Juan R. Pimentel  
Professor of Computer Engineering  
Kettering University

In this book, we have characterized SOTIF, one of the main categories of automated vehicle safety. It is the safety category that is not due to component or element faults but rather to performance limitations or functional insufficiencies. Perhaps the best examples of SOTIF hazards are those due to functional insufficiencies of the perception system of an automated vehicle. There are a number of outstanding safety issues discussed in the book, which will hopefully help clarify this topic, such as the nature of SOTIF, its underlying sources, and specific risk reduction actions. There are two primary approaches to reduce risk, a management approach and a technical approach. The former is based on using system engineering methodologies, particularly the V-model, while the latter involves specific risk reduction measures or mechanisms such as redundancy. In addition to characterizing the safety category of SOTIF, we have included a set of ten papers that are representative of research in this category. Although there is a fair amount of work in this area, much more work is needed to solve a number of outstanding issues, for example, how to properly validate safety targets and how to deal with the inherent uncertainty and complexity of the environment and the intrinsic uncertainty of functional implementations of machine learning.

Accordingly, most SOTIF papers deal with using system engineering techniques or risk reduction measures. Reducing SOTIF risk is challenging because of the nondeterministic and uncertain nature of the environment, particularly during bad weather. In addition, the intrinsic uncertainty of the implementation of some data processing solutions, for example, machine learning, contributes to the challenging nature of validating automated vehicle safety. Papers that promote using system engineering techniques emphasize a thorough approach to generate safety requirement specifications together with detailed plans for testing, verification, and validation. Papers that promote using risk reduction measures or mechanisms emphasize error and failure detection together with fault-tolerant techniques aimed to achieve fault-safe, fail-operational, or fail-silent systems. In addition, the introductory chapter presents a risk-based model that integrates SOTIF into a risk-based approach. This requires additional definitions and/or more general interpretations of those in ISO 26262. The proposed model introduces a new source of error, performance error, that models accident sources in the SOTIF category.

The topic of safety measures for measuring the level of safety is crucial for automated vehicle safety. One type of safety measurement is around standards, processes, procedures, and design, and it is most useful at the design and simulation stages. One example of a safety measure that can be used during design is the number of expected catastrophic failures per year of operation (e.g., 500 hours) [24]. Another example of a safety measure is MDTA, the mean distance to accident (e.g., in km or miles) used in SAE paper #6. It can be argued that it would be difficult for all stakeholders to agree on a universal set of safety measures at this low level of abstraction.
Safety has been ranked as the number one concern for the acceptance and adoption of automated vehicles since safety has driven some of the most complex requirements in the development of self-driving vehicles. Recent fatal accidents involving self-driving vehicles have uncovered issues in the way some automated vehicle companies approach the design, testing, verification, and validation of their products.

Traditionally, automotive safety follows functional safety concepts as detailed in the standard ISO 26262. However, automated driving safety goes beyond this standard and includes other safety concepts such as safety of the intended functionality (SOTIF) and multi-agent safety.

Safety of the Intended Functionality (SOTIF) addresses the concept of safety for self-driving vehicles through the inclusion of 10 recent and highly relevant SAE technical papers. Topics that these papers feature include the system engineering management approach and redundancy technical approach to safety.

As the third title in a series on automated vehicle safety, this contains introductory content by the Editor with 10 SAE technical papers specifically chosen to illuminate the specific safety topic of that book.

These books will contribute to the understanding and development of safety of automated vehicles.

Juan R. Pimental

RELATED RESOURCES:
Autonomous Vehicles for Safer Driving
Author: Ronald K. Jurgen
Product Code: PT-158

V2V/V2I Communications for Improved Road Safety and Efficiency
Author: Ronald K. Jurgen
Product Code: PT-154

Autonomous Technologies: Applications that Matter
Author: William C. Messner
Product Code: JPF-AUV-004

SAE Journal of Connected and Automated Vehicles
Product Code: 2574-075X

more related resources inside...

An SAE Technical Paper Compilation gathers judiciously selected papers important to a topic or theme, often with extensive editorial input and additional content.