A FUNCTIONAL SAFETY METHODOLOGY FOR ADVANCED DRIVER ASSISTANCE SYSTEMS

EBRU CAGLAYAN

Dept. of Mechatronics Engineering, Istanbul Technical University and FEV Turkey
ITU Ayazaga Campus, 34469, Maslak, Istanbul, Turkey
E-mail: caglayaneb@itu.edu.tr

Abstract - Nowadays, there is a large-scale research and investment in automotive safety field, especially for ADAS (Advanced Driver Assistance Systems) in order to make the road vehicles safer as they get more intelligent, more interconnected and more complex, by enabling them to detect and avoid possible accidents, help the driver with changing lanes efficiently and turning in a more accurate way. Almost every automotive OEM is trying to develop an autonomous vehicle now. The automotive companies today spend an immense part of their energy, money and effort and it might lead to make self-driving vehicles part of our lives in a short time. Addition to the benefits of the autonomous vehicles, these vehicles come with some risks also for the road safety. The ISO 26262 is a well-known standard today that defines the functional safety methodology for electrical components of a vehicle. Today, actually there is no direct standard that immediately deals with the functional safety in smart vehicle area and therefore, many developers use this standard as a guideline to design their software and hardware models to make compatible with the functional safety standards. This paper focuses on an overview of a functional safety method that can be applied in autonomous vehicles.

Keywords - ISO 26262, OEM, Functional Safety, ADAS, Autonomous Cars

I. INTRODUCTION

Today, automobiles are one of the important means of transportation. They are widely used and thus, the automotive sector is growing day by day. As of now, modern vehicles are safer, faster and smarter. People and therefore, also the automotive companies seek extra features such as autonomy or specialized driving in the cars. Because of these new requirements, ADAS (advanced driver assistance systems) functions are introduced to the sector for extensively interconnected and networking cyber-physical systems with high complexity of systems-of-systems (SoS).

The introduced SoS in the automotive sector has been designed so that all the information and interaction with its surroundings can be achieved via functions such as sensor fusion. As a whole system, a vehicle is aimed to be able to detect any malfunctions in ADAS functions, which might propagate over the system boundaries and affect other systems to fail in a destructive manner [1].

Unrecognized connections might lead to undesired operational system states and they might not be detected as failure modes. Therefore, functional safety is a very critical topic in order to create fail-safe mechanisms for complex and interconnected automotive systems.

The fundamental achievements have been realized regarding with electrical components in the automotive industry in the previous 30 years [2], e.g. ABS in 1978, ESP in 1995 and Collision Avoidance Systems in 2010 (see Fig. 1).

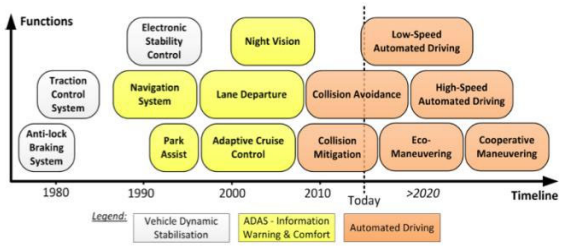


Fig. 1. Developments of advanced driver assistance systems [1]

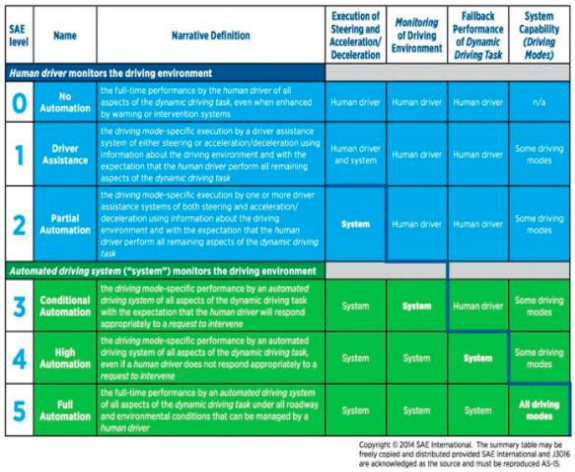
The versions of the ADAS today are even more complex than before when we take two facets into consideration: first of all, from the technical aspect in regard with the emergence of brand new technologies to implement and secondly, from an organizational aspect focusing on the full supply chain in conjunction with the suppliers involved in a various sorts of services and products during the whole lifecycle of producing an autonomous car. In this paper, the technical perspective and the difficulties of ADAS functions and of how to apply the existing version of the ISO 26262 [3] standard considering automotive functional safety for ADAS shall be discussed.

ISO 26262 is the common standard that is applied for functional safety in road vehicles [4]. ISO 26262 explains safety lifecycle of the vehicle and management of safety-related systems for the electrical and/or electronic (E/E) architecture of the car. Functional safety is the whole safety of the system, which is based on the system or component functioning in a correct manner as an answer to the inputs, errors and the operating conditions. A safety goal is a top-level safety requirement, which is derived from the hazard and risk assessment (HARA) of the system. The safety goals and the allocation of

the Automotive Safety Integrity Levels (ASILs) are highly recommended in the standard process of automotive development in order to have safe vehicles on the roads.

The integrity requirements of hardware and software and their development assure that explicit error handling competence is in-built. The safety lifecycle influences the automotive design in remarkably and has to be organized from the beginning phase before the implementation.

The international society of automotive engineers (SAE International) introduces 6 levels of autonomy in vehicles [5] as given in Fig. 2. L5 vehicle is fully autonomous where the system is in charge of the complete functions of a driver in all driving domains. The standard is inadequate to determine the safety requirements of L5 autonomous car as it presumes that the driver is in the loop and is able to handle any likely hazardous incident. Therefore, it is required to redefine the standards that assess the safety requirements of an autonomous car.



SAE level	Name	Narrative Definition	Execution of Steering and Acceleration/ Deceleration	Monitoring of Driving Environment	Fallback Performance of Dynamic Driving Task	System Capability (Driving Modes)
Human driver monitors the driving environment						
0	No Automation	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	Driver Assistance	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes
2	Partial Automation	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/ deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	System	Human driver	Human driver	Some driving modes
Automated driving system ("system") monitors the driving environment						
3	Conditional Automation	the *driving mode*-specific performance by an *automated driving system* of all aspects of the dynamic driving task with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	System	Human driver	Some driving modes
4	High Automation	the *driving mode*-specific performance by an automated driving system of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	System	Some driving modes
5	Full Automation	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	All driving modes

Fig. 2. Levels of autonomy defined by SAE International in J3016 [5]

II. CONCEPT

The functional safety concept as of now depends on acceptable risk for a hazard on a vehicle and/or passengers. Active safety mechanisms require to be embedded into the vehicle system to be able to handle unacceptable niveau of risks. In ISO 26262, **Automotive Safety Integrity Level (ASIL)** is described as a product of severity of harm(Severity), probability of the driving situation (Exposure) and whether in a driving situation the vehicle is controllable by the driver (Controllability) [6].

$$\text{ASIL} = \text{Severity (S)} \times \text{Exposure (E)} \times \text{Controllability (C)} \quad (1)$$

Fig. 3 summarizes the ISO 26262 process in four main steps:

1) Item Definition
2) Hazard and Risk Analysis
3) ASIL Assignment
4) Determination of Safety Goals

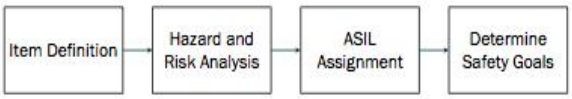


Fig. 3. Summary of current ISO 26262 practice

Each combination of S, E and C correlates to an ASIL levelas shown in Fig. 4 and corresponds to a QM (quality management) where no safety precautions need to be carried over and the standard development process is enough.

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

Fig. 4. Levels of ASIL as defined in ISO 26262 [5]

The term "Controllability" is not applicable as a criterion to decide the ASIL levels for any of the items, as the users of the vehicle shall not take any actions to decrease the possibility of destruction in a hazardous case. Severity and Exposure are on the other hand applicable as the extent of the harm, and the possibility of a specific driving scenario does not alter. Controllability would be convenient only if the system behaviour was modelled after human drivers behave exactly like a human driver would behave and react to a given hazardous situation appropriately. Since this is not the case, today's definition of ASIL requires modification.

The safety goals and functional safety concept for today's vehicles are designed by the assumption that the driver is the superfluous factor in a destructive scenario and can vanish or reduce the hazard using some actions or manoeuvres. In a fully autonomous vehicle, the driver is a user of a service provided by the vehicle, rather than the total responsible for it[7]. The driver is not a part of any decision making or environmental perception mechanisms, these responsibilities have been taken over by the system, namely the vehicle. That is why describing a quantifiable metric that can be used to evaluate this decision-making ability of the vehicle in the absence of driver becomes essential. Without this defined metric, evaluating the functional safety and identifying the set of safety goals for an autonomous vehicle is tough to analyse. Safety of intended function (SOTIF) is another problematic topic in AV

development [8]. Safety of the function on the target is where the system fails to function as desired or targeted in the absence of a fault because of some design oversight leading to a hazardous situation. A few examples are as follows: When a LiDAR incorrectly detects an obstacle due to the dirt piled up on the sensing lens or when a lane recognition system can not recognize the merging of lanes because of vanished lane markings. These errors are a mix of systematic faults that is built-in in the design of the algorithm and the errors in the interpretation because of an undetermined driving situation. These cases are not covered principally by ISO 26262. Any new approach will have to incorporate safety concepts to also cover these kinds of operational situations.

III. A SHORT BACKGROUND – ISO26262

ISO 26262 operates on the focus of unreasonable risk. The standard is split into 10 parts and relies on hazard and risk analysis to evaluate possible hazards. The standard depends on the V-model of development for both hardware and software of the system. The following terms and definitions are defined in part 1 of ISO 26262 [5], [9]:

Harm: It can be defined as the physical injury or damage.

Severity(S): A measure of how much harm to an individual.

Exposure (E): To be in an operational situation that might be destructive if coincident with the failure mode in analysis.

Controllability (C): The capability to prevent damage through on-time reactions of the people involved, probably with the support of external measures. It, in general, depends on the actions of the driver or the pedestrians involved to harm.

Item: System or SoS to develop a function at system level.

Hazard: Potential source of destruction, occurred by the malfunctioning behaviour of the item.

Risk: Mix of probability of occurrence of harm and severity of that harm (S) in a particular situation.

Safety Goal: Top-level safety requirement of the system from HARA analysis.

Safe State: Operating mode of an item without a risk, which is not analysed or reasoned.

Fault tolerant time interval (FTTI): Time span in which a fault would be present before the possible happening of a harmful event (e.g. Fig. 5).

Fault reaction Time (FRT): Time span between detection of a fault until reaching a safe state (e.g. Fig. 5).

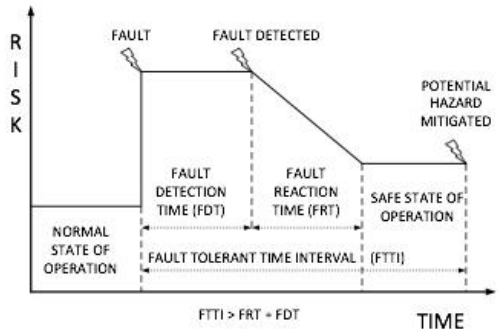


Fig. 5. Fault tolerant time interval [9]

The part 3 of the ISO 26262 focuses on the concept phase. The standard does not address the performance aspect of the electronic subsystems; it deals with the hazards caused by the faulty behavior in the subsystems. The part 3 of ISO 26262 in several paragraphs describes the definition of an item, the hazard and risk analysis (HARA), assignment of ASIL, the derivation of the safety goals, and the functional safety concept. The functional and non-functional requirements with the boundary of the item and its interfaces are parts of the item definition. For the defined item, the potential hazards are identified and categorized that can be experienced due a malfunction. These are defined as hazardous events (HEs). The ASILs are then assigned to the HEs. The assignment of ASILs is followed by the derivation of the appropriate safety goal, which is the top-level safety requirement. ASILs are assigned according to severity, exposure, and controllability shown in Tab. 1, 2 and 3 respectively [5].

S0	S1	S2	S3
No injuries	Light to Moderate injuries	Severe life threatening injuries, survival probable	Severe life threatening injuries, survival uncertain

Tab. 1. Severity levels in ISO 26262 [5]

E0	E1	E2	E3	E4
Incredible	Very Low Probability	Low Probability	Medium Probability	High Probability

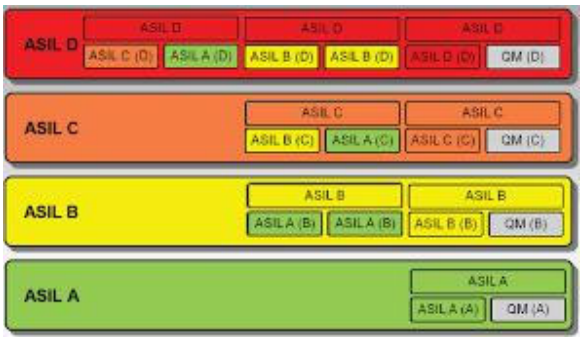
Tab. 2. Exposure levels in ISO 26262 [5]

C0	C1	C2	C3
Controllable in General	Simply Controllable	Normally Controllable	Difficult to control or Uncontrollable

Tab. 3. Controllability levels in ISO 26262 [5]

The standard further explains 4 ASILs (A - D) with A being the lowest and D being the highest levels of integrity. ASILs illustrate the required safety measures that are required to be incorporated into the item or system. The functional safety requirements are derived for the hardware and software components of the architecture and traceability is

built. Afterwards, the technical safety concept is derived, which details the technical implementation for the safety mechanisms. In Tab. 4, ASIL decomposition mechanism is given [9].



Tab. 4. ASIL decomposition [5]

IV. A CASE STUDY ON AN ADAS FUNCTION

As a case study from advanced driver assistance systems functions, AEBS (Advanced Emergency Braking System) was selected.

Advanced Emergency Braking System aims to avoid or mitigate a collision by reducing speed and activating brake system when a forward vehicle/obstacle is detected as a potential forward collision. AEBS is used for motor vehicles and pedestrians on public roads. Also, AEBS is used for stationary and slow-moving objects. AEBS supports and helps the driver but the main responsibility still belongs to the driver.

A. Item Definition

This section describes the functions of the item under consideration. The description is based on ISO 22839-2013 and JT/T 1242-2019 standards. The input and output signals, which are inside of the boundary of the item, are shown in blue, and which are outside of the boundary are shown in red in Fig. 6.

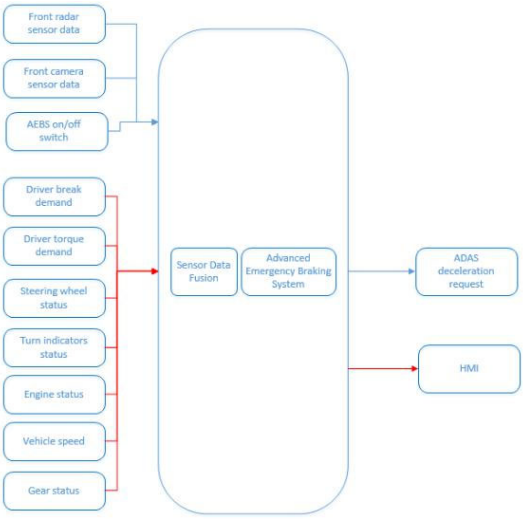


Fig. 6. System boundaries of AEBS

AEBS manages reducing vehicle speed by using the braking system in case of a potential crash. Also, AEBS provides information to the driver. AEBS requires anti-lock brakes, electronic stability control system and disc brakes on all wheels. The primary functions of AEBS are shown in Tab. 5.

Function ID	Function Name	Description
AEBS – F1	Emergency Braking	Provides necessary braking by deceleration to avoid a collision.
AEBS – F2	Inform driver about AEBS status	Informs driver about the state of AEBS.
AEBS – F3	Activation of AEBS	The driver uses on/off switch to activate AEBS manually
AEBS – F4	Deactivation of AEBS	The driver uses on/off switch to deactivate AEBS manually
AEBS – F5	Target object selection	Provides Selection of setting the target vehicle from all possible road participants

Tab. 5. Primary functions of AEBS

AEBS has three operating modes: AEBS off, AEBS inactive and AEBS active and accordingly has four states: warning, speed reduction braking (SRB), mitigation braking (MB) and override. Operating modes are given in Tab. 6, states are given in Tab. 7 and state flow is given in Fig. 7 for AEBS function.

Mode ID	Mode Name	Description
AEBS-M1	Active	AEBS is active if the ignition on and all conditions are met
AEBS-M2	Off	AEBS is off if the ignition is off
AEBS-M3	Inactive	AEBS goes into Inactive mode from off when the ignition on and check all conditions if AEBS can go into active mode. In the opposite way if any fault becomes or AEBS criteria is not provided any more, AEBS goes into inactive mode from active mode.

Tab. 6. Operating modes of AEBS

State ID	State Name	Description
AEBS-S1	Warning	Warns the driver by using FCW
AEBS-S2	Mitigation Braking	Provides braking if the crash is unavoidable
AEBS-S3	Speed Reduction Braking	Provides early warning to the driver about a potential crash
AEBS-S4	Override	If the driver increases throttle position with a position 20% bigger than the current position within 100ms, the system shall switch to override state and the driver takes over. If the driver releases throttle with a throttle position 10% lower than current position within 100ms or the override state last more than 5 seconds, the override state shall release at once.

Tab. 7. States of AEBS

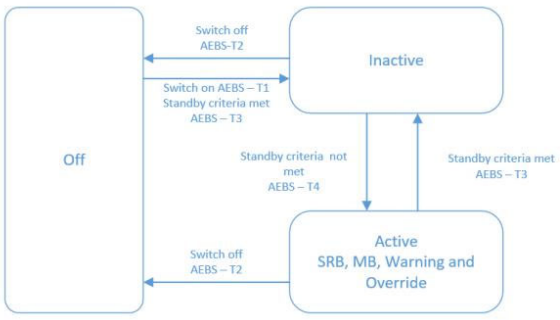


Fig. 7. Stateflow of AEBS

Operational Constraints: Although AEBS supports the driver and reduces the risk of a potential crash, the driver is still responsible. AEBS function is active between 4m/s (15km/h) and 28m/s (101km/h). If the vehicle goes above 28m/s (101km/h) or below 4m/s (15 km/h), then AEBS is deactivated.

AEBS shall operate, if lateral offset of target vehicle < 20% and lateral speed of target vehicle < 0.2 m/s (0.72 km/h).

Environmental Constraints: In weather conditions that affect the front radar's sight (e.g. snow, fog, heavy rain, heavy dust), the AEBS may not work correctly. Also, dirt decreases functionalities of the radar and camera. Curve radius should be less than 125 m for AEBS to work correctly.

Effect of item's behaviour on its environment: If there is a malfunction in AEBS, then braking may not work during a potential collision. Therefore, it may lead to front, rear end or side collisions with other objects.

Functionalities required from other items: Vehicle speed, steering angle, actual gear mode, engine status, right/left turn signal active, driver torque and brake demands are necessary from other items for AEBS.

B. Hazard and Risk Analysis

For HARA activities, the following steps should be applied:

1. Driving scenarios by situation analysis should be realized (manoeuvre at crossroads, environmental situation, operating mode of the vehicle, etc.).
2. Hazard identification should be done (from malfunctions, to malfunction behaviour, to hazard)
3. Derivation of the hazardous events should be done (driving situation should be combined with hazards, potential source of harm should be determined).
4. Hazardous events should be classified (severity, exposure, and controllability classification).

In this section, some examples for HARA on AEBS function shall be given. From the primary functions of AEBS, if it is necessary to analyse the subfunction "Provide emergency braking", it can be examined in the use case of driving with 60 kph constant speed in inner city. In this case, hazard can be defined as "unintended vehicle deceleration" and potential effect is rear-ending collision with other vehicles. More than 90% of the drivers can control the situation by accelerating or changing the lane. Using this information, exposure value can be selected as E4 (high probability), severity value can be selected as S3 (severe life-threatening injuries, survival uncertain) and controllability value can be selected as C2 (normally controllable).

C. ASIL Assignment

Using the severity, exposure and controllability formula given with equation (1) in Concept part, ASIL can be found as C according to functional safety standards. According to ASIL representation, ASIL C is the second highest degree of automotive hazard. In this case, this use case should be treated very carefully in the safety software and correct requirement and validation plans should be managed. Additionally, safe state of this ASIL would be limiting unintended deceleration.

D. Determination of Safety Goals

Now with the same use case, safety goals should be analysed. For this scenario, there are two possible solutions to achieve this safety goal and avoid from hazard of this use case. In Tab. 8, the options are given with advantages and disadvantages for a possible development program.

	Option 1	Option 2
Description	• Develop AEBS function and Sensor Fusion in Safety SW (L2 SW) • Follow ASIL C process (development and testing) for the above	• Develop a simple and independent Safety Mechanism for AEBS and Sensor Fusion
Advantages	• No independent function in L2 is required	• Simple Safety Mechanism (assumption) • Independent Safety Mechanism
Disadvantages	• Since there is no independent safety function, functional safety cannot be achieved • Sensor Fusion and AEBS are complicated functions. It can increase the workload for Safety Development.	• Calculations are simple, may not be accurate

Tab. 8. Options for safety goals against unintended vehicle deceleration in AEBS function

With the trade-off, Option 2 might be selected as a possible solution to achieve the safety goal for the special use case.

Eventually, in Fig. 8 a black box representation of an example architecture to fulfill the safety goal is given.

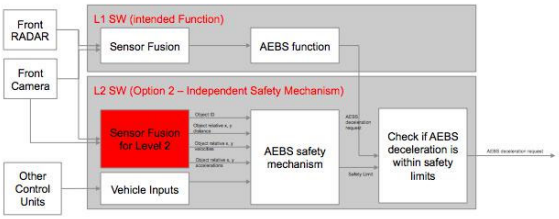


Fig. 8. Architecture to fulfill the specific safety goal

V. CONCLUSION

A conceptual design of a functional safety for ADAS functions is defined in this study. The initial methodology and the necessity for this research are represented in an ordered way. It creates a substitution of ordinary way of functional safety to the new interconnected and autonomous cars.

REFERENCES

[1] H. Martin et al., "Functional Safety of Automated Driving Systems: Does ISO 26262 Meet the Challenges?", Automated Driving, 2017, doi: 10.1007/978-3-319-31895-0_16.

[2] K. Bengler, et al., "Three decades of driver assistance systems: Review and future perspectives", Intelligent Transportation Systems Magazine, IEEE 6.4, 2014, pp. 6-22.

[3] International Organization for Standardization, "ISO 26262 – Road vehicles – Functional Safety, Part 1-10", ISO/TC 22/SC 32 – Electrical and electronic components and general system aspects, Nov. 15, 2011.

[4] ISO, "Road vehicles - functional safety - parts 1-10", Standard, International Organization for Standardization, Geneva, CH, January 2011.

[5] SAE, "Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems", Available: standards.sae.org/j3016_201609/, 2014.

[6] Birolini, A. "Reliability engineering" volume 5, Springer, 2007.

[7] Herwick, M., Siedersberger, K.H. "Strategy and architecture of a safety concept for fully automatic and autonomous driving assistance systems" *IEEE Intelligent Vehicles Symposium*, pages 955-960, June 2010. doi: 10.1109/IVS.2010.5548115.

[8] Behere, S., Törngren, M. "A functional architecture for autonomous driving",*Proceedings of the First International Workshop of Automotive Software Architecture*, WASA'15, pages 3-10, New York, NY, USA,2015. ACM. ISBN 978-1-4503-3444-0. doi: 10.1145/2752489.2752491.

[9] Shastry, A.K., "Functional Safety Assessment in Autonomous Vehicles (Master's Thesis)", Virginia Polytechnic Institute and State University, VA, Virginia, US, 2018.

★★★