Functional Safety Considerations for Autonomous Driving and Advanced Driver Assistance Systems

Add value.
Inspire trust.

White paper

Abstract

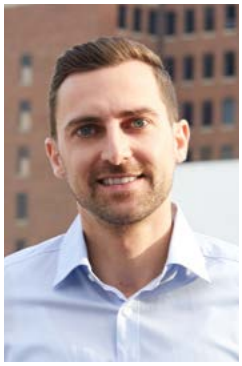
As most new passenger road vehicles are now manufactured with some form of assisted driving module, the future of advanced driver assistance systems (ADAS) and autonomous driving (AD) is looking extremely positive. However, as a failure can be catastrophic for humans that are in or around such vehicles, safety is paramount. This white paper explores the current market situation for AD/ADAS, including the types of vehicles integrating these innovative technologies and end-user perceptions. We will also discuss the relevant functional safety standards, and explore the issues and considerations surrounding functional safety for AD/ADAS vehicles.

TÜV SÜD

TÜV®

Contents

About TÜV SÜD expert



Stefan Merkl

Global Head of Automotive, TÜV SÜD Auto Service GmbH

Stefan Merkl is the Global Head of the Automotive business at TÜV SÜD. He holds a Master's degree in Systems Engineering & Management. In his 10+ year career at TÜV SÜD, he has successfully led local and global teams and driven several customer projects, as well as developed and managed internal global projects and strategies across eight different countries. He has lived in Germany, China and the United States for several years and built an extensive network in industry and government institutions around the world. His current global responsibilities include the fields of homologation for vehicle, systems and components, as well as environment and emissions.

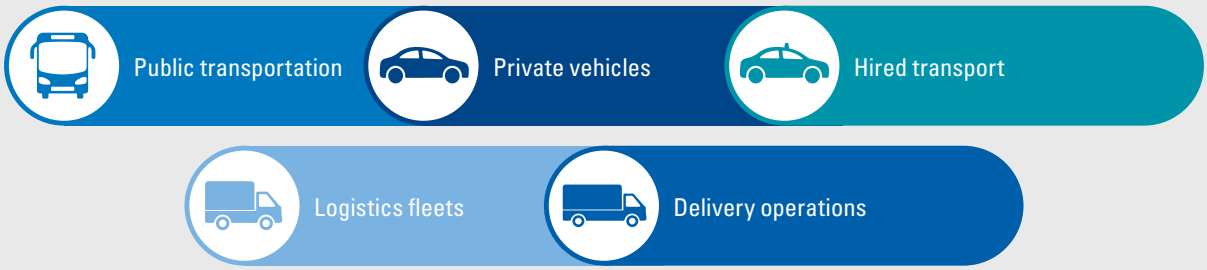
Introduction

Advanced driver assistance systems (ADAS) and autonomous driving (AD) are slowly but surely becoming a reality with the advancement of algorithmic learning. While the artificial intelligence (AI) providing assistance is the core driver of AD/ADAS innovation, functional safety is also critical to the future of AD/ADAS vehicles.

Functional safety is a discipline that must be considered when developing all parts of a vehicle system, including the architectural design, software and hardware components. A failure at any point can be disastrous for humans in or around an AD/ADAS vehicle. Even a single failure can compromise its integrity, and may even generate a cascade of failures. Ensuring functional safety is, therefore, a priority for manufacturers of such vehicles and vehicle systems.

What types of vehicles are implementing AD/ADAS?

The general public tends to immediately associate the idea of autonomous vehicles or driving assistance with passenger vehicles on main roadways. But there are many instances in which driverless on-road vehicles could be beneficial, including:

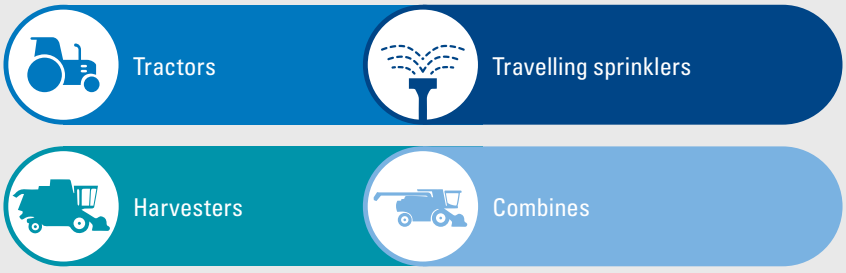


Most newer vehicles already feature some form of ADAS, whether as assisted steering, assisted braking or both. Around the globe, cities are testing fully driverless vehicles in various configurations.

However, passenger on-road vehicles are only one area in which AD/ADAS vehicles can shine. In the agricultural area, semi-autonomous and completely autonomous vehicles have already been in operation for several years.

Several companies pioneered the use of autonomous steering in tractors, and since then those companies have produced multiple vehicles capable of operating efficiently in enclosed fields away from public roadways.

Some still require a person in a cab to monitor other aspects of the machine's job. Others use cameras, GPS and light detection and ranging (LiDAR, typically used to measure distances) to keep the vehicle and its machinery operating at speeds of up to 20 miles per hour. Agricultural vehicles using AD/ADAS technology include but are not limited to:



Industrial use of AD/ADAS vehicles has also experienced major growth over the past few years, with completely autonomous robots used within warehouses and larger machinery used in yard operations. Even some harbours and airports are adopting certain aspects of AD/ADAS technology to minimise worker risk while improving speed and efficiency.

Public perception of AD/ADAS

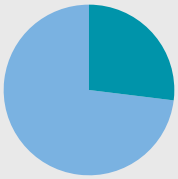
The global automotive industry is working hard on autonomous technologies and future mobility solutions. The US is considered one of the most lucrative markets, especially for ADAS, as it has always been an innovation hub for global automakers [1]. Nevertheless, the Partners for Autonomous Vehicle Education (PAVE) [2] advocacy group has stated that fears surrounding AD/ADAS adoption are largely based on lack of knowledge about the technology, not specific AD/ADAS failures. The 2020 PAVE Poll in the USA revealed that most Americans still feel that ADAS are not very trusted:

Close to 3 out of 5 believe safe AVs will be available in 10 years, but 1 out of 5 believes they will never be safe.

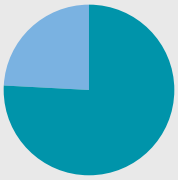
Only a third of Americans think "the advantages of AVs outweigh any potential disadvantages."

Almost half claimed, "would never get in a taxi or ride-share vehicle that was being driven autonomously."

The European Commission's Eurobarometer 496 report, "Expectation and concerns of connected and automated driving", measures public awareness and attitudes towards connected and automated driving, and reveals that [3]:



27% think that automated vehicles will reduce accidents.



76% would not feel comfortable in a fully automated vehicle without any human supervision.

67% would feel comfortable if they could take back control of the vehicle at any point in time.

Other global research reveals that the ADAS technology market will continue to grow:

Global Market Insights predicts that ADAS technology market valuation will exceed $60 billion by 2026 [4].

Research from Canalys shows that a third of new cars in major markets now have ADAS features. It predicts that in 2025 30% of cars will have ADAS features, increasing to 50% in 2030 [5].

A study from Roland Berger expects 86% of the world's vehicles will have ADAS features by 2025, 40% with L1 ("Driver assistance") features, 36% with L2 ("Partial automation") features, and 10% with L3 ("conditional automation) or higher features [6].

It is obvious that education about AD and ADAS, as well as related safety functions, is the path to more market acceptance. Functional safety testing provides valuable information that can increase customer trust and speed up market access.

Applicable functional safety standards

Functional safety standards for AD/ADAS vehicles are typically guided by those set out by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). However, there are also further standards and best practices on functional safety related to AD/ADAS vehicles.

OVERARCHING STANDARD

IEC 61508 "allows for the development of a uniform technical policy that can be applied for all safety systems that are electrically-based," but these standards are not designed to conflict with industry-specific standards.

PASSENGER VEHICLES, MOTORCYCLES, AND BUSES

ISO 26262 "is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production road vehicles ... it addresses possible hazards caused by malfunctioning behaviour of safety-related E/E systems ... [and] describes a framework for functional safety to assist the development of safety-related E/E systems."

AGRICULTURAL

ISO 25119 "sets out general principles for the design and development of safety-related parts of control systems (SRP/CS) on tractors used in agriculture and forestry and on self-propelled ride-on machines and mounted, semi-mounted and trailed machines used in agriculture. It can also be applied to mobile municipal equipment (e.g. street-sweeping machines) ... it covers the possible hazards caused by malfunctioning behaviour of E/E/PES safety-related systems, including the interaction of these systems."

INDUSTRIAL MACHINERY

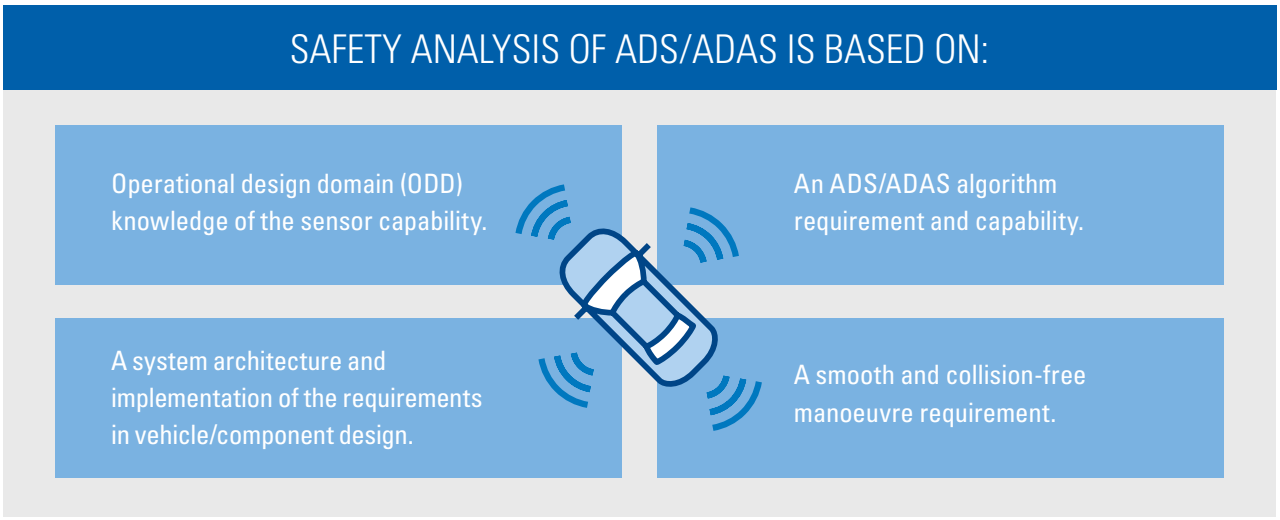
IEC 62061 specifies "requirements and makes recommendations for the design, integration and validation of safety-related control systems (SCS) for machines ... it is concerned only with functional safety requirements intended to reduce the risk of hazardous situations."

ISO 13849 "provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems (SRP/CS), including the design of software... [and] specifies characteristics that include the performance level required for carrying out safety functions."

Complexity of AD/ADAS functional safety

AD/ADAS functional safety is by nature several magnitudes more complex than for regular vehicles.

It's necessary to achieve "fail-operational" properties, meaning that if a component were to fail, there are safeguards in place to allow for safe continuation and eventual termination of the vehicle's path without causing a hazard. There are also complex degradation concepts, requiring time-related testing to achieve assurance that a specific component has a reasonable and predictable life span.



Dependent failure analysis has the goal of identifying failures that may hamper the required independence or freedom from interference between elements (hardware, software, and/or firmware). This process includes two steps:

1. Validate Freedom from Interference (FFI) between elements. This requires ensuring that elements are effectively siloed, preventing failure in one channel from migrating and causing failure in another (thus protecting fail-operational functionality).

2. Validate Independence between elements. This requires examining instances which require multiple functions to be present on one computer, which could potentially interfere with one another (another potential risk to fail-operational functionality).

Dependent failures can arise from systematic failures and random hardware failures, and may be classed as either common cause (a single failure), or cascading (two or more failures from a single root cause). The goal is to provide for isolation and freedom from interference across all elements, so in case of any single failure, fail-operational functionality can be preserved.

Example of a functional safety issue

An AD or ADAS vehicle equipped with cameras and sensors to prevent collision could be rendered unsafe by something as simple as a frozen camera image. Failure on a functional safety level could occur at this single point, but the root cause could be one of several specific points of failure.

Functional safety testing must consider not only all scenarios where safe operation could be compromised, but also all possible points of failure.

POSSIBLE CAUSES OF FUNCTIONAL SAFETY ISSUES

A hardware fault (such as a burned-out pixel impairing the reading of the camera image)	A software fault (preventing data from being sent from the camera to the braking system)	A design fault (improper mounting or angling for the camera to cover a full range of view)

Components for AD/ADAS functional safety

To achieve functional safety for AD/ADAS vehicles, the current process requires three comprehensive steps:

1

First, there must be a complete assessment and/or certification of hardware and software components to be utilised in the AD/ADAS vehicle. These must be found to meet appropriate standards.

2

Second, these pre-assessed and/or pre-certified components must be integrated into a vehicle platform. Currently, there are no AD or ADAS vehicles being manufactured completely independently; all plans hinge on connecting the components to existing vehicle designs.

3

Finally, a complete assessment of the vehicle scope must be conducted, to verify that functional safety standards are being fulfilled. This can be a multi-step process, involving testing and re-testing of individual component performance across hardware and software modules.

Beyond funtional safety

The outlook of ADAS is already bright. As previously mentioned, most new passenger on-road vehicles are coming off the line with some form of assisted driving module. The future of AD is still in flux, but turns on the concept of holistic safety.

Functional safety, specific AD/ADAS functions, and AI interact within the concept of driverless vehicles. Beyond basic functional safety lies the safety of the intended function (SOTIF). This is the next phase of analysis.

To achieve holistic safety in this setting, there is a need for additional analyses that address human-machine interaction as well as the operational aspects and systemic issues that may be affected by the level of situational awareness involved.

TÜV SÜD expertise

TÜV SÜD has decades of experience of assessing vehicle systems for functional safety, cybersecurity, and physical and virtual testing. We have been involved in testing the safety and security of AD and ADAS, as well as complete automated and connected vehicles, for several years and we act as your competent partner for bringing new mobility tehnology safely to the road.

As a member of various committees, we are involved in the development of relevant safety and certification standards, and our experts have in-depth knowledge of relevant standards and regulations and how to apply them.

We offer you a wide range of specialised services designed to facilitate the rapid implementation of AD/ADAS functionality in compliance with relevant regulations.

GLOSSARY OF ACRONYMS

ADAS – Advanced driver assistance systems
AI – Artificial intelligence
AD – Autonomous driving
FFI – Freedom from Interference
IEC – International Electrotechnical Commission
ISO – International Organization for Standardization
LiDAR – Light detection and ranging
SCS – Safety-related control systems
SRP/CS – Safety-related parts of control systems
SOFIT – Safety of the intended function

FOOTNOTES

[1] Global ADAS Market (2020 to 2030) - Emergence of Autonomous (globenewswire.com). Available at https://www.globenewswire.com/news-release/2020/07/09/2059977/0/en/Global-ADAS-Market-2020-to-2030-Emergence-of-Autonomous-Vehicles-Presents-Opportunities.html

[2] "Pave Poll: Americans Wary of AVs but Say Education and Experience with Technology Can Build Trust," survey results posted to the website of Partners for Autonomous Vehicle Education, 2021. Available at https://pavecampaign.org/pave-poll-americans-wary-ofavs-but-say-education-and-experience-with-technology-can-build-trust/ (as of October 1, 2021).

[3] Eurobarometer 496: Expectations and Concerns from a Connected and Automated Mobility. Available at https://data.europa.eu/data/datasets/s2231_92_1_496_eng?locale=en

[4] Global Market Insights, Industry Trends - Advanced Driver Assistance System Market. Available at https://www.gminsights.com/industry-analysis/adas-market

[5] Canalys news release, September 2021. Available at https://www.canalys.com/newsroom/huge-opportunity-as-only-10-of-the-1-billion-cars-in-use-have-adas-features.

[6] Roland Berger, ADAS: A Ubiquitous Technology for the Future of Vehicles, March 2021. Available at: https://www.rolandberger.com/en/Insights/Publications/Advanced-Driver-Assistance-Systems-A-ubiquitous-technology-for-the-future-of.html

Find out more about our functional safety services and training for the automotive industry

www.tuvsud.com/iso-26262-functional-safety
www.tuvsud.com/iso-26262-automotive-training
www.tuvsud.com/autonomous-driving

For more information contact us at automotive@tuvsud.com

Add value. Inspire trust.
TÜV SÜD is a trusted partner of choice for safety, security and sustainability solutions. It specialises in testing, certification, auditing and advisory services. Since 1866, the company has remained committed to its purpose of enabling progress by protecting people, the environment and assets from technology-related risks. Through more than 25,000 employees across over 1,000 locations, it adds value to customers and partners by enabling market access and managing risks. By anticipating technological developments and facilitating change, TÜV SÜD inspires trust in a physical and digital world to create a safer and more sustainable future.

TÜV SÜD AG
Westendstr. 199
80686 Munich, Germany
+49 89 5791 0
www.tuvsud.com