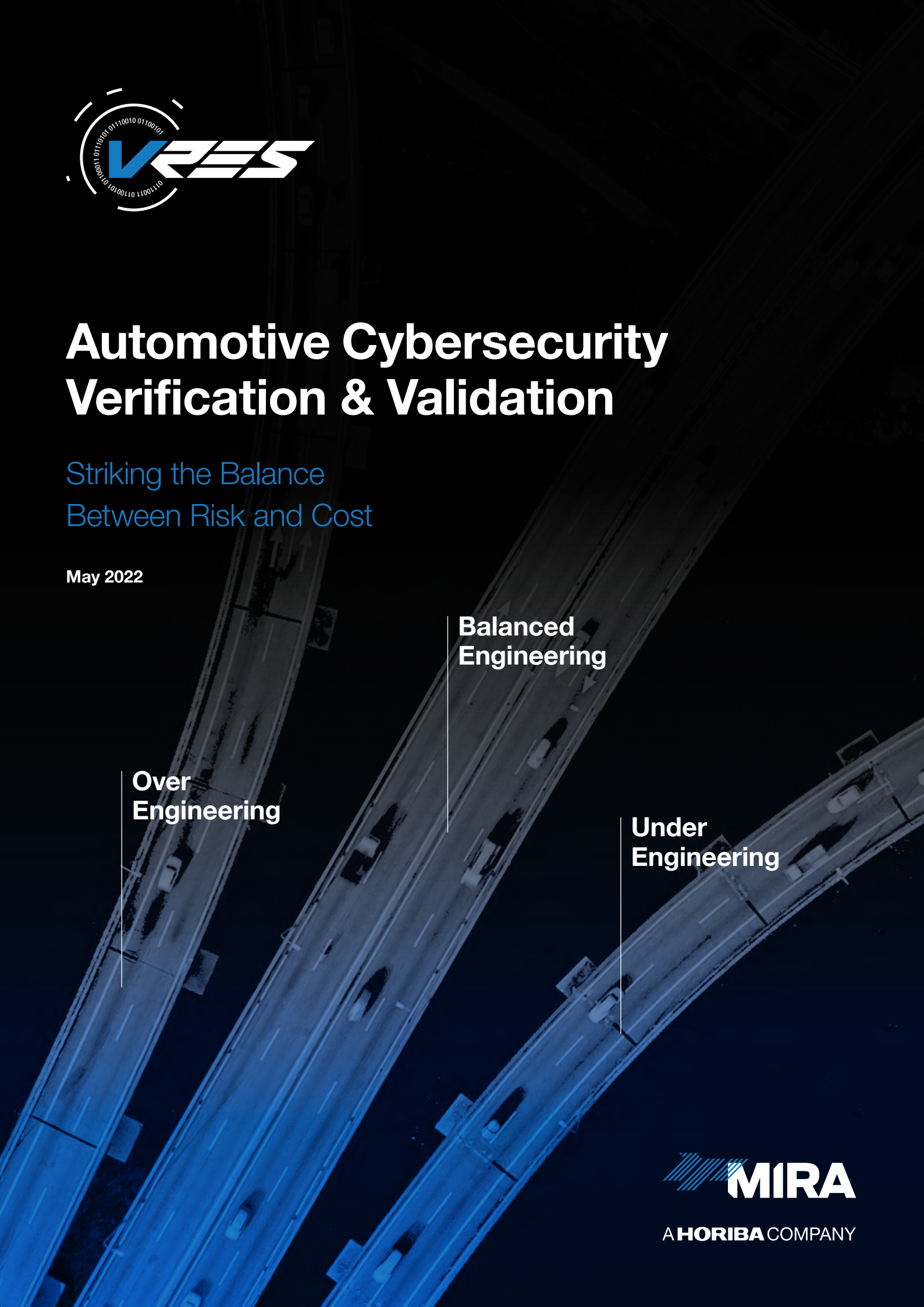
Automotive Cybersecurity Verification & Validation

Striking the Balance Between Risk and Cost

May 2022



MIRA

A HORIBA COMPANY

Introduction

This is the third cybersecurity paper in a series from HORIBA MIRA's Vehicle Resilience experts. It details why cybersecurity must be treated by the automotive industry as inherently different to typical engineering protocols that are clearly prescribed and usually represent a fixed stage in the product development process; automotive cybersecurity is different as it extends across the entire design, manufacture and operational lifecycle of a vehicle. Moreover, the criteria against which cybersecurity should be tested are not codified, nor are the criteria fixed as a consequence of ever-changing and evolving threat scenarios.

This absence of definition across the entire cybersecurity domain presents vehicle manufacturers and the tiered supply chain with a considerable problem that this paper aims to address. It outlines how cybersecurity must extend across the product lifecycle and in the absence of explicit testing requirements, how engineers should develop an approach to testing that results in a sufficiently secure but commercially viable approach to cybersecurity.

For the automotive industry, achieving balance between the risk of liability associated with recalls, warranties and loss of brand reputation and the cost of over-engineering cybersecurity solutions is additionally complex when no clear prescription exists; not only is it a challenge for an individual manufacturer or tier supplier to manage in their own right, but this judgement also needs to be made in a commercial context with an eye to the costs and risks being assumed by competitors. This paper aims to provide some guidance to navigating these considerations.

This paper should be read in conjunction with HORIBA MIRA's other automotive cybersecurity documents, including How to Navigate New Cybersecurity Type Approvals which outlines how to meet UNECE Regulation 155 and Why Automotive Cybersecurity is Different, an analysis of why automotive cybersecurity presents distinct and different challenges to more commonly understood definitions of cybersecurity.

All of these papers are free to download and can be accessed from HORIBA MIRA's website at horiba-mira.com/Vehicle-Resilience.

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.
Cybersecurity Verification and Validation (V&V) Background

Cybersecurity verification and validation is required by the new automotive regulation UN R155 and supported by international standard ISO/SAE 21434. However, due to the inherent variation in vehicle design, its systems and the approaches employed in these processes, it is not possible for the regulation to prescribe a specific set of tests for compliance.

What's more, the regulation demands more than just point-in-time compliance; rather the regulation's ambition is to ensure the industry develops a full system of appropriate testing and risk analysis that extend across the entire product lifecycle. In addition, vehicles no longer operate in isolation, but form one part of a wider mobility ecosystem that provides externalised opportunities for cybersecurity threat agents.

For those concerned with meeting the new cybersecurity requirements, whether vehicle manufacturers, component suppliers, type approval authorities or independent auditors, this absence of prescription presents the challenge of adequately designing the verification and validation framework to appropriately meet the intent of the regulation. HORIBA MIRA, as a key contributor to both the Regulation and the Standard, has developed a risk-based approach that supports the full end-to-end requirements.

In order to address the question of an appropriate level of verification and validation, it is helpful to refer to the definition of these terms in the new ISO/SAE 21434 international standard.

The standard maintains the following definitions:-

Verification *is the confirmation, through the provision of objective evidence, that specified requirements have been fulfilled*. The focus is therefore on confirming the correct implementation of the requirements have been specified during development. In short, in this context, it demands that cybersecurity measures have been correctly implemented.

Validation by contrast is defined as *the confirmation, through the provision of objective evidence, that the cybersecurity goals of the item are adequate and are achieved*. Validation focuses on the ability of the system to achieve the cybersecurity goals, and whether this is sufficient to reduce the risk of the relevant threats. Validation therefore demands that cybersecurity solutions are effective.

The definitions drawn from the international standard support the fundamental requirements of the regulation that require that manufacturers to:-

- Demonstrate the adequacy of the processes they have in place for identifying, assessing and treating the cybersecurity risks to vehicles, and testing the cybersecurity of vehicles
- Perform appropriate and sufficient testing to verify the effectiveness of the cybersecurity mitigations they have implemented
- And demonstrate the adequacy of the processes used to: -
  - Monitor for, detect and respond to cyber attacks, cyber threats and vulnerabilities on vehicle types
  - And assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified

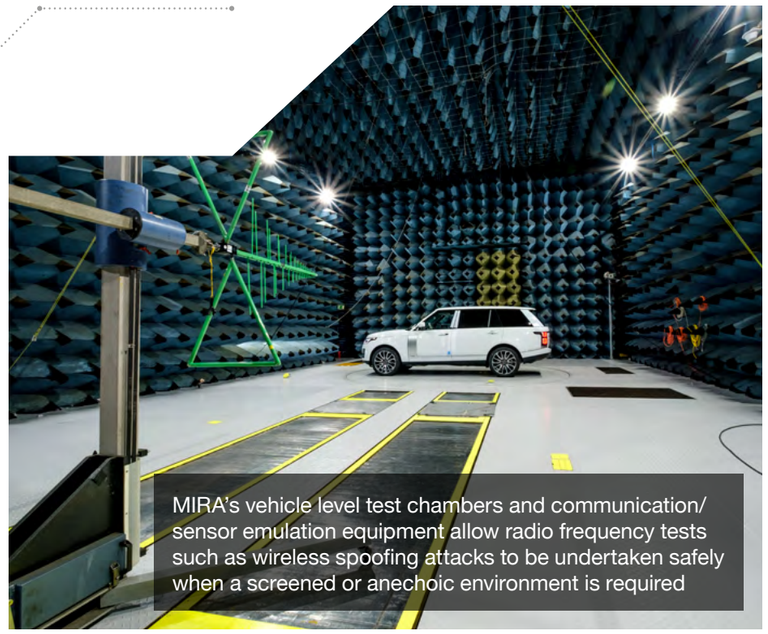
HORIBA MIRA's Vehicle Resilience team have developed a complete ecosystem of facilities for cybersecurity testing and R&D

HORIBA MIRA's ASSURED CAV Parking and City circuits have recently undergone a multi-million pound upgrade to support advanced connected and autonomous test scenarios using the latest V2x infrastructure, including our own privately terminated 4/5g network with our partner Vodafone. With full control of the environment, we undertake a wide variety of controlled real-world cybersecurity tests in a safe and secure proving ground

The ASSURED CAV Highway provides customers with a world-class test environment for advanced dynamic-based cybersecurity attack scenarios, with ample space to ensure controlled test execution

MIRA's dedicated screened and anechoic component laboratories along with advanced support equipment to simulate real-world test modes allow deep analysis of hardware and software in true-world conditions

HORIBA MIRA's purpose built VRES workshops provide dedicated, secure environments for our engineers to undertake detailed V&V testing



MIRA's vehicle level test chambers and communication/ sensor emulation equipment allow radio frequency tests such as wireless spoofing attacks to be undertaken safely when a screened or anechoic environment is required

2.0
The Approach to Cybersecurity Verification and Validation (V&V)

The requirements laid down by UN ECE Regulation 155 summarised in section 1.0 requires its own appropriate approach in the absence of a prescribed set of tests for cybersecurity compliance.

This approach is risk-based rather than prescriptive for a variety of reasons. In the first instance, not all vulnerabilities will be known, nor is it possible to estimate the scope of these unknowns.

Moreover, errors introduced by specification flaws, design errors and implementation defects can introduce behaviours less likely to be detected by functional testing alone. Cybersecurity vulnerability can arise from these hidden additional behaviours that lie beyond the documented specification.

As a consequence of these characteristics of cybersecurity vulnerability, absolute security cannot be achieved. Not only do new threats evolve to exploit weaknesses in the fixed parameters of behaviours that might not have been accounted for, but in-service software updates have the potential to introduce new and additional vulnerabilities.

A risk-based rather than a prescriptive approach therefore provides the only practical solution for cybersecurity. This approach starts with a security-aware design methodology which reduces risks to a minimum, including the foresight to assess whether less consequential vulnerabilities identified in the design stage could become more significant over the course of the vehicle lifecycle, particularly if software updates change the risk parameters.

In addition to a security-aware design methodology, tests must be vehicle and/or component-specific.

Risk assessment is best managed using techniques such as attack tree analysis that allows attack paths to be identified and assessed for their risk versus remediation profile. This allows engineers to make informed decisions about risks that require mitigation and those other known risks that can be reduced or ignored, thereby allowing risks and costs to be appropriately balanced.

10

3.0
The Approach to Cybersecurity Verification and Validation (V&V)

In order to help determine that the type and extent of cybersecurity testing is sufficient for auditing purposes, ISO/SAE 21434 Annex E outlines Cybersecurity Assurance Levels (CAL). CAL provides a risk-based mechanism to measure the depth and rigour of cybersecurity engineering activities. Activities that could be assessed using CAL include the scope, depth, rigour and level of independence of analysis and testing activities.

Suitable metrics addressing the challenges of cybersecurity verification and validation procedures are required for meaningful evidence of effectiveness. This evidence should be sufficiently robust to form the basis of future legal and certification arguments as well as operational assurance and certification in both regulatory and legal contexts.

3.1 Testing Methods, Reviews & Analysis

Although UN R155 does not contain a prescriptive list of tests, some suitable methods are suggested in ISO/SAE 21434 for both verification and validation for cybersecurity, including both desk-based analysis and practical testing methods. As these methods are not all applicable to all cases, it is recommended that vehicle and component manufacturers develop both a cybersecurity verification plan to confirm correct implementation and a cybersecurity validation plan to confirm effectiveness.

Reviews

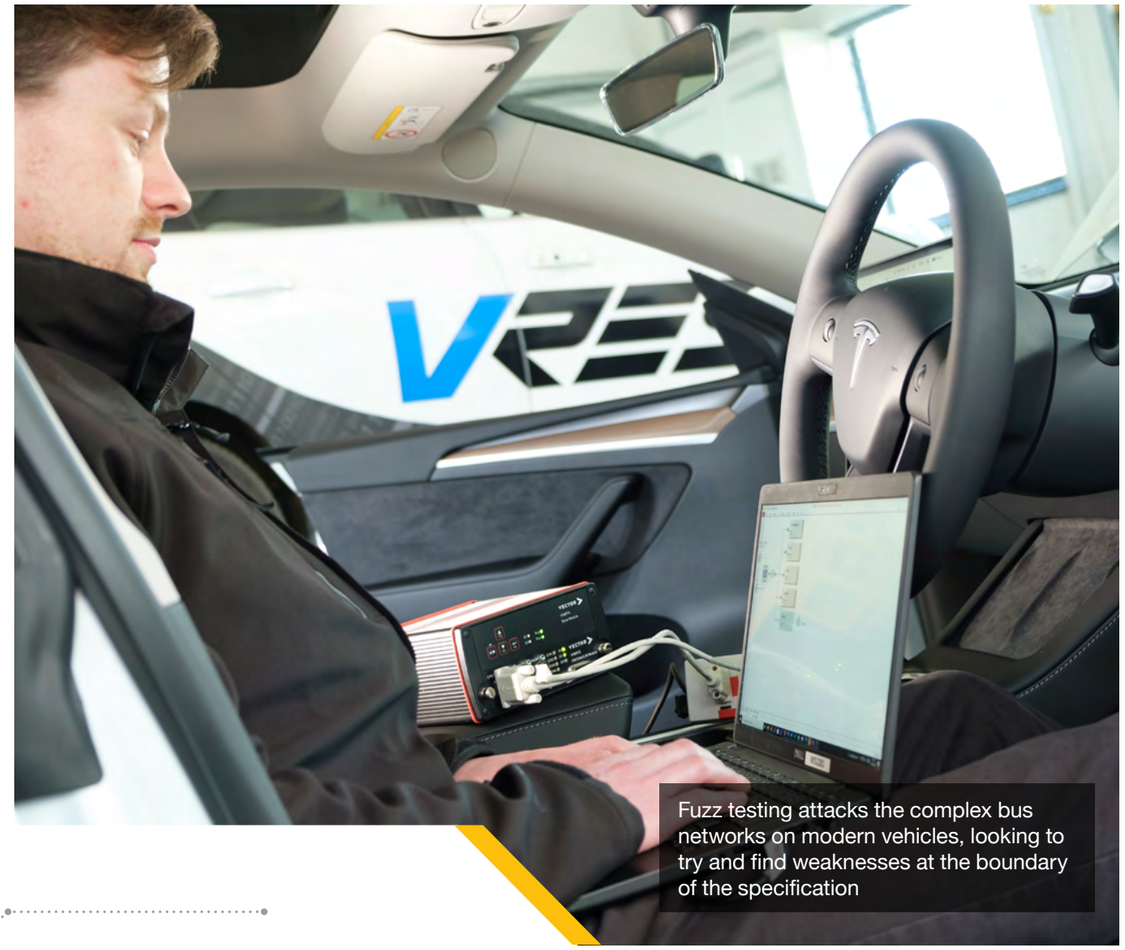
Prior to practical testing, threat modelling and security-focussed reviews should be carried out, including security design reviews of system or component architecture, the design of protocols that use cryptography, source code reviews and hardware schematic reviews. This helps to identify at an early stage any potential or actual vulnerabilities that are specific to particular design, implementation or integration details. In this respect, it is possible to see that some of these activities can take place much earlier on than usual when the finished vehicle is ready, since they are part of the principles on which the V&V activity is based within the overall design approach.

Analysis

Many vulnerabilities can also be identified at an early stage using analysis techniques. Examples include numerical or statistical analysis, such as verifying that a random number generator produces sufficient entropy, and static code analysis of software source code to identify coding implementation defects and to verify conformance to coding guidelines such as MISRA C or CERT C. Analysis activities may be carried out on designs and specifications as well as on simulations, enabling weaknesses and vulnerabilities to be identified much earlier in the development process. While this analysis can also be undertaken when software is mature, this is an additional example of how early activity for V&V can help to ensure the overall resilience and robustness of the cybersecurity solution is considered from the outset.

3.2 What Tests to Perform

Early testing of prototype hardware and software allows quick identification of obvious issues that can be easily rectified



Fuzz testing attacks the complex bus networks on modern vehicles, looking to try and find weaknesses at the boundary of the specification

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 of if the solution addresses whether the implementation delivers the intended functionality.

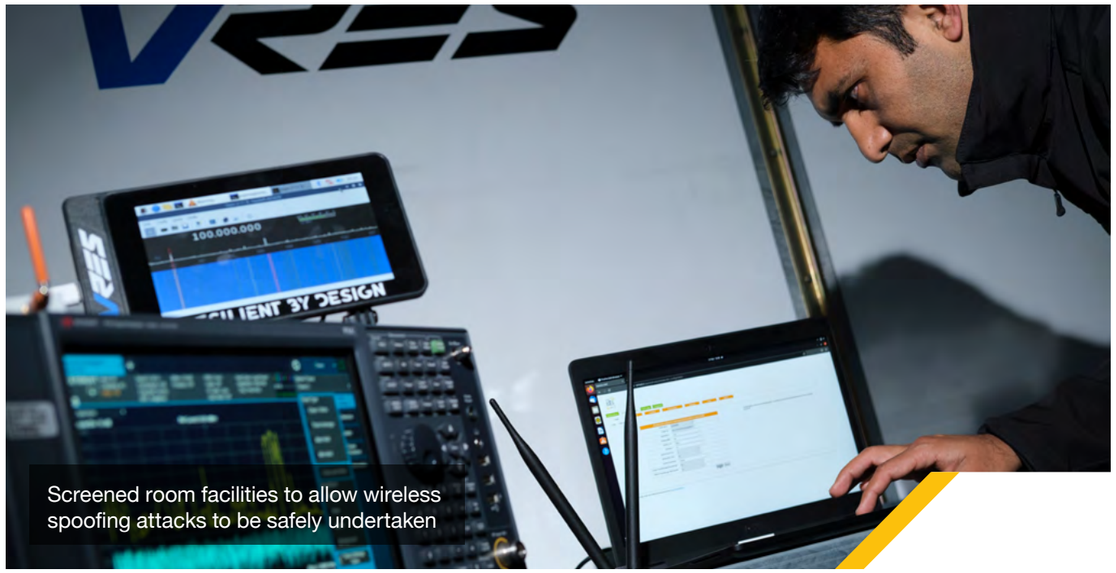
Correctness Testing

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 activities can be carried out at the same test phase process steps 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.

Fuzz Testing

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.



Screened room facilities to allow wireless spoofing attacks to be safely undertaken

Penetration Testing

Even extensive systematic testing for correct observable and non-observable functionality is not sufficient to test whether an implementation really resists the 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 organization or from third parties under relevant non-disclosure agreements.

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

Penetration testing can be carried out using a black box approach, in which the tester puts themselves in the position of an attacker and tries to identify and exploit vulnerabilities without any prior information. An example would be injecting messages on a vehicle CAN bus without prior knowledge of the vehicle's CAN database, meaning that the tester would first need to reverse engineer the CAN database by analysing typical messages observed during normal operation.

At first glance this has the apparent advantage of being a realistic approach; however it is not practical to test every possible attack scenario since no OEM has unlimited time and budget and it may lead to a deep-seated vulnerability being missed due to time constraints.

A white box approach is usually more efficient, as the tester is able to identify vulnerabilities with the help of design or implementation information. This may include design specifications or implementation details such as source code. Clearly this approach gives the tester an advantage over a real attacker, and it is therefore important to provide a justification of how a real attacker could successfully carry out an identified attack path without access to the information. Access to up-to-date sources of threat intelligence is therefore important to assess an attacker's capabilities and motivations relative to the test conditions. However, a white box approach does provide the opportunity to identify more vulnerabilities in the same timescale, thus saving costs in terms of either in-house testing effort or third-party independent testing.

Due to the limited transfer of detailed design information within the automotive supply chain, in practice a hybrid 'grey box' approach may be adopted, which utilizes any available information but adopts the position of a real adversary to determine the missing details.

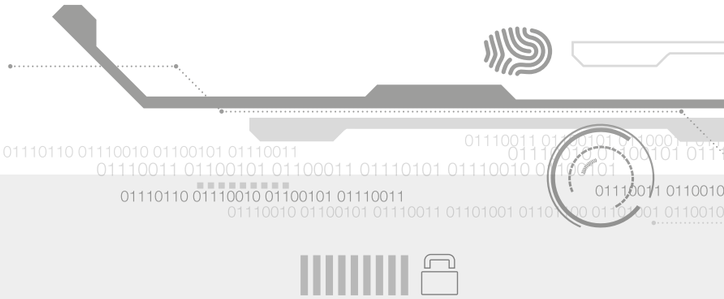
Electronics laboratories for cybersecurity testing and R&D at component level

Vulnerability Scanning

Known vulnerabilities in commonly used software modules and libraries can be identified using vulnerability scanners. These are automated tools which recognise specific versions of software from binary or source code and cross check them against public vulnerability databases, such as the NIST National Vulnerability Database. Other variants exist that can identify code patterns that correspond to classes of weakness, such as buffer overflows or unsafe memory accesses. Vulnerability scanning can also be used as part of a penetration test to passively scan a target system for possible attack points.

3.3 Testing Automation

Test automation can assist with the proliferation of testing requirements caused by vehicle and component-specific requirements of cybersecurity. Some level of cybersecurity-focused Hardware-in-the-Loop solution can help here and also provide a level of repeatable conformity of testing and reporting. The adversarial mindset required to carry out this exploratory testing is difficult to automate effectively and therefore requires specialist expertise.



4.0
Testing Infrastructure

Cybersecurity testing and R&D demands its own specific capabilities and solutions, often in closed and secure environments that can be safely managed like those at MIRA. Controlled testbed facilities are essential for tests such as:-

- Testing assisted or automated features in a dynamic mode of operation, such as investigating attacks on vehicles which affect the safety-related functions of vehicles in realistic but safe conditions
- Testing similar features but integrating connectivity to mobility infrastructure such as C-ITS infrastructure, to include the cybersecurity of V2X in emulated urban and sub-urban environments
- Assessing cybersecurity performance of assisted or automated features when vehicles are travelling at speed to emulate highway or motorway conditions

Beyond the safety critical need for proving ground testing for dynamic cybersecurity assessments, a variety of other facilities and capabilities should be considered as essential to the verification and validation framework, including:-

- Virtual facilities to investigate the potential for simulation, modelling and other virtual verification & research into resilient and self-healing systems
- Electronics laboratories for cybersecurity testing and R&D at component level. These embedded systems laboratories should contain electronic test and measurement equipment as well as specialist tools for security testing
- Vehicle workshops equipped with vehicle lifts and appropriate mechanical and electrical tools are required for the vehicle level experiments. These vehicle workshops should also be equipped with relevant communications infrastructure
- For tests which require the vehicle to be in motion, specialised chassis dynamometer and infrastructure is required
- Electromagnetically screened chambers, equipped with a full range of wireless test equipment at the relevant frequencies for both vehicle and component testing to enable research and tests involving the generation of wireless signals that cannot be carried out in open air environments
- Infrastructure laboratories which provide facilities in controlled, safe, sandboxed environments to emulate connected infrastructure components of the mobility ecosystem, including:-
- Connected vehicle backends to emulate the backend server components of connected services provided by vehicle manufacturers' or other third parties
- Over-the-air (OTA) software update servers to emulate the off-board components of over-the-air software update systems
- C-ITS roadside units and back office to emulate the off-board elements of V2I communications
- Electric vehicle charging infrastructure including charging stations (EVSE), service provision and grid components
- Public key infrastructure (PKI) components associated with each of the above

As with any significant increase in infrastructure, facilities and skills, a key decision for businesses impacted by the new regulation and standard is to determine which elements of cybersecurity verification and validation to bring in-house, and which aspects of these new arrangements can be seamlessly transferred to expert partners.

HORIBA MIRA's Vehicle Resilience 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, operating from state-of-the-art workshops and testing facilities alongside over 100km of advanced proving ground facilities with 24 circuits in the UK's West Midlands. This forms a complete cybersecurity engineering, V&V, assurance and operations eco-system that is uniquely placed to offer customers a flexible solution to the challenge of how to meet the requirements of Regulation 155. HORIBA MIRA has all the various facilities need to address the complex and interrelated V&V activities that an vehicle manufacturer or tier supplier might need, saving the significant expense of investing in new infrastructure that is utilised only in short, intense bursts of activity.

Infrastructure Requirements

Figure 3: Infrastructure Requirements

HORIBA MIRA's Vehicle Resilience Complete Verification and Validation Eco-System

Vehicle Resilience

Ranging from workshops and screened labs for static and dynamic vehicle testing, attack labs and system-level labs through to ASSURED CAV Highway, City and Parking, allowing the safe assessment of vulnerabilities in a controlled real-world environment, this cluster underpins the delivery of globally significant automotive cybersecurity, safety and connectivity excellence.

Customer Accessible Facilities, Workshops and Offices

Comprehensive, independent facilities, workshops and office space to verify, validate and certify class-leading products. HORIBA MIRA's onsite team of specialist consultants, engineers and technicians provide hundreds of years of combined expertise in validating to regulations and standards, to client specific requirements and in the development of appropriate test procedures and methods.

Controlled

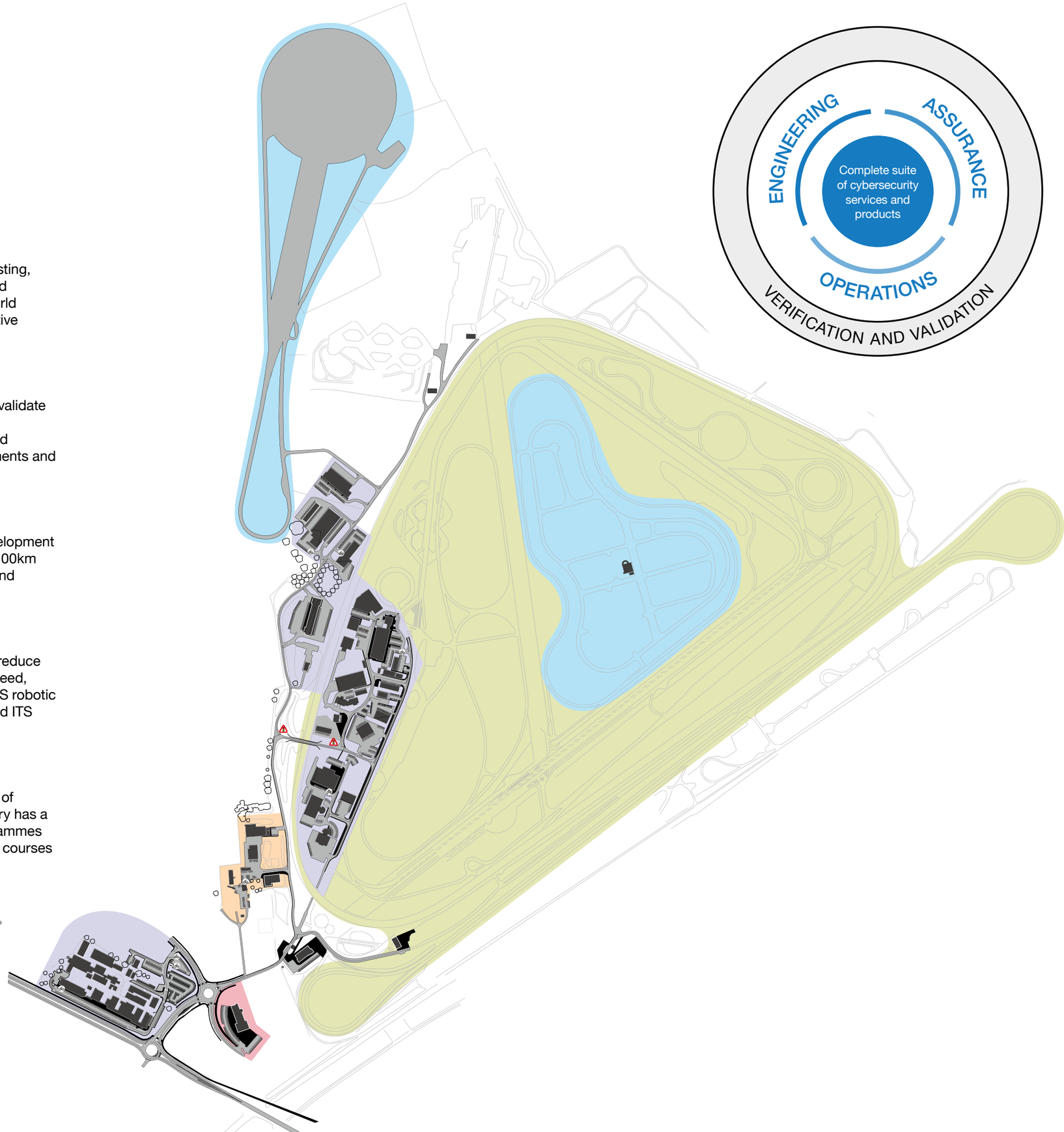
An extensive proving ground providing an unparalleled venue for product development and validation. The comprehensive range of circuits and facilities spans over 100km and enables customers to carry out a wide range of activities in a controlled and secure environment, irrespective of vehicle type or development objective.

Connected

A world-leading connected and automated ecosystem, specially designed to reduce the uncertainty, complexity and time spent in development. It features high speed, urban and automated parking CAV-enabled test environments, extensive ADAS robotic targets and supporting junction layouts, private 4G and 5G mobile network and ITS G5, and a simulation platform for virtual scenario testing.

MIRA Technology Institute

A bespoke education facility designed specifically to train the next generation of engineers in the latest emerging automotive technologies, ensuring the industry has a sustainable supply of future technical specialists. MTI offers accredited programmes from Level 2 to Level 8 (Doctorate level) as well as a range of bespoke training courses and CPD opportunities.



HORIBA MIRA's next cybersecurity white paper will consider the final element in the development of capability to enable vehicle manufacturers and tier suppliers accord with Regulation 155. Beyond testing and infrastructure requirements, the whole lifecycle obligation requires the industry to detect and respond to emerging threats, for example by building and managing Vehicle Security Operations Centres (VSOCs).

Together with BT, the paper will outline how to develop methods for confirming the functionality and establishing the effectiveness of detection solutions such as intrusion detection systems and incident management activities of a Vehicle Security Operations Centre.

Cybersecurity Testing

Infrastructure Requirements

Vehicle Security Operation Centres

5.0
Summary Points

Cybersecurity testing must take place throughout the product lifecycle, including V&V during production development in all aspects from hardware, software, systems and vehicle integration, through the assessment and certification phase and across the operational monitoring and response phase of the vehicle.

Balancing the risk and cost of cybersecurity is key for the industry to preserve reputation while managing cost. This optimisation will ensure solutions are neither over nor under-engineered.

It is impossible to standardise vehicle cybersecurity test requirements, so appropriate and adequate test strategies must be developed by vehicle manufacturers and their suppliers, on a case-by-case basis and reviewed over the product life as part of the operational assurance monitoring.

Vehicle cybersecurity assurance activities need to take account of other elements of the wider connected and automated mobility ecosystem.

Testing before starting production alone is insufficient; as the threat landscape will continually evolve, engineers must rather focus on operational assurance – delivering justifiable confidence that the risks associated with the vehicle, process or service are acceptable to its users throughout its lifecycle.

Cybersecurity verification and validation will require extensive facilities and capabilities, reflecting a significant capital investment requirement or the selection of appropriately equipped expert partners to manage the process in order to meet new regulatory requirements.

6.0
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.

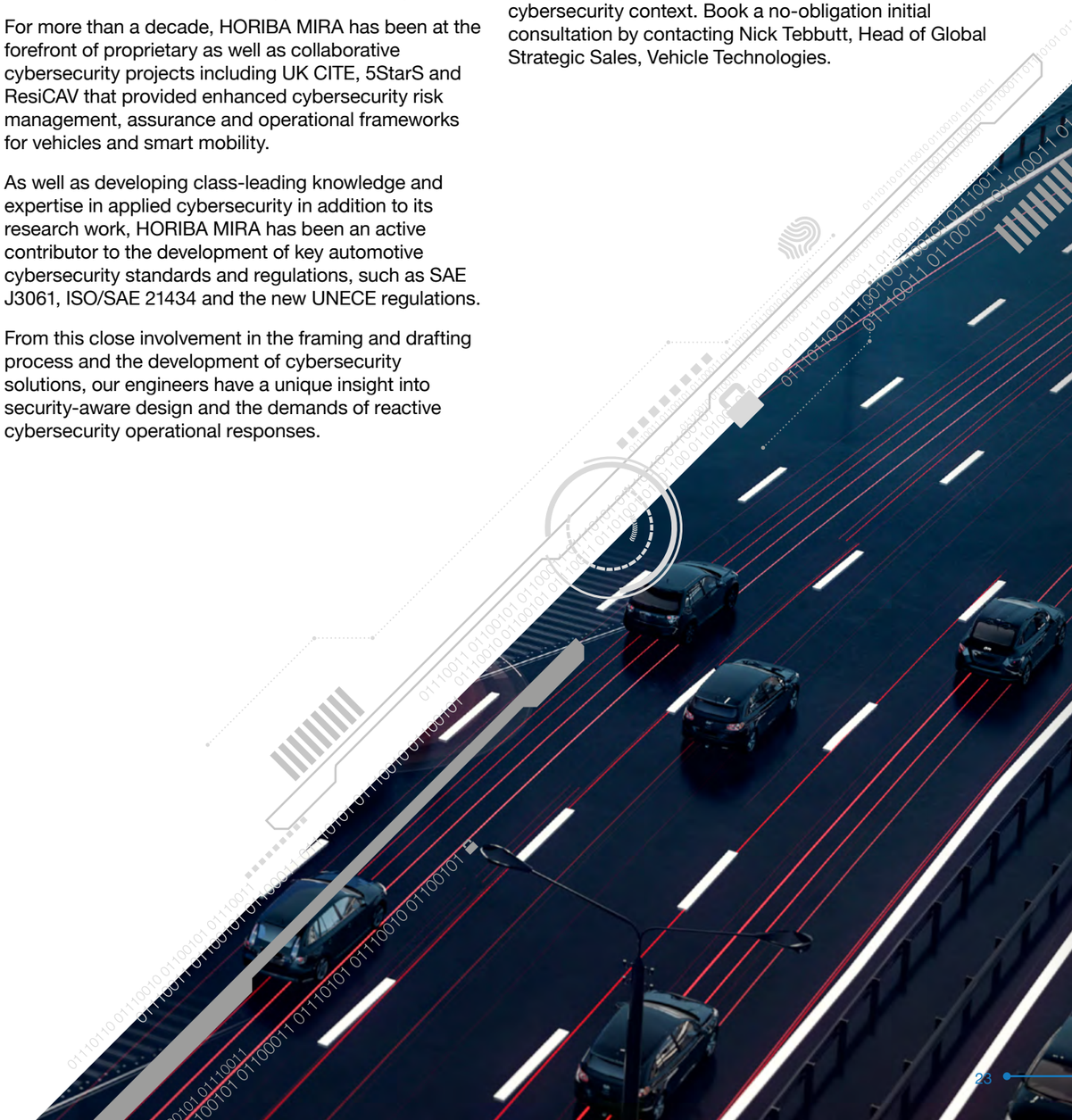
For more than a decade, HORIBA MIRA has been at the forefront of proprietary as well as collaborative cybersecurity projects including UK CITE, 5StarS and ResiCAV that provided enhanced cybersecurity risk management, assurance and operational frameworks for vehicles and smart mobility.

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, 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.

HORIBA MIRA's specialist Vehicle Resilience Team are 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.



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