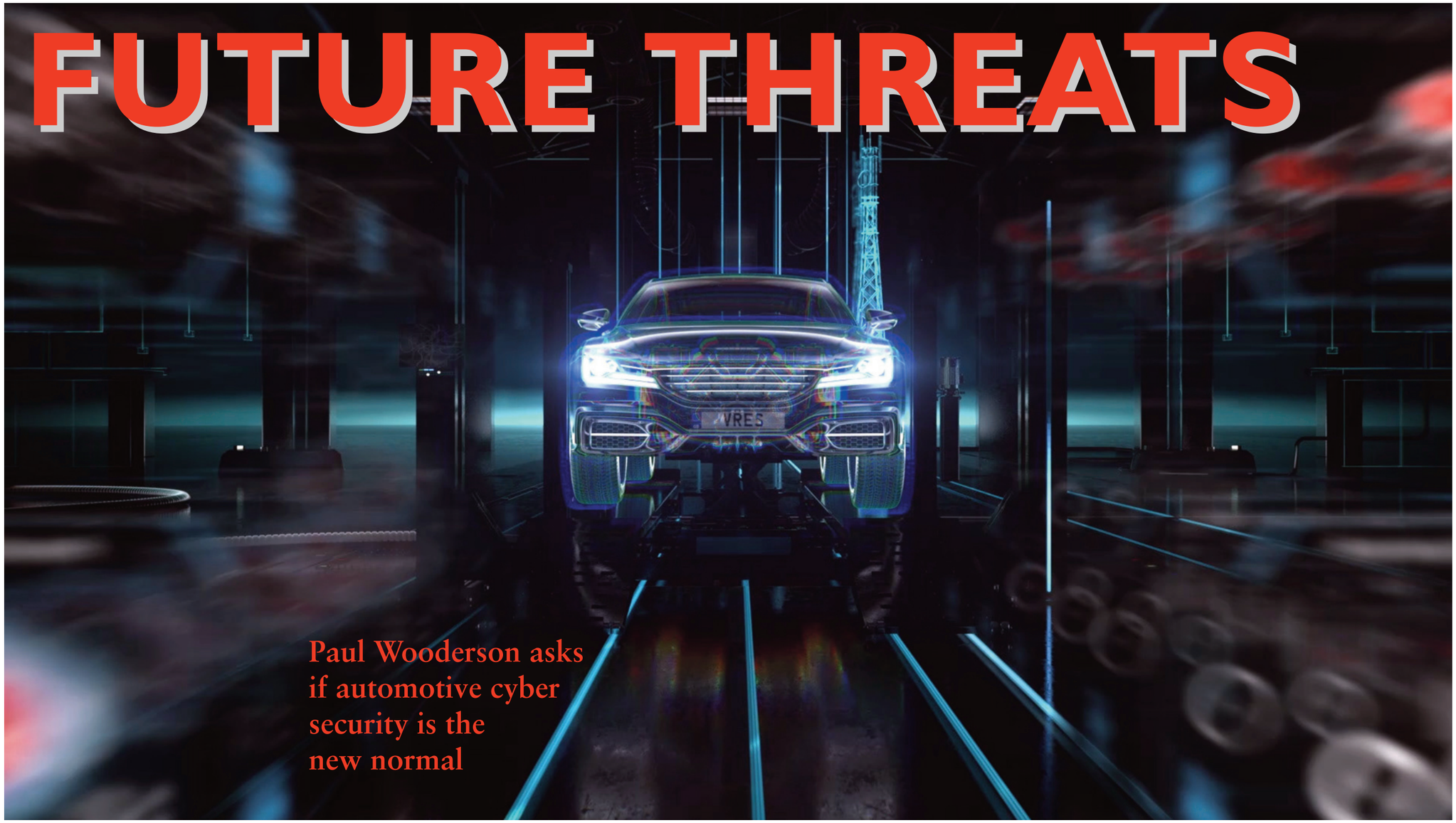
VEHICLE electronics

The monthly magazine for automotive electronics engineers

SAFETY & SECURITY

FUTURE THREATS



Paul Wooderson asks if automotive cyber security is the new normal

As of July 2024, the United Nations Economic Commission (UNECE) for Europe's WP.29 regulations on cyber security, encapsulated in UN Regulation No 155 (R155), have become mandatory for all vehicles produced in several signatory countries, including the EU and Japan.

The full implementation of these regulations has been a long time coming, and their official arrival marks a significant milestone as car makers work to protect their vehicles. Fortunately, the necessity for automotive cyber security is widely recognised across the industry, with the publication and widespread adoption of the international standard ISO/SAE 21434.

In recent times, the conversation has shifted from justifying the need for cyber security to determining how to implement the requirements effectively at scale. The industry must avoid reducing cyber-security measures to a simple checklist-based compliance activity, and instead ensure that cyber-security risks are properly managed in the face of an evolving threat. But this brings its own challenges, particularly in a sector already suffering from a shortage of skilled cyber-security professionals.

Beyond compliance

Many vehicle manufacturers have now successfully navigated at least one cycle of cyber-security approvals under the new regulations, establishing baseline processes to meet compliance requirements.

While initial compliance efforts have laid some solid foundations, the topic of cyber security remains a relatively new field of automotive engineering, with some understanding and capability still needing to be built.

The automotive industry faces a pressing challenge; adherence to regulatory standards while simultaneously increasing maturity and advancing robust cyber-security measures.

Scaling up cyber-security activities requires a multifaceted approach. Technological advancements must be paired with procedural and cultural shifts within organisations to prioritise cyber security, not just as a compliance issue but as a core element of vehicle development and operations. But this is particularly difficult due to the growing volume of vulnerabilities reported each year.

Many new products and methods to address aspects of vehicle cyber-security risk are appearing on the market, for example intrusion detection, hardware security features, and tools for verification and validation. A key difficulty moving forward is finding effective methods to evaluate and validate the myriad of new cyber-security options available on an objective basis.

The industry is now developing more detailed guidance for stakeholders, including several standardisation activities within ISO and SAE, such as ISO/SAE PAS 8475 and ISO/SAE TR 8477, which focus on cyber-security assurance and verification and validation.

Another critical issue is maintaining a vehicle's cyber-security capability after it's been released. Once a vehicle is in production, manufacturers are still obligated to protect it against new risks, but the required R&D resources are often reallocated

towards the development of new models, potentially leaving a critical gap in ongoing cyber-security management.

Cost of safety

There's no question that maintaining cyber security over the lifespan of a vehicle is expensive. Manufacturers must build systems to monitor vehicles, and detect and respond to attacks, all of which require significant investment.

In traditional vehicle sales models, such additional engineering costs may be typically absorbed into the price of the vehicle itself. But it still isn't clear how these costs can be re-distributed within alternative ownership models such as smart mobility and shared vehicles. It also raises the question of who is responsible for cyber security on existing vehicles and how to maintain an acceptable level of protection while managing the long-term costs.

It has been proven that even the most advanced cyber-security measures used in other industries, such as IT, are fraught with risks and problems when it comes to providing robust, long-term protection. The recent global IT outage, linked to the roll-out of a software update from cyber-security firm CrowdStrike, highlights how difficult it is to implement effective security without introducing vulnerabilities.

No price can override the need to ensure people's safety with cyber-security regulations. Unlike a hacked computer or smartphone, a compromised vehicle poses a direct threat to human life. The worst-case scenario of a cyber attack on a vehicle could result in injury or death, making cyber security a critical aspect of vehicle safety.

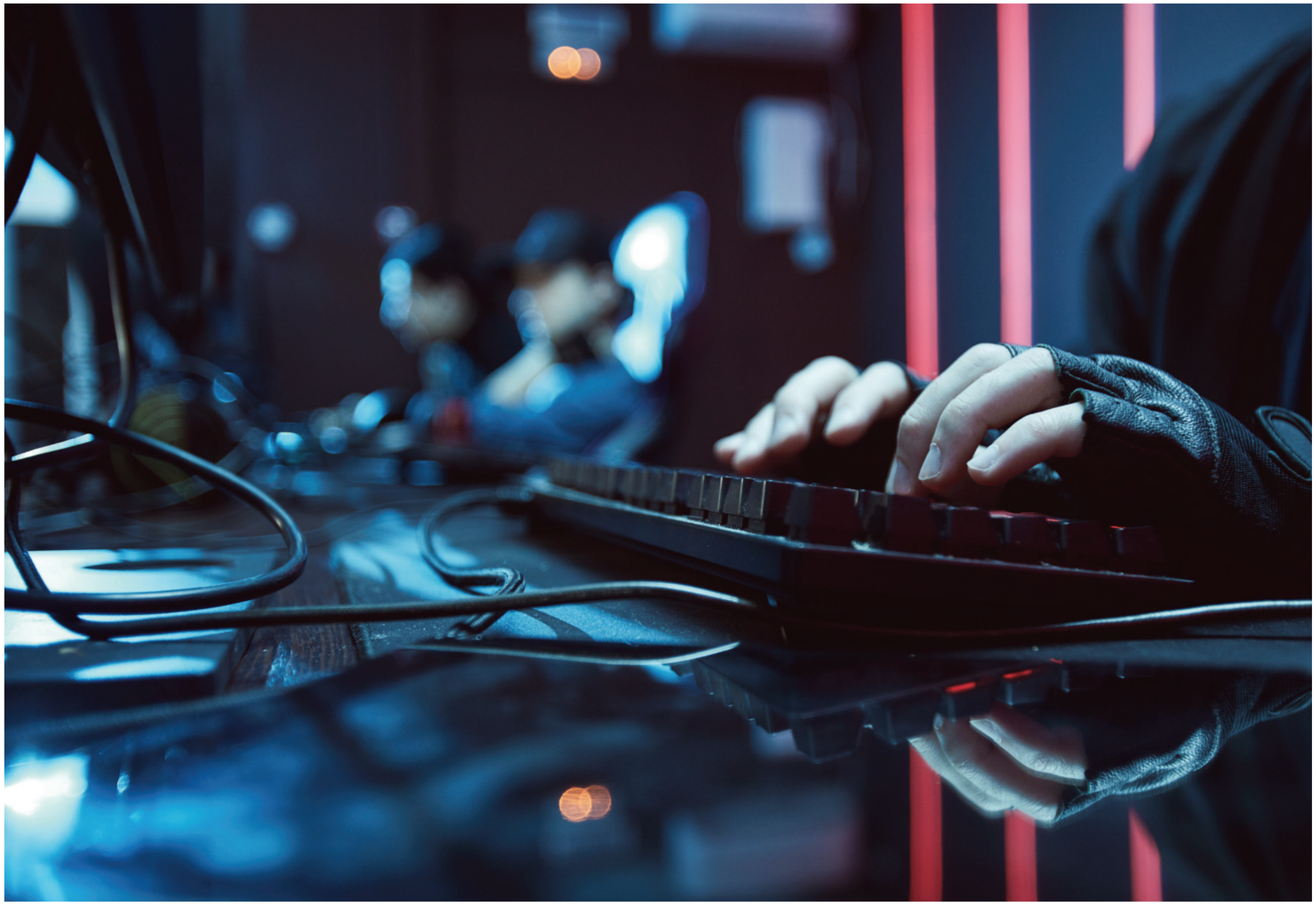
To mitigate these risks, the industry must invest in procedural and technical options, and develop rigorous testing methods to validate them thoroughly. The true challenge lies in determining the appropriate level of rigour for development and testing, and deciding when enough has been done to be confident in a vehicle's security.

As well as the emerging standards in this area, engineering, test and assurance methods are being developed to enhance risk management, identify vulnerabilities more effectively and ensure vehicle systems are robust and resilient against potential threats.

Limitations

As the automotive industry embraces artificial intelligence (AI) and other technologies, it must also address associated cyber-security risks. AI-based technology, which is being increasingly used in automotive applications, such as automated driving, driver assistance and battery management, introduces vulnerabilities. The industry must anticipate how attackers might exploit these systems and develop countermeasures accordingly.

Automated driving systems in vehicles rely on increasingly complex systems to make safety-relevant driving decisions, and any compromise in this capability could have serious consequences. The industry must consider how cyber attacks might exploit weaknesses in these systems to influence these decision-making processes and whether they could be compromised to cause accidents.

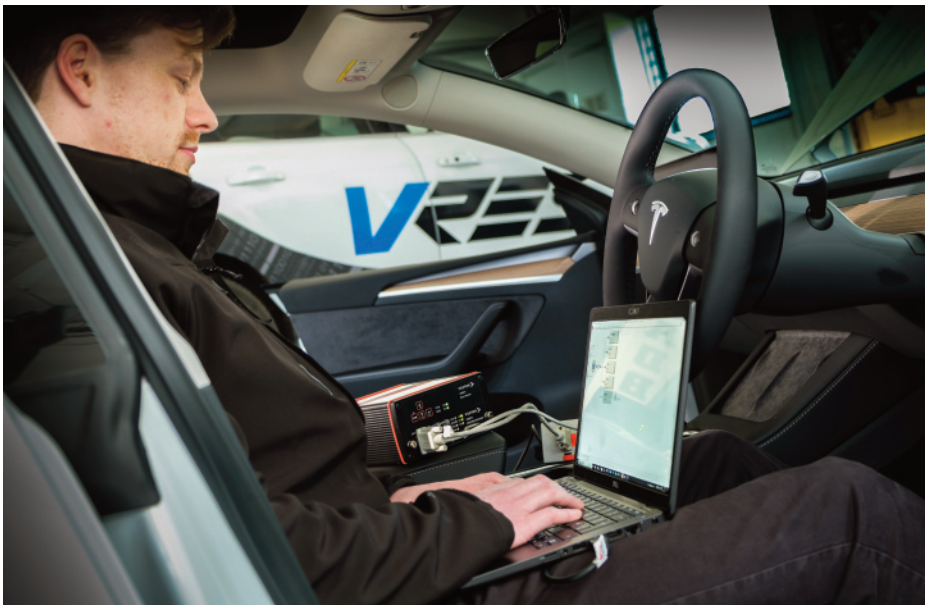


Ensuring the safety of vehicles with robust cyber-security frameworks

Remote operation, where an operator controls a vehicle from a distance, can also be susceptible to security vulnerabilities. Securing the communication link between the operator and the vehicle is crucial, especially if this connection is made over the internet or other long-range communication methods. As the industry moves towards greater connectivity and automation, understanding and mitigating these newly emerging risks are key.

The advent of quantum computing presents another looming hurdle. Quantum computers, once fully realised, could be used to break many of the cryptographic algorithms currently used in vehicle systems. The typical lifetime of a vehicle is much longer than for many other technology products, so there is a significant chance of practical quantum computers becoming feasible while today's vehicles are still on the roads. It is therefore imperative to explore post-quantum cryptography techniques and how these can be implemented in automotive systems to make sure vehicles remain secure across their

SAFETY & SECURITY



Securing connected and autonomous vehicles

lifespans.

Given the extended lifecycle of today's vehicles – commonly amounting to decades – this is a critical issue that must be addressed now to safeguard future safety. Both the ISO/SAE 21434 international standard and the UNECE R155 regulation play key roles in guiding manufacturers to manage cyber-security risks and implement certified cyber-security management systems throughout the vehicle lifecycle.

Learning

The automotive industry can learn valuable lessons from other sectors as it builds its cyber-security infrastructure. The aerospace industry, for instance, has a wealth of experience in cyber security. While some of its methods may be too costly for automotive applications, there is valuable knowledge that can be taken, adapted and implemented.

But not all options from other industries are directly applicable and transferable.

The automotive sector presents unique constraints, such as the need for methods that can be scaled across millions of vehicles, implemented across different entities within the supply chain, and fit within the cost and resource limitations inherent to the industry.

The scarcity of competent cyber-security professionals is a cross-sector challenge, and the automotive industry must invest to develop the right skills. This involves working closely with educational institutions to ensure cyber security is integrated into engineering-based learning. This will help prepare the workforce of tomorrow and secure the skills needed to tackle future problems.

New normal

Cyber security cannot be viewed as a one-time compliance activity, but as an ongoing commitment that starts at the beginning of vehicle development and continues throughout its lifespan. It's not just a technical challenge, but requires organisation-wide support and a fundamental commitment to public safety, calling for continued vigilance and innovation.

The future of cyber security in the automotive industry is complex and requires a combination of technical innovation, cross-sector collaboration and cultural change within organisations to get it right. The goal has to be to make sure technology can protect, detect and respond to threats efficiently and effectively.

While there are misconceptions about the ease or difficulty of achieving effective cyber security, it's clear the industry must strive for continuous improvement. With an ever-evolving threat landscape, there is no such thing as perfect security, but doing nothing is not an option.

The road ahead is difficult but it provides the route for an exciting and creative journey, offering opportunities for engineers to make a significant impact on the safety and security of future vehicles.

Looking to the future, the automotive industry must remain vigilant and committed to adapting constantly to new threats and technologies. By creating a culture to address cyber security properly and investing in the right skills and resources to enable that, the industry can ensure vehicles remain safe and secure in an increasingly connected world.

Paul Wooderson is chief engineer for cyber security at Horiba Mira