

# Automated Decomposition and Allocation of Automotive Safety Integrity Levels Using Exact Solvers

Alexandr Murashkin  
Univ. of Waterloo

Luis Silva Azevedo  
Univ. of Hull

Jianmei Guo, Edward Zulkoski, Jia Hui Liang, and Krzysztof Czarnecki  
Univ. of Waterloo

David Parker  
Univ. of Hull

## ABSTRACT

The number of software-intensive and complex electronic automotive systems is continuously increasing. Many of these systems are safety-critical and pose growing safety-related concerns. ISO 26262 is the automotive functional safety standard developed for the passenger car industry. It provides guidelines to reduce and control the risk associated with safety-critical systems that include electric and (programmable) electronic parts. The standard uses the concept of Automotive Safety Integrity Levels (ASILs) to decompose and allocate safety requirements of different stringencies to the elements of a system architecture in a top-down manner: ASILs are assigned to system-level hazards, and then they are iteratively decomposed and allocated to relevant subsystems and components.

ASIL decomposition rules may give rise to multiple alternative allocations, leading to an optimization problem of finding the cost-optimal allocations. Recognizing the difficulties of the problem, researchers have proposed dedicated tools using heuristics, such as Tabu search and genetic algorithms. However, these algorithms may find near-optimal solutions, potentially missing the optimal solutions desired by stakeholders.

In this paper, we aim at finding all optimal ASIL allocations using off-the-shelf solvers. We implement our approach using three major classes of state-of-the-art solvers: CSP (Constraint Satisfaction Problem), SMT (Satisfiability Modulo Theories), and ILP (Integer Linear Programming). We evaluate the feasibility and performance of our approach on three variants of a real-world Hybrid Braking System for electrical vehicle integration.

**CITATION:** Murashkin, A., Silva Azevedo, L., Guo, J., Zulkoski, E. et al., "Automated Decomposition and Allocation of Automotive Safety Integrity Levels Using Exact Solvers," *SAE Int. J. Passeng. Cars – Electron. Electr. Syst.* 8(1):2015, doi:10.4271/2015-01-0156.

## INTRODUCTION

Automotive systems are increasingly software-intensive and complex. As much as 80% of new vehicle features are partly or fully realized in software [1]. Driver assistance systems, vehicle-to-vehicle and vehicle-to-infrastructure communication, and vehicle electrification reinforce this trend. Many of these systems are safety-critical and the development of such systems requires new methods. The recently released ISO 26262 standard [2] addresses the functional safety of electric and electronic systems within road vehicles.

ISO 26262 prescribes a safety lifecycle, which identifies hazards, and assigns them with ASILs - Automotive Safety Integrity Levels - as a means to impose appropriate requirements and reduce system risk to

an acceptable level; the hazards' ASILs are ultimately inherited by architectural components. The higher the ASIL of a component, the higher the stringency of the requirements to be fulfilled; development cost grows accordingly. However, the standard allows for ASIL decomposition, which means that lower ASILs can be assigned to redundant components, subject to special decomposition rules. These rules typically generate several alternative assignments, leading to an optimization problem of finding assignments with minimum development costs for the overall system architecture.

The cost optimization of ASIL allocation has been studied before. Most importantly, existing works [3-4] have applied heuristic methods to solve this problem. Even though these algorithms can yield solutions

quickly, they suffer from inherent inaccuracy and incompleteness: the solutions they return may not be optimal; and even if these algorithms may happen to find some optimal solutions, they often fail to find all optimal solutions.

This paper addresses these shortcomings and proposes the use of modern exact solvers to compute the complete set of optimal solutions to the cost optimization problem of ASIL allocation, which we call the ASIL allocation problem for short. We aim at the proper encodings of the ASIL allocation problem in formal specifications that enable off-the-shelf solvers to solve the problem exactly and completely. We choose three major classes of state-of-the-art solvers: CSP (Constraint Satisfaction Problem) [5], SMT (Satisfiability Modulo Theories) [6], and ILP (Integer Linear Programming) [7]. In particular, we use Choco CSP [8], Z3 SMT [9], and CPLEX ILP [10] solvers in our experiments, due to their dramatic improvements in performance over the last decade. We demonstrate the feasibility and performance of our approach by experiments on three variants of a real-world hybrid braking system for electrical vehicles. To the best of our knowledge, we are the first to solve the ASIL allocation problem exactly using off-the-shelf solvers.

## BACKGROUND: ISO 26262 SAFETY LIFECYCLE AND ASIL DECOMPOSITION

The introduction of ISO 26262 in late 2011 meant that for the first time in the automotive sector, there is an industry-wide process to follow for the development of safety-critical systems. The standard covers the complete safety lifecycle of a system composed of Electrical or Electronic components - from management and development up to service and decommissioning. ISO 26262 has been around for three years now, but practitioners still struggle to comply with its guidelines. The processes prescribed by the standard are subject to the complexity of modern safety systems and their manual execution is often infeasible. One such process is known as ASIL allocation and decomposition.

Automotive Safety Integrity Levels (ASILs) are a key concept in ISO 26262. ASILs are used to assign requirements of different stringencies for the development and validation activities of safety-critical architectural elements. Four ASILs are defined: ASIL A, ASIL B, ASIL C and ASIL D; the stringency of the requirements grows from ASIL A to D. In addition, a QM level exists (quality management), and it denotes that no requirements apply when complying with ISO 26262. The standard defines the safety lifecycle to identify and assess hazards, determine safety requirements to reduce the risks to acceptable levels, and to manage and track these requirements ensuring adherence to them during vehicle development, production, and operation. The process considers an automotive system or subsystem and:

- identifies hazards as a result of system malfunctions;
- identifies hazardous events, which are a combination of hazards and operational situations;
- assigns an appropriate ASIL to the hazardous events according to their severity, exposure, and controllability;

- determines a safety goal for each hazardous event; the goal inherits the ASIL of its corresponding hazardous event;
- develops a safety concept yielding safety requirements;
- assigns safety requirements to architectural components;
- ensures that the components are developed according to the allocated safety requirements.

In general, each safety requirement inherits its ASIL level from its parent safety goal or requirement; however, the inherited ASIL may be lowered by decomposition of a requirement into redundant requirements implemented by sufficiently independent redundant components - this process is known as *ASIL decomposition*. Further, each component is implemented according to the standards needed to satisfy the highest ASIL allocated to it.

The vehicles we drive every day include multiple safety-critical functions that share components and that often have complex failure modes. It is not trivial to get a clear picture of the relationships between component failures and safety goal violations, and consequently, how system level ASILs can be allocated and decomposed across architectural elements. Classical safety analysis, such as Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA), via their systematic nature, can help us understand the failure behavior of a system. However, given the complexity of the systems at hand, their application is a long and error prone process. HiP-HOPS (Hierarchically Performed Hazard Origin and Propagation Studies) is a state-of-the-art model-based safety analysis technique and it helps by allowing for automated FTA and FMEA. In fact, the tool proposes a method for the assisted allocation of Safety Integrity Levels based on its FTA capabilities [11]. It is not the purpose of this article to describe this method in detail, but we have used it to obtain the information that allows the formulation of the optimization problem we tackle in this article.

## RUNNING EXAMPLE: HYBRID BRAKING SYSTEM

In this section, we go through the description of a Hybrid Braking System (HBS) for electrical vehicle integration [12] that is becoming established as a benchmark optimization problem for ASIL decomposition and allocation. Later on, we will use three variants of the HBS to evaluate our approach using three exact solvers.

The braking system is termed *hybrid* as braking is achieved through the combined action of two types of actuators - Electromechanical Brakes (EMBs) and In-Wheel Motors (IWMs). The IWMs' primary function is in the propulsion system; however, they also offer braking capabilities and can transform the kinetic energy of the vehicle into electrical power, stored in the battery; this increases the vehicle's range. The IWMs have limited braking torque availability at high wheel speeds and when the battery is close to a full state of charge; in these scenarios, the EMBs step in to meet the braking demands. Another key aspect to the HBS is the lack of mechanical or hydraulic link between the braking pedal and the actuators; this is a brake-by-wire system and therefore the driver's requests are transmitted via an electronic communication bus. Figure 1 shows the HBS architecture.

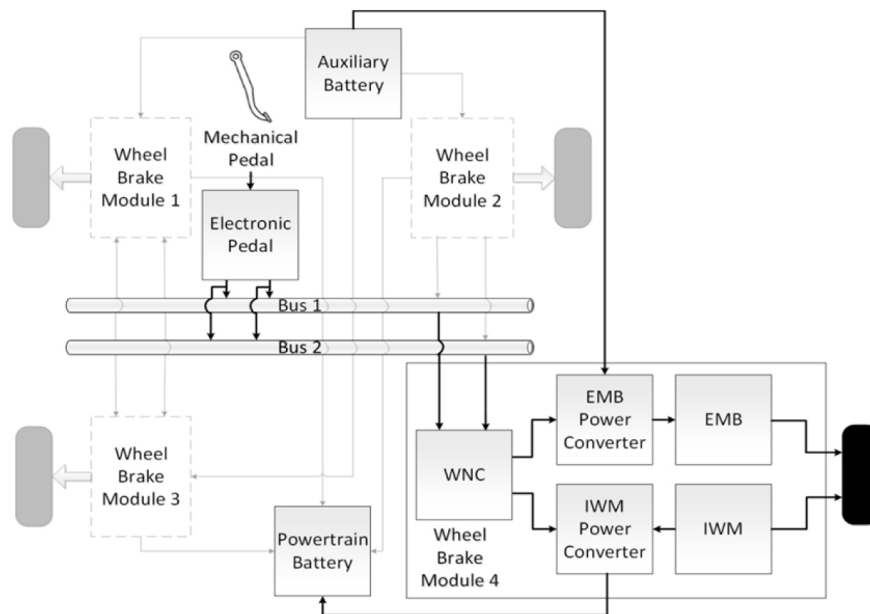


Figure 1. The Hybrid-Braking System example

The structure of the Wheel Brake Modules is shown only for one of the wheels but it is the same across the 4 wheels. There is a chain of components involved in providing the vehicle's braking function: as the driver presses the braking pedal, his actions are sensed and processed at an Electronic Pedal Unit; braking demands are calculated here for each of the vehicle's four wheels, and are sent via a duplex communication bus to individual Wheel Node Controllers (WNC). In the WNC, braking requests are determined for each of the actuators, and commands are sent accordingly to the power converters that control them. As described earlier, while braking, the IWMs produce electric power which is fed to the vehicle's powertrain battery; conversely, for EMB braking, power needs to flow from the auxiliary battery to the actuator.

No system is one hundred percent reliable. Any component in the chain is subject to failure. Some component failures can be tolerated whilst other failures or possible combinations of failures can cause severe system failures - the system's hazards.

### Hazards and ASILs

The three HBS variants we use vary in complexity; in this section we focus on describing the simplest, which only contemplates the braking of one wheel. We consider two system hazards:

- Hazard 1 (H1), *No Braking After Command*, happens when braking is not provided at all after a driver's request has been initiated;
- Hazard 2 (H2), *Wrong Value Braking*, occurs when the output value is different from the requested, leading to excessive or insufficient braking.

Normally, a safety engineer would enumerate operational scenarios, identify respective hazardous events and follow the risk assessment procedure prescribed from ISO 26262 to determine their ASILs. For our illustrative example, we stop at hazard identification and ASILs

are attributed to them solely on the notion of the hazard's severity; H1 was assigned with ASIL D and H2 with ASIL A. The method presented here is still applicable in case one undertakes the whole process from the standard.

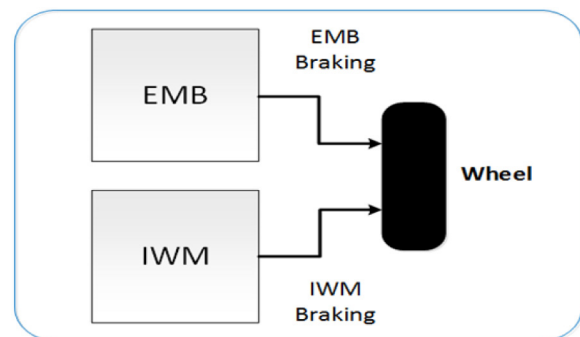


Figure 2. The final part of the braking system; the outputs of Electro-mechanical brake (EMB) and In-Wheel Motors (IWM) provide the total braking required for one wheel

Figure 2 shows the final part of the braking chain for one wheel, which consists of two actuators, Electromechanical Brake (EMB) and In-Wheel Motor (IWM), and the wheel. Hazards can be expressed by incorrect functioning of the system's outputs. In our example, H1 occurs when both braking actuators have their outputs omitted (i.e., they do not provide an output when they are supposed to). H2 happens when at least one of the actuators provides an output with an incorrect value.

### Fault Tree Analysis and Minimal Cut Sets

Fault tree analysis (FTA) allows the analysis of system architectures and can determine how component level failures can cause system hazards. This information is conveniently produced from FTA in the form of *minimal cut sets*, that is, the minimal combinations of component failure modes that, when occurring together, lead to a