

Interactive Safety Analysis Framework of Autonomous Intelligent Vehicles

You Xiang Cui^{1,2}, Lei Sun^a, Li Hui Sui, Jun Kang, Yong Jiang²

¹ Department of Quality Management Engineering, Business School, Shanghai Dianji University
No.1350 Ganlan Road, Lingang New City, Pudong District, Shanghai 201306, China

² Shanghai Connected & Automated Vehicles Industrial Promotion Center

Abstract. More than 100,000 people were killed and around 2.6 million injured in road accidents in the People's Republic of China (PRC), that is four to eight times that of developed countries, equivalent to 6.2 mortality per 10 thousand vehicles—the highest rate in the world. There are more than 1,700 fatalities and 840,000 injuries yearly due to vehicle crashes off public highways. In this paper, we proposed a interactive safety situation and threat analysis framework based on driver behaviour and vehicle dynamics risk analysis based on ISO26262. .

1 Introduction

Safety is one of the key issues of future automobile development. New functionalities not only in areas such as driver assistance, propulsion, in vehicle dynamics control and active and passive safety systems increasingly touch the domain of system safety engineering. Development and integration of these functionalities will strengthen the need for safe system development processes and the need to provide evidence that all reasonable system safety objectives are satisfied.

Automobile safety is the study and practice of design cars, construction, equipment and regulation to minimize the occurrence and consequences of traffic collisions. Road traffic safety more broadly includes roadway design. Improvements in roadway and automobile designs have steadily reduced injury and death rates in all first world countries. Nevertheless, auto collisions are the leading cause of injury-related deaths. In the United States a pedestrian is injured by an automobile every 8 minutes, and are 1.5 times more likely than a vehicle's occupants to be killed in an automobile crash per outing.

The field of intelligent vehicles has become a major research theme in intelligent transportation systems since traffic accidents are serious and growing problems all over the world. The goal of an intelligent vehicle is to augment vehicle autonomous driving either entirely or partly for the purposes of safety, comfortable, and saving energy. Indeed, many technologies of intelligent vehicles root in autonomous mobile robots.

For systems that operate continuously (continuous mode) the allowable frequency of failure must be determined. For systems that operate more than once a year (high demand) the allowable frequency of failure

must be determined. For systems that operate intermittently (less than once a year / low demand) the probability of failure is specified as the probability that the system will fail to respond on demand. ISO 26262 is an adaptation of the Functional Safety standard IEC 61508 for Automotive Electric/Electronic Systems. ISO 26262 defines functional safety for automotive equipment applicable throughout the lifecycle of all automotive electronic and electrical safety-related systems

Safety is NHTSA's number one priority. It's mission is to reduce the number of deaths and injuries on nation's roadways by getting drivers, pedestrians and cyclists to change their behaviors once they get behind the wheel or on the streets. NHTSA(National Highway Traffic Safety Administration) Defines 5 Levels of Vehicle Automation in May 2013.

Level 0: No-Automation

The driver is in complete and sole control of the primary vehicle controls (brake, steering, throttle, and motive power) at all times

Level 1:Function-specific Automation

Automation at this level involves one or more specific control functions if multiple functions are automated, they operate independently from each other.

Level 2:Combined Function Automation

This level involves automation of at least two primary control functions designed to work in unison to relieve the driver of control of those functions.

Level 3: Limited Self-Driving Automation

The vehicle is designed to ensure safe operation during the automated driving mode but can determine when the system is no longer able to support automation and then signals to the driver to reengage in the driving task, providing the driver with an appropriate amount of transition time to safely regain manual control.

^a Lei Sun: Sunlei@sdju.edu.cn

Level 4: Full Self-Driving Automation

The vehicle is designed to perform all safety-critical driving functions and monitor roadway conditions for an entire trip.

2 Passive Safety and Active Safety

The terms "active" and "passive" are simple but important terms in the world of automotive safety. "Active safety" is used to refer to technology assisting in the prevention of a crash and "passive safety" to components of the vehicle (primarily airbags, seatbelts and the physical structure of the vehicle) that help to protect occupants during a crash^[8,9]. As Fig. 1 show.

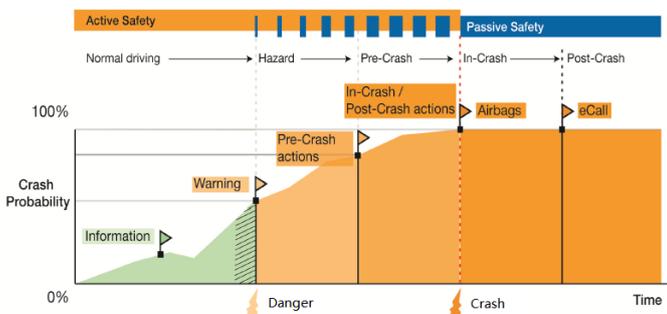


Figure 1. Active safety and Passive safety during a crash

A passive safety system has a passive safety device mounted on a vehicle, and a passive safety control means having an acceleration sensor detecting acceleration caused by an impact at the time of collision. The passive safety control means receives input an impact acceleration detection signal from the acceleration sensor and operates controllably the passive safety device. Further, the passive safety control means computes a physical quantity based on the impact acceleration detection signal inputted from the acceleration sensor, sets maximum and minimum reference values of the physical quantity in normal driving, performs a computation with respect to addition of a present acceleration inputted from the acceleration sensor to an integrated acceleration value at this point in time when the physical quantity crosses a range defined between the maximum and minimum reference values, and performs a computation with respect to a reset process of the integrated acceleration value when the physical quantity remains within the range defined between the maximum and minimum reference values^[10]

Active safety system make vehicles and drivers more aware of the situation around them. Addressing the front, sides, rear and even the interior of vehicles, these systems are designed to help drivers avoid crashes and reduce the effects if a crash can't be avoided.

As industry rushes towards the goal of automated vehicles, the driver-control to system-only narrative becomes more and more critical.

3 Safety Analysis Framework of ISO26262

ISO 26262 is a Functional Safety standard, titled "Road vehicles – Functional safety". Functional safety features form an integral part of each automotive.

System safety is achieved through a number of safety measures, which are implemented in a variety of technologies (e.g. mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic) and applied at the various levels of the development process. Although ISO 26262 is concerned with functional safety of E/E systems, it provides a framework within which safety-related systems based on other technologies can be considered. ISO 26262:

- a) Provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases;
- b) provides an automotive-specific risk-based approach to determine integrity levels [Automotive Safety Integrity Levels (ASIL)];
- c) uses ASILs to specify applicable requirements of ISO 26262 so as to avoid unreasonable residual risk;
- d) provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved;
- e) Provides requirements for relations with suppliers.

Functional safety is influenced by the development process (including such activities as requirements specification, design, implementation, integration, verification, validation and configuration), the production and service processes and by the management processes.

Safety issues are intertwined with common function-oriented and quality-oriented development activities and work products. ISO 26262 addresses the safety-related aspects of development activities and work products.

Figure 2 shows the overall structure of ISO 26262



Figure 2. The overall structure of ISO 26262

With the trend of increasing technological complexity, software content and mechatronic implementation, there are increasing risks from systematic failures and random hardware failures. ISO 26262 includes guidance to avoid these risks by providing appropriate requirements and processes. Automated functionalities are very complex and can take quite some time to reach, as Figure 3 shows.

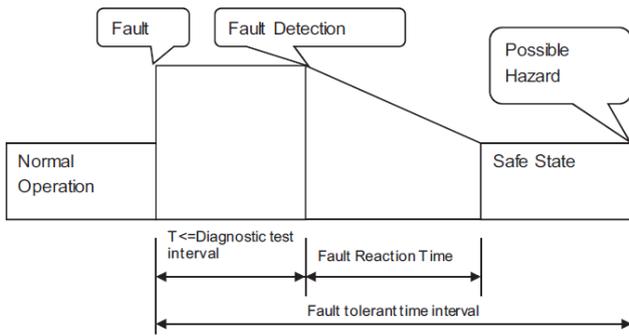


Figure 3. Fault reaction time and fault tolerant time interval

The ISO 26262 safety framework (see Figure 4) encompasses the principal safety activities during the concept phase, product development, production, operation, service and decommissioning. Planning, coordinating and documenting the safety activities of all phases of the safety lifecycle are key management tasks.

interfaces, as well as assumptions concerning other items, elements, systems and components are determined.

b) The subphase: initiation of the safety lifecycle

Based on the item definition, the safety lifecycle is initiated by distinguishing between either a new development, or a modification of an existing item.

c) The subphase: hazard analysis and risk assessment

After the initiation of the safety lifecycle, the hazard analysis and risk assessment is performed as given in ISO 26262-3:2011. First, the hazard analysis and risk assessment estimates the probability of exposure, the controllability and the severity of the hazardous events with regard to the item. Together, these parameters determine the ASILs of the hazardous events. Subsequently, the hazard analysis and risk assessment determines the safety goals for the item, with the safety goals being the top level safety requirements for the item. The ASILs determined for the hazardous events are assigned to the corresponding safety goals.

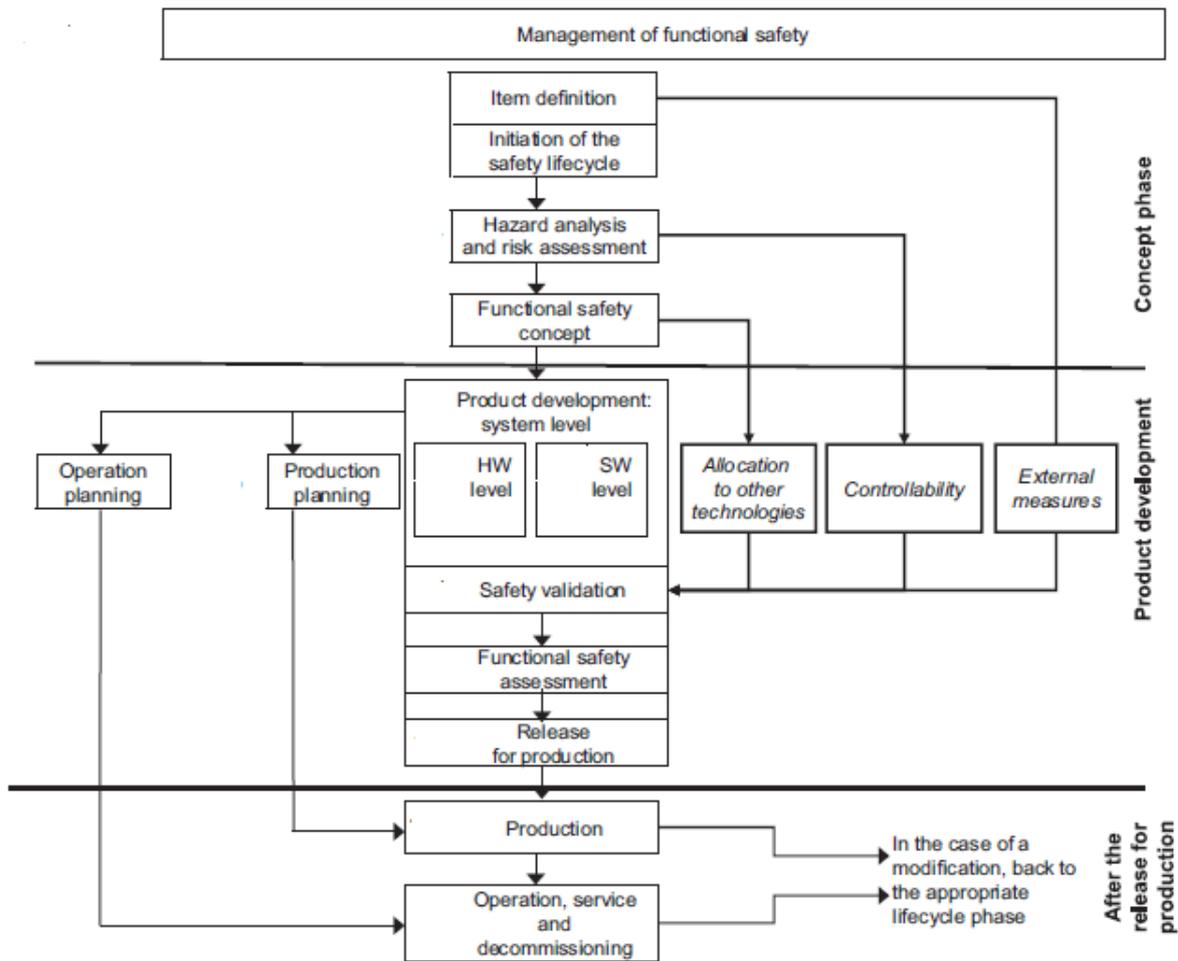


Figure 4 Safety framework of ISO 26262

The following descriptions explain the definitions of the safety framework.

a) The subphase: item definition

The initiating task of the safety lifecycle is to develop a description of the item with regard to its functionality, interfaces, environmental conditions, legal requirements, known hazards, etc. The boundary of the item and its

During the subsequent phases and subphases, detailed safety requirements are derived from the safety goals. These safety requirements inherit the ASIL of the corresponding safety goals.

d) The subphase: functional safety concept

Based on the safety goals, a functional safety concept is specified considering preliminary architectural assumptions. The functional safety concept is specified by functional safety requirements that are allocated to the elements of the item. The functional safety concept can

also include other technologies or interfaces with external measures, provided that the expected behaviours thereof can be validated. The implementation of other technologies is outside the scope of ISO 26262 and the implementation of the external measures is outside the scope of the item development.

e) The phase: product development at the system level

After having specified the functional safety concept, the item is developed from the system level perspective, as given in ISO 26262-4. The system development process is based on the concept of a V-model with the specification of the technical safety requirements, the system architecture, the system design and implementation on the left hand branch and the integration, verification, validation and the functional safety assessment on the right hand branch.

The hardware-software interface is specified in this phase.

The product development at the system level incorporates validation tasks for activities occurring within other safety lifecycle phases, including the validation of the aspects of the functional safety concept that are implemented by other technologies.

4 Conclusions and prospects

To maximize the potential and achieve an optimal ITS ecosystem that supports safety, mobility, increased transportation efficiency, and environmental applications, we must have a clear and implementable ITS privacy and security strategy and framework which harnesses both connected and autonomous technologies.

The Interactive Safety Analysis Framework must include technical and policy solutions, namely a fully secured connected vehicle network and adequate consumer privacy protections that evoke trust from drivers and passengers traveling on roads and highways as follows:

- Required Technologies to be realized in 2014-2020
- Detect exact location of a vehicle (sub cm)
- Detect surrounding obstacles and their next move (sec)
- Stop or determine collision avoidance routing
- Additional Key Factors
- Research of Human Factors

i.e. Evaluate override requirements such that the driver can always or when appropriate override the automated systems and regain control Computational algorithm to perceive, understand and judge vehicle and environmental status in place of a human brain

- Need test of Level 3 vehicles in real life situation to identify answers to many of technical and human factors questions.
- Analyze sensor data from various operating scenarios (traffic dynamics), driver capabilities, environmental variations (rain, snow, etc.), and roadway types/configurations.
- Apply Big Data Analysis on Cloud

- Cyber-security and Privacy issues need to be addressed

Acknowledgment

This research was financially supported by think tank construction project of equipment manufacturing industry development research center: intelligent manufacturing (15AR01) and the Leading Academic Discipline Project of (10XKJ01) in Shanghai Dianji University.

References

1. Gereon Meyer Sven Beiker. Road Vehicle Automation, April 2015 Springer.
2. <http://www.nhtsa.gov/Driving+Safety>
3. Ogiela M R, Hachaj T. Advances in Computer Vision and Pattern Recognition[M]// Advances in computer vision and pattern recognition. Springer, 2015:1-70.
4. Manawadu U, Ishikawa M, Kamezaki M, et al. Analysis of Individual Driving Experience in Autonomous and Human-Driven Vehicles using a Driving Simulator[C]// Advanced Intelligent Mechatronics (AIM), 2015 IEEE International Conference on. IEEE, 2015.
5. Mladenovic M N, Abbas M M. Self-organizing Control Framework for Driverless Vehicles[C]// Intelligent Transportation Systems - (ITSC), 2013 16th International IEEE Conference on. IEEE, 2013:2076-2081.
6. Cheng, Autonomous Intelligent Vehicles (Advances in Computer Vision and Pattern Recognition)[M]//DOI 10.1007/978-1-4471-2280-7 Springer, 2011
7. <http://auto.huanqiu.com/news/2014-10/5161704.html>
8. Yazzie T J, Zhang G, Tarefder R, et al. Autonomous Vehicle System-Driven Innovative Traffic Control and Management Strategy Review[C]// Transportation Research Board 94th Annual Meeting. 2015.
9. "American Honda safety page". Corporate.honda.com. 2006-03-02. Retrieved 2011-09-20.
10. Jump up Gladwell, Malcolm (2004-01-12). "BIG AND BAD: How the S.U.V. ran over automotive safety." (PDF). The New Yorker. Retrieved 2009-07-24.
11. Yamashita T. Passive safety system: US, US6636794 B2[P]. 2003.