Summary of the Doctoral Dissertation
Doctoral Program in Control and Computer Engineering

NOVEL VALIDATION TECHNIQUES FOR AUTONOMOUS VEHICLES

Jacopo Sini
Supervisor: **Prof. Massimo Violante**
Politecnico di Torino

The automotive industry is facing challenges in producing electrical, connected, and autonomous vehicles. Even if these challenges are, from a technical point of view, independent from each other, the market and regulatory bodies require them to be developed and integrated simultaneously.
The development of autonomous vehicles implies the development of highly dependable systems. This is a multidisciplinary activity involving knowledge from robotics, computer science, electrical and mechanical engineering, psychology, social studies, and ethics.
Nowadays, many Advanced Driver Assistance Systems (ADAS), like Emergency Braking System, Lane Keep Assistant, and Park Assist, are available. Newer luxury cars can drive by themselves on highways or park automatically, but the end goal is to develop completely autonomous driving vehicles, able to go by themselves, without needing human interventions in any situation.
The more vehicles become autonomous, the greater the difficulty in keeping them reliable. It enhances the challenges in terms of development processes since their misbehaviors can lead to catastrophic consequences and, differently from the past, there is no more a human driver to mitigate the effects of erroneous behaviors.

Primary threats to dependability come from three sources: misuse from the drivers, design systematic errors, and random hardware failures.
These safety threats are addressed under various aspects, considering the particular type of item to be designed. In particular, for the sake of this work, we analyze those related to Functional Safety (FuSa), viewed as the ability of a system to react on time and in the proper way to the external environment.
From the technological point of view, these behaviors are implemented by electrical and electronic items.
Various standards to achieve FuSa have been released over the years. The first, released in 1998, was the IEC 61508. Its last version is the one released in 2010.
This standard defines mainly:

- a Functional Safety Management System (FSMS);
- methods to determine a Safety Integrated Level (SIL);
- methods to determine the probability of failures.

To adapt the IEC61508 to the automotive industry's peculiarity, a newer standard, the ISO26262, was released in 2011 then updated in 2018.
This standard provides guidelines about FSMS, called in this case *Safety Lifecycle*, describing how to develop software and hardware components suitable for functional safety. It also provides a different way to compute the SIL, called in this case Automotive SIL (ASIL), allowing us to consider the average driver's abilities to control the vehicle in case of failures. Moreover, it describes a way to determine the probability of random hardware failures through Failure Mode, Effects, and Diagnostic Analysis (FMEDA).

This dissertation contains contributions to three topics:

- random hardware failures mitigation;
- improvement of the ISO26262 Hazard Analysis and Risk Assessment (HARA);
- real-time verification of the embedded software.

As the main contribution of this dissertation, I address the safety threats due to random hardware failures (RHFs).
For this purpose, I propose a novel simulation-based approach to aid the Failure Mode, Effects, and Diagnostic Analysis (FMEDA) required by the ISO26262 standard. Thanks to a SPICE-level model of the item, and the adoption of fault injection techniques, it is possible to simulate its behaviors obtaining useful information to classify the various failure modes. The proposed approach evolved from a mere simulation of the item, allowing only an item-level failure mode classification up to a vehicle-level analysis. The propagation of the failure modes' effects on the whole vehicle enables us to assess the impacts on the vehicle's drivability, improving the quality of the classifications. It can be advantageous where it is difficult to predict how the item-level misbehaviors propagate to the vehicle level, as in the case of a *virtual differential gear* or the mobility system of a robot. It has been chosen since it can be considered similar to the novel light vehicles, such as electric scooters, that are becoming more and more popular. Moreover, my research group has complete access to its design since it is realized by our university's DIANA students' team. When a SPICE-level simulation is too long to be performed, or it is not possible to develop a complete model of the item due to intellectual property protection rules, it is possible to aid this process through behavioral models of the item. A simulation of this kind has been performed on a mobile robotic system. Behavioral models of the electronic components were used, alongside mechanical simulations, to assess the software failure mitigation capabilities.

Another contribution has been obtained by modifying the main one. The idea was to make it possible to aid also the

Hazard Analysis and Risk Assessment (HARA).
This assessment is performed during the *concept phase*, so before starting to design the item implementation. Its goal is to determine the hazards involved in the item functionality and their associated levels of risk. The end goal of this phase is a list of *safety goals*. For each one of these safety goals, an ASIL has to be determined.
Since HARA relies only on designers expertise and knowledge, it lacks in objectivity and repeatability.
Thanks to the simulation results, it is possible to predict the effects of the failures on the vehicle's drivability, allowing us to improve the severity and controllability assessment, thus improving the objectivity. Moreover, since simulation conditions can be stored, it is possible, at any time, to recheck the results and to add new scenarios, improving the repeatability.

The third group of contributions is about the real-time verification of embedded software. Through Hardware-In-the-Loop (HIL), a software integration verification has been performed to test a fundamental automotive component, mixed-criticality applications, and multi-agent robots.
The first of these contributions is about real-time tests on Body Control Modules (BCM). These modules manage various electronic accessories in the vehicle's body, like power windows and mirrors, air conditioning, immobilizer, central locking. The main characteristics of BCMs are the communications with other embedded computers via the car's vehicle bus (Controller Area Network) and to have a high number (hundreds) of low-speed I/Os.
As the second contribution, I propose a methodology to assess the error recovery system's effects on mixed-criticality applications regarding deadline misses. The system runs two tasks: a critical airplane longitudinal control and a non-critical image compression algorithm. I start by presenting the approach on a benchmark application containing an instrumented bug into the lower criticality task; then, we improved it by injecting random errors inside the lower criticality task's memory space through a debugger. In the latter case, thanks to the HIL, it is possible to pause the time domain simulation when the debugger operates and resume it once the injection is complete. In this way, it is possible to interact with the target without interfering with the simulation results, combining a full control of the target with an accurate time-domain assessment.
The last contribution of this third group is about a methodology to verify, on multi-agent robots, the synchronization between two agents in charge to move the end effector of a delta robot: the correct position and speed of the end effector at any time is strongly affected by a loss of synchronization.
The last two contributions may seem unrelated to the automotive industry, but interest in these appliactions is gaining. Mixed-criticality systems allow reducing the number of ECUs inside cars (for cost reduction), while the multi-agent approach is helpful to improve the cooperation of the connected cars with respect to other vehicles and the infrastructure.

The fourth contribution, contained in the appendix, is about a machine learning application to improve the social acceptance of autonomous vehicles.
The idea is to improve the comfort of the passengers by recognizing their emotions. I started with the idea to modify the vehicle's driving style based on a real-time emotions recognition system but, due to the difficulties of performing such operations in an experimental setup, I move to analyze them offline. The emotions are determined on volunteers' facial expressions recorded while viewing 3D representations showing different calibrations. Thanks to the passengers' emotional responses, it is possible to choose the better calibration from the comfort point of view.