Safety as Standard – how standards are supporting innovation in the automotive sector

As new regulations for automated driving on UK roads is announced, BSI asks **Edith Holland,** Functional Safety Chief Engineer at HORIBA MIRA to explain the key role that standards will play in maintaining and achieving vehicle safety in the future.

bsi.

...making excellence a habit.™

With the move to automated driving quickly accelerating, the industry is facing a changing landscape when it comes to automotive safety - particularly against the backdrop of standards such as BS ISO 26262 Functional Safety, PD ISO/PAS 21448 Safety of the Intended Functionality (SOTIF) and PAS 1880.

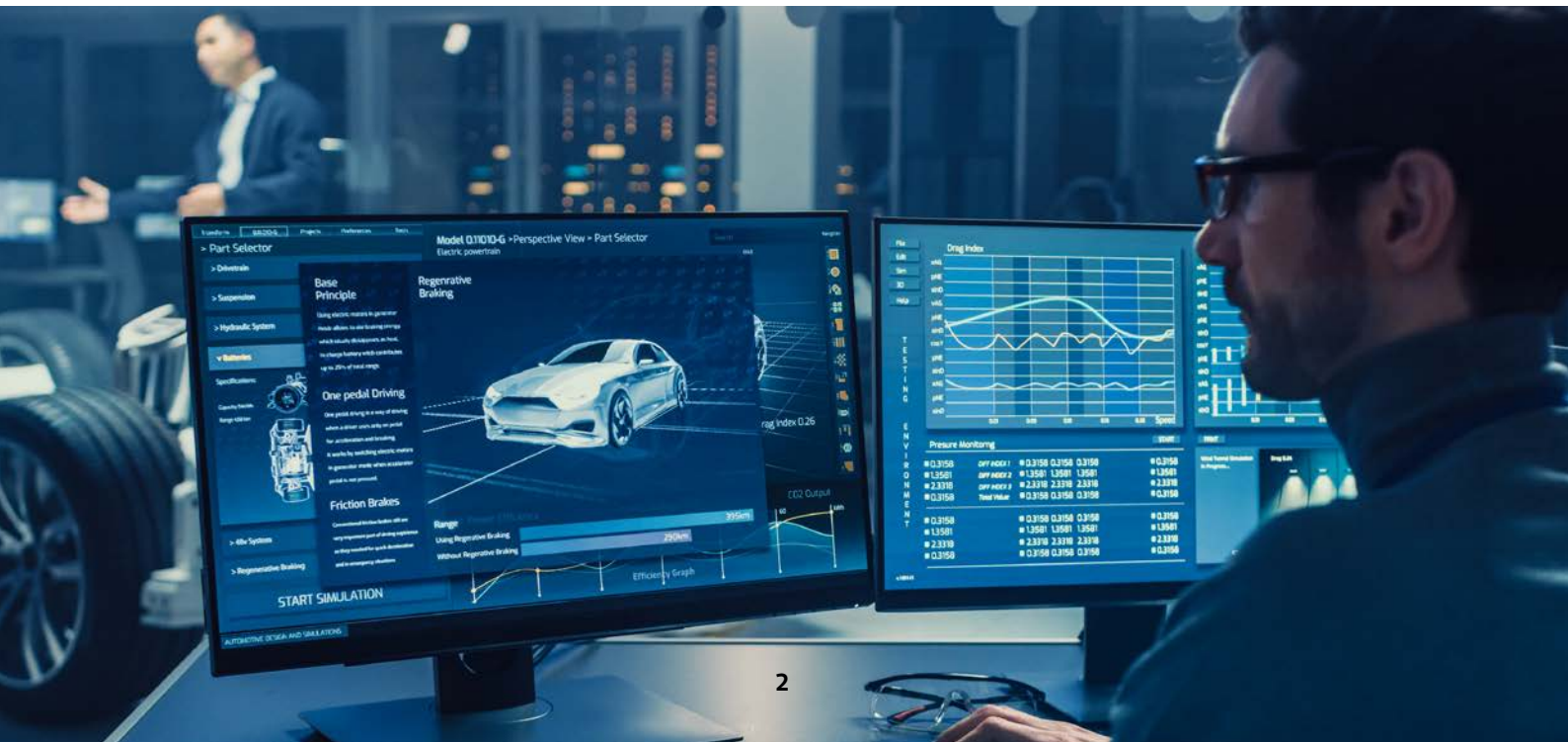
Automotive engineering, test and development consultancy HORIBA MIRA, has been involved in the development of each standard and has over 100 years combined Functional Safety experience within the team.

Here Edith explains how engineers, technologists and safety leads working in the industry can use standards such as ISO 21448, SOTIF and PAS 1880 as part of their toolkit when designing and testing new safety features, plus guidance on how to stay abreast of the changing standards.

History of Vehicle Safety considerations

Safety is a key consideration when making a new car purchase, but this choice is usually focused on advertised safety features, such as ratings that indicate how well a vehicle will perform in a crash. From originally measuring impact strength, these ratings have expanded to not just include active safety features like the number of airbags and Brake pre-charging systems, but also systems assisting the driver in avoiding an accident, like Lane-Keeping Assist systems or Emergency Braking Assists.

Unlike other transport systems, which have regulatory oversight who set targets and criteria for safety and assess and monitor the performance of manufacturers and operators, this is not the case for road vehicles. Currently, passenger cars are sold to the public by vehicle manufacturers through dealer networks, and it is up to the vehicle manufacturer to achieve an acceptable level of safety for their products. Vehicle manufacturers have, of course, been required to achieve type approval prior to being able to sell a particular vehicle for some time. This process ensures that motor vehicles meet relevant environmental, safety and security standards. Type Approval is granted when vehicle components and systems meet the requirements of the type approval regulations. These regulations define certain performance characteristics, (e.g. lighting functionality or braking performance) that are considered necessary for a safe vehicle. Type Approval is obtained by the manufacturer at the end of vehicle development and once achieved, the vehicle can be produced and sold to the public with the type approval process ensuring that the manufacturing process can maintain the validated criteria.

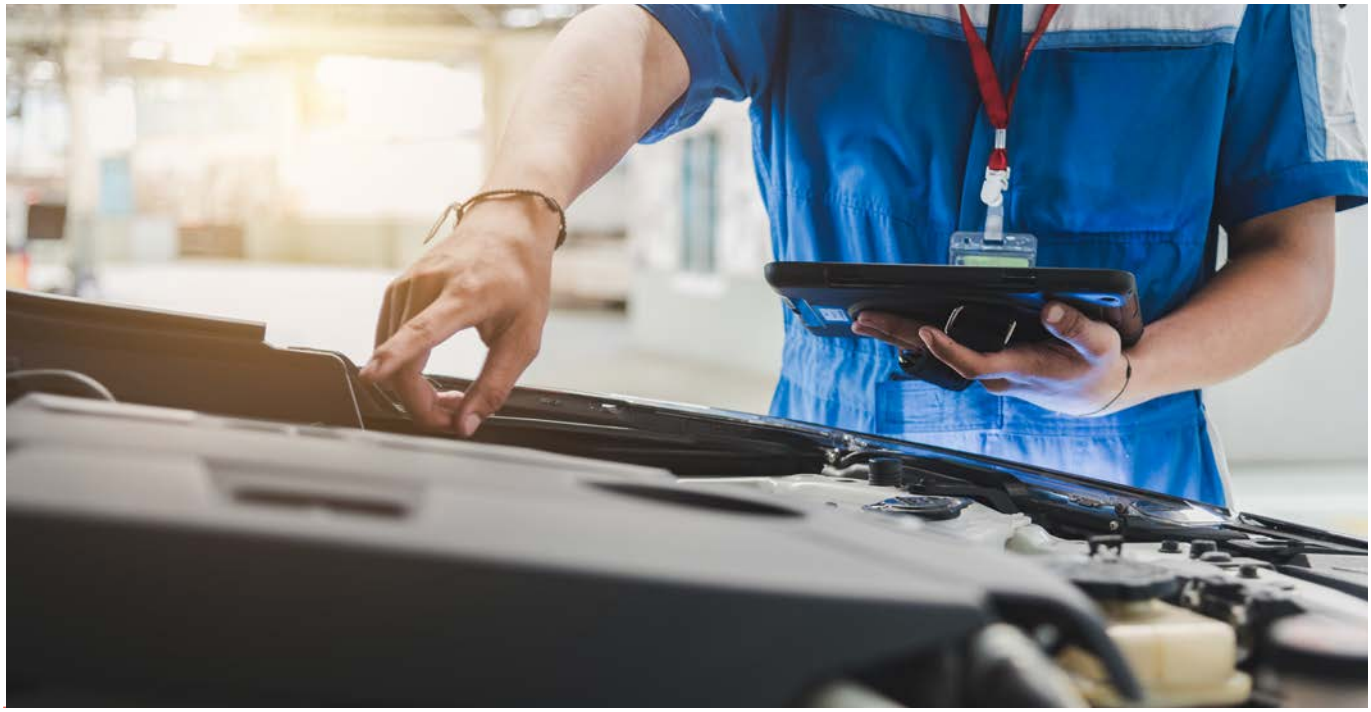


Introduction to Functional Safety

However, product safety for a vehicle goes further than requirements for specific performance criteria, or properties of individual components or systems. This was sufficient for mechanical component or simpler electro-mechanical systems, but the trend to more differentiating content, stricter emissions regulation and the general advancement of mobile technology - which has also found a way into the vehicle - has increased the software content within vehicles rapidly. Based on the need for additional measures to supplement the traditional techniques that ensured safety through reliability and robustness, the discipline of Functional Safety - which is concerned with that part of the overall safety of a system that depends on it operating correctly in response to its inputs - has been adapted to the application of automotive programmable electric, and electronic (EE) systems, and addresses hazards that could be caused by their malfunctions. The guidance from the generic Functional Safety standard IEC 61508 has formed the basis for the ISO 26262 series of standards, which, since its initial release in 2011 is considered best practise for automotive Functional Safety. It provides guidance for establishing a Functional Safety management system, with processes to supplement all development lifecycles of an automotive EE system with Functional Safety activities. From the beginning it has been set up around the organisation of the automotive supply chain and, following additional work and expansion, now facilitates the achievement of Functional Safety for most vehicle types and at all levels of design detail, hence covering activities at vehicle OEMs (original equipment manufacturer), system and component suppliers and even semiconductor manufacturers. In 2018 the guidance, previously aimed at passenger cars, was extended to cover trucks and buses, and guidance for motorcycles and semiconductors - which had previously been published as PAS (publicly available specification) in the phase between the 1st and 2nd edition of ISO 26262 - was incorporated into the 2nd edition of ISO 26262 series of standard. As a result, ISO 26262:2018 gives guidance on the achievement of Functional Safety for automotive EE systems for most production vehicle types at vehicle, system, software and hardware level, including guidance for semiconductor level.

How does ISO 26262 achieve Functional Safety?

ISO 26262 provides guidance on how to achieve Functional Safety of a vehicle system (referred to as an "item" in ISO 26262 terminology) through the implementation of a safety lifecycle that provides an approach to risk management during product development. It provides a particular risk model that has been adapted around a driver control model. Although not setting any quantitative targets for safety, there is an implied "accepted" level of risk that application of ISO 26262 gives. But it should be noted that this risk is concerned with malfunctioning behaviour only and does not cover risk due to the general use of the product - the vehicle - within the road transport environment. Instead the focus of ISO 26262 is how to address malfunctioning behaviour of automotive systems, caused by software or hardware faults.



New trends affecting safety

Vehicle technology continues to advance, and with the trend towards safer, cleaner mobility there is an increased focus on systems that facilitate some level of automated driving capability. This is seen as an enabler for more efficient mobility, through a reduction in accident rates, reduced congestion and improved traffic flow.

But automated driving systems constitute a particular challenge to safety engineers.

ISO 26262 focuses on reducing risk due to malfunctioning behaviour of EE systems. This assumes that the fault-free performance of the EE system is free from risk, and that risk only arises as a result of faults in the hardware and/or software. Guidance is given for addressing random hardware faults (like short circuits in motor driver circuits or an open resistor in a filter circuit) and systematic hardware and software faults, through achieving the requirements the standard sets out. But when advanced automated driving systems were first introduced a new phenomenon was discovered. It was noted that these EE systems could result in hazardous behaviour in the absence of malfunctions.

Safety of the Intended Functionality (SOTIF)

An example for such hazardous behaviour would be if an Automated Braking system, implemented using a radar sensor, performs an emergency braking intervention when traveling down a motorway slip road as a result of misinterpreting the radar reflection of a metallic traffic sign that is indicating a sharp corner as a collision risk despite the driver's full intention to follow the road curvature.

Consequently, additional guidance was needed on how an unreasonable level of risk of these types of systems can be avoided. This divergent aspect of safety to Functional Safety was termed "Safety of the Intended Functionality" and it is described in the publicly available specification ISO/PAS 21448 with a further update to the guidance to be issued as a full standard (ISO 21448) currently underway and nearing DIS stage. The intention of this standard is to ensure that unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality, or from reasonably foreseeable misuse by persons, is avoided. As can be seen, this is a much wider scope than is addressed by ISO 26262, but it is intended to be complimentary. ISO/PAS 21448 gives guidance on addressing causes of hazardous behaviour of functionality that depend on situational awareness through a series of activities that encompass design analysis and verification and validation activities.

The emphasis in ISO/PAS 21448 is on identifying issues with the specification of functionality that could lead to potentially hazardous behaviour, either because it has been incorrectly specified, specification content has been missed or because of limitations of the design to correctly implement the specified functionality. Functionality within scope covers both functionality that implements the driving functionality but also that related to interaction with and monitoring of the driver, as potential misuse of the Automated Driving (AD) system (through misunderstanding, laziness or through mistakes, not though maliciously) also needs to be addressed during development.

The intended functionality is analysed, and later tested, using the concepts of scenes and scenario to describe the driving environment, events within it, and actions by participants of it, in order to determine the required environmental awareness and driver interface. Hence the focus is on identifying the correct required behaviour of the AD functionality and translating this into a technical specification that captures the necessary and sufficient capability of the AD system to ensure that the risk of potentially hazardous behaviour is sufficiently low. It can be seen that, compared to safety considerations within ISO 26262, the safety objective is more closely related to performance aspects.

This reflects in the risk model behind SOTIF, which does not make use of the Automotive Safety Integrity Levels (ASILs) defined in ISO 26262 but requires that acceptance criteria, and from these validation targets, are defined as part of the process.

When assessing risk, the SOTIF standard evaluates the behaviour in the context of the scenario in which the potentially hazardous behaviour might be triggered and requires the setting of acceptance criteria for the risk

Continued >>

associated with each known hazardous scenario, for example a maximum number of incidents per operating hour. These acceptance criteria will in turn be converted into validation targets that need to be shown to be met during verification and validation activities.

It is through the validation targets that the identified functionality influences the specification and performance requirements of the system design, as performance limitations are another contributing factor to SOTIF hazards. As ISO/PAS 21448 does not contain explicit guidance on how to design Advanced Driving Systems (ADS) it might be useful to consider advice from other standards e.g. PAS 1880 when making design decisions. As part of the verification activities described in ISO/PAS 21448, the evaluation of the achievement of a suitable level of performance of the design during the verification and validation activities is another topic that is addressed in the standard.

Scenarios, as well as being the reference point for evaluating the risk with ADS behaviour during SOTIF analysis, are also the concept through which validation of ADS is being structured. The approach here is to use different levels of abstractions containing more and more detail to describe a scenario in sufficient detail to be able to conduct a meaningful test. There are a number of projects underway that investigate ways of structuring and labelling environmental information in order to reason and compare information consistently using either common or compatible formats.

In the UK BSI have published a specification containing a Taxonomy for Operational Design Domains (PAS 1883) and this work is being carried forward towards an international standard (ISO WD 34503). The overall goal of ISO/PAS 21448 is to reduce the risk of ADS functionality to an acceptable level through ensuring that safe behaviour is specified for all required scenarios. The number of scenarios can be influenced through the specification of an Operational Design Domain (ODD).

A common language for describing the ODD of an ADS is specified in PAS 1883. One might ask about the possibility of foreseeing each and every scenario for an ADS. Work is currently underway as part of the update to a full standard to expand on this and to acknowledges that there will be a level of residual risk due to unidentified scenarios that have not been considered during the development and hence require safety activities to extend into the operational phase. Additional risk management measures during this phase might also influence the required capability of the design (e.g. by requiring recording and storage of information regarding the current system status) and result in a suitable approach to how the functionality will be rolled out and made available to the public. Direction on this might be taken from PAS 1881 and PAS 1882.

Outlook

In addition to the creation of new standards, the reliance of vehicle safety on the correct operation of AD system has been recognised by type approval authorities.

The UNECE Global Forum for Road Traffic Safety (WP1), published a Resolution on the deployment of highly and fully automated vehicles in September 2018. This was followed by the approval of a regulation in June this year by the UNECE World Forum for Harmonization of Vehicle Regulations (WP29) for Advanced Lane Keeping Systems (ALKS). The intention of the regulation is to establish provisions concerning the type approval of a system that is capable of controlling lateral and longitudinal movement of a vehicle for extended periods without driver command. This regulation draws on activities that are described in automotive safety standards such as ISO 26262 and ISO/PAS 21448 and also extends to cybersecurity considerations. It requires that evidence in support of adequate safety (and security) considerations for the ALKS are submitted and assessed by the approving authority. This evidence could be created through following the requirements in the above-mentioned standards.

As can be seen, the focus on safety as a key attribute of modern vehicles in the future will remain and is continuing to evolve as new technologies are developed. Evolving safety concerns, either as a result of technologies used (e.g. Deep Learning algorithms) or through increasing connectivity with the surrounding environment or infrastructure will require continuous updates to existing standards and the creation of additional guidance on best practice and design considerations for developers and organisations involved in the development or operation of such vehicles.

Vehicles are designed with increasingly sophisticated safety features and driver assistance technologies using sensors, cameras onboard software and hardware. As well as meeting vehicle (type-approval) regulations, OEMs are keen their vehicles are voted 'best in class' – see NCAP ratings – on both passive and active safety performance.

The automotive industry is also seeing a rise in automated driving technologies that can offer opportunities for improved safety, optimising efficiency and new business models. However safe deployment of automated vehicle technologies, given its reliance on onboard software/ hardware and perception systems, has many challenges to ensure it is deployed safely and successfully.

BSI provides the standards to help automotive manufacturers, and their supplier (Tier 1 and Tier 2) to:

- **Design vehicles and components** to meet with vehicle safety requirements and UN harmonized vehicle regulation – protect drivers and passengers (ISO 26262/21448)
- **Test that active safety features**, and Advanced Driver-Assistance Systems (ADAS) meet with intended functional requirements
- **Get product innovation to market** more rapidly and efficiently by reducing risk, improving quality and performance outcomes – increasing competition
- **Support engineering process** to embed quality and reliability
- **Keep up with pace of change** in terms of innovative new technologies. Help manage safe deployment and testing of automated driving systems or vehicles, such as Automated Lane Keeping Systems (PAS 1880-1881-1882-1883)

Functional Safety/Active Safety	
BS ISO 26262-1:2018 (12 part)	Road Vehicles. Functional Safety requirements.
BS ISO/PAS 21448:2019	Road Vehicles. Safety of The Intended Functionality (SoTIF).
BS ISO 19206-1: 2018	Road vehicles. Test devices for target vehicles, vulnerable road users and other objects, for assessment of active safety functions. Requirements for passenger vehicle rear-end targets.
BS ISO 19206-2:2018	Road vehicles. Test devices for target vehicles, vulnerable road users and other objects, for assessment of active safety functions. Requirements for pedestrian targets.

Advanced Driver Assistance Systems (ADAS) performance + ADAS testing	
BS ISO 11270: 2014	Intelligent transport systems. Lane Keeping Assistance Systems (LKAS). Performance requirements and test procedures.
BS ISO 16787: 2017	Intelligent transport systems. Assisted Parking Systems (APS) Performance requirements and test procedures.
BS ISO 15622: 2018	Intelligent transport systems. Adaptive cruise control systems. Performance requirements and test procedures.
BS ISO 21717: 2018	Intelligent transport systems. Partially Automated In-Lane Driving Systems (PADS). Performance requirements and test procedures.
BS ISO 17361: 2017	Intelligent transport systems. Lane departure warning systems. Performance requirements and test procedures.
BS ISO 19638: 2018	Road boundary departure prevention systems. Performance requirements and test procedures.
BS ISO 20900: 2019	Intelligent transport systems. Partially Automated Parking Systems (PAPS). Performance requirements and test procedures.
BS ISO 20035: 2019	Intelligent transport systems. Cooperative Adaptive Cruise Control systems (CACC). Performance requirements and test procedures.

Automated Driving Systems	
PAS 1880:2020	Guidelines for Developing and Assessing Control System for Automated Vehicles.
PAS 1881:2020	Assuring the Safety of Automated Vehicle Trials and Testing. Specification.
PAS 1883:2020	Operational Design Domain (ODD) taxonomy for an Automated Driving System (ADS). Specification.
PAS 1882:2021	Data collection and management during automated vehicle trialling.
PD ISO/TR 21959-1:2020	Road vehicles. Human performance and state in the context of automated driving. Common underlying concepts.
PD ISO/TR 21959-2:2020	Road vehicles. Human performance and state in the context of automated driving. Considerations in designing experiments to investigate transition processes.
PD CEN/TS 17395:2019	Intelligent transport systems. eSafety. eCall for automated and autonomous vehicles.

How can I access standards?

British Standards Online (BSOL) – a standards management system

BSOL is a simple online tool that gives you access to standards you need, to ensure you stay at the forefront of the automotive innovation, security and operational excellence.

You can view and download standards with multiple user access, across all your sites, facilitating the easy distribution of knowledge throughout your business.

BSOL contains British standards and international and European standards that have been adopted as British standards. It also includes ISO, EN, PAS, ASTM and IEC standards that haven't been adopted as British standards.

You can subscribe to our pre-built modules or build a personalized standards collection, tailored to your organizational needs. Reduce risk within your organization and instil trust with your clients — get in touch to learn more about BSOL.

Get a quote or find out more at:
bsigroup.com/bsol
or call: **+44 (0)208 996 6353**

bsi.