Building a Safety Case for Automated Mobility:

Smart Cities and Autonomous Mobility – Getting There Safely

Building a Safety Case for Automated Mobility:

Smart Cities and Autonomous Mobility – Getting There Safely

Today's world of mobility is dramatically changing, triggered by the development of new technologies, consumer demands, congested roadways, legislation and a focus on accident-free driving. Although full-fledged, self-driving vehicles haven't hit the roads yet, autonomous vehicles are, in a sense, the next generation of mobility.

With the first of three phases of autonomy underway – partial, conditional and fully automated – the global marketplace can expect fully automated vehicles to be on the road by 2025, according to the US Secretary of Transportation, Anthony Foxx. Major auto manufacturers are already implementing automated driving technologies into their fleets at some level. However, continued innovation and advancement of current technologies are needed to meet the safety requirements that society demands from a full-fledged autonomous vehicle.

Urbanization and connectivity: smart cities emerge

According to statistics from the United Nations, more than half of the world's population lives in urban areas, and this number is expected to increase to 66 percent by 2050. By 2030, it is projected that there will be 41 "mega-cities." Managing these fast-growing, densely populated cities will pose numerous challenges, including efficient transportation to meet the needs of residents.

Smart cities are the vision to improve the efficiency and sustainability of urban areas, ultimately improving quality of life. Defined by their ability to ease the lives of their citizens and provide efficient connectivity, smart cities rely heavily on efficient transportation.

A smart city vision of transportation involves the integration of a variety of modes of mobility – public transit, bicycles, walking paths, commercial vehicles and passenger vehicles – into a variety of convenient and accessible systems. In this concept, autonomous vehicles will play an important role in efficient and safe transportation in a densely populated environment as well as fuel efficient transport of goods between cities.

Safety assurance gap for connected and autonomous vehicles

One key issue with the development of autonomous driving and smart cities is safety. In the US, and many other countries around the world, safety policies and regulations are emerging to keep pace with technology advances for connected and automated vehicles. These new technologies present a need for new processes to achieve safety assurance.

As many countries, states and medium-to-large cities look to leverage autonomous driving, there is a need to develop and evaluate the safety case for each application of this form of transportation. Government, insurance providers and manufacturers must consider safety in the early stages of technology and application development, as well as deployment.

Standardized safety practices and processes offer a number of different benefits, including the ability to further advance technologies, define consistent and clear expectations for product performance and reliability, lower trade barriers, decrease design time and more.

While policy and regulation will provide clarity for manufacturers and technology developers to create their safety cases, it is also important for local governments and city planners to consider the environmental conditions of a vehicle during each of the three phases of autonomy – partial, conditional and full automation. Assessing where issues and risks may lie will help with road, city and technology planning for overall mobility and safety.

Policy and regulation emerging

The United States Automated Vehicle Policy – Performance Guidance includes a 15-Point Safety Assessment that provides a roadmap to achieve robust product and system design. The Assessment will include:

- *The operational design domain*: Manufacturers should define the operational design domain including roadway types, geographic area, speed range, environmental conditions and other constraints
- *Object and event detection and response systems*: Organizations should have a documented process for assessing, testing, and validating autonomous vehicle systems to work under normal and other conditions
- *Minimal risk conditions*: Manufacturers should have a documented process for moving to a minimal risk condition when a problem is detected in the system including during the occurrence of malfunctioning, degraded states or other operational issues
- *Validation methods*: Testing and validation methodology should be developed to ensure a high level of safety within an automated system
- *Registration and certification to NHTSA*: The Agency requests that manufacturers submit identifying information on the items they use in autonomous systems to NHTSA as well as provide concise information to human drivers on the system capabilities
- *Data recording and sharing*: Manufacturers should adopt a documented policy to test, validate and collect data on events, incidents, and crashes to report failures, malfunctions, and degradations that can be stored and available for retrieval by NHTSA
- *Post-crash performance and behavior*: Manufacturers should assess, test and validate the autonomous system and prevent use in autonomous mode if safety controls or sensors are damaged
- *Privacy considerations*: Manufacturers should establish privacy policies and practices to ensure transparency, choice, respect for context, minimization, de-identification, retention, data security, integrity and access, and accountability
- *System safety and engineering safety practices*: All companies in the value stream should have a robust design and validation process that verifies the subsystem as an individual component and within the complete vehicle architecture
- *Cybersecurity*: All companies in the value stream should follow a robust development process to minimize safety risks including systematic and ongoing risk assessments following the NIST guidelines
- *Human-machine interface*: Manufacturers should consider the drivers' ability to remain alert and engaged in their environment
- *Crashworthiness*: All autonomous vehicles must continue to meet NHTSA crashworthiness standards
- *Consumer education and training*: Manufacturers should develop consumer and employee, dealer and distributor education and training to address the difference in using an autonomous vehicle
- *Ethical dilemmas and considerations*: All companies should assess situations to ensure ethical judgments and decisions are made to foster safety, mobility and legality
- *Compliance with federal, state and local laws*: Manufacturers should develop plans to detail how they will comply with all applicable laws, including traffic laws within the region of vehicle operation

Courtesy of Butzel Long

The human role and automated vehicle risk - shifting from driver to supervisor

Risk categories		Partial automation	Conditional automation	Full automation*
Human interaction with system/vehicle	• Education • New/other skills • Mental load • Situation awareness • System failiure • System misuse • Unexpected event	Driver risks		Operator risks
Interaction with other road users	• Information for others • Predictable behavior • Traffic regulations • Misuse/"testing" • Mimic automatic vehicle		Other road users risks	
Location and time of testing	• Lane/place on road • Route/speed • Weather and traffic			

There are a number of risks associated with using autonomous technology for mass transit. A safety case helps to ensure overall safety of the vehicle passengers, other road users and pedestrians nearby.

Data provided by: Institute for Road Safety (SWOV) Netherlands

There are two scenarios for safety assurance that ensure a high level of safety is integrated into each vehicle that operates autonomously, as well as the infrastructure used during V2I (vehicle to infrastructure) communication:

- Self-safety assurance – a company develops a safety case independently, after which the safety case is assessed by a third-party organization
- Independent safety assurance – a third-party organization is used to develop the safety case for the vehicle and assure it meets industry standards

Turning to rail – already a leader for autonomous safety

Dating back to the 1990s, the rail industry experienced a similar challenge with its automated systems, and can serve as a reference to transfer knowledge and experience to this new frontier. To ensure a sufficient degree of safety, the European Union (EU) opted for a common approach to approve driverless rail transport systems – defining a process to create a safety case. As highly automated systems are common practice in railway environments, as well as urban transit systems, the industry's process to define a safety case provides experience for developing on-road vehicle safety assurance.

Case study

Truck platooning safety case

Ricardo Rail supported the project management and developed the safety case for a truck platooning system carried out by a the Dutch EcoTwin consortium including DAF, NXP and TNO. The project included a successful two-truck demonstration for the April 2016 European Truck Platooning Challenge (ETPC).

Several challenges were posed in this project, which included driving and control strategies, technology development, safety and robustness measures needed for driving on a public road intermixed with other traffic, in addition to the road-exemption process with Dutch National Vehicle Authority (RDW) for driving on public roads with a prototype system.

The project was successfully demonstrated on public roads with closed-loop Wi-Fi-P longitudinal control and lateral lane-keeping assistance. The Ricardo Rail experts leveraged their knowledge and process approach to successfully develop a detailed safety case for the ETPC test which was approved by the RDW authorities.

Case study

Developing safe autonomous public transportation

Looking to develop the first self-driving electric shuttle for use on public roads in the Netherlands, WEpods developers enlisted the help from an independent third-party organization to write a safety case – in this case, Ricardo Rail.

Transporting up to six passengers between the two towns of Wageningen and Ede, the shuttle needed to function safely in an environment where both pedestrians and other vehicles were present. The third-party safety assurance experts successfully delivered a safety plan for WEpods that included hazard identification sessions, Failure Mode Effects Analysis (FMEA) and collection, coordination and communication of the safety evidence.

This safety case combined the necessary evidence in a consistent and coherent way and aided the authorities to make a final go/no-go decision for the WEpod.

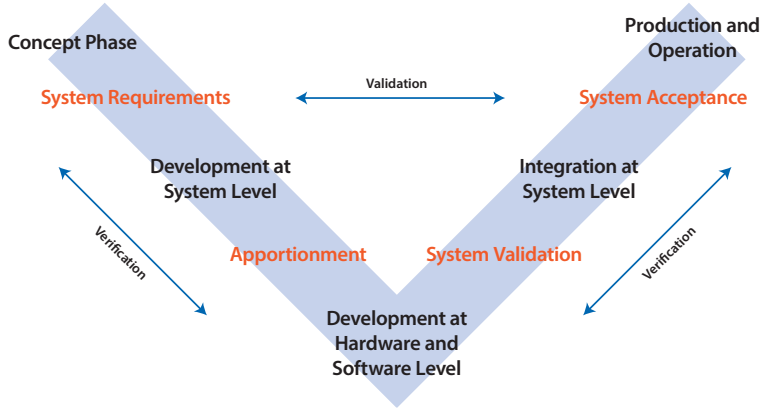
A proven safety case process for autonomous vehicles

One tool that is proven in the development of an autonomous safety case, and used within the rail industry, is the V model. The system lifecycle approach supports the design and execution of safe autonomous transportation concepts based on intended use, the environment in which it will operate, as well as defining limitations and identifying and assessing potential risks.

From vehicle development to testing and simulation, each step builds on the insights of the previous step, leading to multiple layers of safety in the design on a functional, technical and testing level. This process creates a strategic basis for testing the vehicle functionality against the original design, proving the end product does what it is supposed to do.

Creating an autonomous transportation safety case for a dedicated lane in an airport, where no pedestrians are located is one scenario with a certain set of characteristics. A scenario that contains a mixture of vehicle types, unpredictable pedestrian behavior and heavy traffic take much different characteristics into consideration. Although the same lifecycle approach would be taken early on in the development process, each safety case would be unique based on the defined characteristics of each autonomous scenario.

By following the V model during a safety case, engineers and developers can generate the appropriate safety evidence to ensure that the end result meets the needs of consumers while providing adequate safety measures for society. Additionally, the safety case must start early in the development process or the results may extend development time or failure to provide enough evidence of safety assurance for the autonomous system.



System Lifecycle Approach to Safety: Used throughout a safety case, this lifecycle model represents the development of the system from first concept to operation.

Building the foundation: defining the autonomous transportation concept

The first step in the process is to define the autonomous transportation concept including the use, environment and limitations. It is critical to identify all of the key characteristics of the concept and the environment in which it will operate. This definition is used throughout the V-model process.

Key characteristics used to define an autonomous transportation concept

- Infrastructure
- Use
- Users
- Speed limitations
- Weather conditions
- Sensor interference and hacking
- Type and density of traffic
- Technology

Safety goals shaped by risk and hazard analysis

The next step in the process is to analyze the safety hazards and risks associated with the autonomous transportation concept, based on the definition developed in the first step. Hazards might include obstacles in the travel lane or changes in traffic flow that would require crash avoidance capability, and the associated risk would be related to the ability to adjust to a minimal risk condition such as bringing the vehicle safely to a stop.

Once risks and hazards are identified, a list of safety goals are identified based

on established safety protocols such as the Automotive Safety Integration Levels (ASIL). The ASIL specification asks the question, "if a failure arises, what will happen to the driver and associated road user?" The risk is rated, based on a combination of exposure, driver controllability and severity of the possible outcome. Once the ASIL safety classification is identified for the given risks, safety requirements are established.

Identifying safety requirements: two scenarios

Derived from the safety goals, safety requirements serve as the input for the hardware and software development. Two different scenarios regarding safety are expected to arise - for both driver and driverless applications. Driver applications will focus on whether the driver has control when they encounter a hazard or not. However, due to the limited controllability in a driverless vehicle, the requirements must be analyzed differently. A common method of safety analysis in these scenarios involves investigating what level of safety is socially acceptable, based on an analysis of road accident statistics, and then translating that into maximum acceptable failure rates for automated functions.

Continuous testing ensures safety goals are met

Validation and verification activities are conducted throughout the system lifecycle development process. Verification activities are performed to ensure the process and the work conducted on the autonomous concept meets all the necessary requirements and is accurate. Validation tests are designed to make sure the vehicle behaves as designed and the safety goals are met.

Gathering real-world evidence

Testing and simulation are the key sources of information to generate safety evidence in the safety case. The results from the safety activities in Figure X are reported and collected in the safety case, then used as evidence to ensure the autonomous vehicle concept can safely be implemented.

Key testing and simulation activities needed for a safety case:

- Simulation test reports
- Integration rest reports
- Safety functionality test reports
- Validation reports
- Electromagnetic compatibility (EMC) test reports

Test elements required in safety case testing:

- (Non) regression test
- Reproducibility of test results
- Variation of conditions
- Static and dynamic testing
- Module testing, road testing, integrated functional tests

When the safety case combines all of the necessary safety evidence in a consistent and coherent way, it supports the authorities in making the final go/no-go decision of the autonomous application under consideration. This way, it can be demonstrated that this decision is based on documented and traceable safety evidence.

Safety assurance relies on process and application knowledge

While we can expect fully autonomous vehicles and smart cities in the coming years, cost, regulations and safety must be considered thoroughly and proactively. The good news is there are other industries, such as rail in the EU, that have successfully faced a similar challenge to create new safety assurance processes for critical automated transport systems. City infrastructure and automobile industries can leverage this knowledge and experience to accelerate successful deployment.

Cities and manufacturers that deliver automated transport capabilities must consider the safety case at early stages of vehicle and infrastructure development. If the safety case is not considered early in both the application and technology development, it can lead to project failure or, worse, costly adaptations to achieve the desired assurance of safety. Leveraging the knowledge and experience of experts in safety assurance, as well as a proven process to deliver a safety case, such as the approach outlined in this paper, is key to safety assurance. Society must have mobility with knowledge that safety is ensured.

Why Ricardo?

Ricardo is a global strategic, technical and environmental consultancy. It also is a specialist niche manufacturer of high-performance products. The company employs more than 2,000 professional engineers, consultants and scientists who are committed to delivering outstanding projects focused on class-leading innovation in our core product areas of engine, transmission, vehicle, hybrid and electrical systems, environmental forecasting and impact analysis.

On March 1, 2016, Ricardo plc announced the completed acquisition of Lloyd's Register Rail. On July 20, 2016 the company announced that it had been formally accredited by the United Kingdom Accreditation Service (UKAS) to provide independent assurance services for the international rail sector. This experience in safety assurance for the global rail industry, coupled with its knowledge and work in functional safety within the automotive industry, positions the company to support governments, insurance providers, manufacturers and technology developers to establish strategies for safe autonomous driving.

Ricardo's services cover a range of market sectors including passenger car, commercial vehicle, rail, defense, motorsport, motorcycle, off-highway, marine, clean energy and power generation and government. Clients include the world's major transportation original equipment manufacturers, supply chain organizations, energy companies, financial institutions and government agencies.

Services include:

Technical Consulting
Performance Products
Environmental Consulting
Ricardo Strategic Consulting
Ricardo Software
Independent Assurance

For more information on Autonomous Vehicle Safety, e-mail **info@ricardo.com**

RICARDO

Delivering Excellence Through Innovation & Technology

www.**ricardo**.com