The Safety of Self-Driving Vehicles
A Tutorial

© Dr. Juan R. Pimentel
Professor of Computer Engineering
Kettering University, Michigan, USA

President
LeSoft LLC

INTRODUCTION

Safety has been ranked as the number one concern for the acceptance and adoption of autonomous vehicle (AV) or self-driving vehicles and understandably so because safety has one of the most complex requirements for the development of safe self-driving vehicles. Traditionally, safety follows functional safety concepts as detailed in ISO 26262. However, autonomous driving safety goes beyond ISO 26262 and includes other safety concepts such as safety of the intended functionality (SOTIF), and Multi-Agent safety. In addition, governments at all levels are stepping in to help define and address multiple safety requirements appropriate for autonomous vehicles. Thus, safety has become the most important concerns for automakers, service providers, governments, and all associated stakeholders in the self-driving eco-system.

In this tutorial you will be exposed to the main principles and issues behind the safety of autonomous vehicles including functional safety, SOTIF, and behavioral safety. Particular emphasis will be placed on the safety hazards involved when a vehicle shares the road with other vehicles and pedestrians. The role of governments will be also discussed such as the U.S. NHTSA safety guidelines for autonomous vehicles and the main elements to be addressed while writing a corresponding safety report. Several examples and a case study will be used to complement the material.

TUTORIAL OBJECTIVES

After successful completion of this tutorial, the participants should be able to:

- List and describe the most fundamental ideas of Functional safety, Multi-Agent safety, and SOTIF.
- Articulate the concepts of hazard, risk, risk assessment, and risk reduction
- Describe the salient features of the ISO 26262 standard
- Summarize the Functional Safety Concept for a specific subsystem of an AV.
- Summarize the main NHTSA safety guidelines for autonomous vehicles
- Summarize the main elements to be addressed while writing a safety report for an autonomous vehicle.

TUTORIAL SUMMARY

This tutorial covers the fundamental principles, techniques, best practices, and methodologies of functional and behavioural safety for autonomous vehicles. Emphasis is placed on Multi-Agent safety, SOTIF, and the role of governments to deploy safe vehicles. The tutorial begins with an introduction to AV safety and risk management followed by a coverage of Multi-Agent safety and SOTIF and ending with a discussion of government guidelines and writing a safety report.

TUTORIAL OUTLINE

- Introduction
- Errors, faults, failures, hazards, harm, accidents, mishaps
- Risk, Risk Assessment, and Risk reduction
- Safe Autonomous Vehicle platform
    - Functionality
    - Perception system
    - Computing platform
- Risk classification (Automotive safety integrity level: ASIL)
- Preliminary hazard analysis (PHA)
- Overview of functional safety and ISO 26262
- Development of the Functional Safety Concept
- Introduction to Multi-Agent Safety
    - Sharing the road with others
- Vehicle dynamics considerations
- Accidents: Fault, Blame, Guilt
- Responsibility Sensitive Safety (RSS)
    - Ego vehicle
    - Safe actions/behaviors
    - Absolute safety
- Safety Guarantees, Cautious Driving
- Guaranteeing behavioral safety:
    - Safe longitudinal distance
    - Safe cut-in of the ego vehicle
- Safety of the Intended Functionality (SOTIF)
- Role of governments in AV safety
- NHTSA safety guidelines
- Writing a safety report
    - Operational design domain (ODD)
    - Object and event detection and response (OEDR)
    - Fallback (Minimum Risk Condition)

Example # 1:
Example of an autonomous vehicle top level design including:

- Functionality
- Perception system
- Computing platform
- AV platform

Example # 2:
Development of a PHA (preliminary hazard analysis) for your autonomous vehicle.

Example # 3:
Identification of the safety hazards involved when a vehicle shares the road with other vehicles.

Example # 4:
Specification of the main safety critical functions (SFC) for an autonomous vehicle, including:

- ASIL value
- Functional safety
- Safety of the Intended Functionality (SOTIF)
- Multi-agent safety

Case Study
Analysis of the safety reports of two well-known companies.