How to **Navigate New Cybersecurity Type Approvals**

A White Paper outlining how to meet UNECE Regulation 155

Critical industry insight to keep your business trading - from Europe's leading automotive engineering consultancy
March 2021

MIRA
A HORIBA COMPANY

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 to meet these important new requirements.

1. Action Needed to Meet New Type Approval Regulations

In January 2021, a set of three new regulations from the United Nations Economic Commission for Europe's World Forum for Harmonization of Vehicle Regulations came into force. The intent behind these new regulations is to ensure the Type Approval process accounts for the rapidly advancing automated, digital and software-based subsystems now common to most vehicles.

Vehicle Type Approval will therefore be contingent upon meeting these new regulations at the point at which they are adopted into national legislation. Compliance is therefore commercially critical, not just for original equipment manufacturers, but for all businesses supporting the automotive supply chain.

Three New UNECE Regulations

Regulation 155
Cybersecurity

Regulation 156
Software Updates

Regulation 157
Automated Lane Keeping Systems

This white paper is concerned with Regulation 155 and addresses the cybersecurity requirements that will become integral to future Type Approvals. The primary implications for the industry are fourfold:-

- Manufacturers will have to implement an independently-audited cybersecurity management system, or CSMS, for vehicles to gain Type Approval
- The manufacturer's ownership of the CSMS will apply for the entire vehicle lifecycle and is not solely applicable at the date of sale which introduces a need for in-field monitoring and issue resolution
- Manufacturers will have to demonstrate that new vehicles have been developed in accordance with the CSMS and fulfil a set of cybersecurity requirements
- The Type Approval obligations rest with the vehicle manufacturer but will extend across the entire automotive supply chain to include tier suppliers who contribute to OEMs

Read Me in 5

1.
New cybersecurity obligations are mandatory to secure UNECE Type Approval

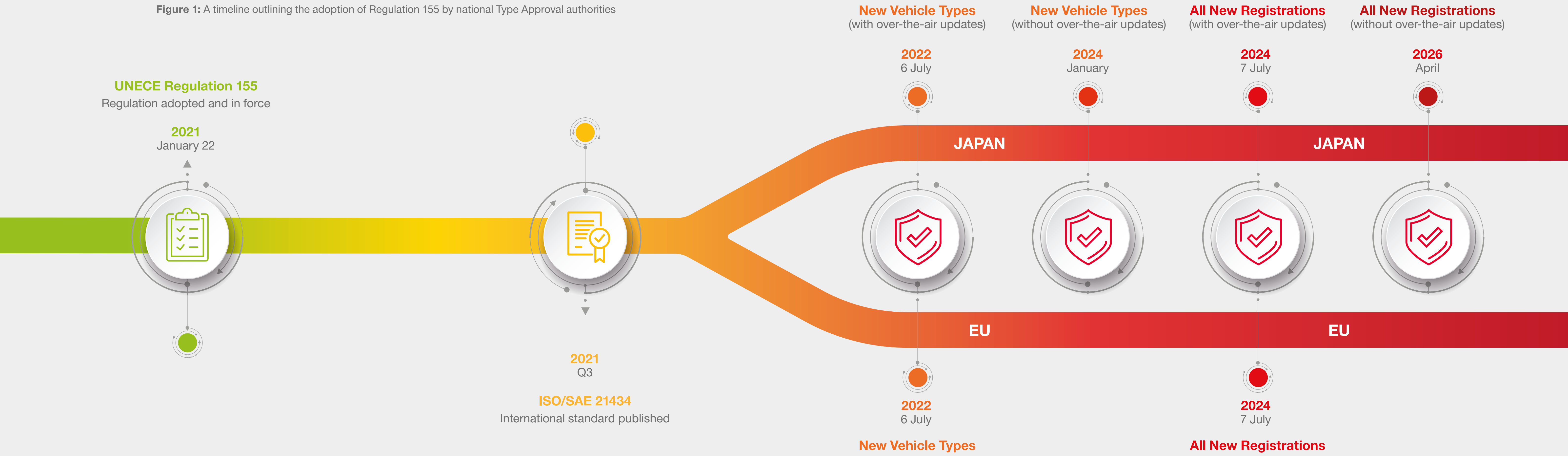
2.
Responsibility lies with the OEM, but businesses across the supply chain must prepare

3.
Non-compliance will prevent vehicles being sold in markets requiring Type Approvals

4.
Timelines for adoption are short, with the new regulation applying from the end of 2020 in some geographies

5.
HORIBA MIRA engineers have contributed to regulation framing and drafting and therefore have unmatched domain expertise to help clients prepare

Figure 1: A timeline outlining the adoption of Regulation 155 by national Type Approval authorities



2.
Understanding the Regulatory Framework

The UN's World Forum for the Harmonization of Vehicle Regulations (otherwise known as WP.29) is a permanent working party within the institutional framework of the United Nations dedicated to harmonising vehicle regulations. 57 contracting parties, representing principal vehicle manufacturing and importing markets, are signatories to the UNECE 1958 Agreement, under which the new Regulation 155 entered into force on 22 January 2021.

Regulation 155 sets out requirements for vehicle manufacturers to establish and maintain a vehicle CSMS that delivers all of the requirements specified in Figure 3 and, additionally, to require independent audits of the CSMS; however, as a goal-based framework, Regulation 155 is not prescriptive and does not stipulate the process by which vehicle manufacturers must achieve compliance with the regulation to meet the relevant national Type Approval requirements.

Useful reference for Regulation 155 is being provided by the development of an international standard that is work-in-progress under the auspices of the ISO & SAE. ISO/SAE 21434 is due to be published in mid-2021 and is already available in draft form.

In addition to the creation of a new standard that provides one reference pathway for meeting the requirements of Regulation 155, there is also guidance pending on standards for the auditing element of the regulation.

Implementation of Regulation 155 in national jurisdictions is the final stage of the process and the point at which the cybersecurity considerations will be binding in the type approval process. Several markets have announced timelines for implementing the regulation. Japan will be one of the early adopters, with requirements forming part of national regulations already in place from late 2020. The EU is scheduled to implement the regulation for new vehicle model type approvals from July 2022, extending to cover all vehicle registrations by July 2024.

HORIBA MIRA's Vehicle Resilience engineers are active participants in the development of these new UNECE regulations and ISO/SAE standards, working in tandem with OEMs, the tiered supply chain, national government agencies and cybersecurity consultants. The critical insight that this provides enables HORIBA MIRA to support the design and application of an appropriately-configured CSMS to meet the requirements of UNECE Regulation 155.

Read Me in 5

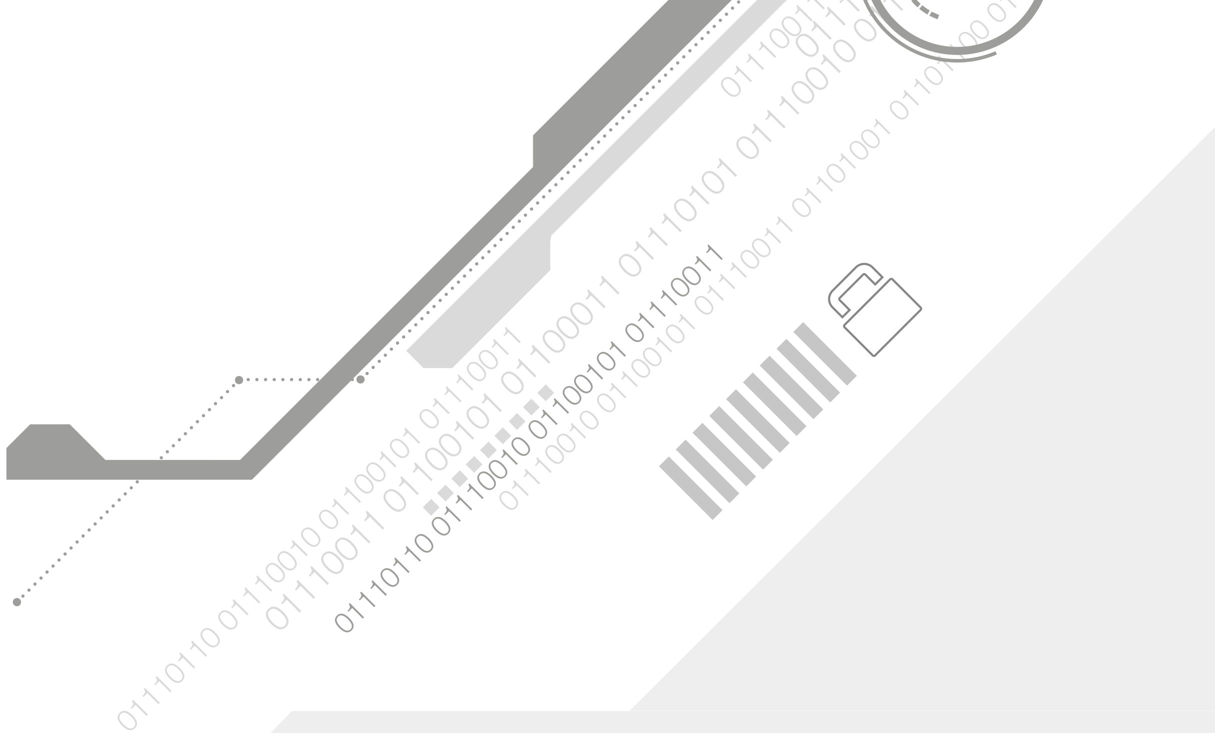
1.
UNECE Regulation 155 sets out the requirements for vehicle cybersecurity

2.
ISO/SAE 21434 will identify current best practice for implementing vehicle cybersecurity and a cybersecurity management system (CSMS)

3.
Regulation 155 will be implemented in national legislation by contracting parties

4.
Competent bodies will be approved to audit compliance with Regulation 155

5.
ISO/PAS 5112 will provide guidance for independent auditors



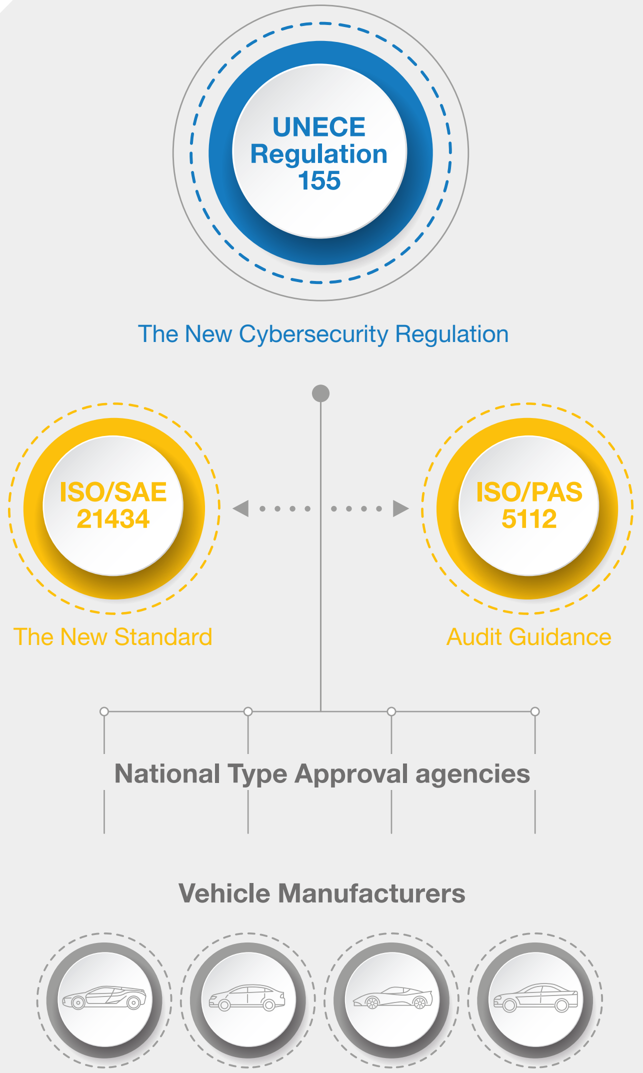


Figure 2: The relationship between UNECE 155, the ISO/SAE standard, Type Approval authorities and vehicle manufacturers

3.
Key Considerations for a Cybersecurity Management System

Regulation 155 does not specify how to design or implement a CSMS. However, the forthcoming ISO/SAE 21434 international standard can provide one pathway to inform the implementation of a CSMS to meet the regulation requirements and will be considered industry best practice. The intent of the ISO/SAE standard is to specify the requirements for cybersecurity risk management for road vehicles, their E/E components and interfaces, throughout engineering (i.e. concept, design, development), production, operation, maintenance, and decommissioning. The standard also sets out a framework for cybersecurity processes and a common language for communicating and managing cybersecurity risk among industry stakeholders.

However, the ISO/SAE standard itself does not provide a comprehensive prescription, but rather an outline of cybersecurity best practice based on expert industry consensus. This standard can be considered as a foundation for deploying rigorous cybersecurity engineering processes and for specifying robust and resilient cybersecurity measures. An interpretation document for the regulation will reference ISO/SAE 21434 along with other relevant guidance sources.

Additional guidance is also under preparation in ISO/PAS 5112, to provide the guidelines to meet the second key intention of Regulation 155, a framework for auditing a CSMS that can be used both by approval authorities as part of the regulatory audit - and by manufacturers to perform internal audits.

Given the extensive scope of Regulation 155 and ISO/SAE 21434, a compliant CSMS that allows manufacturers to achieve vehicle Type Approval will require significant changes to processes throughout the whole vehicle lifecycle from product development, production, maintenance to decommissioning. The CSMS demands an iterative and evolving approach to cybersecurity management, not just because obligations extend across the product lifespan, but also to address the identification, assessment and mitigation of a constantly changing risk horizon during this period.

In this context, a complete CSMS solution should define activities for requirements management, verification and validation as well as detail the capability to monitor, detect and respond effectively to new and emerging threats. Integrating development, testing and operations activities around a common risk management framework is therefore key to an efficient and effective implementation of a CSMS that supports both proactive and reactive cybersecurity engineering.

CYBERSECURITY MANAGEMENT SYSTEM (CSMS) REQUIREMENTS

Organisational Structure and Cybersecurity Processes

VEHICLE REQUIREMENTS

Vehicle Architecture Design, Risk Assessment and Implementation of Mitigations

CSMS REQUIREMENTS

The vehicle manufacturer needs to demonstrate that it has a CSMS in place which covers the following key areas

- Processes for the full vehicle lifecycle including development, production and post-production
- Processes covering cybersecurity management used in the organisation
- Processes to identify, assess, categorise and treat risks, verify that those risks are appropriately managed, and that the risk assessment is kept current
- Processes for cybersecurity testing of vehicles
- Processes to monitor for, detect and respond to cyberattacks, threats and vulnerabilities that emerge during its operation, and to assess the ongoing effectiveness of cybersecurity measures
- Processes used to provide data and support analysis of attacks

The regulation requires an audit by a Type Approval authority or technical service of a vehicle manufacturer's cybersecurity management system (CSMS) resulting in a Certificate of Compliance. The Certificate of Compliance must be in place before a vehicle manufacturer can gain type approval for a new vehicle type and need to be renewed every three years

VEHICLE REQUIREMENTS

The vehicle manufacturer must demonstrate to the approval authority that it meets this set of requirements

- A certificate of compliance for the CSMS relevant to the vehicle being type approved
- Management of supplier-related risks
- Identification of 'critical elements' and 'exhaustive' risk assessment, considering all threats listed in Annex 5 of the regulation and other relevant risks
- Implementation of proportionate mitigations, including relevant mitigations listed in Annex 5 of the regulation or other appropriate mitigations
- Protection of storage and execution of aftermarket software and data
- Testing to verify the effectiveness of the security measures
- Implementation of measures to detect and prevent attacks, support monitoring and data forensic capability for analysis of attempted attacks
- Alignment of any cryptographic functionality with consensus standards

The approval authority or its appointed technical service will verify that a new vehicle has been appropriately engineered according to the certified CSMS with relevant risks identified, analysed and mitigated. The assessment will also check the testing that has been carried out and the processes in place to detect and respond to emerging threats

Figure 3: The key requirements for a Cybersecurity Management System

Read Me in 5

1. Regulation 155 and standard ISO/SAE 21434 will require significant changes across vehicle development, test, manufacture and operation through to decommissioning

2. Manufacturers will need to define and justify components and systems that are critical for cybersecurity

3. Cybersecurity Management System (CSMS) will need to scale to contend with evolving threats

4. Vehicle cybersecurity monitoring need be continuous and span the full lifecycle

5. CSMS obligations will also extend to vehicles in development

3.1 Critical Element Definition and Risk Assessment

The new regulations require vehicle manufacturers to identify the critical elements of vehicle cybersecurity and subject these elements to a comprehensive risk assessment. Consistent with the overall regulatory approach, critical vehicle elements are not defined but can be considered to be components and systems that are highly contingent to overall vehicle function, demonstrating connectivity or have a safety-related dependency. The critical element definition will require the vehicle manufacturer to validate its selection with the relevant approval authority.

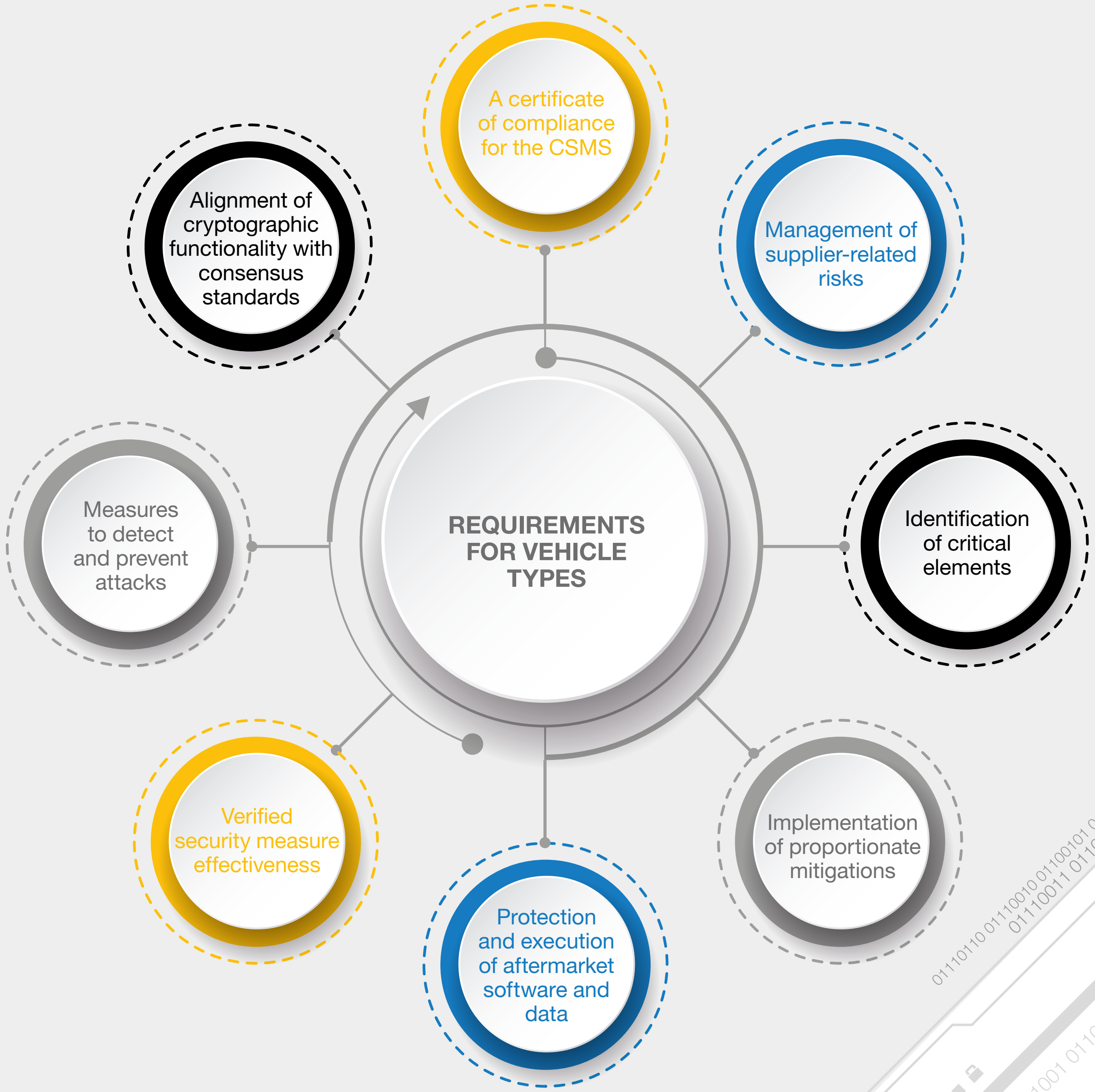

REQUIREMENTS FOR VEHICLE TYPES
A certificate of compliance for the CSMS
Management of supplier-related risks
Identification of critical elements
Implementation of proportionate mitigations
Protection and execution of aftermarket software and data
Verified security measure effectiveness
Measures to detect and prevent attacks
Alignment of cryptographic functionality with consensus standards

Figure 4: Requirements for Vehicle Types

3.2 Contending with Emergent Threats

Alongside critical element definition, the new CSMS must also demonstrate processes capable of monitoring for, detecting and responding to emerging cyber-attacks, cyber-threats and vulnerabilities in a specific automotive context.

While established cybersecurity protocols exist in more generalised applications, the approach and knowledge base for automotive-specific cybersecurity threats and vulnerabilities is at a stage of relative infancy. Therefore threat profiles and response solutions in an automotive setting are neither well established across the automotive sector nor universally present within existing vehicle manufacturer processes.

However, there is a foundation of knowledge that can be called upon to develop robust cybersecurity threat detection and response solutions. Manufacturers need to acknowledge that the obligations under the new regulations will require an ongoing commitment to cybersecurity R&D to provide new solutions for real-time detection and response as well as future engineering resilience methodologies. And as these solutions evolve, so too will the obligation to verify and validate these new operational solutions as an integral part of the CSMS.

3.3 Continuous Monitoring

The requirement to manage the complete vehicle lifecycle and to provide monitoring and mitigation of cyber-attacks as a contingent aspect of Type Approval is particularly problematic as continuous monitoring confers a requirement to maintain unbroken connectivity with vehicles. While vehicle connectivity is increasingly common and widespread, a comprehensive monitoring strategy needs to be implemented, utilising a diverse range of monitoring and detection capabilities as well as flexibility in how data is transmitted off board for analysis and response.

3.4 Managing In-Development Vehicles

Due to the variation of adoption timelines in different geographies and Type Approval jurisdictions, vehicles in development now will confront localised obligations depending on the progression of the adoption of Regulation 155; in some markets, different timelines are being phased in to distinguish between future and existing model development.

Due to the length of development cycles, many vehicles reaching the market in the near future may have been in development before the requirements of the cybersecurity regulation were known, yet will still be subject to the regulation. Provisions are made in the regulation for such cases, for example, for type approvals prior to 1 July 2024, the cybersecurity regulation allows the vehicle manufacturer to demonstrate that cybersecurity has been adequately considered during development. This notion of adequacy is not further defined in the regulation, so it is important that a consistent approach is taken for type approval assessments while these stipulations are more precisely defined through real-world application.

4. HORIBA MIRA's Approach to Developing a CSMS

With deep domain experience in automotive regulatory frameworks, as well as an extensive engineering consultancy track record in all aspects of vehicle resilience solutions, HORIBA MIRA has developed a risk-based approach to vehicle functional safety that is now reflected in ISO 26262:2018, automotive cybersecurity included in SAE J3061 and ISO/SAE 21434, as well as SOTIF (Safety of the Intended Functionality, ISO PAS 21448:2019). HORIBA MIRA is now adapting this risk-based approach to address electromagnetic resilience aspects (including EMC, human exposure to electromagnetic fields and connectivity performance) in order to provide a unified approach to the full spectrum of vehicle resilience issues. As a result HORIBA MIRA does not just consider cybersecurity in isolation, but as part of wider vehicle resilience.

HORIBA MIRA's dynamic risk-based engineering approach is central to developing a CSMS that is consistent with the goal-based form of the regulations. The threat and risk knowledge base is developed and maintained across engineering, test and operations. This ensures for instance that cybersecurity tests align with significant risks identified in the design phase of vehicle development and with a comprehensive operations element provides through-life risk management of emerging vulnerabilities and incidents. This not only ensures a full lifecycle solution, but also provides records for the ongoing CSMS audit obligations.

Read Me in 5

1. HORIBA MIRA's engineers have developed a proprietary risk-based approach to cybersecurity

2. The HORIBA MIRA approach provides a unifying platform for the interaction between cybersecurity, functional safety and other key vehicle resilience considerations

3. The HORIBA MIRA approach is based around a dynamic risk-based systems engineering process, which extends across the V cycle and beyond

4. The process and associated data models are anchored on the fundamental engineering and test foundation of a vehicle, and extend into the operational phase

5. This approach provides a core knowledge base that is continuously augmented across the vehicle lifecycle

5. HORIBA MIRA – Solutions to the Problem

The obligations to vehicle manufacturers under Regulation 155 present several substantial challenges including:-

- The short timelines before compliance becomes obligatory for new and in-design vehicles
- The absence of a prescriptive set of requirements both to inform the CSMS solution design and to guide the consistency of auditing
- Poorly judged CSMS solutions may either not deliver compliance (and thereby jeopardise Type Approval) or provide potentially over-engineered solutions which add significant cost burdens to vehicle development and production and impact bottom-line profitability
- The need for cybersecurity process implementation to provide a long-term and evolving solution that integrates into wider V Cycle processes and beyond in to operations
- An identified requirement for a conspicuous culture shift within organisations to support the effectiveness of cybersecurity engineering

With its deep experience in the automotive engineering domain, familiarity with the regulatory framework for cybersecurity and its proprietary solutions and services, HORIBA MIRA's consultant engineers are well-placed to help vehicle manufacturers develop fit-for-purpose solutions.

Read Me in 5

1.
Without prescriptive regulations, HORIBA MIRA has the expertise to develop CSMS solutions that deliver conformity at the minimum cost and to time

2.
HORIBA MIRA's automotive engineering experience as well as our direct contribution to framing key regulations will help companies navigate interpretation and consistency in their CSMS solutions

3.
HORIBA MIRA's risk-based engineering approach provides an enduring and evolving framework for manufacturers that can spans all vehicle resilience domains

4.
HORIBA MIRA's customer approach includes a four-step readiness approach to identify gaps in current processes

5.
HORIBA MIRA's services are independent and founded on deep automotive domain experience

HORIBA MIRA's Credentials

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.

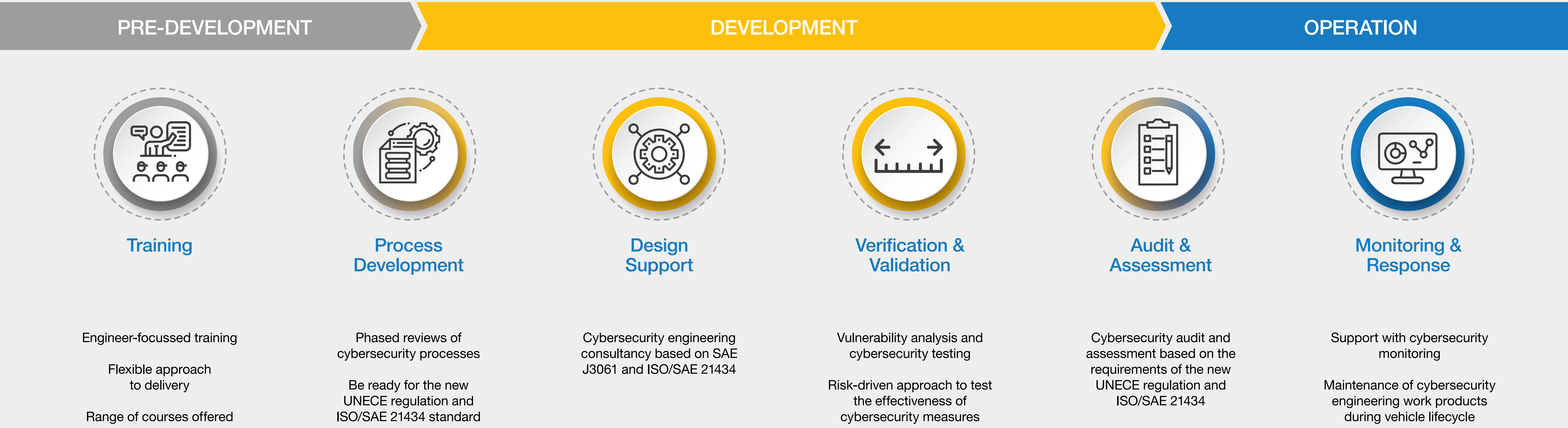
As well as developing class-leading knowledge and expertise in applied cybersecurity in addition to its research work, HORIBA MIRA has been an active contributor to the development of key automotive cybersecurity standards and regulations, such as SAE J3061, ISO/SAE 21434 and the new UNECE regulations.

From this close involvement in the framing and drafting process, 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 knowledge is particularly important in the absence of express prescription, as is the case with Regulation 155.

This regulatory experience, HORIBA MIRA's depth of automotive sector know-how, a testbed eco-system for verification and validation from lab to road and its independent status, makes the organisation uniquely-placed to assist clients in navigating new cybersecurity regulations and standards.

6. 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



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

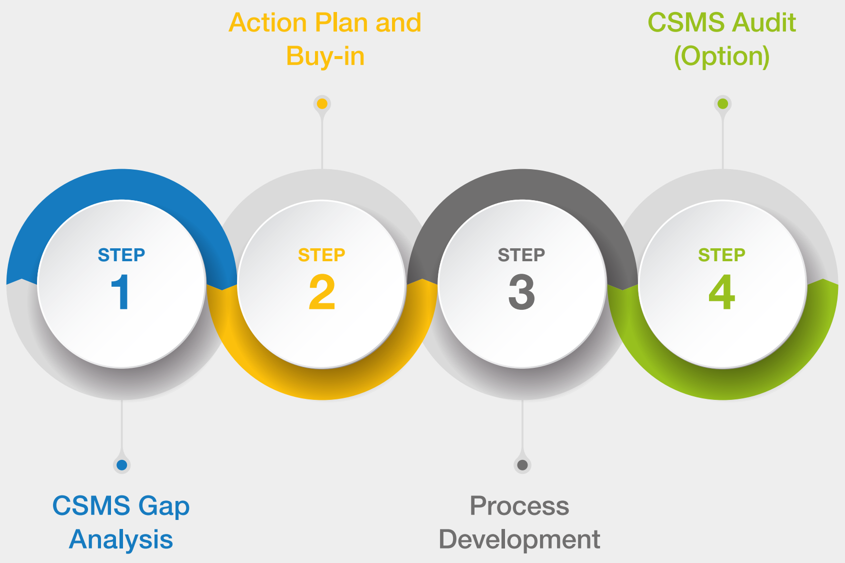
Support with cybersecurity monitoring

Maintenance of cybersecurity engineering work products during vehicle lifecycle

Figure 5: HORIBA MIRA cybersecurity services

Process Development

To assist customers with their preparation for Regulation 155, HORIBA MIRA has developed a four-step readiness programme which can be tailored to an organisation's specific requirements. The intention of the readiness programme is to identify gaps within existing processes and provide solutions to achieve compliance quickly and effectively.



The programme will provide the following key benefits

- Increasing both the cultural awareness and understanding of automotive cybersecurity, the detail of the new regulation and standard and the broader implications for a client's business operations
- The third-party validation from experts of existing cybersecurity processes and their compliance with the new regulation and standard
- Access to expert guidance to embed cybersecurity best practice in your organisational processes

Training

HORIBA MIRA's experts lead peer-to-peer cybersecurity training expressly for engineers with a flexible approach to the content, duration and delivery format, including personal instruction at the MIRA Technology Institute (MTI), with bespoke courses delivered on client sites or by remote instruction.

Engineering Consultancy

Our engineering consultancy services support both preparations for compliance with the new regulation and standard as well as ongoing support through:

- developing internal cybersecurity engineering competence
- support for proactive cybersecurity by design including verification and validation
- support for cybersecurity monitoring and response to new threats

Cybersecurity Audit and Assessment

Central to stress-testing customer CSMS solutions, HORIBA MIRA provides internal cybersecurity audit and assessment services. This includes the provision of competent cybersecurity assessors and conducting independent assessments. An independent assessment can be used to judge compliance with the requirements for vehicle types.

HORIBA MIRA's independent cybersecurity assessment approach is based on the 5StarS assurance framework which defines vehicle assessment criteria mapped to the requirements of ISO/SAE 21434, the UN Regulation 155 and the UK Department for Transport's 'The key principles of vehicle cyber security for connected and automated vehicles.'

Next Steps

It is vital that organisations likely to be impacted by UNECE Regulation 155 and the ISO/SAE 21434 standard begin preparation without delay. This extends to vehicle manufacturers, the tiered supply chain and the many related contributors to automotive infrastructure, including for instance telecoms connectivity providers, all of whom will to a greater or less degree be impacted through the impending changes to Type Approval criteria.

HORIBA MIRA has a highly capable and experienced team to help navigate clients through all stages of this transition, through engaging senior management in the critical business case to developing a broad organisational culture of cybersecurity awareness, ensuring sufficient resource to enable solutions, auditing, reviewing existing quality management and functional safety engineering processes and ultimately helping to architect a fit-for-purpose cybersecurity engineering process that covers the full lifecycle of a complete vehicle portfolio.

The changes that will ensue as a consequence of the new UNECE regulation are profound and require a substantive response from all organisations that fall under the scope of the new rules. Failure to act will unquestionably impact the commercial health of impacted businesses, but there is still sufficient time to prepare thoroughly.

Book an initial consultation

HORIBA MIRA's specialist Vehicle Resilience Team are available to discuss your preparedness. **Book a no-obligation initial consultation by contacting Nick Tebbutt, Head of Global Strategic Sales, Vehicle Technologies**

✉ **nick.tebbutt@horiba-mira.com**

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

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