Safety Analysis Group (GAS)
Computer and Digital Systems Engineering Department (PCS)
School of Engineering (Escola Politécnica - Poli)
University of São Paulo (USP)
São Paulo, Brazil, 2017

Assuring Fully Autonomous Vehicles Safety by Design

The Autonomous Vehicle Control (AVC) Module Strategy

Caroline Bianca S. T. Molina
Jorge Rady Almeida Jr.
Lúcio F. Vismari
Rodrigo Ignacio R. González
Jamil K. Naufal Jr.
João Batista Camargo Jr.

Overview

- Autonomous vehicles are expected to lead a reduction in traffic accidents due to the mitigation of human drivers errors
- Autonomous vehicles shall mitigate the existing hazards at the roadway transportation system while **not creating new hazards**
- There is no specific method to analyze and assure safety levels of the autonomous vehicle systems
- This paper proposes a **design strategy** that may be used at the architecture design level of autonomous vehicles to facilitate the development, analysis and safety level assuring

Overview

- An independent module, the **Autonomous Vehicle Control (AVC),** is going both **to interact with the vehicle's systems** and create a **protection layer**
- The AVC could be used with any autonomous vehicle system and could be tested individually
- This strategy is based on both recommended practices published by Society of Automotive Engineers (SAE) and on approaches used on other transportation system domains
- The proposed module will be intended for **fully autonomous cars** (high levels of driving automation)

Motivation

- Autonomous vehicles embody a **disruptive change** in our society
- Many benefits will come hand in hand with this new technology
  - The end of the need for car drivers
  - Possibility the use of cars by people with disabilities, the elderly, children without assistance
  - The potential **reduction of traffic accidents** caused by human errors
- High-tech sensors, cameras, and radar have been developed and are being applied to monitor the vehicle and the environment around it
- Autonomous vehicles systems are capable of properly guiding the vehicle (defining routes, braking points, and even the acceleration for overtaking), and also controlling possible problems related to the vehicle stability (for example, vehicle maneuver)

Motivation

- Due to the substantial benefits that autonomous vehicles should provide, their development has been attracting the interest of many stakeholders
- It is expected that between **2020** and 2025 the autonomous vehicles will be running in the current Roadway Transportation System (RTS)

Challenge

- Given that these vehicles are been manufactured very fast, **safety aspects could have been overlooked**
- When inserting autonomous vehicles into the RTS, at least the same safety levels that are achieved when human drivers control the vehicle must be guaranteed
- Preexistent rules for operation and manufacturing that are defined by regulatory agencies shall also be followed

Challenge

- However, these preexisting rules are not directly applicable to autonomous vehicle systems
- Autonomous vehicles must be prepared for unexpected, abnormal situations

How to ensure safety in these systems?

How will they behave when facing dangerous events?

AVC Module Proposal

- We propose to develop a system element – the **Autonomous Vehicle Control (AVC) module** – that will execute the driver functionalities in a fully autonomous vehicle
- The AVC module is composed by a two-layer hierarchical architecture, with the lowest layer being responsible for protecting the vehicle movement and controlling it in critical situations
- The AVC module is analogous to the **Automatic Train Control (ATC)** concept, applied in railway systems
  - Automatic Train Control (ATC), automatically controls train movement, both enforcing **train safety** and **managing train movement**
  - ATC system includes a subsystem called **Automatic Train Protection (ATP)**, responsible for maintaining the fail-safe protection against collision, excessive speed, and other hazardous conditions
  - ATC system may also include the **Automatic Train Operation (ATO)** and/or the Automatic Train Supervision (ATS)

AVC Module Proposal

- The same approach could be applied to autonomous vehicles
- The AVC module separates the operational layer from protection layer – the **Autonomous Vehicle Operation (AVO)** and the **Autonomous Vehicle Protection (AVP)**, respectively
- They are responsible for adequate operation (AVO) and safe control (AVP) of the autonomous vehicle.

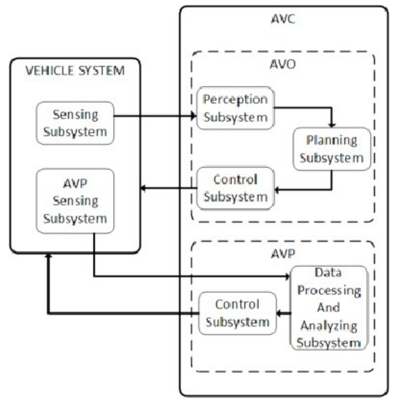

Fig. 1. High-level AVC module structure

SSIV Safety and Security of Intelligent Vehicles — GAS Grupo de Análise de Segurança, Escola Politécnica da USP — 9

AVC Module Proposal

- **AVO** sub-module is responsible for the **navigation** of the vehicle, setting the direction and the correct speed
- AVO is the sub-module who interprets the data coming from the sensing subsystem that is embedded in the vehicle, makes the route plans and maneuvers the vehicle from the processed data, and, finally, issue commands to the vehicle

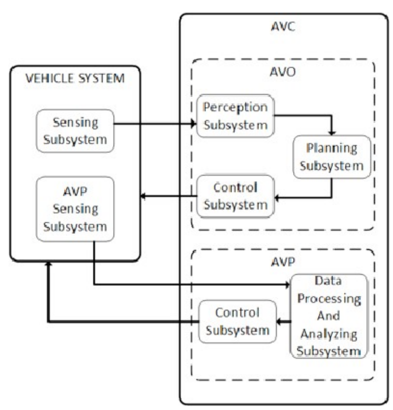

Fig. 1. High-level AVC module structure

SSIV Safety and Security of Intelligent Vehicles — GAS Grupo de Análise de Segurança, Escola Politécnica da USP — 10

AVC Module Proposal

- **AVP** sub-module, in turn, **monitors** the system variables (e.g., vehicle speed) and, if they exceed their respective safety limits (e.g. maximum speed of the road), it takes the vehicle to a **safe state** (e.g. the AVP reduces the vehicle speed)
- AVP also monitors the '**health**' of the system, taking it to a safe state whenever it detects an abnormal/fault situation

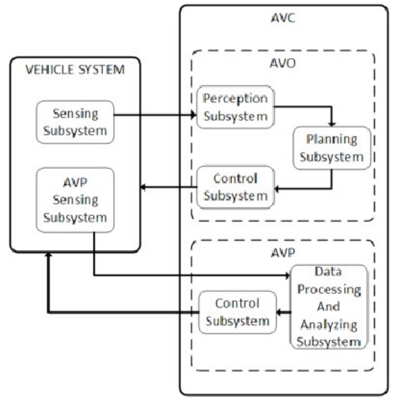

Fig. 1. High-level AVC module structure

AVC Module Proposal

- AVP is also always monitoring the roadway elements in order to **detect problems** that may arise during the vehicle movement, and, when a safety issue is detected, AVP must enforce a safe state to the vehicle
- The AVC module could be used no matter how the vehicle system is implemented, because the AVC module only requires specific data sets to control the vehicle

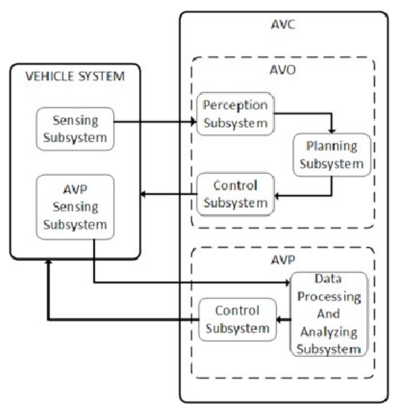

Fig. 1. High-level AVC module structure

AVC Module Proposal

AVP must be safe and reliable

- The AVP sub-module monitors the environment through its own equipment (AVP sensing subsystem), which is **independent** of the vehicle's (sensing) subsystem
- This separate data acquisition by sub-module could avoid the **common cause failure** mode and enables the effectiveness of the fallback plan present in the AVP.
- The AVP sub-module, in addition to being independent from other systems that could perform the same function, shall have more reliable equipment, and may even have **redundancy**

AVC Module Proposal

- The AVP will send commands to the vehicle whenever it detects that something can lead the vehicle, and/or the passengers to an **unsafe situation**
- AVP monitors **environmental obstacles** in order to detect if any of them are in a situation that was not predicted by the AVO. It is also activated when a **malfunction of the AVO** is detected. If such an unsafe situation occurs, AVP sends messages that triggers a fallback plan, activating the emergence brakes or leading to a maneuver
- The AVP also monitors the speed of the vehicle and its direction considering the surrounds of the vehicle

AVC Module Proposal

- The AVP sub-module is designed to support **degraded modes of operation** in the event of failure
- The AVP behavior depends on what generated the risk situation, which may be a mechanical failure, a failure to acquire data, a malfunction of any of the systems, or due to an unexpected situation

AVC and Autonomous Vehicle Systems

- **Society of Automotive Engineers (SAE)** published some recommended practices which present driving automation levels in on-road motor vehicles, including the functional definitions for these advanced driving automation levels
- This document defines some of the vehicle's systems, describes each **driving automation level** and detail how such systems are used in each of these driving automation levels
- SAE presented the definition of **Dynamic Driving Task (DDT)**, which is the system that contains the functions required to operate an autonomous vehicle in on-road traffic

AVC and Autonomous Vehicle Systems

- SAE defines three types of driver effort in order to drive properly
  - ***strategic*** (involves trip planning, best routes to take, etc.)
  - ***tactical*** (maneuvering the vehicle in traffic, selecting an appropriate speed, etc.)
  - ***operational*** (involves micro-corrections to steering, braking and accelerating to maintain lane position in traffic or to avoid hazardous event in the vehicle's pathway)
- **Tactical** and **operational** efforts are considered as part of the **DDT**

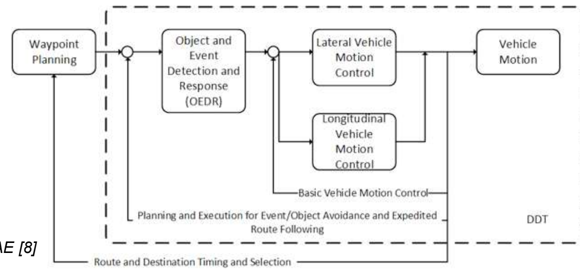

Fig. 2. DDT scheme presented by SAE [8]

AVC and Autonomous Vehicle Systems

AVC and DDT

- The AVC module presents **similarities** with the structure presented in DDT
- Fig. 3 identifies what would be the DDT in the structure proposed in the AVC
- One difference is that the planning system is not present in DDT

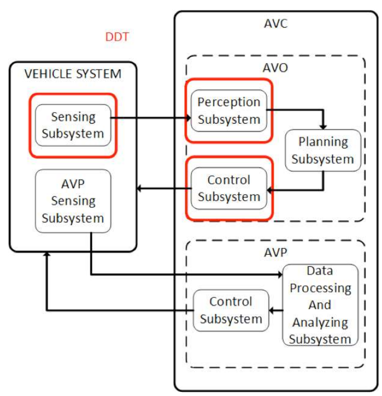

Fig. 3. Representing DDT at the high-level AVC module

Final Remarks

- A design strategy that may be applied in the development of fully autonomous vehicles
- AVC module has the objective to properly control the autonomous vehicle by separating its functionalities into two sub-modules (AVO and AVP)
- The proposal to separate the operational layer from the protection layer in the task of managing the autonomous vehicle movement would facilitate:
  1. The **analysis of safety levels**, because the AVP should be analyzed separately, since it is the responsible for keeping the vehicle safe
  2. The repair and **detection of possible errors**, since the modules would be separated
  3. The process of developing the whole system

Final Remarks

- The proposal is shown to be a potential solution to circumvent, at least conceptually, the **gap** related to the safety assurance of autonomous vehicles
- However, there is still need for a more detailed evaluation of the whole system, including testing to better evaluate this proposal and also to improve the behavior of the AVP

Next steps

- **Development** of the AVC module in an implementable way that enables its test and validation
- More **tests** are going to be performed in order to improve the protection layer (AVP sub-module)
- **Extend** the AVC module to others levels of driving automation (those who have human intervention)

This work was supported by the RLAM Innovation Center, Ericsson Telecomunicações S.A.*, Brazil*

References

1. World Health Organization Website: <http://www.who.int/mediacentre/factsheets/fs358/en> - accessed on March 10th.
2. E. Ohn-Bar and M. M. Trivedi, " Looking at Humans in the Age of Self-Driving and Highly Automated Vehicles", IEEE Transactions on Intelligent Vehicles, vol. 1, no. 1, pp. 90-104, March 2016.
3. M. Campbell, M. Egerstedt, J. P. How and R. M. Murray, "Autonomous driving in urban environments: approaches, lessons and challenges", Philosophical Transactions: Mathematical, Physical and Engineering Sciences, vol. 368, no. 1928, October 2010, pp. 4649-4672.
4. Business Insider News: http://www.businessinsider.com/companies-making-driverless-cars-by-2020-2017-1/#tesla-recently-made-a-big-move-to-meet-its-goal-of-having-a-fully-self-driving-car-ready-by-2018-1 - accessed on March 24th, 2017.
5. A. Avizienis, J. C. Laprie, B. Randell, C. Landwehr, "Basic COncepts and Taxonomy of Dependable and Secure Computing", IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, January-March 2004.
6. B. Paden, M. Čáp, S. Z. Yong, D. Yershov, E. Frazzoli, "Survey of Motion Planning and Control Techniques for Self-Driving Urban Vehicles", IEEE Transactions on Intelligent Vehicles, vol. 1, no. 1, pp. 33-55, March 2016.
7. D. Bevly, X. Cao, M. Gordon, G. Ozbilgin, D. Kari, B. Nelson, J. Woodruff, M. Barth, C. Murray, A. Kurt, K. Redmill, U. Ozguner, "Lane Change and Merge Maneuvers for Connected and Automated Vehicle: A Survey", IEEE Transactions on Intelligent Vehicles, vol. 1, no. 1, pp. 105-120, March 2016.
8. International Organization for Standardization (ISO) website: https://www.iso.org/standard/43464.html - accessed on March 24th, 2017.
9. Society of Automotive Engineers, "SAE J3016 - Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles", 2016.
10. IEEE Vehicular Technology Society, "IEEE Standard for Communications - Based Train Control (CBTC) Performance and Functional Requirements", February 2005.
11. National Highway Traffic Safety Administration Website: <https://one.nhtsa.gov/cars/rules/> - accessed on April 21st.
12. The Guardian News: https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk - accessed on March 24th, 2017.