Framework for Safety in Autonomous Vehicles

Matthieu Carré[*,**] Ernesto Exposito[*]
Javier Ibañez-Guzmán[*,**]

[*] Univ Pau
Pays Adour, E2S UPPA, LIUPPA, EA3000, Anglet, 64600, France
matthieu.carre@univ-pau.fr
ernesto.exposito@univ-pau.fr
[**]Renault S.A.S, 1 av. du Golf, Guyancourt, 78288, France
javier.ibanez-guzman@renault.com

Abstract. The integration of the Safety dimension has been a critical requirement when developing and deploying Autonomous Vehicles (AV). While much progress has been achieved within the past years, most work has centred on providing vehicles with the ability to navigate autonomously. Safety has emerged as the major challenge. This paper proposes a reference architecture that incorporates the notion of self-safety into existing AV architectures. This architecture consists in a multi-layered control loop aimed at managing self-adaptation processes in order to ensure safety at run-time.

1 Introduction

The development and deployment of Autonomous Vehicles (AV) is a very challenging endeavour from a safety perspective. Vehicles must navigate through multiple situations preventing any potential harm and without disturbing traffic flow in order to be accepted by the society. Safe driving under full computer control also requires to interact and operate around with different entities within complex road networks and to appropriately address their different behaviours.

While much progress has been achieved within the past years, most work has centred on providing vehicles with the ability to navigate autonomously. Safety has emerged as the major challenge, not only on the vehicle behavioural side to address edge-cases (i.e. navigate safely) but also to manage malfunctions or external disturbances (i.e. fault tolerant).

Current work in the safety domain has proposed relevant approaches for the analysis, refinement, integration and enforcement of AV safety. Considering safety as a dynamic control problem as proposed by Leveson et al. (2015) and Leveson and Thomas (2018) shows promising applications and several interesting results have been presented in Lefèvre et al. (2014), Raste et al. (2015), Bagschik et al. (2017b) and Cook et al. (2018). Complementary research investigates the trade-off with the traditional failure analysis for hazards coverage as in Sulaman et al. (2019) and Ford (2018) while others address the compatibility of the approach with the current AV standards as in Abdulkhaleq et al. (2017), Sabaliauskaite et al. (2018) and Vernacchia (2018). However, most of these works converges on the difficulty to provide a