

Evaluation of Safety Cases in The Domain of Automotive Engineering

Venkata Satya Rahul Kosuru
Independent Researcher
MS (Electrical and Computer Engineering)
Sunnyvale, CA – 94085, USA

Ashwin Kavasseri Venkitaraman
Independent Researcher
MS (Electrical Engineering)
Fremont, CA- 94536, USA

Abstract:- Manufacturers of automobiles have been under intense pressure from the demand laws and market needs to develop complex and feature-rich vehicles. Such kind of new functionality play an active role significantly in driving which is possessing new difficulties in ensuring the vehicle's safety. The cases of safety primary constitute a technique proven to systematically utilize the information in existence about the system, its context of development and environment so that its safety can be shown. In this paper, there is presentation of a safety case construction for a vehicles cruise control system with the concentration on the automotives' domain-specific models. In the study, there was identification of generic case modules of safety as well as several patterns which reoccur and will assist in the simplification of the future automotive safety cases development.

Keywords:- Functional Safety, ASIL Integrity, Fault Mitagation, Risk and Hazard Analysis and, Severity of exposure.

I. INTRODUCTION

Functional Safety refers to the unreasonable risk absence because of the hazards caused by the behavior of manufacturing of the electronic/ electrical systems. The primary objective of ISO 26262 is ensuring that safety factors are considered from the earliest concepts to the retirement point of the vehicle. To ensure safety of the vehicle, the life cycle of automotive safety in standard outline would capture description of the entire life cycle production. There are requirements of specific steps in each phase of the life cycle of safety (Becker et al.2018). One of the steps which is most important at the life cycle of safety start is the Risk and Hazard Analysis of the potential hazards commonly referred to as the HARA stage. This results into a system of integration known as ASIL or classification system of an Automotive Safety Integrity Level for the hazards and the overall safety formulation. The goals of safety primarily refer to the safety levels required by a component or a system to function without necessarily posing threats to the entire vehicle.

II. BACKGROUND INFORMATION

The assignment of an ASIL is through evaluation of the three parameters of risks, exposure, severity, and controllability. Severity in this case refers or considers the impacts to the people's life because of the potential failure. Exposure is primarily targeting the likelihood of the conditions under which the failure would practically results into the safety hazards. Controllability on the other hand determines the degree with which the driver will be in a position of controlling the vehicle should there be a breach to the goals of safety because of malfunctioning or failure. The method of ISO 26262 assists in the provision of guidance on the way the assignment of ASIL is to be done for the hazard once exposure, severity as well as controllability are obtained (Iturbe et al.2018).

In the next step, there is concept development of a functional safety for each safety goal. The concept of the functional safety defines the requirements of functional safety within the context of the architecture of the vehicle including detection of the fault as well as mechanisms of failure mitigation to ensure satisfaction of the goals of safety. Then there is development of the concept of technical safety to specify the requirements of technical safety within the architecture of the system. The concept of the technical safety is the basis for the derivation of software and hardware requirements which are utilized in the product development. The requirement of safety needs to be traced, validated, and properly managed through the development of the product to ensure that the product is delivered as safe as possible.

III. OBJECTIVES AND RESEARCH STUDY

The objective of this research will be primarily to establish safety assurance methods which are usable for the systems of automotives involving software. In particular, the aim is discovering reusable patterns, structures as well as processes in the safety assurance which supports certain practical applications in Automotive Electronics Engineering.

❖ *Research Questions*

- What are some of the possible cases of safety of modules in the domain of automotives engineering?
- What are some of the reoccurring patterns in cases of safety in the automotives engineering?
- How can cases of safety utilizing existing domain –specific models in the automotives engineering or automotive domain be improved?

IV. METHODOLOGY ON CASE CONSTRUCTION

A. Subject Selection

In this research, there was selection of one case as well as several subjects opportunisticly. The study has utilized a 3-step process for the construction of cases of safety for real components of automotives. Particularly, there was investigation of the applications and structure of the models which guide the safety cases construction. The top-down process for the argumentation about requirements of safety and legible argumentation involved

B. Safety Case Identification

- Identification of hazards
- Eliciting requirements of the system to help in hazards avoidance.
- Breaking down the system’s requirements up to the point of component realization through use of the following argumentations:
 - Evidence provision that realization of the component meets the requirements imposed
 - Derivation of Functional safety requirements for system level (Hardware and Software)
 - Derivation of Technical safety requirements for system level (Hardware and Software)
 - Derivation of sub-system safety requirements (Software-Safety Requirements) and (Hardware – Design Safety Requirements)
 - Splitting the hardware components into sub-components, requirement definition as in continuation of step (iii)
 - Splitting requirements into other sub-units as for the step (iii)
 - Derive the requirements for Fault Tolerant Time Interval of a potential hazard cause dues to fault in (hardware or software). Where Fault Tolerant Time Interval (FTTI) shall always be greater than sum of Fault Occurrence (FO) + Fault Detection Time (FDT) + Fault Reaction Time (FRT)

V. CONSTRUCTION OF SAFETY USE CASE

For the control of cruise, the construction of the case of safety was primarily instantiated as follows:

A. Hazard Identification

The hazard analyzed was that the vehicle’s speed was higher than that which had been set by the driver. For the cruise control, it would be considered as the most relevant hazard since excessive speed maybe subject to other consequences legally besides leading to harm of the equipment and persons.

Eliciting requirements of the systems as way of avoiding the hazards: With the help of the car’s conceptual model as well as the environment itself, there was eliciting several requirements needed by the car to ensure avoidance of hazard. The point of focus therefore was to ensure that the car never increases in speed in case it reaches the speed target (Chen, Jiao, and Zhao 2020).

Breaking down the requirements of the system: There was consideration of the functional models on the subsystem, systems, and function level. Here, the subsystem and system model assist in:

- Differentiating between the cars provided acceleration and environment in the case of declining roads
- Identification of the abstract functionality of the engine as the single point for the provided acceleration of the car.
- Identification of the split sub-requirements between the subsystems
- Splitting between electrics, mechanics, and software functions regarding cruise control as a correspondence to a single functional model in the form of software function actual realization.

B. Modular Construction of The Safety Case Study

In the considered case study, the cruise control functionality depends on the target speed and current speed of input signals accuracy and validity. To allow for the provision of safety arguments for the case that such kind of the signals are never correct, there was employment of fault model in the case of safety using standard failure modes for the signals deemed to be relevant. This leads into various sub-requirements for different failure modes of the input signal failure hence provision of argumentation for activation of fail-safe mode actively.

The modular model construction can be exploited immediately for safety cases modular construction. To demonstrate cases of modular safety, this study included a scenario of sensor supplied with the corresponding supplied cases of safety. In the case of sensor, there was construction of a safety case corresponding to the electronic circuit custom structure as well as functions of the software which is known for pre-processing the raw input for the practical use of the component’s software (Nag et al.2019). This can be presented diagrammatically as shown below:

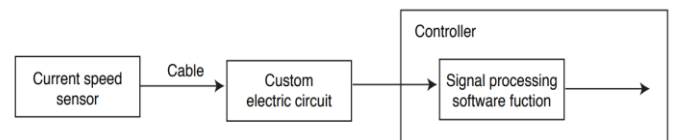


Fig 1:- Signal processing /flow

VI. MODULES OF SAFETY CASES

The safety critical systems which are software intensive like in the case of use a combination of mechanic, like automotive vehicles, software components, electric/electronic among others in the implementation of their functionality overall. As per the provision of ISO 26262, all systems which

are related to safety and constitutes total safety combinations from all the domain needs to be taken into consideration in the cases of safety so that safety argumentations can be suitably supported. To ensure that there was structuring of various safety components, there was construction of a safety case architecture which was made up of safety case modules.

A. Safety Qualification Procedure On Use Case

The standards of certification take into consideration both the process of development and development of the product. As a result, the best option of safety needs to ensure coverage of both areas.

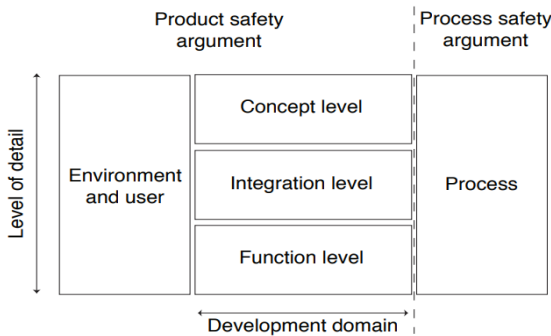


Fig 2:- Safety development domain

In this case, there was focus on the product part. In the case of the cruise control, it was important to have the product-related safety structure case channeled into system's arguments in various levels of abstractions as well as arguments about the system's user and the environment.

B. User and Environment

The argument on safety of the system will only be valid in case the system and people from the surrounding and taken

into consideration. They include the car's driver, the personnel responsible for maintenance and the passengers. The module is containing user's assumption as well as their behavior. The driver's reaction time is very important for cruise control. In addition, there is description of the situations of the environment by the modules like declining roads and inclining roads, wind from various directions, wet surface which all affect the car's deceleration and acceleration.

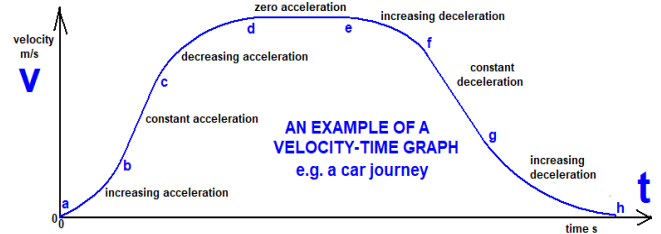


Fig 3:- Vehicle Deceleration and Acceleration Graph work

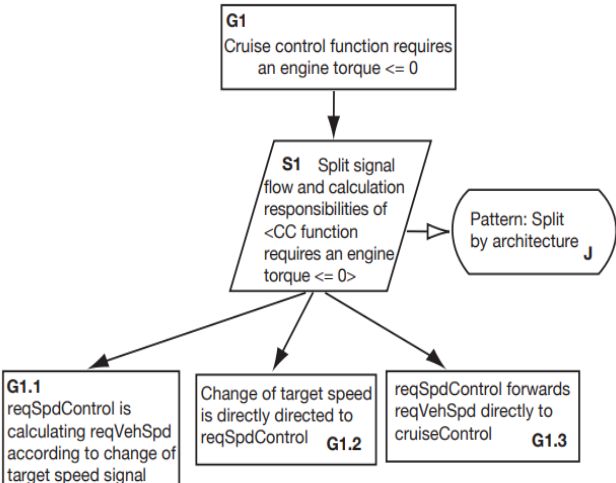
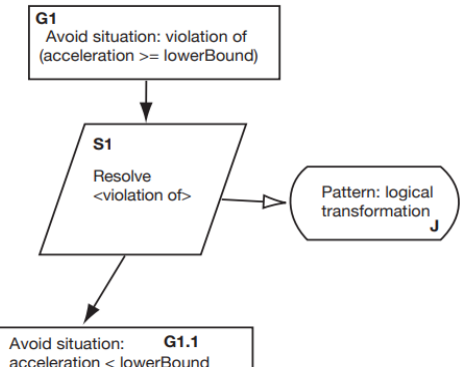
VII. RESULTS AND DISCUSSIONS

Results are conducted to analyze the safety use case study from research (example: taking velocity of car journey) when a potential hazard occurs and how the safety system detects the fault and mitigate the potential hazardous occurrence. For the discussion patterns of safety conducted as explained below:

A. Case Patterns of Safety

In addition to the use of overall structure module, there was employment of patterns of safety cases as the primary building block. The section therefore gives a summary of the patterns as well as their manner of utilization. Finally, there is presentation of brief examples from the identified patterns.

Pattern	Number of usages	About
<p>Using fault model</p>	<p>4</p>	<p>It was utilized during safety consideration of the failures of the speed sensors or the cruise control common failure mode for the cruise control.</p>

<p style="text-align: center;">Split by architecture</p> 	4	<p>In the cases where there was an architecture prescribed by specifications in existence or models, such kind of constraints were utilized in detailing safety case.</p>
<p style="text-align: center;">Logical transformations</p> 	4	<p>In most of the cases, goals are situations logical combination which are admirable and therefore need for their occurrence or otherwise. Through various situation's combinations, such kind of combination potentially be overcomplicated or just get along.</p>

(Results continued...)

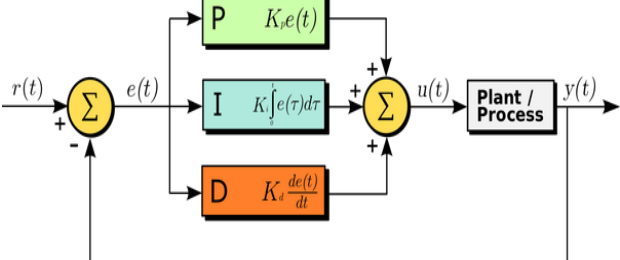
Pattern	Number of usages	About
<p style="text-align: center;">Design of logical transformation</p> 	4	<p>This case, there was checking whether it was possible for the applications of patterns of logical transformation which helps in the resolution of the logical combinations</p>
Model's formal elicitation	3	Model transformation designed for safety use case developing PID controller
Splitting by items	3	Each item is further split to requirements level
Pattern Identification	2	Safe patterns are identified at each requirement for use case considered
Calculation of property probability	1	A probability calculation conducted
Contain and detect fault	1	Fault detection criteria for hazardous occurrence
Expectations failed	1	Number of failures expected for one cause
Fail-safe	1	Mitigations for fault occurrences
Redundant signals	1	Establishing redundancy in both hardware and software as safety mechanism

Table 1

B. Electric Circuit

There was utilization of the electric circuit module in the argument about the failure resistance and correctness of the electric circuits. There could be specific dependencies to the module of mechanical design for example when it comes to the vibration or temperature exposure of the parts of electric circuits. The signal's validity was analyzed as well as their behavior of transmission from the sensors' speed to the cruise control function.

C. Safety Cases Usage With The Requisite Models

Using safety case architecture for automotive as introduced in various sections, there was illustration on the way to link the cases of safety with the respective models used in the process of development. Through utilization of the safety case context in linking the said models, there is proper grounds for argumentation in the case of safety hence making assumptions which are explicit prior to their justification. To this end, there was structuring of safety as per the structure of the system to be developed or under development. In addition, there was use models of development as requirements and information source for the cases of safety as sink for the posed assumptions in the cases of safety (Trovaio 2020).

D. Safety Case Structure And Accordance Model

The safety case that is product-based as constituted was driven by the requirements with the respect that the building goal satisfies requirements of safety. Considering the fact that the case of safety is product-based, those kinds of the requirements were assigned to certain elements only through provision of the link between the artifact in the model of development as well as the corresponding context in the case of safety. To allow for the provision of similar structure in the argument of safety case and in the model of system due to safety cases, there was splitting of requirements of safety as per the design's sub-components.

VIII. CONCLUSION

From this research, it has been established that functional safety of any product constitutes parts which are essential for the development of the product, and it should be addressed as early as possible in the phase of conceptualization and then considered through the entire life cycle of the product. In the case of ISO 26262 a clear method and engineering guideline is offered to at least or avoid failures of the system and mitigate random failures of the Electronic and Electrical System's failure alongside their hardware counterparts. The requirements of the derived functional safety need to be implemented from the lowest possible level to the extreme upper level both from the hardware and software perspective. It forms the basis of proving that the E/E-Systems added are free of the safety risks that are unreasonable.

The engineering approach which would be considered as pragmatic is the utilization of the existing knowledge or simply the utilization of the industry's memory. The focus therefore needs to be on ISO 26262 framework series and the guidelines should be set based on the same. This approach will be very useful particularly for the newcomers in the industry

of automotive and who maybe lacking specific automotive safety for the experience in engineering.

REFERENCES

- [1]. Becker, C., Yount, L., Rozen-Levy, S. and Brewer, J., 2018. Functional safety assessment of an automated lane centering system (No. DOT-VNTSC-NHTSA-17-01). United States. Department of Transportation. National Highway Traffic Safety Administration.
- [2]. Chen, L., Jiao, J. and Zhao, T., 2020. A Novel Hazard Analysis and Risk Assessment Approach for Road Vehicle Functional Safety through Integrating STPA with FMEA. *Applied Sciences*, 10(21), p.7400.
- [3]. Iturbe, X., Venu, B., Jagst, J., Ozer, E., Harrod, P., Turner, C. and Penton, J., 2018. Addressing functional safety challenges in autonomous vehicles with the arm TCL S architecture. *IEEE Design & Test*, 35(3), pp.7-14.
- [4]. Nag, P., Ghanekar, U. and Harmalkar, J., 2019, March. A novel multi-core approach for functional safety compliance of automotive electronic control unit according to ISO 26262. In *2019 IEEE 5th International Conference for Convergence in Technology (I2CT)* (pp. 1-5). IEEE.
- [5]. Pancik, J., Drgona, P. and Paskala, M., 2020. Functional Safety for Developing of Mechatronic Systems–Electric Parking Brake Case Study. *Communications-Scientific letters of the University of Zilina*, 22(4), pp.134-143.
- [6]. Pisoni, F., Avellone, G., Di Grazia, D., Silverio, A., Durand, J., Garcia, J., Tijero, E.D. and Falletti, E., 2019, September. GNSS functional safety for the autonomous vehicle. In *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)* (pp. 1696-1706).
- [7]. Rajasimha, R.C., Arjun, V. and Chandrashekhara, H.G., 2022. *Supplemental FMEA for Monitoring and System Response of Electronic power steering control system functional safety* (No. 2022-28-0404). SAE Technical Paper.
- [8]. Scharfenberg, G., Elis, L. and Hofmann, G., 2019, September. New Design Methodology–Using VHDL-AMS Models to Consider Aging Effects in Automotive Mechatronic Circuits for Safety Relevant Functions. In *2019 International Conference on Applied Electronics (AE)* (pp. 1-5). IEEE.
- [9]. Trovaio, J.P., 2020. Automotive electronics under the COVID-19 shadow [Automotive Electronics]. *IEEE Vehicular Technology Magazine*, 15(3), pp.101-108.
- [10]. Xie, G., Peng, H., Huang, J., Li, R. and Li, K., 2019. Energy-efficient functional safety design methodology using ASIL decomposition for automotive cyber-physical systems. *IEEE Transactions on Reliability*.