Automotive Campus 30
5708 JZ Helmond
P.O. Box 756
5700 AT Helmond
The Netherlands

www.tno.nl

T +31 88 866 57 29
F +31 88 866 88 62

TNO report

P00 | 1

Risk safety assessment framework for products that use batteries

Date November 25th 2022

Author(s)

Copy no	1
No. of copies	1
Number of pages	38 (incl. appendices)
Number of appendices	
Sponsor	Ministry of Infrastructure and Water Management
Project name	
Project number	

All rights reserved.
No part of this publication may be reproduced and/or published by print, photoprint, microfilm or any other means without the previous written consent of TNO.

In case this report was drafted on instructions, the rights and obligations of contracting parties are subject to either the General Terms and Conditions for commissions to TNO, or the relevant agreement concluded between the contracting parties. Submitting the report for inspection to parties who have a direct interest is permitted.

© 2022 TNO

Contents

1 Introduction

This report is a result of a preliminary investigation commissioned by the Ministry of Infrastructure and Water management. The main objective is to set up a framework to assess safety of current and future battery technologies in combination with applications wherein they are used.

The motivation for this investigation is the recommendations from the inventory of current legislation regarding battery safety conducted by Royal Haskoning [1]. From this inventory it appears that current legislation related to battery safety is based on commonly used lithium-ion battery types. Therefore, the advice is given to investigate safety risks also for other battery types.

In this document a framework is presented that can be used as a general approach to identify safety risks of a specific battery and its use in an application. This framework should be applicable for battery powered applications in the field of:

- Vehicles (e.g. passenger car, electrical bike).
- Non admitted vehicles (e.g. electrical step or hoverboard).
- Stationary applications (e.g. power aggregates, home batteries).
- Mobile machinery (e.g. forklift trucks, sweepers, agricultural tractors, mobile signage equipment).

These areas of application are a few examples to point out the diversity of applications for which the safety risk inventory framework shall be useable.

The framework shall provide high level insights in safety risks of batteries and their use in a product. It is a requirement that the framework can be implemented for a specific application and battery type in a pragmatic way. To perform and interpret the results of the assessment no profound expert safety knowledge shall be required. This to promote the safety discussion with several expertise’s and organisational levels.

The framework will limit to technical safety aspects that lead to immediate safety risk, meaning that for example legal aspects regarding safety are not considered.

2 Samenvatting

Dit rapport is een resultaat van een verkennend onderzoek waarvoor opdracht is gegeven door het Ministerie van infrastructuur en waterstaat. Het hoofddoel van het onderzoek is het opzetten van een raamwerk waarmee veiligheid geëvalueerd kan worden voor huidige en toekomstige batterijtechnologieën in de context van applicaties waarin ze gebruikt worden.

Aanleiding

Eén van de conclusies uit het onderzoek van Royal HaskoningDHV [1] 'Verkenning regelgeving veiligheid batterijen' met betrekking tot batterijveiligheid is dat alle fases van de batterij levenscyclus door regelgeving worden afgedekt. Echter veiligheid wordt niet in de verschillende fases integraal meegenomen. Dit leidt ertoe dat veiligheid van een batterij niet in voldoende mate geëvalueerd wordt in de context waarin deze later zal worden gebruikt. De aanleiding om dit onderzoek uit te voeren is de aanbeveling van Royal HaskoningDHV [1] om de informatievoorziening door fabrikanten te verbeteren met name om meer inzicht te verschaffen in de veiligheidsrisico's in relatie tot de toepassingscontext en meer inzicht te krijgen in de risico's van andere batterijtypen in aanvulling op lithium-ion. Dit rapport sluit aan bij die aanbevelingen door een methode te presenteren die gebruikt kan worden om risicoprofielen van batterijen op te stellen en die gebruikt kan worden om de veiligheid te evalueren van batterijen in de context van een gebruiksapplicatie.

Projectdoel

In dit rapport is een generieke aanpak beschreven waarmee op een gestructureerde manier een risico evaluatie voor verschillende batterijtechnologieën kan worden opgesteld . Aan de hand van een voorbeeld wordt geïllustreerd hoe de methode gebruikt kan worden. Ook is er een eerste overzicht met veiligheidsrisico's voor verschillende batterijtechnologieën welke verder uit te bouwen is. Een dergelijk overzicht kan gebruikt worden om, vanuit een veiligheidsoogpunt een geschikte batterijtechnologie te kiezen voor een applicatie. Een dergelijk overzicht kan ook door een batterijproducent aan een applicatiebouwer aangeleverd worden als input voor het opstellen van een risico evaluatie op applicatie niveau. Dit bevordert een integrale veiligheidsaanpak.

Aanpak

Om ervoor te zorgen dat batterijtechnologie in de context van een applicatie geëvalueerd kan worden is een raamwerk voor een evaluatiemethode opgesteld en beschreven. Dit raamwerk is gebaseerd op het raamwerk dat ontwikkeld is voor de Hyperloop technologie ([2], [3], [4]) en beperkt zich tot de technische veiligheidsaspecten gerelateerd aan de batterijtechnologieën in de context van een gebruiksapplicatie. Juridische, compliance en verzekering gerelateerde zaken worden dus bijvoorbeeld niet beschouwt in het raamwerk. Het raamwerk maakt het mogelijk om de veiligheid in kaart te brengen van complexe of nieuwe systemen waar huidige standaarden en methoden niet geschikt voor zijn.

Het raamwerk bestaat uit een set van documenten met ieder een aparte functie in het evaluatieproces die georganiseerd zijn in een overzichtelijke directory structuur. De algehele aanpak, en de implementatie is uiteengezet in een overkoepelend document. Hierin wordt met behulp van een fictief applicatie voorbeeld in de hoedanigheid van een elektrische step, waar een batterij onderdeel van uitmaakt, de

praktische implementatie geïllustreerd. Als handreiking zijn de gebruikte templates bijgevoegd, uitgelegd en deels exemplarisch ingevuld met betrekking tot de elektrische step om als voorbeeld voor de lezer te dienen.

Technische aanpak

De aanpak voor de batterijtechnologie veiligheidsevaluatie en het raamwerk voor de evaluatie van batterijen in de context van een applicatie zijn gebaseerd op de “ISO26262 Functional Safety For Road Vehicles” standaard die afgeleid is van de “IEC61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems”. De ISO26262 standaard is een op de automobielindustrie toegespitste afgeleide van de IEC61508. Beide standaarden beschouwen veiligheid integraal over de gehele levensduur van een product en ondersteunen het gebruik van andere standaarden zodat ook batterij gerelateerde standaarden meegenomen kunnen worden. Omdat de ISO26262 standaard zich richt op veiligheid met betrekking tot de functie en het falen ervan is een combinatie gemaakt met de “ISO/PAS21448 Safety Of The Intended Functionality” (SOTIF) die veiligheid van de beoogde functionaliteit beschouwt. Deze standaard beschouwt bijvoorbeeld onbedoeld- of verkeerd gebruik. Ook al is de basis voor het raamwerk gebaseerd op standaarden gerelateerd aan de automobielindustrie, toch is het resulterende praktische raamwerk generiek van aard. Het kan dus gebruikt worden voor het uitvoeren van veiligheidsevaluaties voor batterijtechnologieën, applicaties die gebruik maken van batterijen maar ook voor andere innovatieve applicaties.

Voor- en nadelen van de voorgestelde methode

Het implementeren van de complete ISO26262 standaard vereist significante inspanning. Om te komen tot een raamwerk dat een goed overzicht verschaft met betrekking tot veiligheidsrisico’s, is een praktische implementatie van de ISO26262 standaard ontwikkelt. Deze heeft de volgende voordelen: het beperkt additioneel werk voor de batterij/applicatie ontwikkelaar omdat het aansluit bij de geaccepteerde ontwerpstandaard; het voorziet in voldoende technisch overzicht dat ook door derden gebruikt kan worden voor evaluatie. Het nadeel van de methode is dat een evaluerende partij over technische veiligheid gerelateerde kennis moet beschikken. Tot op zekere hoogte is dat ook voor de hand liggend omdat er voor nieuwe technologieën of combinaties van bestaande technologieën minder of geen geschikte objectieve faalkans, impact of beheersingsindicatoren en beoordelingscriteria beschikbaar zijn door het ontbreken van praktische ervaring. Verder is er afstemming nodig tussen de ontwikkelaar en de evaluerende partij om de technische diepgang en subjectieve risico-assessment af te stemmen. Het is een proces waar beide partijen een rol en verantwoordelijkheid in hebben.

Aanbevelingen

Op basis van het verrichte onderzoek kunnen de volgende aanbevelingen gedaan worden:

- Omdat het niet mogelijk is om regelgeving geheel sluitend te definiëren voor toekomstige systemen en nieuwe combinaties van systemen, is het aan te bevelen om een partij te benoemen die de analyses en vorming van standaarden en normen structureel voor haar rekening neemt.
- In dit project is een aanpak ontwikkelt om veiligheidsrisico’s met betrekking tot batterijtechnologieën in kaart te brengen. Een logische vervolgstap zou zijn om op basis van deze aanpak een risico overzicht voor de meest voorkomende batterijtechnologieën op te stellen.

- Om het voorgestelde raamwerk te implementeren is het belangrijk om de voorgestelde aanpak af te stemmen met de beoogde partij die batterij risicoprofielen en applicaties die gebruik maken van batterijensystemen gaat evalueren. Op basis van deze afstemming kan indien nodig een verdiepingsslag plaatsvinden.
- Uitvoeren van een verkennende studie met betrekking tot bestaande en nieuw te ontwikkelen regelgeving. Onderwerpen die hierbij aandacht verdienen zijn bijvoorbeeld voorstellen tot aanpassing van normen en standaarden, aansprakelijkheid en verzekering.

3 Abbreviations

Abbreviation	Definition	Additional explanation
BMS	Battery Management System	
CCCV	Constant Current Constant Voltage	Li Ion Charge pattern
ESC	Electronic speed controller	Controller to operate a brushless motor
EV	Electric Vehicle	
FMEA	Failure Modes and Effect Analysis	
HARA	Hazard Analysis and Risk Assessment	
ISO	International Organisation for Standardisation	
ODD	Operational Design Domain	Specific operating domain in which a function is designed to operate properly.
PAS	Publicly Available Specification	
PEV	Personal Electric Vehicle	
SOC	State of Charge	
SOH	State of Health	
SOI	System of Interest	
SOTIF	Safety Of the Intended Functionality	

4 Background

Because of increasing complexity of novel systems (that may exist of a new combination of existing systems) it is more difficult to assess safety properly. This because current standards, normative or analysis methods may not be suitable. To prevent that safety is compromised in despite a novel system is compliant to relevant standards or normative which may not be suitable, an approach must be followed that results in a proof of safety instead of compliance to normative. Such an approach can be used to guard safety and gain knowledge to create or update normative.

Recently for Hyperloop which is considered to be a novel system for which current normative and standards may not hold, a safety framework is developed that enables assessment of safety based on a safety case. This framework allows a system developer to deliver proof that the system is safe by handing in a safety case that argues safety of the system. This safety case structure allows the system developer to use normative and standards but focusses on building on an argumentation why the system is safe. This argumentation can also provide the assessor insight in system knowledge that can be used to update or shape new standards. To interpret the safety case technical knowledge is required at the assessor.

In Table 4-1 an overview is shown of the main documents that describe the Hyperloop safety framework at mid-2022.

Table 4-1: Overview of the documents that form the safety framework developed for the Hyperloop application. The listing is in chronological order.

#	TNO report number	Title	Short description
1	TNO 2021 R10014 [5]	Develop a safety framework for evaluation and assessment of Hyperloop	Literature regarding safety standards and certification is considered and a high-level approach for the framework is presented. Moreover, the technologic independent framework, safety in the testing phase and interaction between developer and authority are discussed.
2	TNO 2021 R11990 [4]	Hyperloop safety framework for testing and certification: General safety approach	In this report the global framework development plan is presented. This plan exists of different steps that need to be taken (maybe in different projects) to develop the safety framework. All reports in this table are part of this development plan.
3	TNO 2021 P11783 [2]	Outline of a safety case	It describes the content related outline of a safety case and requirements that need to be fulfilled. In this report also the interaction process between applicant and assessor is described.
4	TNO 2021 R11991 [3]	Template and example of a safety case	In this report templates and an example of a safety case, that complies with the requirements defined in the reports listed above, is presented.

Parts of the Hyperloop safety framework can be used to assess safety of batteries and applications that included batteries. The advantage of using this approach is that it analyses on system level what possible safety hazards could be and with that provides insight in the safety risks that are involved. In the Hyperloop safety framework also, a part is included that argues how hazards are mitigated. Note that mitigating measures could also be following standards or normative. Although for this project that part will not be considered since this project focusses on risk identification.

At the authority also system knowledge is required in order to assess the safety case. Maybe this seems not desirable, but it will be inevitable to make sure that system safety is pursued instead of compliance to normative since the latter alone will not guarantee safety. Moreover, system knowledge can be used to update existing normative or standards or define new ones. Because one of the important goals of the safety case is to provide overview, a pragmatic implementation is pursued for the framework.

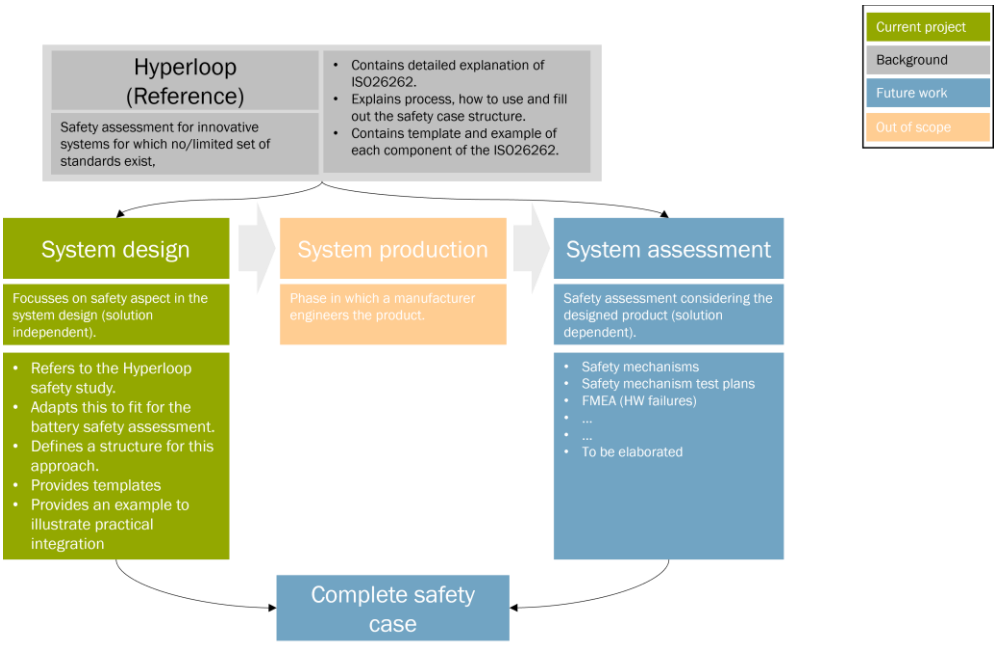

Figure 4-1: Risk safety assessment framework

Figure 4-1 shows the safety assessment framework. The Hyperloop safety framework [3] is used as the basis for the safety assessment framework for battery technologies. The hyperloop safety framework contains detailed explanation of the ISO26262 and explains its structure along with templates explaining how all the components of the ISO2626 can be filled.

The safety assessment framework for battery technology will concentrate on the safety aspects in the design phase of the system. To perform the full system safety assessment, there needs to exist a completed product. Hence, the battery safety assessment framework is limited to identification of risks and not mitigating them. A combination of the defined battery safety assessment framework along with the hyperloop safety framework will result in a completed safety case for a system.

5 Scope

In this chapter the scope of the assessment framework is defined. First the components of the battery that will be considered are defined in Section 5.1. Subsequently the scope of the safety analysis is defined in Section 5.2. Section 5.3 lists some specific items that are excluded from the scope.

5.1 System scope

This analysis focusses on the safety risk assessment for a battery pack and the application wherein it is used. There exist multiple forms of batteries, see [1] appendix 3 and [6] for a short overview. [7] focusses on low power batteries while in [8] a nice overview related to batteries for electric vehicles is given. This project focusses on battery packs that exists of the main components that are depicted in Figure 5-1.

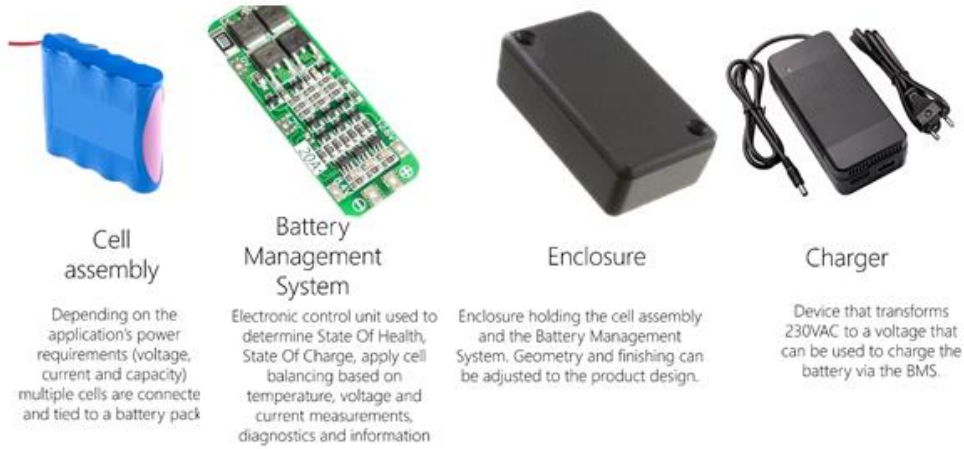

Figure 5-1: The battery pack and its main subcomponents as it will be considered in the assessment framework.

The reason for this focus is that such a pack includes all components to power an application that requires a multi cell battery pack that includes a battery management system for safety, capacity optimization, battery monitoring and charging.

The most important component of the battery pack is the cell assembly. To meet the voltage, current and capacity requirements of the application, multiple secondary cells are combined to a battery assembly as shown in Figure 5-1. This can be done by connecting multiple cells in series or parallel using busbars. To secure the assembly a shrink sleeve, tape or enclosure can be used. For cells also standard form factors are defined. Some well-known cell form factors are 18650 and 21700 which look similar to the basic batteries of which the cell assembly in Figure 5-1 exists.

In more advanced batteries a more advanced Battery Management System (BMS) is used to determine the State of Health (SoH), State of Charge (SoC), apply cell

balancing, diagnostics and information storage for monitoring. Cell balancing is a technique that optimizes the available capacity of cells that are used in series and is required because of variation of cell capacity that is a result of manufacturing variances, assembly variances, aging, impurities or environmental exposure. Due to this when a pack is charging, not all cells are charged equal, the BMS takes excess energy from the cells to get a pack in equilibrium. This is needed because overcharging the cells can lead to failures that compromise safety.
SoC information is used to provide information about the level of charge regarding its (maximum) capacity during the charging cycle. SoH provides information about the (remainder) electrical power available during the use cycle.

The enclosure of the battery pack provides structure to the pack and holds all the sub-components such as the cell assembly and BMS. Some applications require a specific shape, use of material or packaging because of the product's design. In these cases, a specific enclosure is designed by the product or battery manufacturer. For some applications the battery pack is provided by the battery manufacturer in a standard enclosure. These are most commonly used in applications where it is possible to "quickly" exchange the pack. Another way to house the parts is a shrink sleeve that is shrunk around the complete assembly.
The enclosure is included in this study because it is considered as relevant part for the safety analysis.

For charging of the battery pack a specific charger is used. The charger is considered in this analysis because in more advanced applications the charger also communicates with the BMS through a proprietary connector. In less advanced applications there is no communication between the BMS and charger. This can lead to safety implications.

5.2 Safety scope

From technical perspective functional and non-functional safety aspects are considered from design perspective. This means that by the framework only the safety risks of the product are identified. The mitigation measures and their realization are not considered.

In Figure 5-2 an illustration is shown of the main actors that are considered. These are the 'product' in which the 'battery pack' is used, the 'user' who operates the product and the 'environment' in which the product is used.

The safety risks posed by the user and the environment on the battery pack is the main consideration of this report and for the safety assessment framework.

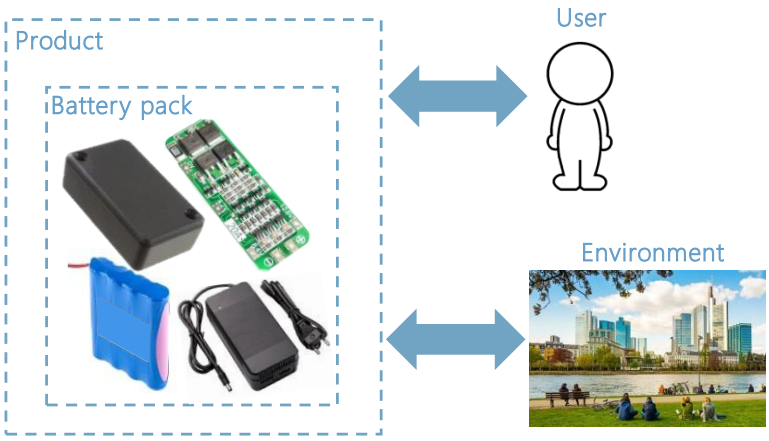

Figure 5-2: Main actors in the scope.

The safety analysis will focus on safety directly related to the battery pack. Safety issues of the product in which the battery is not involved is not considered. In Table 5-1 some examples are given to clarify this.

Table 5-1: Some examples to clarity the safety scope of the framework.

	Behaviour of the .... that leads	to hazardous behaviour of the	In scope?	Example
1.	Battery pack	Battery pack	Yes	A failure in the battery pack leads to a short circuit of battery cells that results in a fire.
2.	Product	Battery pack	Yes	Due to a temperature increase caused by the heating in the product the battery catches fire. The external temperature increase caused leads to an issue with the battery.
3.	User	Battery pack	Yes	The user drops the battery pack on the ground leading to damage to e.g. the battery cells or BMS that results in a short circuit and results in a fire.
4.	Environment	Battery pack	Yes	Due to rainfall and a bad sealing, moisture is entering the battery pack leading to corrosion that causes a short circuit in the BMS.
5.	Battery pack	Product	No	The temperature overheating protection disables the battery of an electrical step (product) that leads to regenerative braking loss while driving downhill. The battery pack itself causes no harm. It works properly. The loss of regenerative braking causes a safety issue.
6.	Product	Product	No	A fault in the product leads to a safety hazard in which the battery is not involved.
7.	User	Product	No	Misuse of the product by the user leads to a safety issue in which the battery is not involved.
8.	Environment	Product	No	The front tire of the bike (product) is punctured by debris leading to the cyclist falling.

The examples (in the fifth column) originate from combinations of the possible root causes (second column) and direct hazard source (third column). For the root causes the user, environment, product and battery pack are considered while for the direct hazard source only the product and battery pack are considered. The combinations that are considered in the safety framework are marked with a “yes” in the fourth column.

5.3 Excluded from scope

Excluded from the scope are legal matters such as the categorization of products to determine applicable normative, standards and legislation to which they need to comply to. Moreover, safety liability is not considered since it does not lead to an imminent safety risk.

6 Approach

In this chapter the approach used to construct the safety assessment framework for battery risk is explained.

6.1 Safety standards

In order to develop the safety framework for assessment of battery risk, the study done in the hyperloop safety framework is taken as basis. The reason for using this approach is due to the study conducted in chapters 4 and 5 of [9], where different safety standards are compared and the benefits and drawbacks of each are mentioned. Figure 6-1, graphically represents this. The safety standards from the domains of Automotive, Aviation, Railway, System Engineering and Battery technology studied in the hyperloop safety framework [4] are considered and the relevant aspects from the combination of these standards are used to define the battery safety assessment framework in this report.

The research about all the safety standards other than the battery specific standards, was already carried out previously in [4]. The main conclusion that can be drawn from this report is that most of these safety standards assess the system from a functional safety perspective and, that most of these standards are a descendant of the ICE61508. Functional safety considers safety critical aspects of the system due to its functionality. These can include safety aspects such as but not limited to charging and discharging of batteries and battery storage.

[1] and [10], outline all the safety standards concerning battery technology. The outcome of these research shows that the standards concerning the battery technology are mostly focused on the use and production of most commonly used battery types, e.g. lithium-ion batteries.

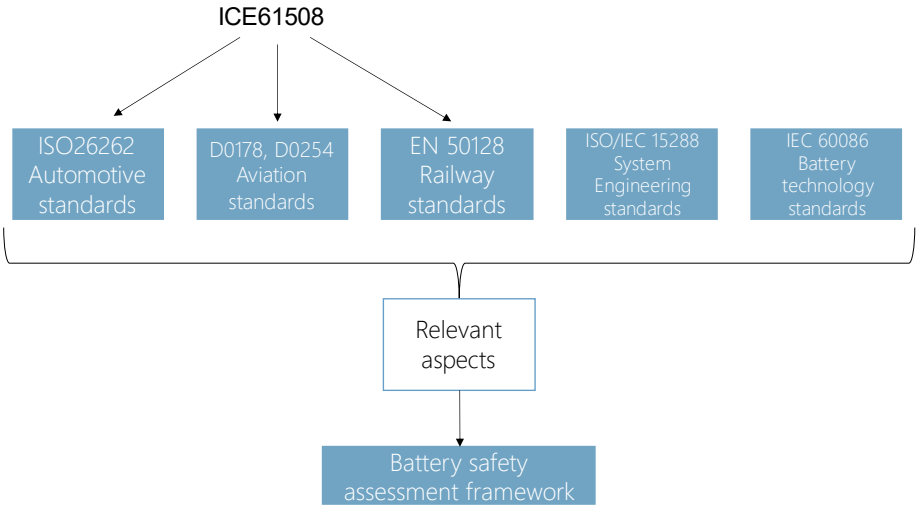

Figure 6-1: Considered safety standards

The studies show that there exist multiple norms and safety standards that can be applicable for the assessment of battery risk. Based on this and considering the expertise of TNO and in order to define a global safety assessment framework, that is applicable to most of the battery types, the following two methods will be considered within the scope of this report;

1. ISO26262 Functional safety of road vehicles, which is derived from ICE 61508.
2. Safety of the Intended Functionality (SOTIF) approach using the ISO21448, to assess the safety risk on the system due to external factors.

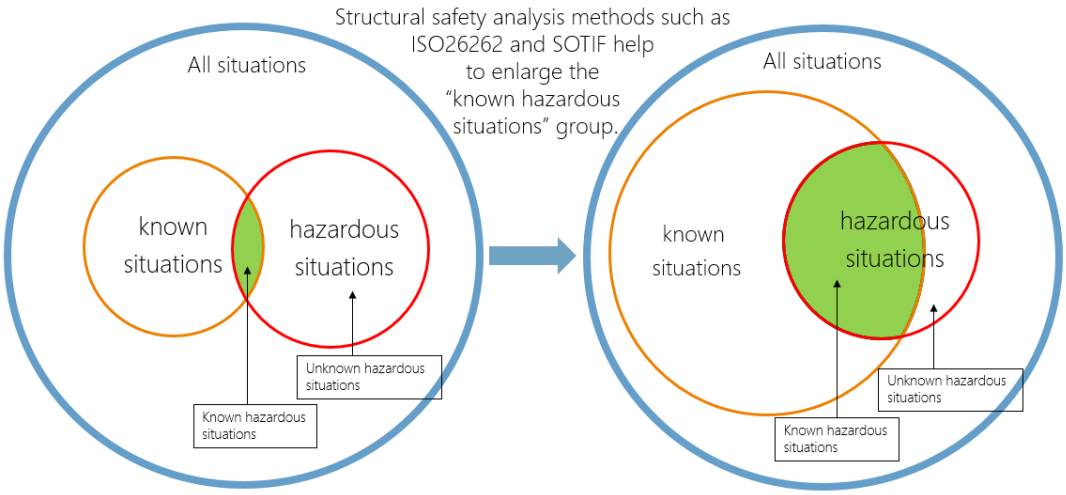

Figure 6-2: Illustrating the purpose of using the ISO26262 and SOTIF approach.

The reason for choosing the combination of these approaches is that they try to enlarge the known hazardous situations group by considering the system from different view angles. A great portion of the hazardous situations that originate from the systems functionality are assessed in the ISO26262 approach. The SOTIF

approach is used to enlarge the known hazardous situations group by considering external influences.

To illustrate this, in Figure 6-2 two Venn diagrams are shown. The blue circle indicates the group of all situations in which the product can be used. In the left diagram the subset of known situations is represented with the orange circle. The subset of hazardous situations is indicated with a red circle. The intersection of both (green part) represents all known hazardous situations. The Venn diagram on the right shows the impact of using structured analysis methods like the ISO26262 and SOTIF. Using these methods, the number of know hazardous situations (green area) can be increased by structural analysis of situations that can occur from perspective of the system functionality and failure (ISO26262) and additionally structural analysis from external aspects (SOTIF). Using this combination, the number of known hazardous situations can be enlarged (green area) because the coverage of known situations and with that probably a bigger portion of hazardous situations is identified.

6.2 ISO26262 approach

The ISO26262 Functional safety for road vehicles [11] is based on the IEC61508 and is tailored for automotive. This is a well-known standard in the field of automotive in which TNO has a lot of expertise and experience. It defines the concept of functional safety and elaborates on the tasks and methods to do the tasks during the safety life cycle of an automotive application.
Within the scope of the framework presented the standard is used to identify part of the hazardous situations. More specifically it provides a structural approach to make an inventory of hazards related to system operation and system failure.

6.3 SOTIF approach

ISO/PAS 21448 [12] is a complement to ISO26262 [11]. It is meant to identify hazards resulting from functional insufficiencies of the intended functionality from different view angles such as, but not limited to, foreseeable misuse and Operational Design Domain (ODD) limitations.

It covers the notion of functional safety with a minor difference in comparison with ISO26262. In ISO26262, the spotlight is on the function itself and failure of the function whereas in SOTIF, the failures of functions pertaining to a system which do not initiate from faults, [12]. This different view angle for identifying root causes for hazardous situation is a good way to increase the coverage of known hazardous situations as depicted in Figure 6-2.

From the SOTIF the following view angles analysis are selected to increase the number of known hazardous situations:

1. Misuse of the system
2. Triggering conditions
3. ODD exploration
4. System weaknesses

6.4 Implementation structure

The safety assessment framework consists of several parts which are organised in a directory structure. This directory structure is chosen to have a layered structured approach, with respect to the level of detail. This directory structure is a result of study carried out in the [3]. The folder structure is further explained in Chapter 7.

7 ISO26262 analysis

This chapter provides the reader of the safety case with some preliminary overview of parts of the safety methodology that can be adopted from the ISO26262 safety case structure. This because the scope of this framework is limited to risk assessment instead of safety evaluation, i.e. it focusses on the system before being build. As a result, the design, implementation, and validation of ISO26262 is not considered in this project. Therefore, only a limited part of the ISO26262 safety case structure is described in full detail. After reading this chapter it should be clear to the reader what parts of the ISO26262 safety case are relevant, how to use them, and where additional information such as the Hazard Analysis and Risk Assessment (HARA) or SOTIF can be found.

7.1 Typical safety case structure

In this section the structure of a typical safety case based on ISO26262 is presented. This structure is tailored for use during early product development but includes crucial elements needed for building a full safety case. How this particular safety case structure is formed and how it relates to the ISO26262, is elaborated in [11].
The same structure is also used for the safety assessment framework for battery technologies, because this structure is generic and can be applied to any system and system specific application. A graphical overview of the ISO26262 safety case structure is provided in Figure 7-1.

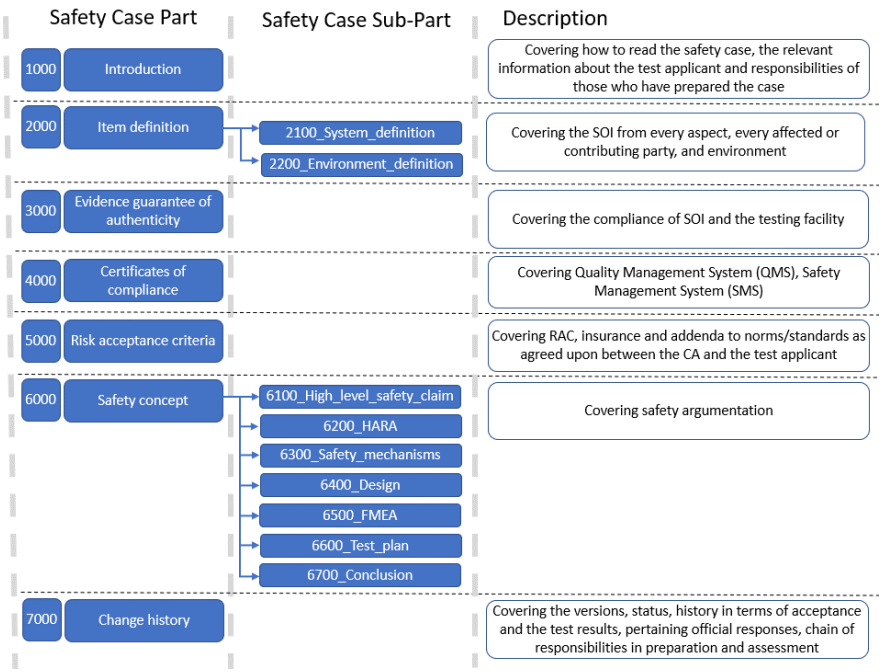

Figure 7-1: Structure of the ISO26262 safety case including a short description.

The structure differentiates between two levels:

Safety Case Part: Each *part* of the safety case is numbered using a 4-digit index number to allow for further nesting of documentation. Each *part* has a directory

assigned which contains existing documentation and typically contains future documentation relevant to those *parts*. At this level, several *parts* contain documentation, other parts merely contain directories assigned to sub-parts.

Safety Case Sub-Part: Certain parts of the safety case require further nesting of documentation. For example, 'Part 6000: Safety Concept' contains multiple *sub-parts* to further elaborate on different aspects of the safety concept. Each sub-part directory contains relevant *documentation* belonging to that specific sub-part.

In the last column of Figure 7-1 a short description is provided that should explain the content on a high level.

7.2 ISO26262 part selection for the battery safety assessment framework

Because this framework focusses on safety assessment no full safety case needs to be made. The subset of the general safety case used to perform the safety risk analysis for the battery can be found in Figure 7-2. The '1000 introduction' is maintained because it describes how the safety case is built and the components are related. To perform an assessment, it is important to describe the item in '2000 item definition'. The item is defined by the system of interest, in this case the battery. The item definition consists of a system and an environment definition.
The Sections '3000 Evidence guarantee of authenticity' and '4000 Certificates of compliance' are part of the risk assessment. This is because the associated risks of the battery are influenced by the production quality induced by the facilities available and its quality management systems. For a detailed description on how to fill in these general chapters is referred to [11].
'5000 Risk acceptance criteria' is relevant because it describes the acceptable risk from the perspective of the accessor. The document '6000 Safety concept', '6100 High level safety claim' which is made prior to the design phase is addressed in this project as well. The '6200 HARA' will be used to assess safety whereas in '6700 Conclusion' the result of the analysis will be summarized.

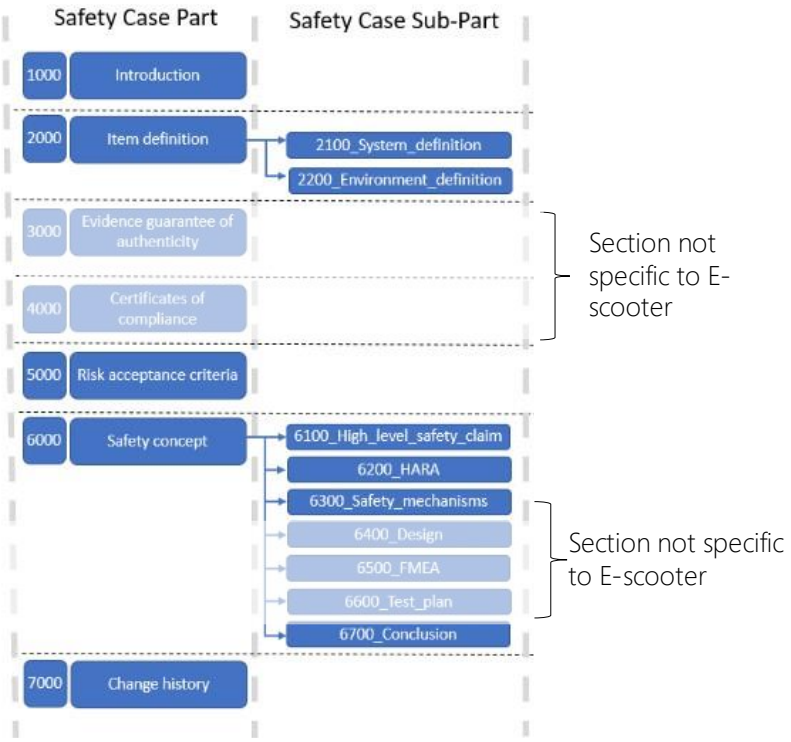

Figure 7-2: Selection of ISO26262 safety case from [3] that is found to be relevant for the battery safety assessment.

7.3 Implementation of the ISO26262 safety case selection

In this section it is described how the selected parts from the ISO262626 safety case of [3] are implemented for the battery framework. For the selected parts the instructions and/or guidance documentation will be used to set up the analysis. For convenience and contractionary to the proposed templates, the work products will be included in this document.

8 SOTIF analysis

In this chapter the approach regarding the use of Safety Of The Intended Functionality (SOTIF) for the battery safety assessment is described. The SOTIF approach used in this work is based on the ISO21448 standard.

Within section 8.1, first it is described what SOTIF is about. Subsequently in section 8.2 it is described how the SOTIF analysis is made. In section 8.3 the relation to the safety case is described briefly. The chapter is concluded with a small section explaining why the SOTIF approach is selected. This approach of explaining the SOTIF is chosen because it is in line with the explanation approach used in the 1000_Introduction document of the [3].

8.1 What is it?

Safety Of The Intended Functionality (SOTIF) focusses on the absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons [12]. It focusses on guidance of the applicable design, verification and validation measures needed to achieve the SOTIF. SOTIF can be considered complementary to the ISO26262.
SOTIF is an analysis methodology that tries to identify lack of safety by considering the product to be assessed from different view angles. Using this approach, the number of known hazardous situations presented in Figure 6-2 can be increased. For the battery safety assessment, not the whole SOTIF is used but a selection of the most applicable analysis methods. If the potential risk of the application is high, additional analysis methods can be selected.

8.2 How is it made?

The SOTIF is made in a Microsoft Excel document that can be found in the ‘Safety_assessment_SOTIF’ directory. The excel contains several tabs in which parts of the analysis is documented. E.g. ‘0. Approach’, ‘1. Cover page’, ‘2. Change tracking’, ‘3. SOTIF’ and, ‘4. Lists’ in which the whole SOTIF is explained and performed. On ‘0. Approach’ the instruction on how to fill in the SOTIF analysis are included. The tab ‘1. Cover page’ and ‘2. Change Tracking’ includes a standard cover page and change tracking that can be used. The actual analysis is included on the tab ‘3. SOTIF’. The last tab ‘4.Lists’ includes the lists that are used in the analysis.

8.3 How does this product relate to the safety case?

SOTIF analyses safety by assessing the system from different view angles that do not focus on the functionality and failure of the design. In that sense it is complementary to the ISO26262. The main purpose of applying a subset of applicable analysis methods proposed in the SOTIF is to increase the number of foreseen hazardous situations.

Below an overview is given of the SOTIF analysis methods that are selected for the application considered.

1. Misuse:
   A method to identify unforeseen hazards is to consider misuse. In [12], section 6.5 and Appendix B.1 Figure B.1 – 'systematic derivation of SOTIF misuse scenarios' an analysis method is provided that focuses on identifying hazardous situations from the perspective of misuse. Misuse situations can be identified using different approaches. E.g. From expert knowledge, brainstorming by designers, evaluating environmental conditions, human errors due to false recognition or human errors due to lack of system understanding.

2. Triggering conditions
   To make sure that the amount of unknown hazardous scenarios is decreased in an early design phase, hazards are identified which results from certain triggering conditions. In this approach it is tried to find hazardous use cases in a structured way that result from triggering use cases according [12], chapter 7 'Identification and evaluation of performance limitations and potential triggering conditions'. This analysis will increase the understanding of the limitations of the system and will improve the identification of the unknow triggering conditions that lead to hazardous situations.

3. ODD boundary exploration:
   It is expected that the exploration of the ODD boundary will also lead to identification of new hazardous events. Here insufficiencies can occur that could affect the system performance. E.g. Poor battery performance in very cold weather. The outcome of this analysis could lead to a modification/redefinition of the ODD. More information about the ODD boundary exploration can be found in Section 7.3, Section 9.2 and Annex C of [12].

4. System weaknesses
   The investigation of unknown hazards due to system weaknesses is described in this section. The activities that need to be performed to evaluate system weaknesses include evaluation of the known component weaknesses as a result of the system design. E.g. image resolution in camera detection systems which results in degraded object tracking. In 'B4.3.1 analysis of system weaknesses' of [12] more details can be found.

8.4 Why is this approach chosen?

The SOTIF is chosen to include "unforeseen" issues and external influences that can have effect on the product safety. SOTIF is also developed because there existed a need to consider safety of a system in a broader context that does not only focus on failure of the system.

9 Battery pack risk safety characteristics overview

In order to perform a detailed analysis of the risks that a battery pack poses, the components, functions and characteristics of the battery pack are described. Then using the analysis methods presented earlier an overview of risks related to battery packs is made that can be used as an input to analyse safety of an application that uses a specific battery pack.

9.1 Goal and approach

In this section the approach to create an overview for different battery pack types that provides insight in immediate safety related properties is given. In Figure 9-1 the five steps that need to be taken to create the overview are shown. In the next sections each of these steps will be discussed.

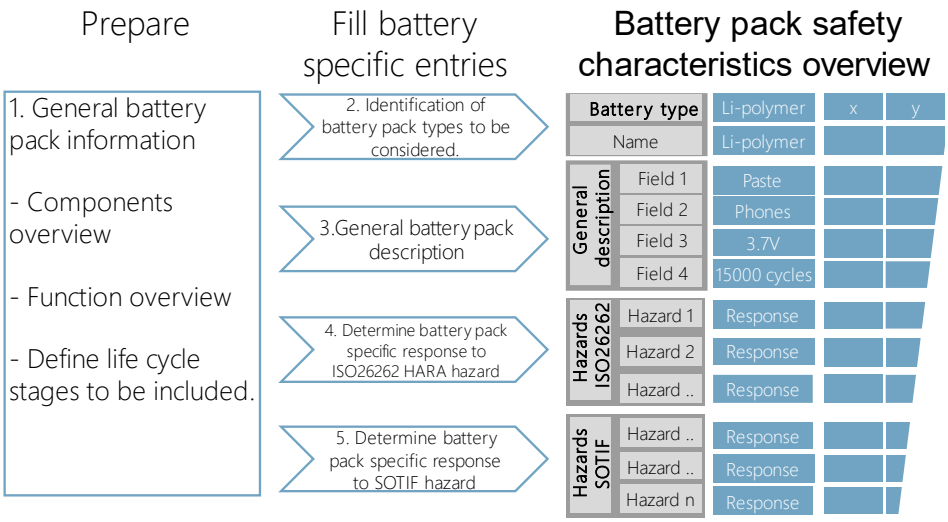

Figure 9-1: Illustration to explain the approach on how to create an overview of safety critical battery pack characteristics for multiple types in a structured way.

The right coloured part of Figure 9-1 shows the rough structure of the Battery pack safety characteristics overview. The blue columns contain information of a specific battery type. The two top rows are used to identify the battery pack type. A suggestion how to create an inventory of battery types is elaborated in section 9.3. In the 'general description' fields some information about the battery pack that foresees the reader with an understanding about the battery pack is provided. In section 9.4 a proposal for these fields is made. In the 'Hazards ISO26262' and 'Hazards SOTIF' part of the overview, hazards resulting from a general battery pack safety risk inventory are listed. For each battery the response to the hazard is described.

In the overview immediate safety related risks that are a result from the ISO26262 approach and SOTIF approach are included. ISO26262, deals with anything related to the functions of a battery, e.g. Charging, Storage and Use. All hazards that are covered in the ISO26262 deals with intended use of the system. SOTIF, deals with

anything that goes beyond the ISO26262, e.g.: Misuse. All hazards in the SOTIF deal with unintended (but foreseeable) use of the system.

To perform the analysis, general information about batteries need to be gathered. The next section will elaborate on this.

9.2 General battery pack information

In this section, the general battery pack information is discussed. This includes the components of the battery pack and their functions, as described in section 9.2.1, and the lifecycle of the battery pack as described in section 9.2.2.

The components and their functions, and the stages of the lifecycle described here will be considered for the identification of hazards, and the subsequent effect of failures (response) of each battery type, as seen in Figure 9-1.

9.2.1 Components and functions

The battery pack considered, will exist of the components shown in Figure 5-1 and the description of the components given in Section 5.1. Table 9-1 shows some additional details, regarding the functions of each battery component. These functions are used to assess the hazards concerning the battery pack.

Table 9-1: Overview of system components and functions

	Component	Function
1	Enclosure	Hold all components
		Protect components
		Provide heat dissipation
		…….
2	Battery management system	Determine state of health
		Determine state of charge
		Apply cell balancing
		…….
3	Cell assembly	Store power
		……..
4	Charger	Charge

9.2.2 Lifecycle

Below an overview is provided of the different lifecycle stages of a battery. These life cycle stages are introduced to make sure that related hazards can be identified by considering a specific life cycle stage.

- Production (Manufacture):
  This is the step where the individual cells are linked together, packaged, and fitted with a BMS. Risks associated with this step can be: e.g. short circuit, cell compression or improper joining of cells.

- Storage (in warehouse): This is “unmonitored” storage in a warehouse before shipping to either vendors or customers. Risks associated with this step can be: e.g. moisture or temperature issues.

- Transport (3rd party/Manufacture/customer):
  This is “unmonitored” shipping of the battery pack, by e.g. plane, ship or truck. Risks associated with this step can be: e.g. shock, over temperature or moisture.

- Use (customer):
  This is actual usage, so the battery is being discharged and charged by usage. Risks associated with this step can be: e.g. system failure or misuse.

- Recycling /Disposal
  This is the stage where the battery is stored to be disposed or recycled into second life.

9.3 Identification of battery pack types to be considered.

To select battery types that will be considered the following approach is suggested. In a literature survey, publications will be identified that provide insight in battery types, their usage (what products, trend) and provide information relation to safety. To provide a practical example a small number of references are studied to illustrate how to create the battery pack safety property overview. To create a more complete overview additional surveys and investigations are required.

Below in table an overview is given of the battery types that will be included in the battery safety property overview. These battery types are mentioned in [6] [7] [8].

Table 9-2: Initial overview of battery packs to be considered.

Battery pack family	**Construction**	**Abbreviation**
Lithium Ion	Jelly roll or pouch pack	Li-Ion
Lead Acid	polymer shell with "wet" anode/cathode	PB
Nickel	Cylindrical	Ni-Mh
Nickel Cadmium	Cylindrical	Ni-Cd
Gel battery (Lead Acid)	polymer shell with "wet" anode/cathode	AGM
Sodium Ion	Jelly roll or pouch pack	Na-Ion
Placeholder	Placeholder	Placeholder

9.4 General battery pack description

To provide the reader of the overview a general idea of the battery and its use, a few fields are added with general information. The number of fields is not fixed and can be extended when needed but to keep overview the following fields are suggested:

- Battery technology: Provides the fundamental technology used to store electrical charge in the battery.

- Chemistry: Provides the information of battery chemistry. Such as, the material from which the anode, cathode and the electrolyte of the battery are made.
- Abbreviation: Provides the working name abbreviation.
- Construction: Provides information about the physically battery cell construction and its shape.
- General use: This gives an outline about the potential use case of the battery type.
- Lifetime: This gives an idea about the lifespan of the battery pack.
- Nominal Single Cell Voltage: Provides the rated nominal voltage of each cell in the battery pack.

9.5 Determine battery pack specific response to ISO26262 hazard

To come up with relevant hazards, a part of the risk and hazard inventory approach of the ISO26262 is used. In particular based on the input gathered in step1 general battery pack information of Figure 9-1 the first two steps of the HARA approach (elaborated in '6200_HARA_application_example' on tab '0.Approach') are performed. In these steps based on the battery pack function break down possible hazards are identified.
Subsequently for each battery the response to the hazard is identified and added to the Battery pack safety characteristics document.

9.6 Determine battery pack specific response to SOTIF hazard

The hazards relevant to the SOTIF approach are derived in this step. The first two steps mentioned in the SOTIF document are used to arrive at the hazards for which for each battery pack the effect of failure is determined. Note that is also can be the case that a certain hazard is not applicable for a certain battery type.

9.7 Battery pack safety characteristics overview

Following the steps mentioned in Figure 9-1 and the explanation in the sections above, a table with the overview of different battery types and their hazards can be compiled. This table can be found in the document named, 'Battery pack safety characteristics overview'.

Figure 9-2, shows a screen shot of this document, this table is set up such that it can be expanded with more battery types and, more functions and hazards that relate to it. Based on the mentioned battery characteristics and hazards of different battery pack types, a choice of battery pack type can be made for the battery application.

Figure 9-2: For illustrational purpose part of the battery pack safety characteristics overview is shown.

10 Exemplary product risk safety assessment

To demonstrate how to practically implement the proposed framework an example is included. In this chapter the example of a fictitious e-scooter is introduced. The e-scooter example focuses only on arriving at the hazards using the ISO26262 and the SOTIF approach. Because the exemplary product is fictitious, not a complete safety case can be created but limited to work products that help the reader with the compilation of the safety case. In section 10.1 the focus is on describing the different components of the safety framework, and to explain the included and the excluded components of the safety framework. The following sections also show how the combination of the safety framework defined in this study along with the safety case of Hyperloop [3] results in a complete safety case of a system. More detailed and extensive instructions per component are described in the respective documents.

10.1 Safety framework component overview

This section gives an overview of the different components involved in the battery safety assessment framework. Figure 10-1, shows the folder structure and the documents involved in setting up the exemplary product risk safety assessment. The following sections explain each of these components in more detail.

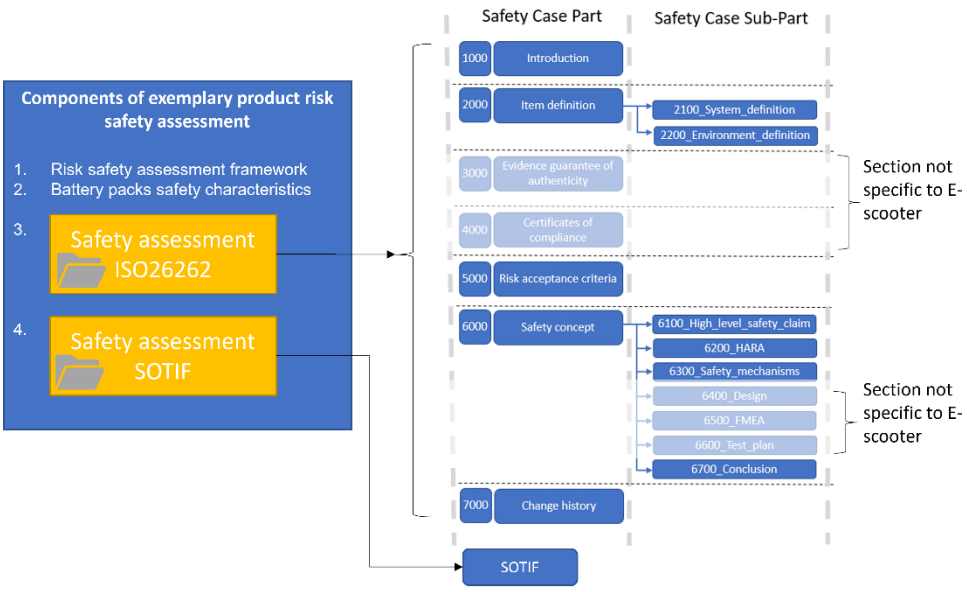

Figure 10-1: Components of the safety framework

Table 10-1, gives an overview of all the safety assessment components. It defines where each component can be found. Since the focus is on arriving at hazards of the exemplary product, some of the components refer to [3], for completeness of the safety case.

Table 10-1: Overview of safety assessment framework components

	Component	Document reference
1.	Risk safety assessment framework	
2.	Battery packs safety characteristics	Battery pack safety characteristics overview.xlsx
3.ISO26262	1000 Introduction	See [3]
	2000 Item definition	
	2100 System definition	2100 System Definition E scooter.docx
	2200 Environment definition	2200 Environment definition E scooter.docx
	3000 Evidence guarantee of authenticity	3000_Evidence_guarantee_of_authenticity _overview_Template_Hyperloop.docx
	4000 Certificates of compliance	4000_Certificates_of_compliance_ Overview_Template_Hyperloop.docx
	5000 Risk acceptance criteria	5000_RiskAcceptanceCriteria_application_example.xlsx
	6000 Safety concept	
	6100 High level safety claim	6100_High_level_safety_claim_E_scooter.docx
	6200 HARA	6200_HARA_E_scooter.xlsx
	6300 Safety mechanisms	6300_SafetyMechanisms_E_scooter.docx
	6400 Design	6400_Physicial_architecture_Example_Hyperloop.pptx
	6500 FMEA	6500_FMEA_Example_Hyperloop.xlsx
	6600 Test plan	6600_Test_Plan_Example_Hyperloop.docx
	6700 Conclusion	6700_Conclusion_Example_Hyperloop.docx
	7000 Change history	7000_VersionControl_application_example.xlsx
4.SOTIF	SOTIF	SOTIF_E_scooter.xlsx

10.2 Risk safety assessment framework

This document is the main report document of the battery risk safety assessment framework. It describes (in this chapter) the example work products.

Figure 10-2 shows the overview of how the safety assessment framework should be used and how the components interface with each other. Within the item definition the System Of Interest (SOI) is defined. This document serves as the input for the SOTIF analysis and the definition of the high level safety claim and the HARA. The outcome of the HARA and the SOTIF analysis is then used to define the safety mechanisms, the outcome of the safety mechanisms then results in the design (redesign or improvement) of the SOI.

The process of incorporating the outcomes of the HARA and SOTIF analysis in the safety mechanism and the design of the system of interest, ensures that relevant tests are defined in the test plan to check the mechanisms and thus the mitigating measures to avoid the hazards identified.

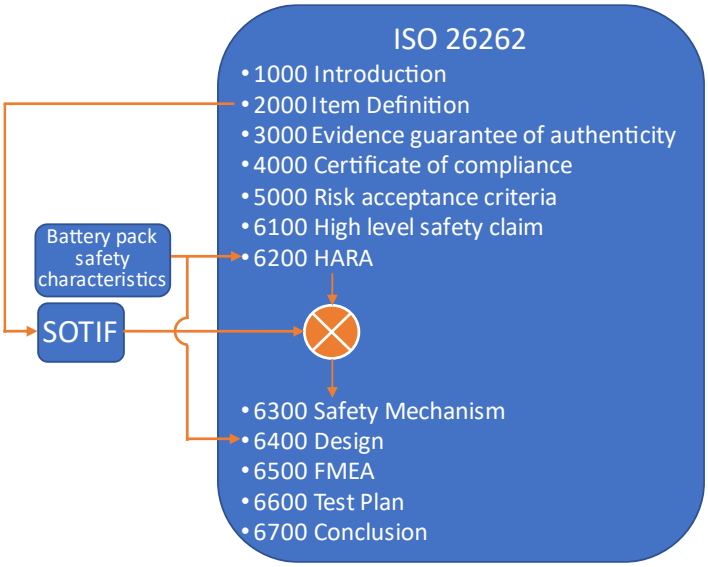

Figure 10-2: Process of filling out the safety case

10.3 Battery packs safety characteristics

The battery packs safety characteristics document gives an overview of all the characteristics and, the hazards of each type of battery pack derived based on the ISO26262 HARA and the SOTIF methods. This document is made in excel, to have a better overview of all the battery packs at once. More information about how the battery packs safety characters overview table is constructed is explained in chapter 9. This document can be extended to fit compare additional types and chemistries of batteries.

The overview of the above-mentioned document is used to fill the 6200 HARA but also to select a more suitable battery pack for the battery application in the 6400 Design. In Figure 10-2 the relation of the battery pack safety characteristics document with the ISO26262 process is illustrated.

10.4 Safety assessment ISO26262

The exemplary product (E-scooter) safety assessment using the ISO26262 is performed according to the explanation in Chapter 7. Detailed explanation of how to conduct each of the safety assessment framework components and their template descriptions are defined in the respective documents located in the folder structure.

The following sections provide an overview of what each component of the safety assessment consists of and explain what document is used to conduct that specific step in the process.

10.4.1 1000 Introduction

This document outlines the safety assessment process using the ISO26262 in detail. The document describes the relation between all documents related to the safety case.

Because the document is not application depended a reference is made to [3], where the document “1000_Introduction_To_The_Safety_Case.pdf” can be found in the folder “1000_Introduction” of the directory structure.

10.4.2 2000 Item Definition

Within this part, the SOI is described in detail. For this, it is important to describe the system itself and the environment in which the system is used. Both are described separately in 2100_System_definition and 2200_Environment_definition.

10.4.2.1 2100 System definition

The fundamental goal of this document is to define the SOI (E-scooter) for which the safety assessment is carried out. This document serves as the basis for the safety case.
The document for the e-scooter can be found in:
...\Safety_assessment_ISO_26262\2000_Item_definition\2100_System_definition\2100_System_Definition_E_scooter.pdf

In this document, the e-scooter is described as a product, together with the battery. The functionality of the e-scooter is described and the characteristics and type of use of the battery types are listed.

More detailed information about the system definition can be found in [3]. To be more precise in the section “2100 System definition” of the document “1000_Introduction_To_The_Safety_Case.pdf” that can be found in the folder “1000_Introduction” of the directory structure.

10.4.2.2 2200 Environment definition

This document describes the environment conditions for the operation of the system (E-scooter). In this case it describes the road related conditions and weather conditions, but more applicable environment conditions may be described if applicable.
This document for the e-scooter can be found in:
…\Safety_assessment_ISO_26262\2000_Item_definition\2200_Environment_definition\2200_Environment_definition_E-scooter.pdf

More detailed information about the environment definition can be found in [3]. To be more precise in the section “2200 Environment definition” of the document “1000_Introduction_To_The_Safety_Case.pdf” that can be found in the folder “1000_Introduction” of the directory structure.

10.4.3 3000 Evidence guarantee of authenticity

The products (subcomponents of the entire system) and/or facilities used during the development of the system of interest, can already be certified. These certificates can be of value in guaranteeing the safety of the SOI (E-scooter). All such certificates are added to this document.

For instance, if the wires used to connect the battery to the propulsion motors are compliant to a specific relevant standard or normative, the specific certificate is added to this document.
Because this document is not specific to the e-scooter example that is discussed, a reference is made to [3]. To be more precise the document "3000_Evidence_guarantee_of_authenticity_overview_Template.pdf" in the folder "3000_Evidence_guarantee_of_authenticity" of the directory structure. A copy of the document from [3] is placed in the folder structure for completeness on the following location:
…\Safety_assessment_ISO_26262\3000_Evidence_guarantee_of_authenticity\3000_Evidence_guarantee_of_authenticity_overview_Template_Hyperloop.pdf

More detailed information about the Evidence guarantee of authenticity can be found also in [3]. To be more precise in the chapter "3000 Evidence/guarantee of authenticity" of the document "1000_Introduction_To_The_Safety_Case.pdf" that can be found in the folder "1000_Introduction" of the directory structure.

10.4.4 4000 Certificate of compliance

The certificates that are related to the way of working standards (such as Quality Management Systems or Safety Management Systems) are added in this document. How to construct this document is not specific for the e-scooter. Therefore a reference is made to the one defined in [3]. To be more precise the document "4000_Certificates_of_compliance_Overview_Template.pdf" in the folder "4000_Certificates_of_compliance" of the directory structure. A copy of the document from [3] is placed in the folder structure for completeness on the following location:
…\Safety_assessment_ISO_26262\4000_Certificates_of_compliance\4000_Certificates_of_compliance_Overview_Template_Hyperloop.pdf. More detailed information about the Certificate of compliance can be found also in [3]. To be more precise in the chapter "4000 Certificates of compliance" of the document "1000_Introduction_To_The_Safety_Case.pdf" that can be found in the folder "1000_Introduction" of the directory structure.

10.4.5 5000 Risk acceptance criteria

This document outlines the risks acceptance criteria for the system (E-scooter) or the operator of the system. Although the SOI and its operating environment are thoroughly evaluated for safety in order to minimise the risk, it does not ensure that the system or the operators are always free of risk. In this document it is listed if a risk can be accepted, and under what conditions, This document can be found in:
…\Safety_assessment_ISO_26262\5000_Risk_acceptance_criteria\
5000_RiskAcceptanceCriteria_E_scooter.xlsx

More detailed information about the risk acceptance criteria can be found also in [3]. To be more precise in the chapter "5000 Risk acceptance criteria" of the document "1000_Introduction_To_The_Safety_Case.pdf" that can be found in the folder "1000_Introduction" of the directory structure.

10.4.6 6000 Safety concept

In this section the safety related components of the safety framework are defined. Globally components are included that focus on

- how the manufacturer intends to guarantee safety (6100 High level safety claim),
- the safety assessment of the intended functionality (6200 HARA),
- mechanisms to mitigate the identified hazards (6300 safety mechanism),
- a (re-)design to realise the system functionality and that includes the safety mechanisms (6400 Design),
- a test plan to verify and validate that the safety mechanisms are in place (6600 Test plan)
- and a conclusion that states to what extend the high level safety claim is realised (6700 Conclusion).

For all these components, that are also treated in the next sections, a detailed description can be found in [3]. To be more precise in the chapter “6000 Safety concept” of the document “1000_Introduction_To_The_Safety_Case.pdf” that can be found in the folder “1000_Introduction” of the directory structure. Please note that the numbering of the safety case parts is similar to the numbering used in this document.

10.4.6.1 6100 High level safety claim

This document defines the principal safety arguments of the system based on its function, with the limited initial understanding of the system.
An example of a high level safety claim for the e-scooter example is that ” The driver is able to safely operate the e-scooter”. This claim is supported by six arguments. These details can be found in detail in the document.

This document can be found in:
…\Safety_assessment_ISO_26262\6000_Safety_concept\6100_High_level_safety_claim\ 6100_High_level_safety_claim_E_scooter.pdf

10.4.6.2 6200 HARA

The HARA is an analysis done to arrive at the hazards resulting from system functionality failure. In the practical implementation presented, the HARA also involves the definition of safety goals to mitigate these hazards. The explanation of how the HARA needs to be filled in is defined in the “0. Approach” tab of the HARA document.

Using the example of the e-scooter, one of the highest rated hazards (Overcharging of battery cells, while standing still, unattended) is translated in a safety goal; “Overcharging of the battery should always be prevented”.
This example can be found on tab “3. Hazards and Risks” cells P11 and tab “4. Safety concepts” cells B4-C5. The method to define the safety goals is also further explained on the tab “0. Approach” row 51 – 64 of the HARA document that can be found in:
…\Safety_assessment_ISO_26262\6000_Safety_concept\6200_HARA\ 6200_HARA_E_scooter_example.xlsx

10.4.6.3 6300 Safety Mechanisms

The safety goals defined in the HARA result in safety mechanisms that actually are designed to realise the safety goals. One safety goal can have multiple safety mechanisms linked to it. The safety mechanism is a measure defined to mitigate or reduce the resulting rating of the hazard. Each safety goal can result in multiple safety mechanisms. Since for the e-scooter example the safety goals are not defined for all entries, one safety mechanism for safety goal “Overcharging of the battery should always be prevented” is treated. Part of the safety mechanism is the statement made: “A cell voltage monitoring system should be installed to cut off power supply when the maximum battery capacity is reached.”
In the tab “4. Safety concepts” of the HARA document, a functional concept is defined that shall lead to fulfilment of the safety goal. In Figure 10-3 the organisation of the safety goals and functional and technical safety mechanisms is illustrated.

Because of practical reasons and to create overview the safety mechanisms are included in the HARA document that can be found in:
…\Safety_assessment_ISO_26262\6000_Safety_concept\6200_HARA\
6200_HARA_E_scooter_example.xlsx

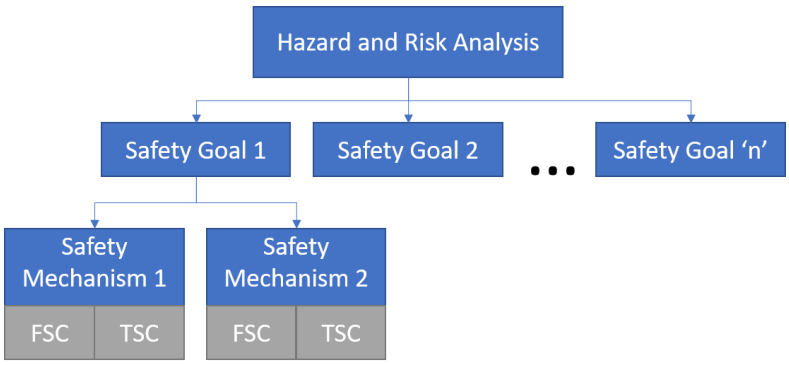

Figure 10-3: Safety Mechanism structure

10.4.6.4 6400 Design

The actual design of the system is defined in this component of the safety case. This can include any kind design description, e.g., software, component list, architecture, text description, presentation etc. The design can be redefined based on the outcomes of the safety mechanisms and the resulting functional and technical safety concepts.

Because this document is not specific for the e-scooter, and the example of the E-scooter is fictitious, a reference is made to [3]. To be more precise the document “6400_Physicial_architecture_Example.ppt” in the folder “6400_Design” of the directory structure. A copy of the document from [3] is placed in the folder structure for completeness on the following location:
…\Safety_assessment_ISO_26262\ 6000_Safety_concept\6400_Design\
6400_Physicial_architecture_Example_Hyperloop.pdf

More detailed information about the design can be found also in [3]. To be more precise in the chapter “6400 Design” of the document “1000_Introduction_To_The_Safety_Case.pdf” that can be found in the folder “1000_Introduction” of the directory structure.

10.4.6.5 6500 FMEA

The FMEA is concentrated on the physical hardware failures of the system (E-scooter) and the hazards related to these failures, these hazards are different from the HARA as they are not linked to the functionality of the SOI, but on the hardware architecture of the system (E-scooter). The FMEA has a similar structure of the HARA and results in Safety measures. These safety measures are then incorporated, and tests are then defined in the test plan to check for these safety measures.

In order to perform a FMEA, a specific product realisation needs to be considered, therefore the FMEA is not considered for this exemplary product. Therefore, a reference is made to [3]. To be more precise the document “6500_FMEA_Template.xls” in the folder “6500_FMEA” of the directory structure. A copy of the document from [3] is placed in the folder structure for completeness on the following location:
…\Safety_assessment_ISO_26262\ 6000_Safety_concept\6500_FMEA\ 6500_FMEA_Example_Hyperloop.xlsx. The Approach page of this document explains in detail how the FMEA needs to be filled.

More detailed information about the design can be found also in [3]. To be more precise in the chapter “6500 FMEA” of the document “1000_Introduction_To_The_Safety_Case.pdf” that can be found in the folder “1000_Introduction” of the directory structure.

10.4.6.6 6600 Test Plan

The test plan document defines all the tests that need to be carried out, in order to validate all the safety mechanisms that arise from the HARA, FMEA and the SOTIF study. Since the exemplary product focuses only on arrive at hazards and not mitigating them, the test plan is not defined for this example.

Therefore, a reference is made to [3]. To be more precise the document “6600_Test_plan_Example.doc” in the folder “6600_Test_Plan” of the directory structure. A copy of the document from [3] is placed in the folder structure for completeness on the following location:
…\Safety_assessment_ISO_26262\ 6000_Safety_concept\6600_Test_Plan\ 6600_Test_Plan_Example_Hyperloop.pdf.

More detailed information about the design can be found also in [3]. To be more precise in the chapter “6600_Test_Plan” of the document “1000_Introduction_To_The_Safety_Case.pdf” that can be found in the folder “1000_Introduction” of the directory structure.

10.4.6.7 6700 Conclusion

This document summarises the findings of the safety case study. The conclusions are reflections of the high level safety claims made in the beginning of the safety case study. The conclusions are supposed to validate these safety claims. The outcome of the test plan will the basis for the argumentation to validate the high level safety claims of the system (E-scooter).

Since the test plan is not defined for the specific exemplary product (E-scooter), no conclusions can be drawn. Therefore, a reference is made to [3]. To be more precise the document “6700_Conclusion_Example.docx” in the folder “6700_Conclusion” of the directory structure. A copy of the document from [3] is placed in the folder structure for completeness on the following location:
…\Safety_assessment_ISO_26262\ 6000_Safety_concept\6700_Conclusion\ 6700_Conclusion_Example_Hyperloop.pdf.

More detailed information about the design can be found also in [3]. To be more precise in the chapter “6700 Conclusion” of the document “1000_Introduction_To_The_Safety_Case.pdf” that can be found in the folder “1000_Introduction” of the directory structure.

10.4.7 7000 Change history

This document shows and tracks the changes made in the safety case. This is important to know what specific component of the safety is revised. This document can be found in:
…\Safety_assessment_ISO_26262\7000_Change_history\7000_VersionControl_application_example.xlsx

10.5 Safety assessment SOTIF

The exemplary product safety assessment using the SOTIF approach is performed in this section. This is an additional safety assessment to arrive at the system hazards that are not covered in the ISO26262 approach. The outcomes of the SOTIF are input for defining the safety mechanisms as shown in Figure 10-2.

10.5.1 SOTIF

The SOTIF for the exemplary product (E-scooter) is carried out in accordance with the method defined in the Chapter 8. This document can be found in:
…\Safety_assessment_SOTIF\ SOTIF_E_scooter.xlsx

The above mentioned document, together with Chapter 8, will act as a guide for performing a SOTIF analysis. Start point is Tab “0. Approach”.

11 Conclusion

This report outlines the framework to assess the hazards of applications that use a battery pack. The defined safety assessment framework considers the combination of the ISO26262 [11] and the SOTIF [12] normative, to arrive at a generic framework that can be applied and potentially used for most of the commonly used battery pack types and system applications involving these battery packs.

The ISO26262 and the SOTIF approach was considered due to existing knowledge of TNO with respect to these normative and extensive study done in setting up a safety case for a novel system in the Hyperloop safety case [3] study.

The defined framework can be expanded to accommodate multiple battery types to have a broader overview and, also scaled up to do an entire safety case study of a system using battery technology. It is important to mention that for a full safety case of a system, alignment is needed between manufacturer and safety evaluating party to reach the required technical detail and avoid subjective risk-assessment as much as possible.

The report includes an exemplary product, to show how the defined framework can be applied to a fictitious application using battery technology. It is also shown that the combination of the defined exemplary product and the Hyperloop study results in a full safety case of a system.

12 Bibliography

[1] J.-M. A. C. S. Lidia Palm, “BH9369MIRP2107151523 Verkenning regelgeving veiligheid,” 2021.

[2] R. W. Chris van der Ploeg, “P11783 Outline of a Safety Case,” TNO, Helmond, 2021.

[3] M. L. A. K. R. W. Chris van der Ploeg, “R11991 Template and Example of a Safety Case,” TNO, Helmond, 2021.

[4] “R11990 Hyperloop safety framework for testing and certification: General safety approach,” TNO, Helmond, 2021.

[5] R. W. -. M. H. -. F. Mobini, “R10014 Develop a safety framework for evaluation and assessment of Hyperloop,” TNO, Helmond, 2021.

[6] “Battery Types & Safety. Batteries power the modern world. Learn how to recognize the different types you may encounter, as well as safety tips, and their recycling process.,” [Online]. Available: https://www.cirbasolutions.com/learning-center/battery-types/. [Accessed 2022].

[7] l. ada, “All About Batteries,” 2021. [Online]. Available: https://learn.adafruit.com/all-about-batteries/overview. [Accessed 2022].

[8] T. P. K. C. Wei Liu, “Overview of batteries and battery management for electric vehicles,” 2021.

[9] M. H. F. M. E. v. D. Ron Wouters, “TNO 2021 R10014 I Final report,” TNO, Helmond, 2021.

[10] H. P. Jones, T. J. Chapin and M. Tabaddor, “Critical Review of Commercial Secondary Lithium-Ion Battery Safety Standards,” 2010.

[11] “ISO 26262-1:2018 Road vehicles — Functional safety,” 2018.

[12] “SO/PAS 21448:2019 Road vehicles — Safety of the intended functionality,” 2019.

Automotive Campus 30
5708 JZ Helmond
P.O. Box 756
5700 AT Helmond
The Netherlands

www.tno.nl

T +31 88 866 57 29
F +31 88 866 88 62

TNO report

2100 System Definition Battery Pack

Draft

Date	06 October 2022
Author(s)	
Copy no	1
No. of copies	1
Number of pages	10 (incl. appendices)
Number of appendices	
Sponsor	
Project name	Hoog risicoprofiel batterijen
Project number	060

All rights reserved.
No part of this publication may be reproduced and/or published by print, photoprint, microfilm or any other means without the previous written consent of TNO.

In case this report was drafted on instructions, the rights and obligations of contracting parties are subject to either the General Terms and Conditions for commissions to TNO, or the relevant agreement concluded between the contracting parties. Submitting the report for inspection to parties who have a direct interest is permitted.

© 2022 TNO

Contents

Draft

1 Introduction

In this document, the system definition of the a battery powered electric scooter is elaborated. The main goal is to explain the product and the involved batter pack to be assessed.

Draft

2 System of Interest

This chapter provides an overview of the System Of Interest (SOI). The system of interest is the battery pack of an electric scooter. For the purposes of this report, a regular arbitrary scooter is considered. The scooter is considered have a general battery pack (no specific battery type is considered). The System Of Interest is indicated in Figure 2-1.

Figure 2-1: System of interest as part of the electric scooter

The purpose of the example is to show how the safety framework can be used and not to provide a full safety assessment of the product. To illustrate how to fill in the safety framework, fictive hazards may be introduced. Moreover, the analysis will not strive for completeness, but aims to provide a concise practical example.

3 Functionality description

This section provides the description of the high level functionalities of the electric scooter. To do so, first the high-level functional architecture of the scooter is given. Within this architecture the boundaries of the SOI are stated as well. Next the function descriptions are stated. As an example, only the relevant functions for the battery are described.

3.1 High level functional architecture

The main functions of the electric scooter and the SOI are given in the high-level functional architecture found in Figure 2. In this functional decomposition four function categories can be observed;

- F1: Sensing
- F2: Power sourcing
- F3: Actuation
- F4: HMI
- F5: Vehicle logics

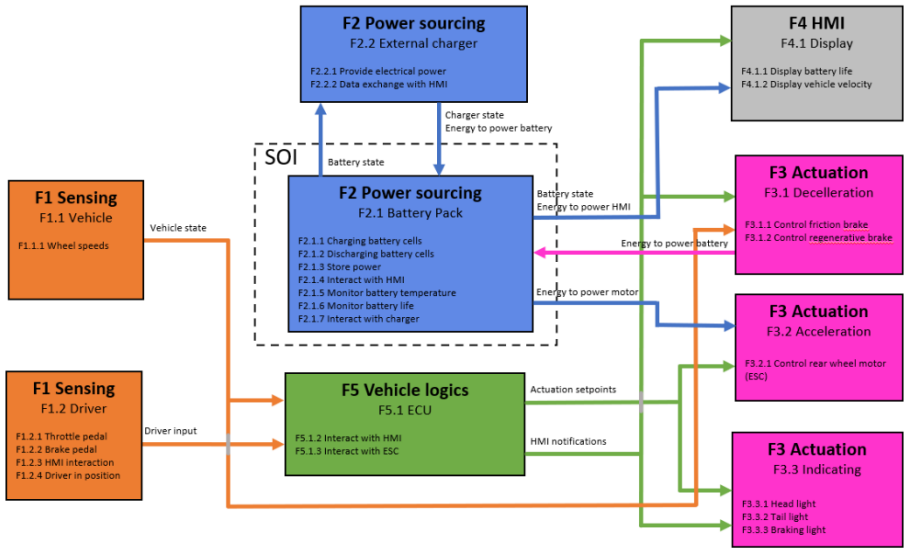

Figure 2: High level functional architecture of the electric scooter including the SOI (dashed)

The function category Sensing (F1) contains Vehicle sensing (F1.1) and Driver sensing (F1.2). Based on the inputs from these blocks the vehicle logics (F5) can actuate the Actuators (F3) and HMI (F4). Note that the brake pedal (F1.2.2) is directly connected to the friction brake actuator (F3). Therefore, it can operate independently from the Vehicle logics (F5). The power sourcing (F2) consists of an external charger (F2.2). While the electric power is stored in the battery pack (F2.1)

In the following section the SOI subfunction F2.1 is elaborated.

3.2 F2.1 Battery Pack

The battery pack consist of functions and operational modes.

3.2.1 Battery pack operational modes

The most important modes of operation of the battery which are used in the HARA are stated next. The stored power mode (F2.1.3) makes sure the battery is able to provide electrical power when requested by the driver. In this case the battery cells are discharged (F2.1.2). The battery pack can be charged (F2.1.1) both via the external charger and via regenerative braking. A short description of these operational modes is provided in the next sections.

- F2.1.1 Charge battery cells
- F2.1.2 Discharge battery cells
- F2.1.3 Store power

F2.1.1 Charging battery cells

This can be done by the charger or the regenerative braking function of the rear wheel motor. The charger takes energy from the 230VAC outlet and converts it into a DC current. The application can also add power to the pack by using regenerative braking to charge the battery cells.

F2.1.2 Discharging battery cells

This can be done by the application by drawing power from the battery cells.

F2.1.3 Store power

The main function of a battery pack is storing power in the battery cells.

3.2.2 Battery pack functions

The battery pack function consists of several subfunctions. Note that not all functions of the battery pack are stated and described in full detail. The goal of the project is to provide a safety assessment framework and not to perform a detailed analysis of a battery pack. The main subfunctions of the battery pack (F2.1) function are summarized below:

- F2.1.4 Interact with HMI
- F2.1.5 Monitor battery temperature
- F2.1.6 Monitor battery life
- F2.1.7 Interact with charger

F2.1.4 Interact with HMI

Provides electrical power to the HMI and creates data exchange to show battery state.

Draft

F2.1.5 Monitor battery temperature

Measures the temperature of the battery pack

F2.1.6 Monitor battery life

The battery pack measures the SOC of each individual battery cell and calculates the SOC

F2.1.7 Interact with charger

Provides electrical power to the battery cells and exchanges data to perform a handshake between battery and charger

Draft

4 Battery pack type

The selected battery pack used to present the safety framework is fictitious and selected manually. The battery is selected in order to allow the writers of the safety framework to provide a practical example of the framework provided. Four well known battery cathode compositions are examined to be used as example battery and stated below:

- Li-Ion (This is the current standard for high energy density battery applications.)
- Ni-Cd (Mostly used up to the 1990's, nowadays mostly superseded by Li-Ion)
- Ni-Mh (Higher energy density than the Ni-Cd. But mostly superseded by Li-Ion)
- Lead acid (Used for car starter batteries)

For each type of cathode composition the typical battery characteristics, application and associated risks are stated in Table 1.

Table 1, Battery types

Type of battery	Cathode composition	Risks	Cycles	Life time	Single cell voltage	Hazardous in case of disposal	Application
Nickel	Nickel Cadmium (Ni-Cd)	Eye effects: Contact with electrolyte extremely corrosive to eye tissues. May result in permanent blindness. Skin effects: Contact with electrolyte solution inside battery may cause serious burns to skin tissues. Ingestion: Ingestion of electrolyte solution causes tissue damage to throat area.	2000 Cycles	15-20 Years	1.3V	Need to disposed off through chemical waste	the only composition that was available up to the mid 90's.
Nickel	Nickel Metal Hydride (Ni-Mh)	Overcharging causes hydrogen gas to form, potentially rupturing the cell. Therefore, cells have a vent to release the gas in the event of serious overcharging. NiMH	2000 Cycles	3-5 Years	1.2V	Need to disposed off through chemical waste	before the Li-Ion became the standard. Ni-Mh was used in high end consumer goods

Draft

		batteries are made of environmentally friendly materials.					among other things.
Lithium	Lithium Ion (Li-Ion)	These flammable gases could be easily ignited by the battery's high temperature, resulting in a fire. In addition, the combustion of these gases when venting from the battery poses another safety concern: the accumulation and potential explosion of the gases themselves.	3000-5000 Cycles	5- 10 Years	3.6V - 3.7V	Need to disposed off through chemical waste	Consumer electronics F.E. Mobile phone, laptop and headphones
Lead	Lead Acid (Pb)	Lead acid batteries can cause serious injury if not handled correctly. They are capable of delivering an electric charge at a very high rate. Gases released when batteries are charging – hydrogen (very flammable and easily ignited) and oxygen (supports combustion) – can result in an explosion.	500 - 1200 Cycles	10 - 15 years	2V	Full recycling process is the standard	Mostly used in cars, trucks and forklifts

For the detailed analysis of a battery pack a fictitious battery pack is chosen, however it does resemble a real-world application.

The battery pack that will be used in the example will be a fictitious 10S 2P pack with a “smart” charger. This means that it is a 36V-42V battery pack with 2 cells in parallel. Construction of the pack is a shrink sleeve and the power terminal is an XT60 towards the application and a proprietary connector towards the charger. This

Draft

is a pack that is built into the application, not meant for easy swapping of the battery.

Draft

Automotive Campus 30
5708 JZ Helmond
P.O. Box 756
5700 AT Helmond
The Netherlands

www.tno.nl

T +31 88 866 57 29
F +31 88 866 88 62

TNO report

2200_Environment_Definition

Draft

Date	06 October 2022
Author(s)	
Copy no	1
No. of copies	1
Number of pages	5 (incl. appendices)
Number of appendices	
Sponsor	
Project name	Hoog risicoprofiel batterijen
Project number	060

All rights reserved.
No part of this publication may be reproduced and/or published by print, photoprint, microfilm or any other means without the previous written consent of TNO.

In case this report was drafted on instructions, the rights and obligations of contracting parties are subject to either the General Terms and Conditions for commissions to TNO, or the relevant agreement concluded between the contracting parties. Submitting the report for inspection to parties who have a direct interest is permitted.

© 2022 TNO

Contents

Draft

1 Introduction

In this document, the environment definition of a battery powered electric scooter is provided. These factors are divided into the following categories,

1. Road related conditions
2. Weather conditions

In the following chapters an overview in the form of a table is made for each of these environmental conditions. In the table the condition type, a description of the condition and whether the electric scooter shall be able to deal with the condition, is indicated.

Draft

2 Road related conditions

Table 1: Road related conditions

Condition	Description	Functional
Road type	Smooth asphalt road	Yes
Road type	Smooth ceramic tiles	Yes
Road type	Sidewalk (concrete tiles)	Yes
Road type	Off road	No
Constructions	Curb stones	Yes
Constructions	Stairs	Yes
Quality	Uneven road	Yes
Slope	The system needs to cope with road slope (up/down hill) situations.	Slope<20%

Draft

3 Weather conditions

Table 2: Weather conditions

Wind conditions	Description	Functional
0 - 6 Beaufort	weak – moderate	Yes
7 - 9 Beaufort	hard wind – storm	Yes
10 - 12 Beaufort	heavy storm - hurricane	Yes

Temperature conditions	Description	Functional
-25 to +5 deg Celsius	low	Yes
+5 to +40 deg Celsius	normal/high	Yes

Precipitation conditions	Description	Functional
None		Yes
Drizzle / mild rain		Yes
Heavy rain		Yes
Sleet / snow		No
Hail		No

Table 3: Visibility conditions

Condition	Description	Functional
All visibility conditions		Yes

Draft

Approach

The SOI and its environment are thoroughly analysed inside the safety concept to ensure a certain quantity of minimised risk. However, it does not mean that the system and the test operator(s) are free of risk. The scope of the risk acceptance revolves around **System Related Risks (SRR)**. **System related risks** are defined as risks that the system can be subject to when not operated in the environment it is designed for, due to misjudgement or sudden change of the environment. Moreover it concerns risks that arise from basic scope and design assumption. It is of vital interest for the applicant to align this risk category with the CA before compilation of the safety case. The risk acceptance criteria are set up in tab 3. The used definitions and way of working will be elaborated below.

SRR ID

Each sepearate risk is assigned a unique identifier by the applicant to guarantee traceability of the risk throughout the approval process for the safety case. In this document the SRR ID's are denoted as SRR.XXX in which XXX refers to a unique numbering.

Source of SRR

The safety case part associated to the SRR can be selected inside this column.

Definition SRR

Specific description of the source of the risk. For example, for an SRR this could be a specific environment condition from 2200, component that is being reused, norm that is not considered due to specifc reasons.

Reason of existence SRR

In this column it is up to the applicant to answer the question: why is the imposed SRR actually a risk? For what reason is this risk occuring and why will not or haven't any mitigating measures already been taken to mitigate it through the safety case?

Potential negative effect(s) of SRR

In order to be able to assess whether the risk is acceptable or not, the potential negative effects of the imposed SRR need to be carefully denoted. It is not necessary and, in fact, not recommended to go into too much detail. The negative effects need to reflect the consequences, their severity and their probability of occurence.

Status of SRR

To track the progress of the applicant and the CA in this interactive discussion on the SRR, it is advised to set up a clear process. The proposed workflow is suggested in Figure 1, where first of all the applicant generates the inventory of SRR and compiles them into this document. Subsequently, the risk is "In discussion", meaning that the overview is reviewed by the CA. During this review, two events can occur: first, the risk could be put under discussion, during which the CA consults with the applicant and other relevant stakeholders whether this risk is acceptable or not, second, the risk can be accepted by the CA. If, after a discussion, it turns out that the risk is accepted, the risk transitions to "Accepted". If the risk is not accepted by the CA, the applicant and CA can go into a form of conflict resolution where, either the applicant gives a counterproposal on possible measures to revise the risk (hence, returning to compilation of 5000), or the CA decides that the risk is "Not accepted", and it is up to the applicant to come up with countermeasures within the safety case to prevent this risk.

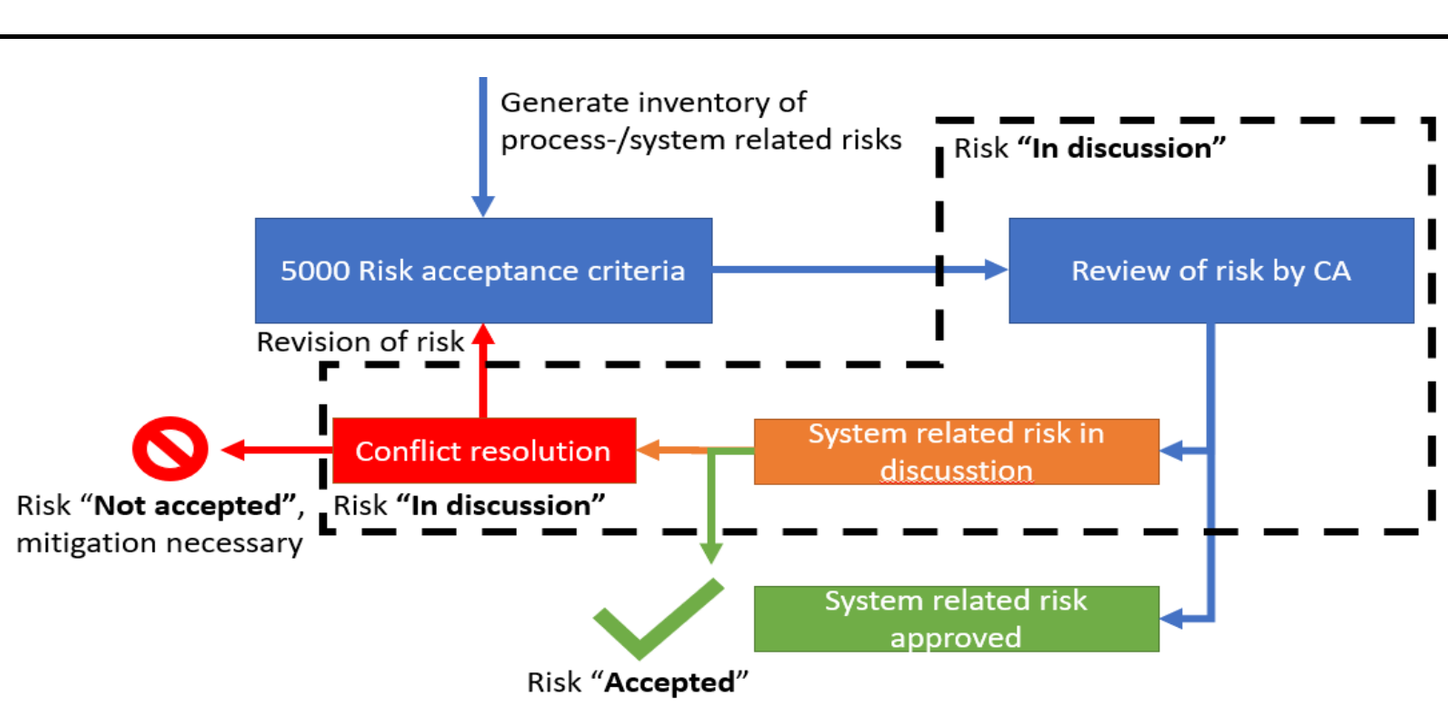

Figure 1: Risk acceptance criteria workflow

Risk Acceptance Criteria

Safety case owner:
Safety case assessor:
Lead author:
Lead reviewer:
Part subject (1000-7000):
Sub-part subject (1000-7000):
Version number:
Date of initiation (DD-MM-YYYY):
Current date (DD-MM-YYYY):

Change Tracking

User	Editted Sheet	Change Description	Date

Safety case - Risk Acceptance Criteria - System Related Risks

System Related Risk ID (SRR ID)	Source of SRR (part/sub-part)	SRR definition	Reason of existence SRR	Potential negative effect of SRR	Status of SRR
SRR.001	2100_System_definition	The standard commercially available scooter that is used, will be excluded from the safety analysis	The standard commercially available scooter is structurally proven to be able to be driven under the same circumstances as posed in 2200. As a result, we believe that it is not necessary to prove the structural integrity and safety of this base vehicle.	We only consider hazards and failure modes from the battery added on top of the base vehicle. If there exist any failure modes of the base vehicle, which do not occur due to the additional battery, these are not included in the safety analysis.	Accepted
SRR.002	2200_Environment_definition	The weather conditions during testing are subjectively judged by the test engineer.	It hinders the efficiency of testing and the focus of the test engineer if all denoted environment conditions are required to be measured using calibrated equipment at all times. Hence, we assume that the test engineer is able to subjectively determine the compliant environment conditions.	Sudden changes in weather or large discrepencies in the judgement of the test engineer can result in operating the vehicle out of the environment definition it is deemed safe in.	Not accepted

Status
Not accepted
In discussion
Accepted

Safety case parts and sub-parts:
1000_Introduction
2000_Item_definition
2100_System_definition
2200_Environment_definition
3000_Evidence_guarantee_of_authenticity
4000_Certificates_of_compliance
5000_Risk_acceptance_criteria
6000_Safety_concept
6100_High_level_safety_claim
6200_HARA
6300_Safety_mechanisms
6400_Design
6500_FMEA
6600_Test_plan
6700_Residual_risk
7000_Change_history

Automotive Campus 30
5708 JZ Helmond
P.O. Box 756
5700 AT Helmond
The Netherlands

www.tno.nl

T +31 88 866 57 29
F +31 88 866 88 62

TNO report

6100_High_Level_Safety_Claim of Application

Draft

Date

Author(s)

Copy no	1
No. of copies	1
Number of pages	8 (incl. appendices)
Number of appendices	
Sponsor	
Project name	Hoog risicoprofiel batterijen
Project number	060

All rights reserved.
No part of this publication may be reproduced and/or published by print, photoprint, microfilm or any other means without the previous written consent of TNO.

In case this report was drafted on instructions, the rights and obligations of contracting parties are subject to either the General Terms and Conditions for commissions to TNO, or the relevant agreement concluded between the contracting parties. Submitting the report for inspection to parties who have a direct interest is permitted.

© 2022 TNO

Contents

Draft

1 Introduction

In this document the high-level safety claim is described. Because the safety claim can be described in many ways, the method used is explained in [REF_002]. The actual safety claim is detailed in Chapter 3 High level safety claim.

Draft

2 Safety claim approach

In the high level safety claim the safety claim on system level is given. This claim is a trade-off between completeness and specificness. In effect it should be broad enough to cover the complete system while on the other hand the stated claim needs to contain enough details to accurately state the area of interest. The safety claim composes of the actual claim followed by six types of safety claim arguments. The six safety claim arguments are found using the 5W1H system [1]. The ingredients to the high level safety claim are visualised in Figure 1. The 5W1H system contains of questions starting with the question words: what, why, where, who, when and how.

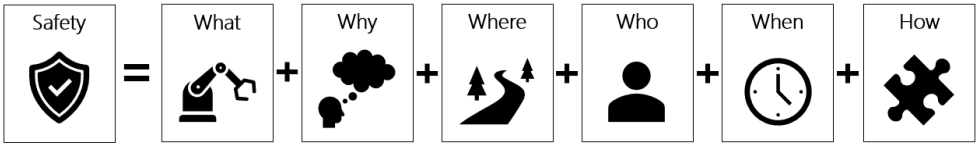

Figure 1, High level safety claim ingredients

The answers to these questions result in the safety claim arguments. For completeness, the safety claim argument should not contain functional requirements. High level evidence to the safety claim argument can be included in the summary below each safety claim argument. The safety claim evidence can be in the form of an object or in the form of an assumption denoted by respectively [O] and [A].
The object form is a direct safety case artefact. The assumption form is difficult to objectively prove but it should be found reasonable. Note that the evidence based on assumptions is not allowed to be vague or unnecessarily broad. An assumption object is therefore closely related to the object form evidence apart. With the difference that it is not possible to proof that the intended use is always respected by all users. This type of safety claim evidence is mostly related to operational instructions. E.g.: it is assumed that the driver and bystanders follow the safety measures stated in the claims. As an example, such safety claim evidence is related to, but not limited to, driver alertness, weather conditions and surrounding traffic. The driver and bystanders are instructed to use the item only at the specified conditions, but they might choose to not follow the instructions.

In the following section the definitions for the different claim components are given. Subsequently in section 2.2 the structure is explained.

2.1 Definitions

Safety claim: One-liner explaining the behaviour of the System Of Interest, SOI, on system level. This claim needs to state the safety on a high system level such that the underlying safety claim arguments can detail the claim and evidence and artefacts can be gathered in a structured manner to support it.

Arguments: In the considered safety case the claim argument can either be functional in nature, or a process (SMS, QMS, etc) referring to the safety of the SOI. The arguments are stated with the purpose that, if eventually supported by appropriate evidence they can results in a safe SOI. They do not prove the safety of the SOI, because these arguments are made in the beginning of the safety case formulation and therefore need supporting evidence. They require that evidences and objects supporting these claim arguments are added in the safety case.

Evidence: the arguments are supported by stating available evidences. Evidences are either of non-technical nature that refer to existing literature and normative, or other sources.

Objects: these are artefacts, that are referred to from the formulated safety case. Objects are evidences supporting the safety claim arguments, that arise from one or more parts of the safety case.

2.2 Structure

The SOI can have multiple high level safety claim arguments. These arguments are justified by providing supporting evidences and objects, which are obtained from the formulated safety case. Figure 2 shows the overview of the high level safety claim and the objects supporting it. The figure illustrates that the high level safety claim is part of the "system definition" and exists of several arguments (1, 2…n). Moreover, several objects are formed in the safety case that serve as artefacts for the arguments.

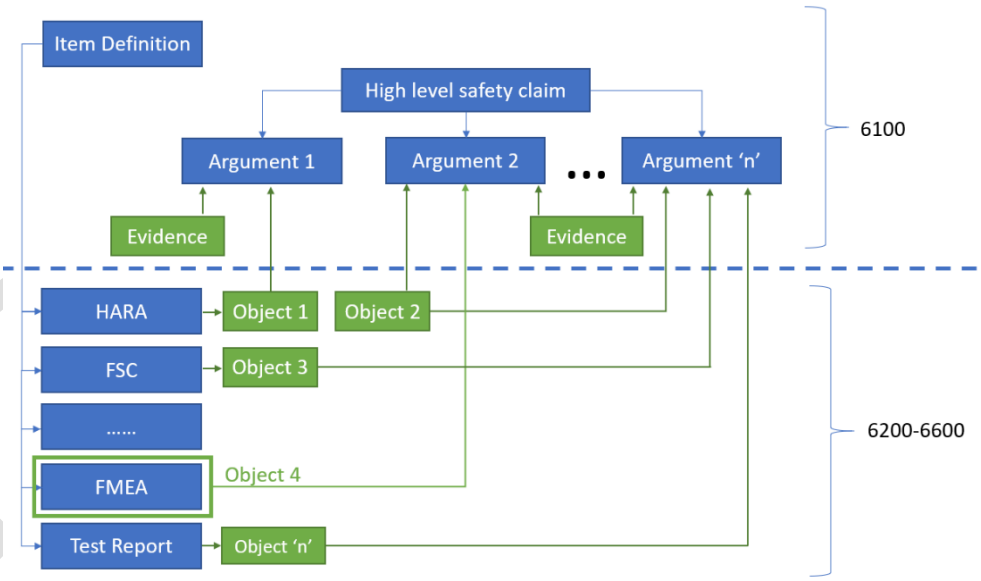

Figure 2: Overview of high level safety claim formulation and justification

3 High level safety claim

In this section the high-level safety claim is stated. The high-level safety claim is supported by six safety claim arguments based on the 5W1H system. The Safety SubClaims (SSC) are subclaims related to the safety claim arguments. The evidence to the safety subclaims is either of the type assumption or of the type object. In Figure 3 a visual aid to the safety claim breakdown is given.

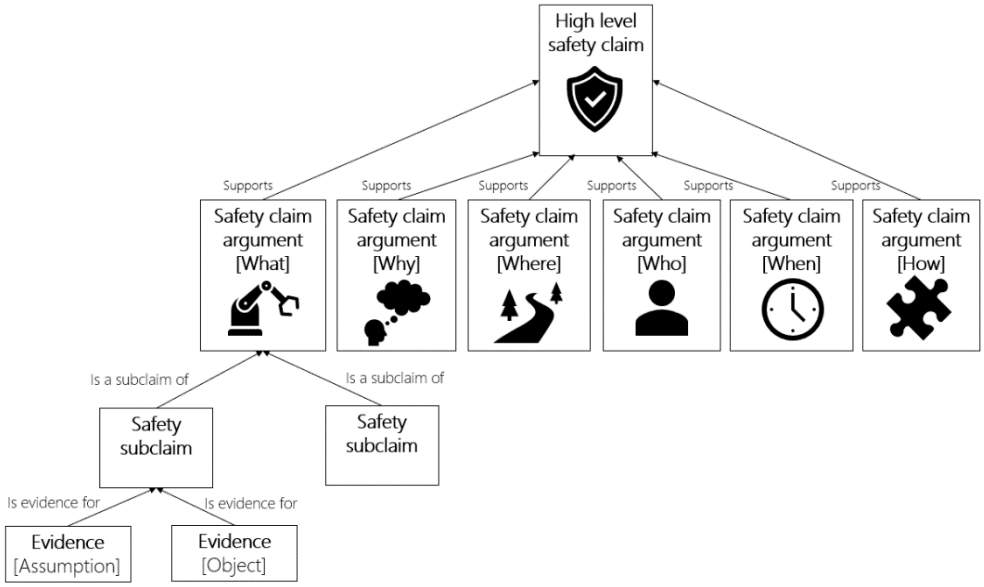

Figure 3, Safety claim breakdown. The safety subclaim and evidence is added for the 'what safety claim argument'. The other safety claim arguments consist of a similar breakdown structure but is not visualised here because of readability.

Safety claim: The driver is able to safely operate the vehicle.

Safety claim argument 1 (WHAT): The novel battery is added on top of an existing production base vehicle.

- [SSC1.1] The base production vehicle is approved for open road access
  - [O] The production vehicle is homologated according to the conditions of the road authority
- [SSC1.2] The base production vehicle is capable of being safely extended with the novel battery [2].
  - [O] Mechanical drawings are included to proof that the base vehicle is structurally capable of being extended with the battery.
  - [O] Design documents are added to proof that the Human Machine Interface (HMI) allows for adaptation with battery state information.
  - [O] The electrical safety is designed according to ISO 14990-1:2016 and can be found in the attached design document.

Safety claim argument 2 (WHY): The driver is able to fall back on the original vehicle.

- [SSC2.1] The operation of the brake system is unchanged.

    - [O] Operation instructions are available
    - [O] Test results are done according to the test plan to validate the operation of the vehicle

Safety claim argument 3 (WHERE): The driver only operates the vehicle during testing in safe areas

- [SSC3.1] During testing the vehicle is not used on the public road
    - [A] During testing the driver shall only operate the vehicle on proving grounds.
- [SSC3.2] During testing the vehicle is used in an environment with sufficient safety distance to road furniture
    - [A] During testing the vehicle is only used at the vehicle dynamics area of the proving ground.
- [SSC3.3] During testing the surrounding traffic is aware of the capabilities of the vehicle
    - [A] All surrounding traffic has received a safety briefing regarding the System Of Interest (SOI) when entering the proving ground.

Safety claim argument 4 (WHO): The driver is instructed on how to use the vehicle

- [SSC4.1] The driver is instructed
    - [A] The driver can provide a certificate of driving for this vehicle type.
    - [O] The driver logbook regarding the operational experience of this vehicle type is included in the safety case documentation.
- [SSC4.2] The driver is alert
    - [A] The driver shall take a 10 minutes rest after every 30 minutes of operation of the SOI.

Safety claim argument 5 (WHEN): The operational life of the vehicle is limited, the driver only operates the vehicle during approved weather and light conditions.

- [SSC5.1] The operational life exceeds the allowed operation time of the SOI
    - [O] The vehicle is able to operate for at least 20 hours.
    - [O] The vehicle is able to operate for at least 1000 km.
    - [A] The vehicle is used for maximum 20 hours or 1000 km, whatever comes first.
- [SSC5.2] The vehicle is only used during the weather conditions stated in 2200 Environment Definition [3].
    - [A] The vehicle is only used during daylight
    - [A] The vehicle is used only when visibility is above 10 km.

Safety claim argument 6 (HOW): The novel battery is added in a safe manner in terms of rigidity, robustness and fault tolerance.

- [SSC6.1] The battery is installed by certified engineers.
    - [O] As can be found in the Quality Management System (QMS) the engineers work according to NEN 9140 (NEderlandse Norm, the Royal Dutch Institute for normalisation).
- [SSC6.2] The materials used are automotive grade
    - [O] Datasheets are provided to prove that all components are compliant. E.g. The braking components are compliant to ISO611:2003

Draft

4 Bibliography

[1] Lean-6-sigma. (2020, 11 14). *5W1H method according Kipling*. Retrieved from Lean-6-sigma: https://www.lean-6-sigma.nl/5w1h-volgens-kipling/
[2] 2100_System_Definition_Application_Example.docx
[3] 2200_Enivornment_Definition_Application_Example.docx

Draft

Approach

The goal of the hazard analysis & risk assessment is to, in an early stage of the design phase, identify hazards that can occur when using the SOI and to define mitigating measures. As a result of this the mitigating measures can serve as engineering safety requirements to ensure that the mitigating measures are realised. In Figure 1 the general process is shown which is based on the ISO26262-part3 Annex B. In the first step the main system functions are identified (as done in 2000_Item_definition). In the second step situations that lead to hazards are identified. In the third step the hazards are classified in order to address the importance of mitigating the hazard. In the last step, step 4, a safety goal to mitigate the hazard is defined. In ISO26262 the hazard classification is done based on statistical information or defined quantities. Because for a novel (and probably still under development) technology no or very limited statistical classification information is available, the rating is done subjectively.

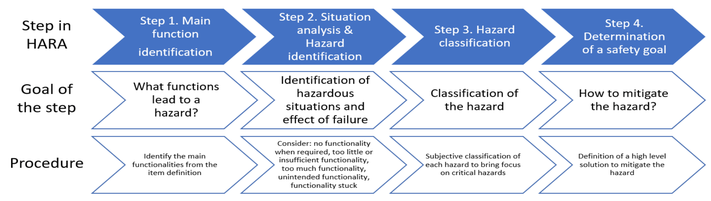

Figure 1: HARA process of hazard identification and classification

Hazards and Risks tab

In the "3.Hazards and Risks" tab of the HARA the process presented in Figure 1 is elaborated. The purple, dark blue, light blue and cyan coloured header columns contain the information related to the main process steps indicated in the top row of Figure 1. Below the information presented in each of the columns is explained.

Step 1. Main function identification

Function: High level function defined for the SOI. Failing of this function will be the source of the hazards.

Step 2. Situation analysis & hazard identification

Hazards: This defines the hazard based on a specific failure of the function, there can be multiple hazards resulting from different kinds of failures of the same functionality.

Scenario: Defines the different situations in which the hazard can be expected.

Weather: Defines the weather conditions, if it is one of the factors that affects the functionality being analysed.

Operating conditions: Includes all the external factors affecting the functionality, for instance radiations, surface on which the system operates, etc.

Effect of failure: The outcome due to the failure of the described hazard.

Step 3. Hazard classification

Severity, probability of exposition and controllability: Rating of the hazards is done based on the parameters Severity, Probability of Exposure and Controllability. Below these are defined in more detail under the "Risk Graph" tab.

Justification – S,E,C: The justification for the assigned Severity, Probability of Exposure and Controllability. It is elaborated in order to make the analysis more readable.

Rating: Based on the levels of Severity, Probability of Exposure and Controllability, a rating is determined as defined in more detail under the "Risk Graph" explanation.

Step 4. Determination of safety goal

Applied safety goal: Each hazard or scenario that results in a rating other than 'QM', should have a safety goal assigned to it. The safety goals are then defined in "4. Safety Concepts". Note that the same safety goal can be applied for multiple Hazards.

Scenarios

Standstill: Ideally the scooter and battery are stored in a dry and heated covered parking place. However it is expected that multiple customers will store the scooter and battery in outside conditions for a major part of the battery life. These conditions include low/high temperatures, low/high humidity levels and low/high wind speeds. The scooter battery will be charged in between scooter use. It is assumed that charging will be performed indoors at typical room humidity and temperature levels. Most likely the operator will remain the charger in place even if the battery is completely charged. Therefore the scooter might be prolonged charged for a major part of its life cycle. While the battery is being charged, input AC might vary and sudden power cuts are expected. The battery and scooter might experience mechanical impacts due to tipping over or falling. Note that storage and external charging is most likely performed unattended.

Driving: Acceleration: This scenario describes the typical usage of the scooter. It is assumed that on average the scooter is used less than 2 hours a day. The scooter will be ridden on any road surface. In particular the scooter is used in urban conditions which will result in high frequent vibrations and mechanical impacts due to bumping off the curbs. In general it is assumed that the scooter is operated in a temperature range of -25 to +40 degrees Celsius. Also the scooter is assumed to be ridden up to hurricane winds while heavy rain and/or snow is present. It is assumed that the acceleration time is typically 10 % of the total driving time.

Driving: Steady state velocity at 25 kph: This scenario describes the typical usage of the scooter. It is assumed that on average the scooter is used less than 2 hours a day. The scooter will be ridden on any road surface. In particular the scooter is used in urban conditions which will result in high frequent vibrations and mechanical impacts due to bumping off the curbs. In general it is assumed that the scooter is operated in a temperature range of -25 to +40 degrees Celsius. Also the scooter is assumed to be ridden up to hurricane winds while heavy rain and/or snow is present. It is assumed that the steady state velocity time is typically 80 % of the total driving time.

Driving: Braking: This scenario describes the typical usage of the scooter. It is assumed that on average the scooter is used less than 2 hours a day. The scooter will be ridden on any road surface. In particular the scooter is used in urban conditions which will result in high frequent vibrations and mechanical impacts due to bumping off the curbs. In general it is assumed that the scooter is operated in a temperature range of -25 to +40 degrees Celsius. Also the scooter is assumed to be ridden up to hurricane winds while heavy rain and/or snow is present. It is assumed that the deceleration time is typically 10 % of the total driving time.

Safety concepts tab

The "4. Safety concepts" page of the HARA links the Hazards to one or more safety mechanisms to mitigate it.

Figure 2: Safety goal definition, realisation and testing process.

In Figure 2, the general approach of defining a safety goal is visualised.

Step 1. Safety Goal ID number: This corresponds to the specified, applied safety goal in the "3. Hazards and Risk" page. The ID is used such that the Safety Goals can be referred to in other documents of the safety case.

Step 2. Safety goal: Defines the proposed goal, to avert the Hazard. The safety goal is specified on a functional or specific component level, which is responsible for mitigating the Hazard.

Step 3. Sub-classification of safety goals: The safety goal is further sub divided into multiple safety mechanisms. Each safety mechanism is a way of mitigating the hazard. A sub-classification of the safety goal number into mechanisms is specified in this column.

Step 4. Functional safety concept: Short description of the proposed functional safety concept to mitigate the hazard.

Step 5. Technical safety concept: Short description of the proposed technical safety concept to mitigate the hazard.

Step 6. Test definition: A test to check the mitigating measure and if the corresponding safety goal is met shall be defined in the test plan (6600_Test_plan).

Risk Graph tab

In order to set the correct safety priority during the design process the hazards can be rated. The rating indicates how critical it is to mitigate the hazard and is based on; 1) how severe it is when the hazard occurs 2) how likely it is that the hazard occurs and 3) how easy/difficult is it to control the hazardous situation. In norms such as the ISO26262 the ratings (ASIL, SIL) are linked to statistical /objective quantities. Because for a novel system, maybe still under development, such objective numbers are not available a subjective rating is applied. The presented rating will also be used for the HARA and FMEA (Failure Modes and Effects Analysis).

The Risk Graph (based on ISO26262 part 3 Annex B), maps the Severity (S), probability of Exposure (E) and Controllability (C) to a rating. This is done according to the equation,

$$Score = \big((S+1)+C+E\big) * min(S;1)$$

The relation between the score and the rating is shown below.

Score	Rating
0	QM
1	QM
2	QM
3	QM
4	QM
5	QM
6	QM
7	QM
8	A
9	B
10	C
11	D

QM: Lowest classification, no safety measures required.
A: Lowest hazard classification level that requires minimal safety measures.
B:
C:
D: Highest hazard classification, additional safety measures required.

When considering the Severity, Probability and Exposure in relation to the rating the following table can be configured.

Controllability C	Exposure (E)	Severity (S)			
		S0	S1	S2	S3
C1	E1	QM	QM	QM	QM
	E2	QM	QM	QM	QM
	E3	QM	QM	QM	A
	E4	QM	QM	A	B
C2	E1	QM	QM	QM	QM
	E2	QM	QM	QM	A
	E3	QM	QM	A	B
	E4	QM	A	B	C
C3	E1	QM	QM	QM	A
	E2	QM	QM	A	B
	E3	QM	A	B	C
	E4	QM	B	C	D

Severity classification

The severity classification is defined in the following table.

Class	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Exposure

The probability of exposition is classified in the following table.

Class	E1	E2	E3	E4
Description	Very low probability	Low probability	Medium probability	High probability
	The hazard occurs in extremely rare situations (incidents).	The hazard occurs in a very specific situation that occurs event based.	The hazard occurs in a situation that occurs less frequently (e.g. start-up, shut-down, special use cases).	The hazard occurs in a situation that frequently occurs because it is normal use .
Subjective rating indication	<< 1% of operating time	< 1% of operating time	1%-10% of operating time	>10% of operating time

Controllability

The controllability is classified in the following table.

Class	C1	C2	C3
Description	Simply controllable. The driver/operator is be able to reduce the severity level to 1 or lower.	Controllable The driver/operator is be able to reduce the severity level to 2.	Difficult to control or uncontrollable. The driver/operator is not be able to reduce severity to a level lower than 3.

HARA

Safety case owner:
Safety case assessor:
Lead author:
Lead reviewer:
Part subject (1000-7000):
Sub-part subject (1000-7000):
Version number:
Date of initiation (DD-MM-YYYY):
Current date (DD-MM-YYYY):

Change Tracking

User	Edited Sheet	Change Description	Date

		Situation analysis & Hazard identification						Hazard Classification								Determination of Safety Goal	
Nr	Function	Hazardous Situation No.	Hazard	Operational situation			Effect of failure	Severity	justification - S	Probability of Exposition	justification - E	Controllability	justification - C	Resulting Rating		Applied Safety Goal ID-No	Comment
				SCENARIO	WEATHER	Operating conditions		0-3		0-4		0-3		QM ... D			
F2.1 Battery Pack																	
1	F2.1.1 (Charging battery cells)	1	Too little charging of battery cells	Standstill	Any weather condition, as specified in Chpt. 5 of Doc.2200 Environment Definition	Any road condition, as specified in Chpt. 3 of Doc.2200 Environment Definition	No failure	0	No injuries	4	>10% of operating time	3	No driver present to control the situation	QM			
2				Driving: Acceleration			n/a							QM			
3				Driving: Steady state velocity at 25 kph			n/a							QM			
4				Driving: Braking			no failure of the battery, but can lead to poor braking performace causing loss in control, due to failure in renerative braking	3	Life-threatening injuries (survival uncertain), fatal injuries	3	1%-10% of operating time	3	The driver is surprised which makes it more difficult to control the vehicle.	C			
5		2	Overcharging of battery cells	Standstill	Any weather condition, as specified in Chpt. 5 of Doc.2200 Environment Definition	On a beach with direct acces to water	Fire or smoke	3	Life-threatening injuries (survival uncertain), fatal injuries	4	>10% of operating time	0	The user is present to reduce severity level because no flamable objects are present and the battery can be cooled immediately	A			
6						underneath a tree	Fire or smoke	3	Life-threatening injuries (survival uncertain), fatal injuries	4	>10% of operating time	1	The user is present to move the battery away from flamable objects	B			
7						Inside a sleeping room	Fire or smoke	3	Life-threatening injuries (survival uncertain), fatal injuries	4	>10% of operating time	3	Unattended charging hence no user present to reduce severity level	D			
8				Driving: Acceleration	Any weather condition, as specified in Chpt. 5 of Doc.2200 Environment Definition	Any road condition, as specified in Chpt. 3 of Doc.2200 Environment Definition	Fire or smoke, crashing into other traffic, possible loss of control	3	Life-threatening injuries (survival uncertain), fatal injuries	3	1%-10% of operating time	1	Difficult to overcharge the battery when drawing power from it	A			
9				Driving: Steady state velocity at 25 kph			Fire or smoke, crashing into other traffic, possible loss of control	3	Life-threatening injuries (survival uncertain), fatal injuries	4	>10% of operating time	1	Difficult to overcharge the battery when drawing power from it	B			
10				Driving: Braking			Fire or smoke, crashing into other traffic, possible loss of control	3	Life-threatening injuries (survival uncertain), fatal injuries	3	1%-10% of operating time	2	easy to overcharge a battery because there is no power being drawn	B			
11		3	Too little power stored (undervoltage)	Standstill	Any weather condition, as specified in Chpt. 5 of Doc.2200 Environment Definition	Any road condition, as specified in Chpt. 3 of Doc.2200 Environment Definition	charging a battery after it has reached the critical minimal cell voltage leads to overheating causing fire and smoke	3	Life-threatening injuries (survival uncertain), fatal injuries	4	>10% of operating time	3	Unattended charging hence no user present to reduce severity level	D			
12				Driving: Acceleration			Loss in vehicle performance due to degraded SOC.	1	Life-threatening injuries (survival uncertain), fatal injuries	3	1%-10% of operating time	2	Trained driver is able to control the situation.	QM			
13				Driving: Steady state velocity at 25 kph			Loss in vehicle performance due to degraded SOC.	1	Life-threatening injuries (survival uncertain), fatal injuries	4	>10% of operating time	2	Trained driver is able to control the situation.	A			
14				Driving: Braking			charging a battery from regenerative braking after it has reached the critical minimal cell voltage leads to overheating causing fire and smoke	3	Life-threatening injuries (survival uncertain), fatal injuries	3	1%-10% of operating time	2	Attended charging hence the user can reduce severity level	B			
15	F2.1.2 (Discharging battery cells)	4	Too little discharging of battery cells (providing too little energy)	Standstill	Any weather condition, as specified in Chpt. 5 of Doc.2200 Environment Definition	Any road condition, as specified in Chpt. 3 of Doc.2200 Environment Definition	discharging below the minimum operating voltage	0	No injuries	4	>10% of operating time	3	No driver present to control the situation	QM			
16				Driving: Acceleration			loss in vehicle performance causing other traffic to crash into ego vehicle, possible loss of control	2	Severe and life-threatening injuries (survival probable)	3	1%-10% of operating time	2	Trained driver is able to control the vehicle.	A			
17				Driving: Steady state velocity at 25 kph			loss in vehicle performance causing other traffic to crash into ego vehicle, possible loss of control	2	Severe and life-threatening injuries (survival probable)	4	>10% of operating time	2	Trained driver is able to control the vehicle.	B			
18				Driving: Braking			No failure	0	No injuries	3	1%-10% of operating time	1	Trained driver is able to control the situation.	QM			
19		5	Too much discharging of battery cells (providing too much energy)	Standstill	Any weather condition, as specified in Chpt. 5 of Doc.2200 Environment Definition	Any road condition, as specified in Chpt. 3 of Doc.2200 Environment Definition	discharging below the minimum operating voltage causing performance loss of the battery	0	No injuries	4	>10% of operating time	1	No need to control the situation since there is no hazard	QM			
20				Driving: Acceleration			draws too much current, causing overheating, smoke and fire	3	Life-threatening injuries (survival uncertain), fatal injuries	3	1%-10% of operating time	2	Trained driver is able to control the situation.	B			
21				Driving: Steady state velocity at 25 kph			draws too much current, causing overheating, smoke and fire	3	Life-threatening injuries (survival uncertain), fatal injuries	4	>10% of operating time	2	Trained driver is able to control the situation.	C			
22				Driving: Braking			No failure	0	No injuries	3	1%-10% of operating time	1	No need to control the situation since there is no hazard	QM			
23				Standstill			No failure	0	No injuries	4	>10% of operating time	3	Unattended charging hence no user present to reduce severity level	QM			

24	F2.1.3 (Store power)	6	Too little power stored (undervoltage)	Driving: Acceleration	Any weather condition, as specified in Chpt. 5 of Doc.2200 Environment Definition	Any road condition, as specified in Chpt. 3 of Doc.2200 Environment Definition	Loss in vehicle performance due to degraded SOC. This can lead to thermal runaway when charging leading to Hazard 2	1	Life-threatening injuries (survival uncertain), fatal injuries	3	1%-10% of operating time	2	Trained driver is able to control the situation.	QM		
25				Driving: Steady state velocity at 25 kph			Loss in vehicle performance due to degraded SOC. This can lead to thermal runaway when charging leading to Hazard 2	1	Life-threatening injuries (survival uncertain), fatal injuries	4	>10% of operating time	2	Trained driver is able to control the situation.	A		
26				Driving: Braking			charging a battery from regenerative braking after it has reached the critical minimal cell voltage leads to overheating causing fire and smoke	3	Life-threatening injuries (survival uncertain), fatal injuries	3	1%-10% of operating time	2	Attended charging hence the user can reduce severity level	B		
27		7	Too much power stored (overvoltage)	Standstill	Any weather condition, as specified in Chpt. 5 of Doc.2200 Environment Definition	On a beach with direct acces to water	fire and smoke	3	Life-threatening injuries (survival uncertain), fatal injuries	4	>10% of operating time	0	The user is present to reduce severity level because no flamable objects are present and the battery can be cooled immediately	A		
28						underneath a tree	fire and smoke	3	Life-threatening injuries (survival uncertain), fatal injuries	4	>10% of operating time	1	The user is present to move the battery away from flamable objects	B		
29						Inside a sleeping room	fire and smoke	3	Life-threatening injuries (survival uncertain), fatal injuries	4	>10% of operating time	3	Unattended charging hence no user present to reduce severity level	D		
30				Driving: Acceleration	Any weather condition, as specified in Chpt. 5 of Doc.2200 Environment Definition	Any road condition, as specified in Chpt. 3 of Doc.2200 Environment Definition	cells already at overvoltage are being used to draw power, leading to overheating causing fire and smoke	3	Life-threatening injuries (survival uncertain), fatal injuries	3	1%-10% of operating time	2	Trained driver is able to control the situation.	B		
31				Driving: Steady state velocity at 25 kph			cells already at overvoltage are being used to draw power, leading to overheating causing fire and smoke	3	Life-threatening injuries (survival uncertain), fatal injuries	4	>10% of operating time	2	Trained driver is able to control the situation.	C		
32				Driving: Braking			adding more power to already overvoltage cells, leads to overheating causing fire and smoke	3	Life-threatening injuries (survival uncertain), fatal injuries	3	1%-10% of operating time	2	Attended charging hence the user can reduce severity level	B		

Safety Goal			Safety Mechanism		
Sl. No.	Safety Goal ID No.	Safety Goal	Safety Mechanism ID No.	Functional Safety Concept	Technical safety concept
Function 'n'					
	F'n' safety goal-'n'				

Hazard Analysis and Risk Assessment
- Risk Graph -

Definitions according to ISO 26262-3

Controllability C	Exposure (E)	Severity (S)			
		S0	S1	S2	S3
C1	E1	QM	QM	QM	QM
	E2	QM	QM	QM	QM
	E3	QM	QM	QM	A
	E4	QM	QM	A	B
C2	E1	QM	QM	QM	QM
	E2	QM	QM	QM	A
	E3	QM	QM	A	B
	E4	QM	A	B	C
C3	E1	QM	QM	QM	A
	E2	QM	QM	A	B
	E3	QM	A	B	C
	E4	QM	B	C	D

If one of the parameters is considered to be 0 the result will be QM !

Excel automation

score = ((S+1)+C+E)*min(S;1)	value
0	QM
1	QM
2	QM
3	QM
4	QM
5	QM
6	QM
7	QM
8	A
9	B
10	C
11	D

EXAMPLE

Severity	Exposure	Controllability		Value
3	2	1		QM
3	4	3		D

Version control

Safety case owner:	
Safety case assessor:	
Lead author:	
Lead reviewer:	
Part subject (1000-7000):	7000
Sub-part subject (1000-7000):	7000
Version number:	1.1
Date of initiation (DD-MM-YYYY):	
Current date (DD-MM-YYYY):	

Document reference:
In the tab “Version control”, using the columns “Part reference” and “Sub-part reference", the applicant can point the CA towards the appropriate location inside the safety case structure to find the “Document reference” (i.e., the actual document which has undergone a change). The sheet “Utilities” provides a location to put the lists of parts/sub-parts/documents and statuses. In case a new document is added to the safety case this would be the first location to add the item to.
Version:
In the template and the example the following rules for version numbering apply: 1. Draft version numbers: The first draft of the document shall be Version 0.1, subsequent drafts shall have an increase of “0.1” inside the version numbering. 2. Final version numbers: Once a document is ready to be reviewed towards the CA, it shall have a full version number, e.g., the first final document is “1.0”, the second revision of the final document is “2.0”. 3. Draft revision after review: If a document has been assessed by the assessor and the document has been given a draft revision, it shall have an increment of “0.1” with respect to the previous version number (e.g., a draft revision of “1.0” will become “1.1”). Note, that once a revised draft is finalized (i.e., deemed ready for review by the CA), it shall be incrementally numbered according to (2) (e.g., draft revision “1.1” shall be numbered as final version “2.0”).
Lead author (applicant):
This column facilitates naming down the main point of contact for the revision of this document. For example, one could choose to provide the name of the lead safety engineer.
Lead reviewer (applicant):
It can be part of the QMS of the applicant to undergo a review phase of the document before it is provided to the CA. In this case, to show compliance with the QMS, the assessor can provide the point of contact for this review process.
Status:

The status of the document shows to the CA which document can be reviewed, which document is still in revision and which document may have not yet been given a revision. The states are defined as follows: - Obsolete: If a more recent revision is available of a certain document or the document no longer forms part of the safety case, it is denoted as obsolete. - In Revision: If, after a review by the CA, the applicant is still in the process of revising the document, it can be denoted as “In Revision”. In this state, the CA could still decide to review the contents, but can also decide to wait for a final revision. - On Hold: If the applicant doesn’t have enough information to provide the necessary changes to a document during the draft phase, or after a review by the CA, the status of the document is set to “On Hold”. - Ready for Review: If a draft is finalized, or when the applicant has updated the documents based on the review of the CA, the document can, once again, be set to “Ready for Review”.
Date of revision:
This column is used to denote the date of revision, coded as (DD-MM-YYYY).
Changelog:
Summarize the changes to a specific document in this location. No rules are set for this column, however it is advised to adhere to the following guidelines: - Summarize the changes in around 100 characters - Explain the “what” and “why” vs. the “how”

Safety case - Version control

Part reference	Sub-part reference
7000_Change_history	7000_Change_history
6000_Safety_concept	6500_FMEA
6000_Safety_concept	6300_Safety_mechanisms
6000_Safety_concept	6200_HARA
6000_Safety_concept	6100_High_level_safety_claim
2000_Item_definition	2200_Environment_definition
2000_Item_definition	2100_System_definition
1000_Introduction	1000_Introduction
7000_Change_history	7000_Change_history
6000_Safety_concept	6500_FMEA
6000_Safety_concept	6300_Safety_mechanisms
6000_Safety_concept	6200_HARA
6000_Safety_concept	6100_High_level_safety_claim
2000_Item_definition	2200_Environment_definition
2000_Item_definition	2100_System_definition
1000_Introduction	1000_Introduction
7000_Change_history	7000_Change_history
6000_Safety_concept	6500_FMEA
6000_Safety_concept	6300_Safety_mechanisms
6000_Safety_concept	6200_HARA
6000_Safety_concept	6100_High_level_safety_claim
2000_Item_definition	2200_Environment_definition
2000_Item_definition	2100_System_definition
1000_Introduction	1000_Introduction
7000_Change_history	7000_Change_history
6000_Safety_concept	6500_FMEA
6000_Safety_concept	6300_Safety_mechanisms
6000_Safety_concept	6100_High_level_safety_claim
2000_Item_definition	2200_Environment_definition
2000_Item_definition	2100_System_definition
1000_Introduction	1000_Introduction

Document reference	Version	Lead author (applicant)
7000_VersionControl_Example.xlsx	0.1	James Johnson
6400_FMEA_Example.xlsx	0.1	Maria Martinez
6300_SafetyMechanisms_Example.docx	0.1	Maria Martinez
6200_HARA_Example.xlsm	0.1	Maria Martinez
6100_HighLevelSafetyClaim_Example.docx	0.1	James Johnson
2200_EnvironmentDefinition_Example.docx	0.1	Maria Martinez
2100_ItemDefinition_Example.docx	0.1	David Smith
1000_IntroductionToTheSafetyCase_Example.docx	0.1	James Johnson
7000_VersionControl_Example.xlsx	0.2	Maria Martinez
6400_FMEA_Example.xlsx	0.2	Maria Martinez
6300_SafetyMechanisms_Example.docx	0.2	David Smith
6200_HARA_Example.xlsm	0.2	James Johnson
6100_HighLevelSafetyClaim_Example.docx	0.2	James Johnson
2200_EnvironmentDefinition_Example.docx	0.2	James Johnson
2100_ItemDefinition_Example.docx	0.2	James Johnson
1000_IntroductionToTheSafetyCase_Example.docx	0.2	James Johnson
7000_VersionControl_Example.xlsx	1.0	Maria Martinez
6400_FMEA_Example.xlsx	1.0	Maria Martinez
6300_SafetyMechanisms_Example.docx	1.0	James Johnson
6200_HARA_Example.xlsm	1.0	James Johnson
6100_HighLevelSafetyClaim_Example.docx	1.0	Maria Martinez
2200_EnvironmentDefinition_Example.docx	1.0	Maria Martinez
2100_ItemDefinition_Example.docx	1.0	James Johnson
1000_IntroductionToTheSafetyCase_Example.docx	1.0	Maria Martinez
7000_VersionControl_Example.xlsx	1.1	Maria Martinez
6400_FMEA_Example.xlsx	2.0	James Johnson
6300_SafetyMechanisms_Example.docx	1.1	James Johnson
6100_HighLevelSafetyClaim_Example.docx	1.1	Maria Martinez
2200_EnvironmentDefinition_Example.docx	1.1	Maria Martinez
2100_ItemDefinition_Example.docx	1.1	James Johnson
1000_IntroductionToTheSafetyCase_Example.docx	2.0	Maria Martinez

Lead reviewer (applicant)	Status	Date of revision	Changelog
David Smith	Obsolete	23-10-2020	
James Johnson	Obsolete	23-10-2020	
David Smith	Obsolete	23-10-2020	
David Smith	Obsolete	23-10-2020	
David Smith	Obsolete	23-10-2020	
David Smith	Obsolete	23-10-2020	System functions need to be ex
James Johnson	Obsolete	23-10-2020	
Maria Martinez	Obsolete	23-10-2020	
David Smith	Obsolete	15-12-2020	
James Johnson	Obsolete	15-12-2020	
James Johnson	Obsolete	15-12-2020	
David Smith	Obsolete	15-12-2020	Hazards are not defined in suffi
Maria Martinez	Obsolete	15-12-2020	
David Smith	Obsolete	15-12-2020	
Maria Martinez	Obsolete	15-12-2020	
Maria Martinez	Obsolete	15-12-2020	
David Smith	Obsolete	2-5-2021	
David Smith	Approved	2-5-2021	
Maria Martinez	Obsolete	2-5-2021	
David Smith	On hold	2-5-2021	
James Johnson	Obsolete	2-5-2021	
David Smith	Obsolete	2-5-2021	
David Smith	Obsolete	2-5-2021	
David Smith	Obsolete	2-5-2021	
David Smith	In Revision	18-11-2021	
David Smith	Ready for review	18-11-2021	
David Smith	In Revision	18-11-2021	
James Johnson	In Revision	18-11-2021	
David Smith	In Revision	18-11-2021	
David Smith	In Revision	18-11-2021	
David Smith	Ready for review	18-11-2021	

Status
Obsolete
On hold
In Revision
Ready for review
Approved

Safety case parts:
1000_Introduction
2000_Item_definition
3000_Evidence_guarantee_of_authenticity
4000_Certificates_of_compliance
5000_Risk_acceptance_criteria
6000_Safety_concept
7000_Change_history

Safety case sub-part:
1000_Introduction
2000_Item_definition
2100_System_definition
2200_Environment_definition
3000_Evidence_guarantee_of_authenticity
4000_Certificates_of_compliance
5000_Risk_acceptance_criteria
6000_Safety_concept
6100_High_level_safety_claim
6200_HARA
6300_Safety_mechanisms
6400_Design
6500_FMEA
6600_Test_plan
6700_Residual_risk
7000_Change_history

List of documents:
1000_IntroductionToTheSafetyCase_Example.docx
2100_ItemDefinition_Example.docx
2200_EnvironmentDefinition_Example.docx
6100_HighLevelSafetyClaim_Example.docx
6200_HARA_Example.xlsm
6300_SafetyMechanisms_Example.docx
6100_HighLevelSafetyClaim_Example.docx
6400_FMEA_Example.xlsx
7000_VersionControl_Example.xlsx

0. Approach

Safety Of The Intended Functionality (SOTIF) focusses on the absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons.
SOTIF is an analysis methodology that tries to identify lack of safety by considering the product to be assessed from different view angles. Using this approach, the number of known hazardous situations of the SOI can be increased. For the battery safety assessment, not the whole SOTIF is used but a selection of the most applicable analysis methods. If the potential risk of the application is high, additional analysis methods can be selected.

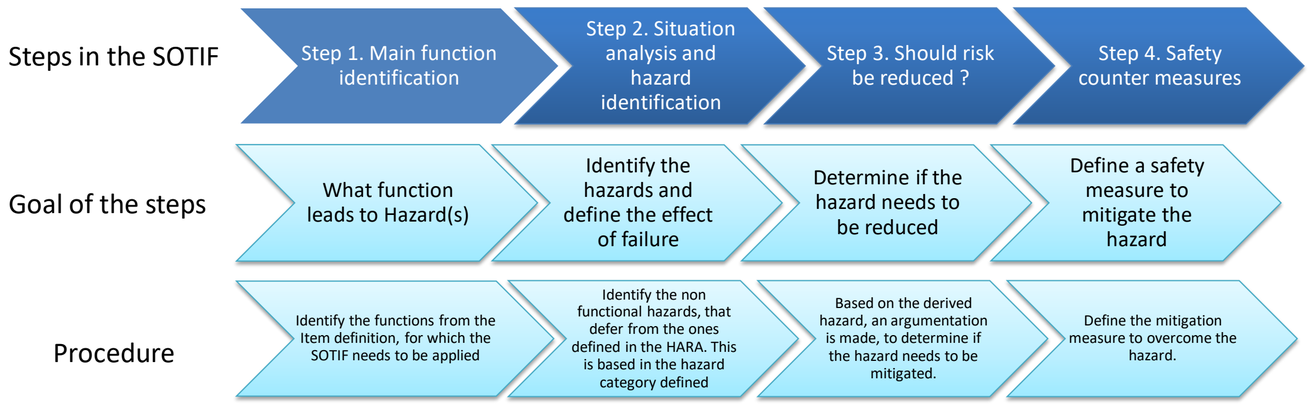

Figure 1. SOTIF process

3. SOTIF

In the 3. SOTIF page the process of the SOTIF as defined in Figure 1, is presented. The purple, blue, green and orange headings colums contain theinformation related to steps defined in Figure 1. The details of the procedure are further explained below.

Step 1. Main functions identification

Funtion class	High level function defined for the SOI. Failing of this function will be the source of the hazards.

Step 2: Situation analysis and hazard identification

Hazard catagory	These are the hazard catogories as defined in the SOTIF normative. For the purpose of this example a subset of these hazard catogories are choosen
Hazards	This defines the hazard based on a specific failure of the function, there can be multiple hazards resulting from different kinds of failures of the same functionality.
Scenario	Defines the different situations in which the hazard can be expected.
Weather	Defines the weather conditions, if it is one of the factors that affects the functionality being analysed.
Conditions	Includes all the external factors affecting the functionality, for instance radiations, surface on which the system operates, etc.
Effect of failure	The outcome due to the failure of the described hazard.

Step 3: Should the risk be reduced

Safety Measure required?	If a safety mesure needs is required is specifed here. This colum answers yes or no.
Argumentation	This column further explains why the safety measure is needed or not needed.

Step 4: Safety Measures

Proposal for improvement	The suggested safety measure to mitigate the hazard is mentioned. This can be to mitigate or reduce the defined hazard.
Argumentation	Further explaination of the propsosed improvement methodology

4. Lists

in this page a list of Scenarios, hazard catagory, effect of failure, Functional architecture components, To be considered and, the safety measures are listed.

One of the options mentioned in these lists are used to fill out the SOTIF. The list is predefined to have a finite number of effects of failure and their mitigating mesasure. This allows to have an overview of all the required safety measures.

More than one Hazard can result in the same mitigating measure.

SOTIF

Safety case owner:
Safety case assessor:
Lead author:
Lead reviewer:
Part subject (1000-7000):
Sub-part subject (1000-7000):
Version number:
Date of initiation (DD-MM-YYYY):
Current date (DD-MM-YYYY):

Change Tracking

User	Edited Sheet	Change Description	Date

			Situation analysis & Hazard identification						Should the risk be reduced?			Safety counter measure			
Nr	Function Class	Hazard category	Hazard	Driving & operation situation			Effect of failure		Safety measure required	Argumentation		Proposal for improvement	Argumentation		
				SCENARIO	WEATHER	Road layout and condition									
1	F2.1 Power Pack	1. Misuse	External charge battery while driving	Charging	Any weather condition, as specified in Chpt. 5 of Doc.2200 Environment Definition	Any road condition, as specified in Chpt. 3 of Doc.2200 Environment Definition	Battery Damage		placeholder	placeholder		placeholder	placeholder		
2	F2.1 Power Pack	1. Misuse	User asleep while charging battery	Charging	Indoors	Indoors	Fire and smoke		placeholder	placeholder		placeholder	placeholder		I
3	F2.1 Power Pack	1. Misuse	Incorrect HMI (user confusion)	placeholder	placeholder	placeholder	placeholder		placeholder	placeholder		placeholder	placeholder		
4	F2.1 Power Pack	1. Misuse	Prolonged charging	placeholder	placeholder	placeholder	placeholder		placeholder	placeholder		placeholder	placeholder		
5	F2.1 Power Pack	1. Misuse	placeholder	placeholder	placeholder	placeholder	placeholder		placeholder	placeholder		placeholder	placeholder		
6	F2.1 Power Pack	2. Triggering conditions	BMS shortage because of corrosion due to prologned usage in salty environments	storage, transport and end-of-life	Salty environments	On a beach with direct acces to water	Battery corossion		placeholder	placeholder		placeholder	placeholder		
7	F2.1 Power Pack	2. Triggering conditions	Overcharging due to faulty external charger	Charging	Any weather condition, as specified in Chpt. 5 of Doc.2200 Environment Definition	Any road condition, as specified in Chpt. 3 of Doc.2200 Environment Definition	Fire and smoke		placeholder	placeholder		placeholder	placeholder		
8	F2.1 Power Pack	2. Triggering conditions	Shortage in charger connection interface	placeholder	placeholder	placeholder	placeholder		placeholder	placeholder		placeholder	placeholder		
9	F2.1 Power Pack	2. Triggering conditions	Termal runaway due to offset in temperature sensor due to aging affects	placeholder	placeholder	placeholder	placeholder		placeholder	placeholder		placeholder	placeholder		
10	F2.1 Power Pack	2. Triggering conditions	Termal runaway due to lack of redundancy to resolve failure of battery temperature	placeholder	placeholder	placeholder	placeholder		placeholder	placeholder		placeholder	placeholder		
11	F2.1 Power Pack	3. ODD boundary exploration	Charging battery in sleeping room	Charging	Indoors	Inside a sleeping room	Fire and smoke		placeholder	placeholder		placeholder	placeholder		
12	F2.1 Power Pack	3. ODD boundary exploration	Operate battery at temperatures above 60 degrees	Driving	Any weather condition, as specified in Chpt. 5 of Doc.2200 Environment Definition	Any road condition, as specified in Chpt. 3 of Doc.2200 Environment Definition	Fire and smoke		placeholder	placeholder		placeholder	placeholder		
13	F2.1 Power Pack	3. ODD boundary exploration	Battery cell damage due to high frequent vibrations	placeholder	placeholder	placeholder	placeholder		placeholder	placeholder		placeholder	placeholder		
14	F2.1 Power Pack	3. ODD boundary exploration	Pierced battery cells due to mechanical impact	placeholder	placeholder	placeholder	placeholder		placeholder	placeholder		placeholder	placeholder		
15	F2.1 Power Pack	3. ODD boundary exploration	placeholder	placeholder	placeholder	placeholder	placeholder		placeholder	placeholder		placeholder	placeholder		

16	F2.1 Power Pack	4. System weaknesses	Diverged temperature sensor output below -10 degrees Celcius	storage, transport and end-of-life	Any weather condition, as specified in Chpt. 5 of Doc.2200 Environment Definition	Any road condition, as specified in Chpt. 3 of Doc.2200 Environment Definition	Battery Damage		placeholder	placeholder		placeholder	placeholder		
17	F2.1 Power Pack	4. System weaknesses	Battery casing not able to resist temperatures above 120 degrees Celcius	storage, transport and end-of-life	Any weather condition, as specified in Chpt. 5 of Doc.2200 Environment Definition	Any road condition, as specified in Chpt. 3 of Doc.2200 Environment Definition	Fire and smoke		placeholder	placeholder		placeholder	placeholder		
18	F2.1 Power Pack	4. System weaknesses	Cells are balanced slowly if temperature is below -10 degrees Celcius	placeholder	placeholder	placeholder	placeholder		placeholder	placeholder		placeholder	placeholder		
19	F2.1 Power Pack	4. System weaknesses	placeholder	placeholder	placeholder	placeholder	placeholder		placeholder	placeholder		placeholder	placeholder		
20	F2.1 Power Pack	4. System weaknesses	placeholder	placeholder	placeholder	placeholder	placeholder		placeholder	placeholder		placeholder	placeholder		

Scenario	Effect of failures	Hazard category	Functional architecture components	To be considered	Safety measure	SafetyMeasureArgumentation
	Fire and smoke Battery corossion Battery lekage Battery Damage short circuit No Failure	1. Misuse 2. Triggering conditions 3. ODD boundary exploration 4. System weaknesses	F2.1 Power Pack	TBD Yes No		

Date	Who		Tab	Change description

				Name	Lithium Ion	Lead Acid	Nickel	Nickel Cadmium	Gel battery (Lead Acid)	Sodium Ion	XXX	XXX	XXX	XXX	XXX
General description				Battery technology	Lithium Ion	Lead Acid	Nickel metal hydide	Nickel Cadmium	Gel battery (Lead Acid)		placeholder	placeholder	placeholder	placeholder	placeholder
				Abbreviation	Li-Ion	PB	Ni-Mh	Ni-Cd	AGM	Na-Ion	placeholder	placeholder	placeholder	placeholder	placeholder
				Construction	Jelly roll or pouch pack	polymer shell with "wet" anode/cathode	Cilindical	Cilindical	polymer shell with "wet" anode/cathode	Jelly roll or pouch pack	placeholder	placeholder	placeholder	placeholder	placeholder
				General use	EV's, Phones, PEV, UAV	Car starter battery	Mobile applications (Legacy)	Mobile applications (Legacy)	Campers,caravans, boats	Grid storage	placeholder	placeholder	placeholder	placeholder	placeholder
				Life time		1500 cycles	<5 year	15-20 year	10 year	5000 cycles	placeholder	placeholder	placeholder	placeholder	placeholder
				Nominal Single Cell Voltage (V)	3.6 - 3.7	2	1,2	1,3	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
ISO26262		Function		Hazard	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure
		F2.1.1 (Charging battery cells)		Too little charging of battery cells	No Failure, if properly cell balanced	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
				Overcharging of battery cells	Fire and Smoke	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
		F2.1.2 (Discharging battery cells		Too little discharging of battery cells	no hazard					placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
				Too much discharging of battery cells	no hazard, may degrade battery performance over time					placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
		F2.1.3 (Store power)		Too little power stored (undervoltage)	no hazard, may degrade battery performance over time					placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
				Too much power stored (overvoltage)	Fire and Smoke	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
		Fx.x.x (Placeholder)		placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder

Cells marked in this color denote placeholder for further expansion.

Nr	Function Class	Hazard category	Hazard	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure
1	F2.1 Power Pack	1. Misuse	Charging battery when in use	Battery Damage	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
2	F2.1 Power Pack	1. Misuse	User asleep (unattentive) while charging battery	Fire and smoke	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
3	F2.1 Power Pack	1. Misuse	Incorrect battery information shown on HMI (user confusion)	Battery Damage	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
4	F2.1 Power Pack	1. Misuse	Prolonged charging	Fire and smoke	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
5	F2.1 Power Pack	1. Misuse	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
6	F2.1 Power Pack	2. Triggering conditions	BMS shortage because of corrosion due to prologned usage in salty environments	Battery corossion	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
7	F2.1 Power Pack	2. Triggering conditions	Overcharging due to faulty external charger	Fire and smoke	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder

	Nr	Function Class	Hazard category	Hazard	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure	Effect of failure
	8	F2.1 Power Pack	2. Triggering conditions	Shortage in charger connection interface	Battery Damage	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
	9	F2.1 Power Pack	2. Triggering conditions	Termal runaway due to offset in temperature sensor due to aging affects	Battery Damage	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
	10	F2.1 Power Pack	2. Triggering conditions	Termal runaway due to lack of redundancy to resolve failure of battery temperature	Fire and smoke	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
		F2.1 Power Pack	2. Triggering conditions	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
	11	F2.1 Power Pack	3. ODD boundary exploration	Charging battery in sleeping room	No Failure	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
	12	F2.1 Power Pack	3. ODD boundary exploration	Operate battery at temperatures above 60 degrees	Fire and smoke	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
	13	F2.1 Power Pack	3. ODD boundary exploration	Battery cell damage due to high frequent vibrations	Battery Damage	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
	14	F2.1 Power Pack	3. ODD boundary exploration	Pierced battery cells due to mechanical impact	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
	15	F2.1 Power Pack	3. ODD boundary exploration	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
	16	F2.1 Power Pack	4. System weaknesses	Diverged temperature sensor output below -10 degrees Celcius	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
	17	F2.1 Power Pack	4. System weaknesses	Battery casing not able to resist temperatures above 120 degrees Celcius	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
	18	F2.1 Power Pack	4. System weaknesses	Cells are balanced slowly if temperature is below -10 degrees Celcius	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
	19	F2.1 Power Pack	4. System weaknesses	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder
	20	F2.1 Power Pack	4. System weaknesses	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder	placeholder

Scenario	Effect of failures	Hazard category	Functional architecture components	To be considered	Safety measure	SafetyMeasureArgumentation
	Fire and smoke Battery corossion Battery lekage Battery Damage short circuit No Failure	1. Misuse 2. Triggering conditions 3. ODD boundary exploration 4. System weaknesses	F2.1 Power Pack	TBD Yes No		