Arthur D Little

Viewpoint

Safety on the move

Evolving risk culture in the automotive sector

The automotive sector is in a period of extreme disruption. Alongside trends in decarbonization of transport, technology is fundamentally shifting the way vehicles work, including increasing levels of automation with the expectation that fully autonomous vehicles will be the vehicles of tomorrow. Today, with advanced driver-assistance systems (ADAS) becoming ever more capable, there is an ongoing shift in safety responsibility from driver to vehicle. This shift brings with it the need for a revised approach to managing vehicle safety to ensure that the increasing share of the risk managed by the vehicle is suitably controlled. Understanding the full impact of this change is not trivial, but we can say with certainty that an increasingly robust approach to safety management from automotive suppliers will be required in the future in order to be ready for the current and future challenges of managing risk.

Safety responsibility shifts from driver to vehicle

Historically, the automotive sector has not been required to follow the same approach as high-hazard industries, such as rail and aviation, as automotive safety responsibility has rested more with the driver than with the vehicle. Over time, however, as electronic systems become essential to the operation of motor vehicles, there has been recognition that appropriate controls for such systems are needed. This is evidenced by the development of standards like the Motor Industry Software Reliability Association (MISRA) C guidelines and, more recently, ISO 26262. As the shift in safety responsibility from driver to vehicle continues, vehicles are now more similar to the safety-critical systems of other high-hazard industries.

Vehicle safety now relies on managing sensor data and the integrity of electronic systems

Driver error is the main cause of road accidents. Human error is involved in 94% of accidents in the US, according to the US Department of Transportation, and suppliers are aware that significant safety benefits are available from the reduction in driver-performed tasks increased automation brings. Managing the required safety transition will create new challenges for both suppliers and regulators.

A safety case approach

A safety case defines and documents a process that summarizes the safety claims that apply to a system, the argument as to why these claims are valid, and the evidence that this argument has been satisfied. The need for a vehicle safety case is documented in ISO 26262, but this standard is not prescriptive in terms of content, which can create uncertainty for suppliers. While not yet as comprehensive as those produced by other high-hazard industries, the safety case in the automotive sector is becoming an increasingly vital part of demonstrating a vehicle's acceptability for use by the public. It plays an important role in demonstrating appropriate safety management to both internal and external stakeholders and is particularly crucial for modern road vehicles, given that they contain a great deal of software and, sometimes, more than 100 electronic control units.

Creating an adequate safety case is as much about fully documenting what is currently being done as it is about adding new processes. The level of documentation needed and the corresponding transparency involved may represent a step change for some parts of the sector, as all processes, whether part of design, safety analysis, verification, or validation, will need to be clearly defined, with evidence available, to show that they have been followed. Other high-hazard sectors like rail have taken time to adapt to such requirements; it is likely the same will be true of automotive.

An approved safety case will become an increasingly vital part of selling a vehicle to the public, but the responsibility for suppliers does not end here. As the use of ADAS increases, through-life vehicle safety management is becoming ever more important. Embedded software changes after a vehicle has been sold (e.g., Tesla's well-known over-the-air updates, which may include potential algorithm changes). This means the safety case continues to evolve through the vehicle's lifetime and needs to be actively managed by the supplier. The implication is that a clear safety case owner is needed within the supplier, through development, the sales cycle, and beyond, to manage evolutions and other issues affecting safety.

Strengthened safety governance and assurance

Safety case ownership will necessitate another change to ensure that the structure, governance, and reporting lines of the supplier enable clear allocations of responsibilities, with separate development and assurance. This is likely to mean having safety representation at the board level supported by a clear allocation of safety responsibility down the management chain, aligning with the signatories of the safety case and other approval documentation. The need for such clear responsibility allocation cannot be overemphasized. Misallocation of such responsibility has been the root cause of many accidents with painful and tragic lessons being learned as a result.

This need is reinforced by the reputational damage arising from ADAS-related incidents. Since the 2018 pedestrian fatality in Arizona (the first recorded case involving an autonomous vehicle), several minor incidents have occurred, resulting in an intense level of media scrutiny far beyond that garnered by similar accidents not involving an automated vehicle. For example, a self-driving car being tested by Google was involved in a collision in 2018, resulting in international news coverage despite the driver only receiving minor injuries. Relatively minor incidents can lead to a disproportionately large amount of reputational damage, and so it is not difficult to imagine the potential significant financial and reputational harm associated with more serious or repeated accidents.

Essential safety information for drivers

A further challenge is that manufacturers will need to provide a mechanism to make drivers fully aware of the safety responsibilities they must fulfill when driving. At present, the situation is relatively straightforward, as drivers retain almost all safety responsibility, but the situation becomes more complicated as safety responsibility splits more evenly between driver and vehicle. Suppliers will need to be extremely clear under what circumstances drivers are expected to intervene (e.g., if an ADAS function fails to maintain safety) and how driver intervention can be managed safely.

This situation presents a challenge as it will not be acceptable to simply state that it is the driver's responsibility to take control under certain circumstances. Drivers will need to be made aware of their specific responsibilities; there must be a practical, acceptable, and legally robust means for such responsibility transfer. Additional driver training may be needed to provide understanding of the capabilities and limits of vehicle functions.

For example, at present drivers must be clearly informed that they remain in control of a vehicle when using ADAS functions (see sidebar below) and that they are responsible for driving safely. This information delivery is currently mainly managed through user manuals, which drivers may neither read nor understand. As more safety responsibility transitions to the vehicle, this approach will not be sufficient.

Integrated sensors

Many autonomous vehicles have integrated sensors within the steering wheel to measure small movements naturally induced by the presence of the driver's hands on the wheel. If the driver does not have his or her hands on the wheel, warnings are repeatedly sent. If the driver does not follow instruction after repeated warnings, the car automatically parks on the side of the road and deactivates autopilot.

Suppliers will need to find other methods of passing on this critical information, such as:

- Clear, timely warnings from the vehicle to the driver when using certain functions.
- Requirement that drivers complete compulsory training when they take ownership of a vehicle.
- Use of individual driver identification to ensure certain warnings have been delivered to specific drivers.
- Inhibition of certain functions until specific acknowledgement that certain information has been understood.

Once vehicles are fully autonomous, there will be less scope for confusion as to whether safety responsibility lies with the vehicle or the driver. However, during the transition period, which may last for several years, this grey area will continue to require detailed attention.

Supply chain management

The automotive supply chain is highly complex – and still evolving as new service delivery patterns emerge, meaning that any individual vehicle integrates components from multiple suppliers, with Tier 1 companies being as much integrators as

manufacturers. For a vehicle as a whole to be shown as safe to operate, each supplier needs to fulfill its responsibilities in terms of risk management. Therefore, the approach used by a Tier 1 supplier must be followed by the entire supply chain. Managing this consistency of approach and ensuring that each member of the supply chain provides consistent evidence that safety responsibilities have been fulfilled will become increasingly challenging as vehicles move toward full automation.

Responsibility will fall on Tier 1 suppliers (as the final system integrators), as many risks will only be manageable at the level of system integration and only the final integrator will be able to assess how best to control certain risks. Therefore, a robust approach to safety management will be essential for Tier 1 suppliers. In this approach, the supplier must:

- Clearly define its safety management systems, which must be comprehensively rolled out and understood.
- Work with the supply chain to ensure that any risk management activity aligns with its own systems. This will require a lengthy and complex process of supplier education and knowledge transfer.

Cybersecurity

A modern vehicle contains multiple interconnected networks, which all present opportunities for cyberattacks (see figure below). The interconnected nature of the networks means any vulnerabilities in any of the vehicle systems (including systems not classified as safety-critical) can result in malicious access to the autonomous driving functions and present a serious safety risk (see sidebar on right).

Thus, suppliers have a duty to ensure that cybersecurity threats do not represent an unreasonable safety risk for their vehicles. They will need to define a clear roadmap of following and implementing best practices, standards, and guidance for cybersecurity management in a timely manner, as practices and the resultant standards evolve within the automotive sector (e.g., ISO/SAE AWI 21434 and SAE-J3061). The safety case should include cybersecurity consideration in order to show that linked safety risks are adequately addressed.

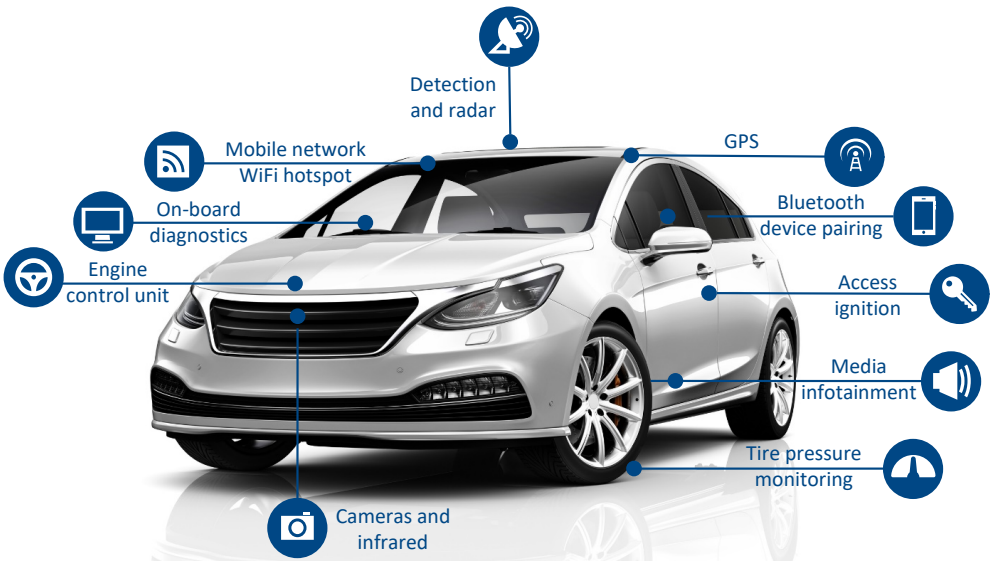
Cybersecurity vulnerabilities

In 2015, the US highways regulator (NHTSA) recalled 1.4 million vehicles owing to cybersecurity vulnerabilities that represented an unreasonable risk to safety. The recall was targeted toward vehicles from Jeep, Dodge, Chrysler, and RAM equipped with radios with software vulnerabilities, which could allow unauthorized third-party access to some networked vehicle control systems.

Regulation

Regulation will evolve as ADAS use increases, continuing an evolution that has been taking place over recent years. It is difficult to predict exactly how regulations will develop, but it is almost certain there will be increased risk control in the future. The best way to prepare for such regulation is to put in place robust risk management, thus providing a level of future-proofing, in addition to providing greater assurance for both suppliers and their customers. By following principles of other safety-critical industries such as rail, car manufacturers can be ready for likely regulation changes.

Vehicle network interactions



Source: Arthur D. Little

Suppliers can also, where possible, work with relevant organizations in the development of regulations and standards which concern the application of artificial intelligence (e.g., ISO/IEC/JTC/SC 42). Many of these standards are still under development and will include risk management.

Conclusion

Increasing vehicle automation is resulting in responsibility for safety shifting from the driver to the vehicle and, by extension, the vehicle manufacturer. As a result, the automotive sector is going through a period of transition with respect to risk management, taking on a more safety-critical role and adapting its safety and risk management processes accordingly. The following key safety management issues for vehicle manufacturers should be addressed:

- A robust approach to safety governance, so all required responsibilities are being appropriately discharged.
- Development of robust safety cases and effective safety management systems, including monitoring and investigating cybersecurity risks.
- Clear definition and documentation of the safety management processes followed.
- Engagement with the supply chain so that safety responsibility is managed consistently at all points.
- Management of the export of safety requirements to the driver or other appropriate party.

Historically, industries and organizations with safety-critical systems that overlooked these approaches have paid for their failure to adapt with loss of life, economic loss, and massive reputational damage. By contrast, early adaptation of the safety management practices we have outlined here will place vehicle manufacturers in a strong position to manage the essential future transitions – as ADAS becomes an increasing part of vehicle control – in the move toward fully autonomous, self-driving vehicles.

Contacts

Austria
virag.bela@adlittle.com

Belgium
vanaudenhove.f@adlittle.com

China
harada.yusuke@adlittle.com

Czech Republic
steif.jiri@adlittle.com

France
bamberger.vincent@adlittle.com

Germany
doemer.fabian@adlittle.com

India
maitra.barnik@adlittle.com

Italy
milanese.stefano@adlittle.com

Japan
ito.yuma@adlittle.com

Korea
lee.kevin@adlittle.com

Latin America
guzman.rodolfo@adlittle.com

Middle East
merhaba.adnan@adlittle.com

The Netherlands
eikelenboom.martijn@adlittle.com

Norway
thurmann-moe.lars@adlittle.com

Poland
baranowski.piotr@adlittle.com

Russian Federation
ovanesov.alexander@adlittle.com

Japan
ito.yuma@adlittle.com

Spain
mira.carlos@adlittle.com

Sweden
kilefors.petter@adlittle.com

Switzerland
doemer.fabian@adlittle.com

Turkey
baban.coskun@adlittle.com

UK
teixeira.tom@adlittle.com

USA
wylie.craig@adlittle.com

Authors

David Boulton, Ben Hansen

Arthur D. Little

Arthur D. Little has been at the forefront of innovation since 1886. We are an acknowledged thought leader in linking strategy, innovation and transformation in technology-intensive and converging industries. We navigate our clients through changing business ecosystems to uncover new growth opportunities. We enable our clients to build innovation capabilities and transform their organizations.

Our consultants have strong practical industry experience combined with excellent knowledge of key trends and dynamics. ADL is present in the most important business centers around the world. We are proud to serve most of the Fortune 1000 companies, in addition to other leading firms and public sector organizations.

For further information please visit **www.adlittle.com** or **www.adl.com**.

www.adl.com/SafetyOnTheMove