

Advancing safety in transport through automation

How a cross-modal approach
will ensure a positive impact

theiet.org/transport



Advancing safety in transport through automation is published by the Institution of Engineering and Technology.

This report represents the views of the Transport Policy and Sector Panels, and has been written on behalf of the IET. The report intends to identify the relevant issues and provide an informed starting point for a debate around the topic and not a definitive solution.

The IET Transport Panel would welcome any comments you may have on the contents of this guide, and your ideas for future publications. Please get in touch by emailing sep@theiet.org.



The Institution of Engineering and Technology (IET) is working to engineer a better world. We inspire, inform and influence the global engineering community, supporting technology innovation to meet the needs of society. The Institution of Engineering and Technology is registered as a Charity in England and Wales (no. 211014) and Scotland (no. SC038698).

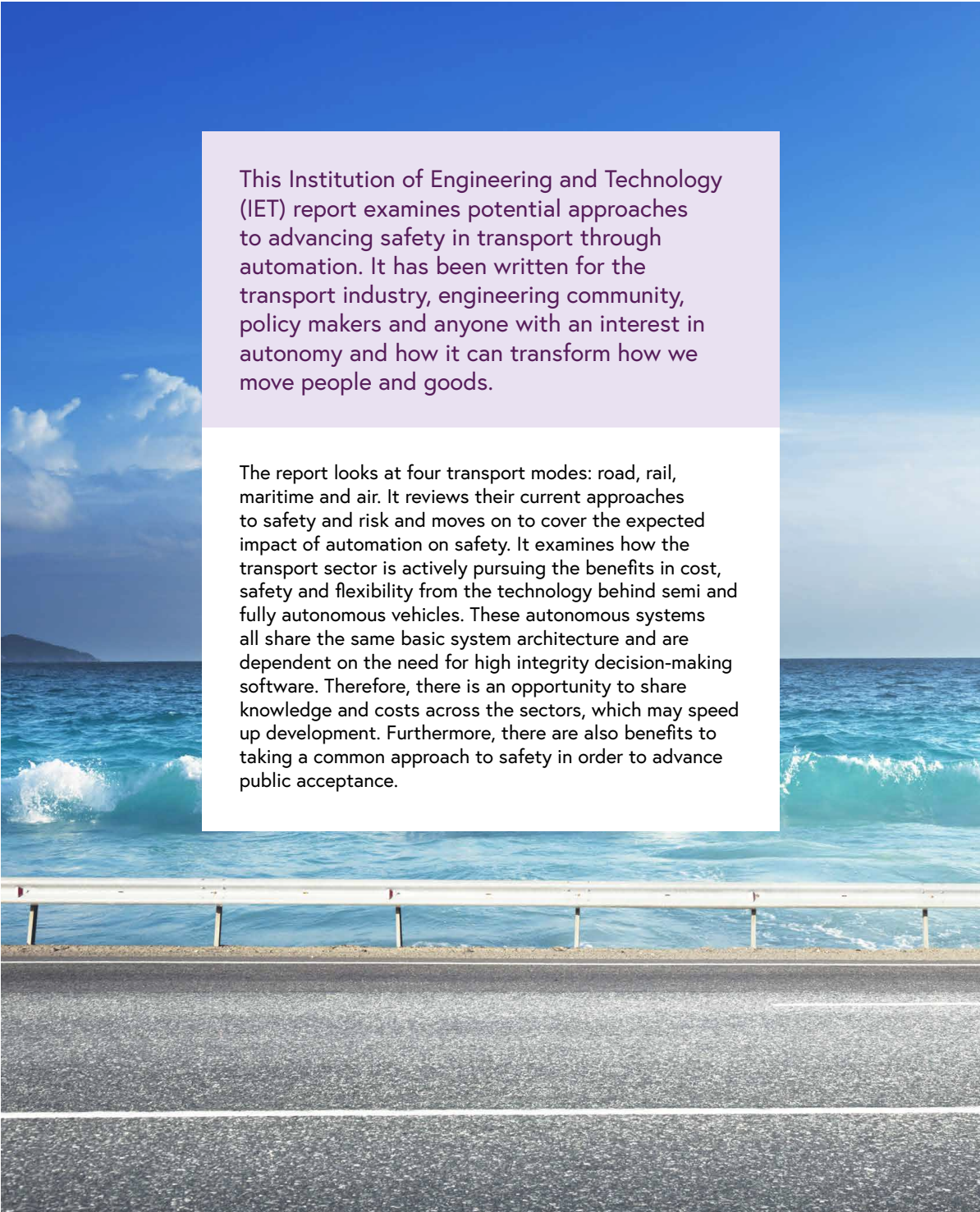
© The Institution of Engineering and Technology 2021.



Contents

1. About this report	04
2. Recommendations	05
3. Approaches to measuring hazards, safety and risk	06
3.1 Definitions	06
3.2 Measurements of risk	07
3.3 Risk analysis and reduction	08
3.4 Current system operation, supervision and incident recording	09
4. Public perception towards automation in transport	10
5. Individual sector approaches to safety	12
5.1 Road	12
5.2 Rail	15
5.3 Maritime	18
5.4 Air	21
6. Expected impacts of automation on safety	23
6.1 Road	23
6.2 Rail	24
6.3 Maritime	25
6.4 Air	26
7. Conclusions	28
8. Acknowledgements	30
9. About the IET	31

1. About this report



This Institution of Engineering and Technology (IET) report examines potential approaches to advancing safety in transport through automation. It has been written for the transport industry, engineering community, policy makers and anyone with an interest in autonomy and how it can transform how we move people and goods.

The report looks at four transport modes: road, rail, maritime and air. It reviews their current approaches to safety and risk and moves on to cover the expected impact of automation on safety. It examines how the transport sector is actively pursuing the benefits in cost, safety and flexibility from the technology behind semi and fully autonomous vehicles. These autonomous systems all share the same basic system architecture and are dependent on the need for high integrity decision-making software. Therefore, there is an opportunity to share knowledge and costs across the sectors, which may speed up development. Furthermore, there are also benefits to taking a common approach to safety in order to advance public acceptance.

2. Recommendations

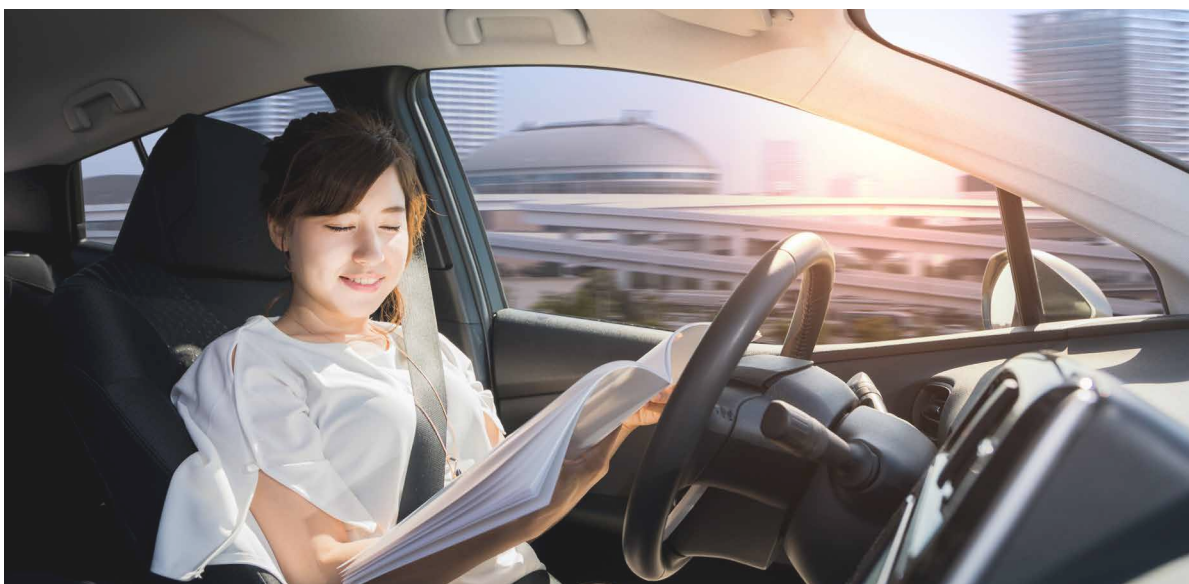
The development of autonomous transport systems brings new challenges. This includes assuring safety in the design and operation of the systems, but it also provides an opportunity to improve safety across all four sectors: road, rail, maritime and air.

Vehicle/vessel safety is only a part of overall safety when it comes to automated vehicles. The focus needs to be on system safety and we need to take full advantage of cross-modal learning and standardisation of approaches. By promoting a common approach to safety analysis and standards, the transport industry will be able to share scarce specialist resources.

1. Department for Transport (DfT) annual UK transport statistics should include a suitable cross-modal comparison of risk and safety. This needs to be properly researched and could involve multi-year average death rates and other data in comparable and relevant units.
2. Invest in approaches to validate/verify data sets for artificial intelligence-based (AI) systems (training and operational) and qualification of AI safety-critical applications. This should include a national infrastructure that enables the collection, dissemination and use of data sets drawn from all sectors, as well as establishing international collaboration. This data could be used for research and to inform standards development.
3. Rail, air and maritime all have investigation branches which have contributed massively to safety improvements over the years. Road has no such function and this has to change as automotive moves towards autonomy, or many lessons will be lost. DfT should establish a road accident investigation branch to bring together expertise in vehicle crashes.
4. Establish a cross-modal working group to develop a new standard for the functional safety of programmable safety-related systems. Recognise that management and maintenance of these complex safety-critical systems will be at least as challenging as their initial design and establish requirements and infrastructure to ensure safety is maintained throughout a system's life.
5. Cyber security is becoming increasingly important in most modes of transportation, particularly as automation and connectivity grows. Therefore, relevant standards should be reviewed for their suitability and adequacy.
6. Invest in further research on the public perception of autonomous systems. This will build trust through the design and development of inclusive solutions that increase adoption, and address concerns around negative impacts of autonomous systems.



3. Approaches to measuring hazards, safety and risk



Each mode of transport takes its own approach to measuring and mitigating risk. In this section, we explore the variety of tools and standards they use.

3.1 Definitions

- A hazard is any source of potential damage, harm or adverse health effects on something or someone.
- A risk is the chance or probability that a person will be harmed or experience an adverse health effect if exposed to a hazard.
- Safety is the state of being safe; the condition of being protected from harm or other non-desirable outcomes.

CENELEC (European Committee for Electrotechnical Standardisation) standards define safety as the freedom from unacceptable levels of risk. The question "how safe is safe enough?" can be replaced by the question "what levels of risk are acceptable?". Risk depends on the frequency and severity of undesirable outcomes.

3.2 Measurements of risk

In the functional safety standards based on *IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, a framework is proposed based on six categories of likelihood of occurrence and four of consequence.

Engineering standard *ISO 26262, Road vehicles – Functional safety*, is an adaptation of *IEC 61508* for Automotive Electric/Electronic Systems and *IEC 62279* and its equivalent European Norm *EN50128* provides a specific interpretation of *IEC 61508* for railway applications. It is intended to cover the development of software for railway control and protection including communications, signalling and processing systems.

Categories of likelihood of occurrence

Category	Definition	Range (failures per year)
Frequent	Many times in system lifetime	$> 10^{-3}$
Probable	Several times in system lifetime	10^{-3} to 10^{-4}
Occasional	Once in system lifetime	10^{-4} to 10^{-5}
Remote	Unlikely in system lifetime	10^{-5} to 10^{-6}
Improbable	Very unlikely to occur	10^{-6} to 10^{-7}
Incredible	Cannot believe that it could occur	$< 10^{-7}$

Consequences categories

Category	Definition
Catastrophic	Multiple loss of life
Critical	Loss of a single life
Marginal	Major injuries to one or more persons
Negligible	Minor injuries at worst

Safety integrity level (SIL)

Safety integrity levels (SILs) can be used to specify a target level of risk reduction.

In the functional safety standards based on *IEC 61508* four SILs are defined, with SIL 4 the most dependable and SIL 1 the least. The definitions and values for a given SIL are not consistent between applications.



Micromort

A micromort is a unit of risk defined as one-in-a-million chance of death. Micromorts can be used to measure the risk of various day-to-day activities.

Travel distance that increases the death risk by roughly one micromort:

- Six miles by motorbike
- Ten miles by bicycle
- 17 miles by walking
- 230 miles by car
- 1,000 miles by jet
- 6,000 miles by train

Some examples¹

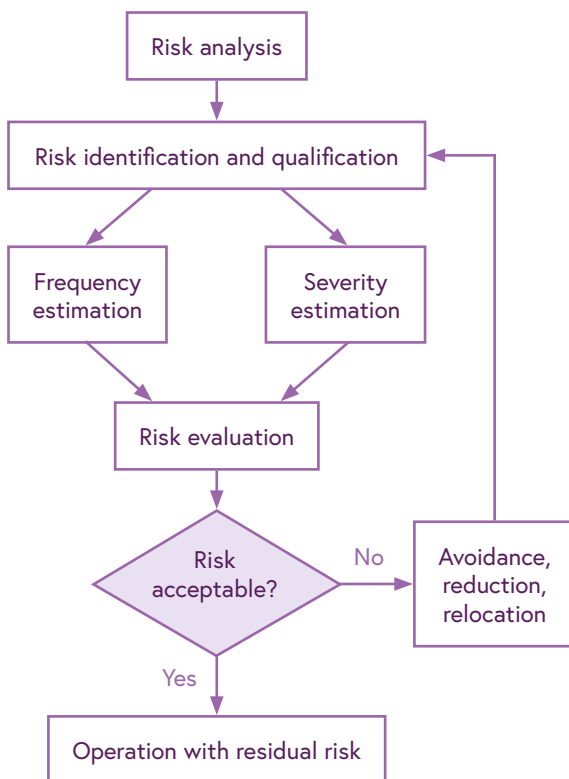
Death from	Micromorts per unit of exposure
All non-natural causes (England and Wales)	0.8/day
Skydiving	8/jump
Giving birth	120



3.3 Risk analysis and reduction

General approach

Having identified and quantified risks, efforts can focus on avoiding and reducing them. A general framework is shown below.



Mitigation of risks continues until their overall contribution to the hazard is considered tolerable. Some risks can be avoided, but ultimately some residual risk remains.

The ALARP, SFAIRP and ALARA approaches

- ALARP - as low as reasonably practicable
- SFAIRP - so far as is reasonably practicable
- ALARA - as low as reasonably achievable

These terms mean essentially the same thing and at their core is the concept of being "reasonably practicable." This involves weighing a risk against the inconvenience, time and money needed to control it.

The presumption is for action to be taken unless those responsible can show it would be grossly disproportionate to the benefits that would be achieved. This approach is widely used in industry and for workplaces.

GAMAB

GAMAB (globalement au moins aussi bon) is a form of risk analysis that focuses on the standard *EN 50126-1999; Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*. This states that all new guided transport systems must provide a level of risk at least as good as the one offered by any equivalent existing system. Several countries have gone as far as to write this concept into law. Any new technology must offer at least the same safety as that which it replaces.

The precautionary principle is also relevant here. This is a strategy for approaching issues of potential harm when lacking extensive scientific knowledge on the matter. It emphasises caution, pausing and review before leaping into new innovations that may prove disastrous.

Any new technology must offer at least the same safety as that which it replaces.

The value of life approach

The value of life approach sets an economic value to the benefit of avoiding a fatality. A statistical term, it quantifies the cost of reducing the average number of deaths by one.

Below are the current values used in the UK for transport appraisal, which comes from the *Department for Transport (DfT) transport analysis guidance (TAG) data book (2019)*:

Current values in the UK for transport appraisal

Severity	Cost £
Fatal	1,554,395
Serious	174,671
Slight	13,465

Minimum endogenous mortality (MEM)

The minimum endogenous mortality (MEM) method is based on there being different mortality rates in society, depending on age and sex. These deaths are partly caused by technical systems. MEM compares the risks due to a new system with existing risks caused by natural mortality. MEM demands that a new system does not significantly contribute to the existing mortality caused by technical systems.

According to *EN 50126*, the individual risk due to a particular technical system must not exceed 1/20th of the minimum endogenous mortality.

As an example, in Germany, MEM is defined based on natural mortality between the ages five and 15 and its value is 2×10^{-4} fatalities/per person per year. The principle is that the hazards due to a new transport system should not significantly increase that value. Therefore, a value of 1×10^{-5} death/per person per year might be considered acceptable using the MEM philosophy.

3.4 Current system operation, supervision and incident recording

System operation, supervision and incident recording for each of the transport sectors can be broadly summarised as follows:

Action	Rail	Road	Air	Maritime
Supervision	Driver/train manager	Driver	Pilot(s)	Captain and officers
Navigation	Remote signalling	Driver and automatic signalling	Pilot and air traffic control	Navigation officer/pilot/officer on watch
Collision avoidance	Signalling and timetable	Driver and signals	Pilot, air traffic control sensors, automatic dependent surveillance–broadcast (ADS–B) and traffic collision avoidance systems (TCAS)	Captain, sensors and automatic identification systems (AIS)
Vehicle health management	On-board sensors and displays	On-board sensors and displays	On-board sensors and displays	On-board sensors and displays
Major failure action	Stop	Stop	Land/ditch	Stop
Crash recording	On-board driving data recording system GM/RT2472	None in most vehicles. Airbags and eCall systems preserve some data	Flight data recorder EUROCAE ED-112 and cockpit voice recorder EUROCAE ED-56A	Voyage data recorder SOLAS chapter V REGULATION 18
Regulatory authority	Office of Rail and Road (ORR)	ORR	European Union Aviation Safety Agency (EASA)/ Civil Aviation Authority (CAA)	International Maritime Organisation (IMO)/ Maritime and Coastguard Agency (MCA)

4. Public perception towards automation in transport

The development of autonomous systems is poised, like other emerging technologies, to reshape almost all aspects of daily life. Against this backdrop is the challenge to build trust and public acceptance.

The interfaces between people and autonomy require much greater focus. Exploring public or user perception can lead you to take one of two perspectives: engineer trusted solutions through adherence with standards, regulations, etc. (the more traditional approach), or consider how to achieve public acceptance, adoption and systemic change, then design a solution that will be acceptable and trustworthy.

Both viewpoints have utility, though the former gets considerably more focus than the latter. This is creating challenges when the technology being developed is new, unfamiliar and somewhat abstract to many potential users (e.g. autonomous cars), and the desired outcome is societal-level change brought about by significant changes in user behaviour (e.g. wide-spread adoption of autonomous cars).

Predominately engineering-driven, developing trusted systems focus on creating autonomous solutions that are safe, reliable and secure. From this perspective public acceptance relates to perceived risk of use, ease of use and usefulness. The role of users is considered to ensure that the human-machine interface is optimal and the system can be relied on to perform as intended. Done well, these technologies enable systems to be efficient and largely error-free.

Significant attention to this, coupled with a rigorous safety approach focused on acting on accident investigation findings has significantly improved aviation safety. This is critical. Systems that perform as expected are more likely to be trusted and therefore used.

However, as the aviation sector is discovering, automation is a double-edged sword that creates systemic vulnerabilities. The aim of automation is often to minimise the role of the user, thereby reducing the likelihood of human error. In 1983, when cognitive psychologist Dr Lisanne Bainbridge published her



seminal paper *Ironies of Automation*², she noted that automation often compounds rather than eliminates problems for users. To paraphrase: if all the things that are technically possible or easy become automated, people are left with the hard things to manage.

This paradox essentially means that the more advanced the autonomous system, the more crucial the role of the user. This is because people are often left to take over when a system critically fails.

Tragically, in the cases of Air France 447 (AF447) in 2009, and the more recent Boeing 737 MAX crashes, this was not possible. In all transport sectors, recognising that automated and autonomous systems are still human-machine systems is central to developing autonomous machines that users can trust and therefore willing to accept. This is true across all transport sectors.

The second viewpoint, focusing on user/public adoption, is more subjective. It requires a shift from seeing autonomy as a technological challenge to one that draws on greater understanding of behavioural sciences, the factors that influence peoples' perception of autonomous systems and the impact of technology on society.

Public perception of an innovation or technology shapes acceptance and adoption. Like the earlier viewpoint, perceived benefit and perceived risk also contribute, but trust is an important factor. The challenge is that trust is dynamic, complex, highly dependent on context and innately personal based on a person's previous experiences, perception of risk and willingness to be vulnerable. How do engineers design trusted systems based on many individual perspectives?

Rachel Botsman's³, Trust Fellow at the University of Oxford, insights into the complex relationship between trust and technology are useful. Engineering approaches are based on removing uncertainty from a system, but she disagrees that trust is about certainty, putting forward that it is in fact the opposite. "If you're sure of the outcome, if there is no risk, no trust is actually required," she says⁴, suggesting that trust is "a confident relationship with the unknown."



Looking at trust through this lens shows us that it allows people to overcome uncertainty, to be vulnerable, to try something new or do something differently, such as be open to new innovations like autonomous cars. More akin to change management than technology design and development, this suggests that shaping public perception and acceptance of autonomous systems lies in our ability to make the unfamiliar familiar.

This requires recognition that the development of publicly acceptable autonomous systems goes well beyond demonstrating compliance with regulations. We need to recognise that just because we call things as 'compliant', it will not automatically translate into being trusted and acceptable to others. Greater insights into what makes autonomous technologies more trustworthy and acceptable would de-risk the engineering process and lead to solutions that are acceptable by design.



Success in public adoption is not simply about resolving technical challenges and de-risking the technology. It involves effectively engaging with people to demystify these technologies and make them directly relevant. A greater understanding of the public perception, as well as a better understanding of what influences our willingness to engage with and trust new technologies, is key to success. This will enable us to build trust through design, develop inclusive solutions that increase adoption, or address concerns around the negative impacts of autonomous systems on society.

If all the things that are technically possible or easy become automated, people are left with the hard things to manage.

² https://ckrybus.com/static/papers/Bainbridge_1983_Automatica.pdf

³ Trust Fellow, Saïd Business School, University of Oxford

⁴ <https://www.i-cio.com/big-thinkers/rachel-botsman/item/the-dynamic-nature-of-trust-in-the-digital-age>

5. Individual sector approaches to safety

Historically, each transport sector has taken a different approach to the measurement of safety and approach to safety and risk.



5.1 Road

Measurement of safety

Road safety is characterised in several ways, the most important is the number of fatalities in one year. In Great Britain there were 1,784 deaths in 2018⁵. Other regularly quoted measures include:

- Number of serious injuries - where 'serious' has a particular technical definition.
- Number killed and seriously injured (KSI).
- Fatality rate – fatalities per 1 billion travel-kilometres.

There are some subtle points around the definitions of these terms⁶. We could also think about near miss and robustness against technical failures as contributing to understanding of safety.

Major factors contributing to increased risk include:

- Excessive speed or speed inappropriate for the conditions.
- Alcohol (and drug) use by drivers.
- Lack of use of proper restraints and safety aids such as motorcycle helmets, seat belts, and child restraints.
- Tiredness.
- Distraction.

In terms of road safety, the UK performs relatively well compared to most countries⁷, but could further improve by learning lessons from other transport modes.

⁵ <https://www.gov.uk/government/statistics/reported-road-casualties-in-great-britain-annual-report-2018>

⁶ See, for example: https://en.wikipedia.org/wiki/Road_traffic_safety

⁷ https://ec.europa.eu/transport/road_safety/sites/roadsafety/files/pdf/scoreboard_2018_en.pdf

Overall safety and risk approach

Unlike other transport systems that have regulatory oversight, including targets and criteria for safety with ongoing monitoring, the road sector has no overall safety or risk approach. Vehicles, road infrastructure and users are governed by different organisations.

Many countries set road safety targets. The UK used to do this, but currently does not. The risk to an individual on a single journey is so small that it is largely ignored by the majority of road users.

Accidentology is applied to better understand road safety by analysing road crashes (the term accident is less commonly used today) and other events in which road users are killed or seriously injured. Accidentology identifies contributory and precipitating factors rather than causes, and analyses factors such as road and environmental properties, vehicle performance and road user behaviour. This analysis can include location, type of road, type of crash, speed, vehicle type as well as the number of people involved.



Safety of sub-systems

Vehicle safety

Vehicle types include cars, motorcycles, light goods vehicles, heavy goods vehicles and buses, and coaches.

There is a complex array of national and international regulations governing requirements and minimum safety performance of each vehicle type. International regulations known as type approvals are set by the United Nations Economic Commission for Europe (UNECE) and cover the performance of steering, brakes, lighting etc. There are also some national construction and use regulations.

New vehicle types and functionality, such as automation, raise difficult questions about the applicability of existing regulatory structures.

Vehicle production samples are tested according to specific procedures and, once approval is granted, it is the responsibility of manufacturers to uphold

standards. Product recalls are then initiated for specific identified safety issues, but it is voluntary for owners to participate in the process of checks and modifications.

After an initial period of three years it is mandatory for vehicles to be inspected and safety-approved annually. Here the testing focuses on mechanical safety components rather than, for example, software modifications or cyber security.

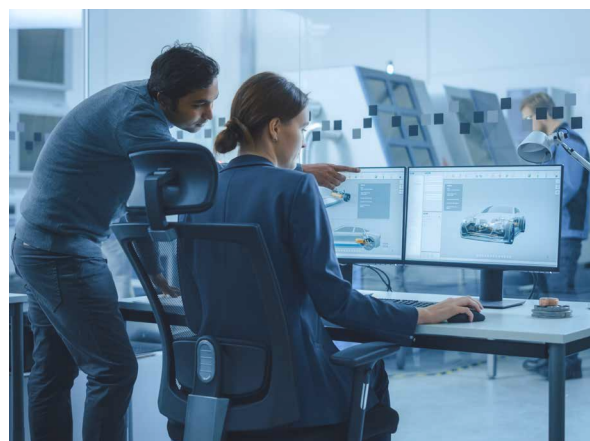
While these regulations and tests have worked reasonably well for simple electro-mechanical systems, manufacturers understand that increasing use of software and hardware in vehicles needs a more sophisticated approach to assuring safety.

Functional safety is currently a widely used approach. This is concerned with the part of the system's overall safety that depends on it operating correctly in response to its inputs. Guidance from the generic functional safety standard *IEC 61508* has formed the basis for the *ISO 26262* series of engineering standards, which have been adapted to include automotive electric, electronic and programmable systems.

ISO 26262's focus is how to address malfunctioning behaviour of automotive systems caused by software or hardware faults. The guidance covers implementation of a safety lifecycle that provides an approach to risk management during product development.

Although not setting any quantitative targets for safety, there is an implied accepted level of risk described by automotive safety integrity levels (ASILs). Importantly, this risk is only concerned with malfunctioning behaviour and does not cover risk due to the vehicle's general use.

With increasingly automated systems, it was realised that new risks may arise as a result of conditions such as sensor limitations or from reasonably foreseeable driver misuse. A new process has been developed to address this termed safety of the intended functionality (SOTIF). This is described in the specification *ISO/PAS 21448*, which in time is expected to become a full standard.



Here the intended functionality is analysed and tested using the concepts of scenes and scenario to describe the driving environment, events within it, and actions by participants of it. This determines the required environmental awareness and driver interface. The focus is on identifying the correct required behaviour of the automated vehicle and translating this into a technical specification so that the risk of potentially hazardous behaviour is sufficiently low. The risk model behind SOTIF does not make use of the ASILs defined in *ISO 26262*, but requires that acceptance criteria and validation targets are defined as part of the process.



Infrastructure safety

Infrastructure is the responsibility of local authorities (for local roads), and highway authorities. There are national and international standards and guidelines for many aspects of road design⁸, such as sight lines, junction layouts, drainage, and signage. However, there is also scope for interpretation.

Documents include the 15-volume *Design Manual for Roads and Bridges* (DMRB), which includes all current standards, advice notes and other documents relating to the design, assessment and operation of trunk roads including motorways. There are also eight dedicated chapters in the *Traffic Signs Manual* giving guidance on the use of traffic signs and road markings prescribed by the *Traffic Signs Regulations* in England, Wales, Scotland and Northern Ireland.

Motorways and city roads tend to be relatively uniform, whereas rural roads can be of very variable quality. Speed limits vary due to the purpose of the road and are generally set by taking account of local conditions and safety issues. On most roads traffic is mixed; a variety of vehicles can use them. However, there are specific restrictions, such as no heavy goods vehicles (HGVs) on narrow roads and no cycles on

motorways. The DfT, companies or private individuals can take action against bodies which fail to maintain infrastructure to the required standards.

User safety and training

Road users include drivers, cyclists and pedestrians. Regulation and enforcement of their behaviour is essentially a national rather than European or international activity and there are many legal requirements and guidelines regarding how road users should behave⁹. These have been put in place to promote the safety of all road users.

To drive a car or light goods vehicle (LGV), users must obtain a licence which now requires a theory and practical test. As most able-bodied adults can do this, the standard of driver safety, behaviour and performance is rather variable. No re-testing is required unless the driver is convicted of certain motoring offences. After the age of 70 medical declarations are required but, again, there is no formal re-testing. The standards for HGV and bus/coach driving are higher and there are certain medical and licence re-testing requirements.

Examples of more risky driving behaviours include speeding, tailgating, not using safety restraints and being distracted, such as using a mobile phone while driving.

Safety is addressed in part by enforcing traffic laws through fines and endorsing drivers' licences with penalty points if convicted of a motoring offence. Endorsements stay on a driver's record for four or 11 years depending on the offence. Drivers who build up 12 or more penalty points within a period of three years can be disqualified from driving. There are different rules for new drivers.



⁸ <https://standardsforhighways.co.uk/ha/standards/>

⁹ <https://www.gov.uk/browse/driving/highway-code-road-safety>



5.2 Rail

Measurement of safety

Rail safety performance is measured in several ways. The most important is fatalities and weighted injuries (FWI), as reported in the Rail Standards and Safety Board's (RSSB) annual *Health and Safety Report*¹⁰. FWI is a combination of fatalities with major and minor injuries weighted accordingly. Any implementation of new technology or changes in working practices, as might be predicted with the introduction of automation, would be expected to maintain or improve this overall performance measure.

In 2019/2020 the level of accidental risk on Great Britain's mainline railway represented as FWI was 132.2 a year for passengers, workforce and the public. Of this, 47% occurred to passengers on the mainline railway and to the public in stations, 20% to the workforce, and 33% to members of the public not in stations. A further 7.2 FWI/year occurred in yards, depots and sidings. Most of this risk affects the workforce, with nearly all of the remainder involving acts of public trespass. None of the public fatalities were due to train accidents up to the data cut-off for the period which was 31 March 2020.

The safety risk on Britain's railways has reduced steadily in recent years. Major factors contribute to this reduction including:

- Improvements in asset management.
- Level crossing safety.

- Minimisation of trains passing a signal at danger or the impact of passing a signal at danger (speed supervision).
- Derailment protection.

Passenger and workforce fatality rates in the UK were well below the EU average over the five-year period 2014-2018¹⁰.

The analyses leading to the railway safety performance figures are based on industry-reported safety events, with the primary source being the railway's safety management intelligence system (SMIS). Its use is mandatory for infrastructure managers and railway undertakings on the British mainline.

It is important to understand the distinction between modelled risk and recorded harm. The safety risk model (SRM) is the primary means of carrying out risk modelling for Great Britain's rail.

It is based on a mathematical representation of all the events (precursors) that could lead directly to an injury or fatality and provides a comprehensive snapshot of the underlying level of risk on the railway. Studies have been carried out using SRM considering the impact of communication-based train control on safety performance. The balance of eliminated, modified and new risk provided a predicted safety benefit of these types of train control. SRM would be a useful tool to explore the impact of automation on rail safety performance.

¹⁰ RSSB Annual Health and Safety Report 2019/2020: A summary of Health and Safety Performance Operational Learning and Risk Reduction activities on Britain's railway. <https://www.rssb.co.uk/en/safety-and-health/monitoring-safety/safety-performance-reports>



Overall safety and risk approach

There is a hierarchy of legislation which drives the approach to, and management of, safety on British railways. Primary legislation includes *The Railways (Interoperability) Regulations 2011* and *The Railways and other Guided Transport Systems (ROGS) (Safety) Regulations 2006*.

ROGS implements European Union (EU) safety requirements for railway operators and infrastructure managers. Now transposed into GB law since Brexit. It requires that those with responsibility for safety must maintain a safety management system and hold a safety certificate/authorisation issued by the Office of Rail and Road (ORR). ROGS also makes provision for the safe design of new vehicles and infrastructure, imposes controls on safety critical work and makes provisions for entities in charge of maintenance of railway vehicles.

Primary legislation is underpinned by several other regulations and supported by technical and process standards. This includes *BS-EN50126 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*, and industry guidance from the Rail Safety and Standards Board.

A key document which defines the process of managing safety risk is the common safety method for risk evaluation and assessment (CSM-RA). CSM-RA provides a framework that describes a common mandatory European risk management process for the rail industry. It applies when any technical, operational, or organisational change is being proposed to the railway system and would be the primary safety management process to be satisfied for any introduction of rail automation.

The purpose of the process is to ensure that all reasonably foreseeable hazards have been identified and that risks have been controlled to an acceptable level. Risks may be controlled by standards, comparison to reference systems, or explicit risk estimation (ERE). Where ERE is used, the risk must be reduced so far as is reasonably practicable.

There are several initiatives working towards improving safety on Great Britain's railways. Leading Health and Safety on Britain's Railway (LHSBR) is a strategy adopted by the industry to identify areas where specific initiatives may reduce harm. A new version of the LHSBR strategy was issued in March 2020. The System Safety Risk Group (SSRG) promotes industry collaboration on safety issues aligned to the risk areas in the strategy.

Mindful of the fact that learning does not just occur after an event, and that many valuable lessons are revealed by what might be termed accidents waiting to happen, issues can also be raised via the industry's confidential incident reporting and analysis service (CIRAS). This mainly focuses on near miss events or perceived deficiencies in safety systems and arrangements. A better understanding of these provides a solid foundation for shared learning across different industry sectors.

The Rail Accident Investigation Branch (RAIB) investigates incidents and accidents and makes recommendations. Its aim is to identify the root cause and prevent recurrence. It does not prosecute, but if the industry fails to take due cognisance of its recommendations it can take legal action.

A precursor indicator model (PIM) looks at trends in the likelihood of precursors. This is to measure the underlying risk from potentially high-risk train accidents (PHRTA) categories of train accidents by tracking changes in the occurrence of their precursors.

Precursors include objects on the line and signals passed at danger (SPAD). The precursors would be a good place to start looking at the potential impact of automated systems on rail risk.



In addition to physical safety, railways also consider health and wellbeing important and various initiatives are underway across the industry. One perception is that on-board train staff provide a feeling of wellbeing, even though their presence does not actually improve safety. This perception needs to be considered when implementing automatic systems in order to develop staff and passenger support.



Public behaviour has a big impact on railway safety. This includes actions at level crossings, adjacent to and over railway infrastructure and when using facilities and trains. The infrastructure manager and railway undertakings have a duty of care to consider the wellbeing of passengers and the public. Initiatives include publicity and awareness campaigns both nationally and locally in schools and communities. Public awareness of the impact of any changes to train operations would be beneficial.

Fatigue risk, especially in drivers, is being considered as a contributor to incidents such as buffer stop collision. It is key to monitor workforce fatigue and this can be done by keeping a close eye on working patterns and trends in precursors and near misses that involve tiredness.

Safety of train operation, workforce, passengers and public

Train operation safety

Until the Stonehaven accident, which occurred in Scotland in August 2020, there had not been any train accident fatalities in the preceding 13 years¹⁰. However, potentially high-risk train accidents (PHRTAs) continue to be a concern. These are circumstances where there was potential for a large number of fatalities or major injuries. The largest contributor to this risk is infrastructure failures including track failure.

Overall there has been a similar number of PHRTAs to last year, although level crossing collisions and derailments have fallen after seeing a rise in recent years. There were 25 PHRTAs in 2019/20. Much of the decrease in overall risk in recent years has come about from the railway's ability to learn from accidents and introduce more technology to mitigate risk. For example, the continuing fitment of the Automatic Warning System (AWS) (and later the Train Protection and Warning System (TPWS)) to cut SPAD risk, the withdrawal of less crashworthy Mark 1 rolling stock, and installation of in-cab communications systems.

Workforce safety

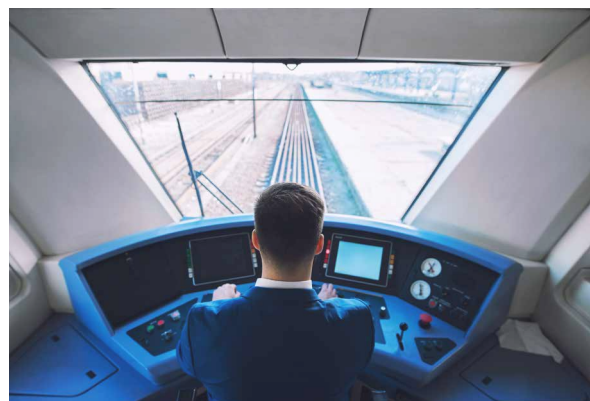
The number of accidents involving the workforce has lowered from quite high levels in the past century to very low levels in recent years. This is thanks to safety initiatives, good working practices and the promotion of a culture of safety.

In 2019/2020, three workforce fatalities were recorded, two on the running line, the other in a depot. The level of physical harm to members of the workforce was 24.1 fatalities and weighted physical injuries (FWPI) in 2019/20, a slight decrease on the previous year.

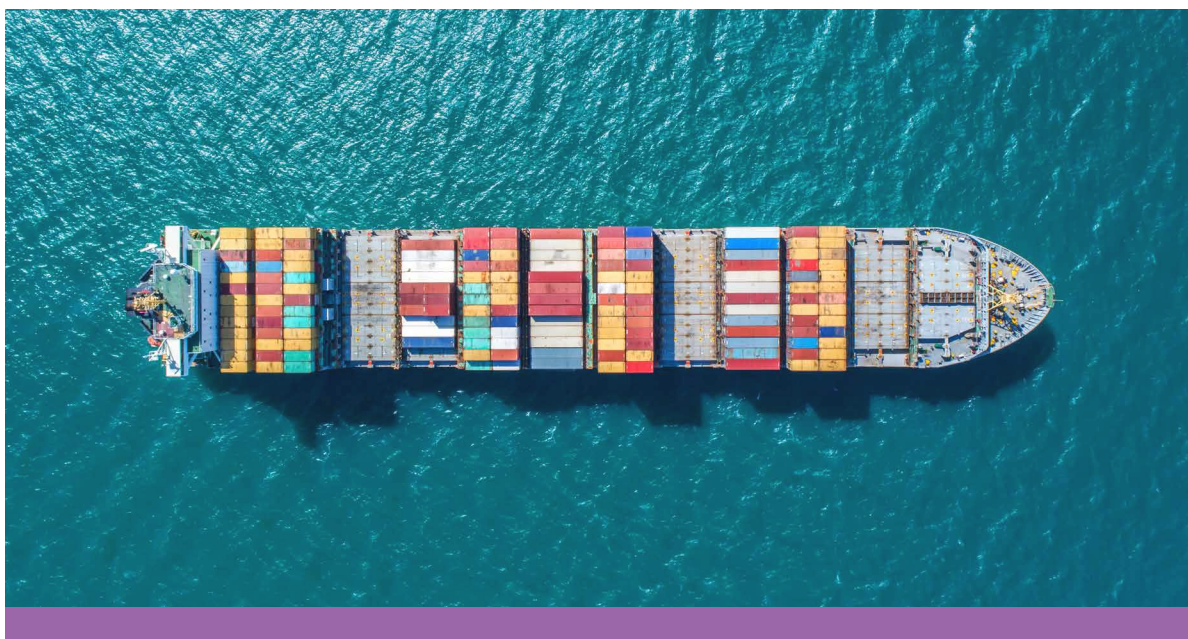
Passenger and public safety

In 2019/2020, seven people were killed on trains or in stations. There were 21 fatalities to members of the public from accidental causes which is seven fewer than the previous year. The overall level of harm recorded was 53.4 FWPI. This is lower than the level recorded in 2018/19. When normalised by passenger journeys, there was a 13% decrease in the rate of FWPI.

Note that the UK railway is the only one in Europe that is required to be continually fenced.



¹⁰ RSSB Annual Health and Safety Report 2019/2020: A summary of Health and Safety Performance Operational Learning and Risk Reduction activities on Britain's railway. <https://www.rssb.co.uk/en/safety-and-health/monitoring-safety/safety-performance-reports>



5.3 Maritime

Measurement of safety

In the UK it is a legal requirement that marine casualties and incidents are reported to the Marine Accident Investigation Branch (MAIB). There is an exception for certain craft – such as recreational and smaller commercial craft – unless the marine casualty involves an explosion, fire, capsizing of a power-driven vessel or results in death, serious injury or severe pollution.

A marine casualty¹¹ is an event or sequence of events that occurred directly in connection with the operation of a ship, and resulted in:

- The death of, or serious injury to a person.
- The loss of a person from a ship.
- The loss, presumed loss or abandonment of a ship.
- Material damage to a ship.
- The ship being unfit to proceed or requires flag state approval or a condition of class before it may proceed.
- A breakdown of the ship at sea requiring towage.
- The stranding or disabling of a ship, or the involvement of a ship in a collision.
- Material damage to marine infrastructure external of a ship that could seriously endanger the safety of the ship, another ship or any individual.
- Pollution caused by damage to a ship or ships.

A marine incident is an event, or sequence of events, which occurred directly in connection with the

operation of a ship but that does not classify as a marine casualty. These are categorised as events that endangered or, if not corrected, would endanger the safety of the ship, its occupants or any other person or the environment.

Examples of marine incidents include:

- Close-quarter situations where urgent action was required to avoid collision.
- Any event that had the potential to result in a serious injury.
- A fire that did not result in material damage.
- An unintended temporary grounding on soft mud, where there was no risk of stranding or material damage.
- A person overboard who was recovered without serious injury.
- Snagging of fishing gear resulting in a dangerous heel.

In the European Maritime Safety Agency (EMSA) *Annual Overview of Marine Casualties and Incidents 2019*, key figures for 2011-2018 indicate that 25,614 ships were involved in marine casualties or incidents and 230 ships lost. During this time there were 23,073 casualties and incidents, 665 very serious casualties, 7,694 persons injured, 696 fatalities and 1,377 investigations launched.

Overall safety and risk approach

Maritime safety is covered at an international, national and local level through a series of codes and conventions. Primary international safety is under the jurisdiction of the International Maritime Organisation (IMO). Before the IMO came into existence in 1958, several important international conventions had already been developed. These included the *International Convention for the Safety of Life at Sea (SOLAS) of 1948*¹², the *International Convention for the Prevention of Pollution of the Sea by Oil of 1954*¹³ and treaties dealing with load lines and the prevention of collisions at sea. The IMO is responsible for ensuring that these conventions are kept up to date and for developing new ones as and when the need arises.



IMO has also developed and adopted international collision regulations and global standards for seafarers, as well as international conventions and codes relating to search and rescue, the facilitation of international maritime traffic, load lines, the carriage of dangerous goods, and tonnage measurement. There are many other conventions relating to maritime safety and security and ship/port interfaces.

The Maritime Safety Committee (MSC) is IMO's senior technical body on safety-related matters. It deals with all business related to maritime safety and maritime security which fall within the scope of the IMO, covering both passenger and cargo ships.

This includes updating the *SOLAS Convention* and related codes such as those covering dangerous goods, life-saving appliances, and fire safety systems. MSC also deals with human element issues including training and certification of seafarers.

Key IMO conventions are the:

- *International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended.*
- *International Convention for the Prevention of Pollution from Ships, 1973, as modified by the Protocol of 1978 relating thereto and by the Protocol of 1997 (MARPOL).*
- *International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) as amended, including the 1995 and 2010 Manila Amendments.*
- *Convention on the International Regulations for Preventing Collisions at Sea (COLREG), 1972.*

International Convention for the Safety of Life at Sea (SOLAS), 1974

The SOLAS Convention in its successive forms is generally regarded as the most important of all international treaties concerning the safety of merchant ships. The first version was adopted in 1914 in response to the Titanic disaster, the second in 1929, the third in 1948, and the fourth in 1960. The 1974 version includes the tacit acceptance procedure, which notes that an amendment shall enter into force on a specified date unless objections to the amendment are received from an agreed number of parties before that date.

The main objective of the *SOLAS Convention* is to specify minimum standards for the construction, equipment, and operation of ships compatible with their safety. Flag states are responsible for ensuring that ships under their flag comply with its requirements, and a number of certificates are prescribed in the convention as proof that this has been done.

Control provisions also allow contracting governments to inspect ships of other contracting states if there are clear grounds for believing that the ship and its equipment do not substantially comply with the requirements of the convention. This procedure is known as port state control.



European Maritime Safety Agency (EMSA) and ship safety standards

EMSA provides European monitoring of IMO's work regarding ship safety standards, including reporting on developments in the relevant international legislation. This task entails technical evaluation of IMO submissions and technical assistance in the preparation of submissions to IMO as appropriate.

¹² [https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-\(SOLAS\),-1974.aspx](https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx)

¹³ [https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Prevention-of-Pollution-from-Ships-\(MARPOL\).aspx](https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Prevention-of-Pollution-from-Ships-(MARPOL).aspx)



Classification societies

A classification society is a non-governmental organisation that establishes and maintains technical standards for the construction and operation of ships and offshore structures. Classification societies certify that the construction of a vessel complies with relevant standards and carries out regular in-service surveys to ensure continuing compliance.

A classification certificate – issued by a classification society recognised by the proposed ship register – is required for a vessel's owner to be able to register the ship and obtain marine insurance. It may also need to be produced before a ship's entry into some ports or waterways and may be of interest to charterers and potential buyers. To avoid liability, classification societies explicitly disclaim responsibility for the safety, fitness for purpose or seaworthiness of the ship. Their role is to verify that the vessel is in compliance with the classification standards of the society.

At the same time, the United Nations Convention for the Law of the Sea (UNCLOS) and *SOLAS Convention* have made special provisions to specify that in the better interests of the shipping community, vessels need to be classed.

UK Maritime and Coastguard Agency (MCA)

UK national safety aspects are overseen by the Maritime and Coastguard Agency (MCA). An executive agency of Department for Transport (DfT), it is the UK flag state representative on the IMO. Its responsibilities include:

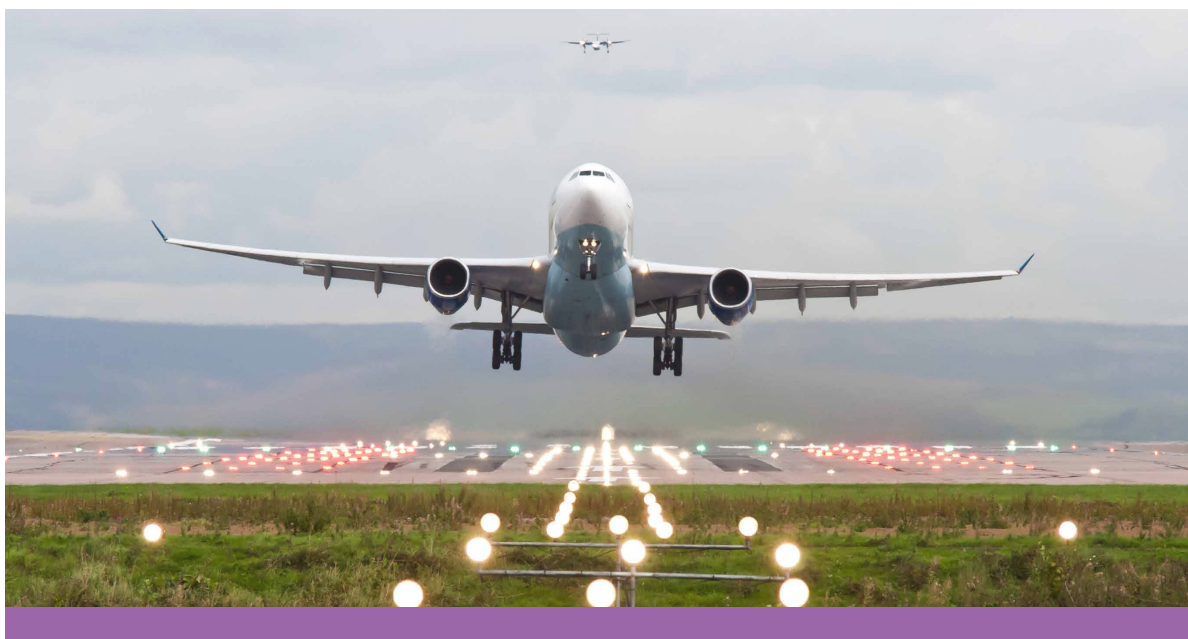
- The safety of everybody in a vessel in UK waters.
- The safety of all seafarers on UK flagged vessels.
- Making sure all equipment on UK vessels is fit for purpose.
- Making sure all seafarers on UK vessels have the correct documentation.
- The environmental safety of UK coast and waters.
- The accuracy of hydrographic data on UK charts.
- Overseeing coastal rescue volunteers, hydrographics, seafarer certification and the port state control inspection regime.

Risk assessments

Regular risk assessments are required to see how accidents, injuries or illnesses could be caused on a ship and how risks can be reduced.

They must be reviewed every year and whenever there are significant changes to either the ship or working activities.





5.4 Air

Air safety is covered at both international and national levels. The International Civil Aviation Organization (ICAO) is a United Nations (UN) specialised agency, established in 1944 to manage the administration and governance of the *Convention on International Civil Aviation (Chicago Convention)*.

ICAO works with the convention's 193 member states and industry groups to reach consensus on international civil aviation standards and recommended practices (SARPs) and policies in support of a safe, efficient, secure, economically sustainable and environmentally responsible civil aviation sector.

These SARPs and policies are used by ICAO member states to ensure local civil aviation operations and regulations conform to global norms. This in turn permits more than 100,000 daily flights in aviation's global network to operate safely and reliably.

Members of the European Union are collectively regulated by the European Aviation Safety Agency (EASA). In the UK, this responsibility lies with the UK Civil Aviation Authority (CAA).

Measurement of safety

ICAO reports safety in terms of accidents and fatalities per million departures. These are then subdivided by geographical area and by harmonised accident categories such as controlled flight into terrain (CFIT).

Other metrics are also used. For example, CAA quotes an average of one fatality for every 287 million passengers carried by UK operators¹⁴. The last fatal accident involving a large UK passenger aircraft was 1989 in the UK and 1999 outside the UK. The fatal accident rate for general aviation (GA) aircraft is significantly higher, at an average of 16 fatal accidents per annum since 1999.

ICAO reports that in 2018 nearly half of all commercial aircraft accidents were related to runway safety, although this only represents around 10% of fatalities. Loss of control in flight accounts for only 5% of accidents but 85% of fatalities. CFIT represented only 1% of accidents and no fatalities¹⁵.

The other internationally harmonised accident categories are:

- Ground safety.
- Operational damage, including in-flight damage.
- Injuries to and/or incapacitation of persons.
- Other.
- Unknown.

As autonomy is likely to make its initial impact on urban air mobility and medium-sized delivery drones, the GA accident rate is probably a more relevant target for equivalence.

¹⁴ <https://www.caa.co.uk/Consumers/Guide-to-aviation/Aviation-safety>

¹⁵ https://www.icao.int/safety/Documents/ICAO_SR_2019_final_web.pdf

Overall safety and risk approach

Aircraft, air traffic management (ATM) and infrastructure – including airfields – are separately regulated. However, the global nature of both operations and the industry means that common approaches and standards are required to safely allow aircraft to operate internationally.

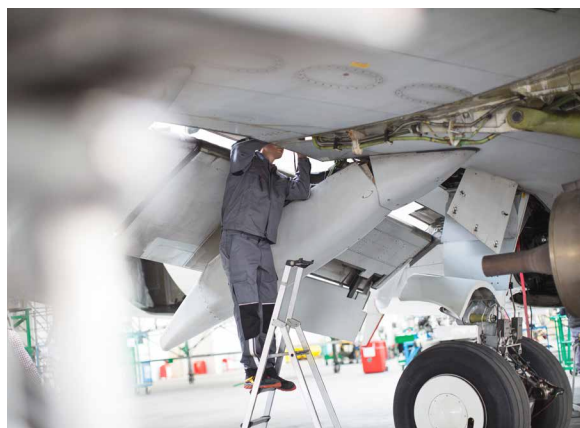
There is a formal requirement for design organisations to seek approval to design, make changes to aircraft and supply parts and appliances. They need to demonstrate that they have the right organisation, procedures, competencies, and resources under the *Part 21* process. The regulatory authorities produce certification specifications as non-binding technical standards for various classes of aircraft – such as the *EASA CS-25* for large commercial aircraft – to meet the essential requirements of the basic regulation. These are supported by *Acceptable Means of Compliance (AMC)* standards.

A type certificate (TC) is issued to signify the airworthiness of the approved aircraft design prior to manufacturing. Once issued by the regulatory authority, the design cannot be changed unless at least part of the certification process is repeated. The TC reflects a determination made by a regulatory authority that the type design complies with airworthiness requirements. Each individual aircraft will also have a Certificate of Airworthiness (CoA).



An important premise of aircraft design is the recognition that during service the aircraft may encounter problems that might compromise its safety, or which had not been anticipated in the design. This was recently demonstrated with the Boeing 737 Max accidents. This results in a reappraisal of the design and the issue of an airworthiness directive by the regulator to restore the type's airworthiness.

A further requirement is to maintain airworthiness throughout the life of the aircraft, referred to as continuing airworthiness. This requires a formal maintenance programme to be issued by the aircraft operator to correct any degradation in performance caused by wear and tear.



CAA CAP 795 Safety Management Systems (SMS) Guidance for Organisations provides guidance on the implementation of SMS. It applies to air operator certificate holders, continuing airworthiness management organisations, maintenance organisations, air navigation service providers, aerodromes, and approved training organisations. SMS will also be introduced as a mandatory requirement in 2022 for initial airworthiness organisations that hold a design or production approval.

Aviation has an occurrence reporting system through ICAO which requires states to establish mandatory incident reporting systems to gather information on actual or potential safety deficiencies. There is a no blame culture in this reporting; European Union Aviation Safety Agency (EASA) occurrence reporting is for safeguarding trust in the aviation safety system, without prejudice to the applicable rules of law. Therefore, EASA ensures that reported occurrence data is not held against the reporting parties and is solely used in the interest of aviation safety.

In the UK, aircraft accidents and serious incidents are investigated by the Air Accidents Investigation Branch under the DfT.

6. Expected impacts of automation on safety

The aim for each transport mode must be that autonomous systems achieve at least the same safety levels currently experienced, with the longer-term aim being significant improvement.

While this should be realisable from initial introduction in the rail, air and maritime sectors, this may not be possible in the significantly more complex environment of road. This is because the simulation and live testing of all possible scenarios for all environmental conditions may be incomplete.

For all sectors, there needs to be strategies for dealing with degraded modes of operation. While in the air, rail and maritime sectors this might involve intervention by a highly trained operator, this is unlikely to be a viable strategy for road.



6.1 Road



Automation is widely expected to have positive results for safety in the road sector. This is because it partially or fully takes control away from the driver, which accidentology shows is a major risk factor.

Transport and mobility consultancy and research firm, TRL, has studied road vehicle crashes and estimated the impact that automation could have had on safety outcomes. The form of accidents – such as type or road users involved – may also change¹⁶. There may be an increase in crashes caused by technical faults with automated vehicles, but this is expected to be more than offset by a reduction of crashes caused by poor driver behaviour.

Despite the expected overall long-term benefits of road automation, ethicists have cautioned against a solutionist approach. Instead, they propose that a broader set of ethical, legal and societal considerations need to be applied throughout development, deployment and use¹⁷.

This approach challenges the expectation that increased safety can be easily achieved. The broader aim is to ensure that relevant scientific, technical, societal and legal challenges are raised and addressed in a timely manner, that the risk of adverse, undesirable outcomes is minimised, and that the expected gains of the technology are accomplished for society as a whole.

The first six of the 20 ethical principles recently published by the European Commission (EC) for connected and autonomous vehicles (CAVs), relate closely to safety:

¹⁶ PPR851 - Automated Driving Systems - Understanding Future Collision Patterns Report v2 TRL December 2017

¹⁷ Ethics of Connected and Automated Vehicles: https://ec.europa.eu/info/news/new-recommendations-for-a-safe-and-ethical-transition-towards-driverless-mobility-2020-sep-18_en

- Ensure that CAVs reduce physical harm to persons.
- Prevent unsafe use by inherently safe design.
- Define clear standards for responsible open road testing.
- Consider revision of traffic rules to promote safety of CAVs and investigate exceptions to non-compliance with existing rules by CAVs.
- Redress inequalities in vulnerability among road users.
- Manage dilemmas by principles of risk distribution and shared ethical principles.

An example of the complexities particularly apparent in road automation is provided by an examination of the many unwritten rules through which road users negotiate shared use of the road space. These include hand signals, flashing lights and vehicle positioning, such as when entering a dense traffic stream from a side road or when two lanes of traffic merge into one.

Another example is when it becomes necessary to break one of the rules or guidelines, such as mounting a pavement in order to give passage to an emergency vehicle. One of the suggestions emerging from a recent Law Commission consultation¹⁸ is the need for the development of a digital highway code that defines all the unwritten rules and common-sense behaviour that human drivers use, but which automated vehicles may not have access to.

Unless this complexity is addressed, some argue that automated road vehicles will not find public acceptance and therefore potential safety benefits will not be realised.

It is important to recognise that automation will not take over all driving tasks for the foreseeable future and that its introduction will be progressive as new vehicles replace existing ones. Therefore, automation needs to be considered alongside other road safety improvements, particularly:

- Increased driver or vehicle perception through connectivity.
- Better driver training, graduated driver licencing and driver re-testing.
- Technical measures to help adherence to speed limits.
- Technical measures to reduce intoxicated driving (alcohol interlocks).
- Continued improvement in vehicle passive and active safety.
- Continued improvement in road design and speed limit setting.
- Increased enforcement of poor driver behaviour such as speeding and tailgating.

6.2 Rail



Automatic train control offers the possibility of improving the efficiency of the control of the movement of trains on the network by removing the variabilities of human driving and by eliminating human error.

This gives the opportunity to increase capacity, reduce energy usage, eliminate availability of staff as a cause of train delays and lower the overall cost of running the railway. At the same time consideration must be given to the impact on safety.

Automated train control on main lines may be perceived to impact everyone from train passengers and staff through to members of the public using level crossings.

The interlocking system implemented on most rail lines provides safety by presenting cautionary signals to prevent trains entering occupied sections. This would remain in all but the most advanced of train control systems, providing a consistent layer of protection against most in-motion accidents.

The primary means of protection on UK rail systems is the train protection and warning system (TPWS). This provides protection against trains passing signals at danger and is fitted to all critical signal locations. Automatic train protection (ATP) is a type of system which continually checks that the speed of a train is compatible with the permitted speed allowed by signaling, including automatic stop at certain signal aspects. If it is not, the system activates an emergency brake to stop the train.

Various implementations of communication-based train control (CBTC), including the European train control system (ETCS), have inherent forms of ATP. These warn the driver and apply brakes where necessary, also providing speed control and braking where movement authorities (MA) may be exceeded. A radio block centre (RBC) ensures that trains are not given conflicting MAs.

Automatic train operation is a form of train control which sits on top of the train control system. It provides enhanced driving and is mainly used to improve efficiency by providing an optimum speed, reducing the need to brake/accelerate.

Various forms of enhanced driving are currently being considered and implemented.

Drivers advisory system (DAS, also known as S-DAS) can be deployed by the train operator in isolation.

S-DAS:

- Knows the speed on each section of line.
- Knows where the train should be on its journey.
- Knows the optimum acceleration and deceleration of the train.
- Advises the driver to speed up or slow down.

Connected DAS (C-DAS) requires some form of real-time intelligence (traffic management).

C-DAS:

- Utilises information available outside the train (can be processed on and off the train).
- May know where other trains are.
- May know the condition of the track ahead.
- Can optimise for energy efficiency, operational capacity, and disruption management.

Automatic train operation (ATO) offers various grades of automation.

Specified grades of automation (GOA) are:

- GOA 0: Manual operation with no automatic train protection.
- GOA 1: Manual operation with automatic train protection.
- GOA 2: Semi-automatic train operation.
- GOA 3: Driverless train operation.
- GOA 4: Unattended train operation.

Computer controlled/electronic interlocking of track switches (points) provides the interface between train control and signalling - ATO, ATP, CBTC and so on - and the track infrastructure requires the highest safety integrity; SIL 4 (see Safety Integrity Level section 3.2).

All forms of enhanced driving require new rules, human factor analysis, training and potentially culture change. The implementation of any new technology for train speed and position management needs to consider the culture of the environment into which it is adopted and be supported by a holistic assessment. This needs to take full account of the human element in the cause consequence chain of possible hazardous events.

It will be very important that the division of safety responsibility between ATO and the underlying safety layer are clear. It should not be possible for ATO to override, challenge or provoke the safety layer.

Cybersecurity is also becoming increasingly important in railway systems due to the extensive use of telecommunication networks. If potential attacks are not adequately mitigated, these could cause severe interruption to train services and even serious safety implications.

6.3 Maritime



Under the International Maritime Organisation (IMO), the 98th session of the Maritime Safety Committee (MSC 98) agreed to work on a regulatory scoping exercise for the use of maritime autonomous surface ships (MASS), with a target completion year of 2020, but this is still underway.

IMO framework – degrees of autonomy:

Under the IMO scoping study, they have identified four degrees of autonomy which form the starting point for the work.

1. Ship with automated processes and decision support: seafarers on-board but some operations may be automated and at times unsupervised.
2. Remotely controlled ship with seafarers on-board; the ship is controlled and operated from another location. Seafarers are available on-board to take control.
3. Remotely controlled ship without seafarers on-board: the ship is controlled and operated from another location.
4. Fully autonomous ship: the operating system of the ship can make decisions and determine actions by itself.

The fast pace of change in maritime autonomy demands updated and relevant guidance for those owning and operating MASS. The Maritime UK Autonomous Systems Regulatory Working Group (MASRWG) published the first *Code of Practice* to global industry-wide acclaim in November 2017, with the second version following in November 2018. A fourth version was published in November 2020¹⁹.

While not a legal text, the code has been used by manufacturers, service providers and others as part of their day-to-day work. Many manufacturers have reported clients requiring compliance with the code as a basis for contractual negotiations.

Previous versions were focused on the design and manufacture of vessels, the operation of autonomous vessels and in particular skills and training. Version three of the *UK Industry Code of Practice* demonstrates the UK's continued leadership on autonomy, with new sections on inland waterways. There is also an enhanced section on the principles that should underpin the design, manufacture and operation of autonomous vessels. This version replaces the *Code of Conduct (2016)* and version two of the *Code of Practice (2018)*²⁰.

¹⁹ <https://www.maritimeuk.org/priorities/innovation/maritime-uk-autonomous-systems-regulatory-working-group/mass-uk-industry-conduct-principles-and-code-practice/>

²⁰ <https://www.maritimeuk.org/media-centre/publications/maritime-autonomous-surface-ships-industry-conduct-principles-code-practice/>

IMO, under MSC, has developed interim guidelines for MASS trials. Among other things, the guidelines say that trials should be conducted in a manner that provides at least the same degree of safety, security and protection of the environment as the relevant instruments. Risks associated with the trials should be appropriately identified, and measures to reduce risks to as low as reasonably practicable and acceptable should be put in place.

Any personnel involved in MASS trials, whether remote or on-board, should be appropriately qualified and experienced to safely undertake them. Suitable steps should be taken to ensure sufficient cyber risk management of the systems and infrastructure used.

In addition, the IMO are undertaking a scoping exercise to look at how the safe, secure and environmentally sound operation of MASS may be introduced in IMO instruments.

This is currently identifying, in the relevant treaties, provisions which:

- Apply to MASS and prevent MASS operations.
- Apply to MASS and does not prevent MASS operations and require no action.
- Apply to MASS and does not prevent MASS operations but may need to be amended or clarified and/or may contain gaps.
- Have no application to MASS operations.

Once the first step is completed, a second step will be conducted to analyse and determine the most appropriate way of addressing MASS operations. This will consider, among other things, the human element, technology, and operational factors.

The Maritime and Coastguard Agency (MCA) is in the process of consulting with the autonomy industry to help develop UK regulations in the following areas:

- Appropriate regulation and useful guidance.
- Identification and highlighting existing regulations and guidance that already apply to lower levels of autonomy.
- Ensuring that UK activity is coordinated and consistent with IMO developments for autonomy, leading and guiding where appropriate.
- Encouraging a positive environment and culture for growth of the UK maritime autonomous system sector.
- Working with MCA, classification societies and certifying authority colleagues to ensure growth of understanding.

6.4 Air



Automation not only has the potential to further improve the safety of aircraft, but also to extend the use of aircraft in undertaking dull, dirty, and dangerous activities in addition to new ventures such as urban air mobility.

For the dull, dirty, and dangerous activities – such as pipeline inspections, freight delivery or crop spraying – the main benefit is removing the human factor from the aircraft. This reduces one level of risk but might, without mitigation, increase the risk of collision with other air users, or with people or infrastructure on the ground. Although all current applications are unmanned, new applications of passenger transport, such as air taxis, will ultimately be pilotless and be fully autonomous. There will also be additional challenges in addressing complex air traffic management in urban areas.

The UK Civil Aviation Authority (CAA) was one of the first regulators to issue guidance and policy for unmanned aircraft systems (UAS) in 2002. *CAP 722 – Unmanned Aircraft Systems Operations in UK Airspace – Guidance*²¹, is now in its 8th edition. In 2019 the EC issued a package of regulations relating to the use of UAS; *Commission Implementing Regulation (EU) 2019/947*²² and *Commission Delegated Regulation (EU) 2019/945*²³. Their implementation was postponed until 31 December 2020 but have now become legally applicable in the UK. The 8th edition is a major revision and takes a risk and operation centric approach to UAS operations, creating three categories, Open, Specific and Certified.

In the UK, airspace is divided into five classes: A, C, D and E of controlled airspace and G of uncontrolled airspace. In controlled airspace, separation safety is principally the responsibility of the ground-based air traffic control (ATC) system, although the pilot has final responsibility for visual identification of threats. In uncontrolled, Class G, airspace, navigation and separation are the responsibility of the pilot, although some assistance can be sought from ATC. At present interaction between ATC and the aircraft is by voice instruction. To further develop the use and extent of automation there will need to be closer integration between: aircraft; aircraft and ATC; and aircraft and infrastructure.

Flying is one of the safest ways to travel, with an accident rate for commercial passenger aircraft of approximately 0.6 fatal accidents per million departures²⁴. Accomplishing this took the airline

²¹ <https://publicapps.caa.co.uk/modalapplication.aspx?appid=11&mode=detail&id=415>

²² <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0947>

²³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0945>

²⁴ https://en.wikipedia.org/wiki/Aviation_safety

industry decades, however autonomous air vehicles will be expected to meet or exceed these standards at the outset. The current developments of fully electric and hybrid electric aircraft adds a further dimension to this challenge as these will be expected to operate in a very different environment from traditional aviation. As a result, autonomous air vehicle designers and builders will need to implement the necessary safety precautions and redundancies to ensure that air vehicles can operate safely even under highly unusual circumstances.

The design of autonomous air vehicles will be qualified and certified in a very similar manner to crewed aircraft. This is because they will need to integrate transparently with current operations.

The main challenges will be:

- Initial airworthiness
- Maintaining airspace.
- Integrated and constrained take offs and landings.
- Remote and autonomous piloting.
- Flight readiness certification.
- Continuing airworthiness.

The regulatory framework

The principal objective of the aviation regulatory framework is to achieve and maintain the highest possible level of safety. In the case of autonomous air vehicles this means ensuring the safety of any other airspace user as well as people and property on the ground.

Identifying the commonalities and differences between manned and unmanned aircraft is the first step toward developing a regulatory framework that will provide, at a minimum, an equivalent level of safety for the integration of UAS into non-segregated airspace and aerodromes. However, with uncrewed aviation, the primary consideration is the type of operation being conducted, rather than who or what is conducting it, or why it is being done. If there is 'no one on-board' the aircraft, the consequences of an incident or accident are purely dependent on where that incident/accident takes place. The CAA's focus is therefore on the risk that the UAS operation presents to third parties, which means that more effort or proof is required where the risk is greater.

Technical specifications to support airworthiness, command, and control (C2), detect and avoid, and other functionalities are being addressed by various industry standards development organisations around the world. As individual technologies reach maturity, the relevant standards and recommended practices (SARPs) will be adopted. This will be an evolutionary process, with SARPs added gradually.

Certification basis

Type certification of autonomous air vehicles will differ from conventional rotorcraft or fixed-wing aircraft. In the absence of suitable certification specifications, a complete set of dedicated technical specifications in the form of a special condition for autonomous aircraft will be developed.

Special conditions will be defined to address the unique characteristics of these aircrafts and will prescribe airworthiness standards for the issue of a type certificate, and changes to this type certificate.

The special conditions establish the safety and design objectives. This approach, previously used for the development of the certification standard (CS) basis, is designed to not limit technical innovation by describing prescriptive design solutions as certification standards, including safety. The special conditions do not contain the means to demonstrate compliance with the safety and design objectives and this is an area that needs to be developed, building on the current aviation safety standards.

UAS standards are very conservative in terms of level of autonomy. CAP 722 proposes that UAS must meet at least the same safety and operational standards as crewed aircraft; the technologies used by the UAS must be demonstrably equivalent to human capabilities. For example, uncrewed detect-and-avoid systems must provide the same level of collision avoidance as crewed see-and-avoid systems. Furthermore, UAS should provide transparency; the air traffic control operator must not have to apply a different set of rules or assumptions when providing an air traffic service to a UAS. CAP 722 currently requires that a general principle be observed - that all UAS must be under the command of a remote pilot.

It follows that regulators want to avoid changes to the existing rules of the air, although this approach may sacrifice valuable opportunities to achieve increased levels of safety.

In summary, significant development and change to existing safety standards for the development, test, certification, and operations of autonomous air vehicles is required. Both the regulatory authorities and industry will need to take key stakeholder roles in their development and acceptance.

7. Conclusions



The current approaches to describing safety in all four sectors are, to some extent, empirical. These have been reasonable methods until now, as advances in sectors have been somewhat incremental.

However, autonomy presents a complete paradigm shift that is heavily dependent on recent advances in data sciences (DS) and artificial intelligence (AI). Many of the AI/DS technologies that contribute to autonomy rely on scientific and theoretical advances in these fields made in the last 10 years. Consequently, the field of verification and validation providing system assurance has yet to bridge the enormous semantic gap between these new technologies and, to varying degrees, the empirical models of safety employed in the four transport sectors.

An example includes phenomena such as data bias, where the behaviours of a software element will depend on the data sets used to develop it, and the overall effect this has on a system's behaviour and therefore safety. Others include errors in data sets and how, or indeed when, they should be corrected, and the impact that they may have on a safety specification.

We need to rethink the safety standards and regulations for safety critical AI-based systems, especially those that have a real-time role. This extends beyond traditional software standards and into challenges around data selection and application, particularly for machine learning. The challenges include ongoing data usage when in operation and the behavioural aspects of AI-to-AI connectivity, particularly as connected autonomous vehicles become more prevalent. Generic standards such as *IEC 61508*, which is used as the basis for most sectors' safety related systems standards, require a fundamental rethink to address these new challenges.

Aviation has perhaps made the most progress over the past 20 years in terms of bridging the gap between software specification and safety specification. This is thanks to *DO178C* and the techniques and formalisms it permits and mandates. However, state of the art verification and validation techniques still do not permit complete specifications of behaviours of these systems, although they go some way to quantifying what is expected. The road sector is now also developing new approaches through "Safety of the Intended Functionality" standards.

However, these approaches do not go very far in bridging the enormous semantic gap with system level safety, such as certification or type approval,

or the standards presented in each of the four modes of transport. These semantic bridges are likely to be very similar across all modes of transport in terms of underlying theoretical techniques, if not perhaps languages, tools and supporting technologies.

The development of these underlying theoretical techniques is a vital and significant step to enable the wider deployment of autonomous systems in a way that can be demonstrated to have known and quantifiable levels of safety and risk.

All four transport sectors stand to benefit significantly from improved safety and mobility through the further developments in automation. They share all the same basic principles although the details of implementation may differ. The transport sectors have grown largely independently but there is now an opportunity for them to share in this revolution, making efficient use of scarce specialist resources and increasing the pace of developments.

Each sector takes a different approach to assessing and reporting on risk and safety. We recommend that the DfT makes cross-modal comparisons when reporting their annual statistics. The best metrics to be used needs some detailed research and could include multi-year average death rates and other comparable units to gain the greatest learning benefit.

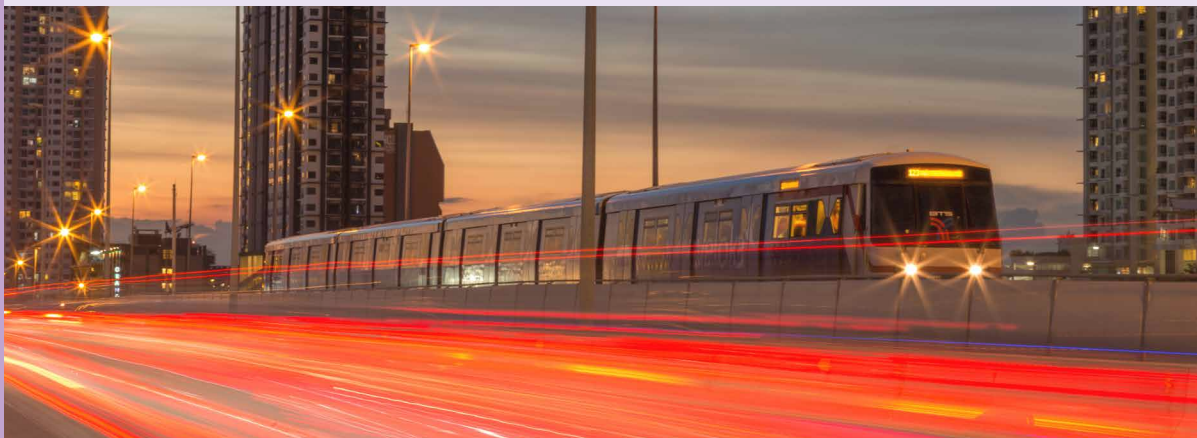
Further investment is needed into the validation and verification of AI systems, both training and operational, and the qualification of safety critical AI applications. This needs to include a national

resource for the collection, dissemination and use of data sets drawn from all sectors, as well as establishing international collaboration. This data could be used for research and to inform standards development.

The rail, air and maritime sectors have benefitted from having formal independent accident investigation branches and with the air sector adopting a no blame culture of incident reporting. This has contributed massively to safety improvements. We recommend that the DfT establishes a road accident investigation branch along similar lines to bring together the expertise in vehicle crashes that is currently widely distributed.

As the autonomous system architectures for all transport sectors will follow the same basic form, there should be significant benefit from establishing a cross-modal working group to develop a new standard for the functional safety of programmable safety-related systems. It will need to recognise that management and maintenance of these complex safety critical systems will be at least as challenging as their initial design and establish requirements and infrastructure to ensure safety is maintained throughout a system's life.

The introduction of the benefits to be derived from these complex systems does, however, also increase the risk of both malicious and non-malicious cyber-attacks. We recommend that existing standards be reviewed for their suitability and adequacy and that investment is made to address any shortfalls.



8. Acknowledgements

The authors of this report are members of the IET Transport Policy and Sector Panels and represent a wide array of backgrounds from industry and academia across the road, rail, maritime and air sectors. They are as follows:

Lambert Dopping-Hepenstal, DH Future Systems and Chair of the IET Transport Policy Panel Safety in Autonomy Working Group

Steve Denniss, WSP and member of the IET Transport Sector Committee

David Lindley, Volocopter and member of the IET Transport Policy Panel

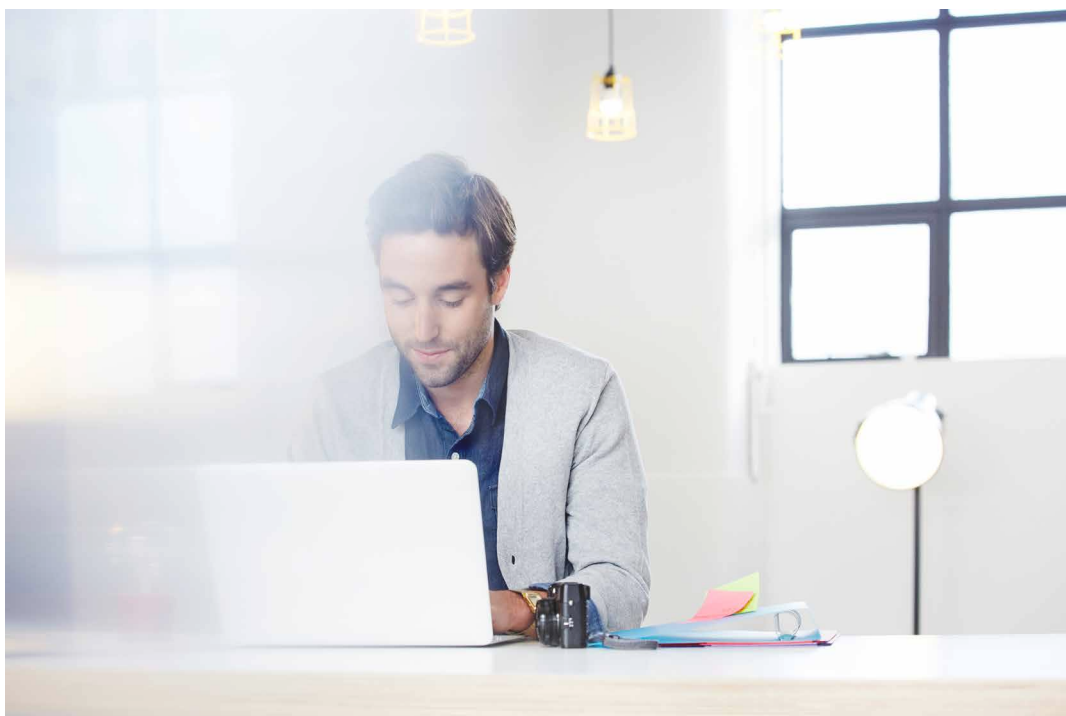
Freyja Lockwood, Bristol City Council and member of the IET Transport Sector Committee

Alistair McEwan, University of Derby

Peter Sheppard, WSP and member of the IET Transport Policy Panel

Alan Stevens, University of Southampton and member of the IET Transport Policy Panel

Richard Westgarth, BMT and member of the IET Transport Sector Committee



9. About the IET



We are the IET – a charitable engineering institution with over **158,000 members** in **150 countries** – working to engineer a better world.

Our mission is to inspire, inform and influence the global engineering community to advance technology and innovation for the benefit of society.

As a diverse home across engineering and technology, we share knowledge that helps make better sense of the world in order to solve the challenges that matter. It is why we are uniquely placed to champion engineering.

We bring together engineers, technicians and practitioners from industry and business, from academia and research, and from government and the third sector. We are member-led, independent and impartial.

We cover engineering across industry from design and production, digital and energy to healthcare, transport and the built environment. Passionate about transport, we bring together expert practitioners from the transport industry, academia and third sector.

We champion engineers and technicians working in the sector by offering networking, volunteering and thought leadership opportunities. Together, we campaign on issues of the day around transport and provide policy input to government.

Your specialist knowledge can inspire others and make a difference. To find out more contact sep@theiet.org

Our offices

London, UK

T +44 (0)20 7344 8460

E faradaycentre@ietvenues.co.uk

Stevenage, UK

T +44 (0)1438 313311

E postmaster@theiet.org

Beijing, China

T +86 10 6566 4687

E china@theiet.org

W theiet.org.cn

Hong Kong

T +852 2521 2140

E adminap@theiet.org

Bangalore, India

T +91 80 4089 2222

E india@theiet.in

W theiet.in

New Jersey, USA

T +1 (732) 321 5575

E ietusa@theiet.org

@TheIET      

theiet.org

The Institution of Engineering and Technology (IET) is working to engineer a better world. We inspire, inform and influence the global engineering community, supporting technology innovation to meet the needs of society. The Institution of Engineering and Technology is registered as a Charity in England and Wales (No. 211014) and Scotland (No. SC038698). Michael Faraday House, Six Hills Way, Stevenage, Hertfordshire, SG1 2AY, United Kingdom.