An Overview of the  Approaches for Automotive Safety Integrity Levels Allocation

Sohag Kabir

Youcef Gheraibia

Khaoula Djafri

Habiba Krimou

ISO 26262, titled Road Vehicles–Functional Safety, is the new automotive functional safety standard for passenger vehicle industry. In order to accomplish the goal of designing and developing dependable automotive systems, ISO 26262 uses the concept of Automotive Safety Integrity Levels (ASILs), the adaptation of Safety Integrity Levels (SILs). ASILs are allocated to the components and subsystems that can cause system failure and malfunctions that lead to hazards. ASILs allocation is a hard problem consists of finding the optimal allocation of safety levels to the system architecture which must guarantee that the highest safety requirements are met while development cost of the automotive system is kept minimum. There were many successful attempts to solve this problem using different techniques. However, it is worth pointing that there is an absence of a review that provides an in-depth study of all the existing methods and highlights their merits and demerits. This paper presents an overview of different approaches that were used to solve ASILs allocation problem. The review provides an overview of safety requirements including the related standards followed by a study of the resolution methods of the existing approaches. The study of each approach provides a detailed explanation of the used methodology and a discussion of its strength and weaknesses including the main open challenges.

# Introduction

Due to the rapid advancement of technologies, an increasing number of electric and electronic devices are used every day in people’s lives, in home, office and even in public spaces. Some of these devices can represent a danger or a threat to human health and environment by causing harm. The latter is a physical injury or damage to the health of persons [1]. Here where the assurance of the safety becomes a primary necessity. IEC 61508 [2] is an international standard for the functional safety of electrical, electronic and programmable safety related systems (E/E/PE). Safety related systems are systems that perform a function or a set of functions that ensure that risks are kept at an acceptable level (Lowrance, 1976)[3]. IEC 61508’s role is to minimise the likelihood of failure of these systems by ensuring that they provide the required safety integrity levels (SILs). SILs are presented as five safety levels, which are used to make sure that E/E/PE systems do meet the highest safety requirements against the highest risks.

It is noticed in the last two decades that the number of road accidents has increased significantly and as an outcome, a massive number of casualties have occurred. According to the [global status report on road safety](http://injuryprevention.bmj.com/content/15/4/286.short) released by the world health organisation, over 1.2 million people die each year on the world’s roads and between 20 and 50 million suffer non-fatal injuries (Toroyan, 2009). Reliability of automotive devices and systems is one of the major factors that have a direct effect on the safety of road users, therefore, standards like ISO 26262 have come to light. ISO 26262 is an adaptation of the IEC 61508 standard for the automotive industry. This new automotive functional safety standard defines a safety life cycle applied to automotive electronics, where designs must comply with the standard by going through an overall safety process (Parker *et al.*, 2013). ISO 26262 uses the concept of Automotive Safety Integrity Levels (ASILs) which are an adaptation of SILs in the automotive industry.

ASILs are the key component of ISO 26262, used to represent the severity of safety requirements. They are 5 levels (QM, A, B, C, D) from the least strict ASIL (A) to the strictest ASIL (D) where QM means no safety requirements. Each level has a cost associated with it, which refers to the used cost function. According to ISO 26262’s algebra, ASILs are assigned integer values as: ASIL(QM)=0, ASIL(A)=1, ASIL(B)=2, ASIL(C)= 3 and ASIL(D)=4. ASILs are allocated to hazardous components based on the severity of the hazard caused by the failure of that component. ASILs decomposition concept allows the ASIL to be decomposed over components that together provide the same hazard. ASILs allocation is a hard, complex problem of finding the most appropriate allocation of safety requirements to the components of the automotive system. An appropriate ASILs allocation to components and subsystems must guarantee the fulfilment of highest safety requirement with the least development cost.

Due to the criticality of the ASILs allocation problem and its crucial importance in any automotive system’s safety, an appropriate allocation must be found. To attain this objective, exact solution techniques and optimisation methods are used. Although these two methods aim to solve ASILs allocation problem, generally optimisation solvers converge faster by finding at least a near optimal solution, however, no guarantee is given that this solution will be found. On the other hand, exact solvers may take extra time, but they can find all exact optimal solutions.

In this review, after presenting an overview of the background of safety requirements including safety standards, an in-depth study of the existing approaches for ASILs allocation problem is presented. Here, different approaches are categorised into exact and optimisation methods, and described while identifying their strength and weaknesses. Finally, future outlook for ASILs allocation approaches is provided.

The rest of the paper is organised as follows: in the next section, the background study of safety requirements is introduced. In the third section, the ASILs allocation problem is described. Section 4 reviews both exact and optimisation approaches used for solving ASILs allocation problem. Section 5 presents a discussion and summarises the open challenges for the ASILs allocation approaches. Finally, in section 6, concluding remarks are presented.

Aizpurua et al. (2013)[4]

Allaire (2008) [5]

Anton (2010) [6]

ATESST2 (2010) [7]

Azevedo et al (2013) [8]

Azevedo (2012)[9]



Pellentesque suscipit risus massa, non vestibulum libero euismod feugiat. In hac habitasse platea dictumst. Maecenas rutrum lobortis lobortis. Vestibulum convallis porttitor sem ac ultricies.

# Section

Nunc a aliquet sem, eget aliquet purus. Vestibulum ac placerat mauris. Proin sed dolor ac justo semper iaculis. Donec varius, nibh sit amet finibus tristique, sapien ante interdum odio, et pretium sapien libero nec massa. In hac habitasse platea dictumst. Donec vel augue ac sapien imperdiet pretium. Maecenas gravida risus id ultricies dignissim. Maecenas gravida felis quis dolor faucibus, sed maximus lorem tristique

# Acknowledgements

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras egestas auctor molestie. In hac habitasse platea dictumst. Duis turpis tellus, scelerisque sit amet lectus ut, ultricies cursus enim. Integer fringilla a elit at fringilla. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nulla congue consequat consectetur. Duis ac mi ultricies, mollis ipsum nec, porta est.

# References

1. I. O. for Standardization, *ISO 26262 Road Vehicles - Functional Safety* (2011).

2. I. E. Commission, *IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, Ed. Geneva: Switzerland* (1997).

3. W. W. Lowrance, *Of Acceptable Risk: Science and the Determination of Safety* (Altos, California: William Kaufmann Inc., 1976).

4. J. I. Aizpurua and E. Muxika, International Journal on Advances in Security **6**, (2013).

5. G. Allaire and S. M. Kaber, *Numerical Linear Algebra* (New York: Springer, 2008).

6. H. Anton, *Elementary Linear Algebra* (John Wiley & Sons, 2010).

7. A. T. E. S. S. T. P. Consortium, *EAST-ADL Domain Model Specification* (ATESST2, Deliverable D.4., 2010).

8. L. P. Azevedo, D. Parker, M. Walker, Y. Papadopoulos, and R. E. Araujo, in *SAFECOMP 2013-Workshop CARS (2nd Workshop on Critical Automotive Applications: Robustness & Safety) of the 32nd International Conference on Computer Safety, Reliability and Security* (2013).

9. L. P. Azevedo, Hybrid Braking System for Electrical Vehicles: Functional Safety, Master’s thesis, Department of Electrical Engineering, Porto Uniersity., Porto, Portugal, 2012.