# Why Automotive Cybersecurity is Different

## A White Paper outlining how to meet UNECE Regulation 155

The critical lessons for industry

A roadmap to designing and operating cybersecure vehicles

**July 2021**

## About HORIBA MIRA

HORIBA MIRA is a global provider of pioneering engineering consultancy, research, verification and validation services to the automotive, defence, aerospace and rail sectors. We work in close collaboration with vehicle manufacturers and suppliers around the world, providing comprehensive support ranging from individual product tests to turnkey multi-vehicle design, development and build programmes.

With 75 years of experience in developing some of the world's most iconic vehicles, our engineers utilise the latest facilities and simulation tools to make vehicles and journeys safer, cleaner and smarter. Our suite of over 40 major facilities, 100km of specialised proving ground and wealth of engineering experience, combined with our expanding international presence, means we are confident that we can achieve our vision – that every journey in the world will be positively influenced by us.

## About HORIBA MIRA's Vehicle Resilience Team

HORIBA MIRA's Vehicle Resilience (VRES) team is a globally-recognised expert consultancy service made up of over 100 engineers and scientists with an inter-disciplinary focus in cybersecurity, functional safety and electromagnetic resilience. As both independent consultants assisting clients across the automotive supply chain and active contributors to regulatory UNECE, SAE & ISO frameworks, the Vehicle Resilience capability is uniquely placed to provide OEMs, tier suppliers, and government defence and security with solutions to integrate new cybersecurity protocols into engineering workflows for meet these important new requirements.

# 1. Why is Automotive Cybersecurity Important?

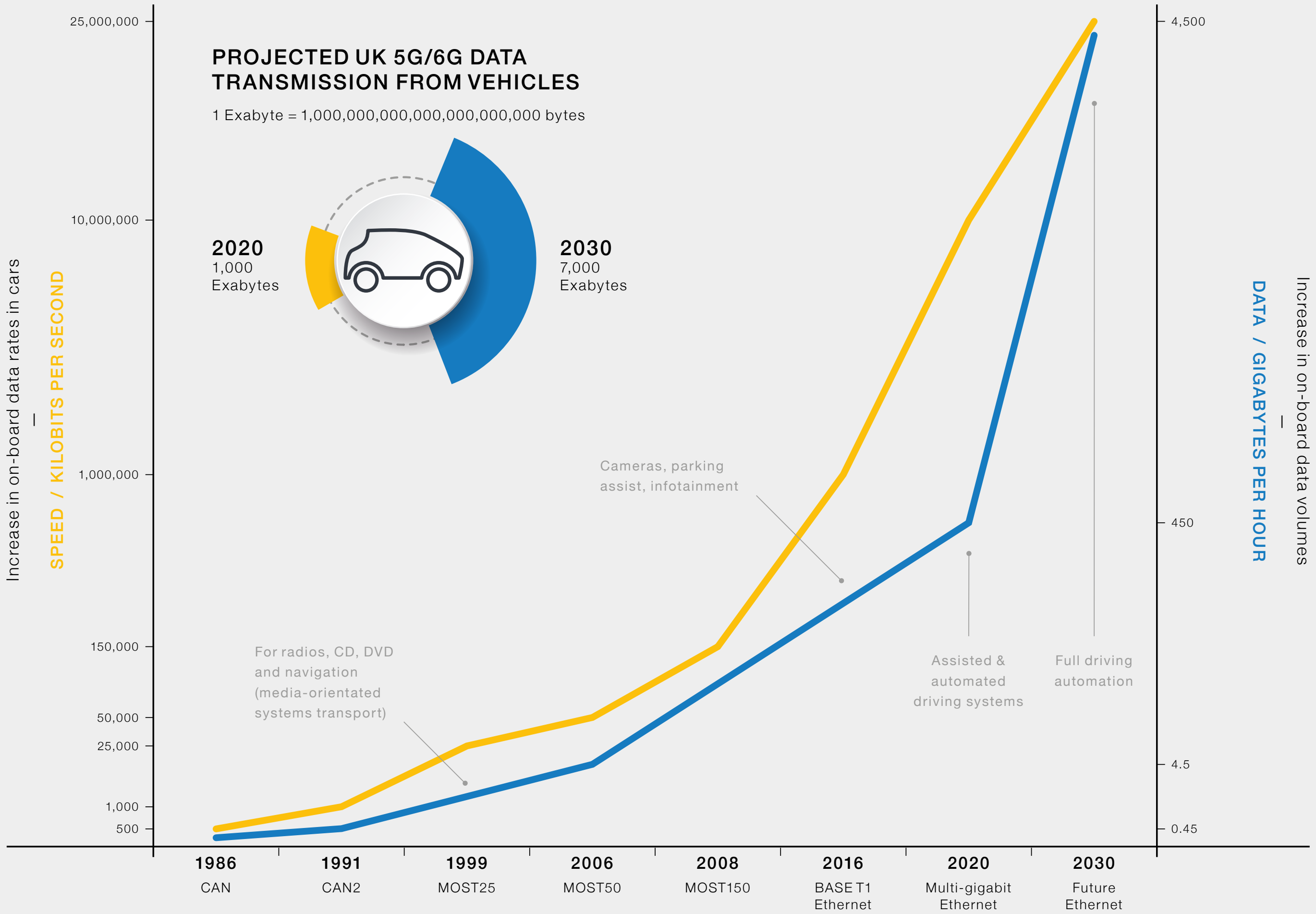
By common consent, the future of road-based transportation will embrace high levels of automation, networked vehicles and intelligent transport systems in order to enhance the safety of road users, minimise pollution and increase the efficiency of travel.

However, the benefits delivered by these smart technologies come at the cost of increased opportunity for cybersecurity attacks against vehicles and the wider mobility ecosystem. While the IT industry has established approaches to contend with cyber threats, these protocols do not directly translate to automotive cybersecurity which presents a wholly different set of considerations.

This white paper outlines the issues for automotive cybersecurity and an approach to developing appropriate solutions for all future mobility stakeholders, including vehicle manufacturers, the tiered supply chain and the myriad public and private organisations contributing to infrastructure, services and regulation of road transport. It is of particular relevance to engineers tasked with the design and operational management of vehicles as the requirements demand a fundamental re-consideration of all aspects of the automotive V-cycle.

> Automotive cybersecurity presents a wholly different set of challenges to established IT cybersecurity protocols

**Figure 1:** Growth in car data rates, volume and transmission



## 1.1 Why is Automotive Cybersecurity Important?

Automotive Cybersecurity is concerned with the preservation of confidentiality, integrity and availability for all data that is received from sensors and communications, processed by systems in the vehicle, or transmitted via actuators and communications to any product, process or service.

Recent automotive industry trends towards increasing connectivity, driving automation, and electrification are leading to cybersecurity concerns as vehicle behaviour is increasingly dependent on internally generated data as well as inputs from sources such as vehicle environment sensors, wireless radiocommunications and the electricity grid.

These interfaces provide opportunities for data manipulation, which allow privacy and financial transactions to be compromised and vehicle behaviour influenced. Integration with personal mobile devices provides further channels for conducting malicious interference.

> Automotive cybersecurity is distinct insofar as it protects against threats to life of drivers, passengers and other road-users

What distinguishes automotive cybersecurity in the most extreme of circumstances is that it protects against threats to the physical safety of the individual, should vehicle operation on the public highway be compromised.

## 1.2 A Growing Need – Why Cybersecurity is a Priority Concern for Automotive Engineering

Influencing factors such as driver utility and safety kick-started the transition of road vehicles from a predominantly mechanical foundation towards integrated electro-mechanical systems at an accelerating rate from the mid-1980s onwards.

However, while on-board data processing was increasing, the vehicle system remained isolated until the advent of low-cost data transmission via cellular communications. Today the exponential advance of vehicle ECUs, increasing use of data-driven on-board processes and the rise of high-speed wireless data transmission has accelerated this transition. Meanwhile, the more recent rise of electric drivetrains is reducing the reliance of vehicles on mechanically complex subsystems such as the internal combustion engine. In short, vehicle content is now skewed in favour of electronic as opposed to mechanical systems. In 1980, according to Deloitte Touche Tohmatsu, electronic systems represented 10% of total vehicle costs. By 2030, it is expected to represent half of the forecourt cost of the average car.

From a cybersecurity perspective, however, this transition to electronic and data-dependent vehicle systems is reflected in more than just cost, with production car models with a complex array of features including ADAS requiring 150 microprocessors that generate in the order of 1TB of data per day of operation. The rate of increase of in-vehicle data volume adheres to a growth projection not dissimilar to Moore's Law, with the number and sophistication of situational sensors for automated vehicles creating a forecast total sensor bandwidth of up to 40Gbit/second, equivalent to 18TB of data processing per hour for smart vehicles coming into production. Not only do the volumes of data present risk, but the processing of raw data into system commands and actions presents opportunities for unsanctioned manipulation.

> 5G/6G will enable terrabytes of vehicle data to be transmitted, presenting new data vulnerabilities

While onboard data processing rapidly scales, 5G/6G connectivity will progressively allow a proportion of these increasing volumes of data to be moved off the vehicle in situations where it provides some utility in being shared. As sensor data rates grow, current estimates for UK vehicle data transmission by 2030 exceed 14,000 Exabytes (where 1EB = $10^{18}$ Byte).

The growth in scope of electronic control functions, the volume of data processed on board vehicles and its propensity to be transmitted from vehicle-to-vehicle or vehicle-to-infrastructure is the backdrop against which the increasing challenge of cybersecurity is evolving.

## 1.3
## Distinguishing Vehicle Cybersecurity from IT Security

With an established tradition in contending with cybersecurity threats in the IT sector, it is tempting to consider that solutions for automotive cybersecurity can simply be transferred from one context to another. But today's increasingly 'smart' cars and their evolving successors, connected and autonomous vehicles (CAVs) cannot be considered as simply computers on wheels.

Today's vehicles are increasingly highly complex cyber-physical systems that respond to and interact with their physical operating environment. To determine their location and assess the state of their surroundings, CAVs combine data from active sensors including radar and LIDAR (Light Detection and Ranging), as well as passive sensors such as cameras and GNSS (Global Navigation Satellite System), together with external data sources provided via communications such as those between vehicles and infrastructure. However, all of these data streams are susceptible to external manipulation for example by jamming, spoofing and tampering attacks.

Consequently, there is a rich source of additional cyber attacks that do not exist in a traditional IT context, such as the manipulation of on-board sensors and external data sources which in turn may falsely modify a CAV's awareness of its surroundings. These attacks are often not amenable to traditional IT responses based on intrusion detection, as no direct interference with on-board systems is required and the vehicle itself cannot readily distinguish between real and spoofed messages or inputs.

The sources of cyber attacks are therefore more wide-ranging in the automotive context, and the liabilities these threats present can also be more extensive.

### Forms of external manipulation of data streams

- Jamming – preventing the legitimate flow of data that supports correct system operation
- Spoofing – disguising a communication from one source as being from another to disrupt proper systems operation
- Tampering – the modification of bona fide code and data to corrupt the proper operation of systems

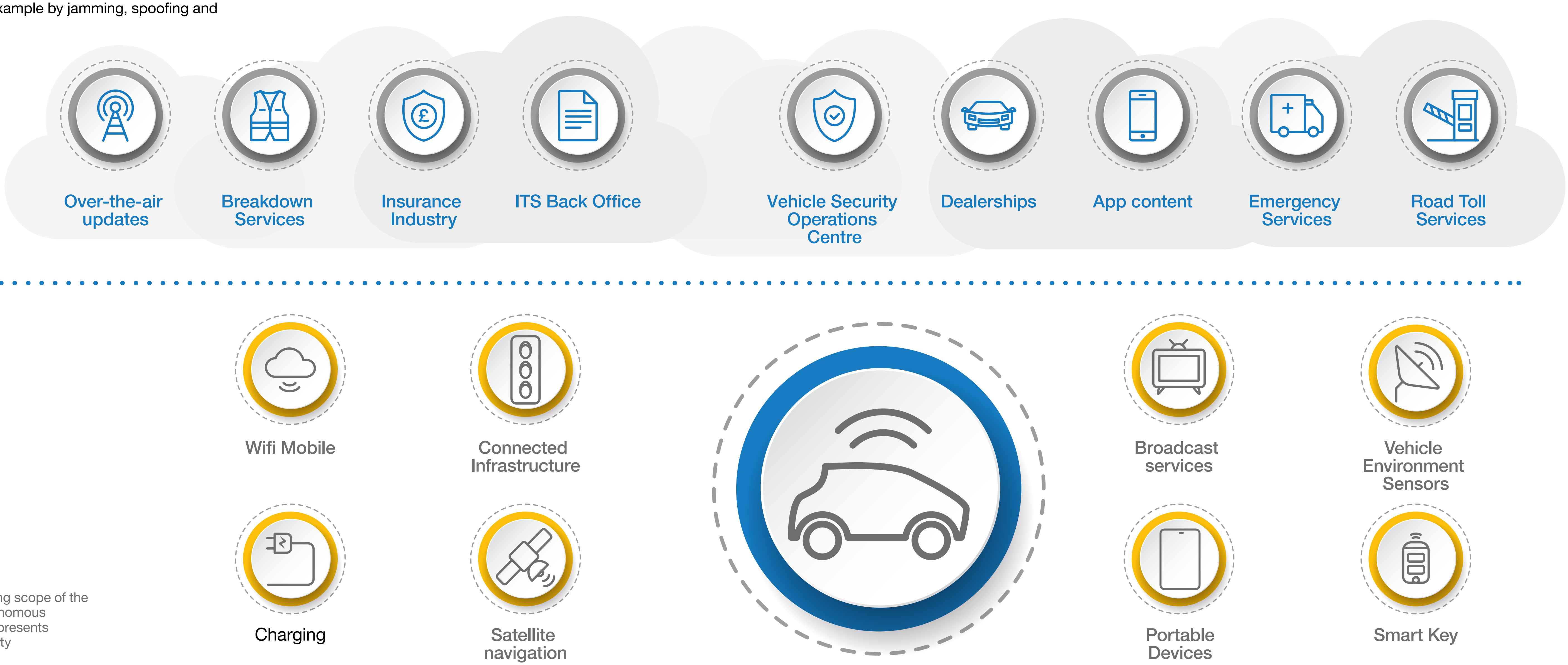


**Figure 2:** The growing scope of the connected and autonomous mobility ecosystem presents increased vulnerability

# 2.
# Automotive Cybersecurity Threats

Data flow and automation will become the lifeblood of future mobility schemes. The ambition of these schemes is to reduce fatalities, congestion and pollution while enhancing the urban economy, improving energy efficiency and sustainability and enriching the passenger experience of integrated and seamless journeys.

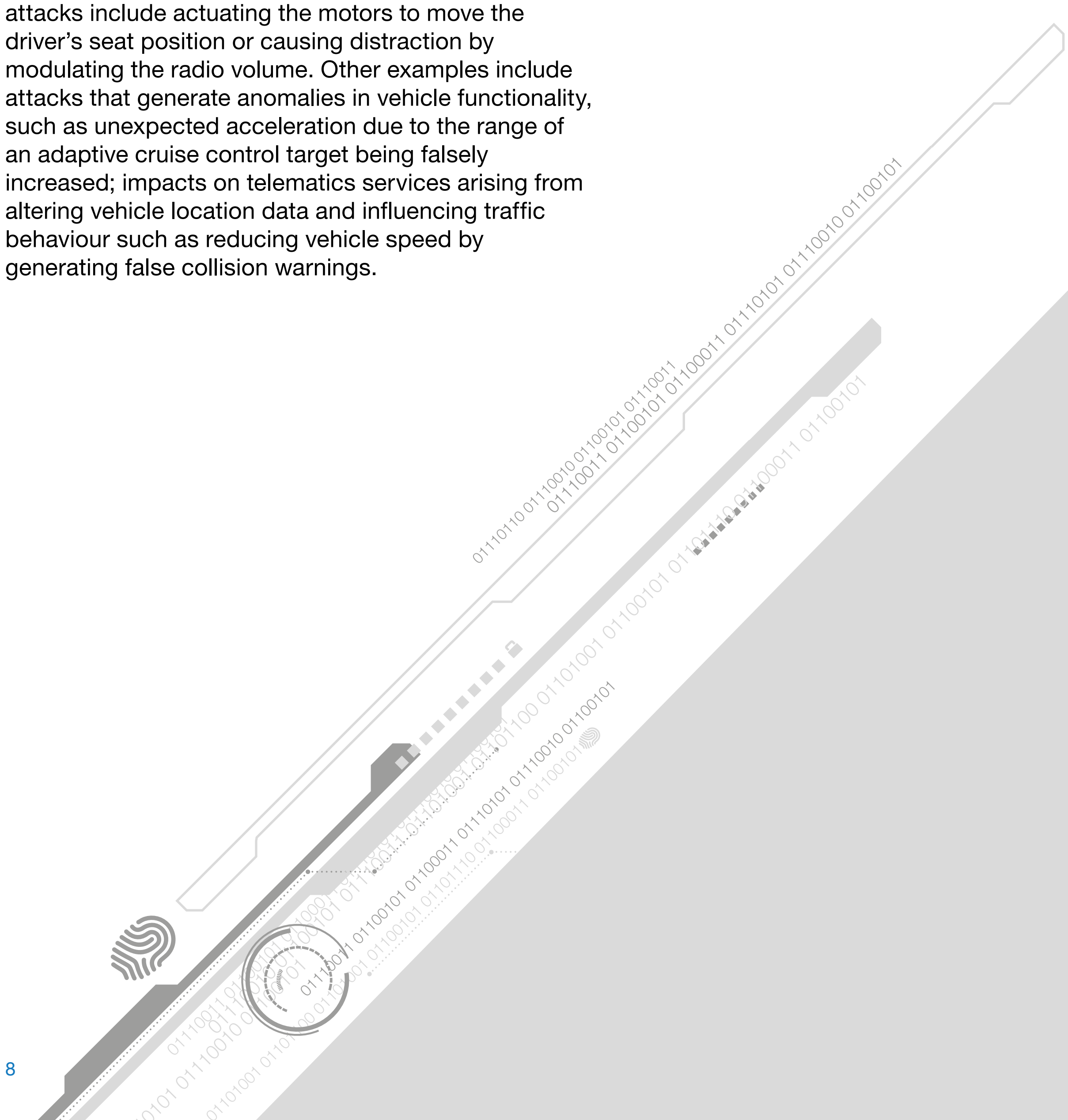
In assessing possible cybersecurity threats, it is necessary to consider the security actors that may be involved, including both the *threat agents*, that is the attackers and their motivations, as well as the *stakeholders*, that is the potential victims and their interests.

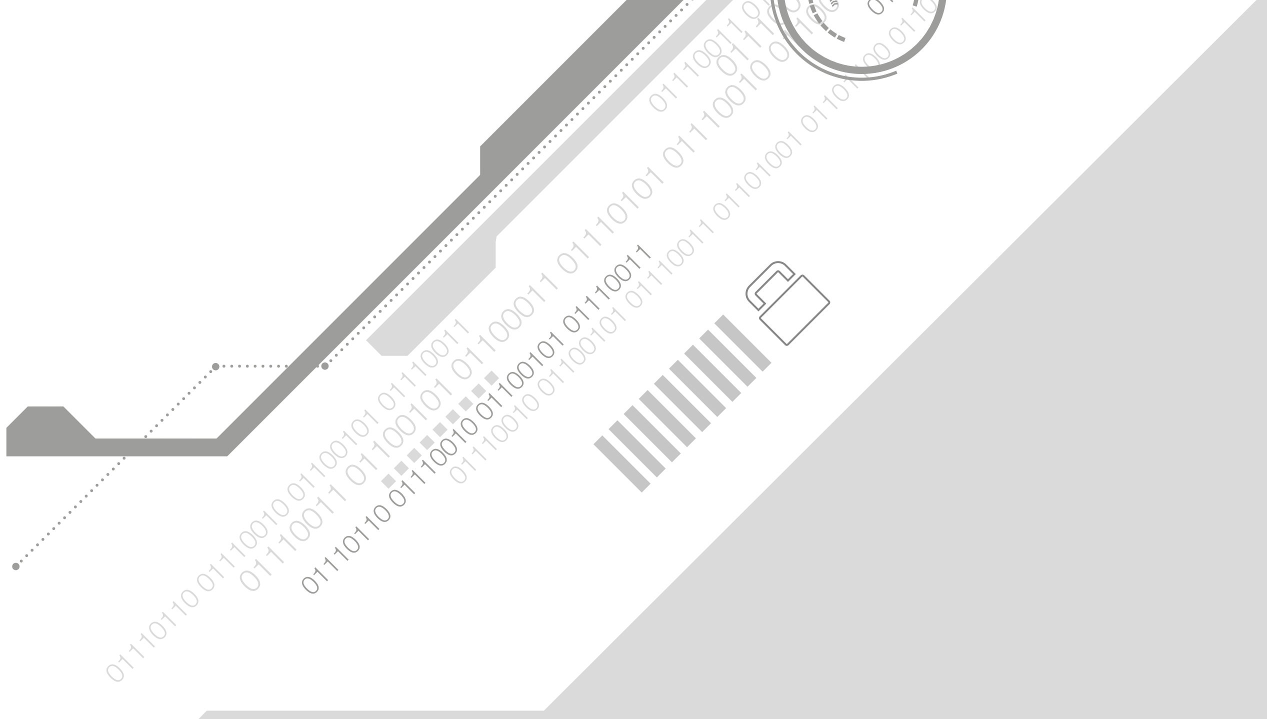
For networked vehicles participating in intelligent transport systems and telematics applications, unauthorised access to personal or vehicle data can be varied. The malicious corruption of data or software could impact critical vehicle control systems, managing primary inputs to throttle, brake or steer. More indirect attacks include actuating the motors to move the driver's seat position or causing distraction by modulating the radio volume. Other examples include attacks that generate anomalies in vehicle functionality, such as unexpected acceleration due to the range of an adaptive cruise control target being falsely increased; impacts on telematics services arising from altering vehicle location data and influencing traffic behaviour such as reducing vehicle speed by generating false collision warnings.

The stakeholders involved in future road transport systems range from road users with a simple need to travel from point to point through to civil authorities responsible for ensuring efficient traffic flow.

Potential threat agents range from dishonest drivers seeking personal advantage through to *rogue states* aiming to achieve large scale disruption or harm to other societies as well as curious hobbyists in pursuit of the challenge. Consequently, the financial and technical resources available to different categories of threat agents to mount cybersecurity attacks will vary significantly.

The cybersecurity of vehicle systems, data and associated communications are therefore of increasing importance to a very wide range of stakeholders involved with the mobility ecosystems that are now emerging.





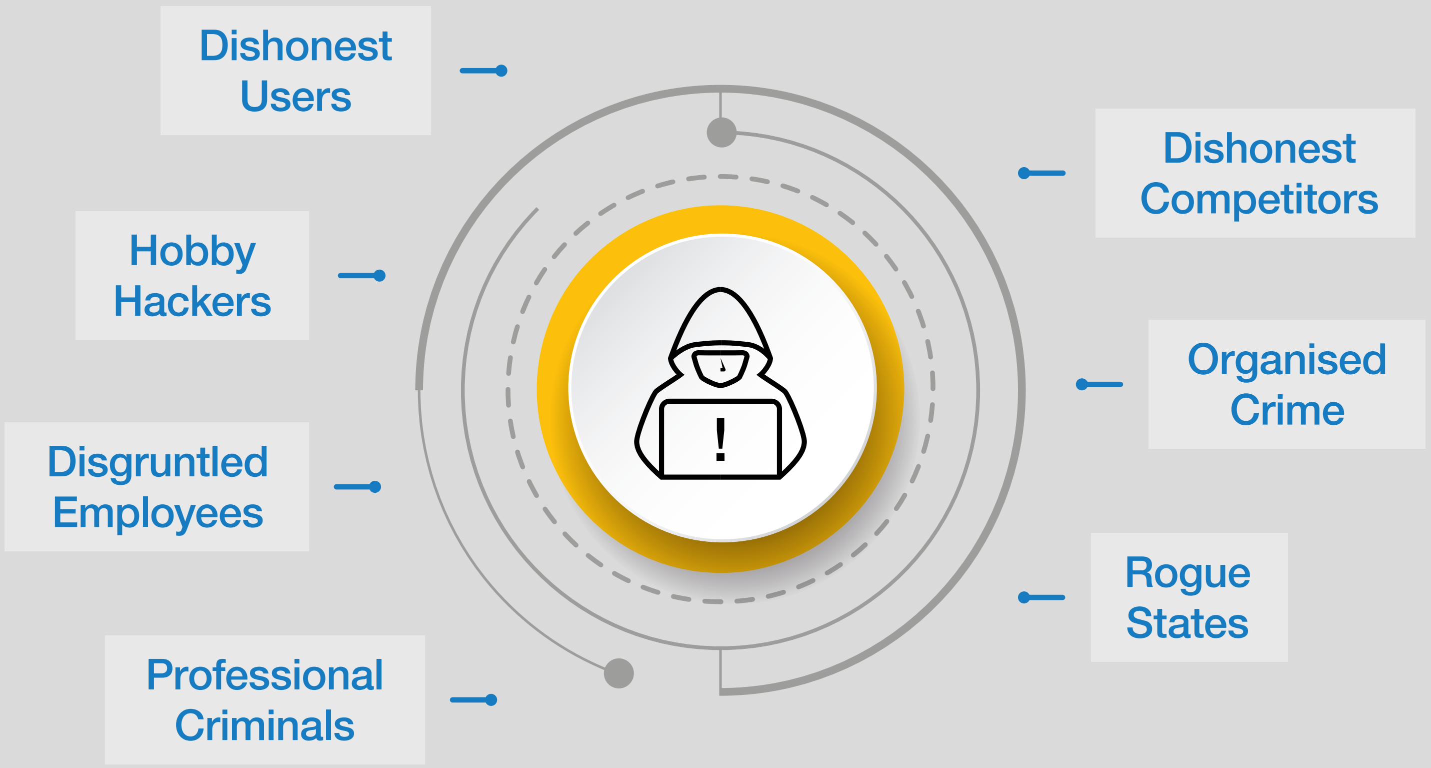


**Figure 3:** Different categories of threat agent

## 3.
## Emerging Cybersecurity Regulations & Standards

To contend with both the identified growth in data-dependency in next-generation mobility and the continuous evolution of the threat landscape, a number of important new automotive cybersecurity standards and regulations are emerging, including process and technical standards either recently published or approaching publication. At present, the most significant of these are:

ISO/SAE 21434, due to be published in 2021 - expected to be the state-of-the-art reference for automotive cybersecurity engineering

UN Regulation 155 took effect in January 2021 - specifying regulatory requirements for cybersecurity

**The UN regulation requires:**

- A mandatory audit of a vehicle manufacturer's cybersecurity management system
- An assessment against the cybersecurity requirements for vehicle types to be carried out by a type approval authority or technical service and must be in place before vehicle manufacturers can gain type approval for all new vehicles from 2022

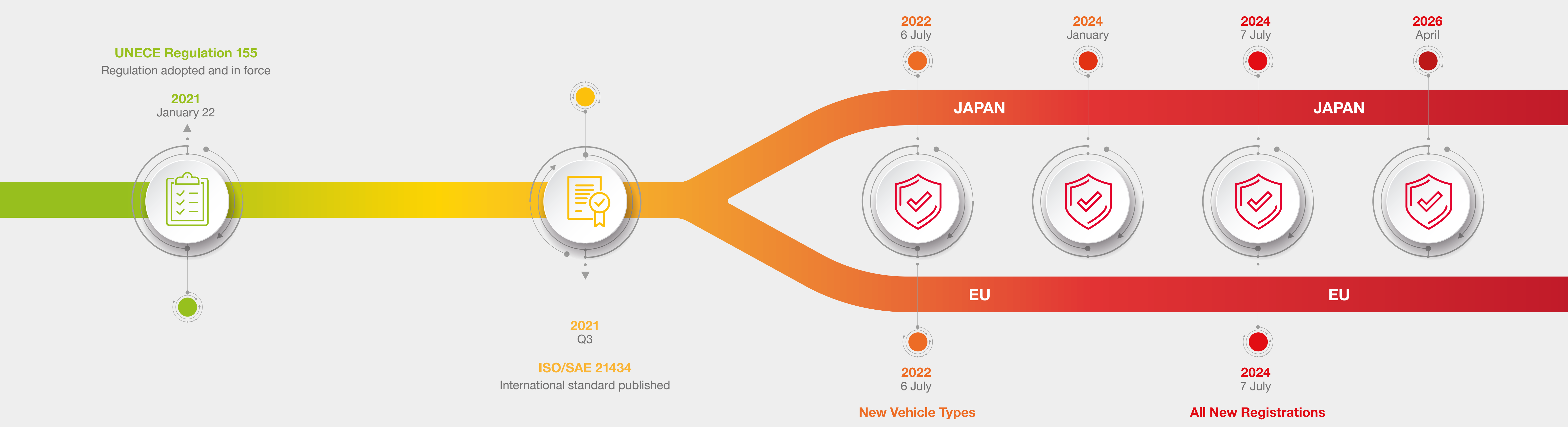
HORIBA MIRA's Vehicle Resilience engineers are active participants in the development of key automotive cybersecurity standards and regulations, such as SAE J3061 [1], ISO/SAE 21434 and the new UNECE regulations.

From this close involvement in the framing and drafting process, our engineers have a unique insight into the intent behind the requirements, how they were formulated and how they can be implemented in practice.

This regulatory experience, HORIBA MIRA's depth of automotive sector know-how and its independent status, makes the organisation uniquely well-placed to assist clients in navigating new cybersecurity regulations and standards.

Published in March 2021, HORIBA MIRA's Vehicle Resilience and Cybersecurity experts released a white paper entitled How to Navigate New Cybersecurity Type Approvals - Critical industry insight to keep your business trading. For more information concerning emerging cybersecurity regulations and specifically UN Regulation 155, refer to this free report available on the HORIBA MIRA website.

**Figure 4:** A timeline outlining the adoption of Regulation 155 by national Type Approval authorities



# 4. How Can Automotive Cybersecurity be Best Implemented?

It is important to recognise that it is impracticable to identify all possible threats and vulnerabilities, and therefore impossible to eliminate all cybersecurity risks. Cybersecurity is a constantly evolving problem, which tracks the vulnerabilities emerging from developing technologies and is driven by human ingenuity.

This does not mean that the automotive industry is powerless to mitigate potential threats. Failing to plan for the growth in cybersecurity considerations is planning to fail as the exposure to threats increases, the duty of care to customers grows and the potential to suffer significant damage to corporate reputation takes on a significant new dimension.

However, in order to contend with the continuous and evolving nature of threat potential, HORIBA MIRA have developed a dual approach that combines two key considerations. The first consideration is *proactive security-aware design* in order to reduce the risks associated with foreseeable threats to the mobility ecosystem to acceptable levels. The second consideration is *reactive operational responses*, providing ongoing monitoring and the delivery of validated updates that enable timely responses to the emerging threats.

> Implementation require both proactive security-aware design and reactive operational response

This balanced and pragmatic approach aims to avoid under-engineering of vehicles by pre-empting foreseeable attacks that could otherwise lead to serious harm or damage and negatively impact brand reputation. At the same time, this dual approach aims to avoid the potential for over-engineering vehicles which impacts marketability due to overly restrictive cybersecurity measures and inflated retail prices.

To achieve resilience, it is essential to consider not only the intended functionality and use cases of the complete mobility ecosystem, but also a range of other use contexts, including unintended use and deliberate misuse.

The first of these use contexts is that of *reasonably foreseeable* use premised on anecdotal experience or predictable driver behaviour, such as driving a road vehicle off road in a field, driving through fords or flooded road sections or using cruise control on winding roads, steep hills or in icy conditions.

The next category is that of *reasonably foreseeable intentional misuse*, for instance the recording and replay of keyless entry transmissions to facilitate theft, the broadcast of false vehicle to infrastructure messages to disrupt traffic flow, spoofing or jamming GPS to disguise or hide vehicle location or dazzling vehicle cameras using laser pens.

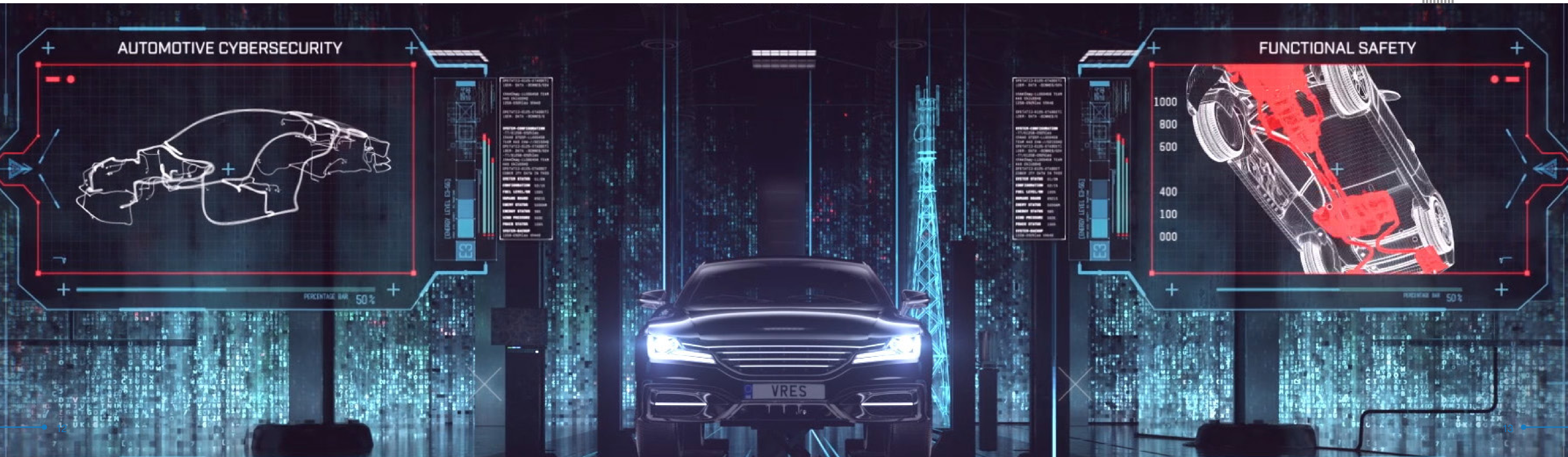
*Unintended functionality* contexts relate to actions that are possible but not desirable, for example the operation of rear-seat entertainment system via infra-red remote control from beyond the cabin of a vehicle.

When the location of a kangaroo was misunderstood by an OEM animal detection system because it jumped rather than moving with its feet in contact with the ground, this might be considered *missing functionality* – or in other words, a required functionality but one not considered or implemented.

The final two contexts relate to *unforeseeable unintended* use and *intentional misuse.* In the first of these contexts, a plug-in vehicle monitoring device was designed with GPS capability to allow breakdown patrol vehicles to locate stricken motorists. But the technology had a variety of unintended applications ranging from helping police to find stolen vehicles to use in insurance fraud prevention and timestamping staff arriving and departing their places of work.

An illustration of intentional misuse is the demonstration by security researchers of how vulnerabilities in the internet-connected entertainment system in the Jeep Cherokee could be exploited to take control of the vehicle.

All of these situations present use-cases that extend beyond the design intent of the vehicle, not all of which will be foreseeable during development. Automotive cybersecurity engineering must therefore be an ongoing process that remains active throughout the operational lifespan of the vehicle.



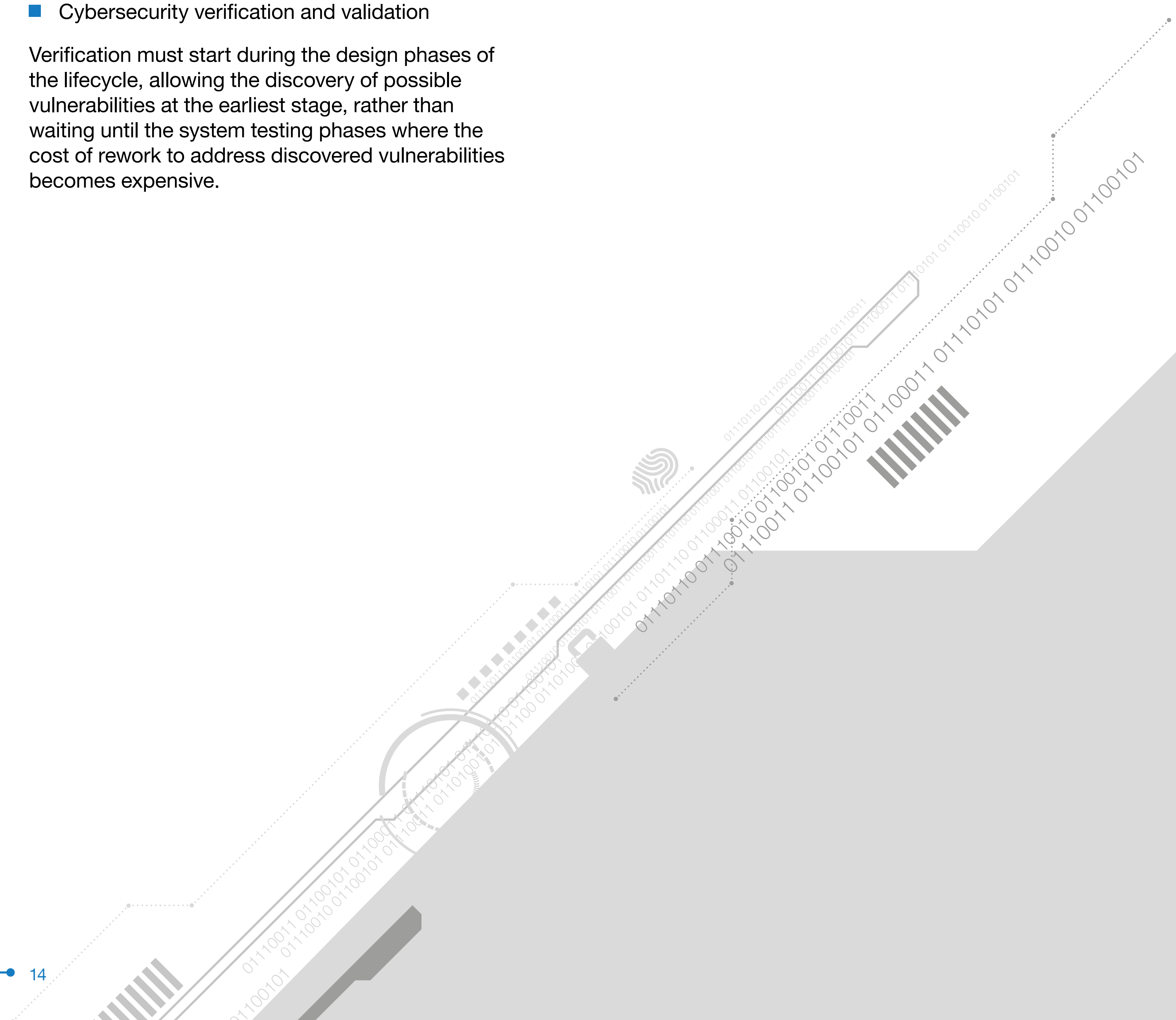
## 4.1
## Proactive security-aware design

A significant difficulty for cybersecurity engineering is that the environment and its threats are constantly evolving. Nonetheless, it is prudent to take a snapshot of risks during the development window and aim to ensure they are assessed, and where necessary, reduced to acceptable levels.

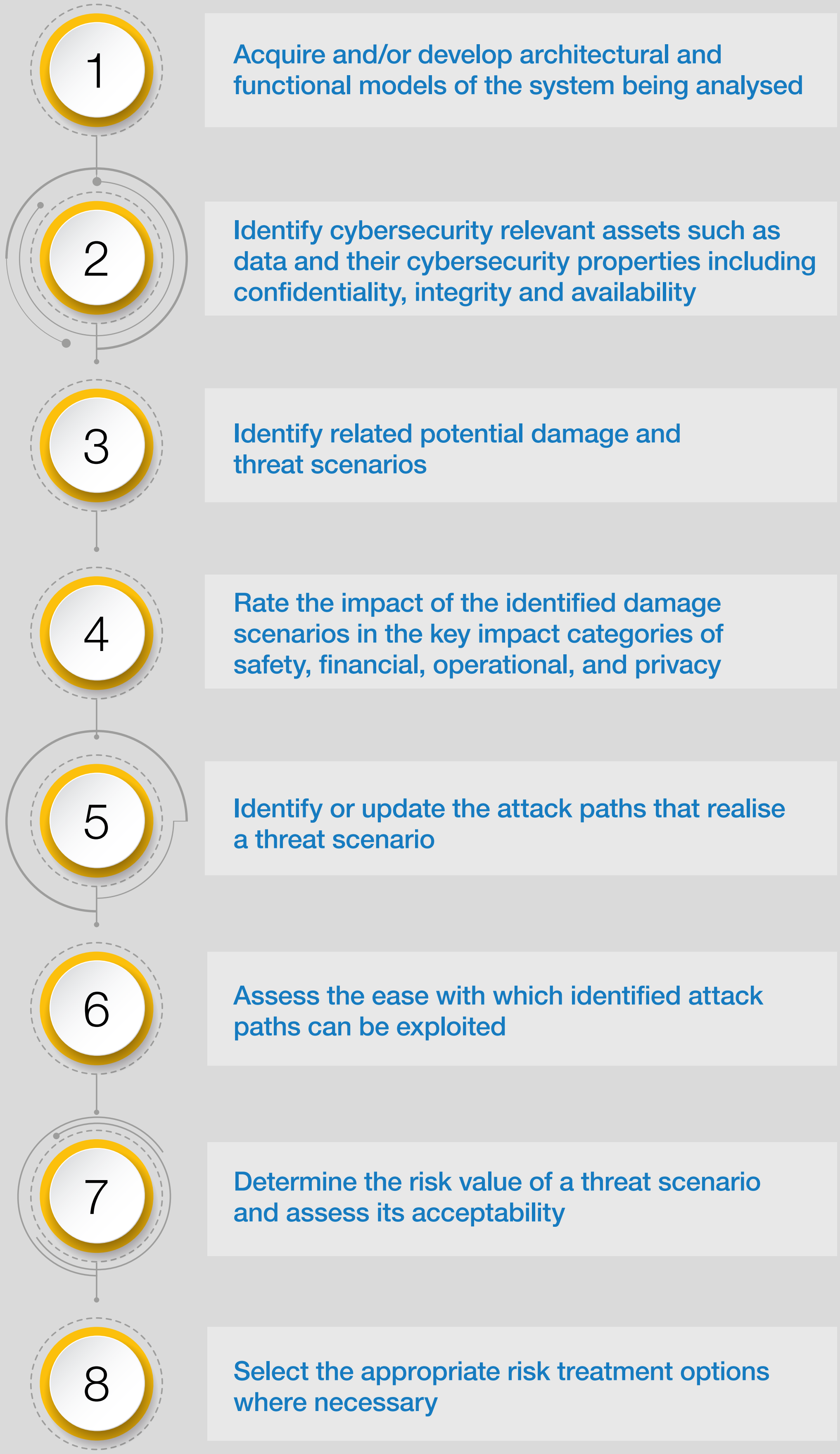
HORIBA MIRA's state-of-the-art proactive cybersecurity engineering involves a range of analysis and requirements management activities during the design phase based on a risk-based systems engineering approach, including:-

- Threat analysis and risk assessment
- Cybersecurity concept development and elicitation of cybersecurity requirements
- Specification, design and implementation of cybersecurity controls
- Cybersecurity design verification
- Cybersecurity verification and validation

Verification must start during the design phases of the lifecycle, allowing the discovery of possible vulnerabilities at the earliest stage, rather than waiting until the system testing phases where the cost of rework to address discovered vulnerabilities becomes expensive.



## Threat analysis and risk assessment for cybersecurity includes the following tasks:



1. Acquire and/or develop architectural and functional models of the system being analysed
2. Identify cybersecurity relevant assets such as data and their cybersecurity properties including confidentiality, integrity and availability
3. Identify related potential damage and threat scenarios
4. Rate the impact of the identified damage scenarios in the key impact categories of safety, financial, operational, and privacy
5. Identify or update the attack paths that realise a threat scenario
6. Assess the ease with which identified attack paths can be exploited
7. Determine the risk value of a threat scenario and assess its acceptability
8. Select the appropriate risk treatment options where necessary

**Figure 5:** Threat analysis and risk assessment for cybersecurity

## 4.2 Reactive operational response

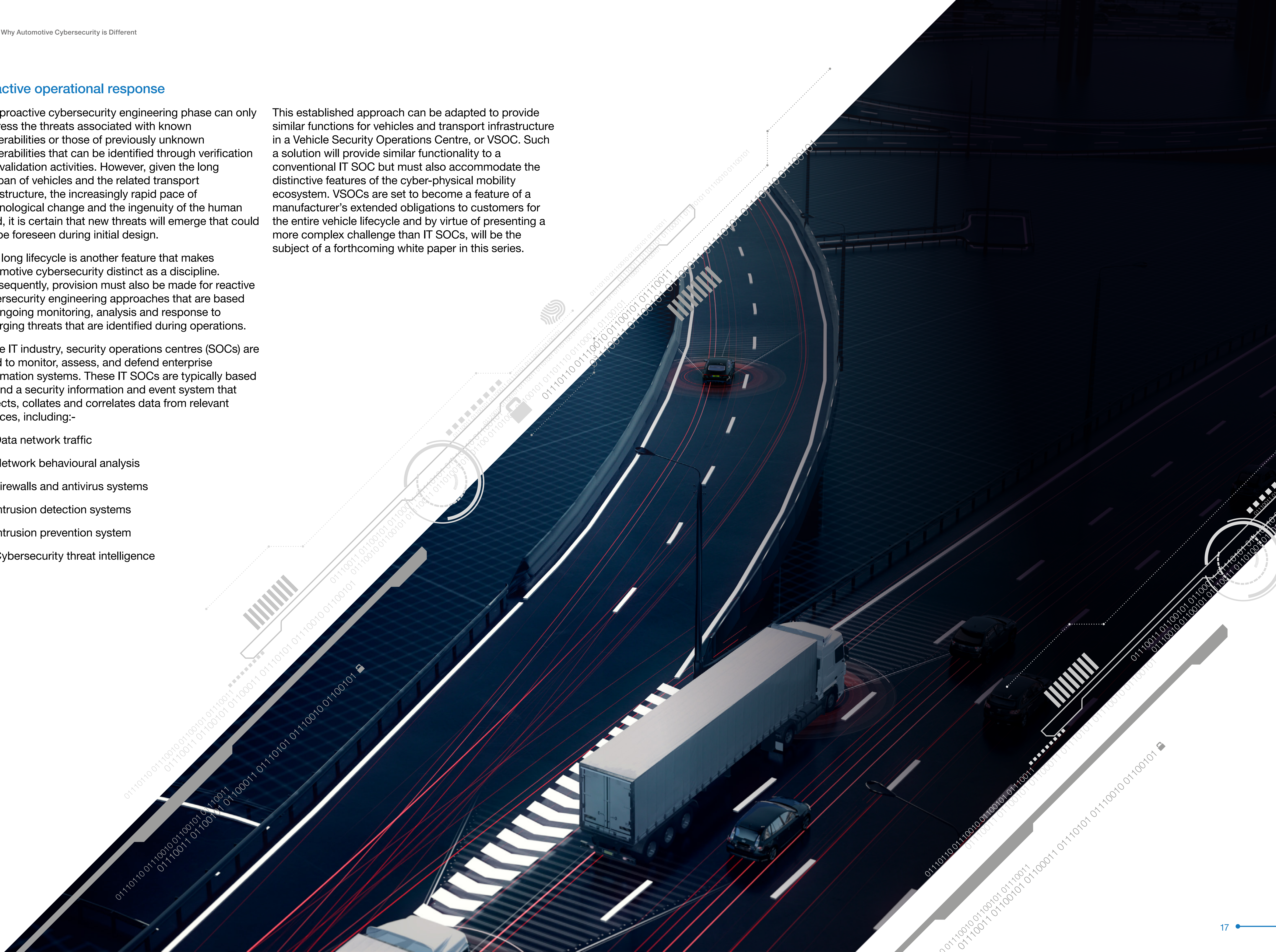
The proactive cybersecurity engineering phase can only address the threats associated with known vulnerabilities or those of previously unknown vulnerabilities that can be identified through verification and validation activities. However, given the long lifespan of vehicles and the related transport infrastructure, the increasingly rapid pace of technological change and the ingenuity of the human mind, it is certain that new threats will emerge that could not be foreseen during initial design.

This long lifecycle is another feature that makes automotive cybersecurity distinct as a discipline. Consequently, provision must also be made for reactive cybersecurity engineering approaches that are based on ongoing monitoring, analysis and response to emerging threats that are identified during operations.

In the IT industry, security operations centres (SOCs) are used to monitor, assess, and defend enterprise information systems. These IT SOCs are typically based around a security information and event system that collects, collates and correlates data from relevant sources, including:-

- Data network traffic
- Network behavioural analysis
- Firewalls and antivirus systems
- Intrusion detection systems
- Intrusion prevention system
- Cybersecurity threat intelligence

This established approach can be adapted to provide similar functions for vehicles and transport infrastructure in a Vehicle Security Operations Centre, or VSOC. Such a solution will provide similar functionality to a conventional IT SOC but must also accommodate the distinctive features of the cyber-physical mobility ecosystem. VSOCs are set to become a feature of a manufacturer's extended obligations to customers for the entire vehicle lifecycle and by virtue of presenting a more complex challenge than IT SOCs, will be the subject of a forthcoming white paper in this series.



# 5. Cybersecurity Testing

Testing products and services at all lifecycle phases and by all organisations within the CAV and mobility ecosystem enables verification of the cybersecurity of each individual element and also helps provide assurance that no additional vulnerabilities are introduced during integration.

Cybersecurity testing is required at all critical phases including hardware and software development, systems integration and vehicle integration.

Vulnerability analysis must continue throughout the operational phase of the vehicle's lifecycle to identify and analyse emerging events and their impact on the vehicle and the wider system to which it is connected.

Therefore additional activities are undertaken to capture cybersecurity-relevant information during field monitoring to identify new vulnerabilities as part of the overall process.

## 5.1 Pre-testing Analysis

Prior to practical testing, threat modelling and security-focussed reviews are carried out, including security design reviews, static code analysis, source code reviews and hardware schematic reviews. This helps to identify any vulnerabilities that are specific to a particular design, implementation or integration at an early stage.

These activities play an important part in identifying potential vulnerabilities requiring further investigation to assess their exploitability using a combination of the following practical testing methods.

## 5.2 Functional Testing

This involves testing whether the implementation produces the correct functional behaviour under a valid set of inputs defined by the specification, for example the correct result of a cryptographic computation. Usually functional testing is restricted to the specified operating range and answers the question *does the implementation deliver the intended functionality?*

As well as verifying correct response to intended inputs, it is critical to test that the target behaves correctly for out of specification or malformed inputs, for example input data of incorrect length or out of the specified bounds. This is typically achieved by dynamic analysis methods such as fuzzing, which generates random or directed sets of test input data designed to exercise the system near the boundaries of its specification.

## 5.3 Correctness testing

Cybersecurity-relevant functions often contain countermeasures against attacks whose correct operation is not observable through the function outputs or the interfaces of the system. Correctness testing is therefore used to verify that the internal behaviour of the implementation is as expected.

This activity requires alternative methods to functional testing and is usually carried out using white box techniques and development tools such as debuggers, simulators or emulators.

Correctness testing can be carried out in the same phase as functional testing, although some tests may be better executed during the design phase, particularly if internal behaviour needs to be monitored using an emulator.

## 5.4 Penetration Testing

Even extensive systematic testing is not sufficient to test whether an implementation is able to resist relevant attacks.

Penetration testing is used to determine this by simulating the actions of a real attacker and therefore requires sufficient time and resource to adaptively follow interesting leads as they are uncovered.

It is also necessary to test for the presence of other vulnerabilities, for example due to additional functionality outside the specification or due to physical characteristics of the device such as side channel information leakage or susceptibility to fault injection attacks.

Penetration testing typically involves multi-disciplinary skills such as software, electronics, RF and cryptography. These skills may need to be brought in from different parts of an organisation or from third parties under relevant non-disclosure agreements.

Carrying out penetration tests for all possible attacks is impractical, so a programme of directed tests must be planned based on the findings of earlier activities.

# 6. How can Cybersecurity Assurance be Achieved?

Operational readiness is the objective for the level of assurance that should be available before a vehicle is released for sale. Operational readiness can be defined as justifiable grounds for confidence that reasonably foreseeable threats have been considered in the design and development phases, such that the cybersecurity risks of using the product, process or service are acceptable to the stakeholders.

The need for ongoing monitoring of possible cybersecurity attacks and mitigation of the associated risks suggest the corresponding need for a new kind of assurance activity that extends over the full operational lifecycle – or operational assurance, which can be defined as justifiable grounds for confidence that the risks of continuing to use a product, process or service remain acceptable to the stakeholders throughout its life.

Operational assurance is a dynamic activity, unlike the situation with product safety, where assurance is largely a static activity at product launch, although occasional recalls for remedial action may occur if any previously unidentified safety hazards come to light.

For cybersecurity, however, an ongoing programme of monitoring and reactive mitigation will be essential to maintain confidence that the associated risks are being maintained at a level that is acceptable to the stakeholders.

### Key Considerations

A dual proactive and reactive approach to cybersecurity is a well-established paradigm in traditional IT contexts. But adopting this approach in automotive contexts marks a step change for the industry.

The mere possibility of malfeasance that presents a physical threat and risk to life by taking remote control of a moving vehicle means that the automotive context is different and requires a more comprehensive holistic approach; moreover, vehicles, as systems that are reliant on sensor-generated situational data, also require a differentiated approach as jamming or spoofing of these external inputs can be used to disrupt behaviour without interfering with vehicle IT systems

Despite these considerations, it is also essential to note that complete indemnity from cybersecurity risk cannot be achieved, rather risk can be managed to an acceptable level.

## 7. HORIBA MIRA Services

HORIBA MIRA offers automotive clients an end-to-end portfolio of cybersecurity services to navigate the required changes throughout the vehicle lifecycle.

HORIBA MIRA has been developing and delivering automotive cybersecurity solutions since 2008, commencing with the EU-led EVITA collaborative research project that provided an automotive cybersecurity threat analysis and risk assessment method which remains in widespread use today.

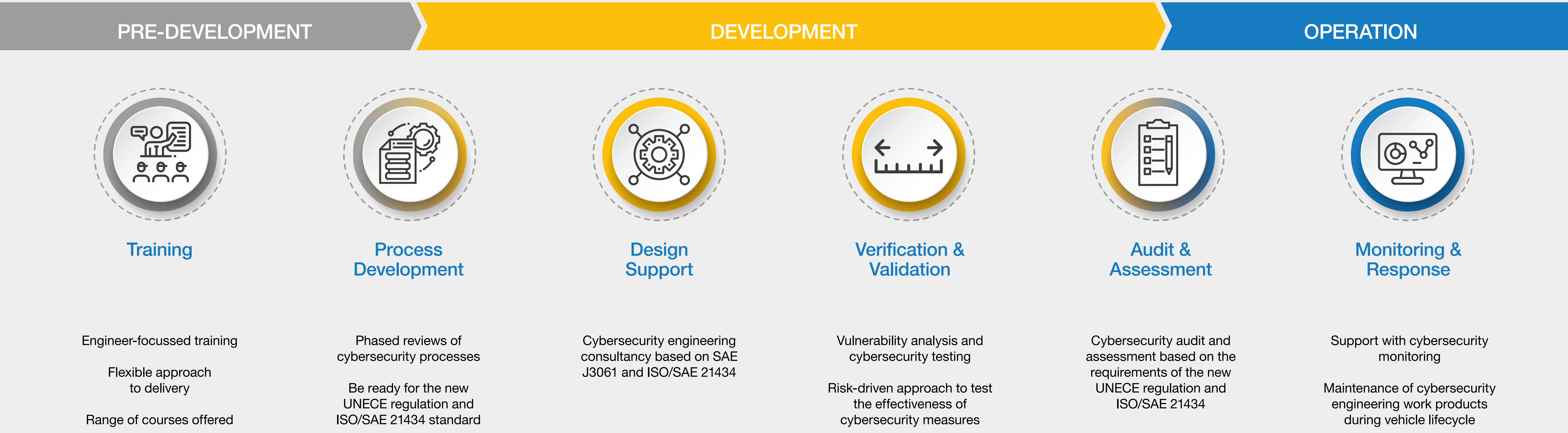
For more than a decade, HORIBA MIRA has been at the forefront of proprietary as well as collaborative cybersecurity projects including UK CITE, 5StarS and ResiCAV that provided enhanced cybersecurity risk management, assurance and operational frameworks for vehicles and smart mobility.

As well as developing class-leading knowledge and expertise in applied cybersecurity in addition to its research work, HORIBA MIRA has been an active contributor to the development of key automotive cybersecurity standards and regulations, such as SAE J3061, ISO/SAE 21434 and the new UNECE regulations.

From this close involvement in the framing and drafting process and the development of cybersecurity solutions, our engineers have a unique insight into security-aware design and the demands of reactive cybersecurity operational responses. This experience and our depth of automotive sector know-how, our testbed ecosystem for verification and validation from lab to road and our independent status make us uniquely placed to assist clients navigating new cybersecurity considerations.

HORIBA MIRA's specialist Vehicle Resilience Team enable your engineering teams to develop a robust design and operations solution to contend with the new cybersecurity context. Book a no-obligation initial consultation by contacting Nick Tebbutt, Head of Global Strategic Sales, Vehicle Technologies.

**Figure 6:** HORIBA MIRA cybersecurity services



PRE-DEVELOPMENT

DEVELOPMENT

OPERATION

**Training**

Engineer-focussed training

Flexible approach to delivery

Range of courses offered

**Process Development**

Phased reviews of cybersecurity processes

Be ready for the new UNECE regulation and ISO/SAE 21434 standard

**Design Support**

Cybersecurity engineering consultancy based on SAE J3061 and ISO/SAE 21434

**Verification & Validation**

Vulnerability analysis and cybersecurity testing

Risk-driven approach to test the effectiveness of cybersecurity measures

**Audit & Assessment**

Cybersecurity audit and assessment based on the requirements of the new UNECE regulation and ISO/SAE 21434

**Monitoring & Response**

Support with cybersecurity monitoring

Maintenance of cybersecurity engineering work products during vehicle lifecycle

# HORIBA MIRA

Improving lives by making journeys safer, cleaner and smarter.

**HORIBA MIRA Ltd.**
Watling Street, Nuneaton,
Warwickshire, CV10 0TU, UK

**+44 (0)24 7635 5000**
**www.vehicle-resilience.com**

MIRA
A HORIBA COMPANY