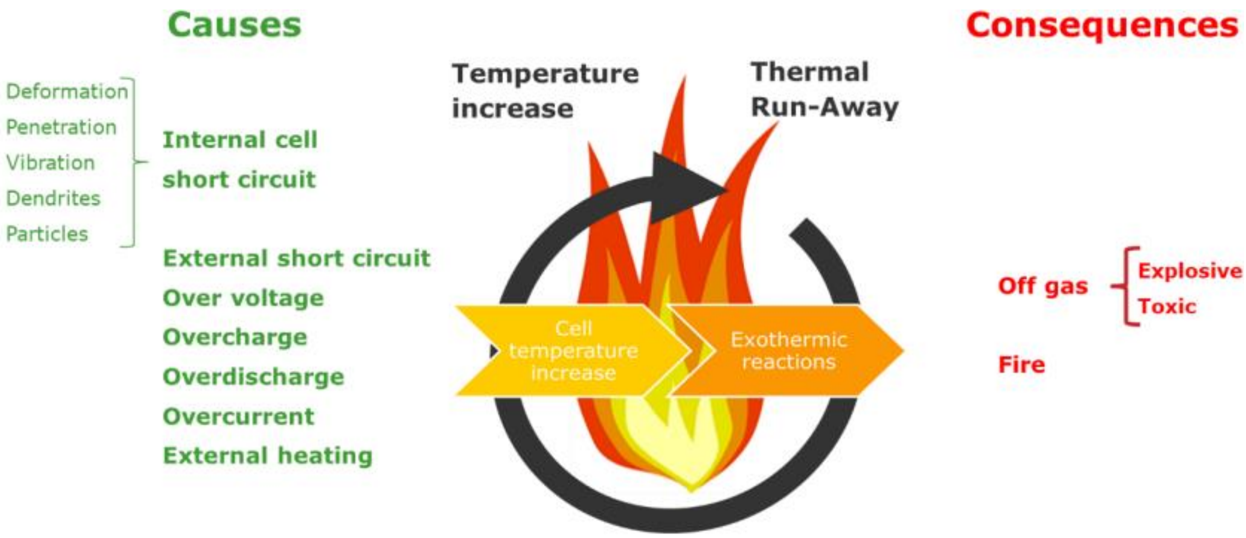


Figure 6 – «Battery Fire Causes and Consequences”. Retreived from DNV GL. *https://www.dnv.com/maritime/publications/Technical-Reference-for-Li-ion-Battery-Explosion-Risk-and-Fire-Suppression-report-download.html*

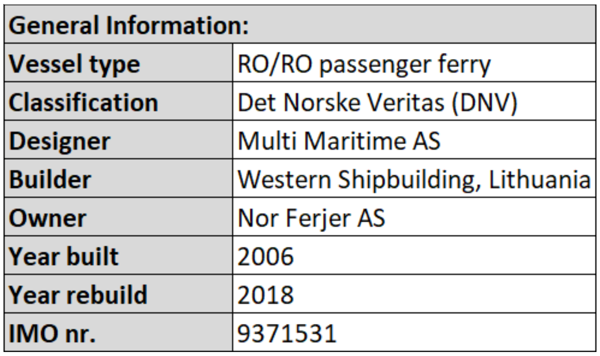
DNV points at thermal runaway as the greatest threat since the heat often exponentially increases and propagates throughout the rest of the battery. This obviously leads to potentially more released toxic and explosive gases with an increasing risk of explosion. “Battery modules and systems must be engineered to protect against propagation based on the cell that is used, and these cascading protections are the key feature with regard to system design for safety” (DNV, 2019, p. 68).

3.2 Battery accident report analysis – MF Ytterøyningen

3.2.1 Vessel information

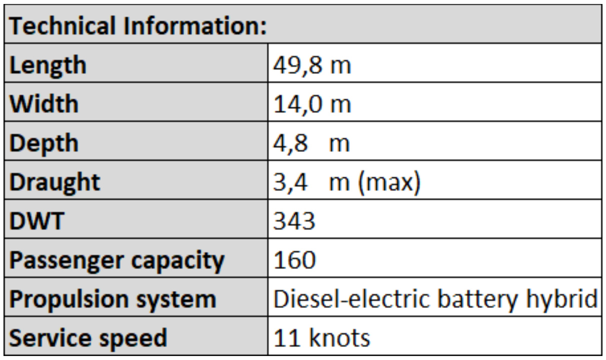
Table 1 and 2 on the following page briefly represent general and technical information about the vessel MF Ytterøyningen (Vest brann- og redningsregion, 2019). The vessel is a relatively small RO/RO passenger ferry. The ferry was built already back in 2006 with a diesel mechanic propulsion system but was rebuilt to a diesel-electric battery hybrid in 2018. The battery pack consists of 352 lithium batteries adding up to about 2 megawatts.

Table 2 – General information



General Information:	
Vessel type	RO/RO passenger ferry
Classification	Det Norske Veritas (DNV)
Designer	Multi Maritime AS
Builder	Western Shipbuilding, Lithuania
Owner	Nor Ferjer AS
Year built	2006
Year rebuild	2018
IMO nr.	9371531

Table 1 – Technical information



Technical Information:	
Length	49,8 m
Width	14,0 m
Depth	4,8 m
Draught	3,4 m (max)
DWT	343
Passenger capacity	160
Propulsion system	Diesel-electric battery hybrid
Service speed	11 knots

The technical design and fire safety system is a highly relevant topic for the safety aspect related to battery fire detection and handling systems. Below is a general arrangement figure of the vessel which also indicates the exposed rooms. Relevant for this investigation, the battery- and switchboard room onboard Ytterøyningen is located next to each other and separated by a self-closing fire door (see figure 5). The door separating the rooms is the only normal entrance to the battery room except a hatchet leading to deck. To enter the switchboard room ("Tavlerom" in figure 5), a hydraulic controlled door has to be opened. As for fire extinguishing systems the vessel was equipped with three different systems. First is a water sprinkler system using saltwater which had to be manually activated and covered both the battery- and switchboard room. Second system was an automatic gas extinguishing system delivered by Novac only covering the battery room. The third was an automatic foam based extinguishing system which covers both the battery- and switchboard rooms.

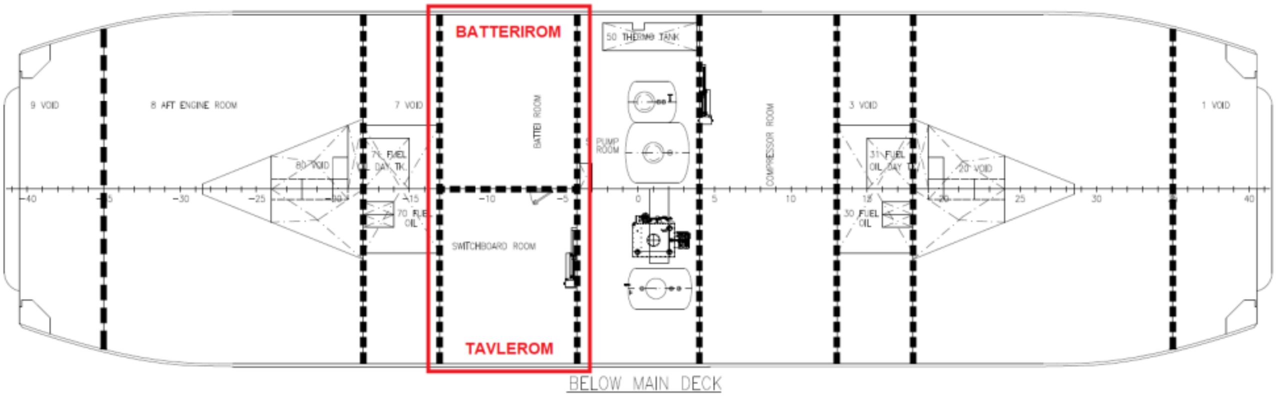


Figure 7 – «General arrangement MF Ytterøyningen». Retreived from fire report from Vest brann- og redningsregion, 2019, p. 6.

3.2.2 Overview of the fire accident

On October 10th, 2019, the fire department received a call about a fire onboard the diesel-electric battery hybrid passenger ferry MF Ytterøyningen. The ferry were a few hundred meters away from Sydnes port in Halsnøy in Norway when the fire department received the call about smoke development in the battery and switchboard room. When the accident initially occurred, the vessel was operating on diesel generators and not batteries. The batteries were not even connected to the power system due to an undergoing update by battery manufacturer Corvus Energy (Stensvold, 2019).

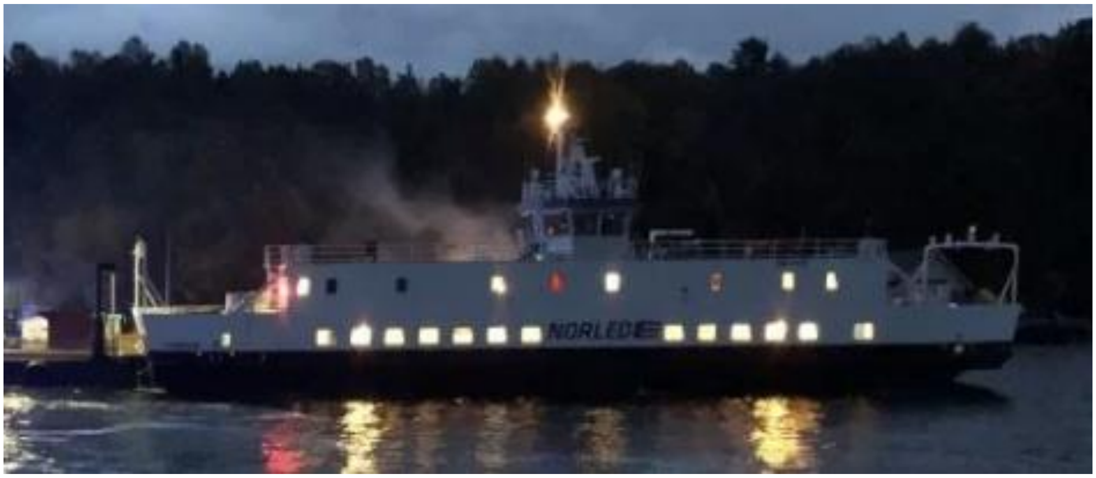


Figure 8 – MF Ytterøyningen fire accident. Image retrieved from IIMS. https://www.iims.org.uk/norwegian-maritime-authority-issues-warning-about-lithium-ion-power-following-ferry-fire-and-explosion/

It was initially alarmed that it was a fire in both the battery and switchboard rooms which are located next to each other in the middle of the ship (see "Batterirom and Tavlerom in figure 7). About 12 hours after the initial call the battery pack onboard the vessel exploded. The causal factor is yet to be confirmed in a final report from the authorities, despite the accident occurring years ago. After investigating the accident for almost two months, all parties have given indications that the initial causal factor is due to a leakage inside the battery pack. The battery pack used a water-cooling system which supposedly leaked coolant because of a twisted rubber gasket inside the battery. The leakage then led to electrical arc flashes causing a continuous increase of heat development which led to a fire. At the initial stage of the accident, the Battery Management System (BMS) were not even connected to the ships system which resulted in a late alarming of the heat, smoke and fire development. The installation of a salt-water sprinkler system near the battery pack were clearly a bad judgement as the salt-water initiated more short circuits after hitting the battery. Despite everyone involved were lucky to avoid any personal injuries, it was clear that the hazardous event had strong forces with critical and unacceptable loss scenario as even the fire trucks on the quay was damaged after the explosions. See figure 9 below for simplified overview of events.

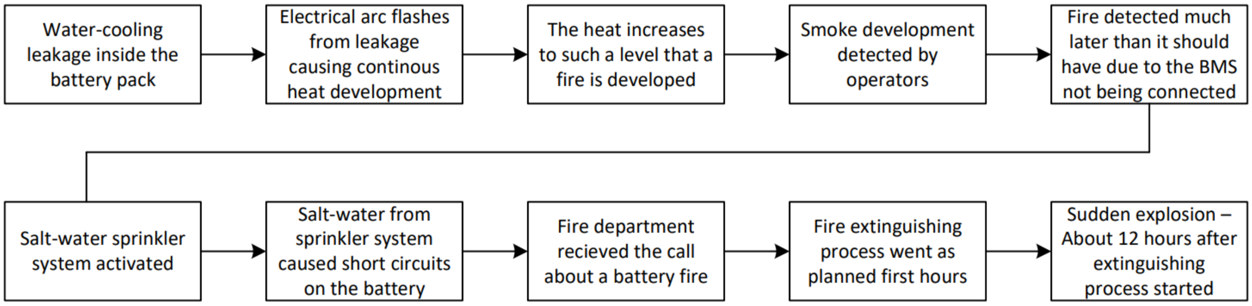

Water-cooling leakage inside the battery pack
Electrical arc flashes from leakage causing continous heat development
The heat increases to such a level that a fire is developed
Smoke development detected by operators
Fire detected much later than it should have due to the BMS not being connected
Salt-water sprinkler system activated
Salt-water from sprinkler system caused short circuits on the battery
Fire department recieved the call about a battery fire
Fire extinguishing process went as planned first hours
Sudden explosion – About 12 hours after extinguishing process started

Figure 9 – Overall summary of fire procedure onboard MF Ytterøyningen

3.2.3 Timeline of the accident – firefighters' perspective

To describe the course of events of the accident on MF Ytterøyningen in an accurate manner, the fire evaluation report published by the local fire department "Vest brann- og redningsregion" themselves will be used as a main source (Vest brann- og redningsregion, 2019). The regional fire department's organization is a cooperation between 19 different municipalities. The report is written and described from the firefighters' perspective. To get a good understanding of the situation, the recap is written step-by-step. All details in this section related to the event is taken from the fire evaluation report.

When the fire department received the call at 18:42 in the evening three people were onboard the vessel. They were informed about a fire inside both the battery and switchboard room which were located next to each other. Luckily for everyone involved the vessel was close to port at the time the fire occurred. Right away the leading firefighter called in additional smoke divers, coast guard, ambulance boats and a nearby fire station were alarmed. As soon as the firefighters arrived, the situation was first analysed from a distance without entering the vessel.

At this time a lot of smoke were observed, but there were no visible flames. At this stage the situation was declared to be a low risk and non-life threatening because the vessel was in port and all people evacuated.

Available information at this initial stage was quite limited. The fire chief was informed by the ship's crew members that work was currently being worked on and they believed the fire was not in the battery itself but nearby cables and/or equipment. They also informed about an attempt to extinguish the fire in the battery room but were unsuccessful before they decided to switch focus to evacuating the vessel. As for the fire safety system both the fire alarms and extinguishing systems were activated. The vessel was equipped with an automatic gas-based system and a saltwater sprinkler system. They added that they did not know if the gas extinguisher system had any effect on the fire. An interesting thing to notice is that the battery alarm itself had not been triggered. In the following procedure drawings of the vessel were provided by the crew to assist smoke divers on their mission to contain and control the fire. The area surrounding the vessel at the quay were defined as the "inner zone" which was strictly off limits unless people were equipped with suitable smoke diver equipment. Initial equipment prepared was a standard fire hose together with a compressed air for system (CAFS) which contained dry foam. The first attempt regain control of the situation were to inject CAFS foam into the emergency exit hatchet leading to the battery room. This hatched was initially measured to be 50°C at the time. A defensive strategy was opted into due to uncertainty from limited information as they pulled all smoke divers back to evaluate how to go proceed. The hatchet was after a short while measured again on the inside of the hatchet before pulling out again. Interestingly they measure similar values which could indicate a stable event.

Later on, it was decided to investigate the smoke development and if the battery room was completely tight by investigating surrounding rooms next to the battery room which was below deck. Smoke divers measured the temperature on the door leading to the switchboard room, which again is leading to the battery room (see figure 7). The door was measured to be 60°C and there were no signs of smoke development outside the two rooms. With a 20-minute gap the smoke divers were again ordered to measure the temperatures on the same two locations as previously. The hatch leading to the battery room had decreased to 35°C from 50°C. and the door leading to switchboard room 60°C to 40°C. Considering the temperature development, the fire was assumed to be deprived of oxygen and being extinguished slowly. Due to the downward trending temperature and no visible smoke development the fire chief announced 20:54 in the evening that the fire was under control.

Not long after, at 21:23, the situation escalated as more smoke were detected and it was quickly decided to try to extinguish the fire in the switchboard room. The procedure was considered low risk only because of the compact battery room with a self-closing door and fire walls. The smoke divers opened the hydraulic door leading to the switchboard room and used water. Shortly after the smoke divers pulled out of the vessel as they were exposed to a lot of smoke which caused very difficult working conditions. A new attempt was made at 22:07 but they quickly had to pull out because they were unable to open the hydraulic door leading to the switchboard room. New temperatures were then measured. Battery hatchet increased to 40°C from 35°C, switchboard room door from 40°C to 30°C and the hull outside the battery room to be 20°C. At 22:40 and 23:00 approximately the same temperatures were measured, which implies that the situation was again relatively stable. At 23:28 a decision was made to stay passive and only monitor the situation until the next morning.

An important factor to point out here is that during the initial stages the fire department were continuously gathering information on lithium batteries and the risk involved due to a lack of knowledge and preparation. During the night stable temperatures were measured in 15-minute intervals on the same spots as earlier. Early in the morning at 05:00 the crew decided to ventilate the battery room through the hatchet. Uncertainty quickly started to spread as the temperatures suddenly slowly started to rise. Not long after at 06:52 the same morning the fire station received a call requesting assistance as there had been an explosion on the ferry. Luckily there were no casualties or personal injuries, but fire fighters were described to be shaken. There were no visible flames, but they sat up safety borders 150 meters away from the vessel. Viewing the ferry through binoculars showed it was visibly damaged and lights were blinking. Everyone was ordered back and wait for battery specialists to arrive. After the explosion they quickly understood that a new issue with oil and diesel leakage. This was not prepared so they had to go and get an oil boom. It was informed by the crew that the only dangerous substances onboard were about 21 000 litres diesel and 40-50 litres of glycol stored in the battery room.

After some time, the fire department agreed that it was time to attempt to gain control. The smoke diver team prepared a normal hose and a drone with IR camera to monitor the situation from above (see figure 10). At 12:21 the hatchet leading to the battery room were measured to be 20-30°C. The infrared camera showed clear signs of heat surrounding the hatchet, but there were uncertain if the heat was from steam or other gasses. To clarify if there were hydrofluoric acid in the area, gas measurements were done both above and below deck but there were no findings at that time. At 13:26 fluoric acid was detected near the battery hatchet. One meter down the hatchet, 2 ppm were measured. At 14:07 a new measurement was done in the bottom of the battery room at 10 ppm. The battery room itself had major damage and the highest temperature were measured to be 70°C. At 15:34 divers were pulled out.

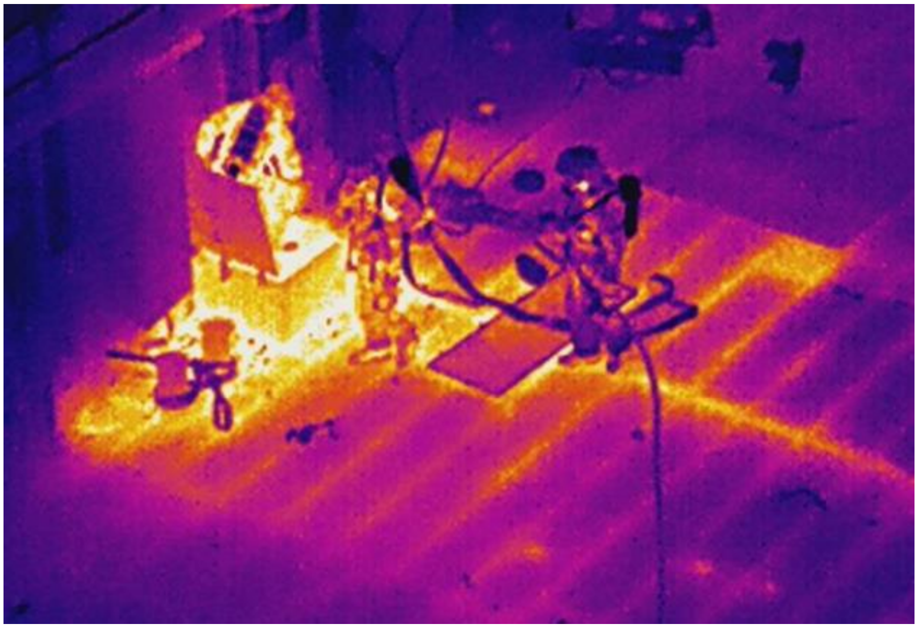


Figure 10 – "Infrared drone image of the battery room hatchet".
VIB. Retreived from: Vest brann- og redningsregion, 2019, p. 10).

Battery specialists wanted even more measurements but the fire chief called it off for safety reasons and preferred the gas to be siphoned out right away. At 16:33 the overall situation was calming down and there were no further actions until the ferry was dragged to a more appropriate spot the next day. As for medical consequences only one out of nineteen fire fighters showed symptoms of fluoric acid exposure. The symptoms were no longer showing after two days in the hospital and the person were sent home.

3.2.4 Fire departments' opinions and findings

This section summarizes the fire departments own opinions from the fire evaluation report on their experiences, conclusions, and future measures they will implement based on the event onboard Ytterøyningen. In general the situations were very demanding overall due to the scope and uncertainty since the local fire and rescue department had no previous experience related to battery fire in ferries. Due to the inexperience with similar events, uncertainty around risk factors and damage potential they opted for a passive approach which seemed to work well. As for simple measures setting up a safety barrier surrounding the area and having a minimal amount of personnel in close proximity to the vessel was a correct decision based on the lack of knowledge. They also recommend both these points as part of the safety procedure for similar hazardous events.

It is mentioned that it is of high importance to have a good flow of essential information between all the crucial parties involved. As a sidenote to this it is highlighted that it is very important to avoid misunderstandings and ensure that all work tasks get taken care of in all parts of the process. Due to the criticality of the type of situation and time intense events, it is obviously important to remove all unnecessary and disturbing elements. As an example, it is mentioned in the report that the battery specialists which were summoned did not provide much help and were instead a disturbing element in the process. As for technical findings they point out that based on the course of events and knowledge acquired in retrospect shows that overheating of batteries inside closed spaces makes explosion a great danger. The use of drone with an advanced infrared camera to provide video images of the thermal energy on the vessel was very beneficial to get the valuable information and a better understanding of the situation. Of medical matters luckily there was no personal injuries and the collaboration with the medical team worked well. As soon as one fire fighter showed symptoms on fluoric acid exposure, all other potentially exposed fire fighters were examined and observed until declared safe.

Regarding research and knowledge on the matter it seems clear that there is room for improvement. They mention that it is insufficient knowledge available on lithium-ion battery fire and the hazardous gases and not sufficient knowledge on battery fires within the fire department. The fire department itself concludes that they have not followed the development of the battery technology which led to them not being prepared for this type of situation. Prior and during the accident they had some knowledge about hydrofluoric acid and the potential danger of batteries leading electricity after a fire occurs, but not enough. For the fire department to handle the same type of situations in the future they are clear on having to update all analyses related to risk, emergency- and prevention. After the accident new initiatives have already been taken by the fire organization "Vest brann- og redningsregion" to gather expertise on battery technology. Their purpose is to map out if there is sufficient research and knowledge to be able to create proper safety guidelines on how to handle battery fires in the future, or if more research is needed. They conclude with the fact that based on existing knowledge and experience new guidelines has to be made no matter what. They also point out that in order to prepare as well as possible special units for each region should be established for similar situations and be ready to assist at any time. It is also mentioned that evaluation routines of events should be reviewed to ensure that the situation was handled efficiently and to best learn from the process overall.

3.2.5 Cause of accident – Investigation and findings

The local police lead the investigation about a week after the accident. The investigation was in collaboration with Norwegian Maritime Authority, KRIPOS, Norled, Corvus Energy and other subcontractors in order to find the cause of the fire leading to an explosion. It took approximately 6 days after the explosion for the investigation to start, which the police said was due to inefficient coordination of everyone who had a purpose in participating (Stensvold, 2019).

Two months after the accident an article was released which points at the most likely cause. All parties investigating were relatively certain that the initial cause was due to a twisted rubber gasket from the water-cooling system inside the battery pack were leaking between a cooling plate and a 1000V battery module creating electrical arc flashes (Stensvold, 2019). The electrical arc flashes developed more and more heat inside the battery, which eventually caused a fire. It was also pointed out that there were various unfortunate reasons to leading to the leakage and arcs not being detected, which could stop it from developing a fire. Both the coolant leakage from the battery water-cooling system and the heat development were not detected before it was too late because the Battery Management System (BMS) were not connected to the ships system. The battery manufacturer Corvus reported that the explosion itself was likely due to the salt-water sprinkler system itself, which were installed to increase the fire safety (Anthun & Lura, 2019). They mention that the salt-water likely contributed to even more short circuits which resulted in an explosion. The newly installed sprinkler system inside the battery room had been approved by authorities prior to the accident. Corvus emphasized that they had no responsibility of the sprinkler implementation. The battery pack was 1980kW and consisted of water-cooled lithium-ion batteries of Orca ESS. MF "Ytterøyningen" is the first hybrid ferry with water-cooled battery pack, which was approved April 2019 (Anthun & Lura, 2019).

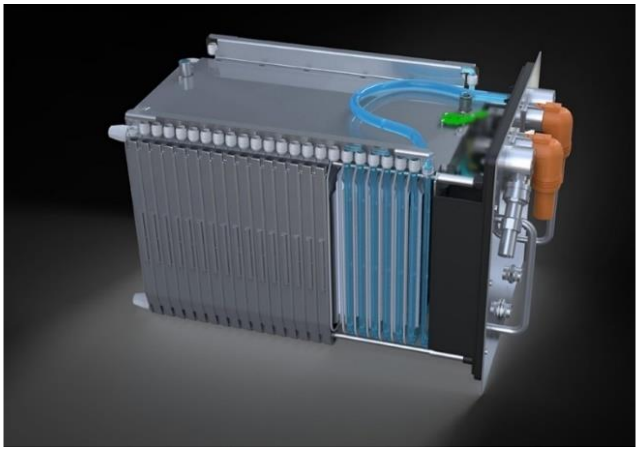


Figure 11 – «Water-cooled battery». Image retrieved from Sterling PlanB Energy Solution.. https://spbes.com/products/planb-cellcool/

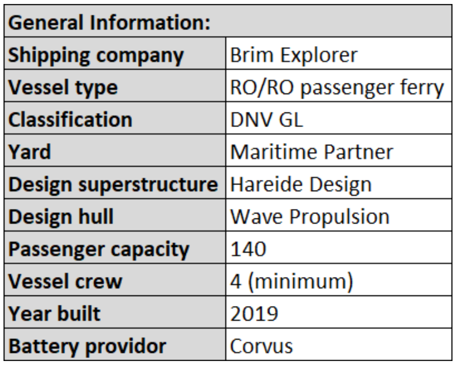
The Norwegian Maritime Authority in collaboration with battery producer Corvus published a safety message a few days after the accident that all battery systems onboard ships had to be connected to ensure connection with alarm and failure systems. In the same security alert, they encouraged all vessels with battery systems to perform a new risk analysis on gas development from battery incidents. (Stensvold, 2019). The days following the explosion same two parties together with Norled also recommended that all owners and/or operators of electrical battery systems are encouraged to perform new risk analyses on hazards related to gas development from battery fires and heating (Lura & Olsen, 2019).

3.3 Battery accident report analysis – MS Brim

3.3.1 Vessel information

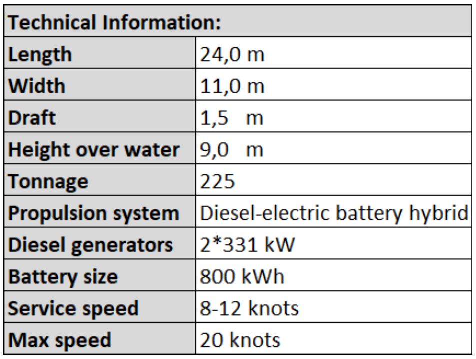
The vessel MS Brim is a relatively small passenger catamaran owned by Brim Explorer. The DNV classified vessel is a diesel-electric battery hybrid catamaran capable of carrying 140 passengers. The vessel mainly uses batteries while sailing but has diesel generators as back-up and in case the system needs longer range or more electrical power. Total cost of the project is 46 million NOK. Below is general and technical information (Vestfold Interkommunale Brannvesen IKS, 2021):

Table 3 – General Information MS Brim



General Information:	
Shipping company	Brim Explorer
Vessel type	RO/RO passenger ferry
Classification	DNV GL
Yard	Maritime Partner
Design superstructure	Hareide Design
Design hull	Wave Propulsion
Passenger capacity	140
Vessel crew	4 (minimum)
Year built	2019
Battery providor	Corvus

Table 4 – Technical Information MS Brim



Technical Information:	
Length	24,0 m
Width	11,0 m
Draft	1,5 m
Height over water	9,0 m
Tonnage	225
Propulsion system	Diesel-electric battery hybrid
Diesel generators	2*331 kW
Battery size	800 kWh
Service speed	8-12 knots
Max speed	20 knots

The general arrangement below shows that each side of the catamaran from the middle line is mirrored and has one battery- and engine room each.

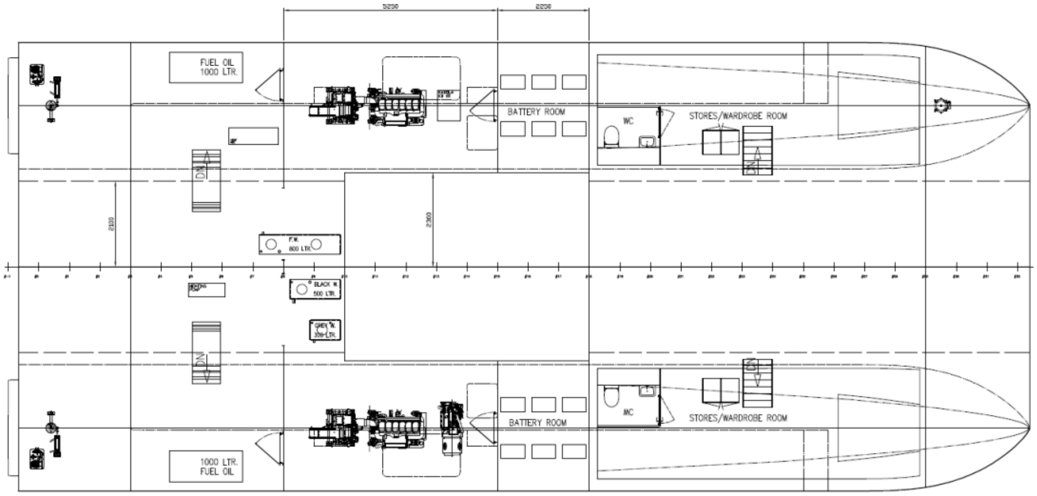


Figure 12 – «Overview of vessel and truck setup». VIB. Retreived from: https://www.facebook.com/brannvesenet/posts/3756751254409973

3.3.2 Overview of the fire accident

On March 11th, 2021, the fire department received a call about a fire inside the engine room onboard the diesel-electric battery hybrid catamaran MS Brim. At the time there was only 4 operators onboard the vessel and no additional passengers. Due to the smoke development fire the operators were picked up by another vessel as the catamaran was dragged Vallø port in Tønsberg. The accessible quay allowed the task force to perform the extinguishing procedure as easy as possible. Awaiting the vessel in Vallø, the task force used the evaluation report from the accident onboard MF Ytterøyningen as part of the preparation.

Fires in lithium-ion batteries is known to release toxic and explosive gases. Due to the tight compartments below deck the battery manufacturer Corvus Energy advised to siphon out explosive gases while supplying nitrogen to reduce the chance of explosion. The proposal was approved by leading researcher on power supplies from the FFI. After various challenges the method was a success in order to gain control of the battery fire. In the end there was no explosion nor personal injuries, which is likely due to the way the situation was handled from start until finish. From the initial rescue call until the vessel was considered safe and handed over to police was 7 days. The main challenge to regain control of the situation were the accessibility and ventilation solutions to the battery- and engine room. Based on a passive, well thought out process based on advice from various specialists with different expertise it turned out successfully. See figure 13 below for an overview of the situation.

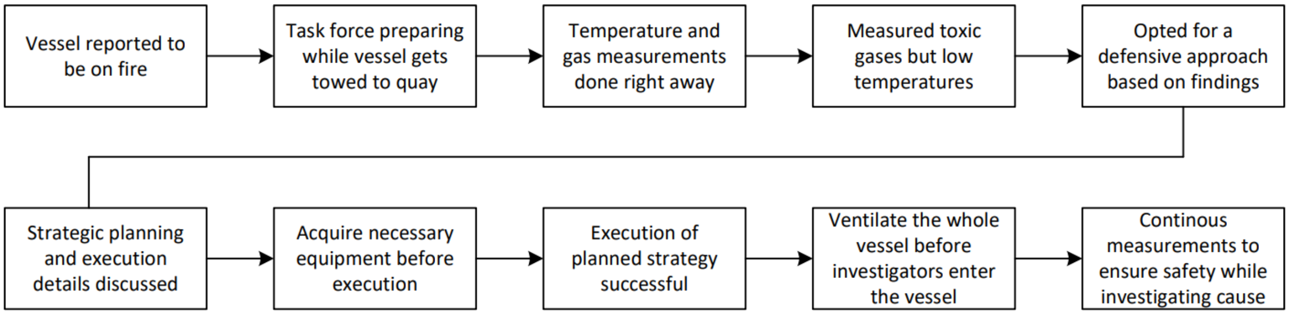

Vessel reported to be on fire
Task force preparing while vessel gets towed to quay
Temperature and gas measurements done right away
Measured toxic gases but low temperatures
Opted for a defensive approach based on findings
Strategic planning and execution details discussed
Acquire necessary equipment before execution
Execution of planned strategy successful
Ventilate the whole vessel before investigators enter the vessel
Continous measurements to ensure safety while investigating cause

Figure 13 - Overall summary of fire procedure onboard MS Brim

3.3.3 Timeline of the accident – firefighters' perspective

To describe the course of events of MS Brim, the evaluation report published by the local fire department "Vestfold Interkommunale Brannvesen" (VIB) will be used as a main source. (Vestfold Interkommunale Brannvesen IKS, 2021). The recap is written and described from the firefighters' perspective.

The initial call about fire were received 16:14 on March 11th. At the time of the call the vessel was at sea. Due to the possibility of the fire being from or near the battery room the fire department used the time from the emergency call until the vessel was moored to the docks to plan a best possible response. With the experience from Ytterøyningen and acquired knowledge on battery fires they knew that toxic gases and explosion were potential dangers from battery fire events. The planning included organization of role distribution, what safety gear and equipment they could potentially use. While the initial response team were on their way to the port, they received information about there being less smoke than it previously was. At this time the battery manufacturer recommended the response team to act as soon as the vessel was moored. As a precaution for possible hydrofluoric acid exposure the emergency crew opted for splash suits. The ambulance was also ordered to stand by in port.

At 19:40 the vessel was at the quay. To get an understanding of the situation gas and temperature measurements were done right away. Two firefighters measured the battery room door to be only 30°C. Despite the low temperature, carbon monoxide and explosive gases were detected in the engine room. The two fire fighters suddenly got an odour of either gas or smoke inside the mask and pulled out immediately. The equipment is intended to be completely tight with an overpressure from within to avoid these scenarios. Both were decontaminated and given oxygen right away while waiting for the ambulance to be checked. Arterial blood gas test at the hospital showed normal values for both. At this stage it was opted for a more defensive approach by measuring from the quay and not the vessel itself before making a new strategic plan. Early next morning it was decided to take new measurements inside the boat. Various kinds of gases got detected right away which was reason enough to pull out of the boat again right away. At this point they established their base around 300 meters away from the vessel while measuring gas and temperatures of the hull while being on shore. As for procedure planning a meeting with various important parties such as firefighters, police, coast guard, advisors and more was held. Their conclusion on the biggest risk at this stage was a possible explosion and preparations was made thereafter. A decision was made to put up a 300-meter safety sone in all directions as well as oil booms in the water in case of an oil spill.

The ships battery rooms have A-60 fire doors installed which is supposed to keep the room completely tight. Measurements outside the battery room detected gas without opening the door which confirmed that the room were not completely tight as it was supposed to be. The explosive gases leaking from the battery room were gathering up below deck and based on a suggestion from battery manufacturer Corvus Energy, the new strategic plan was to siphon the gases out in a controlled manner (see figure 14 below). The purpose of siphoning the gas out is to avoid the gas being spread throughout the vessel to maintain as much control as possible. If the gases spread out too much, the task force would have no control of the flammable gases. The plan also involved to add nitrogen to displace the oxygen in the air to prevent an explosive gas mix.

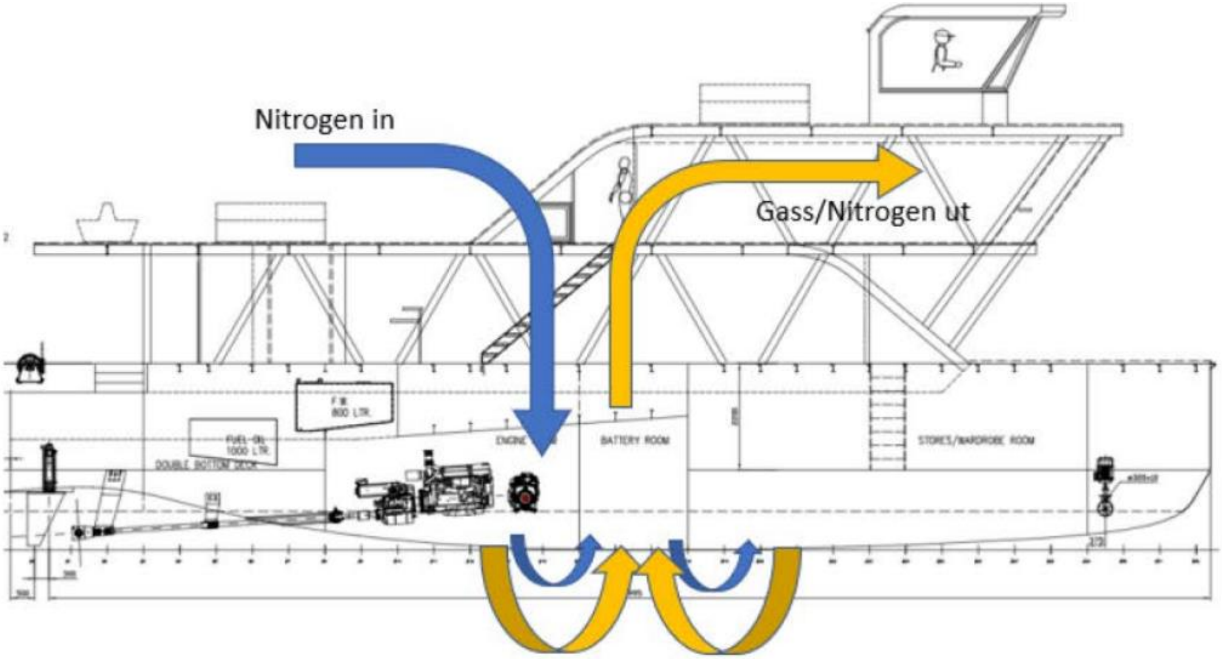


Figure 14 – "Execution plan based on suggestion from battery provider". Retreived from: («Vestfold Interkommunale Brannvesen IKS – Evaluering av MS Brim» p. 10).

The idea of circulating the explosive gases out is theoretically straight forward, but the procedure turned out to be quite the challenge due to the accessibility- and ventilation design of the battery- and engine room. The biggest challenge as obviously to maintain the safety of the task force attempting to regain control of the situation. Other challenges were planning of the execution and acquire necessary equipment such as safety gear, nitrogen supply tanks, equipment to properly connect supply and extract hoses.

The execution details were still being discussed Saturday morning. From the discussion it was decided that they were going to take their time and not rush the execution of the plan. Despite some level of uncertainty, Sissel Forseth, the leading researcher for Norwegian Defence Research Establishment (FFI) approved the theoretical solution. She also assisted in the further planning. Clear priorities were pointed out from the discussion between all parties in a specific order in human lives, health, pollution and lastly material. A Safe Job Analysis (SJA) was the foundation for the next stages. They planned to finalize the risk analyses and preparations Sunday and execute the plan on Monday. In collaboration with the coastguard and local port authorities, about 950 meters with oil booms were put out in a ring approximately 300 meters out from the vessel. This measure is mainly to avoid pollution but also to ensure that other vessels does not enter the safety zone.

On Sunday all parties participating were a part in the risk assessment process. This included the staff, various specialists and the task force entering the vessel. The execution plan itself was proposed by a representative from the battery manufacturer. The plan was to supply nitrogen through the engine rooms ventilation system while siphoning the gas from the battery room through a ball valve. A result of the risk assessment several good measures were brought to the table, uncertainties were cleared up and all parties established a common understanding on the whole situation. Three points from the meeting which had to be investigated was the nitrogen connection plate on the ship, the nitrogen truck’s gas flow as well as the outlets. After the risk assessment meeting the task force started practicing on critical tasks based on the risk analysis. A plate constructed to supply nitrogen through a damper was tested on the other side of the catamaran which is equal to the exposed side. This was to minimize the risk of unwanted events and get a feel of the process. After measuring low enough gas levels on the exposed side of the catamaran, the task force went ahead and prepared the execution by loosening bolts on relevant flanges. The truck intended to supply nitrogen had no measuring instruments to know how much gas it was sending out which was not ideal. As preparation to be able to control a balanced level of gas, they practiced on special bags to figure out how much gas which was being filled per hour. New details in planning were made based on these tests. A set date of execution was now March 15th which was 4 days after the initial call.

On Monday morning the goal, strategy and risk factors were carefully explained before the plan was executed. Fire trucks, gas trucks, equipment etc. were placed accordingly based on different zones around the vessel which had been established (see figure 15). They used one truck to supply nitrogen and one truck used to suck out gases. The figure below represents the execution setup. The yellow represents the nitrogen truck and hose, while the blue represents the extraction truck, hose and area it releases the gas.

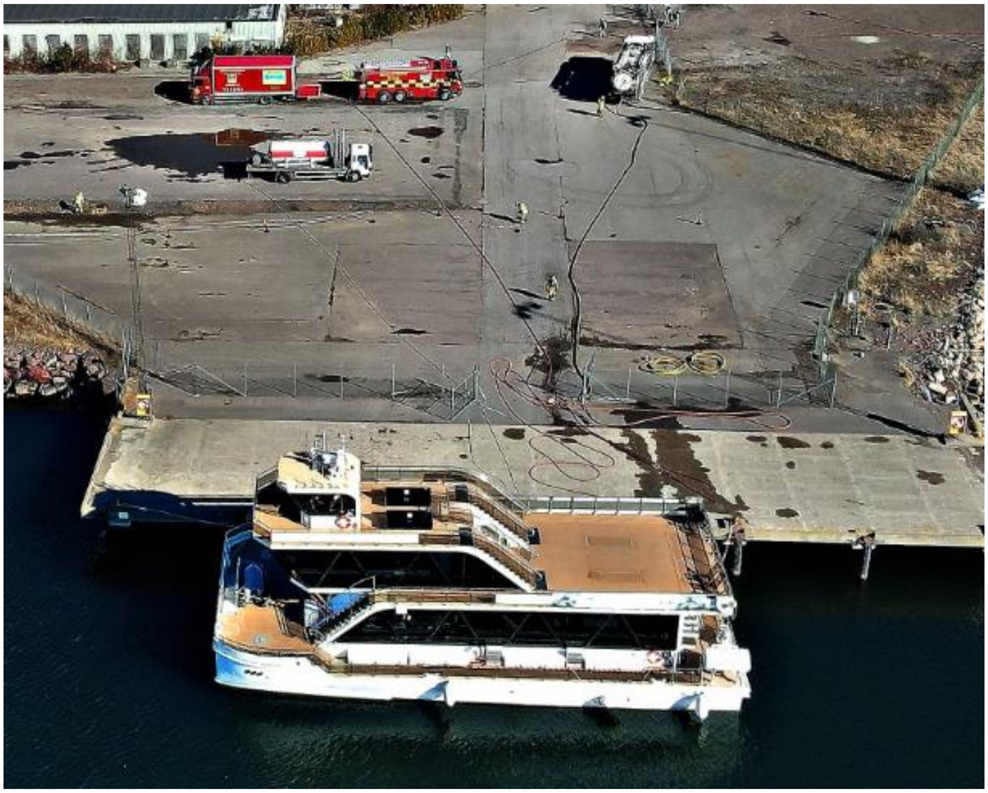


Figure 15 – Strategic overview of the MS Brim procedure. Image retreived from Vestfold Interkommunale Brannvesen

As the operation started drone technology was used to maintain a good overview of the situation. Continuous temperature and gas measurements were taken and IR cameras were diligently used. The task force was equipped with four gas meters to detect explosive and toxic gases as well as low oxygen levels. The representative from battery manufacturer Corvus Energy led the walkthrough of the procedures of supplying nitrogen, gas extraction and measurements. The first step of the onboard procedure was to connect hoses to extract and supply gases. To supply nitrogen the hose was connected to the ventilation system from deck which led to the engine room. The suction hose was connected to a ball valve to extract gas from the battery room. After properly connecting the two hoses, the task force withdrew to a safe distance from the vessel. The most critical part of this process was the first hour. All crews were called back to safe zones as they started the procedure. Nitrogen was supplied for about an hour before extraction of gases started. Infrared drone images were essential at the initial stage to detect temperatures becoming more and more cold. After an hour of supplying nitrogen, they measured -23°C on the extraction hose flange and -3°C on the nitrogen supply entrance. The low temperatures were a deciding factor to start the extraction of gases. The ventilation process creates a circulation of gases inside the hull as they suck out the gases. Temperature measuring keeps getting taken as the process is going on. New measurements show signs of explosive gases being extracted from the vessel which was a strong indication that the plan was working as intended. Continuous measurements for the next three hours showed signs of decreasing levels of explosive gases. The nitrogen supply tank was supposed to be able to supply for nine hours but was empty after three hours. It was decided to continue the extraction despite not having more nitrogen supply. This extraction process continued overnight.

In the morning there was low enough explosive gas levels to reduce the safety zone distance and start onboard hull measurements. Based on the positive measurements they decided to disconnect the nitrogen supply hose and ventilate the boat. To effectively ventilate the vessel, they created a negative pressure from the suction truck. The negative pressure was increased in intervals from -0,1 bar up to -0,4 bar. Measurements on the air being sucked out showed a decreasing level of explosive gases. This went on until the atmosphere was /declared non-explosive, and the task force got a green light to enter vessel to proceed with measurements below deck. Before entering, the crew went through a Safety Job Analysis (SJA) with the safety coordinator to ensure the safety. They used video images from a sistership as well as drawings to prepare the task force entering the vessel.

Entering the engine room, they did not detect any abnormal gases and measured the temperature to be 4°C. Approaching the door leading to the battery room low levels of hydrofluoric acid was detected. When they got down below deck, they did not manage to open the battery room door. Initially they thought that was due to the possible vacuum due to the circulation process. As an attempt to open the door they stopped the pressure created from the suction truck, but still could not manage to open it. After picking up equipment they managed to open the door which seemed to be stuck due to a smelted gasket surrounding the door. After entering the battery room, it was completely burnt down.

After measuring a temperature of 7°C and not detecting abnormal gases inside the battery room, they pulled out. All possible windows and hatchets were then opened to create a natural ventilation of the vessel. The suction hose also got disconnected. All of the people who entered the vessel got decontaminated. To ensure that there was not going to be an unexpected scenario they continued to measure gas and temperatures throughout the next night. The firefighters' finishing contributions were to facilitate for the accident investigators. First of all, the vessel had to confirmed to be clear of toxic and explosive gases before the investigation started. As part of this process, hatchets were opened to improve the atmosphere and starting batteries to engines on both sides of the catamaran were disconnected. The remaining work was mainly to assist the fire specialist from Kripos in the investigation inside the battery- and engine room and the vessel itself.

3.3.4 Fire departments' opinions and findings

This subsection is strictly based on the local fire departments own evaluation report (Vestfold Interkommunale Brannvesen IKS, 2021). Evaluating the event in hindsight several key factors were identified. In general, the overall risk assessment prior to the execution phase was considered an extremely important element. This was essential in the planning phase to clarify the procedure for all parties involved. This allowed all different parties to express opinions contributing with their expertise. Several good resources and specialists were present and were very valuable and ensured a high quality on decisions and procedures. Especially beneficial was representative from Corvus Energy and FFI to share knowledge on batteries and thermal events. Certain issues were addressed and the plan adjusted to increase the safety and efficiency of the procedure prior to execution. It is mentioned that the resource composition was a key to a successful operation. As a general conclusion they say that it is incredibly important to organize properly and efficiently to be able to utilize all resources as much as possible. It is also mentioned that a very beneficial point in the planning phases that the task force designated to enter the vessel could be part of the risk assessment and equipment preparations prior to executing the plan. Similar to the event on Ytterøyningen a defensive approach from the beginning was taken and considered a big success factor in hindsight. Fire in battery was a new experience for most parties since there has not been many similar situations previously. Despite the insufficient knowledge within the field of lithium-ion batteries as a starting point, they acquired many different learning points.

As for positive points the fire department seemed to take many good decisions. After receiving the call about a battery fire, the decision to place the vessel in an open accessible spot was one of the most deciding success factors. It greatly helped the process of regaining control of the situation and to set up boundaries for people not participating. The partnering with the external drone specialists turned out to be a great asset. The use of infrared cameras they had a good overview over the vessel and the procedure mid execution and was very helpful in order to make quick and decisive decisions. In terms of HMS there is not much research on hydrofluoric acid’s ability to penetrate firefighting equipment. With existing knowledge and experiences the VIB had, it was decided to use firefighting suit, additional breathing air supply, splash suits and gas meters whenever they were near the vessel. Normal splash suits protect against chemical spill but are not completely gas tight. This is why it is so important with frequent use of gas meters. If the crew are in near proximity to toxic gases which are hazardous when in contact with skin, such as hydrofluoric acid, it is critical to detect. The fear of explosions is also obviously high for smoke divers getting closer to the battery room. As a tool they frequently used gas meters which essentially works as a protective equipment and was reported highly successful to make the task force feel safe and to quickly take critical decisions based on gas findings.

Despite a good risk assessment and planning several challenges were identified after evaluating the process. First of all, the vessel was not designed to handle this type of situation inside the battery room. A challenge that could have easily been avoided was the custom flange that had to be made to connect the suction hose during the ventilation process. This could easily be more efficient if it was designed for the purpose. The nitrogen supply emptied much earlier than planned which again shows clear lack of preparation for such scenarios. Another important point which others should learn from as well is that it is mentioned that the task force could have good use of more practise regarding similar fire safety procedures. VIB were also clear on having to improve the use of measuring equipment, alarms, and interpretation of measured results. In terms of communication, it was agreed in the review that they should have had more internal staff meetings since there was so many external parties involved. To conclude they are also of the opinion that there is insufficient knowledge on battery fire onboard vessel prior to the accident led to several challenges. Limited resources were also an issue. Major learning points is that competence, procedures, and the definition of battery fires has to be improved both internally and on a national level. VIB also encourages other organizations to use the report to see how their fire department solved the situation from start to finish.

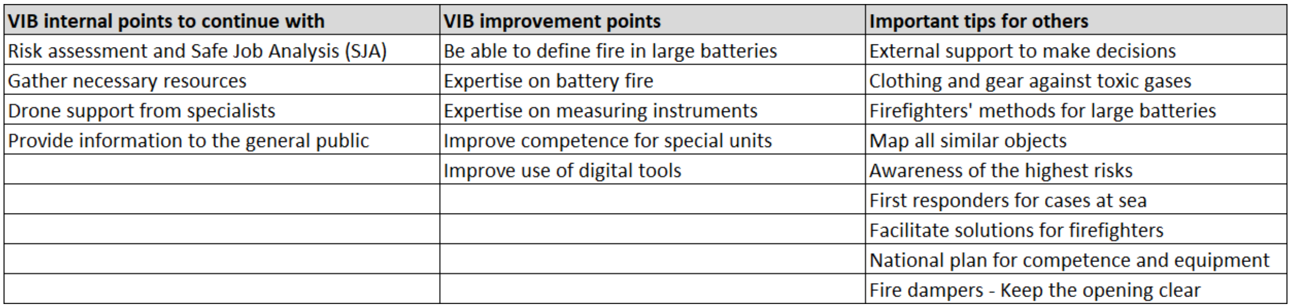
3.3.5 Cause of accident – Investigation and findings

Although the final conclusion is yet to be confirmed in the accident report from "Norwegian Safety Investigation Authority" a strong indication is an article published by The Norwegian Maritime Authority (NMA) about two weeks after the accident. MS Brim's sistership Bard was ordered to improve a design challenge detected in the investigation of the accident, which can be interpreted as a possible cause of accident. "In connection with our review of documents and information from the parties, the NMA has identified a design challenge in the ventilation arrangement, which could have led to the incident where sea/salt water leaked into the battery room" (Nilsen, 2021). It is reported that about two months after the accident that The Norwegian Safety Investigation Authority is currently doing surveys and instigating the accident and will provide a report within a year (Stensvold, 2021). So, despite them being able to successfully evacuate the vessel and regaining control of the situation, in a worst-case scenario with passengers it could end in a catastrophic manner due to an unexpected and unpredictable causal factor.

3.4 Summary of fire accidents

Referring to both accidents there should be no doubt about the criticality and possible worst case scenarios for battery solutions onboard ships. Most key points from both accidents are quite similar other than root causal factors which is most likely a cooling water leakage onboard Ytterøyningen and sea water entering the battery room ventilation system onboard Brim. There are quite a few negative takeaway points from both accidents. Clear lack of experience and knowledge of both safety and risks of lithium-ion batteries and the handling of them during fire events. Other negatives are lack of procedure preparations, ineffective basic fire extinguishing systems, inaccessible exposed rooms, ships not designed to handle these types of events and more. There are not too many positive takeaway points from either of the accidents other than a heroic effort from the response teams, no personal injuries, and the incredibly valuable experience with responding to battery fire events in ships. From the two accidents it surely is key to be as ready and prepared as possible for various hazardous events to minimize risk and avoid fatalities and major structural damage. Below is a table based on a summary from the fire department themselves from the accident onboard MS Brim: retrieved

Table 5 – VIB learning points from MS Brim, information from fire evaluation report (Vest brann- og redningsregion, 2019)



VIB internal points to continue with	VIB improvement points	Important tips for others
Risk assessment and Safe Job Analysis (SJA)	Be able to define fire in large batteries	External support to make decisions
Gather necessary resources	Expertise on battery fire	Clothing and gear against toxic gases
Drone support from specialists	Expertise on measuring instruments	Firefighters' methods for large batteries
Provide information to the general public	Improve competence for special units	Map all similar objects
	Improve use of digital tools	Awareness of the highest risks
		First responders for cases at sea
		Facilitate solutions for firefighters
		National plan for competence and equipment
		Fire dampers - Keep the opening clear

4 STPA result - Sundbåten

This section only contains key results and a brief introduction to each step of the STPA procedure applied on Sundbåten’s fire safety system taking the human elements into consideration. The version of the STPA method conducted in this thesis follows the standard procedure from Thomas & Leveson’s handbook. For the second part of step two as well as the remaining parts of step 3 and 4 only one controller will be presented in section 4. For the full procedure and remaining parts of the other controllers see Appendix B.

3.5 Step 1 – Define Purpose of the Analysis

To define the boundaries of the risk analysis figure 16 below is the basis for the thought process during step 1. Definition of losses, system level hazards and system level constraints can be found in table 6, 7 and 8 below. These results is the foundation of the next steps and final findings.

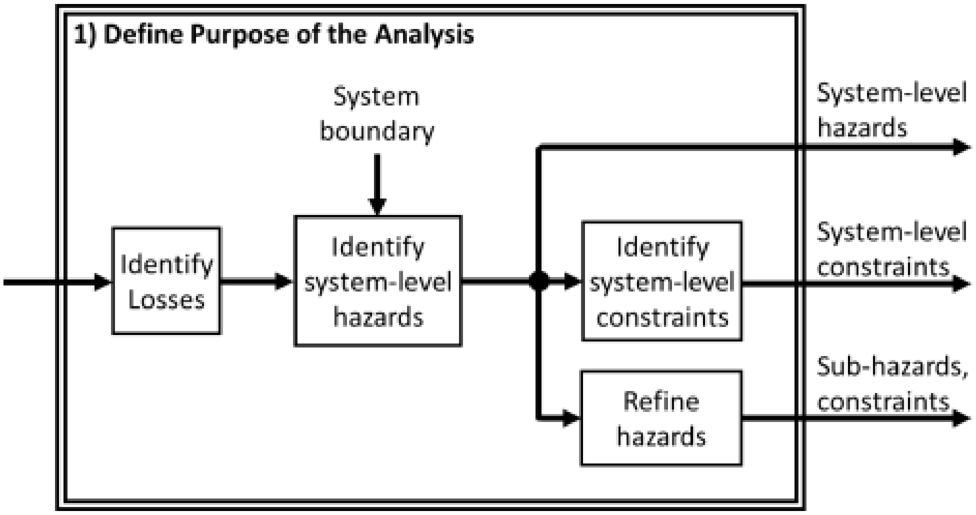
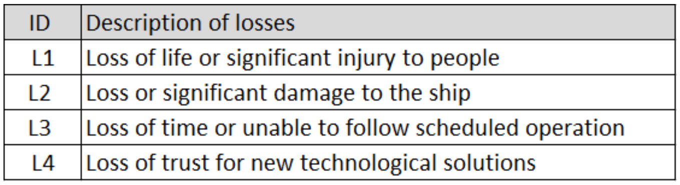


Figure 16 – “Overview of defining the analysis purpose”. Figure 2.3 retrieved from the STPA handbook (Thomas and Leveson, 2018, p. 16).

Table 6 below represents the high level losses identified for Sundbåten’s system:

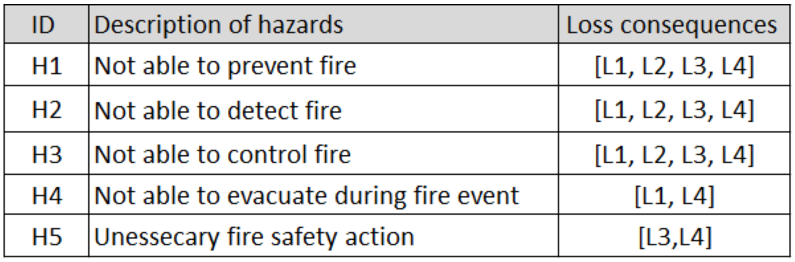
Table 6 – Losses identified



ID	Description of losses
L1	Loss of life or significant injury to people
L2	Loss or significant damage to the ship
L3	Loss of time or unable to follow scheduled operation
L4	Loss of trust for new technological solutions

Table 7 below represents system-level hazards that can potentially lead to unacceptable losses:

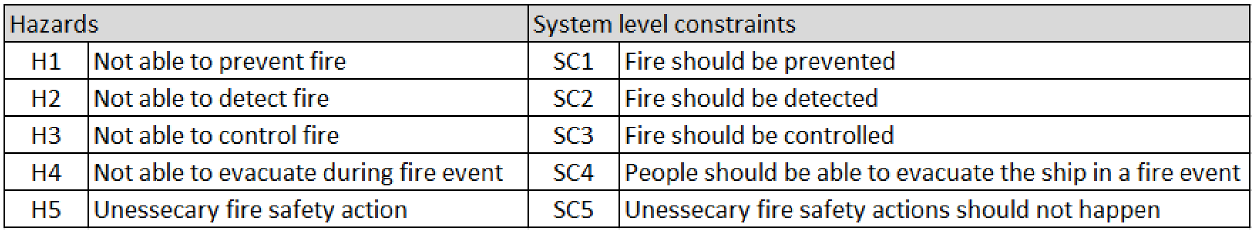
Table 7 – System-level hazards identified



ID	Description of hazards	Loss consequences
H1	Not able to prevent fire	[L1, L2, L3, L4]
H2	Not able to detect fire	[L1, L2, L3, L4]
H3	Not able to control fire	[L1, L2, L3, L4]
H4	Not able to evacuate during fire event	[L1, L4]
H5	Unessecary fire safety action	[L3,L4]

Table 8 below represents system-level constraints that has to be satisfied to prevent the critical hazards identified in table 7.

Table 8 – System-level constraints



Hazards		System level constraints	
H1	Not able to prevent fire	SC1	Fire should be prevented
H2	Not able to detect fire	SC2	Fire should be detected
H3	Not able to control fire	SC3	Fire should be controlled
H4	Not able to evacuate during fire event	SC4	People should be able to evacuate the ship in a fire event
H5	Unessecary fire safety action	SC5	Unessecary fire safety actions should not happen

All three tables above is critical for the further steps of the procedure as it defines the clear boundaries of the risk analysis.

3.6 Step 2 – Control Structure Model

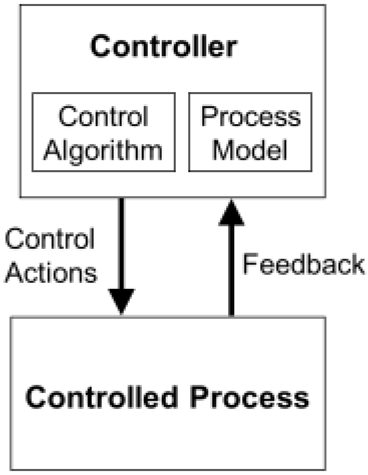


Figure 17 – "Figure 2.6: Generic control loop". Retrieved from the STPA handbook (Thomas and Leveson, 2018, p. 23).

Figure 18 below is the CSM representing Sundbåten's technical fire safety system and the connectivity between the different elements. The scope for the CSM is narrowed down to safety regarding battery fire scenarios inside the battery room including the interactivity between the human elements, fire detection- and extinguishing system as well as the software controller. The four controllers to be analyzed is the Onboard Captain (OC), Remote Human Operator (RHO), Integrated Automation and Safety System (IASS) and the Battery Management System (BMS). Again, the procedure follows the general procedure with the thought process as presented in figure 17. Each of the boxes in figure 18 represent a separate part of the overall system which is connected in one way or another. Solid lines represents control actions or commands, and dotted lines represent feedback signals. It is important to clarify that these lines does not represent physical connections, but rather a functional connection. For a brief description of all numbered signals in the figure, see table 9 below the CSM. The CSM is very much connected and crucial for the remaining parts of the procedure.

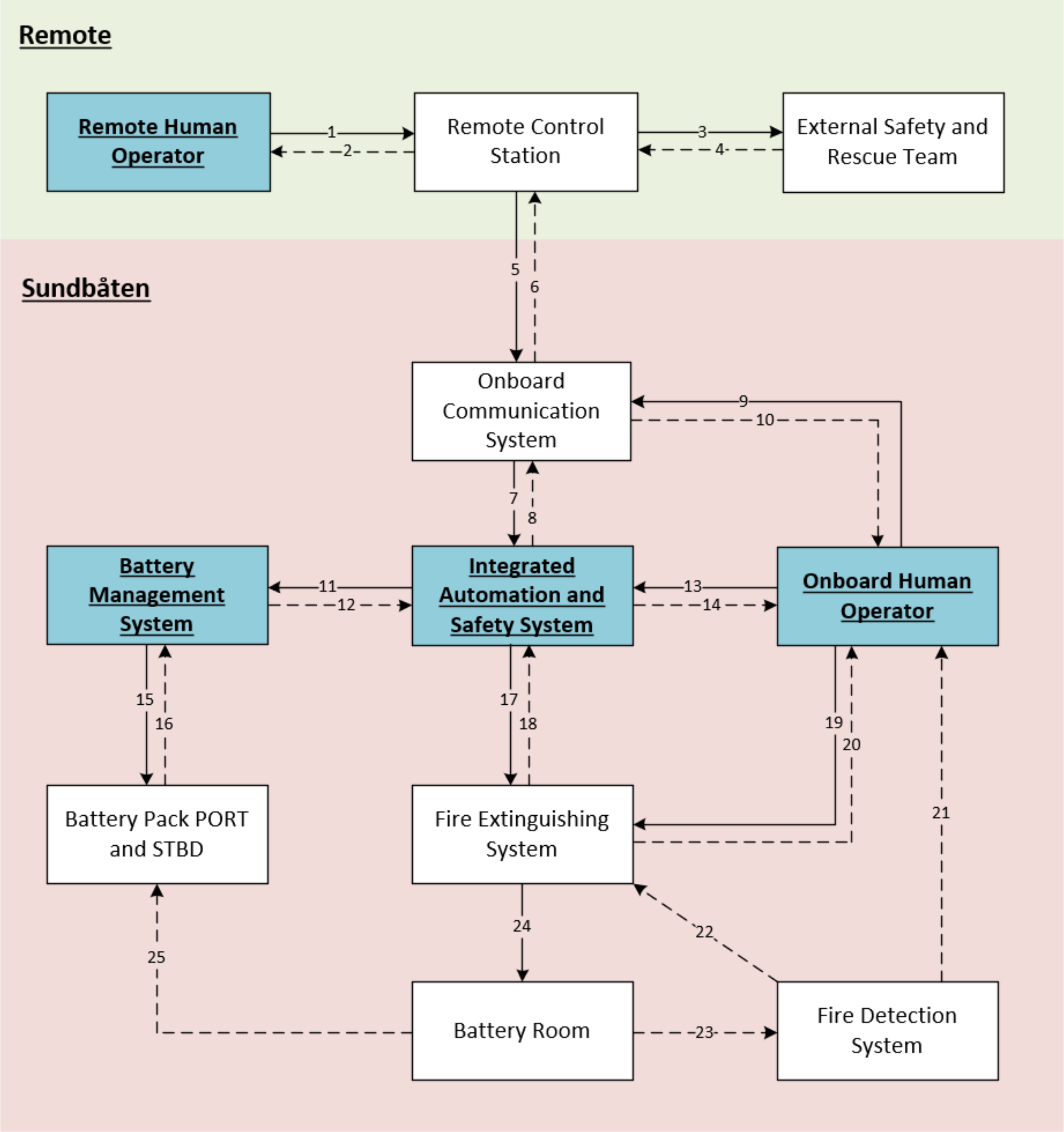
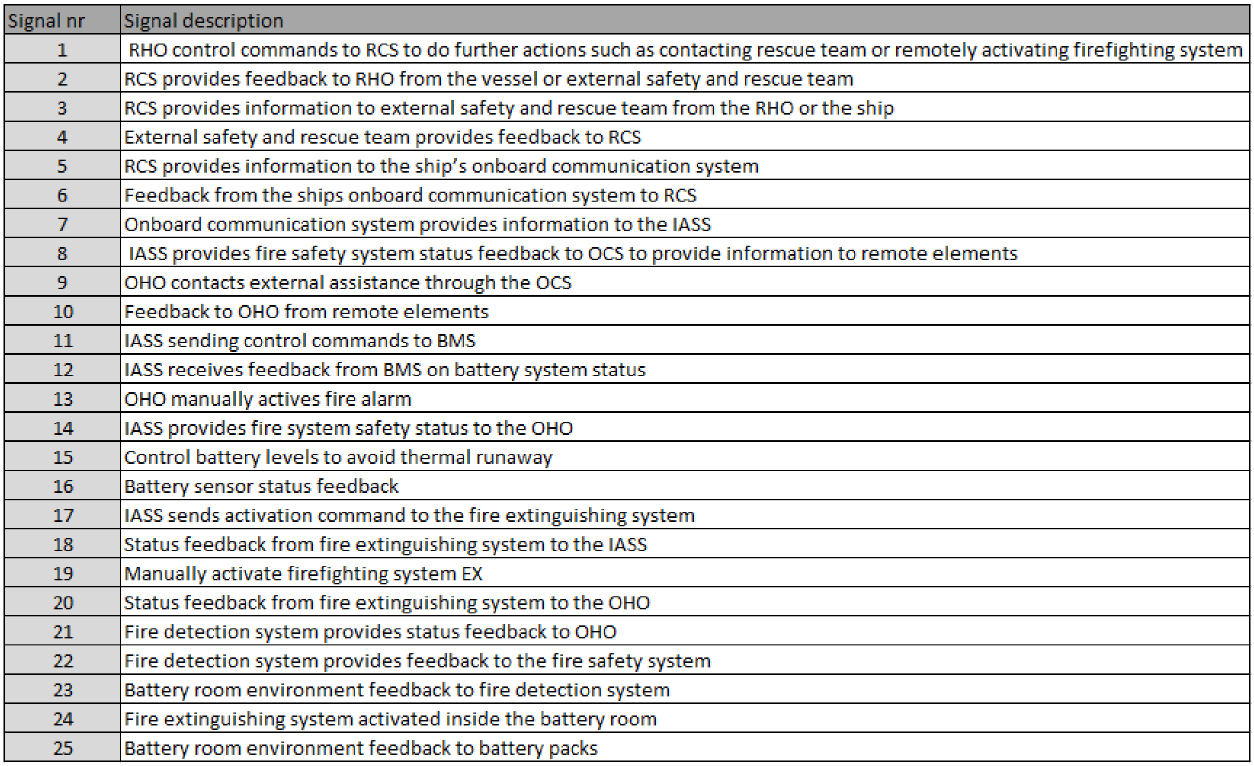

Remote
Remote Human Operator
1
2
Remote Control Station
3
4
External Safety and Rescue Team
5
6
Sundbåten
Onboard Communication System
9
10
7
8
Battery Management System
11
12
Integrated Automation and Safety System
13
14
Onboard Human Operator
15
16
17
18
19
20
21
Battery Pack PORT and STBD
Fire Extinguishing System
22
24
25
Battery Room
23
Fire Detection System

Figure 18 – Control Structure Model

Table 9 – CSM Signal List



Signal nr	Signal description
1	RHO control commands to RCS to do further actions such as contacting rescue team or remotely activating firefighting system
2	RCS provides feedback to RHO from the vessel or external safety and rescue team
3	RCS provides information to external safety and rescue team from the RHO or the ship
4	External safety and rescue team provides feedback to RCS
5	RCS provides information to the ship's onboard communication system
6	Feedback from the ships onboard communication system to RCS
7	Onboard communication system provides information to the IASS
8	IASS provides fire safety system status feedback to OCS to provide information to remote elements
9	OHO contacts external assistance through the OCS
10	Feedback to OHO from remote elements
11	IASS sending control commands to BMS
12	IASS receives feedback from BMS on battery system status
13	OHO manually actives fire alarm
14	IASS provides fire system safety status to the OHO
15	Control battery levels to avoid thermal runaway
16	Battery sensor status feedback
17	IASS sends activation command to the fire extinguishing system
18	Status feedback from fire extinguishing system to the IASS
19	Manually activate firefighting system EX
20	Status feedback from fire extinguishing system to the OHO
21	Fire detection system provides status feedback to OHO
22	Fire detection system provides feedback to the fire safety system
23	Battery room environment feedback to fire detection system
24	Fire extinguishing system activated inside the battery room
25	Battery room environment feedback to battery packs

The table below is represents the responsibilities of the Battery Management System (BMS) in the CSM.

Table 10 – BMS responsiblities

Battery Management System (BMS)		
Responsibilities	Process Model	Feedback
Control battery levels to prevent thermal runaway	• Battery levels within SOA	• Battery state
Send alarm(s) to IASS	• Battery levels within SOA	• Battery alarm(s) activated

3.7 Step 3 – Identifying Unsafe Control Actions

Table 11 and 12 below represents each of the crucial control action that the BMS is responsible for. Tables have specific conditions for the defined control action with various scenarios in order to identify if it should be considered an unsafe control action. It is structured in a way that UCA's for each of the control actions is listed after the relevant table. Each of the UCA's is also connected to specific system-level hazards identified in step 1 of the procedure.

Table 11 – "Identifying UCAs - Preventing thermal runaway"

Controller: Battery Management System (BMS)								
ID	**Control Action**	**Condition**	**Unsafe Control Actions?**					
		Is the battery operating within SOA?	**Not Provided**	**Provided**	**Too early**	**Too late**	**Too short**	**Too long**
CA.BMS.001 **CA.BMS.002** **CA.BMS.003** **CA.BMS.004**	Control battery levels to prevent thermal runaway	Yes	Unsafe [H1]	Safe	N/A	N/A	N/A	N/A
		No	Unsafe [H1]	Safe	Safe	Unsafe [H1]	N/A	N/A

UCA.BMS.001: The BMS does not control battery levels to prevent thermal runaway while operating within SOA [H1].

UCA.BMS.002: The BMS does not control battery levels to prevent thermal runaway while operating outside SOA [H1].

UCA.BMS.003: The BMS control battery levels to prevent thermal runaway too late while operating outside SOA [H3].

Table 12 – "Identifying UCAs – Sending critical alarms to the IASS".

Controller: Battery Management System (BMS)								
ID	**Control Action**	**Condition**	**Unsafe Control Actions?**					
		Is the battery operating within SOA?	**Not Provided**	**Provided**	**Too early**	**Too late**	**Too short**	**Too long**
CA.BMS.005 **CA.BMS.006** **CA.BMS.007**	Send critical alarm(s) to IASS	Yes	Safe	Unsafe [H5]	N/A	N/A	N/A	N/A
		No	Unsafe [H1]	Safe	Unsafe [H5]	Unsafe [H1]	N/A	N/A

UCA.BMS.004: The BMS send critical alarms to the IASS while operating within SOA [H5].

UCA.BMS.005: The BMS does not send alarms to the IASS when the battery is operating outside SOA [H1].

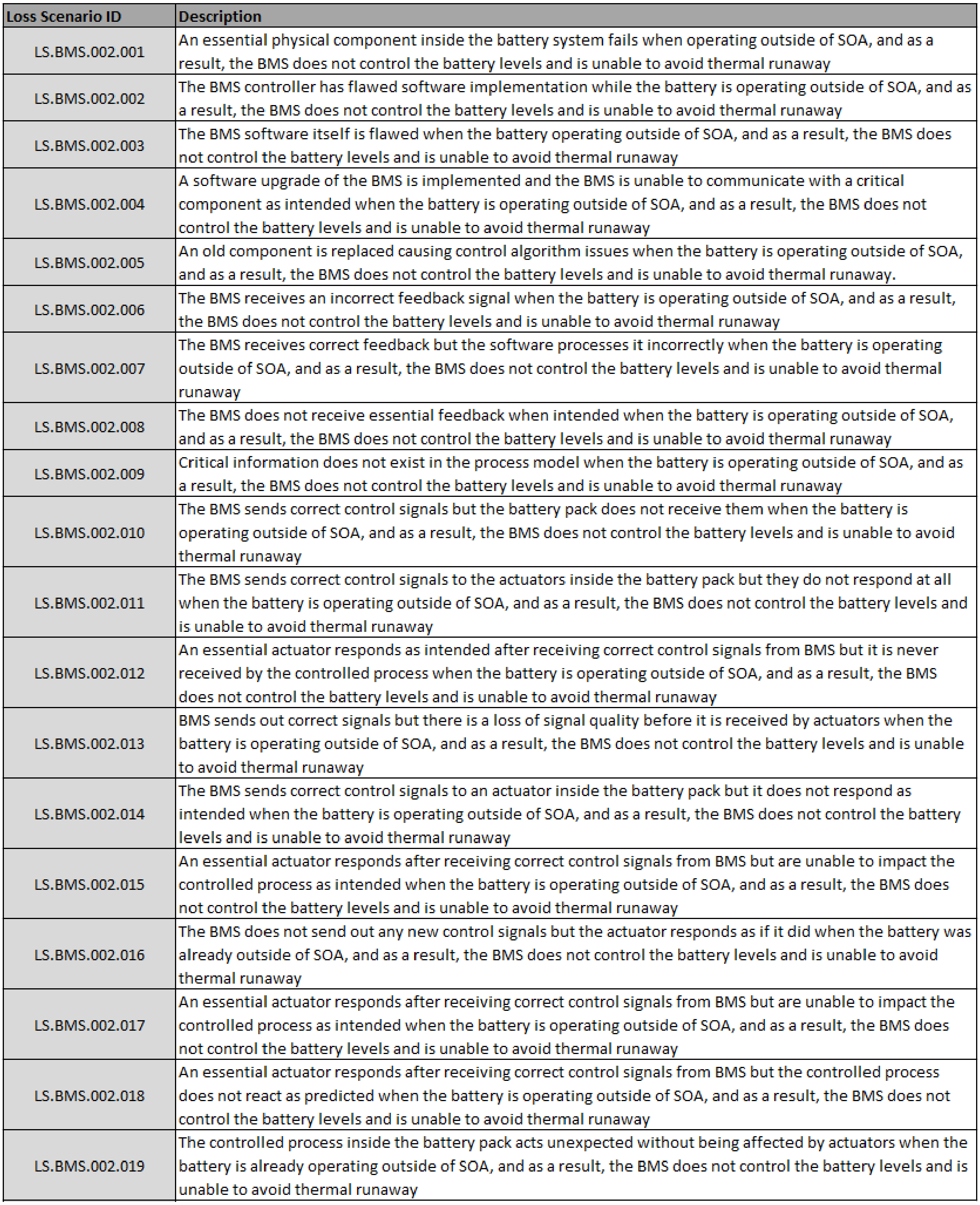
UCA.BMS.006: The BMS send alarms to the IASS too late when the battery is operating outside SOA [H1].

In this section only one of the UCA's will be further investigated in step 4. Selected as the most crucial UCA is **UCA.BMS.002:** The BMS does not control battery levels to prevent thermal runaway while operating outside SOA [H1].

3.8 Step 4 – Identifying Loss Scenarios

Loss scenarios in this section is directly connected to the UCA mentioned above in step 3. Below is a table representing high-level loss scenarios identified for arguably the most important unsafe control action above for the battery fire safety system onboard Sundbåten. To see loss scenarios identified for the different controllers see Appendix B.

Tabell 13 – Loss Scenarios identified for UCA.BMS.002



Loss Scenario ID	Description
LS.BMS.002.001	An essential physical component inside the battery system fails when operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.002	The BMS controller has flawed software implementation while the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.003	The BMS software itself is flawed when the battery operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.004	A software upgrade of the BMS is implemented and the BMS is unable to communicate with a critical component as intended when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.005	An old component is replaced causing control algorithm issues when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway.
LS.BMS.002.006	The BMS receives an incorrect feedback signal when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.007	The BMS receives correct feedback but the software processes it incorrectly when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.008	The BMS does not receive essential feedback when intended when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.009	Critical information does not exist in the process model when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.010	The BMS sends correct control signals but the battery pack does not receive them when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.011	The BMS sends correct control signals to the actuators inside the battery pack but they do not respond at all when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.012	An essential actuator responds as intended after receiving correct control signals from BMS but it is never received by the controlled process when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.013	BMS sends out correct signals but there is a loss of signal quality before it is received by actuators when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.014	The BMS sends correct control signals to an actuator inside the battery pack but it does not respond as intended when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.015	An essential actuator responds after receiving correct control signals from BMS but are unable to impact the controlled process as intended when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.016	The BMS does not send out any new control signals but the actuator responds as if it did when the battery was already outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.017	An essential actuator responds after receiving correct control signals from BMS but are unable to impact the controlled process as intended when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.018	An essential actuator responds after receiving correct control signals from BMS but the controlled process does not react as predicted when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.019	The controlled process inside the battery pack acts unexpected without being affected by actuators when the battery is already operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway

5 Discussion

5.1 Battery fire accidents

Based on the findings on the battery fire accidents it is fair to say that most parties involved have a lot to learn about fire safety of battery solutions onboard ships in general. Referring to both Ytterøyningen and Brim there are quite a few indications that there is a lack of understanding of the possible worst-case scenario and preparations were not optimal. This includes fire safety procedures, ship design to handle fire events in battery rooms, arrangement of procedure executions and the overall understanding of the risk involved. There are very clear indications that there is lack of understanding regarding key aspects such as location-, accessibility-, and ventilation of the ship's most important rooms as well as fire detection- and prevention systems. Referring to the investigation of MS Brim, it was clearly not a simple procedure to regain control of the engine and battery rooms during the hazardous event. This was partly due to the battery room being located below deck with tight pathways leading to the entrance. A key aspect of regaining control was the ventilation process of siphoning out explosive and toxic gases. This can be considered an important aspect for new designs with battery solutions implemented. Brim which is supposed to be a modern solution had some critical design flaws considering the battery room was not completely tight and likely never been properly pressure tested. Spending time on creating custom connections for ventilation hoses should also not be an issue during a fire event itself which shows lack of knowledge about the possible hazardous fire events. Ytterøyningen also had questionable solutions as the salt-water sprinkler system was hitting the battery creating more short-circuits. The effectiveness of fire extinguishing systems is also a point which is up for discussion and it seems fair to say that the optimal solution is yet to be invented. Naive ship owners opting for easy solutions that is not prepared for battery fire events should arguably not be accepted with today's knowledge and should have strict acceptance criteria such as various pressure and ventilation tests in battery rooms or proper facilitation for handling fire events. It is also fair to say based on the two accidents on Ytterøyningen and Brim that the basic fire safety measures such as water sprinklers, gas and foam extinguishing systems are not sufficient to handle battery fires.

In terms of obvious key improvement points that should be up for discussion there are quite a few based on all the findings. To respond as efficient as possible there should be clear pre-organized task forces. When similar accidents occur there should be no doubt about whom to contact and who is participating. For the procedure to be as efficient and professional as possible, a pre organized team should always stand by. This includes all external organizations, various specialists, key contacts, and others which can provide educated assistance. Referring to both accidents, the uncertainty about partners seemed to be a challenge and caused certain things to take longer time than needed. The different parties should also have some sort of pre-planned or prepared scenarios to make sure that all parts of the procedure are as efficient as possible. This also includes organizations having a good overview of marine vessels with battery solutions which is normally operating within their region. This way they can familiarize them with each of the technical designs and prepare for actual scenarios. Planning also includes being prepared to use rarely used equipment. A good example is the nitrogen supply truck used in the procedure onboard MS Brim, where the supply tank only lasted for a third of the time that was expected. These situations should not be a surprise mid operation. People in certain positions should continuously acquiring up-to-date theory and knowledge within the field should be of high priority for any parties or organizations related to battery solutions onboard ships. Task forces should also have continuously train on practical routines and procedures. This is especially important for efforts in challenging environments. Tight compartments with bad accessibility, tight compartments, toxic and flammable exposed areas are just some examples. This point also includes training with all new and rarely used fire prevention- and safety systems and equipment such as protective gear and gas meters. Referring to the procedure onboard MS Brim, knowledge within the process of supplying and extracting gases from areas which is not very accessible can be very beneficial. Related to operations in gas exposed areas and the use of gas meters there is a few very important pointers which is also mentioned in the fire evaluation reports. It is incredibly important to have sufficient knowledge of all possible gases that can be released from batteries as well as what measuring different levels of each gas indicates. By having this knowledge, it can drastically help the ability to make quick and difficult decisions while operating in difficult conditions.

A fair statement regarding future research on battery fire safety systems onboard ships should be continuously researched for years to come and adapting is always going to be key. Since the development of battery solutions onboard ships are still arguably at a relatively early stage there are likely many risk factors that are yet to be identified due to lack of research and experience. A key point for other researchers and safety system developers is that there is absolutely no doubt that accidents should be included into research and development as soon as they occur. We are already seeing some incredibly interesting solutions on how to handle worst-case scenarios with battery solutions. A great example is KRISO which is currently developing an electric ferry with a mobile battery solution. The battery packs can simply be detached and dropped into the water during a critical hazardous fire event (KRISO, n.d.). This solution would then replace a worst-case scenario potentially injuring people with a predictable and fixed loss scenario of "minor" material damage. Main point here being that personally I believe it is incredibly important for both safety system developers and researchers to learn from each other and built on proper research and experiences because it is fair to say that there are still a lot of question which is yet to be answered.

5.2 STPA results and experiences

Again, it is important to clarify that this is simply a preliminary risk analysis. After conducting the STPA procedure on Sundbåten's battery fire safety system it was identified 27 UCAs. All of these are obviously different and should in general be further defined or categorized. For this case, it was identified 6 purely human related UCAs, 12 autonomous related UCAs and 9 UCAs with a combination of the two. This can arguably be a good indication as to why it is so important to use modern risk analysis methods to be able to include the human element, software aspect and the interactivity between the different elements. As for which hazards the UCAs is connected to, it varies quite a bit. Referring to table 7 in step 1 there are 5 UCAs connected to H1, 4 UCAs to H2, 6 UCAs to H3, 4 UCAs to H4 and 8 UCAs to H5. Interestingly H5 has the most which indicates the fact that there can be a lot of various causal factors leading to unnecessary fire safety actions which essentially costs time and money.

When it comes to loss scenarios there are quite a few discussion points that should be taken into consideration. For this thesis it was only identified 75 relatively high level LSs for 5 different UCAs. Depending on the in-depth detail the analyst is able to go there can be so many LSs that it becomes an issue. The whole purpose is obviously to shed light meaningful findings that can actually prevent fire which possibly means that thousands of LSs has to be identified. An example is identifying all possible LSs for a flawed algorithm which for a complex system could be thousands on its own. If this happens for many different UCAs it will also be increasingly difficult to organize and handle all the LSs. So, to end that point, it is not necessarily that helpful to find the high level LSs, but there can be just as big issue the other way when going too much into detail. Referring to both battery fire accidents it is also quite an interesting point that it would not be an issue to identify the roots for the hazard development. An example to this is the battery system onboard Ytterøyningen not being connected to the ships system, and therefore an alarm was sent too late. In other words, it is clearly theoretically possible, but in practice it can be difficult if the causal factor is unknown and never experienced. If hypothetically after a proper STPA procedure there is identified 10 000 different LSs, it can be incredibly difficult to prevent all of them from occurring. An interesting article discussing the topic of optimizing the STPA method is “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” published by Kim et al. in 2021.

Other experiences with the method is that it is quite clear that experience with applying the method and the analyst’s knowledge within the topic is essential to conduct a solid STPA. Lack of insight within the topic to be analyzed or an unorganized way of conducting and handling the information from the procedure the method can negatively impact the procedure and create a lot of confusion for an inexperienced analyst. Examples of this can be to identify a random crucial control action or feedback that is essential for the process is purely up to the insight of the analyst. A key aspect pointed out in an article from Chaal et al. is that the advanced starting point in the procedure will likely improve the analyst’s ability to clarify and define possible interactions between all the different controllers and controlled processes defined in the system. The authors then follows by saying this for analyzing autonomous ships which can also be argued to be relevant for other systems as well: “The control structure will then be used as an advanced starting point to apply STPA analysis to enhance the control structure and identify the eventual safety, resilience, and reliability requirements of autonomous ships” (Chaal et al., 2020).

5.3 Research question and thesis objective

Referring to the research question it is up for discussion if it is answered satisfyingly or not. First of all, there are different factors that highly impact the quality of the findings which is touched upon under subsection 5.4 about limitation . In short, various elements have impacted the outcome such as general STPA factors, state and available information of what is being researched, researchers experience with STPA and knowledge within the field and more. From an academic standpoint arguments can be done both ways. Personally, I believe the findings can be argued to answer the research question in a good manner considering the early stage of the project and a lack of project details regarding the battery fire safety system. Regarding the academic value of the thesis overall there are a few different elements that can be discussed to contribute and add value. Literature review creating an overview of relevant academic research, investigating battery fire accidents onboard ships, preliminary STPA conducted on the human interaction with the battery fire safety system onboard Sundbåten and adding certain value to the development of the STPA method in general.

When it comes to existing academic research on STPA in general there seemed to be several solid academic papers conducting the modern risk analysis method, but not directly related to battery safety systems onboard ships. The degree of value of the findings from conducting the STPA procedure can obviously be discussed back and forth, but since there is a clear lack of existing academic research on the specific topic it is fair to argue that it adds a certain level of value. The findings itself is also difficult to discuss since there is a lack of relevancy compared to other academic studies. If the findings can be generalized is obviously up for discussion, but there are certain key findings which is very important no matter the system safety design.

As for existing academic research on battery fire safety systems it seemed quite clear that there were research gaps in terms of the overall safety for battery solutions onboard marine vessels. The lack of research can potentially be quite limiting if the goal would be to make "groundbreaking" research on the topic. From an academic standpoint I personally believe this a factor in not being able to identify more key unsafe control actions and loss scenarios from the STPA procedure and slightly weakening the value of the research. In other words, lack of research can impact new research within the field because it seems essential to have proper research and knowledge within the specific field in order to create maximum value from the new research. From a battery fire safety system developers view it can have also potentially have the same negative impact to not have proper up-to-date high quality research to build upon in order to analyze human interaction with the system and develop the optimal safety solution for ships.

5.4 Limitations for the thesis

Discussing the reliability, validity and ensuring the credibility of this thesis can be difficult since it is mostly qualitative research. The findings from the STPA procedure itself can be considered quite reliable but it the academic rigor is certainly up for discussion. It is quite difficult to determine the accuracy or justify the findings due to the qualitative style. A key aspect of the STPA procedure that can certainly question the reliability is the highly flexible procedure that creates windows for the analysts' personal opinions and bias. This is certainly a point that makes it difficult to academically justify and to ensure the overall integrity of findings. This is even more of an important point if the researcher also lacks experience within the field and experience and knowledge it can be very difficult to show academic rigor. If other risk analyses were conducted analyzing the human element interacting with the battery safety systems with same operational conditions the likelihood of resulting in similar findings is relatively high in other studies. Although there is a high chance that findings will be similar, it can be argued that due to the flexibility of the STPA method there is certainly a chance that it could look quite different which could make it unreliable in some way. This is because the method in all of the four steps can look very different based upon the person conducting the analysis. Especially in step 2-4 in the STPA procedure can look very different based on the style of the analyst, knowledge within the field and experience with conducting the risk analysis method. It should also be mentioned that findings are highly depending on the development stage and available data and information. The reliability can again be further questioned due to the emerging variations of the STPA procedure. Referring to the literature review there are quite some studies that has identified the downsides of the procedure and applied different extensions and variations of the standard STPA procedure. Certain variations can likely vary the findings and impact the reliability. To conclude there are certain points that limit the credibility of this thesis such as lack of qualitative analysis, researcher being a novice at conducting STPA procedures, possible hints of personal views in the procedure itself, lack of directly relevant studies in the literature review to compare and reduce bias and lack of knowledge within the field.

As a general limitation of this thesis' risk analysis is the current development stage of the Sundbåten project. Since its still in an early stage there are certain there are still many decision yet to be made. As a result, there are still quite a few assumptions and generalizations that has to be made for many important aspects. This includes details on the fire safety system, the human elements' procedure and decision planning, uncertainties regarding vessel design, rescue and evacuation procedures and so on. Testing of the technical system and the important safety procedures is not possible in the current development phase which would be considered a limitation if this was the main risk analysis for the project. But again, it is important to clarify that this thesis should only be assessed as a preliminary risk analysis and merely a small part of the overall risk analysis. Therefore, it should rather be argued that a preliminary risk analysis is a great benefit for the overall risk assessment for a project to increase the chances of identifying possible causal scenarios before experiencing critical loss scenarios during operation testing.

6 Conclusion and Suggestions for Further Research

First of all, there were two research questions defined in the early stages of the thesis. First being "What are the main causes of previous battery fire accidents onboard ferries?" and the second being "What kind of additional hazards should be considered for the battery fire safety system?".

Despite waiting for official reports describing the main causes are clear. Onboard Ytterøyningen Stensvold reported that it was due to a twisted rubber gasket causing a leakage in the water-coolant system in the battery pack. As for MS Brim, the most recent update is from the technical responsible onboard the ship writing that the preliminary conclusion is sea water entering the ventilation system leading to the battery room (Brim Explorer, n.d.). To the second question it can be difficult to answer in a simple manner. Referring to all the results from the STPA procedure there are several correct answers but there are still hazards obviously hazards that are not yet identified. To answer the question several critical unsafe control actions and loss scenarios is identified for all four critical controllers in the battery fire safety system onboard Sundbåten.

Referring to the introduction and the defined research questions and research objectives in section 1.3 it is fair to say that the goal was successfully achieved, and the research questions is answered in a satisfying manner. The degree of academic value added for the different research objectives is obviously up for discussion, but it is fair to conclude with the fact that it adds a certain level to each of the objectives. The qualitative procedures in all the literature reviews has gathered important information and certain key aspects has been further identified and discussed. Some level of research value has also been provided for application of STPA on modern socio-technical systems by applying the method on the fire safety system onboard Sundbåten. As for investigation potentials hazards in the fire safety system with focus on the interactivity between the different controller's certain findings provide research value, despite being certain that more loss scenarios are yet to identify.

Safety of human lives are inarguably always going to be the number one priority when developing novel socio-technical system and it can be difficult to find the perfect balance between risk and safety. To continue the development for future battery solutions onboard marine vessels it should be of high importance to go forward with a controlled approach by combining existing knowledge and experiences from similar solutions to have the highest degree of safety possible. Awareness needs to be raised for the possible worst-case scenarios and safety measures has to be improved and implemented to maintain the highest degree of safety possible despite certain impractical safety steps that has to be implemented. Overall, it is clear that authorities, ship owners, ship designers, battery specialists, firefighters and other relevant parties has a lot to learn before the implementation of battery solutions onboard ships should be considered safe.

When it comes to further research there it seems clear that all research objectives used in this thesis can be further investigated. There is undoubtedly room for research and development in terms of various aspects when it comes to fire safety for battery solutions onboard ships. This includes aspects like fire extinguishing systems for lithium-ion batteries, ventilation- and ship design, fire safety procedure development, and so on. As for risk analysis in general there is certainly room for more research. We have likely just seen the beginning of groundbreaking socio-technical systems which makes it incredibly important to continue the development and experience with analyzing the safety aspect with proper methods such as STPA. Despite the standard procedure having certain limitations due to heavily qualitative aspects, there is only a lack of development and research holding it back. Referring to the literature review there is researchers already developing variations of the method to include qualitative aspects in order to analyze the risk for a wide range of systems from different angles.

7 Bibliography

Ahvenjärvi, S. (2016). The Human Element and Autonomous Ships. *TransNav, International Journal on Marine Navigation and Safety Od Sea Transportation*, *10*(3). http://www.transnav.eu/Article_The_Human_Element_and_Autonomous_Ships_Ahvenjärvi,39,675.html

Basso, E. A., Thyri, E. H., Pettersen, K. Y., Breivik, M., & Skjetne, R. (2020). *Safety-critical control of autonomous surface vehicles in the presence of ocean currents*. 396–403. Scopus. https://doi.org/10.1109/CCTA41146.2020.9206276

Bratić, K., Pavić, I., Vukša, S., & Stazić, L. (2019). Review of Autonomous and Remotely Controlled Ships in Maritime Sector. *Transactions on Maritime Science*, *8*, 253–265. https://doi.org/10.7225/toms.v08.n02.011

Brim Explorer. (n.d.). *Oppdatering og gode nyheter!* [Facebook]. Retrieved 17 April 2022, from https://www.facebook.com/brimexplorer/photos/a.2261405617470755/3126414314303210/

Carreras Guzman, N. H., Zhang, J., Xie, J., & Glomsrud, J. A. (2021). A Comparative Study of STPA-Extension and the UFoI-E Method for Safety and Security Co-analysis. *Reliability Engineering and System Safety*, *211*. Scopus. https://doi.org/10.1016/j.ress.2021.107633

Chaal, M., Valdez Banda, O. A., Glomsrud, J. A., Basnet, S., Hirdaris, S., & Kujala, P. (2020). A framework to model the STPA hierarchical control structure of an autonomous ship. *Safety Science*, *132*. Scopus. https://doi.org/10.1016/j.ssci.2020.104939

Chae, C.-J., Kim, M., & Kim, H.-J. (2020). A study on identification of development status of MASS technologies and directions of improvement. *Applied Sciences (Switzerland)*, *10*(13). Scopus. https://doi.org/10.3390/app10134564

Chen, M., Liu, J., Dongxu, O., Cao, S., Wang, Z., & Wang, J. (2018). A simplified analysis to predict the fire hazard of primary lithium battery. *Applied Sciences (Switzerland)*, *8*(11). Scopus. https://doi.org/10.3390/app8112329

Dghaym, D., Hoang, T. S., Turnock, S. R., Butler, M., Downes, J., & Pritchard, B. (2021). An STPA-based formal composition framework for trustworthy autonomous maritime systems. *Safety Science*, *136*, 105139. https://doi.org/10.1016/j.ssci.2020.105139

DNV GL AS Maritime. (2020). *Electrical Energy Storage for Ships* (p. 184).

Escande, J., Proust, C., & Le Coze, J. C. (2016). Limitations of current risk assessment methods to foresee emerging risks: Towards a new methodology? *Journal of Loss Prevention in the Process Industries*, *43*, 730–735. Scopus. https://doi.org/10.1016/j.jlp.2016.06.008

Glomsrud, J. A., & Xie, J. (2020). *A structured STPA safety and security co-analysis Framework for autonomous ships*. 38–45. Scopus. https://doi.org/10.3850/978-981-11-2724-3_0105-cd

Goerlandt, F., & Pulsifer, K. (2022). An exploratory investigation of public perceptions towards autonomous urban ferries. *Safety Science*, *145*, 105496. https://doi.org/10.1016/j.ssci.2021.105496

Guidance in connection with the construction or installation of automated functionality aimed at performing unmanned or partially unmanned operations—Norwegian Maritime Authority. (n.d.). Retrieved 27 January 2022, from https://www.sdir.no/en/shipping/legislation/directives/guidance-in-connection-with-the-construction-or-installation-of-automated-functionality-aimed-at-performing-unmanned-or-partially-unmanned-operations/

Guo, C., Haugen, S., & Utne, I. B. (2021). Risk assessment of collisions of an autonomous passenger ferry. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*. Scopus. https://doi.org/10.1177/1748006X211050714

Hoem, Å., Porathe, T., Rødseth, Ø., & Johnsen, S. (2018). *At least as safe as manned shipping? Autonomous shipping, safety and "human error"*.

How to write a research methodology. (2019, February 25). Scribbr. https://www.scribbr.com/dissertation/methodology/

Hüffmeier, J., & Bram, S. (2019, October 22). *Human Contribution to Safety of Smart Ships*.

Johansen, T., & Utne, I. B. (2020). *Risk analysis of autonomous ships*. 131–138. Scopus.

Kim, H., Haugen, O. I., Rokseth, B., & Lundteigen, M. A. (2020). *Comparison of hazardous scenarios for different ship autonomy types using systems-theoretic process analysis*. 4130–4137. Scopus. https://doi.org/10.3850/978-981-11-2724-30813-cd

Kim, H., Lundteigen, M. A., Hafver, A., & Pedersen, F. B. (2021). 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. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, *235*(1), 92–107. https://doi.org/10.1177/1748006X20939717

KRISO. (n.d.). *Construction of Korea's first fully electrically propelled car ferry begins*. KOREA RESEARCH INSTITUTE OF SHIPS & OCEAN ENGINEERING. Retrieved 18 April 2022, from https://www.kriso.re.kr/gallery.es?mid=a20301000000&bid=0014&list_no=503&act=view

Kristensen, S. D. (2021). *Risk acceptance criteria for autonomous ships*. https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2781532

Leveson, N. (n.d.). *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.* 188.

Leveson, N. G., & Thomas, J. P. (2018). *STPA HANDBOOK*. MIT Partnership for Systems Approaches to Safety and Security (PSASS).

Listou Ellefsen, A., Han, P., Cheng, X., Holmeset, F. T., Aesoy, V., & Zhang, H. (2020). Online Fault Detection in Autonomous Ferries: Using Fault-Type Independent Spectral Anomaly Detection. *IEEE Transactions on Instrumentation and Measurement*, *69*(10), 8216–8225. Scopus. https://doi.org/10.1109/TIM.2020.2994012

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing*, *18*(2), 34–35. https://doi.org/10.1136/eb-2015-102054

Norwegian Maritime Authority. (2020). *Circular—Series V, RSV 12-2020*. Norwegian Maritime Authority. https://www.sdir.no/contentassets/2b487e1b63cb47d39735953ed492888d/rsv-12-2020-guidance-in-connection-with-the-construction-or-installation-of-automated-functionality.pdf?t=1644969600040

Ramos, M. A., Thieme, C., Utne, I. B., & Mosleh, A. (n.d.). *Autonomous Systems Safety – State of the Art and Challenges*. 15.

Rao, H., Huang, Z., Zhang, H., & Xiao, S. (2015). *Study of fire tests and fire safety measures on lithiumion battery used on ships*. 865–870. Scopus. https://doi.org/10.1109/ICTIS.2015.7232158

Rosewater, D., & Williams, A. (2015). Analyzing system safety in lithium-ion grid energy storage. *Journal of Power Sources*, *300*, 460–471. Scopus. https://doi.org/10.1016/j.jpowsour.2015.09.068

Rutledal, D., Relling, T., & Resnes, T. (2020). *It's not all about the COLREGs: A case-based risk study for autonomous coastal ferries*. *929*(1). Scopus. https://doi.org/10.1088/1757-899X/929/1/012016

Silverajan, B., Ocak, M., & Nagel, B. (2018). Cybersecurity Attacks and Defences for Unmanned Smart Ships. *2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 15–20. https://doi.org/10.1109/Cybermatics_2018.2018.00037

Sjøholt, N. B. (2018). *Reliability Centered Maintenance (RCM) of the Autonomous Passenger Ferry in Trondheim*. https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2563980

Thieme, C. A., Guo, C., Utne, I. B., & Haugen, S. (2019). Preliminary hazard analysis of a small harbor passenger ferry – results, challenges and further work. *Journal of Physics: Conference Series*, *1357*(1), 012024. https://doi.org/10.1088/1742-6596/1357/1/012024

Towards the assessment of potential impact of unmanned vessels on maritime transportation safety | Elsevier Enhanced Reader. (n.d.). https://doi.org/10.1016/j.ress.2017.03.029

Utne, I. B., Rokseth, B., Sørensen, A. J., & Vinnem, J. E. (2020). Towards supervisory risk control of autonomous ships. *Reliability Engineering and System Safety*, *196*. Scopus. https://doi.org/10.1016/j.ress.2019.106757

Valdez Banda, O. A., Kannos, S., Goerlandt, F., van Gelder, P. H. A. J. M., Bergström, M., & Kujala, P. (2019). A systemic hazard analysis and management process for the concept design phase of an autonomous vessel. *Reliability Engineering and System Safety*, *191*. Scopus. https://doi.org/10.1016/j.ress.2019.106584

Vartdal, B. J., Skjong, R., & St.Clair, A. L. (2018). *Remote-controlled and autonomous ships in the maritime industry* (p. 36). DNV.

Ventikos, N. P., Chmurski, A., & Louzis, K. (2020). A systems-based application for autonomous vessels safety: Hazard identification as a function of increasing autonomy levels. *Safety Science*, *131*. Scopus. https://doi.org/10.1016/j.ssci.2020.104919

Wei, L., Zhou, Z., & Wang, Z. (2021). *Fire monitoring system for power batteries on ship*. *1802*(2). Scopus. https://doi.org/10.1088/1742-6596/1802/2/022022

Wróbel, K., Gil, M., & Montewka, J. (2020). Identifying research directions of a remotely-controlled merchant ship by revisiting her system-theoretic safety control structure. *Safety Science*, *129*. Scopus. https://doi.org/10.1016/j.ssci.2020.104797

Wróbel, K., Montewka, J., & Kujala, P. (2018). Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels. *Reliability Engineering and System Safety*, *178*, 209–224. Scopus. https://doi.org/10.1016/j.ress.2018.05.019

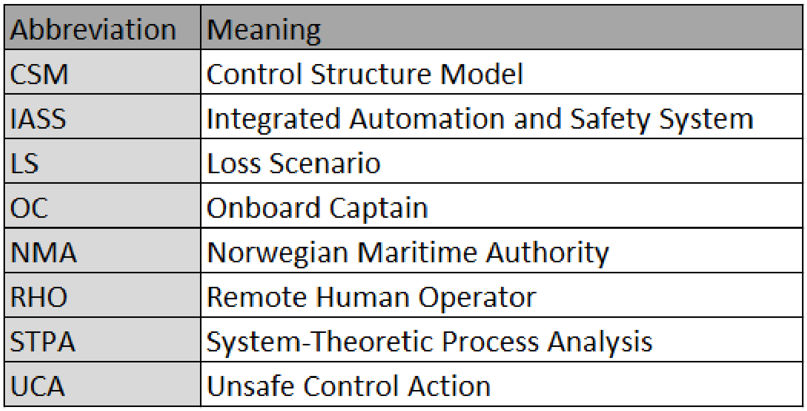
Zhang, J., Zhang, L., Sun, F., & Wang, Z. (2018). An Overview on Thermal Safety Issues of Lithium-ion Batteries for Electric Vehicle Application. *IEEE Access*, *PP*, 1–1. https://doi.org/10.1109/ACCESS.2018.2824838

Zhou, X.-Y., Liu, Z.-J., Wang, F.-W., & Wu, Z.-L. (2021). A system-theoretic approach to safety and security co-analysis of autonomous ships. *Ocean Engineering*, *222*. Scopus. https://doi.org/10.1016/j.oceaneng.2021.108569

Zhou, X.-Y., Liu, Z.-J., Wang, F.-W., Wu, Z.-L., & Cui, R.-D. (2020). Towards applicability evaluation of hazard analysis methods for autonomous ships. *Ocean Engineering*, *214*. Scopus. https://doi.org/10.1016/j.oceaneng.2020.107773

Appendix A - Acronyms

Table 14 - Abbreviations



Abbreviation	Meaning
CSM	Control Structure Model
IASS	Integrated Automation and Safety System
LS	Loss Scenario
OC	Onboard Captain
NMA	Norwegian Maritime Authority
RHO	Remote Human Operator
STPA	System-Theoretic Process Analysis
UCA	Unsafe Control Action

Appendix B – STPA procedure

This appendix includes additional findings and results from the STPA procedure conducted on the overall fire safety system in a high-level. This section contains results from step 2, step 3 and step 4 for the different controllers presented in the CSM in section 4.2. Findings from one controller will be presented one by one starting with OC followed by RHO, IASS and lastly BMS. For each controller responsibilities is defined based on the CSM in section 4.2. Based on the responsibilities there will be presented a table including crucial control actions which is the basis for identifying the different unsafe control actions. The most crucial UCAs for the different controllers is further investigated by identifying loss scenarios.

Controller 1: Onboard Captain:

Table 15 – OC responsibilties

Onboard Captain (OC)		
Responsibilities	Process Model	Feedback
Manually activate battery fire alarm if fire is detected and the automatic fire alarm is inactive	• Fire inside battery room • Automatic alarm not activated	• Fire alarm status
Manually activate firefighting system if the system is not automatically activated	• Fire inside battery room • Automatic firefighting system not activated	• Firefighting system operating status
Contact rescue team and initiate evacuation process	• Uncontrollable fire event	• Rescue team feedback • Evacuation progress status

Table 16 – OC control action: Manually activate battery fire alarm

Controller: Onboard Captain									
ID	**Control Action**	**Condition**		**Unsafe Control Actions?**					
		Is there a fire inside the battery room?	**Is the automatic battery fire alarm activated?**	**Not Provided**	**Provided**	**Too early**	**Too late**	**Too short**	**Too long**
CA.OC.001 **CA.OC.002** **CA.OC.003**	Manually activate battery fire alarm	Yes	Yes	Safe	Safe	Safe	Safe	Safe	Safe
		Yes	No	Unsafe [H2]	Safe	N/A	Unsafe [H2]	N/A	N/A
		No	Yes	Safe	N/A	N/A	N/A	N/A	N/A
		No	No	Safe	Unsafe [H5]	N/A	N/A	N/A	N/A

UCA.OC.001: OC does not manually activate battery fire alarm when there is a fire inside the battery room and the automatic fire alarm is not activated [H2].

UCA.OC.002: OC manually activate battery fire alarm too late when there is a fire inside the battery room and the automatic fire alarm is not activated [H2].

UCA.OC.003: OC manually activate battery fire alarm when there is not a fire inside the battery room and the automatic fire alarm is not activated [H5].

Table 17 – OC control action: Manually activate firefighting system

Controller: Onboard Captain									
ID	**Control Action**	**Condition**		**Unsafe Control Actions?**					
		Is there a fire inside the battery room?	**Is the firefighting system automatically activated?**	**Not Provided**	**Provided**	**Too early**	**Too late**	**Too short**	**Too long**
CA.OC.004 **CA.OC.005** **CA.OC.006**	Manually activate firefighting system	Yes	Yes	Safe	Safe	Safe	Safe	Safe	Safe
		Yes	No	Unsafe [H3]	Safe	N/A	Unsafe [H3]	N/A	N/A
		No	Yes	Safe	N/A	N/A	N/A	N/A	N/A
		No	No	Safe	Unsafe [H5]	N/A	N/A	N/A	N/A

UCA.OC.004: OC does not manually activate firefighting system when there is a fire inside the battery room and the automatic fire alarm is not activated [H3]

UCA.OC.005: OC manually activate firefighting system too late when there is a fire inside the battery room and the firefighting system is not automatically activated [H3]

UCA.OC.006: OC manually activate firefighting system when there is not a fire inside the battery room and the automatic fire alarm is not activated [H5]

Table 18 – OC control action: Contact rescue team and initiate evacuation

Controller: Onboard Captain								
ID	**Control Action**	**Condition**	**Unsafe Control Actions?**					
		Is there an uncontrollable fire inside the battery room?	**Not Provided**	**Provided**	**Too early**	**Too late**	**Too short**	**Too long**
CA.OC.007 **CA.OC.008** **CA.OC.009**	Contact rescue team and initiate evacuation process	Yes	Unsafe [H4]	Safe	Safe	Unsafe [H4]	N/A	N/A
		No	Safe	Unsafe [H5]	N/A	N/A	N/A	N/A

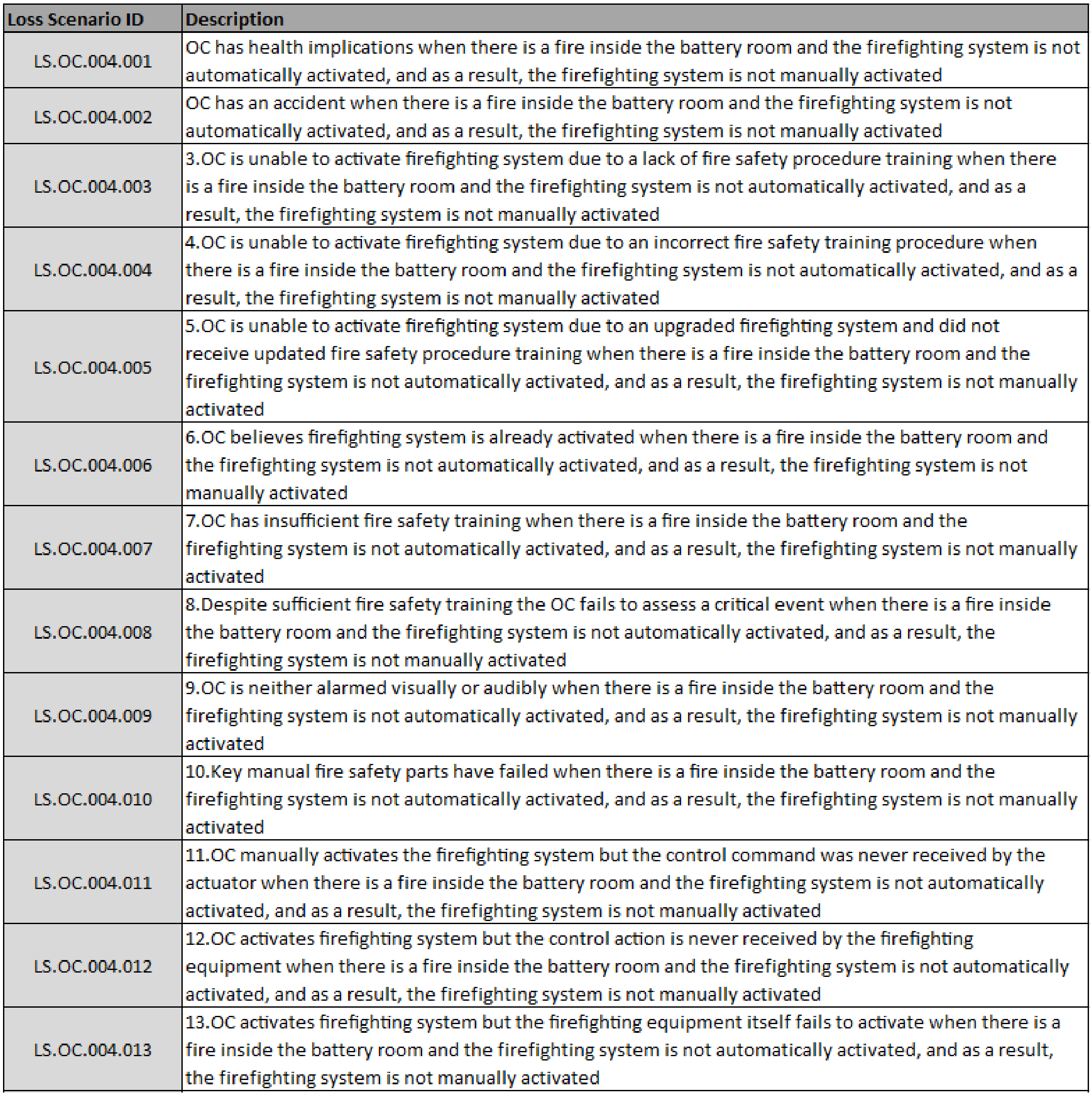
UCA.OC.007: OC does not contact rescue team and initiate evacuation process when there is a fire an uncontrollable fire inside the battery room [H4]

UCA.OC.008: OC contact rescue team and initiate evacuation process too late when there is a fire an uncontrollable fire inside the battery room [H4]

UCA.OC.009: OC do contact rescue team and initiate evacuation process when there is not an uncontrollable fire inside the battery room [H5]

The table below represents loss scenarios for UCA.OC.004:

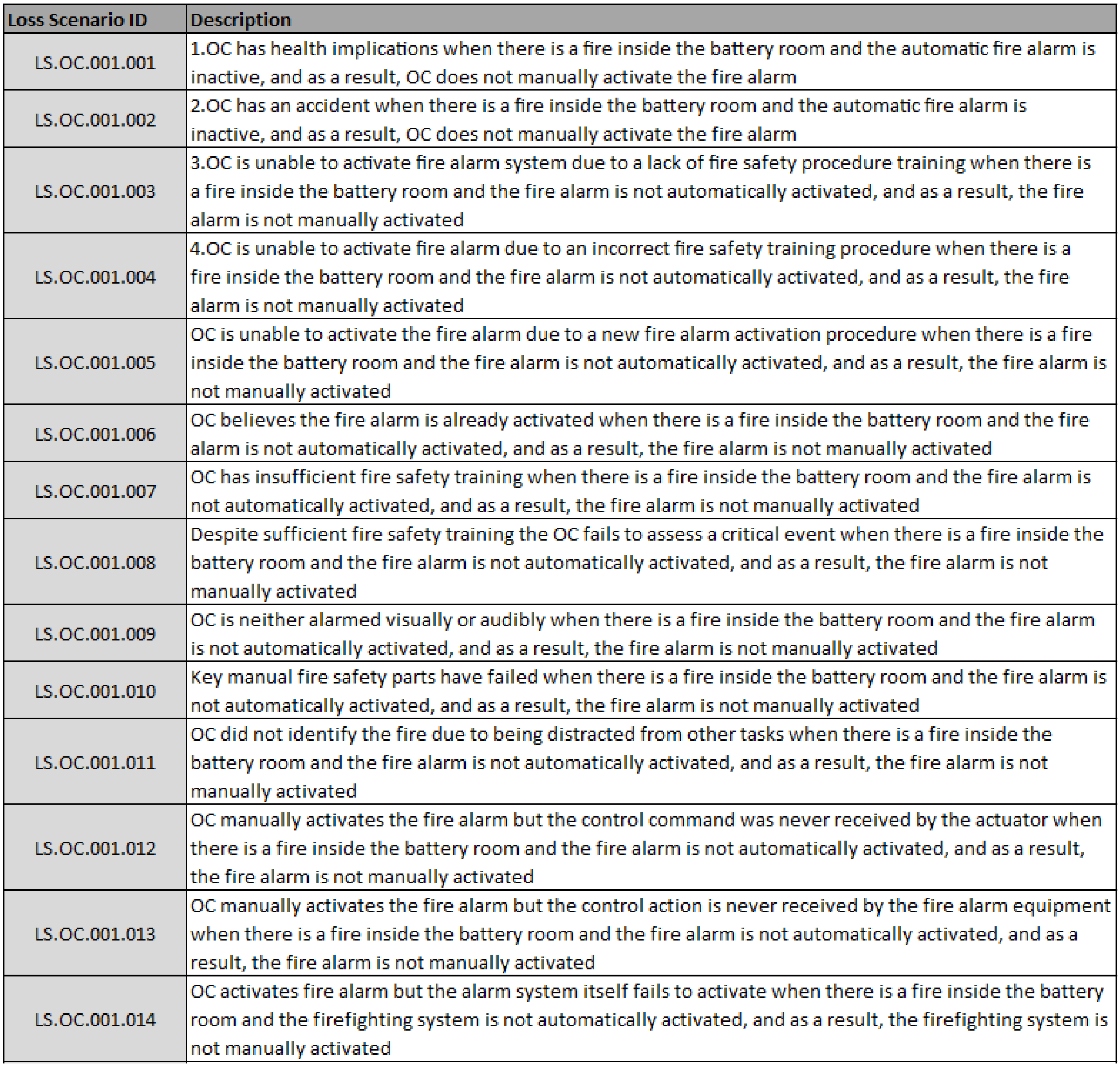
Table 19 – Loss Scenarios identified for UCA.OC.004



Loss Scenario ID	Description
LS.OC.004.001	OC has health implications when there is a fire inside the battery room and the firefighting system is not automatically activated, and as a result, the firefighting system is not manually activated
LS.OC.004.002	OC has an accident when there is a fire inside the battery room and the firefighting system is not automatically activated, and as a result, the firefighting system is not manually activated
LS.OC.004.003	3.OC is unable to activate firefighting system due to a lack of fire safety procedure training when there is a fire inside the battery room and the firefighting system is not automatically activated, and as a result, the firefighting system is not manually activated
LS.OC.004.004	4.OC is unable to activate firefighting system due to an incorrect fire safety training procedure when there is a fire inside the battery room and the firefighting system is not automatically activated, and as a result, the firefighting system is not manually activated
LS.OC.004.005	5.OC is unable to activate firefighting system due to an upgraded firefighting system and did not receive updated fire safety procedure training when there is a fire inside the battery room and the firefighting system is not automatically activated, and as a result, the firefighting system is not manually activated
LS.OC.004.006	6.OC believes firefighting system is already activated when there is a fire inside the battery room and the firefighting system is not automatically activated, and as a result, the firefighting system is not manually activated
LS.OC.004.007	7.OC has insufficient fire safety training when there is a fire inside the battery room and the firefighting system is not automatically activated, and as a result, the firefighting system is not manually activated
LS.OC.004.008	8.Despite sufficient fire safety training the OC fails to assess a critical event when there is a fire inside the battery room and the firefighting system is not automatically activated, and as a result, the firefighting system is not manually activated
LS.OC.004.009	9.OC is neither alarmed visually or audibly when there is a fire inside the battery room and the firefighting system is not automatically activated, and as a result, the firefighting system is not manually activated
LS.OC.004.010	10.Key manual fire safety parts have failed when there is a fire inside the battery room and the firefighting system is not automatically activated, and as a result, the firefighting system is not manually activated
LS.OC.004.011	11.OC manually activates the firefighting system but the control command was never received by the actuator when there is a fire inside the battery room and the firefighting system is not automatically activated, and as a result, the firefighting system is not manually activated
LS.OC.004.012	12.OC activates firefighting system but the control action is never received by the firefighting equipment when there is a fire inside the battery room and the firefighting system is not automatically activated, and as a result, the firefighting system is not manually activated
LS.OC.004.013	13.OC activates firefighting system but the firefighting equipment itself fails to activate when there is a fire inside the battery room and the firefighting system is not automatically activated, and as a result, the firefighting system is not manually activated

The table below represents loss scenarios for UCA.OC.001:

Table 20 – Loss Scenarios identified for UCA.OC.001



Loss Scenario ID	Description
LS.OC.001.001	1.OC has health implications when there is a fire inside the battery room and the automatic fire alarm is inactive, and as a result, OC does not manually activate the fire alarm
LS.OC.001.002	2.OC has an accident when there is a fire inside the battery room and the automatic fire alarm is inactive, and as a result, OC does not manually activate the fire alarm
LS.OC.001.003	3.OC is unable to activate fire alarm system due to a lack of fire safety procedure training when there is a fire inside the battery room and the fire alarm is not automatically activated, and as a result, the fire alarm is not manually activated
LS.OC.001.004	4.OC is unable to activate fire alarm due to an incorrect fire safety training procedure when there is a fire inside the battery room and the fire alarm is not automatically activated, and as a result, the fire alarm is not manually activated
LS.OC.001.005	OC is unable to activate the fire alarm due to a new fire alarm activation procedure when there is a fire inside the battery room and the fire alarm is not automatically activated, and as a result, the fire alarm is not manually activated
LS.OC.001.006	OC believes the fire alarm is already activated when there is a fire inside the battery room and the fire alarm is not automatically activated, and as a result, the fire alarm is not manually activated
LS.OC.001.007	OC has insufficient fire safety training when there is a fire inside the battery room and the fire alarm is not automatically activated, and as a result, the fire alarm is not manually activated
LS.OC.001.008	Despite sufficient fire safety training the OC fails to assess a critical event when there is a fire inside the battery room and the fire alarm is not automatically activated, and as a result, the fire alarm is not manually activated
LS.OC.001.009	OC is neither alarmed visually or audibly when there is a fire inside the battery room and the fire alarm is not automatically activated, and as a result, the fire alarm is not manually activated
LS.OC.001.010	Key manual fire safety parts have failed when there is a fire inside the battery room and the fire alarm is not automatically activated, and as a result, the fire alarm is not manually activated
LS.OC.001.011	OC did not identify the fire due to being distracted from other tasks when there is a fire inside the battery room and the fire alarm is not automatically activated, and as a result, the fire alarm is not manually activated
LS.OC.001.012	OC manually activates the fire alarm but the control command was never received by the actuator when there is a fire inside the battery room and the fire alarm is not automatically activated, and as a result, the fire alarm is not manually activated
LS.OC.001.013	OC manually activates the fire alarm but the control action is never received by the fire alarm equipment when there is a fire inside the battery room and the fire alarm is not automatically activated, and as a result, the fire alarm is not manually activated
LS.OC.001.014	OC activates fire alarm but the alarm system itself fails to activate when there is a fire inside the battery room and the firefighting system is not automatically activated, and as a result, the firefighting system is not manually activated

Controller 2: Remote Human Operator:

Table 21 – RHO responsibilities

Remote Human Operator (RHO)		
Responsibilities	Process Model	Feedback
Remotely activate firefighting system when it is neither activated automatically nor by onboard captain	• Fire inside battery room • Firefighting system not activated automatically nor by captain	• Firefighting system operating status
Contact rescue team and initiate evacuation process if OC is unable to	• Uncontrollable fire event • Evacuation initiated by OC is not possible	• Rescue team feedback • Evacuation progress status

Tabell 22 - RHO control action: Remotely activate firefighting system

Controller: Remote Human Operator									
ID	Control Action	Condition		Unsafe Control Actions?					
		Is there a fire inside the battery room?	Is the firefighting system already activated?	Not Provided	Provided	Too early	Too late	Too short	Too long
CA.RHO.001 CA.RHO.002 CA.RHO.003	Remotely activate firefighting system	Yes	Yes	Safe	Safe	Safe	Safe	Safe	Safe
		Yes	No	Unsafe [H3]	Safe	N/A	Unsafe [H3]	N/A	N/A
		No	Yes	Safe	N/A	N/A	N/A	N/A	N/A
		No	No	Safe	Unsafe [H5]	N/A	N/A	N/A	N/A

UCA.RHO.001: RHO does not remotely activate firefighting system when there is a fire inside the battery room and the firefighting system is not yet activated [H3].

UCA.RHO.002: RHO remotely activate firefighting system too late when there is a fire inside the battery room when the firefighting system is not yet activated [H3].

UCA.RHO.003: RHO do remotely activate firefighting system when there is not a fire inside the battery room and the automatic fire alarm is not activated [H5].

Tabell 23 – RHO control action: Contact rescue team and initiate evacuation

Controller: Remote Human Operator									
ID	**Control Action**	**Condition**		**Unsafe Control Actions?**					
		Is there a fire inside the battery room?	**Is OC able to contact rescue team and initiate evacuation?**	**Not Provided**	**Provided**	**Too early**	**Too late**	**Too short**	**Too long**
CA.RHO.001 **CA.RHO.002** **CA.RHO.003**	Contact rescue team and initiate evacuation	Yes	Yes	Safe	Safe	Safe	Safe	Safe	Safe
		Yes	No	Unsafe [H3]	Safe	N/A	Unsafe [H3]	N/A	N/A
		No	Yes	Safe	N/A	N/A	N/A	N/A	N/A
		No	No	Safe	Unsafe [H5]	N/A	N/A	N/A	N/A

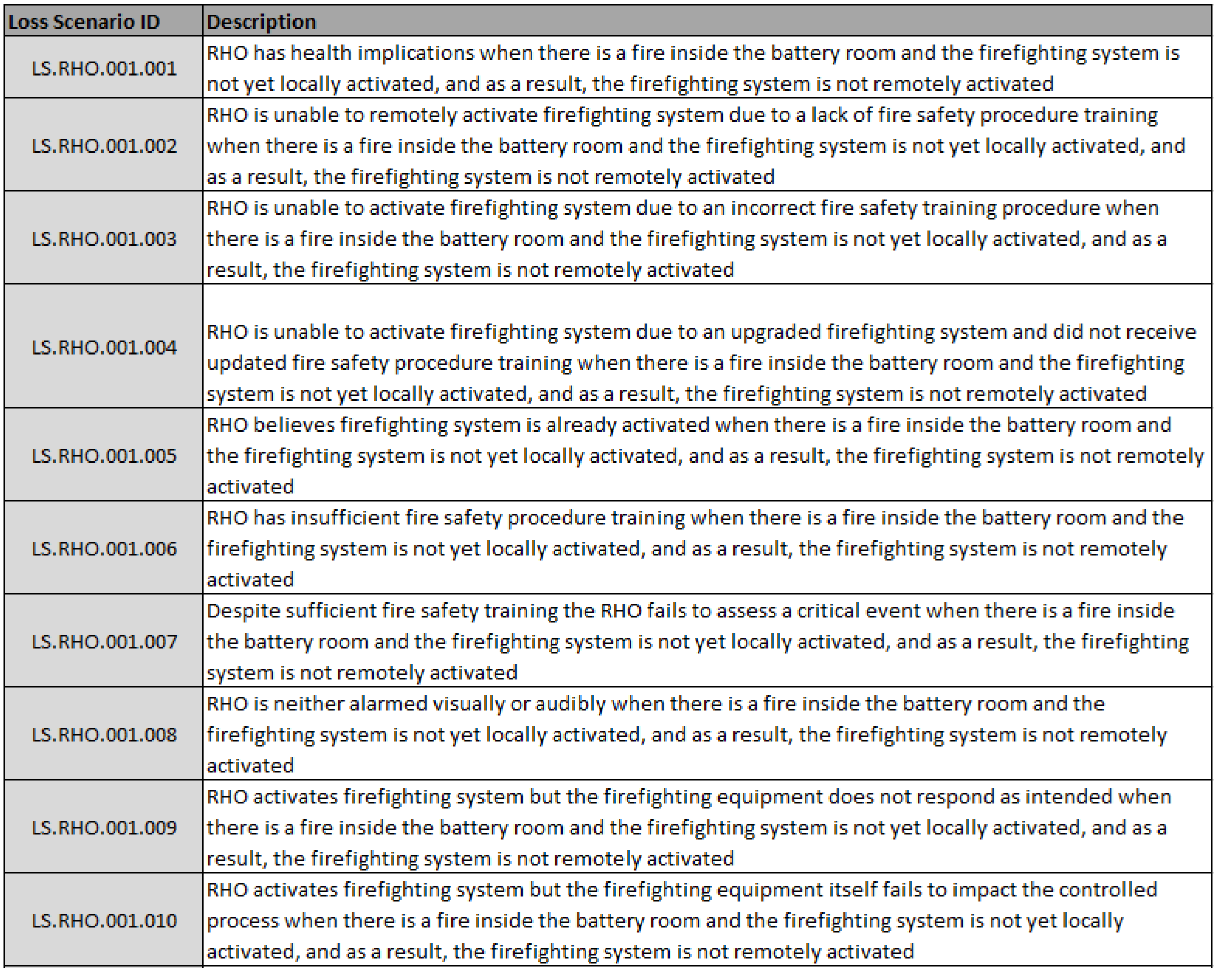
UCA.RHO.004: RHO does not contact rescue team and initiate evacuation process when there is an uncontrollable fire inside the battery room and the OC is unable to conduct the fire safety procedure [H4].

UCA.RHO.005: RHO contact rescue team and initiate evacuation process too late when there is an uncontrollable fire inside the battery room and the OC is unable to conduct the fire safety procedure [H4].

UCA.RHO.006: RHO do contact rescue team and initiate evacuation process when there is not an uncontrollable fire inside the battery room and the OC is unable to conduct the fire safety procedure [H5].

The table below represents loss scenarios for UCA.RHO.001:

Table 24 – Loss Scenarios identified for UCA.OC.001



Loss Scenario ID	Description
LS.RHO.001.001	RHO has health implications when there is a fire inside the battery room and the firefighting system is not yet locally activated, and as a result, the firefighting system is not remotely activated
LS.RHO.001.002	RHO is unable to remotely activate firefighting system due to a lack of fire safety procedure training when there is a fire inside the battery room and the firefighting system is not yet locally activated, and as a result, the firefighting system is not remotely activated
LS.RHO.001.003	RHO is unable to activate firefighting system due to an incorrect fire safety training procedure when there is a fire inside the battery room and the firefighting system is not yet locally activated, and as a result, the firefighting system is not remotely activated
LS.RHO.001.004	RHO is unable to activate firefighting system due to an upgraded firefighting system and did not receive updated fire safety procedure training when there is a fire inside the battery room and the firefighting system is not yet locally activated, and as a result, the firefighting system is not remotely activated
LS.RHO.001.005	RHO believes firefighting system is already activated when there is a fire inside the battery room and the firefighting system is not yet locally activated, and as a result, the firefighting system is not remotely activated
LS.RHO.001.006	RHO has insufficient fire safety procedure training when there is a fire inside the battery room and the firefighting system is not yet locally activated, and as a result, the firefighting system is not remotely activated
LS.RHO.001.007	Despite sufficient fire safety training the RHO fails to assess a critical event when there is a fire inside the battery room and the firefighting system is not yet locally activated, and as a result, the firefighting system is not remotely activated
LS.RHO.001.008	RHO is neither alarmed visually or audibly when there is a fire inside the battery room and the firefighting system is not yet locally activated, and as a result, the firefighting system is not remotely activated
LS.RHO.001.009	RHO activates firefighting system but the firefighting equipment does not respond as intended when there is a fire inside the battery room and the firefighting system is not yet locally activated, and as a result, the firefighting system is not remotely activated
LS.RHO.001.010	RHO activates firefighting system but the firefighting equipment itself fails to impact the controlled process when there is a fire inside the battery room and the firefighting system is not yet locally activated, and as a result, the firefighting system is not remotely activated

Controller 3: Integrated Automation and Safety System:

Table 25 – IASS responsibilities

Integrated Automation and Safety System (IASS)		
Responsibilities	Process Model	Feedback
Activate fire alarm	• Fire inside battery room	• Fire detection system status
Activate firefighting system	• Fire inside battery room	• Firefighting system status

Tabell 26 - IASS control action: Activate fire alarm

Controller: Integrated Automation and Safety System (IASS)								
ID	**Control Action**	**Condition**	**Unsafe Control Actions?**					
		Is there a fire inside the battery room?	**Not Provided**	**Provided**	**Too early**	**Too late**	**Too short**	**Too long**
CA.IASS.001 **CA.IASS.002** **CA.IASS.003**	Activate fire alarm	Yes	Unsafe [H2]	Safe	N/A	Unsafe [H2]	N/A	N/A
		No	Safe	Unsafe [H5]	N/A	N/A	N/A	N/A

UCA.IASS.001: IASS does not activate the fire alarm when there is a fire inside the battery room [H2].

UCA.IASS.002: IASS activate the fire alarm too late when there is a fire inside the battery room [H2].

UCA.IASS.003: IASS activate the fire alarm when there is not a fire inside the battery room [H5].

Tabell 27- IASS control action: Activate firefighting system

Controller: Integrated Automation and Safety System (IASS)								
ID	**Control Action**	**Condition**	**Unsafe Control Actions?**					
		Is there a fire inside the battery room?	**Not Provided**	**Provided**	**Too early**	**Too late**	**Too short**	**Too long**
CA.IASS.001 **CA.IASS.002** **CA.IASS.003**	Activate firefighting system	Yes	Unsafe [H3]	Safe	N/A	Unsafe [H3]	N/A	N/A
		No	Safe	Unsafe [H5]	N/A	N/A	N/A	N/A

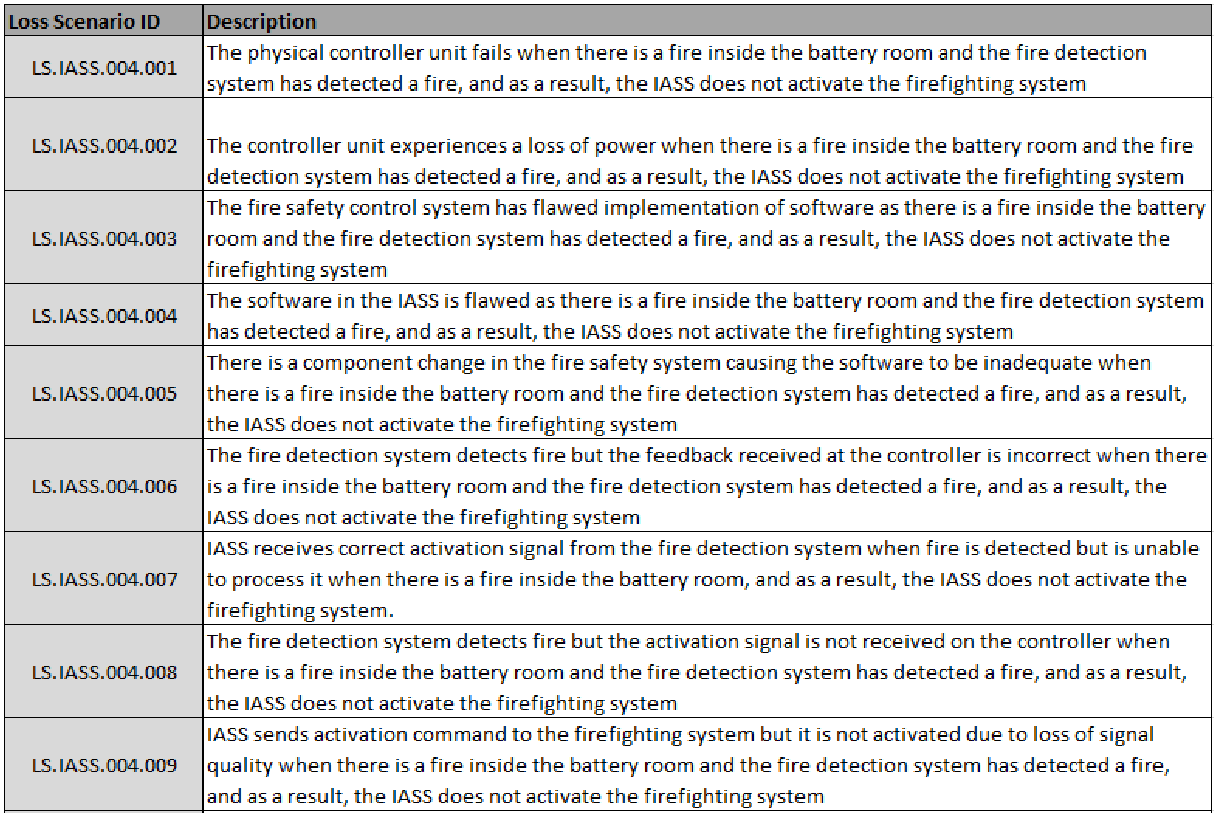
UCA.IASS.004: IASS does not activate firefighting system when there is a fire inside the battery room and the fire detection system has detected fire [H3].

UCA.IASS.005: IASS activates firefighting system too late when there is a fire inside the battery room and the fire detection system has detected fire [H3].

UCA.IASS.006: IASS activates firefighting system when there is not a fire inside the battery room, but the fire detection system has detected fire [H5].

The table below represents loss scenarios for UCA.RHO.001:

Table 28– Loss Scenarios identified for UCA.IASS.004



Loss Scenario ID	Description
LS.IASS.004.001	The physical controller unit fails when there is a fire inside the battery room and the fire detection system has detected a fire, and as a result, the IASS does not activate the firefighting system
LS.IASS.004.002	The controller unit experiences a loss of power when there is a fire inside the battery room and the fire detection system has detected a fire, and as a result, the IASS does not activate the firefighting system
LS.IASS.004.003	The fire safety control system has flawed implementation of software as there is a fire inside the battery room and the fire detection system has detected a fire, and as a result, the IASS does not activate the firefighting system
LS.IASS.004.004	The software in the IASS is flawed as there is a fire inside the battery room and the fire detection system has detected a fire, and as a result, the IASS does not activate the firefighting system
LS.IASS.004.005	There is a component change in the fire safety system causing the software to be inadequate when there is a fire inside the battery room and the fire detection system has detected a fire, and as a result, the IASS does not activate the firefighting system
LS.IASS.004.006	The fire detection system detects fire but the feedback received at the controller is incorrect when there is a fire inside the battery room and the fire detection system has detected a fire, and as a result, the IASS does not activate the firefighting system
LS.IASS.004.007	IASS receives correct activation signal from the fire detection system when fire is detected but is unable to process it when there is a fire inside the battery room, and as a result, the IASS does not activate the firefighting system.
LS.IASS.004.008	The fire detection system detects fire but the activation signal is not received on the controller when there is a fire inside the battery room and the fire detection system has detected a fire, and as a result, the IASS does not activate the firefighting system
LS.IASS.004.009	IASS sends activation command to the firefighting system but it is not activated due to loss of signal quality when there is a fire inside the battery room and the fire detection system has detected a fire, and as a result, the IASS does not activate the firefighting system

Controller 4: Battery Management System:

Table 29 – BMS responsibilities

Battery Management System (BMS)		
Responsibilities	**Process Model**	**Feedback**
Control battery levels to prevent thermal runaway	• Battery levels within SOA	• Battery state
Send alarm(s) to IASS	• Battery levels within SOA	• Battery alarm(s) activated

Tabell 30 - BMS control action: Control battery levels

Controller: Battery Management System (BMS)								
ID	**Control Action**	**Condition**	**Unsafe Control Actions?**					
		Is the battery operating within SOA?	**Not Provided**	**Provided**	**Too early**	**Too late**	**Too short**	**Too long**
CA.BMS.001 **CA.BMS.002** **CA.BMS.003** **CA.BMS.004**	Control battery levels to prevent thermal runaway	Yes	Unsafe [H1]	Safe	N/A	N/A	N/A	N/A
		No	Unsafe [H1]	Safe	N/A	Unsafe [H1]	N/A	N/A

UCA.BMS.001: BMS does not control battery levels to prevent thermal runaway despite operating within SOA [H1].

UCA.BMS.002: BMS does not control battery levels to prevent thermal runaway while operating outside SOA [H1].

UCA.BMS.003: BMS control battery levels to prevent thermal runaway too late while operating outside SOA [H1].

Tabell 31 - BMS control action: Send alarm(s) to IASS

Controller: Battery Management System (BMS)								
ID	**Control Action**	**Condition**	**Unsafe Control Actions?**					
		Is the battery operating within SOA?	**Not Provided**	**Provided**	**Too early**	**Too late**	**Too short**	**Too long**
CA.BMS.005 **CA.BMS.006** **CA.BMS.007**	Send critical alarm(s) to IASS	Yes	Safe	Unsafe [H5]	N/A	N/A	N/A	N/A
		No	Unsafe [H1]	Safe	Unsafe [H5]	Unsafe [H1]	N/A	N/A

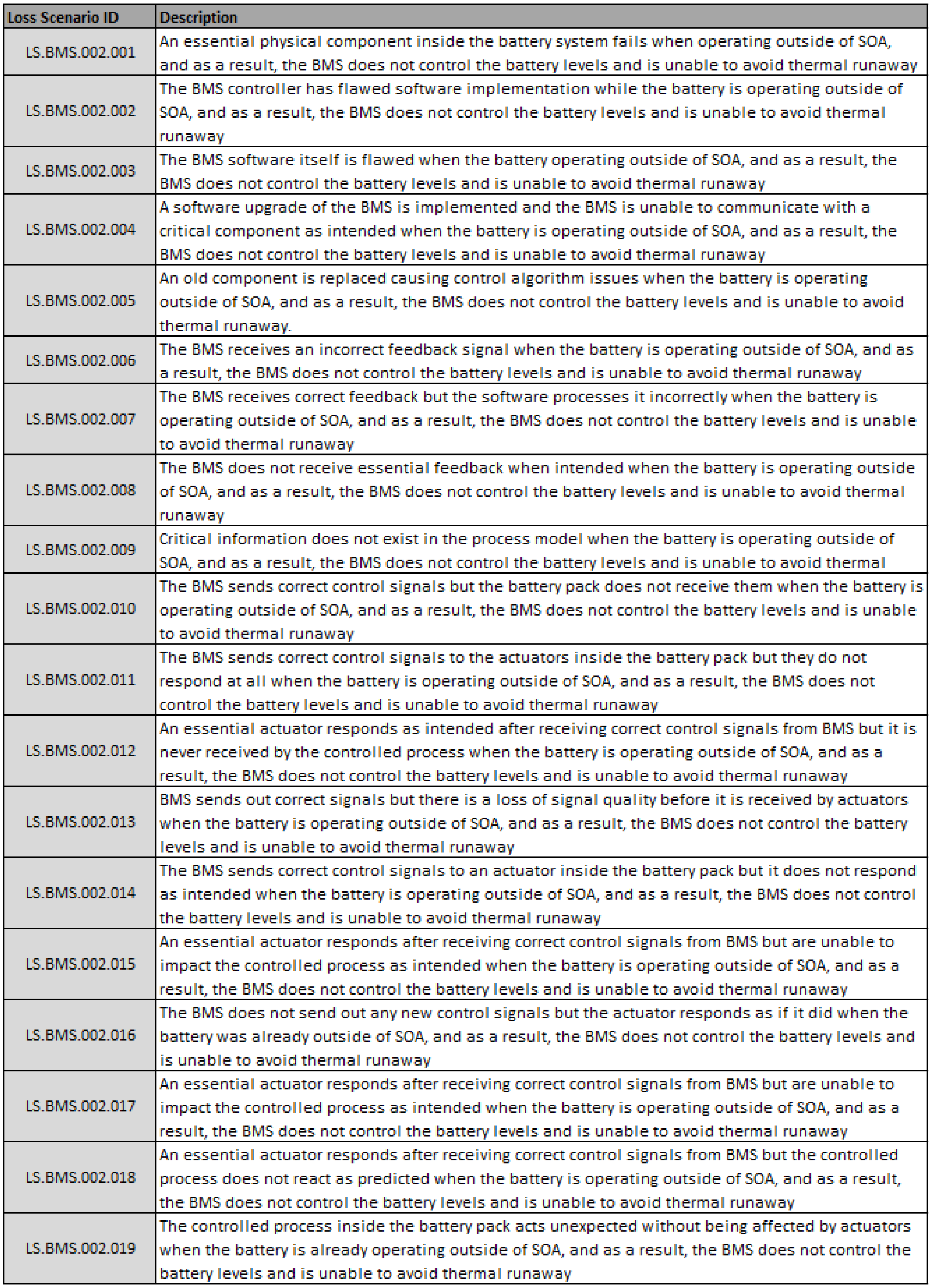
UCA.BMS.004: BMS send critical alarms to the IASS while operating within SOA [H5]

UCA.BMS.005: BMS does not send alarms to the IASS when the battery is operating outside SOA [H1]

UCA.BMS.006: BMS send alarms to the IASS too late when the battery is operating outside SOA [H1]

The table below represents loss scenarios for UCA.BMS.002:

Table 31 – Loss Scenarios identified for UCA.BMS.002



Loss Scenario ID	Description
LS.BMS.002.001	An essential physical component inside the battery system fails when operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.002	The BMS controller has flawed software implementation while the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.003	The BMS software itself is flawed when the battery operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.004	A software upgrade of the BMS is implemented and the BMS is unable to communicate with a critical component as intended when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.005	An old component is replaced causing control algorithm issues when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway.
LS.BMS.002.006	The BMS receives an incorrect feedback signal when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.007	The BMS receives correct feedback but the software processes it incorrectly when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.008	The BMS does not receive essential feedback when intended when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.009	Critical information does not exist in the process model when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal
LS.BMS.002.010	The BMS sends correct control signals but the battery pack does not receive them when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.011	The BMS sends correct control signals to the actuators inside the battery pack but they do not respond at all when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.012	An essential actuator responds as intended after receiving correct control signals from BMS but it is never received by the controlled process when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.013	BMS sends out correct signals but there is a loss of signal quality before it is received by actuators when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.014	The BMS sends correct control signals to an actuator inside the battery pack but it does not respond as intended when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.015	An essential actuator responds after receiving correct control signals from BMS but are unable to impact the controlled process as intended when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.016	The BMS does not send out any new control signals but the actuator responds as if it did when the battery was already outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.017	An essential actuator responds after receiving correct control signals from BMS but are unable to impact the controlled process as intended when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.018	An essential actuator responds after receiving correct control signals from BMS but the controlled process does not react as predicted when the battery is operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway
LS.BMS.002.019	The controlled process inside the battery pack acts unexpected without being affected by actuators when the battery is already operating outside of SOA, and as a result, the BMS does not control the battery levels and is unable to avoid thermal runaway