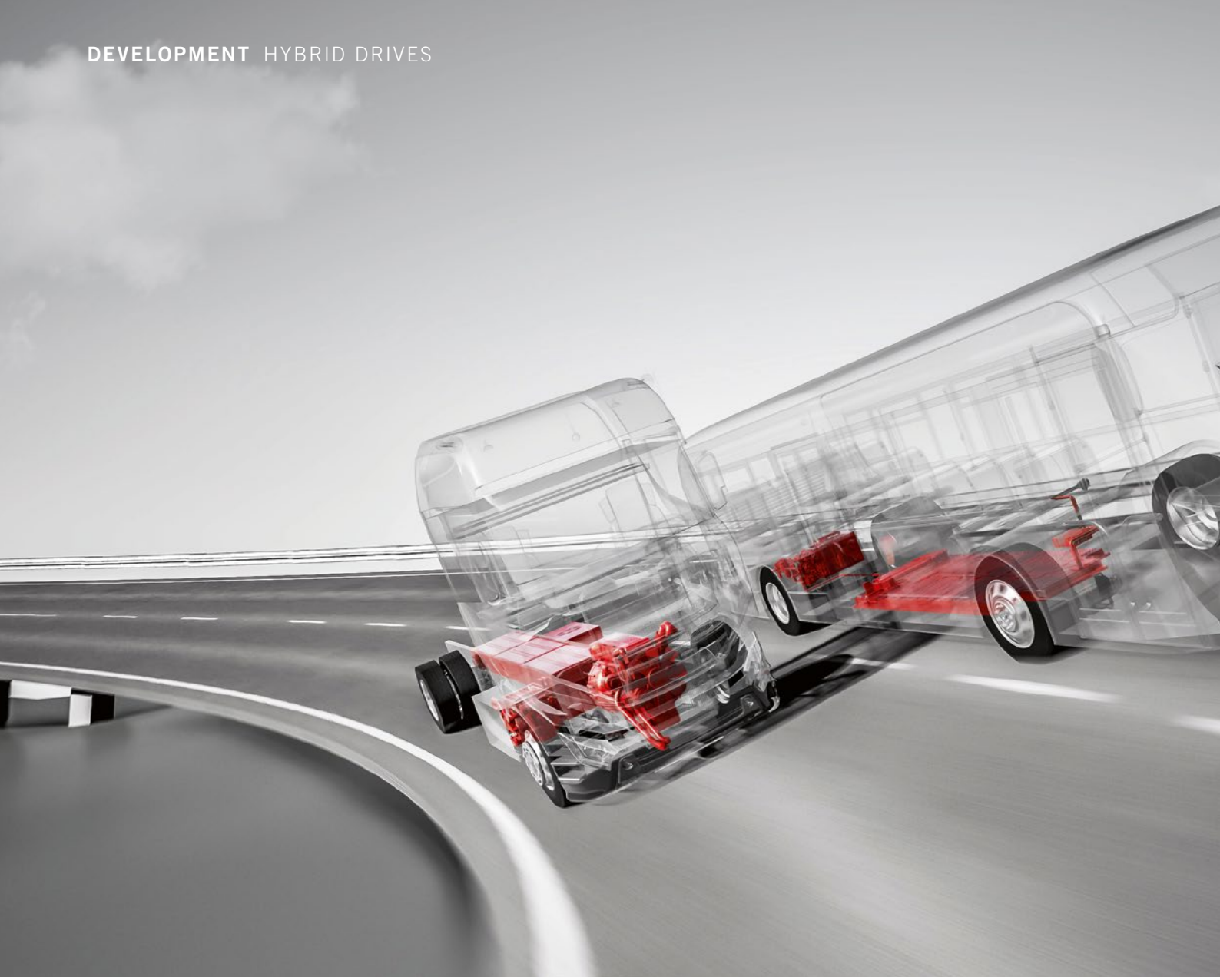


AUTHORS

Anunay Krishnamurthy, M. Sc.
is Project Engineer in the Department for Functional Safety (BEF-A) at FEV Europe GmbH in Aachen (Germany).

Dr.-Ing. Bastian Holderbaum
is Manager of the Department for Functional Safety (BEF-A) at FEV Europe GmbH in Aachen (Germany).

INTRODUCTION

With the objective to improve performance, comfort and emissions below the Euro-VI threshold values, hybrid powertrains will become a major choice not only for passenger cars, but also for commercial vehicles (buses, medium and heavy duty trucks). The development of hybrid powertrains provides challenges to functional safety due to additional Electric and Electronic (E/E) components. The additional E/E components lead to more potential malfunctions as compared to a conventional powertrain. The functional safety of hybrid powertrain functions for commercial vehicles can be achieved by developing the powertrain in accordance to ISO DIS 26262:2016(E), which is the second edition of ISO 26262 in its preliminary draft state. The second edition describes the safety lifecycle of an item, including the hazard analysis and risk assessment, which results in the safety goals, safe states and Automotive Safety Integrity Level (ASIL) ratings for the item. This information is used as an input to systematically derive the functional safety concept. This is described, in detail, in this paper with the example of a hybrid powertrain for a heavy duty vehicle.

PROJECT INFORMATION

The project discussed here is called Ecochamps (European Competitiveness in Commercial Hybrid and Automotive Powertrains). This is a single coordinated

Functional Safety Concept of a Hybrid Powertrain for a Heavy Duty Vehicle

The trend toward electrified powertrains in commercial vehicles places increased demands on functional safety. The development service provider FEV shows how a standard-compliant safety concept can be developed for a hybrid drive train in commercial vehicles.

project that is conducted by 26 members of the European automotive industry. One of the objectives of the project is the development of a hybrid powertrain for a heavy duty vehicle. The hybrid powertrain consists of an Internal Combustion Engine (ICE), a clutch, and a hybrid transmission including an electric motor. The e-motor is powered by a high voltage system. The power input to the high voltage system is provided by a lithium ion battery. The powertrain interacts with the Advanced Driver Assistance System (ADAS), the brake system and the display unit. The physical architecture of the powertrain is shown in **FIGURE 1**.

The powertrain performs several functions. They include accelerator pedal function, cruise control, engine start/stop, interaction with Anti-lock Braking System (ABS) and Vehicle Stability Control (VSC), and High Voltage (HV) battery functions like HV battery charging or HV battery State Of Charge (SoC) and State of Health (SoH) management.

This overview is not complete. It is only to provide a high level of understanding of the system for which functional safety was investigated. The preliminary powertrain architecture, the powertrain functions, their description and the interactions between the functions together form the item definition.

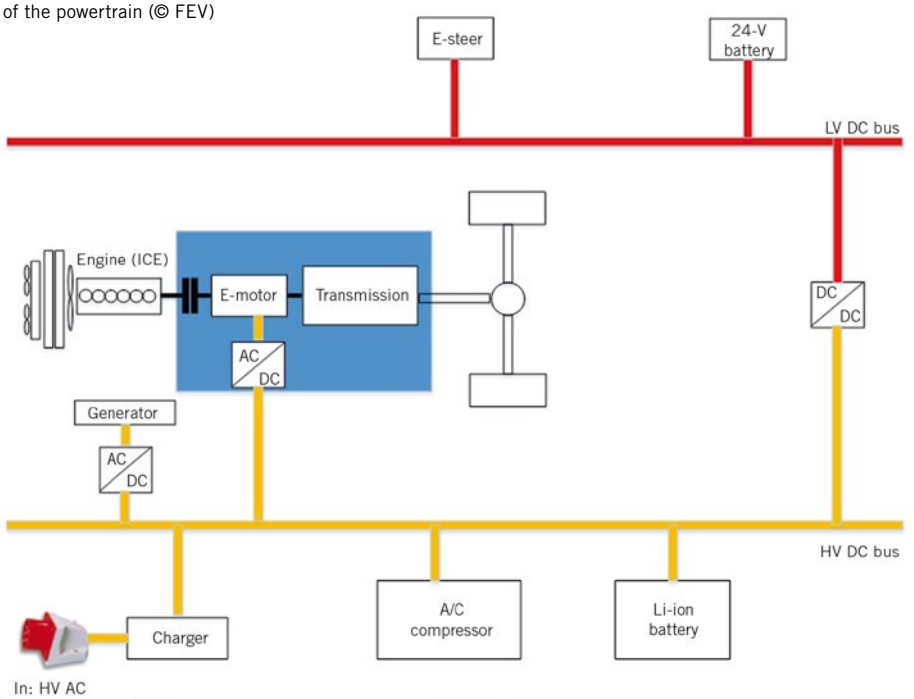
FUNCTIONAL SAFETY CONCEPT

According to [1], a Functional Safety Concept (FSC) consists of the Functional Safety Requirements (FSRs) and the allocation of these requirements to elements in the preliminary architecture. The ISO DIS 26262:2016(E) standard describes what information shall be included in the FSC. However, it does not define a specific process for creating the FSC. Several approaches have been proposed. Beckers, Côté, Frese, Hatebur and Heisel define a process for creating the FSC using Unified Modified Language (UML) and Goal Structuring Notation (GSN) [2]. Oertel, Schulze and Peikenkamp define a process for developing a common FSC that can be used for various system architectures [3].

This paper presents a five-step method to systematically generate the FSC for a hybrid powertrain along with examples. In order to derive the functional safety

requirements, the Safety Goals (SG), safe states of the SGs and their ASILs must be available. These criteria are identified by a systematic process called Hazard Analysis and Risk Assessment (HARA). This process involves identifying malfunctions of powertrain functions, determining hazards caused by malfunctions, evaluating the severity and controllability of these hazards as well as the exposure of the respective operating scenario. Two exemplary SGs, together with their safe states and ASILs, are shown in **TABLE 1**.

FIGURE 1 Physical architecture of the powertrain (© FEV)



STEP 1: CREATING A FAULT TREE ANALYSIS

The first step is to create a Fault Tree Analysis (FTA) diagram for each SG that is rated ASIL A and above. No fault trees are drawn for safety goals rated Quality Management (QM). ISO DIS 26262:2016(E) highly recommends deductive analysis (FTA) for ASIL C and D. However, it is a good practice to create FTAs for all safety goals (ASIL A, B, C, and D). The FTA is a powerful tool not only for defining requirements, but also for defining test cases. A small section of an FTA for safety goal 006 (SG006 – Preventing thermal runaway of the battery) is shown in **FIGURE 2**.

STEP 2: CREATING FUNCTIONAL SAFETY REQUIREMENTS

For each bottom level event in the FTA, at least two types of FSRs are derived:

- One set of FSR is derived to detect/prevent the failure mode of the function that leads to an SG violation. This can include safety mechanisms to prevent the violation of safety goals or functional limitations or establishing arbitration between functionalities etc.
- One set of FSR is derived to enter/exit a safe state if the failure mode is detected. The safe state is obtained from the Hara.

The driver warnings and functional degradation can be specified as a part of this requirements group.

STEP 3: ADDITIONAL PROPERTIES

Each FSR is specified with properties shown in **TABLE 2**.

A selection of FSRs (along with their properties) is shown in **TABLE 3**. FSR082 and FSR083 are derived from intermediate gate E96 in the FTA, **FIGURE 2**. FSR082 represents the FSR for detecting overcharging of the HV battery and FSR083 represents the safe state once an error is detected. FSR090, FSR091 and FSR092 are derived from intermediate gate E112 in the FTA. FSR090 represents the FSR for detecting the temperature of the HV battery cells. FSR091 and FSR092 represent the safe states if the temperature is too high or too low.

STEP 4: CREATE TRACEABILITY MATRIX

A traceability matrix is created to show the relationship between the safety goals and safety requirements. The traceability matrix provides a summary of information which makes it easy to identify if there are any SGs with no FSR or vice versa. This is very helpful to perform reviews and assessments. An extract of the traceability matrix is shown in **TABLE 4**.

STEP 5: VERIFICATION OF FSC

Verification of the FSC should be performed during the concept phase according to [4]. If the verification of the FSC is performed by a review, it can be supported by checklists. An example of a checklist is shown in **TABLE 5**.

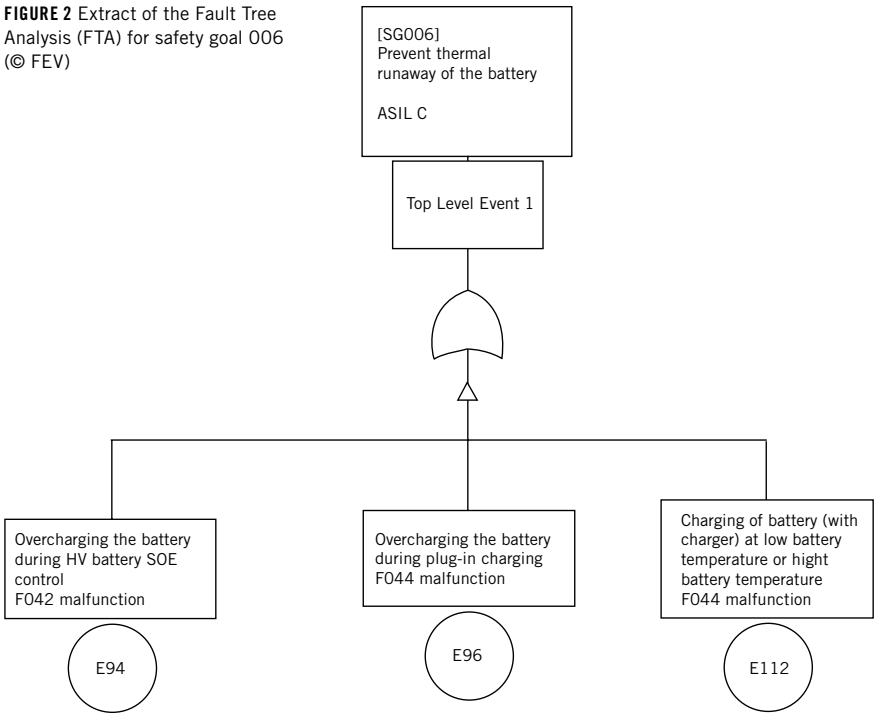
INFORMAL DESCRIPTION

Informal descriptions are used to support the understanding for a safety mechanism, especially in case that several functional safety requirements are defined to reach the same safety goal. For two exemplary safety goals, the respective informal descriptions are as follows:

Safety goal ID	Safety goal description	Safe state	ASIL
SG006	Prevent thermal runaway of the battery	Disconnected battery from HV vehicle electrical system	C
SG013	Electric drive torque only to be generated when a driver request is given	Disabled E-motor	A

TABLE 1 Description of two exemplary safety goals (© FEV)

FIGURE 2 Extract of the Fault Tree Analysis (FTA) for safety goal 006 (© FEV)



Name	This property indicates the name of a functional safety requirement. This is required for good organization of the requirements. Some examples of requirement name are: – FSR_xxyy – This represents the name of the functional safety requirement for detection/prevention of a failure mode of a function. xxyy represents the function/component for which the requirement is written. – FSR_safestate_xxyy – This represents the name of the safe state of the FSR. – FSR_warning_xxyy – This represents the name of the requirements for driver warning. – FSR_decomposition_xxyy – This represents the name of requirements if ASIL decomposition is performed.
ASIL	Each FSR has an ASIL. The ASIL is derived from the higher level safety goal. If ASIL decomposition is used to lower the ASIL of the requirement, the clauses mentioned in ISO DIS 26262:2016(E) Chapter 10 Clause 11 must be fulfilled.
Related safety goal	This is the higher level safety goal to which the FSR is connected.
Allocation	This property indicates the element in the preliminary architecture to which the FSR is allocated.
Fault Tolerance Time Interval (FTTI)	According to [1], FTTI is defined as the time span in which a fault or faults can be present in a system before a hazardous event occurs. FTTI can be determined by performing vehicle tests, introducing faults in the system and determining the maximum time before which a hazardous event (violation of a safety goal) occurs. The Hara is a good source to identify scenarios where vehicle tests should be performed. If an FSA is assigned to several safety objectives, the smallest FTTI value from these is used for the FSA.

TABLE 2 Properties of functional safety requirements (© FEV)

ID	Name	Description	ASIL	Related safety goals	Allocations	FTTI
FSR082	FSR_Overcharging of battery	The control unit should detect overcharging of the HV battery.	C	SG006 (ASIL C)	HV battery controller	To be defined by vehicle testing (or simulation)
FSR083	FSR_safe-state_Overcharging of battery	If overcharging of the HV battery is detected, the HV battery cells should be disconnected from the power source.	C	SG006 (ASIL C)	HV battery controller	To be defined by vehicle testing (or simulation)
FSR090	FSR_Charging/discharging at low battery temperature or high battery temperature	The control unit should monitor temperature of the individual cells of the HV battery.	C	SG006 (ASIL C)	HV battery controller	To be defined by vehicle testing (or simulation)
FSR091	FSR_safestate_Charging/discharging of battery at high battery temperature	If the control unit detects a cell temperature exceeding the HV battery specification (too high), the HV battery cells should be disconnected from the power source.	C	SG006 (ASIL C)	HV battery controller	To be defined by vehicle testing (or simulation)
FSR092	FSR_safestate_Charging/discharging of battery at low battery temperature	If the control unit detects a cell temperature falling below the HV battery specification (too low), the HV battery cells should be disconnected from the power source.	C	SG006 (ASIL C)	HV battery controller	To be defined by vehicle testing (or simulation)

TABLE 3 Exemplary functional safety requirements (© FEV)

Violation of SG006 is caused by overcharging the HV battery or charging the HV battery at too low or too high battery temperatures. Overcharging of the HV battery cells should be prevented by determining the state of charge of the battery cells and stopping charging when an upper threshold is reached. In addition, charging of the battery cells should be prevented if the temperature of the cells is too high or too low.

Violation of SG013 is caused by unintended torque generated due to a fault in the powertrain during e-drive or during plugin charging. Unintended torque during e-drive can be detected by comparing the driver's requested torque with the actual torque. Unintended torque during plugin charging can be prevented by ensuring that there is no torque request to the e-motor (or ICE) during charging. In addition, it may also be required to ensure that the parking lock is engaged.

Traceability matrix Safety goals to functional safety requirements	Safety goals	
	[SG006] SG_battery _thermal_ runaway	[SG013] SG_e-drive _unintended_ torque
Functional safety requirements		
[FSR082] FSR_overcharging of battery	X	–
[FSR083] FSR_safestate_overcharging of battery	X	–
[FSR084] FSR_erroneous e-motor torque request during gear shift	–	X
[FSR085] FSR_safestate erroneous e-motor torque request during gear shift	–	X
[FSR086] FSR_erroneous e-motor torque request during vehicle mode transitions	–	X
[FSR087] FSR_safestate erroneous e-motor torque request during vehicle mode transitions	–	X
[FSR088] FSR_unintended torque request during plug-in charging	–	X
[FSR089] FSR_unintended e-motor torque request during plug-in charging	–	X
[FSR090] FSR_charging/discharging of battery at low battery temperature or high battery temperature	X	–
[FSR091] FSR_safestate charging/discharging of battery at high battery temperature	X	–
[FSR092] FSR_safestate charging/discharging of battery at low battery temperature	X	–

TABLE 4 Traceability matrix for two exemplary safety goals and their assigned functional safety requirements (© FEV)

SUMMARY

The five-step process is an efficient process for creating the functional safety concept. With this process, a traceability between the FTA, FSRs and the elements of the preliminary architecture is achieved. This provides a very good argument for the completion of the FSC. This process can be used to create FSC for all E/E systems in the vehicle.

FUTURE WORK

The FSC is a the basis for creating the technical safety requirements. The tech-

Attribute ID	ISO-26262 reference		Attribute	Rationale	Attribute complied with?
	Part-#	Clause-#			
FSK_FCL_13	3	8.4.3.1 a)	Inheritance of ASIL from source requirement (safety goal)	Do all safety requirements inherit the ASIL from the associated safety goal?	Yes
FSK_FCL_14	3	8.4.3.1 b)	Allocation of highest ASIL to the same architectural element	In case of several safety requirements being allocated to an architectural element, was the highest ASIL allocated to the specific element?	Yes
FSK_FCL_15	3	8.4.3.1 c)	Safety requirements definition for systems and interfaces	If the item consists of more than one system, are safety requirements defined for all systems, including interfaces?	Yes
FSK_FCL_16	3	8.4.3.1 d)	Application of ASIL decomposition	If ASIL decomposition was applied, was it conducted in accordance with ISO 262626 part 9 clause 5?	N/A
FSK_FCL_17	3	8.4.3.2 a)	Allocation to elements of other technologies	If the safety concept relies on elements of other technologies, are the safety requirements allocated to the elements of other technologies?	N/A
FSK_FCL_18	3	8.4.3.2 b)	Interfaces to elements of other technologies	If the safety concept relies on elements of other technologies, are safety requirements describing the interfaces to the elements of other technologies?	N/A

TABLE 5 Checklist for verification of functional safety concept (© FEV)

nical safety requirements provide technical solutions for the FSRs. The technical safety requirements are supported by inductive and deductive methods. This is used for creating the technical safety concept and the powertrain system design.

Based on the technical safety requirements, the hardware and software safety requirements are created and verified according to [4]. The next step is to verify (by testing) technical safety requirements according to [4]. Once verification is complete, validation of the functional safety concept should be performed according to [4]. For each FSR, an acceptance criteria for validation shall be specified. The specified criteria shall be validated on the vehicle. Validation is considered outside the scope of the FSC and is considered as a part of testing.

REFERENCES

[1] International Organization for Standardization (ISO): Road Vehicles – Functional Safety. ISO/DIS 26262:2016(E)

[2] Beckers, K.; Côté, I.; Frese, T.; Hatebur, D.; Heisel, M.: Systematic Derivation of Functional Safety Requirements for Automotive Systems. In: Bondavalli, A.; Di Giandomenico, F. (eds.): Computer Safety, Reliability, and Security – Proceedings of Safevomp. LNCS 8666, Springer, 2014, pp. 65–80

[3] Oertel, M.; Schulze, M.; Peikenkamp, T.: Reu-sing a Functional Safety Concept in Variable System Architectures. 7th International Workshop on Model-Based Architecting and Construction of Embedded Systems, Valencia, 2014

[4] International Organization for Standardization (ISO): Road Vehicles – Functional Safety. ISO 26262, 2011

THANKS

The authors would like to thank Stefan Wedowski, David Seibert, and Thomas Nowak for their contributions to Project Management, Hazard Analysis and Risk Assessment as well as Review of the Functional Safety Concept respectively.

This project has received funding from the European Union's Horizon2020 research and innovation program under Grant Agreement no. 653468.