Dealing with Functional Safety Requirements for Automotive Systems: A Cyber-Physical-Social Approach

Conference Paper · October 2017

CITATIONS
3

READS
195

4 authors:

Mohamad Gharib
University of Florence
25 PUBLICATIONS **78** CITATIONS
SEE PROFILE

Paolo Lollini
University of Florence
92 PUBLICATIONS **387** CITATIONS
SEE PROFILE

Andrea Ceccarelli
University of Florence
82 PUBLICATIONS **388** CITATIONS
SEE PROFILE

Andrea Bondavalli
University of Florence
343 PUBLICATIONS **2,578** CITATIONS
SEE PROFILE

Dealing with Functional Safety Requirements for Automotive Systems: A Cyber-Physical-Social Approach

Mohamad Gharib, Paolo Lollini, Andrea Ceccarelli, Andrea Bondavalli

University of Florence - DiMaI, Viale Morgagni 65, Florence, Italy
{mohamad.gharib,paolo.lollini,andrea.ceccarelli,andrea.bondavalli}@unifi.it

Abstract. Road transport system is an essential infrastructures in the world, where the majority of the population use its facilities on a daily basis. That is why ensuring their safety has been always a growing concern for most authorities. The automotive industry is already aware of that, and the ISO 26262, a standard for developing functional safety systems for vehicles, has been developed. Although current studies have shown that the root cause for most of the accidents has shifted from vehicle-centric to driver-centric, the main objective of ISO 26262 is covering electronic and electric (E/E) systems of vehicles with almost no emphasis on the driver itself. To this end, we propose a holistic approach based on the ISO 26262 standard that not only considers the E/E systems of the vehicle but also the driver's behaviour. We illustrate the utility of the approach with an example from the automotive domain.

Keywords: Transport, Automotive systems, Functional safety requirements, ISO 26262, Cyber-Physical-Social systems

1 Introduction

Automotive systems can be described as safety-critical systems, which have to fulfil safety requirements in addition to functional requirements [1]. More specifically, safety requirements describe the characteristics that a system must have in order to be safe [1], and it is a crucial property that must be ensured to avoid or mitigate any potentially unacceptable hazards events [2]. Failing to comply with safety requirements leave the system open to various kinds of vulnerabilities that might endanger the safety of its users. Therefore, it is very important to consider safety requirements during the design and development of automotive systems to reduce the risk of hazards events occurrence [3].

The automotive industry is already using safety analysis, validation and verification techniques to increase vehicle safety. Moreover, the ISO 26262 [4], a functional safety standard has been developed, which provides appropriate development processes, requirements and safety integrity levels specific for the automotive manufacturer. However, ISO 26262 has been mainly developed to cover E/E systems of vehicles and it assumes that vehicle drivers can perform the necessary actions to stay safe. But this is not always the case, since several studies

have shown that drivers are the main reason for many accidents [5,6], i.e., the challenges of vehicle safety are more than purely technical. In this context, the focus should be on mitigating the root cause of these accidents (i.e., drivers) [5]. Therefore, to design an effective safety automotive system, the driver behaviour should be better understood, modeled and considered during the system design.

Driving is a situation awareness process, and more than half of the crashes that require the driver awareness were caused by driver inattention and/or distraction [8]. Although modeling the driver behaviour is not new, it has not been considered in well-adopted standards such as ISO 26262. We advocate that integrating the social (driver behaviour) and technical (E/E systems) components of automotive systems during the system design is essential for the development of safer systems. More specifically, an approach that addresses the driver behaviour along with the E/E systems of the vehicle can significantly improve the safety of road transport system [6]. To this end, we propose a holistic approach based on the ISO 26262 standard that not only considers the E/E systems of the vehicle but also the driver and his behaviour as an integral of the system.

The rest of the paper is organized as follows; Section (§2) presents the research background, and we describe an illustrative example in Section (§3). In Section (§4), we present our approach for dealing with functional safety requirements, and we apply it to the illustrative example in (§5). Related work is presented in Section (§6), and we conclude and discuss future work in Section (§7).

2 Background

1. ISO 26262 [4] is a functional safety standard that has been developed with a main objective to provide guidelines and best practices to increase the safety of E/E systems in vehicles. It covers the overall automotive safety life cycle including specification, design, implementation, integration, verification and validation. ISO 26262 focuses on the hazards of the E/E systems and their associated risks. The associated risks are then assigned an Automotive Safety Integrity Level (ASIL). The ASILs can be classified under, Quality Management (QM[1]), ASIL A, ASIL B, ASIL C, and ASIL D, where ASIL D requires the highest risk reduction effort. Table 1 shows the clauses of ISO 26262 relevant to this paper.
2. Cyber-Physical-Social Systems (CPSSs) can be described as systems consisting of cyber components (e.g., computer system), controlled components (e.g., physical objects) and interacting social components (e.g., humans). For example, a vehicle is seen as a combination of cyber components (e.g., software, sensors, actuators), controlled components (e.g., other vehicles, road objects) and interacting social components (e.g., drivers, passengers, pedestrian). Ensuring the safety of a CPSS requires considering the three main components along with their interactions. For instance, we cannot guarantee the safety of such system by considering only its cyber and/or controlled components since many safety related hazards might be due to its social components, and vice versa.

[1] QM is assigned to hazards with very low probability or causing only slight injuries

Table 1. Clauses of ISO 26262 we consider in this paper

Clause	Description
3-5	**Item definition,** aims to develop a description of the item with regard to its functionality, interfaces, known hazards, etc.
3-6	**Hazard Analysis and Risk Assessment (HARA),** aims to estimate the probability of exposure, controllability and severity of hazardous events with regard to the item. Based on these parameters, the ASILs of the hazardous events are determined and then assigned to corresponding safety goals.
3-7	**Functional safety concept** is developed by deriving functional safety requirements from safety goals and allocating them to the elements of the item.
4-6	**Technical safety concept,** aims to specify the technical implementation of the functional safety concept, and to verify that the technical safety requirements comply with the functional safety requirements.
5-6	**Specification of Hardware Safety Requirements (HWSRs)**, aims to provide specifications on how to elicit and manage the HWSRs.
6-6	**Specification of Software Safety Requirements (SWSRs)**, aims to provide specifications on how to elicit and manage the SWSRs.
4-9	**Safety validation,** aims to provide evidence that the safety goals are adequate, can be achieved at the vehicle level, and the safety concepts are appropriate for the functional safety of the item.

3 Illustrative Example: Maneuver Assistance System

Although most Advanced Driver Assistance Systems (ADAS) are developed to meet specific functional safety requirement provided by ISO 26262, they are developed with the implicit assumption that driver's actions are intended. Therefore, the focus of this example is on driver's unintended actions that may result due to its lack of awareness (inattention or distraction). Our example concerns the Maneuver Assistance System (MAS), which is expected to increase the driver's safety by monitoring its behaviour, detecting unintended maneuvers, and respond in a way that guarantees the highest possible level of driver safety.

In [9], three different types of maneuvers have been identified: 1- *strategically-planned* are associated with long-term time scale (minutes or hours), and they are motivated by destination goal of the driver; 2- *tactical-planned* are associated with a short-term timescale (few tens of seconds), and they are motivated by a recently modified desire of the driver (e.g., lane changes, turns, upcoming exit); 3- *operational* are associated with a very short time scale (hundreds of milliseconds), and they are generally a result of a driver's desire to remain safe.

We will focus on the last two types of maneuvers since the first one does not involve safety-critical situation. In both of them, the MAS is expected to collect information about the vehicle, vehicle surroundings, as well as driver behaviour. Then, it analyzes such information to determine whether the driver's maneuver (action) is intended or unintended. More specifically, when the analysis determines that there is a need, desire and/or a motivation for the maneuver, it is considered as an *intended* maneuver. Otherwise, it is considered as an *unintended* one. Consequently, MAS should either allow or halt the maneuver.

4 A Holistic Approach to Deal with Functional Safety Requirements for Automotive Systems

Our approach adopts and extends the ISO 26262 standard to consider both the E/E systems of the vehicles along with the driver's behaviour. The process underlying our approach (depicted in Figure 1[2]) consists of eight main activities. Activities 1, 2, 3, 4, and 8 are based on ISO 26262 clauses C.3-5, C.3-6, C.3-7, C.4-6, and C.4-9 respectively, and they have been extended to consider the driver behaviour. Activities 5 & 6 are based on clauses C.5-6 and C.6-6 respectively, and activity 7 is a new activity that focuses mainly on the specification of social safety requirements. In what follows, we discuss each of these activities.

1- Item definition is the first activity of the process, and it aims to define the item in terms of its main functionalities, interfaces, known hazards, its dependencies and interactions with the environment [4]. In our approach, this activity is extended to consider the driver as an integral part of the item, i.e., dependencies and interactions between the driver (social component) and the cyber and physical components of the item are considered as well during the definition of the item. The outcome of this activity is the item definition.

2- Hazard Analysis and Risk Assessment (HARA), which can be started when the item definition is considered complete. HARA activity can be divided into two related sub-activities, 1- hazard analysis, in which the item definition is used to identify possible hazards events. Since the driver is considered as an integral part of the item, this activity should consider the hazards that may result from their behaviour and interactions/dependencies with other components of the item. 2- risk assessment, in which the identified hazards events are categorized based on three variables. 1- *Severity,* measures the potential harm for each hazardous event, and it can range from S0 to S3, where S0 means no injuries and S3 means life-threatening injuries. 2- *Exposure,* measures the probability of the item being in an operational situation that is described in the hazardous event, and it can range from E0 to E4, where E0 means the lowest occurrence probability and E4 means high probability. 3- *Controllability,* measures the ability to avoid a specified *harm/damage* through the timely reactions of the persons involved, and it ranges from C0 to C3, where C0 means controllable in general and C3 means difficult to control or uncontrollable.

Based on these three parameters, an ASIL is assigned for each hazard. ASIL is a measure of necessary risk reduction, and its level range from QM, ASIL A, ASIL B, ASIL C, and ASIL D, where ASIL D is the highest. Then, at least one Safety Goal (SG)[3] is assigned to each hazard rated as ASIL A, B, C or D as it is required by ISO 26262. These SGs can be used to derive the Functional Safety Requirements (FSRs), which specify the functionality required to mitigate their corresponding hazard. The outcome of this activity is SGs.

3- Functional safety concept, the main objective of this activity is developing the functional safety concept by deriving FSRs from the SGs, and then allocat-

[2] P. and C. represent the Parts and Clauses of ISO 26262 respectively

[3] A SG may cover multiple hazardous events

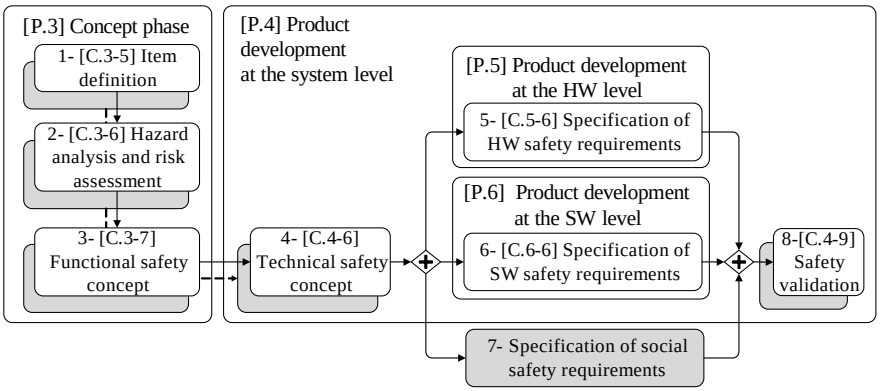

Fig. 1. A process compliant with ISO 26262 for dealing with FSR

ing FSRs to the elements of the item. According to ISO 26262, FSRs are specification(s) of implementation-independent safety behaviour/safety measure(s), including their safety-related attributes. Therefore, FSRs are used for defining the safety functionalities of the item without specifying how such functionalities can be implemented. Unlike ISO 26262, this activity should specify the FSRs taking into consideration the behaviour of driver with a special emphasis on its interaction/dependencies with other components of the item, which facilitates the allocation of the FSRs to the elements of the item in latter activities.

4- Technical safety concept aims to derive the Technical Safety Requirements (TSRs) from the FSRs. In particular, FSRs might be at a high level of abstraction, and they need to be refined into more detailed technical requirements. Similar to activity 4, this activity should specify the TSRs in a way that provides more detailed information about the driver behaviour along with its interaction/dependencies with other components of the item. Note that fulfiling the complete set of TSRs is considered sufficient to ensure that the item is compliant with its functional safety concept.

5- Specification of Hardware Safety Requirements (HWSRs) aims to derive HWSRs from TSRs that can be allocated to hardware. The HWSRs are safety requirements related to the physical hardware of the item. According to ISO 26262, HWSRs shall include information about each hardware requirement that relates to functional safety, including relevant attributes of safety mechanisms to a) control internal failures of the hardware of the element; b) control or tolerate failures external to the element; c) comply with the safety requirements of other elements; and d) detect and signal internal or external failures. In addition, criteria for design specification & verification of the hardware elements of the item shall be specified at this activity.

6- Specification of Software Safety Requirements (SWSRs) aims to derive SWSRs from TSRs that can be allocated to software. The SWSRs are safety requirements related to the software functionality of the item. According to ISO 26262, SWSRs shall be derived from TSRs considering the required safety-related

functionalities and properties of the software, whose failures could lead to violations of a technical safety requirement allocated to software. Then, SWSRs can be used to define software design specification.

7- Specification of SoCial Safety Requirements (SCSRs) aims to derive SCSRs from TSRs that can be allocated to the driver's social behaviour. The SCSRs are safety requirements related to the social aspects of the item. Unlike the previous two activities, this activity is not based on any of the ISO 26262 clauses. Yet it follows the same pattern of activity 5 & 6, i.e., SCSRs also use TSRs to define clear design specification concerning the driver's behaviour and its interactions and dependencies with other components of the item.

8- Safety validation aims to 1- provide evidence that the safety goals are adequate, 2- provide evidence that the safety goals are achieved at the vehicle level, and 3- provide evidence that the safety concepts are appropriate for the functional safety of the item.

5 The Application of the Approach to the MAS Example

In this section, we apply our approach to the MAS example.

1- Item definition. The main function of MAS is to allow/prevent intended/unintended drivers' tactical and operational maneuvers when the vehicle is moving faster than 50 km/h. MAS depends on sensors to collect informational cues about the driver: 1- head pose and motion, which can be used to identify the driver's visual orientation, and predict some driver's maneuvers, e.g, head motion may precede a maneuver; 2- hands/foot location and motions, which can be used to predict some driver's actions. Moreover, MAS depends on LIDAR and Radar, which can provide information about surrounding vehicles/objects. In addition, MAS will include software system that enables for analyzing all cue information in appropriate time to determine whether a driver's maneuver is intended, i.e., it is a result of a need, desire and/or a motivation, or it is unintended, i.e., there is no need, desire and/or a motivation to perform such maneuver. Finally, MAS depends on lock actuator to prevent a driver's unintended maneuvers.

2- Hazard analysis and risk assessment. This activity has two sub-activities:

1- Hazard identification. It analyzes the item definition focusing mainly on hazard events that may result due to the behaviour of the item components along with their interaction and dependencies. Two main hazards[4] related to MAS have been identified:

H1: categorizing an intended maneuver as an unintended one when the vehicle is moving faster than 50 km/h, which prevents the driver from performing an intended maneuver.

H2: categorizing an unintended maneuver as an intended one when the vehicle is moving faster than 50 km/h, which allows an unintended maneuver to be performed.

[4] The identified hazards are not complete nor exclusive due to space limitation

2- Risk assessment. Each identified hazard is categorized based on its severity, exposure and controllability.

The occurrence of **H1** prevents a driver from performing an intended maneuver, which may lead to life-threatening injuries or even death. Therefore, the highest severity level (S3) is chosen. The exposure level E3 (medium probability) is chosen because several reasons could result in categorizing an intended maneuver as an unintended one (e.g., wrong informational cues about the head pose and motion, hands/foot location). Finally, the highest controllability level C3 is chosen since the driver will not have the required time to perform any corrective action to avoid a potential harm. Based on the severity (S3), exposure (E3) and controllability (C3) of **H1**, ASIL C is determined for this hazard.

Similarly, the occurrence of **H2** is of highest severity level (S3) because allowing an unintended maneuver to be performed may lead to life-threatening injuries or even death. The exposure level is of a medium probability (E3) since identifying the unintended might be mistaken due to wrong informational cues. Moreover, the highest controllability level C3 is chosen since the driver might not be aware of such maneuver to perform any corrective action to avoid a potential harm/ damage. Hence, ASIL C is determined for this hazard. Following our approach, at least one Safety Goal (SG) should be assigned to each hazard rated as ASIL A, B, C or D. To this end, we assign the following two SGs (SG1 and SG2) to hazards **H1** and **H2** respectively:

SG1: a driver intended maneuver shall not be prevented when the vehicle is moving faster than 50 km/h.

SG2: a driver unintended maneuver shall be prevented when the vehicle is moving faster than 50 km/h.

3- Functional safety concept. Based on the **SGs** identified in the previous activity we derive the related Functional Safety Requirements (FSRs). In particular, we derive the following FSRs from **SG1**:

- **FSR1.1:** MAS shall be activated when the vehicle is moving faster than 50 km/h.
- **FSR1.2:** MAS shall be able to collect all related cue information to determine whether there is a need for a maneuver.
- **FSR1.3:** MAS shall be able to collect all related cue information to determine whether the driver has a desire or a motivation to make a maneuver.
- **FSR1.4:** MAS shall be able to verify whether the driver's maneuver is intended within an appropriate time.
- **FSR1.5:** MAS shall not prevent intended maneuvers.

From **SG2**, we derive the following FSRs[5]:

- **FSR2.1:** MAS shall be able to identify drivers unintended maneuvers within an appropriate time.

[5] **FSR1.1**, **FSR1.2**, **FSR1.3** can also be derived from SG2, but since ISO 26262 requires to keep the FSRs list atomic, they are not derived again from **SG2**.

– **FSR2.2:** MAS shall prevent unintended maneuver.

4- Technical safety requirements. The main purpose of this activity is refining the FSRs identified in the previous activity into more detailed technical requirements. The process of deriving the TSRs is similar to the process of deriving the FSRs from SGs, yet ISO 26262 does not require that for each FSR at least one TSR should be defined. It only requires that TSRs should be specified in accordance with FSRs. Based on the FSRs identified in the previous activity, we derive the following TSRs:

– **TSR1.1.1:** MAS shall depend on reliable sensor(s) to identify vehicle speed and activate/deactivate MAS when the vehicle is moving faster/slower than 50 km/h.
– **TSR1.1.2:** MAS shall depend on reliable technique(s) (e.g., sensors, LIDAR, Radar) that allows to predict needed operational maneuvers.
– **TSR1.1.3** MAS shall depend on reliable technique(s) (e.g., head pose and motion, hands and foot location and motions) that allows predicting desired and/or motivated tactical maneuvers.
– **TSR1.1.4:** MAS shall be able to verify whether the driver's operation maneuvers are needed within an appropriate time.
– **TSR1.1.5:** MAS shall be able to verify whether the driver's tactical maneuvers are desired and/or motivated within an appropriate time.
– **TSR1.1.6:** MAS shall not prevent needed operational maneuvers.
– **TSR1.1.7:** MAS shall not prevent desired and/or motivated tactical maneuvers.
– **TSR1.2.1:** MAS shall depend on reliable technique(s) that allows identifying unneeded operational maneuvers.
– **TSR1.2.2:** MAS shall depend on reliable technique(s) that allows identifying undesired and/or unmotivated tactical maneuvers.
– **TSR1.2.3:** MAS shall prevent unneeded operational maneuvers.
– **TSR1.2.4:** MAS shall prevent undesired and/or unmotivated tactical maneuvers.

5- Specification of Hardware Safety Requirements (HWSRs). After identifying the TSRs list, TSRs that can be allocated to the physical hardware of the item are used to derive the specification of HWSRs. Based on the TSRs identified in the previous activity, we derive the following HWSRs:

– **HWSR.001:** Each hardware component of/related to MAS (e.g., sensors, actuators, radars, etc.) shall be described by its hardware safety requirements and relevant attributes of safety mechanisms to control internal failures.
– **HWSR.002:** Each hardware component of/related to MAS shall be described by its hardware safety requirements and relevant attributes of safety mechanisms to control or tolerate failures external to the element.
– **HWSR.003:** Each hardware component of/related to MAS shall be described by its hardware safety requirements and relevant attributes of safety mechanisms to comply with the safety requirements of other elements.

- **HWSR.004:** Each hardware component of/related to MAS shall be able to deal with any disturbances/noise on their inputs.
- **HWSR.005:** Each hardware component of/related to MAS shall not allow any unintended signal on their outputs.
- **HWSR.006:** Each hardware component of/related to MAS shall be described by its hardware safety requirements and relevant attributes of safety mechanisms to detect and signal internal or external failures.
- **HWSR.007:** Any communication errors/lost between hardware components of/related to MAS shall be identified.
- **HWSR.008:** Any unusual behaviour of each hardware component of/related to MAS that may result due to error, fault or a failure shall be identified by diagnosing their inputs/outputs signals.
- **HWSR.009:** Each hardware component of/related to MAS should be tested in an environment complying with the same real environmental it might function in.
- **HWSR.010:** Communications and dependencies among hardware components of/related to MAS should be tested in an environment complying with the same real environmental it might function in.

6- Specification of Software Safety Requirements (SWSRs). After identifying the TSRs list, TSRs that can be allocated to the software functionality of the item are used to derive the specification of SWSRs. Based on the TSRs identified in the previous activity, we derive the following SWSRs:

- **SWSR.001:** MAS shall be able to detect and appropriately communicate any error in signals received from its related component (e.g., sensors, actuators, radars, etc.).
- **SWSR.002:** MAS shall be able to detect any delay, loss, corruption in signals received from its related components.
- **SWSR.003:** MAS shall be able to detect if any of its related components is not responding and/or is not responding in an appropriate time.
- **SWSR.004:** MAS shall implement a mitigation plan to deal appropriately with any error, delay, loss, corruption in signals received from its related component.
- **SWSR.005:** MAS shall be able to detect errors, faults, malfunctions in its related components that might lead to failures.
- **SWSR.006:** MAS shall implement a mitigation plan to deal appropriately with errors, faults, malfunctions in its related components in order to avoid potential failures.
- **SWSR.007:** MAS shall assign a special code for each error, faults, malfunctions, etc., which enables to easily identify them and differentiate them from one another.
- **SWSR.008:** MAS safety-related software functionalities and properties concerning timely response should be tested in an environment complying with the same real environmental it might function in.

– **SWSR.009:** MAS safety-related software functionalities and properties (e.g., robustness against erroneous inputs, fault tolerance capabilities of the software, etc.) should be tested in an environment complying with the same real environmental it might function in.

7- Specification of SoCial Safety Requirements (SCSRs). After identifying the TSRs list, TSRs that can be allocated to the driver's social behaviour of the item are used to derive the SCSRs.

– **SCSR.001:** MAS shall be able to identify available information concerning the driver state (e.g., head pose and motion, hands and foot location and motions) at any point in time.
– **SCSR.002:** MAS shall be able to collect all possible information concerning the driver state at any point in time.
– **SCSR.003:** MAS shall be able to evaluate the correctness of collect cues information concerning the driver state.
– **SCSR.004:** MAS shall be able to fuse all available cues information to determine the driver awareness state (e.g., attention, inattention) within an appropriate time.
– **SCSR.005:** MAS shall be able to fuse all available cues information to predict whether a driver tactical maneuver is desired and/or motivated with respect to cue information collected from driver state, vehicle (e.g., speed) and vehicle environment (e.g., LIDAR and Radar information) within an appropriate time.
– **SCSR.006:** MAS shall be able to determine whether a driver's tactical maneuver is intended within an appropriate time.
– **SCSR.007:** MAS shall be able to fuse all available cues information to determine whether a driver's operational maneuver is needed with respect to cue information collected from driver state, vehicle and vehicle environment within an appropriate time.
– **SCSR.008:** MAS shall be able to implement the lock actuator to prevent a driver's unintended (operational/tactical) maneuver within an appropriate time.
– **SCSR.009:** Each technique/mechanism that is used for determining the driver awareness state, predicting driver tactical maneuver, evaluating whether a driver's tactical maneuver is intended, determining whether a driver's operational maneuver is needed should be tested in an environment complying with the same real environmental it might function in.
– **SCSR.010:** The implementation of the actuator mechanism to prevent a driver's unintended operational/tactical maneuver should be tested in an environment complying with the same real environmental it might function in.

8- Safety validation. The main purpose of this activity is assuring that the safety goals are sufficient and have been achieved, based on examination and tests, providing reliable evidence that the identified safety goals have been realized at the vehicle level. Such validation can only be performed on a complete

implementation of the proposed system, which is outside of the scope of this paper. In our approach, we validated the results by manually reviewing the derived HWSRs, SWSRs, and SCSRs lists, which if realized appropriately can fulfil the TSRs. In turn, fulfiling the complete set of TSRs is considered sufficient to ensure that the item is compliant with its functional safety concept.

6 Related Work

Several works for dealing with functional safety requirements for automotive systems have been proposed. For example, Jesty et al. [10] propose guidelines for hazard identification and analysis, and identifying the safety integrity levels. Giese et al. [11] develop an approach for systematically identifying which hazards/failures are most critical, which components require a more detailed safety analysis, and which restrictions to the failure propagation should be considered. Zhang et al. [3] introduce a comprehensive hazard analysis method based on functional models. Li and Zhang [12] present a software hazard analysis method for automotive control systems that extends the traditional software development process to incorporate safety procedures as a fundamental part of the process.

While Basir et al. [13] propose an approach that adopts the Goal Structuring Notation (GSN) to construct safety cases. In which, the defined safety cases reflect the results of the system analysis and provide a high-level argument that traces the requirements on the model via inferred model structure to code. Palin et al. [14] provide guidelines, patterns, and a number of reusable safety arguments covering all parts of ISO 26262 for creating safety cases. Habli et al. [15] examine how model-driven development and assessment can provide a basis for the systematic generation of functional safety requirements. Finally, Mehrpouyan et al. [16] introduce a model-based hazard analysis methodology that maps hazard and vulnerability models to specific components in the system and analyzes the hazard propagation paths for risk control and protection strategies.

To the best of our knowledge, no existing work extends the ISO 26262 standard by integrating the driver and his behaviour as an integral part of the item.

7 Conclusions and Future Work

We discussed the limitation in the current standard (ISO 26262) for developing functional safety systems for vehicles, which mainly cover E/E systems of vehicles. Therefore, we proposed a holistic approach built based on the ISO 26262 standard and considers both the E/E systems and the driver's behaviour. We described the approach in terms of its main activities, and we have illustrated its utility by applying it to an example from the automotive domain.

For future work, we intend to formalize all the previously introduced concepts and develop SysML profiles based on them, which allows for modeling FSRs, derive the TSRs, and then derive the HWSRs, SWSRs, and SCSRs from TSRs. Moreover, we are planning to propose a set of Object Constraint Language

(OCL) constraints for specifying rigorous rules for the derivation of HWSRs, SWSRs, and SCSRs from TSRs, and the derivation of TSRs from FSRs.

Acknowledgment

This work has been partially supported by the "Ente Cassa Di Risparmio di Firenze", Bando per progetti 2016, and by the FAR-FAS 2014 TOSCA-FI project funded by the Tuscany Region.

References

1. Ridderhof, W., Gross, H.G., Doerr, H.: Establishing evidence for safety cases in automotive systems–A case study. In: International Conference on Computer Safety, Reliability, and Security (SAFECOMP), Springer (2007) 1–13
2. Törner, F., Öhman, P.: Automotive Safety Case A Qualitative Case Study of Drivers, Usages, and Issues. In: 11th HASE, IEEE, (2008) 313–322
3. Zhang, H., Li, W., Chen, W.: Model-based hazard analysis method on automotive programmable electronic system. In: International Conference on Biomedical Engineering and Informatics (BMEI), IEEE (2010) 2658–2661
4. ISO: 26262: Road vehicles-Functional safety. IS ISO/FDIS **26262** (2011)
5. McCall, J.C., Trivedi, M.M.: Driver behavior and situation aware brake assistance for intelligent vehicles. PROCEEDINGS-IEEE **95**(2) (2007) 374
6. Taib, R., Yu, K., Jung, J., Hess, A., Maier, A.: Human-centric analysis of driver inattention. In: Intelligent Vehicles Symposium Workshops, IEEE (2013) 7–12
7. Dong, Y., Hu, Z., Uchimura, K., Murayama, N.: Driver Inattention Monitoring System for Intelligent Vehicles: A Review. IEEE Transactions on Intelligent Transportation Systems **12**(2, SI) (2011) 596–614
8. Lee, J.D., Young, K.L., Regan, M.A.: Defining driver distraction. Driver distraction: Theory, effects, and mitigation **13**(4) (2008) 31–40
9. Tawari, A., Sivaraman, S., Trivedi, M.M., Shannon, T., Tippelhofer, M.: Looking-in and looking-out vision for urban intelligent assistance: Estimation of driver attentive state and dynamic surround for safe merging and braking. In: Intelligent Vehicles Symposium Proceedings, IEEE (2014) 115–120
10. Jesty, P.H., Hobley, K.M., Evans, R., Kendall, I.: Safety analysis of vehicle-based systems. In Proceedings of the Safety-critical Systems Symposium, (2000), 90–110
11. Giese, H., Tichy, M., Schilling, D.: Compositional Hazard Analysis of UML Component and Deployment Models. In: SAFECOMP, Springer (2004) 166–179
12. Li, W., Zhang, H.: A software hazard analysis method for automotive control system. In: International Conference on Computer Science and Automation Engineering (CSAE) . Volume 3., IEEE, (2011) 744–748
13. Basir, N., Denney, E., Fischer, B.: Deriving safety cases for hierarchical structure in model-based development. In: SAFECOMP, Springer (2010) 68–81
14. Palin, R., Ward, D., Habli, I., Rivett, R.: ISO 26262 safety cases: Compliance and assurance. In: International Conference on System Safety, (2011) 1–6
15. Habli, I., Ibarra, I., Rivett, R.S., Kelly, T.: Model-Based Assurance for Justifying Automotive Functional Safety. Technical report, SAE Technical Paper (2010)
16. Mehrpouyan, H., Bunus, P., Kurtoglu, T.: Model-based hazard analysis of undesirable environmental and components interaction. In: Aerospace Conference, IEEE (2012) 1–8