applied sciences

MDPI

Article

A Novel Hazard Analysis and Risk Assessment Approach for Road Vehicle Functional Safety through Integrating STPA with FMEA

Lei Chen [1,2], Jian Jiao [1] and Tingdi Zhao [1,*]

[1] School of Reliability and Systems Engineering, Beihang University, Beijing 100191, China; zheermao1005@163.com (L.C.); jiaojian@buaa.edu.cn (J.J.)

[2] School of Safety Engineering, Shenyang Aerospace University, Shenyang 110136, China

* Correspondence: ztd@buaa.edu.cn

Received: 20 September 2020; Accepted: 18 October 2020; Published: 22 October 2020

Abstract: ISO26262: 2018 is an international functional safety standard for electrical and/or electronic (E/E) systems within road vehicles. It provides appropriate safety requirements for road vehicles to avoid unreasonable residual risk according to automotive safety integrity levels (ASILs) derived from hazard analysis and risk assessment (HARA) required in the ISO26262 concept phase. Systems theoretic process analysis (STPA) seems to be designed specifically to deal with hazard analysis of modern complex systems, but it does not include risk evaluation required by most safety related international standards. So we integrated STPA into Failure Mode and Effect Analysis (FMEA) template to form a new method called system theoretic process analysis based on an FMEA template, STPAFT for shot, which could not only meet all the requirements of the concept phase in ISO26262, but also make full use of the advantages of the two methods. Through the focus of FMEA on low-level components, STPAFT can obtain more detailed causal factors (CFs), which is very helpful for derivation of safety goals (SGs) and the functional safety requirements (FSRs) in the concept phase of ISO26262. The application of STPAFT is described by the case study of fuel level estimation and display system (FLEDS) to show how the concept phase of ISO26262 could be supported by STPAFT.

Keywords: hazard analysis and risk assessment; STPA; FMEA; ISO26262; ASIL; safety goal; functional safety requirement

1. Introduction

Nowadays, the intensive use of software and the increase in functional requirements have significantly increased the complexity of road vehicle systems. Therefore, developing safety requirements for road vehicle electrical and/or electronic (E/E) systems is challenging. First, in the early conceptual phase, engineers need to consider not only safety-related goals, but also other system-level goals, such as performance and information security, which determines whether stakeholders' will be satisfied with the new product [1,2]. Second, traditional safety analysis methods focusing on component failures are difficult to be used alone in safety analysis of software-intensive modern complex systems [3–5]. ISO26262, as a domain-specific standard for functional safety of road vehicles, was born to deal with these challenges [6]. It has developed various procedures and processes to ensure functional safety, but does not restrict type of methods for hazard and safety analysis. Systems theoretic process analysis (STPA) [3–5] is a relatively new hazard analysis

technology for software intensive complex systems, which views safety as a control problem. In STPA, accidents result from inadequate control of component failures, dysfunctional interaction of components, external disturbance, etc. Since the implementation of ISO26262, STPA has attracted growing attention in the automotive industry [7–14].

Although STPA does have advantages in hazards analysis, which traditional methods do not have, the key obstacle for STPA to satisfy the requirements of the hazard analysis and risk assessment (HARA) process of ISO26262 is that STPA does not directly consider hazards qualification as some traditional hazard analysis methods do. Therefore, we proposed a new method named STPAFT. Through integrating STPA into a failure mode and effect analysis (FMEA) technique, STPAFT could not only give full play to the two methods, but could also meet all the requirements of the concept phase in ISO26262. In STPAFT, STPA is still responsible for hazard analysis and FMEA is responsible for risk assessment according to ISO26262. FMEA technology can also help STPA to analyze causal factors more systematically by focusing on the lowest level components, and more safety constraints (SCs) could be generated here, which could provide more guidance for the derivation of functional safety requirements (FSRs). In fact, through the integration of STPA and FMEA, STPAFT not only has a complete risk assessment process, but also is superior in the identification of causal factors. Therefore, using STPAFT instead of some single method will satisfy the requirements of HARA process in ISO26262 concept phase and handle the increasing complexity of systems.

The primary purpose of our study is to show how the work products required by ISO26262 concept phase could be generated by STPAFT. The safety constraints generated by STPAFT could provide strong support for the derivation of ISO26262 safety goals (SGs) and FSRs. In addition, with the rapid improvement of vehicle automation, ISO26262 may one day need to include causes of hazards other than malfunctioning behavior due to component failures to keep up to date with technological trends and STPAF as a hazard analysis method with the functions of risk assessment and constraints derivation, is especially in line with this development trend.

Our paper is organized as follows: Section 2 provides the background of our study. Section 3 represents a brief overview of ISO26262, STPA and FMEA. In addition, foundations and key terms of STPA and ISO26262 concept phase are analyzed to prove that STPA is suitable for ISO26262 concept phase. Section 4 represents how our proposed method formed and how to apply STPAFT in compliance with ISO26262. At last, we demonstrate an application of STPAFT in the case study of fuel level estimation and display system (FLEDS) to show how the concept phase of ISO26262 could be supported by STPAFT in Section 5. Sections 6 and 7 are the discussion, and conclusion and future work of our research, respectively.

2. Background

In this section, some clauses of ISO26262 concept phase relevant to this paper, STPA and FMEA technology are briefly introduced. Additionally, we provide a detailed comparative analysis on the theoretical foundations and key terms of STPA and ISO262626 concept phase.

2.1. ISO26262 for Road Vehicle Functional Safety

ISO26262, published in late 2011, is an international standard concerned with functional safety of safety-related E/E systems within the automotive systems. The purpose of this standard is to constructs a framework to integrate functional safety activities into the development of safety-related E/E systems through providing guidance, recommendation and argumentation [6]. The stipulation of each new product to be state-of-the-art could be helped by putting forward suggestions on specific safety development processes and safety classifications.

ISO26262 consists of 10 parts and the safety activities are mainly described in seven parts (from Part 3 to Part 9). Part 3 gives a clear explanation of the specific contents of the concept phase [6]:

1. Item definition: the object of this process is to describe the functionality, interfaces between other items, the driver and the environment of an item. This step is the input of the HARA process.
2. The HARA process is made up of three steps:

(1) Determine the hazardous events according to identified vehicle-level hazards, corresponding operational situations and operating modes.
(2) For each identified vehicle-level hazard, the risk assessment framework of ISO26262 is applied:

- The probability of exposure (E) to the operational situation is assessed.
- Identify potential scenarios which can cause a crash. The severity (S) of the harm to the persons involved is assessed if the crash happened.
- The controllability (C) of the vehicle and the operational situations is assessed.
- Determine the automotive safety integrity level (ASIL) based on E, S and C according to ISO 26262 as shown in Figure 1.

(3) The worst-case ASIL is assigned to the hazardous event.

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

(**a**)

Exposure Probability (E)	Class				
	E0	**E1**	**E2**	**E3**	**E4**
Description	Incredible	Very low probability	Low probability	Medium probability	High Probability

(**b**)

Controllability (C)	Class			
	C0	**C1**	**C2**	**C3**
Description	Controllable in general	Simply controllable	Normally Controllable	Difficult to control or uncontrollable

(**c**)

Severity class	Exposure class	Controllability class		
		C1	**C2**	**C3**
S1	**E1**	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	**E1**	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	**E1**	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

(**d**)

Figure 1. The determination of automotive safety integrity levels (ASILs) according to severity (S), controllability (C), and exposure (E): (**a**) classes of the impact factor S; (**b**) classes of the impact factor E; (**c**) classes of the impact factor C; (**d**) determination of ASILs.

3. SGs shall be determined for each identified hazardous event with its ASIL.

4. Functional safety concept: the most important objective of this step is the derivation of FSRs from the SGs, considering the system architectural design.

2.2. System Theoretic Process Analysis

STPA is a hazard analysis technique based on the STAMP framework, which was developed by Leveson in 2004 [5]. STPA regards safety as a control problem, and uses hierarchical safety control structures to describe systems. Accidents occur when unsafe interactions among components, external disturbance, and/or component failures are inadequately controlled. Analysis of the safety control structure could determine why inadequate control and enforcement of safety related constraints occurred [3–5]. There are mainly three steps in STPA:

1. The first is to establish the engineering fundamentals, including the determination of accidents, identification of system-level hazards leading to accidents, and the contribution of the system safety control structure.
2. Identify potential unsafe control actions (UCAs) leading to hazards using the safety control structure constructed in the previous step.
3. Identified causal factors leading to UCAs or a violation of SCs by examining each part in the control structure.

In recent years, STPA has been successfully used in various safety-critical systems of many fields [7–33], such as STPA for automotive systems [2,7–14], STPA for defense system [15], for medical devices such as a radiation therapy system [16], for nuclear industry [17] and for aerospace related systems [18–22], etc.

2.3. Failure Mode and Effect Analysis

FMEA is an inductive analysis method, which is used in the early development process to identify the potential failure modes and their causes of all components in the system [34,35]. FMEA calculates the effects of the identified failure modes through measurement of the severity, occurrence and detection probability. The analysis starts with the lowest level components and goes on to the effect of the failures on the whole system. At last, countermeasures will be proposed to reduce or minimize the negative effects of the identified failure modes. The steps in usual FMEA are shown in Figure 2.

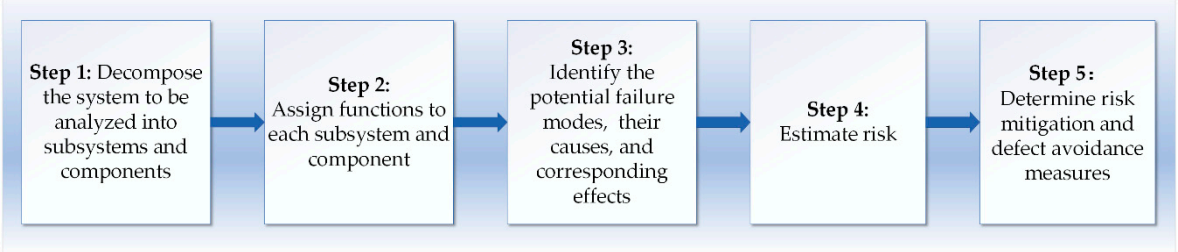

Figure 2. Steps of implementation process of failure mode and effect analysis (FMEA).

2.4. Related Work

Due to the advantages of STPA in safety analysis, some scholars used it in the HARA process of ISO26262. Hanneet [8] applied STPA to a lane keeping assist system to derive safety-driven design constraints and requirements. Abdulkhaleq [9] developed a dependable architecture for fully automated driving vehicles based on STPA. Abdulkhaleq also compared the results of STAMP/STPA with the safety case on the same system [10]. Then, safety engineering and software engineering are combined in [11,12] through a STPA-based approach for software-intensive systems. Suo [2] proposed a method using a meta-model based on System Model Language (SysML) to support the integration of STPA into ISO26262.

In [13,14], Hommes pointed out the hazard analysis methods recommended in ISO26262 are not sufficient in dealing with the rapidly increasing complexity of modern software-intensive systems through an assessment and emphasized the advantages of using STPA as a hazard analysis technology in the concept phase of ISO26262. This is a strong motivation for us to develop a new method based on STPA which can keep the superiority of STPA and assess risk at the same time.

3. Hazard Analysis Foundations and Key Terms of STPA and ISO26262

STPA is the core of our proposed method, so it is important to prove that STPA is suitable as a hazard analysis method for the ISO26262 concept phase. For this purpose, we first analyze the hazard analysis foundations of ISO26262 and STPA. Then, the key terms used in ISO26262 concept phase and STPA are compared to prove that STAP is applicable for ISO26262 from another view.

3.1. Hazard Analysis Foundations of the HARA Process in ISO26262 and STPA

First of all, both STPA and ISO26262 are based on the system engineering framework which views a system as an integrated whole. They both aim to embed safety into a system engineering process and to design safety into the system from the very beginning of a development process. Another thing in common is that both the STPA and HARA process are top-down processes. The HARA process of ISO26262 only focuses on hazards caused by component failures, while hazards in STPA may result from dysfunctional interactions among components, design flaws, human factors and external disturbance, beyond component failures. Activities in the HARA process are mainly divided into three parts as mentioned above. The most important difference between the HARA and STPA processes here is that the HARA process requires risk assessment according to the classification of hazardous events and determination of ASIL, while STPA does not intend to estimate risk. We list foundations of STPA and ISO26262 in Table 1.

Table 1. The foundations of ISO26262 hazard analysis and risk assessment and systems theoretic process analysis (STPA).

Foundations	ISO26262 HARA	STPA
Characteristics	Focus hazards on only component failures. HARA and determination of ASIL are used to determine SGs for the item.	Have a broader scope of hazards causes. View safety as a control problem. Use an hierarchical safety structure to describe a system and explain why accidents occur. Do not estimate risk.
Application Phase	Applicable in the development stage a system, with little known about the detail design.	Assumed to be used in any stages within the whole life cycle of a system, especially in the early stage of the development process.
Objectives	Identify and classify hazardous events. Formulate SGs and corresponding ASIL, for each hazardous event	Identify reasons for inadequate control or enforcement of safety related constraints.
Output Results	Hazardous events and their classifications, SGs and associated ASILs	Accidents and associated hazards of a system, UCAs, SCs to be enforced

3.2. Key Terms of ISO26262 Concept Phase and STPA

Key terms of STPA and ISO26262 HARA process are listed in Table 2. We could see the conceptual differences between the two from the table. Taking the definitions of hazard as an example, firstly, the scope of a hazard in STPA is much broader than the scope of a hazard in the HARA process as mentioned above. Next, the definition of hazard in STPA includes both "a system state or condition" and "a specific set of worst-case environmental conditions" which describe the contexts of "a system state or condition", while in ISO26262 hazards are only "potential source" of harm [3–6]. The meaning of "harm" in ISO26262 is similar to what "loss" means in STPA, but "harm" only means "injuries or damage to the health of person", while "loss" includes damage of property, pollution of environment, loss of mission, etc., besides human injuries or death. Although there is no

definition of "operating mode and operational situation" in STPA, according to the description of these two concepts in ISO26262, we can infer that these two concepts can be included in the definition of hazard in STPA. So, if we limit the scope of "loss" in an "accident" in STPA to "harms" in ISO26262, an "accident" in STPA could be equivalent to a "consequence of hazardous events" in our study. As for safety goals in ISO26262, they could be equivalent to the system-level SCs in STPA, because they are similar in definition.

Table 2. Key terminologies of STPA and ISO26262 concept phase.

Terminologies	STPA	ISO26262
Accident	Events leading to loss result from lack of enough control and enforcement of SCs	Not specifically defined
Hazard	The combination of a system state or set of conditions and a specific set of worst-case environmental conditions, will lead to an accident	Potential source of physical injury or damage to the health of persons caused by malfunctioning behavior of the item
Harm	Not specifically defined	Physical injury or damage to the health of person
Failure	A component's (or system's) non-performance or inability to perform as expected or designed.	Termination of an intended behavior of an element or an item due to a fault manifestation
Operation Situations	Not specifically defined	Scenarios that may occur within the life of a vehicle
Operating modes	Not specifically defined	Perceivable functional state of an item or element
Hazardous event	Not specifically defined	The result of integrating a hazard with an operational situation
ASILs	Not specifically defined	Levels used to specify safety measures and necessary requirements of an element or item for avoiding unreasonable residual risk
Safety Constraints (System Level)	System-level safety requirements to prevent hazards from leading to accidents and ensure safety	Not specifically defined
Safety Goals	Not specifically defined	Top-level safety requirements for an item as a result of vehicle-level HARA, expressed as functional objectives
Malfunctioning Behavior	Not specifically defined	An item's failure or unintended behavior with respect to its design intent
Unsafe control actions (UCAs)	Inadequate control actions within four types leading to hazards	Not specifically defined
Causal Factors	Scenarios that could explain how inadequate control actions might occur	Not specifically defined
SCs for UCAs and Causal Factors	Safety requirements derived from the identified UCAs and corresponding causal factors	Not specifically defined

According to the analysis above, the differences between STPA and ISO26262 are mainly reflected in the fact that STPA covers a wider scope than ISO26262 in many key factors, such as hazard, accident, etc. Therefore, if STPA is to be used for hazard analysis in ISO26262, it is necessary for STPA to adapt to the current requirements of the concept phase of ISO26262. In this paper, certain key terms in STPA will be limited to the scope of ISO26262 requirements, such as "loss" in STPA and "harm" in ISO26262, and some could be equivalent in this paper, such as "accident" in STPA and "consequence of hazardous event" in ISO26262. So that the work products required by the concept phase of ISO26262 can be obtained through the analysis of STPA. Moreover, we will explain how to map corresponding key terms of STPA and ISO26262 in Section 5. In a word, all the distinctions are understandable, since STPA is a general safety analysis method, and ISO26262 only serves road vehicles. So, if we make some appropriate adjustments to STPA, it can fully meet the requirements of ISO26262 for hazard analysis.

4. The Proposed Method

In order to generate (or support) the relevant work products required in the concept phase of ISO26262, we proposed an improved approach called STPAFT, which integrates STPA into the FMEA technique to conduct both hazard analysis and risk assessment. STPA could also be supported by the FMEA technique in the systematic identification of causal factors through the focus of FMEA on associated components of the system, and more SCs could be formulated here which means the proposed method will provide more information for the FSRs determination.

4.1. Integrating STPA into FMEA

Although STPA and FMEA are two different methods, from the analysis process of the two methods, FMEA first identifies the failure mode after assigning functions to subsystems and components, and then determines the causes of the failure modes. This process is similar to the process of identifying unsafe control actions and then confirming the causal factors after establishing the safety control model of STPA. Therefore, in order to make full use of FMEA templates for causal factors analysis and risk assessment, some concepts of STPA are corresponding to FMEA in this paper. This is not to say that their essence is the same, but to enable STPA to make full use of the FMEA template in the analysis process. Figure 3 illustrates the correspondence between key concepts of STPA and FMEA.

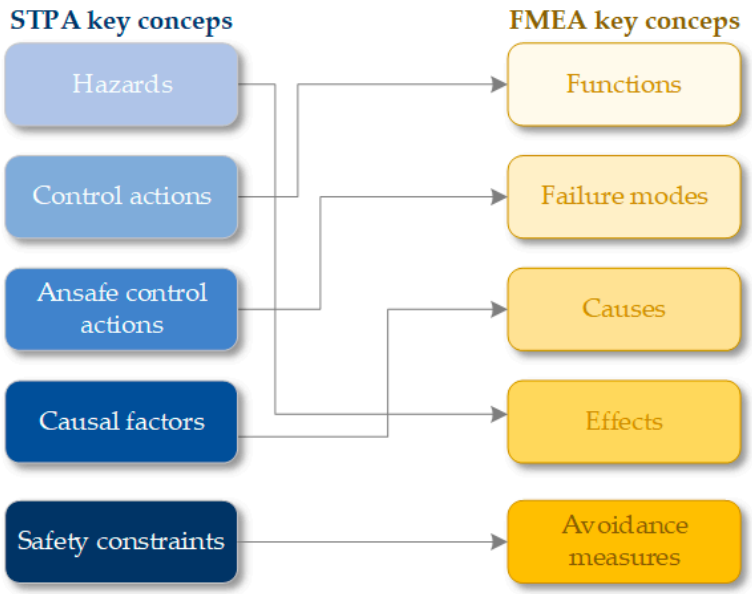

Figure 3. Correspondence between key concepts of STPA and FMEA.

Before the integration of the two methods, we will complete Step 1 and 2 of STPA first, that is, to determine an accident, identify the system-level hazards and the unsafe UCAs. Here, as shown in Figure 3, a control action in STPA can be equivalent to a function in FMEA, while a UCA can be equivalent to a failure mode in our paper. Combine Step 3 of STAP and Step 3 of FMEA to determine the causal factors (causes) of UCAs (failure modes), and Step 4 of FMEA can be used to assess risk according to ISO26262. The general steps of our proposed method are shown in Figure 4, and the specific steps of STPAF are described in detail below.

4.2. Step 1: System Engineering Fundamentals Establishment and UCAs Identification

STPAFT begins with the establishment of system engineering fundamentals which is similar to the first step of STPA, including system-level accidents and hazards identification, corresponding SCs determination and safety control structure establishment.

4.2.1. System Engineering Fundamentals Establishment

As mentioned in Section 3, the consequences of hazardous events in ISO26262 could be determined by integrating accidents in STPA with operating modes and operational situations. A "hazard" of STPA could be mapped to a "hazardous event" of ISO26262. In order to distinguish the "hazard" of STPA from the "hazard" of ISO26262, we use " the system-level hazard" here to present the "hazard" of STPA, and the "vehicle-level hazard" to present the "hazard" of ISO26262 in the rest part of this paper.

The first step of STPA includes:

- Define the "loss" of the system accident in STPA with limitation to the scope of harm defined by ISO26262 to be analyzed.
- Identify system-level hazards leading to the accidents and corresponding operating modes and operational situations from the descriptions of identified system-level hazards.
- Determine corresponding vehicle-level SCs which could be used to support the SGs determination subclause of ISO26262, as the SGs are high-level requirements too. However, the SGs in ISO26262 are more specific than the SCs of the same level in STPA [9].
- Draw the safety control structure of the system to identify the potential UCAs leading to the system-level hazards. The control structure diagram shows the boundary of the system under analysis and its interface, and information it contains can be used to define an item.

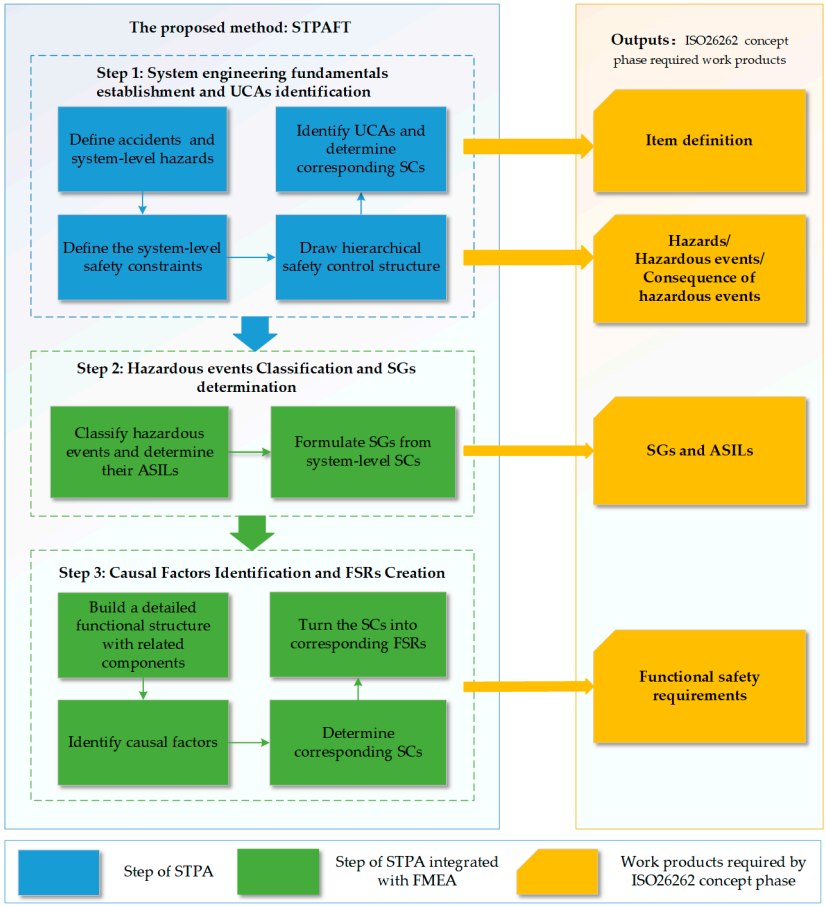

Figure 4. General steps of the proposed method with the implementation steps of STPAFT on the left hand side and the outputs of STPAFT required in ISO26262 concept phase on the right hand side.

4.2.2. UCAs Identification

- Identify the UCAs leading to system-level hazards identified in the last step according to the four categories [3] (a control action not provided, a control action provided incorrectly, a control action provided at wrong timing/order, and a control action stopped too soon/applied too long)

by examining the safety control structure. Information of UCAs could be helpful in the determination of operating modes, operational situations and the controllability for each hazardous event.
- Corresponding SCs could be determined by adding leading words like "should" or "must" in the description of UCAs.

4.3. Step 2: Hazardous Events Classification and SGs Determination

In this step, the FMEA technique is integrated for risk assessment.

- Each hazard identified could be classified with two factors (S and E) [9]. The controllability for each hazardous event to assess whether a situation is usually controllable [36] could be determined by the identified operational situations and UCAs.
- Turn the SCs for system-level hazards determined above into the SGs for each hazardous event corresponding to their ASILs.

4.4. Step 3: Causal Factors Identification and FSRs Creation

- With the help of the FMEA technique and the guide words provided by STPA [37], the identification of possible causal factors becomes more detailed at the components level. In order to make better use of FMEA, a functional structure with more details of the system under analysis should be created.
- Generate corresponding SCs for causal factors identified. Since SCs for UCAs and causal factors are all used to describe how to avoid or mitigate hazards, they could be mapped with FSRs of ISO26262.
- Turn the SCs into corresponding FSRs according to the requirements in the 7.4 subclause in ISO26262 Part 3 [6].

5. Case Study

In this section, we will use the FLEDS in the Scania trucks [38] as a case study to show how STPAFT performs analysis and how to generate/support all work products required/recommended in the concept phase of ISO26262. The FLEDS is one of the safety-critical E/E system in Scania trucks. Dysfunctional behaviors of such system could result in hazards, such as stop of the engine and loss of power-assisted steering [38].

5.1. The FLEDS

In this section, we will show how the FLEDS works and what components it consists of. There are two major functions in the FLEDS: FC1: Low fuel level warning and FC2: Fuel level estimation and display. FC1 is responsible for warning a driver that the fuel level is below a measurable limit of the tank capacity, even if the driver does not often check the fuel gauge. FC2 is to measure and present the fuel level in the instrument cluster to meet the need of the driver to know the current fuel level in the fuel tank. The estimated fuel level and the warning are both presented in the instrument cluster.

Three electronic control unit (ECU) systems make up the FLEDS, which are engine management system, instrument cluster, and coordinator. Each ECU system contains several allocation elements (AEs) which are pieces of code responsible for realizing user functions. There are two AEs allocated in the coordinator ECU system (COO) used to estimate and display the fuel level: AE01 and AE02. Other parts of the FLEDS include a fuel level sensor (FLS) placed in the tank to estimate and check the fuel level, a parking brake switch (PBS) to provide parking brake status which is required for the purposes of refuel detection, and a battery to supply power to ECU systems. We show the components and functional structure of the FLEDS in Figure 5.

- Engine management system ECU (EMS) is responsible for all the engine related functions.
- The function of instrument cluster ECU system (ICL) is to display indications to the driver, such as warning lamps.

- Coordinator ECU system (COO) is the core ECU of FLEDS and responsible for all functions related to the fuel level calculation. Three inputs are required by COO. They are:
  - Fuel level signal from fuel level sensor (FLS)
  - Fuel rate signal from EMS
  - Parking brake status from parking brake switch (PBS)

AE01 is the allocation element responsible for the fuel level estimation. The fuel level measured by the FLS is first converted to a voltage value and then converted to a percentage of the total capacity. The result and the fuel consumption rate calculated by EMS are used as the input of Kalman filter algorithm, and the current fuel level is finally obtained. This result will be sent to ICL to display the current fuel level. Then AE02 compares the calculation results from AE01 with the tank capacity to determine whether to activate a low fuel level warning.

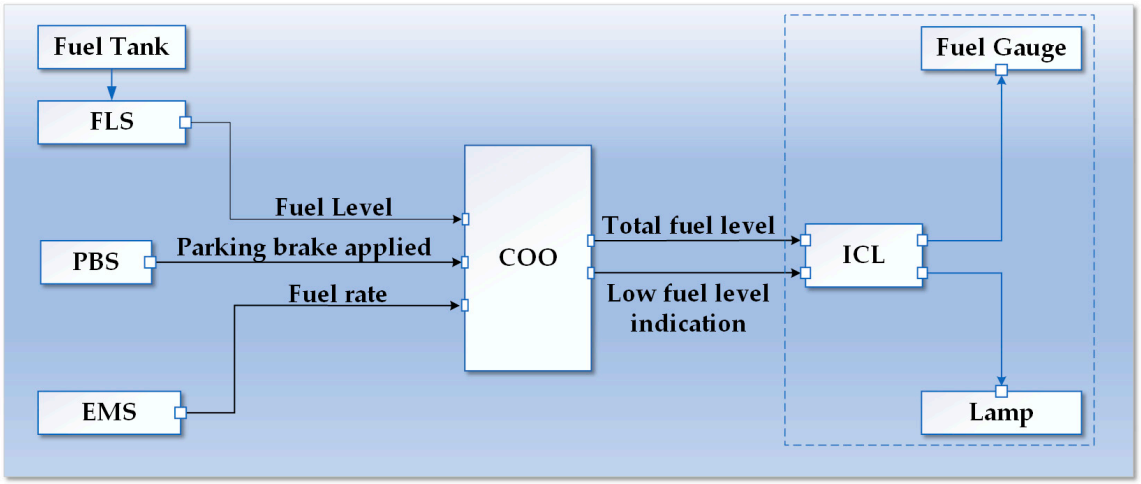

Figure 5. Functional structure composed of electronic control unit (ECU) systems of fuel level estimation and display system (FLEDS).

5.2. Applying STPAFT

Figure 6 presents the results of STPAFT process which could support the generation of the work products required by the concept phase of ISO26262, described with one of the results of our analysis. The blue arrows between the boxes, such as S1, S2 to I5, S2 to I2, I3, I4, and SF1 to I6, SF2 to I7, indicate that the work products of ISO26262 can be directly obtained from the results of STPAFT. The gray arrows between the boxes, such as S3, S5 to I8, S4 to I1, indicate that the products required by ISO26262 can be derived from the analysis results of STPAFT. The orange blocks from SF1 to SF3 are results obtained by integrating FMEA. SF1 and SF2 present the hazardous event classification and the ASIL determination results. SF3 is an example of the causal factors and corresponding SC identified. STPAFT realizes the classification of hazardous events and the determination of ASILs through the integration of FMEA technique. Another reason for integrating FMEA is that FMEA could help STPA with the identification of causal factors by focusing on the lowest level components. More detailed information about the whole process of applying STPAFT will be covered in the following sections.

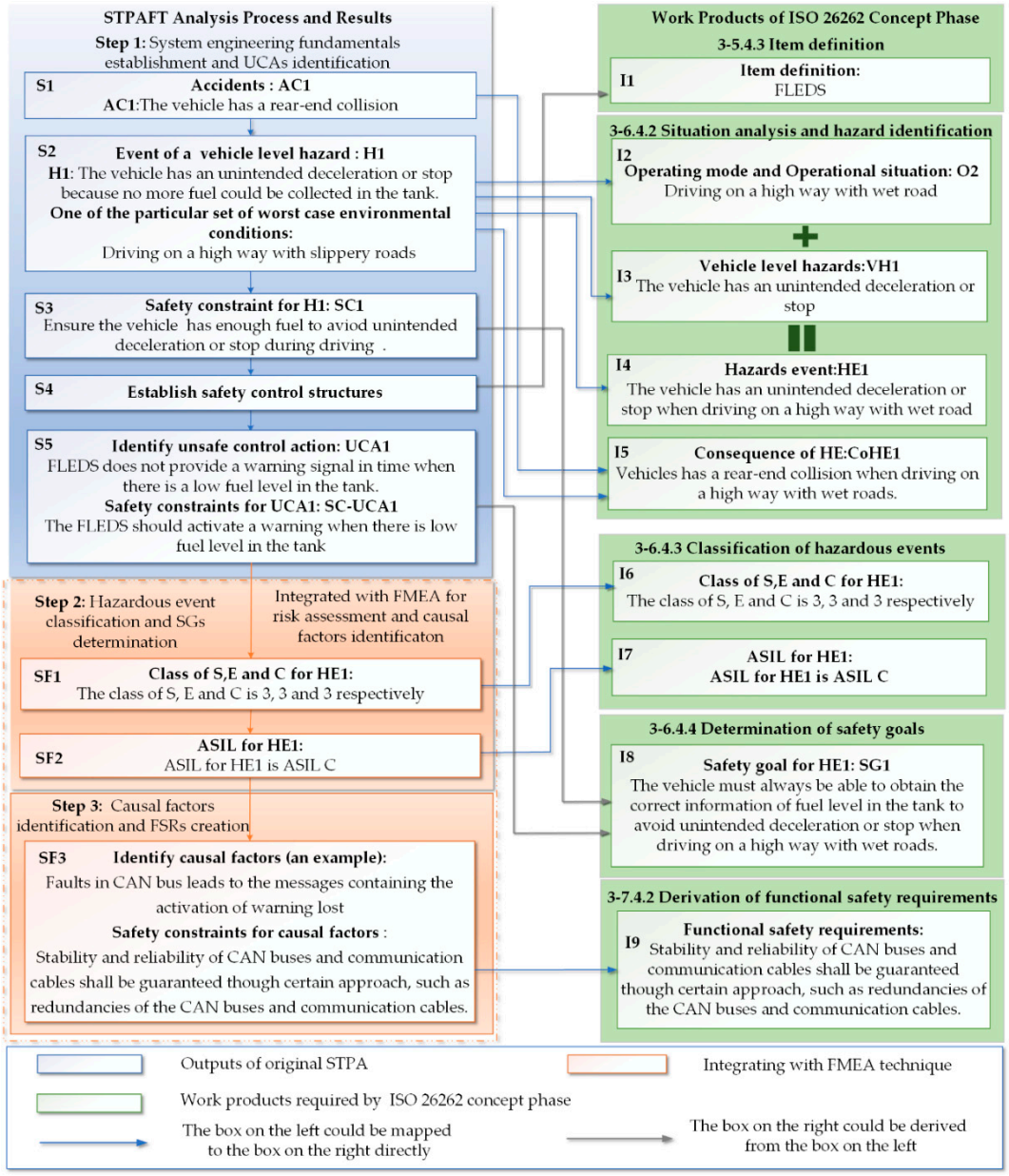

Figure 6. The analysis process of STPAFT and the corresponding relationship between the analysis results and the work products required by ISO26262-Part 3: Concept phase.

5.2.1. System Engineering Foundations Establishment

As mentioned in Section 4, the first step begins with determining vehicle-level accidents, associated hazards, corresponding system-level SCs, and drawing a safety control structure. An example of vehicle-level accidents related to the FLEDS could be defined as AC1: The vehicle has a rear-end collision. One of the system-level hazards that could result in AC1 is determined as H1 (an example): The vehicle has an unintended deceleration or stop because no more fuel could be collected from the tank when driving on a highway with wet roads. The safety constraint for H1 is SC-1: The vehicle must always have enough fuel to avoid unintended deceleration or stop when driving on a highway with wet road. In STPAFT, system-level SCs as top-level safety requirements are used to mitigate hazards, which is similar to the role of SGs in ISO26262. Therefore, system-level SCs in STPAFT could correspond to SGs in ISO26262.

The vehicle-level hazard VH1 for ISO26262 could be derived as: The vehicle has an unintended deceleration or stop because no more fuel could be collected in the tank. The particular worst-case environmental condition here is “driving on a highway with wet roads” which is represented in S2

in Figure 6. Therefore, the operating mode and operational situation can be determined as O1: Driving on a highway with wet roads. More possible operational situations are represented in Section 5.2.3. Then the corresponding hazardous event HE1 could be determined by combining VH1 with O1: The vehicle has an unintended deceleration or stop because no more fuel could be collected in the tank when driving on a highway with wet roads and the consequence of hazardous events could also be derived as CHE1: The vehicle has a rear-end collision with the following vehicle travelling at high speed when driving on a highway with wet roads.

The next step in STPAFT is to establish a safety control structure to identify potentially hazardous control actions that could violate the SCs and lead to H1. The information from safety control structure could be taken to conduct the item definition. So, S4 in STPAFT is mapped to I1 in ISO26262 in Figure 6. Figure 7 shows the control structure diagram of the FLEDS at the architectural design level. In this structure, FLEDS is considered as a controller, the fuel tank is a controlled process and the driver is treated as an actuator to refuel the tank according to the FLEDS's commands.

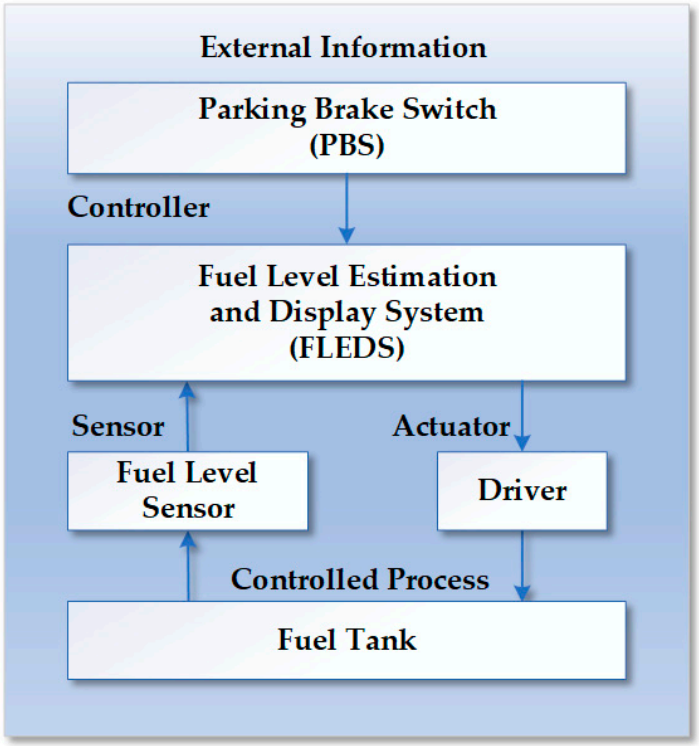

Figure 7. STPA high level control structure for the identification of unsafe control actions.

5.2.2. UCAs Identification

As mentioned above, the FLEDS has two main functions: FC1 and FC2. For FC1, the control action is CA1: Provide a warning to indicate the driver when there is a low fuel level. For FC2, the control action is CA2: Supply the current fuel level to the driver. Therefore, according to three of the four UCA types (the control actions in our study do not have a duration problem), the unsafe control actions UCA1 for CA1, the unsafe control actions UCA2-1 and UCA2-2 of CA2 could be identified, as shown in Table 3. For further exploration of causal factors and determination of ASIL for HE1, the control actions and the UCAs identified here will correspond to functions and failure modes in the following FMEA analysis.

We transform the description of unsafe control actions into corresponding security constraints by adding guide words, such as "should" and "must", as shown in Table 4.

Table 3. Possible unsafe control actions leading to H1.

Control Action	Not Provide	Provide But Incorrect	Provide at Wrong Time/Order
Provide a warning signal	UCA1: No warning signal provided	…	
Supply the current fuel level value	UCA2-1: No fuel level supplied	UCA2-2: Supplied but too high	…

Table 4. Safety Constraints for UCAs.

SC.UCA1	The FLEDS should activate a warning to indicate the driver when there is a low fuel level in the tank
SC.UCA2-1	The deviation of the estimation of fuel level shall not exceed the preset allowable deviation from the actual volume in the tank.
SC.UCA2-2	The FLEDS shall always indicate the total fuel level in the tank when driving.

5.2.3. Classification of Hazardous Events and Determination of ASIL

FMEA now could be used for the classification of HE1 according to ISO26262. Steps will be performed as follows:

- Fill CA1, CA2, UCA1, VH1, AC1 and possible operational situations into corresponding columns of FMEA in Table 5.
- Determine the ASIL for each hazardous event identified, taking HE1 as an example. As mentioned above, HE1 identified could be classified with two factors (S and E). The controllability for each hazardous event could be determined by the operational situations together with UCAs identified. The hazard events HE1 is a rear end collision on a highway with wet roads, which could cause fatal injuries, so the severity is determined as S3.
- Probability of exposure could be E3, medium probability. According to the operating modes and operational situation O1: driving on a highway with wet roads, and the unsafe control action UCA1: The FLEDS does not provide a warning signal when there is a low fuel level; the situation is difficult to control or uncontrollable, so the controllability is assigned as C3. Therefore, the ASIL of the hazardous event HE1 could be determined as ASIL C. The ASILs for VH1 under different operational situations are represented in Table 5.
- Formulate SGs according to each corresponding ASIL, still taking HE1 as an example. The SG for HE1 could be formulated according to SC-1 as SG.1: The vehicle must always provide correct information about the current fuel level in the tank to avoid unintended deceleration or stop when driving on a highway with wet roads.

Table 5. Hazardous events classification and ASIL determination using FMEA.

Function	Failure Modes (UCAs)	Cause (CFs)	Actions (SCs)	Effect						
				Accident	System-Level Hazard	Operational Situations	S	E	C	ASIL
Provide a warning to indicate the driver when there is a low fuel level	The FLEDS does not provide a warning to indicate the driver when there is a low fuel level in the tank.	Shown in Section 5.2.4		AC1	H1	Highway with wet roads	3	3	3	C
						City driving, snow and ice driving speed 50km/h	3	2	3	B
Supply the current fuel level to the driver	The FLEDS does not supply a fuel level to a driver.					City driving slippery road, high traffic	2	3	2	A
	The fuel level supplied by FLEDS is much higher than the actual level.					1Free way	3	2	2	A

5.2.4. Causal Factors Identification and FSRs Creation

- In order to determine how each UCA could happen using FMES, a detailed structure of the FLEDS is illustrated in Figure 8. We use Figure 8 and the guide words for causal factors in Figure 9 [39] to identify possible causal factors leading to UCAs. With the focus of FMEA on the lowest level components, we can identify the causal factors more systematically, so more detailed safety constraints could be derived, which is conducive to the refinement of FSR.
- We use a hierarchical structure to describe the identified causal factors for each UCA in Table 6, in which "①" represents the highest level and "⑤" represents the lowest. This hierarchical structure presents how unsafe interactions, errors and failures propagate through the system and lead to UCAs. The most important thing is that the hierarchical structure of causal factors would be of great benefit for the allocation of FSRs to the system architecture design.
- Next, the SCs for causal factors are generated and the results of this step will be used to build the functional safety concept and determine the FSRs. The primary intention of the presentation of all the SGs and FSRs derived from SCs in this section are to illustrate how a comprehensive set of requirements could be derived from STPAFT analysis results.

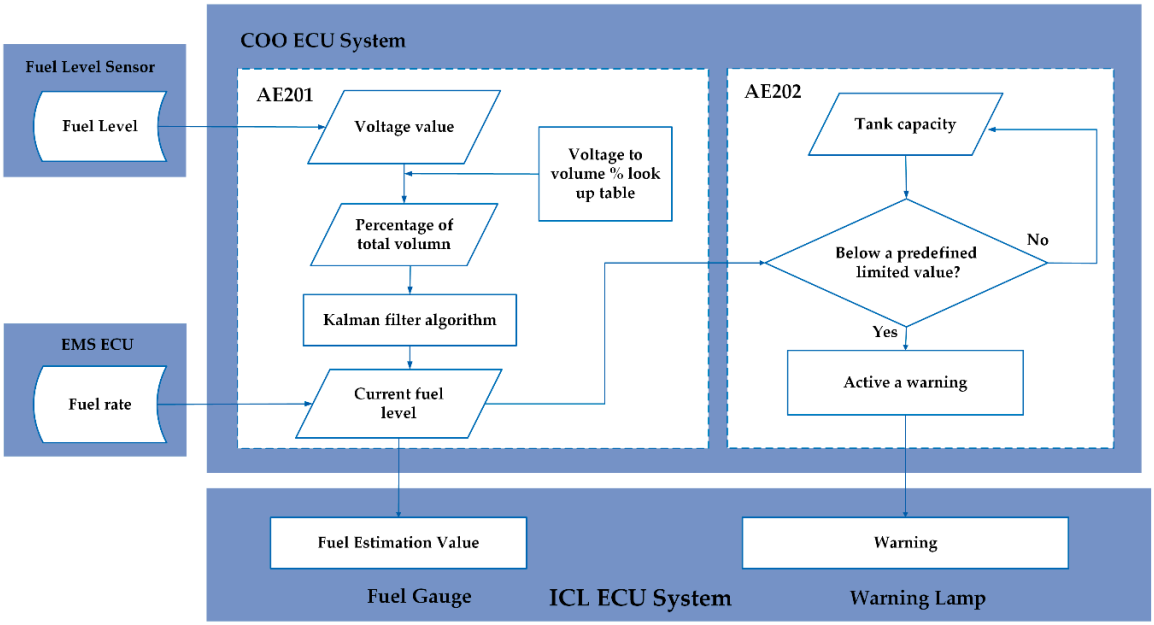

Figure 8. Detailed function structure of FLEDS with ECU systems and allocation elements (AEs).

According to the causal factors identified in Table 6, related SCs could be identified:

- SC.CF.1: The input signals for estimating the total fuel level shall be good status (meaning the signals are in the range and correct).
  - SC.CF.1-1: The FLS shall always keep running normally, and measure fuel level data accurately.
  - SC.CF.1-2: The EMS shall always calculate the fuel rate correct.
- SC.CF.2: The input parameters used for estimation of the total fuel level shall be of good status; a replacement value shall be considered and kept.
  - SC.CF.2-1: The correct parameters of FLS shall be set.
  - SC.CF.2-2: The correct parameters of the fuel tank shall be set.
- SC.CF.3: The measured fuel level signal shall be filtered to avoid the fuel level changing rapidly in some situations, such as driving in long curves, hills and slopes.

- SC.CF.4: The algorithm for total fuel level estimation shall be designed appropriately and a feedback should be set to avoid the deviation of more or less than a permissible error when there are erroneous or unavailable input signals or parameters.
    - SC.CF.4-1: The mapping of voltage to volume shall be correct.
- SC.CF.5: When the estimated fuel level reaches a limit of the measurable volume in the tank, the low fuel level warning shall be provided one time.
- SC.CF.6: The ICL shall always function properly, including the gauge and the lamp.
- SC.CF.7: Stability and reliability of Controller Area Network (CAN) buses and communication cables shall be guaranteed through certain approaches, such as redundancies of the CAN buses and communication cables.
- SC.CF.8: The battery shall have enough capacity and ensure power supply continuous and reliable. The electrical connections between the battery and ECUs shall be stable.

Then, the corresponding FSRs could be derived from these SCs according to the requirements that FSR shall specify strategies for fault avoidance, fault detection and control of faults or the resulting of malfunctioning behaviors, etc. in ISO26262 Part 3.

- FSR1: The input signals for estimating the total fuel level shall be good status (meaning the signals are in the range and correct). Considered input signals are: fuel level, fuel rate, and parking brake applied. In case input signals are not of good status, a replacement value shall be considered.

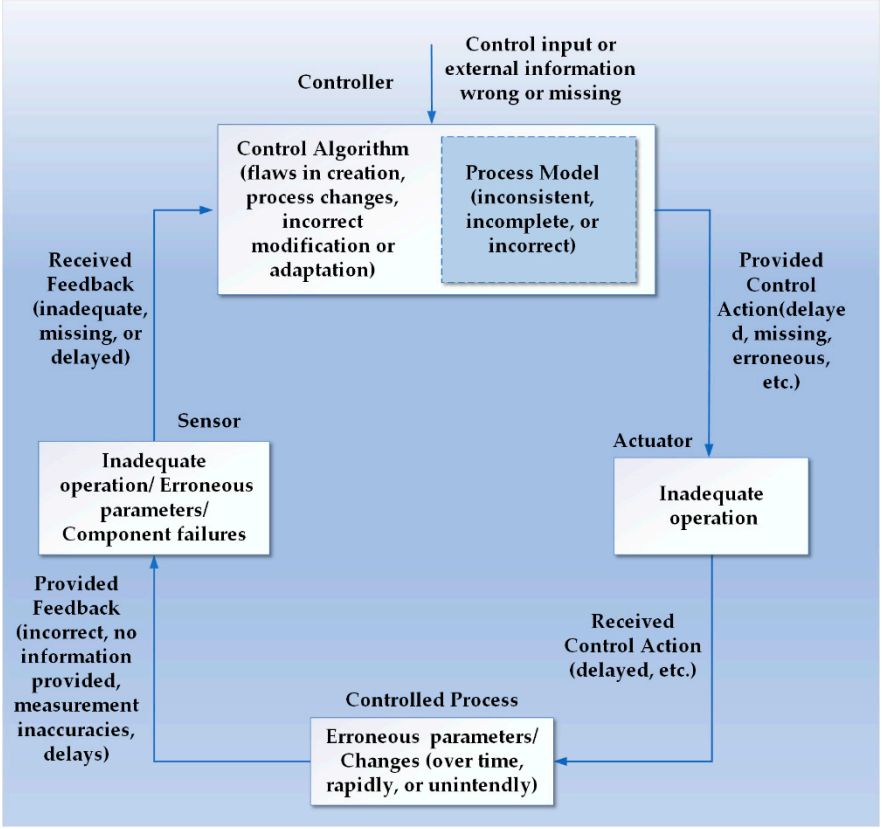

Figure 9. Causal factors of UCAs to be considered in each part of the safety control structure.

Table 6. Causal factors analysis for unsafe control actions of FLEDs.

UCAs	Causal Factors			
The fuel level supplied by FLEDS is much higher than the actual level.	① The gauge has a mechanical fault			
	① The gauge function in ICL has bugs			
	① Incorrect estimation of fuel level by Kalman filter	② Incorrect fuel level	③ Incorrect FLS value	④ Electrical fault in FLS
				④ Mechanical fault in FLS
			③ Incorrect calculation of tank capacity	④ Tank parameter set incorrectly
				④ Incorrect FLS parameters
			③ Incorrect mapping of voltage to volume %	④ Fault in mapping look up table
		② Incorrect fuel rate	③ The calculations of fuel rate by EMS is incorrect	
The FLEDS does not supply a fuel level to a driver.	2460 The gauge function in ICL has bugs			
	① No total fuel level received by ICL	② Problems in COO	③ Hardware fault in COO	
			③ No power supply fed to COO	④ Fault in the power supply
				④ There is a fault in the power cable between COO and power supply
		② Communication problem between COO and ICL	③ Cut in communication cable	
			③ CAN message that has total fuel level lost	④Fault in CAN bus
	① Hardware fault in ICL			

The FLEDS does not provide a warning to indicate the driver when there is a low fuel level in the tank.	① The low fuel level warning function in COO outputs incorrectly	① The gauge has a mechanical fault			
		② Kalman filter estimates fuel level erroneously	① Communication problem between COO and ICL		
			② Message that contains the activation of warning is lost	② Cut in communication cable	
				③ Fault in CAN bus	
			① Fault in warning lamp		
			① Bug in warning lamp function in ICL		
			② Erroneous value of tank size		
		③ Erroneous fuel level	④ Incorrect mapping of voltage to volume %	⑤ Fault in mapping look up table	
			④ The fuel level value is filtered incorrectly	⑤ Low pass filter equation has faults	
			④ Incorrect FLS value	⑤ Electrical fault in fuel sensor	
				⑤ Mechanical fault in fuel sensor	
			④ Errors in the calculation of tank capacity	⑤ The tank parameters set incorrectly	

			⑤ Incorrect FLS parameters
		③ Fuel rate errors	④ The calculations of fuel rate by EMS is incorrect

- FSR2: The input parameters used for estimation of the total fuel level shall be of good status; a replacement value shall be considered and kept. Considered input parameters are sensor parameters and tank parameters.
- FSR3: The measured fuel level signal shall be filtered to avoid rapid fuel level changes in some situations, such as driving in long curves, hills and slopes.
- FSR4: The algorithm for total fuel level estimation shall be designed appropriately and use feedback to gain information that should be adjusted in a way that will not result in a deviation of more or less than a permissible error when there are erroneous or unavailable input signals or parameters.
- FSR5: Stability and reliability of CAN buses and communication cables shall be guaranteed through certain approaches, such as redundancies of the CAN buses and communication cables.
- FSR6: When the estimated fuel level reaches below the predetermined limit value, the low fuel level warning should warn one time.
- FSR7: There shall be fault detection strategies for hardware in the FLEDS such as the lamp, gauge, and the battery, etc., and shall active warnings when they go wrong. If the FLEDS lose its function, there shall be certain approaches for the driver to obtain the fuel level value.

6. Discussion

Although ISO26262 Part 3 has stated in its scope of application that the hazards addressed in this document refer to the hazards caused by malfunctioning behaviors of items and their interaction, the HARA process only focuses on hazards caused by malfunctioning behaviors, and if every other system in the vehicle is sufficiently independent, they are assumed to be functioning correctly. However, it would be a bit arbitrary to conclude that HARA is only aimed at the hazards caused by item failures, because malfunctioning behavior refers to failure or unintended behaviors related to the design intent, but ISO26262 does not specify what "unintended behavior" exactly includes. While for STPA, accidents result from inadequate control of component failures, dysfunctional interaction of components, external disturbance, etc. In addition, STPA does not deal with risk assessment and only focuses on the causes of inadequate control or enforcement of safety constraints leading to accidents. In order to meet all the requirements of ISO26262 in the concept phase, we combine STPA and FMEA to form a new analysis method STPAFT. STPA and FMEA can complement each other, so STPAFT not only has the advantages of STPA in hazard analysis, but also can evaluate risk. Through the focus of FMEA on low-level components, STPAFT can obtain more detailed causal factors, which is very helpful for the functional safety requirements derivation in the concept stage of ISO26262. Another point worthy of note is that ISO26262 does not seem to make systematic requirements for the definition of an item. Therefore, we can use information of STPA on safety control structure to clearly describe an item in terms of system function and system boundary. In the area of the rapidly developing automotive domain, the increasing implementation of advanced functions and intelligence in vehicles greatly improves the degree of vehicle automation. In order to ensure functional safety, factors leading to hazards other than component failure must be taken into account. Therefore, it may be a trend to integrate STPA into the functional safety standards.

7. Conclusions and Future Work

For automotive systems, which could be described as a safety-critical system, they must fully satisfy the safety requirements as well as the functional requirements. Safety requirements describe the characteristics that a system must have in order to remain safe, and also key attributes that must be ensured to mitigate or avoid potentially unacceptable hazards. Violation of safety requirements will expose the system to various possible risks. Therefore, safety requirements must be considered to reduce risk in the design and development process of automotive systems. Nowadays, the intensive use of software and the increase in functional requirements have significantly increased the complexity of automotive systems. Therefore, the traditional safety analysis technology based on reliability theory will have certain limitations in the safety analysis of a modern complex safety-critical system, so it is not suitable to be used alone.

In this paper, we combined STPA and FMEA to obtain a new method called STPAFT, which has the advantages of both STPA and FMEA. It not only expands the scope of causes of hazards, but also could assess risk. Taking the FLEDS system as a case study, we described in detail the analysis process of STPAFT and the corresponding relationship between the analysis results and work products required in the ISO26262 concept phase. It is found that the analysis results of STPAF can fully meet the requirements of ISO26262. In addition, through the analysis process, the information used to establish safety control structure can make up for the lack of systematic requirements of an item in ISO26262. Then, through the focus of FMEA on related components level, we created more targeted safety constraints, which is conducive to the derivation of safety goals and functional safety requirements.

So, the use of STPAFT will be helpful to give recommendations for the early development and design process of automotive systems. In our future work, we plan to explore the role of STPAFT in the safety analysis of fully automated vehicles with a higher proportion of software, and further understand the advantages and limitations of using STPA to support the ISO26262 concept phase. In addition, we plan to introduce the model-based safety analysis technique into the implementation process of STPAF, and strive to abstract STPAFT into a standard architecture, so as to facilitate its automatic implementation, and improve the analysis efficiency, correctness, consistency and traceability.

Author Contributions: Conceptualization, L.C. and J.J.; methodology, L.C. and T.Z.; writing—original draft preparation, L.C.; writing—review and editing, L.C. and T.Z.; project administration, J.J.; funding acquisition, T.Z. and J.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Flemming, C. Safety-Driven Early Concept Analysis and Development. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2015.
2. Suo, D.; Yako, S.; Boesch, M.; Post, K. *Integrating STPA into ISO26262 Process for Requirement Development; Safety of the Intended Functionality*; SAE: Washington DC, USA, 2017; doi:10.4271/2017-01-0058.
3. Leveson, N. *Engineering a Safer World*; MIT Press: Cambridge, MA, USA, 2012.
4. Leveson, N. Completeness in formal specification language design for process-control systems. In Proceedings of the Third Workshop on Formal Methods in Software Practice, Portland, OR, USA, August 2000; pp. 75–87.
5. Leveson, N. A new accident model for engineering safer systems. *Saf. Sci.* **2004**, 42, 237–270.
6. ISO. *26262: Road Vehicles—Functional Safety, International Organization for Standardization*; ISO: Geneva, Switzerland, 2018.
7. Sundaram, D.; Vernacchia, P.; Wagner, M.S.; Thomas, J.; Placke, S. *Application of STPA to an Automotive Shift-by-Wire System*; STAMP Workshop: Cambridge, MA, USA, 2014.
8. Haneet, S.M.; Thomas B.; Sudeep, P. Application of systems theoretic process analysis to a lane keeping assist system. *Reliab. Eng. Syst. Saf.* **2017**, 167, 177–183.
9. Abdulkhaleq, A.; Daniel, L.; Stefan, W.; Jürgen, R.; Norbert, B.; Ludwig, R.; Thomas, R.; Hagen, B. A Systematic Approach Based on STPA for Developing a Dependable Architecture for Fully Automated Driving Vehicles. *Procedia Eng.* **2017**, 179, 41–51.
10. Abdulkhaleq, A.; Wagner, S. Experiences with Applying STPA to Software-Intensive Systems in the Automotive Domain. In Proceedings of the 2013 STAMP Conference at MIT, Boston, MA, USA, 26–28 March 2013.
11. Abdulkhaleq, A.; Wagner, S. A software safety verifification method based on system-theoretic process analysis. In Proceedings of the International Conference on Computer Safety, Reliability, and Security, Delft, The Netherlands, 22–25 September 2014; Springer: Berlin/Heidelberg, Germany, 2014; pp. 401–412.
12. Abdulkhaleq, A.; Wagner, S.; Leveson, N. A Comprehensive Safety Engineering Approach for Software-Intensive Systems Based on STPA. *Procedia Eng.* **2015**, 128, 2–11.

13. Hommes, Q.V. E. *Review and Assessment of the ISO26262 Draft Road Vehicle—Functional Safety*; SAE Technical Paper 2012-01-0025; ISO: Geneva, Switzerland, 2012, doi:10.4271/2012-01-0025.
14. Hommes, Q.V.E. Safety Analysis Approaches for Automotive Electronic Control Systems. 2015. Available online: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/2015sae-hommes-safetyanalysisapproaches.pdf/2015SAE-Hommes-SafetyAnalysisApproaches.pdf (22 January 2015).
15. Periera, S.; Grady, L.; Howard, J. A system-theoretic hazard analysis methodology for a non-advocate safety assessment of the ballistic missile defense system. In Proceedings of the 2006 AIAA Missile Sciences Conference, Monterey, CA, USA, 14–16 November 2006.
16. Bladine, A. Systems Theoretic Hazard Analysis (STPA) Applied to the Risk Review of Complex Systems: An Example from the Medical Device Industry. Ph.D. Thesis, MIT, Cambridge, MA, USA, 2013.
17. Martin, R.; Christian, H. Use of STPA as a diverse analysis method for optimization and design verification of digital instrumentation and control systems in nuclear power plants. *Nucl. Eng. Des.* **2018**, 331, 125–135.
18. Fleming, C.H.; Spencer, M.; Thomas, J.; Leveson, N.; Wilkinson, C. Safety assurance in NextGen and complex transportation systems. *Saf. Sci.* **2013**, 55, 173–187.
19. Hu, J.; Zheng, L.; Xu, S. Safety analysis of wheel brake system based on STAMP/STPA and Monte Carlo simulation. *J. Syst. Eng. Electron.* **2018**, 29, 1327–1339.
20. Mogles, N.; Padget, J.; Bosse, T. Systemic approaches to incident analysis in aviation: Comparison of STAMP, agent-based modelling and institutions. *Saf. Sci.* **2018**, 108, 59–71.
21. Wang, Y.; Sun, Y.; Li, C. Aircraft flight safety analysis and evaluation based on IDAC-STPA model. *Syst. Eng. Electron.* **2019**, 41, 1056–1062.
22. Wang, Y.; Wang, L.; Hu, J.; Zhou, Y. Modeling and analysis of IMA inter-partition communication safety requirement based on STPA. In Proceedings of the 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 24–26 November 2017; pp. 284–287.
23. Yang, Z.; Lim, Y.; Tan, Y. An Accident Model with Considering Physical Processes for Indoor Environment Safety. *Appl. Sci.* **2019**, 9, 4732.
24. Bolbot, V.; Theotokatos, G.; Boulougouris, E.; Psarros, G.; Hamann, R. A Novel Method for Safety Analysis of Cyber-Physical Systems—Application to a Ship Exhaust Gas Scrubber System. *Safety* **2020**, 6, 26.
25. Banda, O.A.V.; Goerlandt, F.; Salokannel, J.; van Gelder, P.H. An initial evaluation framework for the design and operational use of maritime STAMP-based safety management systems. *WMU J. Marit. Aff.* **2019**, 18, 451–476.
26. Zhou, Z.; Zi, Y.; Chen, J.; An, T. Hazard Analysis for Escalator Emergency Braking System via System Safety Analysis Method Based on STAMP. *Appl. Sci.* **2019**, 9, 4530.
27. Nan, Q.; Liang, M. Safety Requirements Analysis for a Launching Control System Based on STPA. In Proceedings of the 2019 IEEE International Conference on Mechatronics and Automation (ICMA), Tianjin, China, 4–7 August 2019; pp. 1201–1205.
28. Jiang, W.; Han, W.; Zhou, J.; Huang, Z. Analysis of Human Factors Relationship in Hazardous Chemical Storage Accidents. *Int. J. Environ. Res. Public Health* **2020**, 17, 6217.
29. Feng, T.; Wang, L.; Hu, J.; Chen, M. A Safety Analysis Method for FGS Based on STPA. In *Advances in Intelligent, Interactive Systems and Applications. IISA 2018. Advances in Intelligent Systems and Computing*; Xhafa, F., Patnaik, S., Tavana, M., Eds.; Springer: Cham, Switzerland, 2018; Volume 885; pp. 936–944.
30. Schmid, D. Pilot Homicide-Suicide: A System-Theoretic Process Analysis (STPA) of Germanwings GWI18G. In *Advances in Human Aspects of Transportation. AHFE 2018. Advances in Intelligent Systems and Computing*; Stanton, N., Ed.; Springer: Cham, Switzerland, 2019; Volume 786.
31. Hardy, K.; Guarnieri, F. Using STAMP in the Risk Analysis of a Contaminated Sediment Treatment Process. In *Safety Dynamics. Advanced Sciences and Technologies for Security Applications*; Guarnieri, F., Garbolino, E., Eds.; Springer: Cham, Switzerland, 2019.
32. Samadi, J.; Garbolino, E. Systemic Risk Management Approach for CTSC Projects. In *Safety Dynamics. Advanced Sciences and Technologies for Security Applications*; Guarnieri, F., Garbolino, E., Eds.; Springer: Cham, Switzerland, 2019.
33. Yang, P.; Karashima, R.; Okano, K. Automated inspection method for an STAMP/STPA-fallen barrier trap at railroad crossing. *Procedia Comput. Sci.* **2019**, 159, 1165–1174.
34. MIL-STD-1629A. *Procedures for Performing a Failure Mode, Effects and Criticality Analysis*; U.S. Department of Defense: Washington, DC, USA, 1980.

35. I.E.C. 60812: 2018. Analysis Techniques for System Reliability-Procedure for Failure Mode and Effects Analysis (FMEA). Available online: http://www.iec.ch (accessed on 10 August 2018)
36. Monkhouse, H.; Habli, I.; Mcdermid, J. The Notion of Controllability in an autonmous vehicle context. In *CARS 2015-Critical Automotive Applications*; Robustness & Safety: Paris, France, 2015.
37. Thomas, J. Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis. Ph.D. Thesis, Massachusetts Inst. Technol., Cambridge, MA, USA, 2013.
38. Dardar, R. Building a Safety Case in Compliance with ISO26262 for Fuel Level Estimation and Display System. Master's Thesis, Mälardalen University, School of Innovation, Design and Engineering, Västerås, Sweden, 2014.
39. Rastayesh, S.; Bahrebar, S.; Blaabjerg, F.; Zhou, D.; Wang, H.; Dalsgaard Sørensen, J. A System Engineering Approach Using FMEA and Bayesian Network for Risk Analysis—A Case Study. *Sustainability* **2020**, 12, 77–89.