Juan R. Pimentel  
Professor of Computer Engineering  
Kettering University  

In this book, we have discussed the ISO standard 26262 in the context of the safety of automated vehicles. Although the second edition of ISO 26262 (2018) included many enhancements to the original edition of 2011, it did not include automated vehicles. As noted in the epilogue of book 3 in this SAE collection, there are two primary approaches to reduce risk, a management approach and a technical approach. The former is based on using systems engineering (SE) methodologies, particularly the V-model, while the latter involves specific risk reduction measures or mechanisms such as redundancy. In this book we have summarized the main concepts of SE as applied to automated vehicles, emphasizing the concept of MBSE (model-based systems engineering) and the use of the SysML language. It is not claimed that SysML is the most complex or best language; however, it is one that is often used in automotive and automated vehicle applications. 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 various underlying areas such as SE, control systems, DFMEA, STPA, HARA, and risk reduction techniques, more work is needed to unify these areas into a coherent body of knowledge with explicit applications to automated vehicles.

It is noteworthy that STPA is a relatively new methodology (at least when compared to DFMEA) that explicitly uses SE principles and control systems structures to identify hazards and to design mitigation solutions for risk reduction. As demonstrated in some of the papers included in this collection, STPA can benefit immensely from MBSE and SE languages such as SysML. Nevertheless, the STPA process is somewhat ad hoc, and more work is needed to define a possible international standard. Such standard would greatly contribute to the application of STPA for automated vehicles.
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.

The Role of ISO 26262 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 model-based systems engineering (MBSE) and the use of SysML language in a management-based approach to safety.

As the fourth 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.

ISBN: 978-0-7680-0274-4