

HORIZON EUROPE PROGRAMME
TOPIC HORIZON-CL5-2022-D5-01-08
Clean and competitive solutions for all transport modes
GA No. 101084046

**Zero Emission flexible vehicle platform with modular
powertrains serving the long-haul Freight Eco System**



ZEFES - Deliverable report

D5.2 Functional Safety Concept



Funded by
the European Union

Deliverable No.	ZEFES D5.2	
Related WP	WP5	
Deliverable Title	Functional Safety Concept	
Deliverable Date	2024-06-28	
Deliverable Type	REPORT	
Dissemination level	Public (PU)	
Author(s)	Henning Wittig (FHG) Jakub Rehor (FHG)	
Checked by	Henning Wittig (FHG)	2024-06-26
Reviewed by (if applicable)	Johanna Axelsson (VOL) Gerd Schünemann (ZF)	2024-06-26
Approved by	Omar Hegazy (VUB) – Project coordinator	2024-06-27
Status	Final	2024-06-28

Publishable summary

Within the Green Deal, Europe commits itself to be the first CO₂ neutral continent by 2050. To achieve this, a first milestone is defined as an overall CO₂ reduction target of 55% by 2030. For the road transport sector, the target is set at 30% less CO₂ emissions by 2030, following Regulation (EU) 2019/1242. The regulation requires that manufacturers of heavy-duty vehicles (HDV) deliver more efficient vehicles to achieve a reduction of CO₂ emissions for the newly produced fleet of 15% in 2025 and 30% in 2030. This deliverable presents the investigation of functional safety of the modular multi-powertrain concept according to ISO 26262-3. It describes the main results that are documented in the work products item definition, hazard analysis and risk assessment, and functional safety concept of an e-trailer as part of the distributed powertrain.

After the scope of the investigation in terms of the different types of e-trailers that are considered and the vehicle combinations that can use these e-trailers is defined, the functional concept of the e-trailer including the basic functions of the powertrain and the functional behaviour of the system on the level of the vehicle combination is described. The hazards for the driver or other road users are identified by analysing potential malfunctioning behaviours or fault characteristics of the e-trailer functions.

First requirements are derived in terms of technical constrains and organizational measures regarding the e-trailer and the vehicle combinations. The technical constrains are defined during the concept phase of the ZE modular multi-powertrain and should be considered when discussing or changing the concept. The organizational measures shall be fulfilled during the use cases since they ensure safety by avoiding potentially hazardous situations.

As the result of the hazard analysis and risk assessment, the safety goals and functional safety requirements with an ASIL classification are presented. These requirements are the main content of the functional safety concept. They represent the requirements on the e-trailer powertrain concept from a functional point of view and must be considered in the development and application of the e-trailer in the ZEFES use cases.

Contents

1	Introduction.....	9
2	Background and procedures	12
3	Scope of the item	13
4	Functional concept of e-trailer powertrain.....	15
4.1	Forward propulsion by EMG	16
4.2	Enable coasting	16
4.3	Regenerative Braking by EMG (recuperation)	17
5	Identification of hazards.....	17
5.1	Determination of malfunctions.....	17
5.2	Description of hazards	18
5.2.1	Frontal collision	18
5.2.2	Lateral collision.....	19
5.2.3	Rear collision.....	19
5.2.4	Unintended drive off, frontal collision	19
5.2.5	Unintended drive off, rear collision.....	19
5.2.6	Unintended movement of wheels.....	19
5.2.7	Trailer swing, lateral collision	19
5.2.8	Jack knifing, lateral collision	20
5.2.9	Straightening	20
6	Technical constraints and organizational measures	21
7	Description of Safety Goals	22
7.1	SG-01 As long as the vehicle is accelerating, the e-trailer shall not push its towing vehicle because of MF-1: too high acceleration.....	23
7.1.1	Description of Safety Goal	23
7.1.2	Criteria to achieve the Safety Goal.....	23
7.1.3	ASIL	23
7.1.4	Safe state	23
7.1.5	Associated functional safety requirements.....	23
7.2	SG-02 As long as the vehicle is accelerating, the e-trailer shall prevent wheel slip at its driven axle because of MF-1: too high acceleration.	23
7.2.1	Description of Safety Goal	23
7.2.2	Criteria to achieve the Safety Goal.....	23

7.2.3	ASIL	24
7.2.4	Safe state	24
7.2.5	Associated functional safety requirements.....	24
7.3	SG-03 As long as the vehicle is at standstill, the e-trailer shall not push its towing vehicle because of MF-3: unintended acceleration.	24
7.3.1	Description of Safety Goal	24
7.3.2	Criteria to achieve the Safety Goal.....	24
7.3.3	ASIL	24
7.3.4	Safe state	24
7.3.5	Associated functional safety requirements.....	24
7.4	SG-04 As long as the vehicle is driving forward, the e-trailer shall not push its towing vehicle because of MF-3: unintended acceleration.	24
7.4.1	Description of Safety Goal	24
7.4.2	Criteria to achieve the Safety Goal.....	25
7.4.3	ASIL	25
7.4.4	Safe state	25
7.4.5	Associated functional safety requirements.....	25
7.5	SG-05 As long as the vehicle is driving forward, the e-trailer shall prevent wheel slip at its driven axle because of MF-3: unintended acceleration.....	25
7.5.1	Description of Safety Goal	25
7.5.2	Criteria to achieve the Safety Goal.....	25
7.5.3	ASIL	25
7.5.4	Safe state	25
7.5.5	Associated functional safety requirements.....	25
7.6	SG-06 As long as the vehicle is accelerating, the e-trailer shall not increase its pulling force on the towing vehicle because of MF-4: wheel torque in wrong direction.....	26
7.6.1	Description of Safety Goal	26
7.6.2	Criteria to achieve the Safety Goal.....	26
7.6.3	ASIL	26
7.6.4	Safe state	26
7.6.5	Associated functional safety requirements.....	26
7.7	SG-07 As long as the vehicle is accelerating, the e-trailer shall prevent wheel slip at its driven axle because of MF-4: wheel torque in wrong direction.	26
7.7.1	Description of Safety Goal	26

- 7.7.2 Criteria to achieve the Safety Goal 27
- 7.7.3 ASIL 27
- 7.7.4 Safe state 27
- 7.7.5 Associated functional safety requirements 27
- 7.8 SG-08 As long as the vehicle is decelerating, the e-trailer shall prevent wheel slip at its driven axle because of MF-5: too high deceleration..... 27
 - 7.8.1 Description of Safety Goal 27
 - 7.8.2 Criteria to achieve the Safety Goal 27
 - 7.8.3 ASIL 27
 - 7.8.4 Safe state 27
 - 7.8.5 Associated functional safety requirements 27
- 7.9 SG-09 As long as the vehicle is driving forward, the e-trailer shall not increase its pulling force on the towing vehicle because of MF-6: unintended deceleration. 28
 - 7.9.1 Description of Safety Goal 28
 - 7.9.2 Criteria to achieve the Safety Goal 28
 - 7.9.3 ASIL 28
 - 7.9.4 Safe state 28
 - 7.9.5 Associated functional safety requirements 28
- 7.10 SG-10 As long as the vehicle is driving forward, the e-trailer shall prevent wheel slip at its driven axle because of MF-6: unintended deceleration. 28
 - 7.10.1 Description of Safety Goal..... 28
 - 7.10.2 Criteria to achieve the Safety Goal..... 28
 - 7.10.3 ASIL..... 29
 - 7.10.4 Safe state..... 29
 - 7.10.5 Associated functional safety requirements 29
- 7.11 SG-11 As long as the vehicle is decelerating, the e-trailer shall not increase its pushing force on the towing vehicle because of MF-7: wheel torque in wrong direction..... 29
 - 7.11.1 Description of Safety Goal..... 29
 - 7.11.2 Criteria to achieve the Safety Goal..... 29
 - 7.11.3 ASIL..... 29
 - 7.11.4 Safe state..... 29
 - 7.11.5 Associated functional safety requirements 29
- 7.12 SG-12 As long as the vehicle is decelerating, the e-trailer shall prevent wheel slip at its driven axle because of MF-7: wheel torque in wrong direction. 30

7.12.1	Description of Safety Goal.....	30
7.12.2	Criteria to achieve the Safety Goal.....	30
7.12.3	ASIL.....	30
7.12.4	Safe state.....	30
7.12.5	Associated functional safety requirements	30
7.13	SG-13 Prevent harm by a thermal runaway of the battery.	30
7.13.1	Description of Safety Goal.....	30
7.13.2	Criteria to achieve the Safety Goal.....	30
7.13.3	ASIL.....	30
7.13.4	Safe state.....	30
7.13.5	Associated functional safety requirements	31
8	Safe States.....	31
9	Functional safety requirements	31
10	Results and Discussion	34
10.1	Results.....	34
10.2	Conclusion and Recommendation	35
10.3	Contribution to project (linked) Objectives	35
10.4	Contribution to major project exploitable result.....	36
11	Risks and interconnections.....	36
11.1	Risks/problems encountered.....	36
11.2	Interconnections with other deliverables.....	36
12	References.....	37
13	Acknowledgement	38

List of Figures

Figure 1-1: Relation of deliverable D5.2 to deliverables of WP5 and other WPs	10
Figure 4-1: Block diagram of functions on vehicle level.....	15

List of Tables

Table 3-1: Vehicle combinations considered to be equipped with a modular multi-powertrain.....	13
Table 3-2: Scope of the item definition: e-trailers considered to be part of a vehicle combination equipped with a modular multi-powertrain	14
Table 3-3: Vehicle combinations and position of e-trailer	14

Abbreviations & Definitions

Abbreviation	Explanation
BEV	Battery Electric Vehicle
EMG	Electric Motor Generator of the e-trailer
EMS	European Modular System
EMS1	EMS vehicle combination consisting of truck, dolly, and semitrailer.
EMS2	EMS vehicle combination consisting of tractor, semitrailer, dolly, and semitrailer.
FSC	Functional Safety Concept
FSR	Functional Safety Requirement
HARA	Hazard Analysis & Risk Assessment
MF	Malfunction
SG	Safety Goal

Item	Definition
Prime mover	Truck or tractor
Trailer	Semitrailer or dolly
Vehicle	Truck, tractor, semitrailer, or dolly
Vehicle combination	Combination of a truck or tractor with up to five trailers

1 Introduction

In the ZEFES work package 5 the modular and flexible battery-electric powertrains and their integration in five demonstrators is realized. These demonstrator vehicle combinations consist of five battery-electric towing vehicles, two electrified semitrailers, and one electrified converter dolly.

The work includes the development of a modular battery-electric powertrain concept for long-haul heavy-duty vehicle combinations, which are adaptable to daily demands of mission profiles in terms of range and power, and flexible in terms of integration of batteries and powertrains in different vehicle units. For this powertrain concept a functional safety concept is created.

To realize the vehicle units, specific powertrain components, subsystems, control systems and energy & thermal management systems are adapted and integrated in the prime mover battery-electric powertrains. Development and integration effort are also made to realize the next generation e-trailers serving as range extender integrated in the electric powertrain of the prime mover.

The following list shall clarify the context of deliverable D5.2:

D5.1 - System specification for ZE modular multi-powertrain concepts: In this deliverable the system specification of the battery-electric vehicle combinations with a modular multi-powertrain is verified and evaluated. The upgraded vehicle simulation tool IVision is used to verify the final design specifications of each targeted BEV demo.

D5.2 – Functional Safety Concept: The deliverable investigated the functional safety concept for the vehicle combinations with a modular multi-powertrain. The concept of an additional powertrain located in a trailer is described in terms of its application area, its functional behaviour on vehicle level, the powertrain functions, and a draft system architecture. Furthermore, the results of the hazard analysis and risk assessment are presented including the derived safety goals and functional safety requirements for the development of the electrified trailers and the application in the ZEFES use cases.

D5.3 - Powertrain components and control systems for next generation battery-electric trucks: Within the deliverable the innovations and system improvements for the battery-electric towing vehicles developed by SCA, VOL and REN are described. This includes results of the proof of concept.

D5.4 - Next generation battery-electric trailers: The deliverable describes the adaptations and improvements of the e-semitrailer and the e-dolly as part of the modular multi-powertrain vehicle combinations. This includes the improvement of the mechanical design for the trailer chassis, based on the existing ZF e-trailer, and the development efforts regarding the powertrain components, controls, and auxiliary systems.

D5.5 - Commissioning, testing and verification connectivity between BEV demonstrators and digital twin tool: The deliverable briefly describes the results of the commissioning and testing of the data interface between the demonstrator vehicles and the digital twin tool developed in work package 4.

D5.6 - Realization and commissioning of all BEV demonstrators: In this deliverable the commissioning and testing of the six battery-electric demonstrator vehicle combinations is

presented including the results of short dry run tests. As a result of the work described in this document the vehicle combinations can be handed over to WP7 use cases.

The position of deliverable D5.1 within WP5 and the relation to other deliverables and work packages is shown in Figure 1-1.

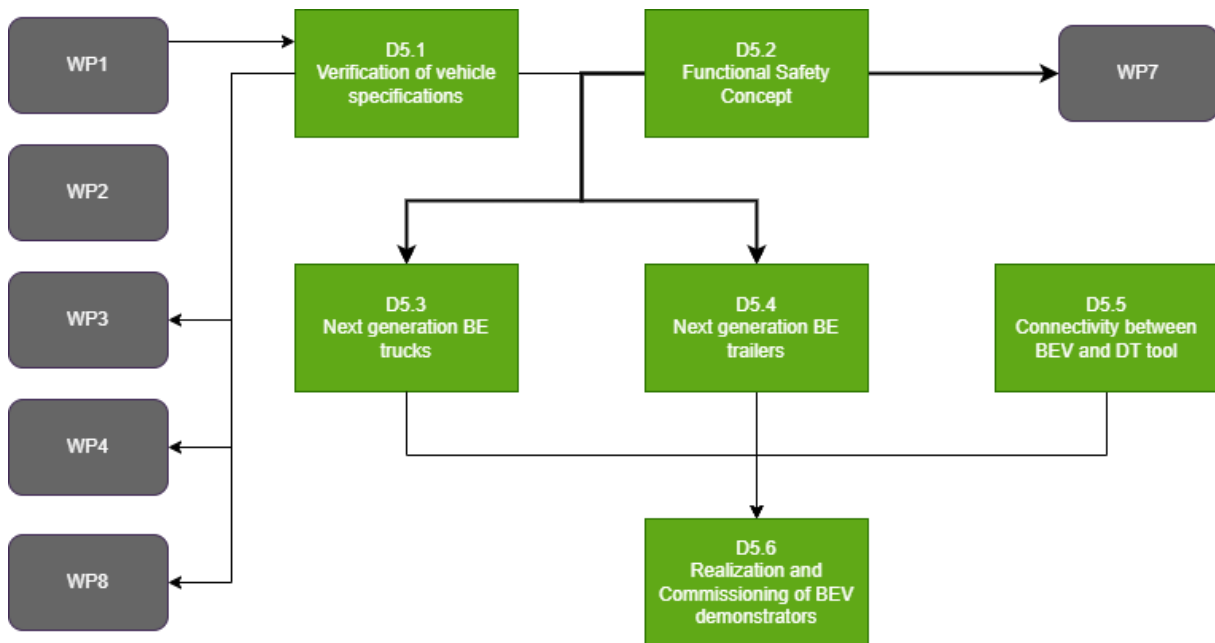


Figure 1-1: Relation of deliverable D5.2 to deliverables of WP5 and other WPs

Chapter 2 of the present document presents the procedure that was followed for creating the functional safety concept for the modular multi-powertrain. It gives an overview of the three steps including the creation of the item definition in Task 5.1, the design of the hazard analysis and risk assessment in subtask 5.2.1 and the derivation of the functional safety concept in subtask 5.2.2. Chapter 3 describes the scope of the investigation in terms of the different types of e-trailers that are considered and the vehicle combinations that can use these e-trailers.

In chapter 4 the functional concept of the e-trailer is presented. The main functions of the e-trailer powertrain as part of the modular multi-powertrain concept are “forward propulsion by EMG”, “enable coasting” and “regenerative braking by EMG (recuperation)”. The relevant preconditions that must be considered to realize the e-trailer functions are introduced and the functional behaviour of the e-trailer on the level of the vehicle combination is described.

Chapter 5 presents hazards that are identified by analysing the e-trailer functions and potential malfunctioning behaviours or fault characteristics.

Chapter 6 describes the technical constraints and organizational measures regarding the e-trailer. The technical constraints are defined during the concept phase of the ZE modular multi-powertrain and should be considered when discussing or changing the concept. The organizational measures shall be fulfilled during the use cases since they ensure safety by avoiding potentially hazardous situations.

Chapter 7, chapter 8, and chapter 9 describe the safety goals, the safe states, and the functional safety requirements, respectively. These are the results of the HARA and the main content of the functional safety concept. They represent the requirements on the e-trailer powertrain concept from a functional point of view and must be considered in the development and application of the e-trailer in the ZEFES use cases.

In chapter 10 the results are summarised and conclusions for the further realization and commissioning of the e-trailer in Task 5.4 and Task 5.5 as well as the application in the use case demonstration in WP8 are drawn.

2 Background and procedures

The investigation of functional safety of the vehicle combinations with a modular multi-powertrain done in work package 5 task 5.2 and presented in this deliverable includes

- the description of the considered system and its functionalities in an Item Definition,
- the identification and classification of the hazardous events caused by a malfunctioning behavior of the system in a Hazard Analysis and Risk Assessment (HARA) and
- the definition of a functional safety concept

to prepare the development and application of vehicle combinations with a modular multi-powertrain in the ZEFES use cases.

The item definition describes the considered item in terms of a trailer with an electric powertrain. The trailer can be a semitrailer or a dolly. The item is meant to be applied in a vehicle combination containing other vehicles equipped with a conventional (ICE) or a zero-emission powertrain. This combination of powertrains is hereinafter referred to as modular multi-powertrain.

The item described in the item definition is developed to be used in certain use cases of the ZEFES project during a demonstration phase of up to six months. Thus, the application area and operating environment is limited to the ones prevailing in the use cases during the demonstration.

The item definition further describes the operating modes and functional behaviour of the e-trailer at the level of the vehicle combination. Based on these definitions the effects of operational shortfalls on the vehicle combination are derived. Considering the functional dependencies and the dependencies of the item on other items of the e-trailer, a preliminary functional architecture of electric/electronic systems that must be considered in the investigation of functional safety is also derived.

Existing knowledge from former developments is included in the item definition.

The HARA contains an Excel file [1] and a corresponding explanatory document [2]. It identifies the hazards (hazard analysis) and assesses the resulting risks (risk assessment) by the e-trailer. The cause of the hazards is considered to be the non-fulfilment of the functions of the e-trailer (also: malfunction of the e-trailer). The hazardous events resulting from the hazards are evaluated with regard to the severity of their impact (severity), the probability of their occurrence (exposure) and their controllability in the various operating situations of the vehicle combination that uses the e-trailer. This evaluation was done by all ZEFES partners involved in the realization of vehicle combinations with a modular multi-powertrain (ZF, KAE, VET, SCA, VOL, FHG) in a workshop followed by several reviews to align the results. Finally, Safety Goals are derived with an ASIL classification.





The supporting document for the HARA describes several intermediate steps from the definition of the elements used to create the operating scenarios till the definition of the hazardous events and the final risk assessment. Along with the pure definitions the reasons for certain decisions are given.

3 Scope of the item

This section is a copy of section 2 from “Item Definition for ZE modular multi-powertrain concepts” [3] and gives an overview of the vehicle combinations and e-trailers under consideration.

Table 3-1 shows the vehicle combinations that are considered to be equipped with a modular multi-powertrain and the distribution of the battery electric powertrains among the vehicle units. The tractor – semitrailer, EMS1 and EMS2 vehicle combinations have one use case each in the ZEFES project.



Table 3-1: Vehicle combinations considered to be equipped with a modular multi-powertrain

Type of vehicle combination	Prime mover	1 st trailer	2 nd trailer	3 rd trailer
Tractor – semitrailer 	BEV tractor	e-semitrailer	-	-
EMS1 	BEV truck	Standard dolly	e-semitrailer	-
EMS1 	BEV truck	e-dolly	Standard semitrailer	-
EMS2 	BEV tractor	Standard semitrailer	e-dolly	Standard semitrailer

In an early stage of the project, it was decided not to develop a dedicated vehicle-to-vehicle interface to control the available battery electric powertrains in the vehicle combination by one centralized energy and torque management system located in the prime mover. Thus, the powertrains in the trailer units are controlled based on information available on the standard ISO 11992-2 EBS interface or given by other sources (e.g., sensors) located on the individual trailer unit.

Therefore, the prime mover is not in the scope of this item definition. The item definition describes only a trailer, be it a dolly or a semitrailer, equipped with a battery electric drivetrain (see Table 3-2). This trailer is hereinafter referred to as e-trailer.

Table 3-2: Scope of the item definition: e-trailers considered to be part of a vehicle combination equipped with a modular multi-powertrain





ID	e-trailer	Description
T-01		Two- or three-axle-semitrailer with a battery electric powertrain
T-02		Two axle converter dolly with a battery electric powertrain (due to the limited space the energy storage unit is not visualized in the pictogram of the e-dolly)

Each e-trailer has despite the driven axle at least one further non-driven axle, that is not a lift axle. This is a mechanical constraint, that ensures a stabilization of the e-trailer in case of malfunctions of the battery electric powertrain in well-defined scenarios (see HARA [1]).

To further narrow down the scope of the item definition, the item described contains only the battery electric drivetrain and its control system installed in the e-trailer.

In the considered vehicle combinations only one e-trailer is used to create a multi-powertrain. This e-trailer can be of different type and located in different trailer positions. Table 3-3 shows the position of the e-trailer in the vehicle combination with a multi-powertrain.

Table 3-3: Vehicle combinations and position of e-trailer

ID	e-trailer in vehicle combination	Description
VC-01		Vehicle combination: tractor – semitrailer e-trailer: e-semitrailer position: 1 st trailer
VC-02		Vehicle combination: truck – dolly – semitrailer e-trailer: e-semitrailer position: 2 nd trailer
VC-03		Vehicle combination: truck – dolly – semitrailer e-trailer: e-dolly position: 1 st trailer
VC-04		Vehicle combination: tractor – semitrailer – dolly – semitrailer e-trailer: e-dolly position: 2 nd trailer

In case of an e-dolly the system is defined in a way that in principle allows an autonomous yard operation of an e-dolly – semitrailer combination. In this scenario the electric powertrain of the e-dolly will deliver the power exclusively to operate the vehicle combination with shunting speed. As this scenario applies special requirements to the vehicle equipment and the operation environment, it is not part of the modular multi-powertrain and is therefore not covered by this document.

4 Functional concept of e-trailer powertrain

The following section describes the functional behaviour of the item on vehicle level. The provided functions are:

- Forward propulsion by EMG,
- Enable coasting and
- Regenerative braking by EMG (recuperation).

These three functions are separated into blocks and shown in Figure 4-1. They are described in detail in sections 4.1 to 4.3.

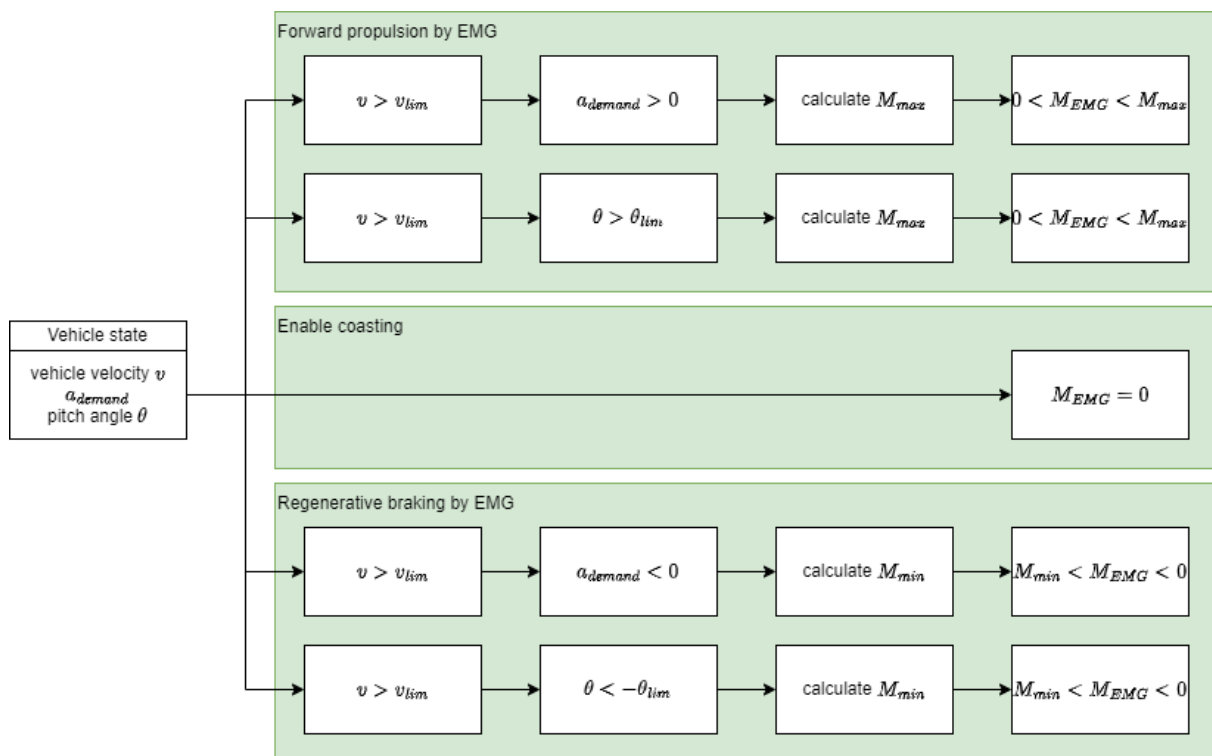


Figure 4-1: Block diagram of functions on vehicle level

The blocks represent necessary preconditions for the functions and the according effect on the drive torque of the EMG. Following information are part of the functional concept:

- Vehicle velocity v
- Wheel speed
- acceleration or deceleration a_{demand} demanded by driver or driver assistance system
- Pitch angle of the e-trailer θ
- Minimal possible drive torque M_{min}
- Maximum possible drive torque M_{max}

- Current drive torque of the EMG M_{EMG}

After all, the functional safety requirements in chapter 9 can be derived from this functional concept.

4.1 Forward propulsion by EMG

This section is a copy of section 5.2.1 from “Item Definition for ZE modular multi-powertrain concepts” [3].

The system shall support the acceleration request of the driver or driver assistance system during forward driving. This is done by driving with the EMG of the e-trailer under the following conditions that have to be detected by the system:

- the vehicle combination is driving in forward direction **and**
- the vehicle combination
 - is accelerating **or**
 - is going uphill.

To not influence the driving stability of the vehicle combination negatively, the e-trailer always remains a towed vehicle. It supports the prime mover by reducing the necessary drag forces to tow the e-trailer.

Usually, vehicle diagnostic systems of the prime mover are determining e.g., the axle loads during gearshifts in low speed. Thus, the vehicle control system is able to provide dynamic traction and brake performance depending on the operating conditions. To not influence these vehicle diagnostic systems negatively, the system does not support the acceleration request during low speed and gearshifts of the prime mover. It must also be considered to not negatively influence vehicle diagnostic system in zero-emission prime movers that are not equipped with a conventional gearbox.

4.2 Enable coasting

This section is a copy of section 5.2.3 from “Item Definition for ZE modular multi-powertrain concepts” [3].

The system shall minimize the drag torque of the driven axle while neither an acceleration request nor a deceleration request of the driver or driver assistance system is detected. Furthermore, the system shall minimize the energy consumption of the e-trailer while neither forward propulsion nor regenerative braking with the EMG of the e-trailer is necessary.

The function “enable coasting” might be realized in different ways, depending on the characteristics of the implemented EMG and powertrain components of the e-trailer:

- by implementing a specific functionality,
- by using a neutral gear or
- by deactivating the EMG.

4.3 Regenerative Braking by EMG (recuperation)

This section is a copy of section 5.2.2 from "Item Definition for ZE modular multi-powertrain concepts" [3].

The system shall support the deceleration request of the driver or driver assistance system during forward driving. This is done by regenerative braking with the EMG of the e-trailer under the following conditions that have to be detected by the system:

- the vehicle combination is driving in forward direction **and**
- the driver or driver assistance system is requesting deceleration.

Furthermore, the item uses regenerative braking by EMG if it detects:

- the vehicle combination is driving in forward direction **and**
- the vehicle combination is driving downhill above a specific incline.

Energy that is recuperated by the EMG is stored in the battery of the e-trailer.

5 Identification of hazards

This chapter is a copy of chapter 3 from "Supporting document to e-trailer hazard analysis and risk assessment" [2].

The hazards are systematically determined using the HAZOP procedure. The basis is the assignment of the required functions that describe the functional behavior at the level of the vehicle combination (see chapter 4) to certain fault characteristics. The combination of the functions with the fault characteristics results in malfunctions that are evaluated in the context of hazard analysis with regard to potential hazards.

5.1 Determination of malfunctions

In order to determine the corresponding malfunctions, five fault characteristics are considered for the vehicle or system functions, apart from the correct performance of the function:

- "correctly" provided (exactly the specified effect is present),
- "not" (there is no effect at all),
- "too weak"¹ (the effect is weaker than specified),¹
- "too strong"¹ (the effect is stronger than specified)¹,
- "invers" (the effect is in the opposite direction or contrary to the driving requirement),
- "without requirement" (there is an unsolicited effect).

The assignment of functions and fault characteristics is shown in Table 5-1 . "x" marks a semantically meaningful combination of function and fault characteristics.

¹ The fault values "too weak" and "too strong" are generally formulated and independent of a physical quantity. They can be related, for example, to the torque or to the change of torque applied by the driven axle.

Table 5-1: Semantically meaningful combination of functions and fault characteristics

Fault characteristics \ function	not	too weak	too strong	invers	no requirement
Forward propulsion by EMG		x	x	x	x
Regenerative braking by EMG (recuperation)		x	x	x	x
Enable coasting					x
Driver warning	x				

This results in 10 combinations of function and fault expression. These combinations are the starting point for the Hazard Analysis. Taking into account point 6.4.2.3 of [ISO26262-3]: "Hazards caused by malfunctioning behavior of the item shall be defined at the vehicle level"², each of the faults is described (column B "Malfunction") and analyzed with regard to its effect on the vehicle (column D "Malfunction on vehicle level").

Afterwards, each fault case is assigned to the identified hazards (column E "Potential Hazard"). If a fault does not result in a hazard, this is justified in column F "Comment". The hazards listed have been identified in several iterations during the creation and editing of the HARA [1] worksheets and are described in more detail in Chapter 5.2.

5.2 Description of hazards

This section describes the hazards identified during the hazard analysis.

5.2.1 Frontal collision

The hazard relates to the forward driving. The vehicle behaviour differs from the driving behaviour that is expected by the driver or other road users.

In case the acceleration support by the e-trailer is not present, the driver might misjudge a situation, e.g. overtaking other vehicles, which results in a frontal collision with other road users. The hazardous events only consider frontal collisions while overtaking with protected road users, since collisions with unprotected road users will cause comparable harm.

In case there is too high acceleration support by the e-trailer, the driver might not handle the overall vehicle acceleration correctly, which results in a frontal collision, e.g. with other road users in front of the vehicle combination.

Usually, frontal collisions should be avoided by maintaining the safety distance between the vehicle combination and other road users in front. Nevertheless, this hazard is taken into consideration since the safety distances are undercut in various situations.

² In general, each hazard will have a variety of potential causes related to the item's implementation, but these causes do not need to be considered in the hazard analysis and risk assessment for the analysis of the malfunctioning behavior.

Only hazards associated with malfunctioning behavior of the item are considered; every other system (external measure) is presumed to be functioning correctly provided it is sufficiently independent.

5.2.2 Lateral collision

The hazard relates to the forward driving. The vehicle behaviour differs from the driving behaviour that is expected by other road users.

In case the acceleration support by the e-trailer is not present, the driver might misjudge a situation, e.g. turn into a busy road, which results in a lateral collision with other road users.

5.2.3 Rear collision

The hazard relates to the forward driving. The vehicle behaviour differs from the driving behaviour that is expected by other road users.

In case

- the acceleration support by the e-trailer is too low,
- the e-trailer applies a wheel torque in wrong direction while acceleration or
- the deceleration by the e-trailer is unintended or too high,

other road users might misjudge a situation. This situation can be, e.g., acceleration of the vehicle combination on an entrance ramp to the highway, which results in a rear collision with other road users behind the vehicle combination.

Usually, rear collisions should be avoided by maintaining the safety distance between the vehicle combination and other road users in behind. Nevertheless, this hazard is taken into consideration since the safety distances are undercut in various situations.

5.2.4 Unintended drive off, frontal collision

The hazard relates to the standstill of the vehicle combination.

In case of an unintended acceleration by the e-trailer in forward direction, the driver might not handle the unintended drive off of the vehicle correctly, which results in a frontal collision, e.g. with other road users in front of the vehicle combination.

An unintended drive off is not possible in situations where the parking brake of the vehicle is activated since this will prevent the vehicle combination from being pushed by the e-trailer.

5.2.5 Unintended drive off, rear collision

The hazard relates to the standstill of the vehicle combination.

In case of an unintended acceleration by the e-trailer in rearward direction, the driver might not handle the unintended drive off of the vehicle correctly, which results in a rear collision, e.g. with other road users behind the vehicle combination.

An unintended drive off is not possible in situations where the parking brake of the vehicle is activated since this will prevent the vehicle combination from being pushed by the e-trailer.

5.2.6 Unintended movement of wheels

The hazard relates to the workshop situation when the vehicle is raised.

In case of an unintended acceleration by the e-trailer, workshop employees might be dragged into the driven wheels of the e-trailer.

5.2.7 Trailer swing, lateral collision

The hazard relates to forward driving.

In case of

- too high acceleration,
- an unintended acceleration,
- a wheel torque in wrong direction while acceleration,
- too high deceleration,
- unintended deceleration or
- wheel torque in wrong direction while deceleration

by the e-trailer, the driven axle can show wheel slip combined with reduced cornering forces. If the vehicle combination is driven at the physical limit of the stabilizing axles of the e-trailer (so-called “foreseeable misuse”), it might result in trailer swing and lateral collision with other road users.

While driving on highway like roads the physical limits can only be reached in situations with a reduced friction value (“reduced μ ”). Otherwise (on normal friction value), the road characteristics like lane width and curve radius do not enable driving at the physical limit.

While driving on country/secondary roads it is also possible to reach the physical limit on normal friction value.

Trailer swing is considered to result in a hazard for

- unprotected road user (in front/behind/next to ego),
- protected road user in hazardous area < 2m (in front/behind/next to ego).

5.2.8 Jack knifing, lateral collision

The hazard relates to forward driving.

In case of

- too high acceleration,
- unintended acceleration or
- wheel torque in wrong direction while deceleration

by the e-trailer, the e-trailer can push its predecessor to an extent that results in a loss of cornering forces of the rear axles of that predecessor. This causes a swing out (skid) of the predecessor until it spins around and faces backwards.

Jack knifing is considered to result in a hazard for

- unprotected road user (in front/behind/next to ego),
- protected road user in hazardous area < 2m (in front/behind/next to ego).

5.2.9 Straightening

The hazard relates to the forward driving.

In case of an unintended deceleration by the e-trailer or a wheel torque in wrong direction by the e-trailer while the vehicle combination is accelerating, the whole vehicle combination might be straightened. While driving in a curve, in a worst-case vehicle units might be dragged inside the curve.

The described vehicle behaviour was not evaluated as a hazard. This evaluation is based on a geometrical analysis of the vehicle combination (see [2]).

6 Technical constraints and organizational measures

This section describes constraints that were defined during the concept phase of the ZE modular multi-powertrain. These should be considered when discussing or changing the concept. The organizational measures shall be fulfilled during the use cases since they ensure safety by avoiding potentially hazardous situations.

The following technical constraints were considered, while analysing the hazards and assessing the risks of the item:

ID & FSR	I-FSR-06 Second stabilizing axle present
Description	Each e-trailer has despite the driven axle at least one further non-driven axle, that is not a lift axle. This is a mechanical constraint, that ensures a stabilization of the e-trailer in case of malfunctions of the battery electric powertrain in well-defined scenarios.

ID & FSR	I-FSR-07 Friction brakes capable of exceeding the maximum wheel torques of the EMG
Description	The brakes of the driven e-trailer axle must be designed with the potential to exceed the maximum wheel torques of the EMG in any situation.

ID & FSR	I-FSR-08 Emergency stop switch
Description	The emergency stop switch shall switch the powertrain torque-free.

ID & FSR	I-FSR-09 Electric drives on/off switch
Description	Electric drives on/off switch shall shut off the electric drives of the e-trailer.

ID & FSR	I-FSR-12 Only one e-trailer shall be used
Description	In the considered vehicle combinations only one e-trailer is used to create a multi-powertrain. Multiple e-trailers shall not be jointed to a vehicle combination.

The following organizational measures shall be satisfied during the use cases:

ID & FSR	I-FSR-01 Only instructed/trained and professional driver
Description	<p>All drivers shall meet the following requirements:</p> <ul style="list-style-type: none"> • Professional truck driver or experienced test driver, • Driver safety training, • Instructed to specific safety and operating requirements for the vehicle, • Familiar with vehicle behavior and high-voltage type briefing. <p>This must be confirmed by signature.</p>

ID & FSR	I-FSR-02 Only instructed/trained staff
Description	<p>All staff working at the vehicle shall meet the following requirements:</p> <ul style="list-style-type: none"> • Suitably trained, • Instructed to specific safety and operating requirements for the vehicle, • Familiar with vehicle behavior and high-voltage type briefing. <p>This must be confirmed by signature.</p>

ID & FSR	I-FSR 03 Comply high-voltage safety standards
Description	<p>The vehicle shall meet all the usual safety standards for high-voltage systems (e.g. equipotential, isolation, short-circuit protection, contact protection, labelling)</p>

ID & FSR	I-FSR-04 No operation on test bench
Description	<p>During the use cases, an operation of the e-trailer on a test bench is forbidden. If a test on a test bench is needed, the manufacturer of the e-trailer and the manufacturer of the propulsion system is present.</p>

ID & FSR	I-FSR-05 Use parking brakes and switch off ignition
Description	<p>The parking brake shall be activated and the ignition shall be switched off when leaving the vehicle.</p>

ID & FSR	I-FSR-10 Sleeping in the towing vehicle forbidden
Description	<p>As long as the e-trailer is coupled to the towing vehicle, no person shall sleep in the towing vehicle.</p>

ID & FSR	I-FSR-11 Driving through tunnels longer than 5 minutes forbidden
Description	<p>Driving with the e-trailer through tunnels for longer than 5 minutes is prohibited. Respective long tunnels are not part of the Use Case routes. In case of a necessary deviation from the route respective long tunnels shall be avoided.</p>

7 Description of Safety Goals

The following sections describe the Safety Goals that were defined as result of the HARA [1].

Safety Goals are safety requirements for the e-trailer at vehicle level. They describe requirements from a functional point of view but no technical solutions. Each hazardous event identified in the hazard analyses with an ASIL classification shall be assigned at least one Safety Goal. Similar Safety Goals can be summarized. Each Safety Goal is assigned the ASIL rating of the underlying hazardous event. If similar Safety Goals are combined into a common Safety Goal, this Safety Goal receives the highest ASIL rating of the underlying hazardous event.

The combination of Safety Goals and failure characteristics enables the formulation of validation tests and criteria as well as the verification of these in the system development phase.

7.1 SG-01 As long as the vehicle is accelerating, the e-trailer shall not push its towing vehicle because of MF-1: too high acceleration.

7.1.1 Description of Safety Goal

The malfunction “MF-1: too high acceleration” is considered while the vehicle combination is accelerating. In consequence of the malfunction the e-trailer can push its towing vehicle. This can result in the following hazards that shall be avoided by the safety goal SG-01:

- Frontal collision with other road users,
- Jack knifing of the vehicle combination resulting in a lateral collision with other road users.

7.1.2 Criteria to achieve the Safety Goal

During acceleration, the e-trailer controls its drive torque in such a way that the pushing force in the coupling between the e-trailer and its towing vehicle never is increased by a torque of the e-axle greater than zero. The pushing force in the failure-free state is compared with the pushing force in the faulty state of the e-trailer.

7.1.3 ASIL

ASIL-D

7.1.4 Safe state

Enable coasting: The e-trailer powertrain shall set the drive torque to 0.

7.1.5 Associated functional safety requirements

- FSR-01 Determine vehicle speed
- FSR-02 Determine demand for acceleration
- FSR-03 Determine pitch angle
- FSR-04 Determine drive torque
- FSR-05 Set upper limit for drive torque while acceleration to prevent pushing the towing vehicle

7.2 SG-02 As long as the vehicle is accelerating, the e-trailer shall prevent wheel slip at its driven axle because of MF-1: too high acceleration.

7.2.1 Description of Safety Goal

The malfunction “MF-1: too high acceleration” is considered while the vehicle combination is accelerating. The malfunction can cause wheel slip at the driven axle of the e-trailer. This can result in the following hazards that shall be avoided by the safety goal SG-02:

- Trailer swing of the e-trailer resulting in a lateral collision with other road users.

7.2.2 Criteria to achieve the Safety Goal

During acceleration, the e-trailer controls its drive torque in such a way that no wheel slip occurs at the driven axle of the e-trailer. The wheel slip in the failure-free state is compared with the wheel slip in the faulty state of the e-trailer.

7.2.3 ASIL

ASIL-B

7.2.4 Safe state

Enable coasting: The e-trailer powertrain shall set the drive torque to 0.

7.2.5 Associated functional safety requirements

- FSR-01 Determine vehicle speed
- FSR-02 Determine demand for acceleration
- FSR-03 Determine pitch angle
- FSR-10 Determine wheel speed
- FSR-06 Set upper limit for drive torque while acceleration to prevent wheel slip

7.3 SG-03 As long as the vehicle is at standstill, the e-trailer shall not push its towing vehicle because of MF-3: unintended acceleration.

7.3.1 Description of Safety Goal

The malfunction “MF-3: unintended acceleration” is considered while the vehicle combination is in standstill. In consequence of the malfunction the e-trailer can push its towing vehicle. This can result in the following hazards that shall be avoided by the safety goal SG-03:

- Unintended drive off of the vehicle combination resulting in a frontal collision with other road users.

7.3.2 Criteria to achieve the Safety Goal

During standstill, the e-trailer controls its drive torque in such a way that no unintended drive off can occur. The maintenance of standstill in the failure-free state is compared with the maintenance of standstill in the faulty state of the e-trailer.

7.3.3 ASIL

ASIL-A

7.3.4 Safe state

Powertrain off: The e-trailer powertrain shall power off.

7.3.5 Associated functional safety requirements

- FSR-04 Determine drive torque

7.4 SG-04 As long as the vehicle is driving forward, the e-trailer shall not push its towing vehicle because of MF-3: unintended acceleration.

7.4.1 Description of Safety Goal

The malfunction “MF-3: unintended acceleration” is considered while the vehicle combination is driving forward (without accelerating or decelerating). In consequence of the malfunction the e-trailer can push its towing vehicle. This can result in the following hazards that shall be avoided by the safety goal SG-04:

- Frontal collision with other road users,
- Jack knifing of the vehicle combination resulting in a lateral collision with other road users.

7.4.2 Criteria to achieve the Safety Goal

During driving forward (without acceleration or deceleration), the e-trailer controls its drive torque in such a way that the pushing force in the coupling between the e-trailer and its towing vehicle never is increased by a torque of the e-axle greater than zero. The pushing force in the failure-free state is compared with the pushing force in the faulty state of the e-trailer.

7.4.3 ASIL

ASIL-D

7.4.4 Safe state

Powertrain off: The e-trailer powertrain shall power off.

7.4.5 Associated functional safety requirements

- FSR-04 Determine drive torque

7.5 SG-05 As long as the vehicle is driving forward, the e-trailer shall prevent wheel slip at its driven axle because of MF-3: unintended acceleration.

7.5.1 Description of Safety Goal

The malfunction “MF-3: unintended acceleration” is considered while the vehicle combination is driving forward (without accelerating or decelerating). The malfunction can cause wheel slip at the driven axle of the e-trailer. This can result in the following hazards that shall be avoided by the safety goal SG-05:

- Trailer swing of the e-trailer resulting in a lateral collision with other road users.

7.5.2 Criteria to achieve the Safety Goal

During driving forward (without acceleration or deceleration), the e-trailer controls its drive torque in such a way that no wheel slip occurs at the driven axle of the e-trailer. The wheel slip in the failure-free state is compared with the wheel slip in the faulty state of the e-trailer.

7.5.3 ASIL

ASIL-B

7.5.4 Safe state

Powertrain off: The e-trailer powertrain shall power off.

7.5.5 Associated functional safety requirements

- FSR-04 Determine drive torque

7.6 SG-06 As long as the vehicle is accelerating, the e-trailer shall not increase its pulling force on the towing vehicle because of MF-4: wheel torque in wrong direction.

7.6.1 Description of Safety Goal

The malfunction “MF-4: wheel torque in wrong direction” is considered while the vehicle combination is accelerating. In consequence of the malfunction, the e-trailer can increase the pulling force that it is exerting on the towing vehicle. This can result in the following hazards that shall be avoided by the safety goal SG-06:

- Rear collision with other road users.

7.6.2 Criteria to achieve the Safety Goal

During acceleration, the e-trailer controls its drive torque in such a way that the pulling force in the coupling between the e-trailer and its towing vehicle never is increased by a torque of the e-axle smaller than zero. The pulling force in the failure-free state is compared with the pulling force in the faulty state of the e-trailer.

7.6.3 ASIL

ASIL-A

7.6.4 Safe state

Enable coasting: The e-trailer powertrain shall set the drive torque to 0.

7.6.5 Associated functional safety requirements

- FSR-01 Determine vehicle speed
- FSR-02 Determine demand for acceleration
- FSR-03 Determine pitch angle
- FSR-04 Determine drive torque
- FSR-07 Set lower limit for drive torque while acceleration
- FSR-08 Turn on brake light

7.7 SG-07 As long as the vehicle is accelerating, the e-trailer shall prevent wheel slip at its driven axle because of MF-4: wheel torque in wrong direction.

7.7.1 Description of Safety Goal

The malfunction “MF-4: wheel torque in wrong direction (while acceleration)” is considered while the vehicle combination is accelerating. The malfunction can cause wheel slip at the driven axle of the e-trailer. This can result in the following hazards that shall be avoided by the safety goal SG-07:

- Trailer swing of the e-trailer resulting in a lateral collision with other road users.

7.7.2 Criteria to achieve the Safety Goal

During acceleration, the e-trailer controls its drive torque in such a way that no wheel slip occurs at the driven axle of the e-trailer. The wheel slip in the failure-free state is compared with the wheel slip in the faulty state of the e-trailer.

7.7.3 ASIL

ASIL-C

7.7.4 Safe state

Enable coasting: The e-trailer powertrain shall set the drive torque to 0.

7.7.5 Associated functional safety requirements

- FSR-01 Determine vehicle speed
- FSR-02 Determine demand for acceleration
- FSR-03 Determine pitch angle
- FSR-04 Determine drive torque
- FSR-07 Set lower limit for drive torque while acceleration
- FSR-08 Turn on brake light

7.8 SG-08 As long as the vehicle is decelerating, the e-trailer shall prevent wheel slip at its driven axle because of MF-5: too high deceleration.

7.8.1 Description of Safety Goal

The malfunction “MF-5: too high deceleration” is considered while the vehicle combination is decelerating. The malfunction can cause wheel slip at the driven axle of the e-trailer. This can result in the following hazards that shall be avoided by the safety goal SG-08:

- Trailer swing of the e-trailer resulting in a lateral collision with other road users.

7.8.2 Criteria to achieve the Safety Goal

During deceleration, the e-trailer controls its drive torque in such a way that no wheel slip occurs at the driven axle of the e-trailer. The wheel slip in the failure-free state is compared with the wheel slip in the faulty state of the e-trailer.

7.8.3 ASIL

ASIL-C

7.8.4 Safe state

Enable coasting: The e-trailer powertrain shall set the drive torque to 0.

7.8.5 Associated functional safety requirements

- FSR-01 Determine vehicle speed
- FSR-09 Determine demand for deceleration
- FSR-03 Determine pitch angle
- FSR-10 Determine wheel speed
- FSR-11 Set lower limit for drive torque while deceleration

7.9 SG-09 As long as the vehicle is driving forward, the e-trailer shall not increase its pulling force on the towing vehicle because of MF-6: unintended deceleration.

7.9.1 Description of Safety Goal

The malfunction “MF-6: unintended deceleration” is considered while the vehicle combination is driving forward (without accelerating or decelerating). In consequence of the malfunction, the e-trailer can increase the pulling force that it is exerting on the towing vehicle. This can result in the following hazards that shall be avoided by the safety goal SG-09:

- Rear collision with other road users.

7.9.2 Criteria to achieve the Safety Goal

During driving forward (without acceleration or deceleration), the e-trailer controls its drive torque in such a way that the pulling force in the coupling between the e-trailer and its towing vehicle never is increased by a torque of the e-axle smaller than zero. The pulling force in the failure-free state is compared with the pulling force in the faulty state of the e-trailer.

7.9.3 ASIL

ASIL-A

7.9.4 Safe state

Powertrain off: The e-trailer powertrain shall power off.

7.9.5 Associated functional safety requirements

- FSR-04 Determine drive torque
- FSR-08 Turn on brake light

7.10 SG-10 As long as the vehicle is driving forward, the e-trailer shall prevent wheel slip at its driven axle because of MF-6: unintended deceleration.

7.10.1 Description of Safety Goal

The malfunction “MF-6: unintended deceleration” is considered while the vehicle combination is driving forward (without accelerating or decelerating). The malfunction can cause wheel slip at the driven axle of the e-trailer. This can result in the following hazards that shall be avoided by the safety goal SG-10:

- Trailer swing of the e-trailer resulting in a lateral collision with other road users.

7.10.2 Criteria to achieve the Safety Goal

During driving forward (without acceleration or deceleration), the e-trailer controls its drive torque in such a way that no wheel slip occurs at the driven axle of the e-trailer. The wheel slip in the failure-free state is compared with the wheel slip in the faulty state of the e-trailer.

7.10.3ASIL

ASIL-C

7.10.4Safe state

Powertrain off: The e-trailer powertrain shall power off.

7.10.5Associated functional safety requirements

- FSR-04 Determine drive torque
- FSR-08 Turn on brake light

7.11 SG-11 As long as the vehicle is decelerating, the e-trailer shall not increase its pushing force on the towing vehicle because of MF-7: wheel torque in wrong direction.

7.11.1Description of Safety Goal

The malfunction “MF-7: wheel torque in wrong direction (while deceleration)” is considered while the vehicle combination is decelerating. In consequence of the malfunction, the e-trailer can increase the pushing force that it is exerting on the towing vehicle. This can result in the following hazards that shall be avoided by the safety goal SG-11:

- Frontal collision with other road users,
- Jack knifing of the vehicle combination resulting in a lateral collision with other road users.

7.11.2Criteria to achieve the Safety Goal

During deceleration, the e-trailer controls its drive torque in such a way that the pushing force in the coupling between the e-trailer and its towing vehicle never is increased by a torque of the e-axle greater than zero. The pushing force in the failure-free state is compared with the pushing force in the faulty state of the e-trailer.

7.11.3ASIL

ASIL-D

7.11.4Safe state

Enable coasting: The e-trailer powertrain shall set the drive torque to 0.

7.11.5Associated functional safety requirements

- FSR-01 Determine vehicle speed
- FSR-09 Determine demand for deceleration
- FSR-03 Determine pitch angle
- FSR-04 Determine drive torque
- FSR-12 Set upper limit for drive torque while deceleration

7.12 SG-12 As long as the vehicle is decelerating, the e-trailer shall prevent wheel slip at its driven axle because of MF-7: wheel torque in wrong direction.

7.12.1 Description of Safety Goal

The malfunction “MF-7: wheel torque in wrong direction (while deceleration)” is considered while the vehicle combination is decelerating. The malfunction can cause wheel slip at the driven axle of the e-trailer. This can result in the following hazards that shall be avoided by the safety goal SG-12:

- Trailer swing of the e-trailer resulting in a lateral collision with other road users.

7.12.2 Criteria to achieve the Safety Goal

During deceleration, the e-trailer controls its drive torque in such a way that no wheel slip occurs at the driven axle of the e-trailer. The wheel slip in the failure-free state is compared with the wheel slip in the faulty state of the e-trailer.

7.12.3 ASIL

ASIL-C

7.12.4 Safe state

Enable coasting: The e-trailer powertrain shall set the drive torque to 0.

7.12.5 Associated functional safety requirements

- FSR-01 Determine vehicle speed
- FSR-09 Determine demand for deceleration
- FSR-03 Determine pitch angle
- FSR-04 Determine drive torque
- FSR-12 Set upper limit for drive torque while deceleration

7.13 SG-13 Prevent harm by a thermal runaway of the battery.

7.13.1 Description of Safety Goal

The malfunction “MF-8: thermal runaway of battery without warning of driver” is considered in every operational situation of the vehicle combination as well as in situations where the vehicle combinations is parked (ignition switched off). The malfunction can harm the driver, especially when he or she is sleeping in the cabin of the towing vehicle, and other road users.

7.13.2 Criteria to achieve the Safety Goal

The e-trailer shall always warn the driver of the vehicle combination in an appropriate way if a thermal runaway of the battery occurs.

7.13.3 ASIL

ASIL-D

7.13.4 Safe state

none

7.13.5 Associated functional safety requirements

- FSR-13 Determine battery status
- FSR-14 Warn person in driver cabin

8 Safe States

The following tables describe the safe states that are allocated to the safety goals in chapter 7. The safe states enable the safe operation of the e-trailer.

Safe State	Enable coasting
Description	The e-trailer powertrain shall set the drive torque to 0.
Additional explanation	The safe state shall be realized in a way that the electric motor is controlled in a way that does not result in a wheel torque.

Safe State	Powertrain off
Description	The e-trailer powertrain shall power off.
Additional explanation	The safe state shall be realized in a way that the electric motor of the driven axle is not powered by the high voltage system.

9 Functional safety requirements

The following tables describe the functional safety requirements (FSR) that are derived from the safety goals. The FSR result from the e-trailer functions presents in chapter 4 and the malfunctions that can cause a hazard according to the hazard analysis of the HARA [1] and have led to the definition of the corresponding safety goals. The FSR consider the preconditions (see chapter 4) that must be fulfilled to guarantee the proper operation of the e-trailer functions.

ID & FSR	FSR-01 Determine vehicle speed
Description	The e-trailer powertrain shall be able to determine the current vehicle speed.
ASIL	D
Additional explanation	technical requirement, mandatory

ID & FSR	FSR-02 Determine demand for acceleration
Description	The e-trailer powertrain shall be able to determine that the vehicle combination demands an acceleration.
ASIL	D
Additional explanation	technical requirement, mandatory

ID & FSR	FSR-03 Determine pitch angle
Description	The e-trailer powertrain shall be able to determine the pitch angle of the e-trailer.
ASIL	D
Additional explanation	technical requirement, mandatory

ID & FSR	FSR-04 Determine drive torque
Description	The e-trailer powertrain shall be able to determine the current drive torque.
ASIL	D
Additional explanation	technical requirement, mandatory

ID & FSR	FSR-05 Set upper limit for drive torque while acceleration to prevent pushing the towing vehicle
Description	As long as the maximum possible drive torque would result in pushing the towing vehicle, the e-trailer powertrain shall limit the maximum possible drive torque to a lower value.
ASIL	D
Additional explanation	technical requirement, mandatory

ID & FSR	FSR-06 Set upper limit for drive torque while acceleration to prevent wheel slip
Description	As long as the maximum possible drive torque would result in wheel slip, the e-trailer powertrain shall limit the maximum possible drive torque to a lower value.
ASIL	B
Additional explanation	technical requirement, mandatory

ID & FSR	FSR-07 Set lower limit for drive torque while acceleration
Description	As long as the vehicle demands an acceleration, the e-trailer powertrain shall limit the possible drive torque > 0 Nm.
ASIL	B
Additional explanation	technical requirement, mandatory

ID & FSR	FSR-08 Turn on brake light
Description	As long as the drive torque is < 0 Nm, the system should turn on the brake lights.
ASIL	QM
Additional explanation	technical requirement, optional

ID & FSR	FSR-09 Determine demand for deceleration
Description	The e-trailer powertrain shall be able to determine that the vehicle combination demands a deceleration.
ASIL	D
Additional explanation	technical requirement, mandatory

ID & FSR	FSR-10 Determine wheel speed
Description	The e-trailer powertrain shall be able to determine the current wheel speed.
ASIL	B
Additional explanation	technical requirement, mandatory

ID & FSR	FSR-11 Set lower limit for drive torque while deceleration
Description	As long as the minimum possible drive torque would result in wheel slip, the e-trailer powertrain shall limit the minimum possible drive torque to a higher value.
ASIL	B
Additional explanation	technical requirement, mandatory

ID & FSR	FSR-12 Set upper limit for drive torque while deceleration
Description	As long as the vehicle demands a deceleration, the e-trailer powertrain shall limit the possible drive torque < 0 Nm.
ASIL	D
Additional explanation	technical requirement, mandatory

ID & FSR	FSR-13 Determine battery status
Description	The e-trailer powertrain shall be able to determine a battery status.
ASIL	D
Additional explanation	technical requirement, mandatory

ID & FSR	FSR-14 Warn person in driver cabin
Description	As soon as no correct battery status could be determined, the e-trailer powertrain shall warn the person in the driver cabin.
ASIL	D
Additional explanation	technical requirement, mandatory

10 Results and Discussion

10.1 Results

The main results of the work presented in this deliverable are the safety goals, safe states and functional safety requirements in chapter 7, chapter 8 and chapter 9, respectively. These top-level requirements are applicable to both types of e-trailers – the e-semitrailer and the e-dolly – and to all vehicle combinations the e-trailer is used with. Beside the technical measures that must be derived from the functional safety requirements, also technical constrains are defined (see chapter 6) that effect the design of the e-trailer and put requirements on the equipment of the vehicle combinations that are used in the demonstration phase of the ZEFES project. Additionally, organizational measures are defined, which are e.g., directly related to the required skills of the drivers or the distribution of payload.

To achieve functional safety, the requirements and processes provided by the ISO 26262 series of standards must be taken into account in the development of the systems that are part of the modular multi-powertrain concept.

Furthermore, the ECE Regulations aim to create a uniform system of regulations relating to the design of vehicles and vehicle components. Among others, there are regulations regarding electromagnetic compatibility of components³, with regard to braking⁴, for vehicles with an electric powertrain⁵ and for cyber security⁶. These regulations also include specifications for control units and

³ With regard to electromagnetic compatibility, the vehicle manufacturer can, for example, use the following norms and standards:

- UN/ECE R10, UN Regulation No. 10, Uniform provisions concerning the approval of vehicles with regard to electromagnetic compatibility
- ISO 16750 Road vehicles – Environment conditions and testing for electrical and electronic equipment
- ISO 11452 Road vehicles – Component testing, methods for the determination of electrical interferences caused by short wave electromagnetic energy emissions
- CISPR 25 Radio disturbance characteristics for the protection of receivers used on board vehicles, boats, and on devices – Limits and methods of measurement

⁴ UN/ECE R13, UN Regulation No. 13, Uniform provisions concerning the approval of vehicles of categories M, N and O with regard to braking

⁵ With regard to the electric powertrain of a vehicle, the vehicle manufacturer can, for example, use the following norms and standards:

- UN/ECE R100, UN Regulation No. 100, Uniform provisions concerning the approval of vehicles with regard to specific requirements for the electric power train
- ISO 6469, Electrically propelled road vehicles – Safety specifications, parts 2, 3 and 4

⁶ UN/ECE R155, UN Regulation No. 155, Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

components with regard to aspects of e.g., electromagnetic compatibility and resistance to mechanical and chemical influences from the environment.

10.2 Conclusion and Recommendation

The functional safety of the modular multi-powertrain concept was investigated in contribution with all partners involved in the realization of that kind of vehicle combinations – the trailer manufacturers VET and KAE, the manufacturers of the battery-electric powertrain for the e-trailers ZF and FHG, and the vehicle manufacturers VOL and SCA. The safety goals and functional safety requirements must be considered in the further development and application of the e-trailers in the ZEFES use cases. Thus, they are input to the tasks 5.3 and 5.4 that deal with the realization of the battery-electric prime movers and trailers and to task 5.5 where the battery-electric vehicles and vehicle combinations are commissioned and tested.

Furthermore, the organizational measures are input to work package 7 that orchestrates the demonstration of the different use cases.

The functional safety concept will be further verified and commissioned in task 5.4 “Adaption and implementation of powertrain components for next generation e-trailers” and task 5.5 “Realization and commissioning of vehicle combinations according to use cases”.

Disclaimer :

The functional safety concept according to this document is the result of a generic assessment for e-trailers and e-dollies. The result of the functional safety assessment for the dedicated products used in ZEFES (KAE Trailer; ZF e-trailer system; BEVs of SCA and VOL) as elaborated e.g. for the e-trailer system/vehicle within the product development process by ZF, is not identical to the results as presented in this document.

Nevertheless, a first benchmark of the safety goals and the Functional Safety Requirements show the feasibility to map the structure and contents sufficiently. It will be possible to prove the safety concept according to this document with reference to the validated safety concept by the partners providing the vehicles and the systems.

Within the proceeding development, the partners will take care, that the goals and requirements declared in this document find a representation in further development of the vehicles and systems.

10.3 Contribution to project (linked) Objectives

The work done in task 5.2 and documented in this deliverable contributes reaching several objectives that have been defined in the ZEFES description of action. The results of the investigation of functional safety of the modular multi-powertrain concept are input to task 5.3 and task 5.4 that realize the next generation battery-electric trucks, tractors, and trailers. By supporting the further development and the safe application of the e-trailer the results contribute to objective 1, in particular to sub-objective 1.2 “develop a vehicle concept with enhances energy storage and e-axles”.

The recommendations for the application of the vehicle combinations in the use cases also contributes to objective 4 “demonstrate missions on cross-border, TEN-T corridors, [...]”.

10.4 Contribution to major project exploitable result

The work done in task 5.2 and the documentation in this deliverable indirectly contributes to the project exploitable results. The investigation of the functional safety of the modular multi-powertrain enables a targeted development and adaptation of vehicle units that can be combined to a distributed powertrain and thus, serve the logistics missions demonstrated in the use cases.

11 Risks and interconnections

11.1 Risks/problems encountered

Risk No.	What is the risk	Probability of risk occurrence ¹	Effect of risk ¹	Solutions to overcome the risk
WP5.2	Certain safety goals and functional safety requirements cannot or not to the necessary extent be fulfilled by the realization of the vehicle units.	2	2	Requirements concerned must be compensated by organizational measures that can be applied in the use cases.

¹) Probability risk will occur: 1 = high, 2 = medium, 3 = Low

11.2 Interconnections with other deliverables

This deliverable is connected to the deliverables D5.4 “Next generation battery-electric trailers” and D5.6 “Realization and commissioning of all BEV demonstrators”, since the top-level requirements for functional safety shall be considered in the developments presented in these documents.

12 References

- [1] H. Wittig und J. Rehor, „ZEFES – WP5 Task 5.1: Hazard Analysis and Risk Assessment and Derivation of Functional Safety Requirements,“ Dresden, 2024.
- [2] H. Wittig und J. Rehor, „ZEFES – WP5 Task 5.1: Supporting Document to e-trailer Hazard Analysis and Risk Assessment,“ Dresden, 2024.
- [3] H. Wittig und J. Rehor, „Item Definition for ZE modular multi-powertrain concepts (V2.2),“ Dresden, 2024.
- [4] H. Wittig und R. Schmid, „ZEFES Deliverable D1.1: Technical requirements - Needs and requirements for BEV and FCEV combinations,“ Brussels, 2023.

13 Acknowledgement

The author(s) would like to thank the partners in the project for their valuable comments on previous drafts and for performing the review.

Project partners:

#	Partner short name	Partner Full Name
1	VUB	VRIJE UNIVERSITEIT BRUSSEL
2	FRD	FORD OTOMOTIV SANAYI ANONIM SIRKETI
4	KAE	KASSBOHRER FAHRZEUGWERKE GMBH
5	REN	RENAULT TRUCKS SAS
6	SCA	SCANIA CV AB
7	VET	VAN ECK TRAILERS BV
8	VOL	VOLVO TECHNOLOGY AB
9	ABB	ABB E-MOBILITY BV
9.1	ABP	ABB E-MOBILITY SPOLKA Z OGRANICZONAODPOWIEDZIALNOSCIA
10	AVL	AVL LIST GMBH
11	CM	SOCIEDAD ESPANOLA DE CARBUROS METALICOS SA
11.1	APG	AIR PRODUCTS GMBH
12	HEPL	HITACHI ENERGY POLAND SPOLKA Z OGRANICZONA ODPOWIEDZIALNOSCIA
13	MIC	MANUFACTURE FRANCAISE DES PNEUMATIQUES MICHELIN
14	POW	PLASTIC OMNIUM NEW ENERGIES WELS GMBH
15	RIC-CZ	RICARDO PRAGUE S.R.O.
15.1	RIC-DE	RICARDO GMBH
16	UNR	UNIRESEARCH BV
17	ZF	ZF CV SYSTEMS HANNOVER GMBH
18	ALI	ALLIANCE FOR LOGISTICS INNOVATION THROUGH COLLABORATION IN EUROPE
19	DPD	DPD (NEDERLAND) B.V.
20	COL	ETABLISSEMENTEN FRANZ COLRUYT NV
21	GRU	GRUBER LOGISTICS S.P.A.
22	GBW	GEBRUEDER WEISS GESELLSCHAFT M.B.H.
23	PG	PROCTER & GAMBLE SERVICES COMPANY NV
23.1	PGP	PROCTER AND GAMBLE POLSKA SPOLKA Z OGRANICZONA ODPOWIEDZIALNOSCIA
23.2	PGA	PROCTER & GAMBLE AMIENS
24	PRI	PRIMAFRIO CORPORACION, S.A.
25	PTV	PTV PLANUNG TRANSPORT VERKEHR GmbH
26	Fraunhofer	FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV

27	HAN	STICHTING HOGESCHOOL VAN ARNHEM ENNIJMEGEN HAN
28	IDI	IDIADA AUTOMOTIVE TECHNOLOGY SA
29	TNO	NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO
30	UIC	UNION INTERNATIONALE DES CHEMINS DE FER
31	CFL	CFL MULTIMODAL S.A.
32	GSS	Grupo Logistico Sese
33	HIT	Hitachi ABB Power Grids Ltd.
34	IRU	UNION INTERNATIONALE DES TRANSPORTS ROUTIERS (IRU)
35	RIC-UK	RICARDO CONSULTING ENGINEERS LIMITED

Disclaimer/ Acknowledgment



Copyright ©, all rights reserved. This document or any part thereof may not be made public or disclosed, copied or otherwise reproduced or used in any form or by any means, without prior permission in writing from the ZEFES Consortium. Neither the ZEFES Consortium nor any of its members, their officers, employees or agents shall be liable or responsible, in negligence or otherwise, for any loss, damage or expense whatever sustained by any person as a result of the use, in any manner or form, of any knowledge, information or data contained in this document, or due to any inaccuracy, omission or error therein contained.

All Intellectual Property Rights, know-how and information provided by and/or arising from this document, such as designs, documentation, as well as preparatory material in that regard, is and shall remain the exclusive property of the ZEFES Consortium and any of its members or its licensors. Nothing contained in this document shall give, or shall be construed as giving, any right, title, ownership, interest, license or any other right in or to any IP, know-how and information.

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.