FROST & SULLIVAN

50 Years of Growth, Innovation and Leadership

AN INSIGHT ON CYBERSECURITY COMPLEXITIES AND INITIATIVES IN THE AUTOMOTIVE INDUSTRY

Byron Messaris & Krishna Jayaraman

A Frost & Sullivan
White Paper

www.frost.com

TABLE OF CONTENTS

Cybersecurity in the Automotive Industry—an Introduction

The Evolution of Connected and Autonomous Vehicles

The automotive industry is evolving at a scale and pace not seen since its inception.

Over 100 years ago the Ford Model T ushered in the era of personal car ownership. Today, the successes and failures of a century of research and development (R&D) have inaugurated a new era of connected, autonomous, shared and electric vehicles.

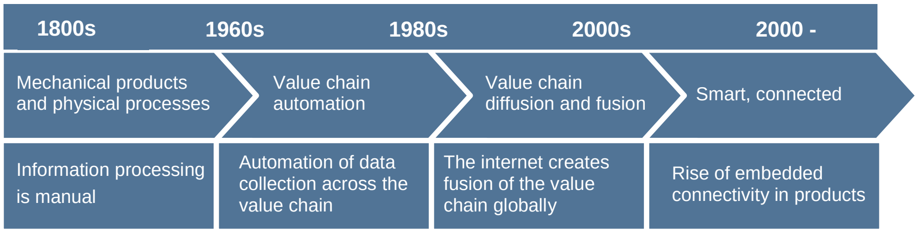
In an already connected world, it is easy to imagine highways where vehicles communicate and interact with one another and their environments. Almost any vehicle can be connected in this way, provided it has either built-in connectivity technology or is equipped with it, enabling the vehicle to send or receive data to or from networks, other vehicles and the surrounding environment.

Frost & Sullivan posits that by 2025, 80% of new vehicles sold in Europe will be connected while in the United States, this number goes up to 90%.

The development of Internet of Things (IoT) technology is having an impact on the way the world economy and global value chains function. IoT's transformative power is found in the enormous amount of data that is generated by these devices and how this data can be harvested to drive efficiencies and enhance value.

IoT is a key development driving the rapid proliferation of the connected car.

Figure 1: The Rise of the Internet of Things



1800s	1960s	1980s	2000s	2000 -
Mechanical products and physical processes	Value chain automation	Value chain diffusion and fusion	Smart, connected	
Information processing is manual	Automation of data collection across the value chain	The internet creates fusion of the value chain globally	Rise of embedded connectivity in products	

Source: Adapted from HBR, M.E Porter, & J E Heppelmann, 2015; Frost & Sullivan

As legacy systems are replaced, the automotive and manufacturing sectors will be further transformed by the disruptive impact of IoT.

The product design of IoT-enabled devices has evolved faster than the security features inherent in them, leading to a gap between level of product development and security enhancement.

Securing the product throughout its lifetime will be a key challenge for companies but one that will ultimately result in more collaboration and innovation.

The Complexity of Changing Automotive Electronic Architecture

The vehicles of today are advanced in terms of their design, features and functionalities. Over the past fifty years, the car has transformed to accommodate a growing number of on-board systems such as wireless communications, infotainment, and driving assistance.

The complexity of the vehicle's electronic architecture is driven by increasing levels of production innovation and maximisation. The standard level of technology in vehicles is more feature-rich and affordable. Customer-demand for standard technology features drove a surge in the complexity of the vehicle's electronic architecture.

Today, vehicles contain more electronics and code than ever before. Connected cars generate data from at least 200 different sensors within the vehicle and can profile everything from the vehicle's location to the user's driving habits. Volume passenger cars have anywhere between 20 million to 30 million lines of software code, while in the more premium segment, that number can exceed 100 million lines, which are found across hundreds of electronic control units (ECUs).

The complexity of the modern automobile and its electronic architecture have increased its risk profile as these units are vulnerable to external exploitation and hacking. These vulnerabilities illustrate the importance of security solutions that strengthen both the digital and electronic systems of vehicles.

Cybersecurity in the Automotive Domain

Automotive security includes information technology security and car cybersecurity. While the advantages of wireless technologies are clear and abundant, every technology comes with inherent safety challenges. Software developers need to encrypt and safeguard remote interactions to prevent unauthorised access to vehicle systems.

Currently, the critical threat vectors are in-vehicle software, cloud services, physical and remote access, design platforms, as well as wireless systems like Bluetooth and WiFi.

Why Commercial Vehicle Security Requires a Unique Approach

Modern economies are wholly dependent on their transport infrastructure. As the trucking industry moves closer to complete connectivity and autonomous technology, data security and privacy will become top priorities.

Connected fleets bring large-scale commercial benefits but also several challenges for operators. While connectivity allows operators to boost the efficiency of their fleets through smart systems, it also leaves their fleets exposed to a range of cyber risks that can significantly damage their businesses. And these risks are not static and isolated. Cyberattacks on fleets are likely to be asymmetric with clear and unknown motivations for attack.

These attacks could be designed to sabotage business operations by reducing fleet operability and uptime; defraud operators through ransomware style attacks that are designed to affect a financial return for the attacker; or exert full control of the vehicle with the intent of causing harm, and even terror.

Commercial vehicles of all types, through their applications, have more complex operating parameters than passenger vehicles. Buses are high-capacity vehicles and trucks are high-payload vehicles. A gas tanker or a vehicle carrying hazardous materials across national or international borders has a much higher risk profile than a mass market sedan on a regular commute.

The risks of operations present a case for value-creating cybersecurity layers of protection for commercial vehicles should be a top priority for automakers. Furthermore, most of the potential cyber threats are still unknown and ever-evolving.

This reinforces the need for companies at either end of the value chain to build layered end-to-end cybersecurity systems for commercial vehicles to safeguard operations and protect people.

Case Studies of Security Threats to Commercial Vehicles

A variety of very high profile, public cyberattacks against automotive companies have occurred over the past few years.

Tesla and Jeep, for instance, have had their share of being the target of hackers. And while the primary intent of these attacks was to expose the vulnerabilities in their respective automotive systems and not cause harm, they created a very public awareness of the substantial known and hidden risks of connected vehicles.

Tesla and Jeep aren't the only automakers who have been targets. Many other automakers have been at the receiving end of hacks by security experts. Although, the security experts who executed the cyberattacks have kept the companies they've been able to exploit and hack, anonymous.

In 2016, a research team from the University of Michigan published a detailed report on its automotive intrusion activities, which involved hacking a 2006 Class-8 semi-tractor and a 2001 school bus. The team exploited weaknesses in the SAE J1939 Standard which is used in the internal networks of heavy duty trucks and buses in the United States. By exploiting the vehicle's standard network, the team was able to stage several attacks on different parts—the instrument cluster, the powertrain, and engine brake—of both vehicles. These three attacks were the most severe because they allowed hackers to increase and decrease the acceleration of the vehicle as well as disable the engine brakes.

The team underlined the extent of the risk and the vulnerability of these vehicles due to the use of a common standard. The outcome of the hack further demonstrated the intrinsic danger and vulnerabilities of the internal electronic structures of commercial vehicles.

The study reinforced the view that without the introduction of an “active adversary” in the design process of these vehicles, they would remain high risk targets.

Automotive Cybersecurity Industry Challenges

The rapid pace of technology and product introduction poses a challenge for new industries.

The challenge for automakers and suppliers, and the industry as a whole, is to ensure greater focus on security during the product and service development process.

This is because of the gap between the creation of new products and services, and the technologies designed to secure them. The time lag between the appearance of threats and creation of corresponding defences leaves these products and services vulnerable to attack.

Firms will need to bring greater security considerations into the development process from conceptualisation to delivery. This is of course technically and commercially challenging for companies. It requires driving investments in technical and commercial expertise, and also mobilising these resources over a period against an evolving threat landscape.

As passenger safety became a focal point in automotive design over time, so too must securing vehicles’ software and electronic systems. And while this will include the standard physical safety features typically found in vehicles, greater emphasis will need to be placed on protecting the security of any and all vehicle’s electronic and digital architecture.

Furthermore, given their lifespan, the production of connected vehicles will need to be future-proofed with the ability to apply necessary upgrades. Over-the-air (OTA) platforms, which include firmware (FOTA) and software (SOTA), are used by automakers such as Tesla to deliver software updates that enhance the operability and functionality of their vehicles.

OTA updates would offset the cost and reputational impact that car recalls have had on some automakers.

There are limitations to FOTA and SOTA. One of main trends in the cybersecurity landscape is providing protection against unknown, quantified and qualified threats. Keeping a vehicle's systems updated is an adequate solution for improving vehicle security (against known threats and bugs), operability and features, but does not account for a range of unknown threats. OTA updates offer only a limited level of protection against an infinite number of potential threats.

At a macro-level, challenges around expertise—both security and legal—exist. With the automotive industry racing towards an electric and autonomous future, the need to build solid legal and investigative frameworks to address cyber threats will increase.

Mapping the Cybersecurity Landscape in the Automotive Industry

The Automotive Security Landscape of Today

When it comes to cybersecurity, the automotive industry has not been quick enough to drive change and enhance their capabilities. Security developments have seemingly been driven more by external threats, and not by proactive internal innovation. However, this reactive environment is slowly starting to give way as the automotive cybersecurity industry expands, leading to the creation and launch of new products and services, enterprises, partnerships and acquisitions.

The increasing growth of autonomous and self-driving vehicles will propel automakers into a race against time to create secure systems solutions capable of capturing the opportunities that will come with this great shift in security needs and requirements.

Current Regulatory Frameworks and Public Sector Participation

2018 will be a watershed year for the public and private sector when it comes to enacting regulation and legislation on data and automotive cybersecurity.

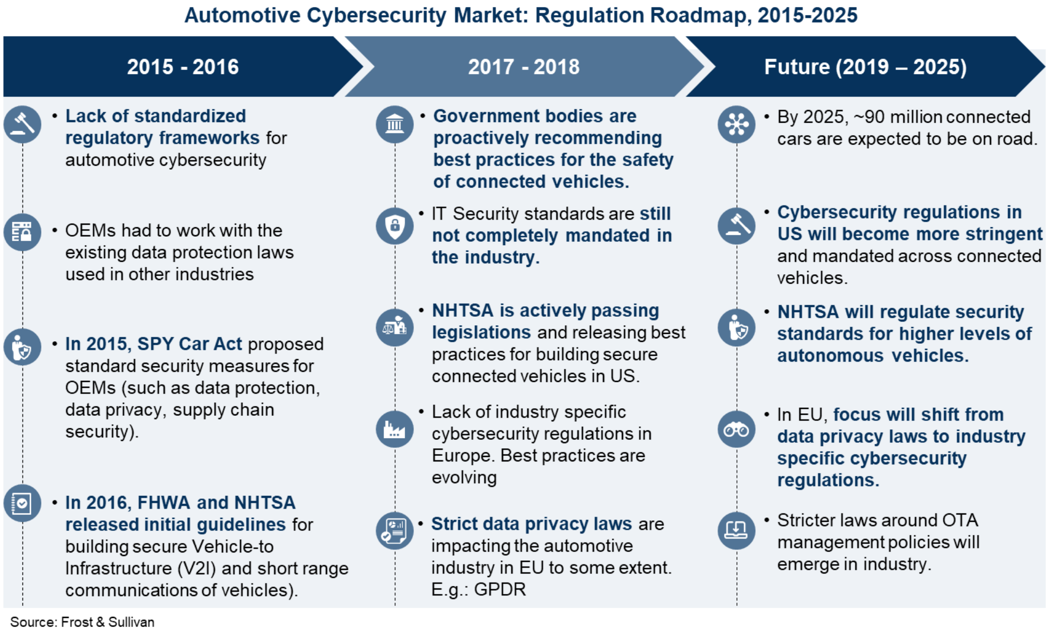
Creating best practices relies on ensuring that adaptation and adoption are considered. Each company will need to focus on adapting global best practices to their products and solutions. Simultaneously, the adoption of best practices requires effectively linking planning with implementation.

This is becoming more critical in the 21st century as the number of companies involved in the design and manufacture of electronic goods has increased, creating more complex supply chains and the therefore need for better risk management strategies.

Automotive vendors that take the lead in creating security standards and best practices will have the advantage of being the first to follow these standards. It will, at the same time, provide them with a platform to promote the experiential learnings of standard setting.

In the last 5 to 8 years, governments and regulators have sought to develop the necessary regulatory and legal frameworks to enhance standards and practices for connected and autonomous vehicles. While much has been done to rollout these frameworks there is still much a lot more to be done in creating regulatory frameworks which provide opportunities for better commercial solutions.

Figure 2: Automotive Cybersecurity Market: Regulation Roadmap



Automotive Cybersecurity Market: Regulation Roadmap, 2015-2025

2015 - 2016

- **Lack of standardized regulatory frameworks** for automotive cybersecurity
- OEMs had to work with the existing data protection laws used in other industries
- **In 2015, SPY Car Act** proposed standard security measures for OEMs (such as data protection, data privacy, supply chain security).
- **In 2016, FHWA and NHTSA released initial guidelines** for building secure Vehicle-to Infrastructure (V2I) and short range communications of vehicles).

2017 - 2018

- **Government bodies are proactively recommending best practices for the safety of connected vehicles.**
- IT Security standards are **still not completely mandated in the industry.**
- **NHTSA is actively passing legislations** and releasing best practices for building secure connected vehicles in US.
- Lack of industry specific cybersecurity regulations in Europe. Best practices are evolving
- **Strict data privacy laws** are impacting the automotive industry in EU to some extent. E.g.: GPDR

Future (2019 – 2025)

- By 2025, ~90 million connected cars are expected to be on road.
- **Cybersecurity regulations in US will become more stringent** and mandated across connected vehicles.
- **NHTSA will regulate security standards for higher levels of autonomous vehicles.**
- In EU, **focus will shift from data privacy laws to industry specific cybersecurity regulations.**
- Stricter laws around OTA management policies will emerge in industry.

Source: Frost & Sullivan

Ecosystem Mapping and Value Proposition of Key Market Participants

The automotive ecosystem is in a period of expansion. And the role of new partnerships between different segments in the automotive ecosystem is increasing.

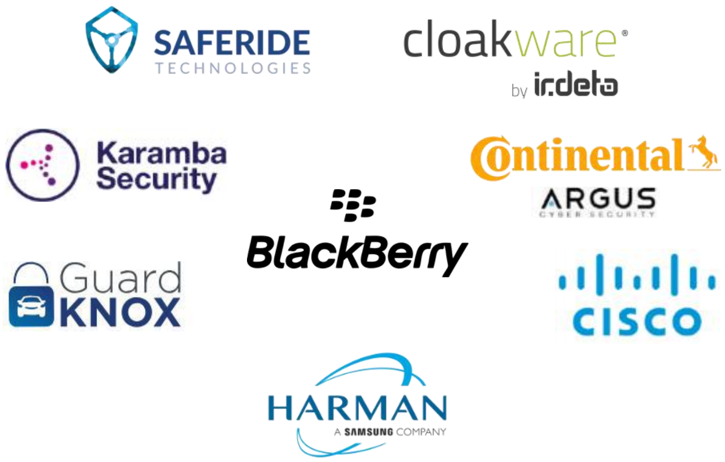
In the past, the automotive ecosystem comprised of only a handful of OEMs and suppliers. As the developers and manufacturers of vehicles, OEMs continue to occupy the top of the ecosystem with an evolving portfolio of suppliers.

New technological trends have spurred interest and investments in the automotive industry with mobility companies, software providers, telecom operators and wireless communications providers becoming enmeshed in the automotive ecosystem.

In the last five years, the industry has seen more automotive firms coordinating with the cybersecurity value chain, which is providing the necessary expertise to automakers who previously had little requirement for such know-how in product development.

The industry has also seen growing activity in mergers and acquisitions.

Figure 3: Company mapping of key market participants



Source: Frost & Sullivan

In 2016, Harman, a Samsung company, that boasts an impressive automotive supplier in Harman Kardon, acquired TowerSec, an automotive cybersecurity supplier.

In a similar acquisition in 2017, German automotive and tyre giant, Continental, acquired Argus Cyber Security.

TowerSec and Argus emerged from the expertise that has become a unique proposition of the dynamic Israeli cybersecurity industry.

The solutions offered by these companies rely on traditional perimeter protection technologies for market adoption but the differentiating factor for these companies, as start-ups, was that they offered expertise and technology that large corporations like Harman and Continental regarded as crucial to enhancing their future solutions and driving customer value.

Today’s ecosystem includes startups and established companies that are targeting to provide the next level of automotive security.

Pure-play cybersecurity industry participants include:

SafeRide Technologies, an Israeli start-up that went out of stealth mode at CES 2018, became the first automotive cybersecurity vendor to provide a security solution that protects connected vehicles against known threats using traditional cybersecurity technologies as well as unknown, “zero-day” threats using Artificial Intelligence (AI) technologies, such as machine learning and deep learning.

Irdeto, a Netherlands based digital platform security vendor pioneer. Irdeto protects over 5 billion devices and applications. Irdeto’s Cloakware™, offers a framework for protecting the digital assets of vehicles, including software and proprietary data, against tampering and data and intellectual property theft.

Near Future Outlook of Cybersecurity

Executives, shareholders, and customers are determined to see automakers develop end-to-end security in not only their products and services but also across the entire value chain from R&D to manufacturing and retail.

Frost & Sullivan’s research suggests that customers buying or using more connected and autonomous vehicles will begin to place greater value on an OEM’s reputation-driven values such as security and privacy.

Different Disciplines for the Implementation of Vehicle Security

In recent years different security techniques have been proposed and implemented for robust security of vehicles. In order to provide a robust security solution, it is recommended to combine multiple security disciplines.

Operational Profiling for the Discovery of Unknown Threats

An operational profiling mechanism is based on machine learning and deep learning technologies that build mathematical models that profile the vehicle’s baseline behaviour and identify operational anomalies through detection of deviations from the learnt baseline. Since this mechanism does not require familiarity with the threat profile, it allows detection of unknown threats and anomalies, and provides a valuable complementing layer to the conventional cybersecurity layer that focuses on detection and prevention of known threats.

Multi-Layer Security for Providing More Lines of Defence

Multi-layer security is a security concept that is built on cascading security defence layers around the core of a secured entity, eliminating a single point of weakness. The different security layers that are built around the core of a typical connected vehicle are the connectivity security layer, the software security layer, and the in-vehicle security layer.

Connectivity Protection for Controlling Access and Preventing Data Loss

Connectivity protection is the first layer of defence. Connectivity is the gateway between the vehicle and the outside world. This is the most vulnerable part of the vehicle. The protection of this layer includes various techniques and technologies such as strict access control to internal and external data sources.

Software and Digital Asset Protection to Prevent Tampering and Securing Sensitive Assets

Digital asset protection refers to the protection of software, and sensitive assets such as IP, digital keys or private information.

Cyberattacks that target the digital assets of the vehicle can include an attempt to tamper with in-vehicle software, scanning of the software for targeting vulnerabilities, scanning for internal digital keys to be used for unauthorized access and the copying of proprietary protected data.

Digital asset protection can be achieved by implementing mechanisms to authenticate the source and integrity of the software, encrypt data or use other mechanisms to prevent reverse engineering or unauthorized use.

In-Vehicle Network Protection for Securing Core Vehicle Operations

Protection of the in-vehicle network is vital because the network serves as the vehicle's core operations backbone. Cyberattacks targeted at this layer can include brute force attacks that block communications altogether by flooding the network, or more subtle attacks in which the attacker injects messages in a way that manipulates or removes control of specific in-vehicle subsystems. Operational profiling and access control can enable blocking unauthorised access and detection discovering anomalies that result from unknown threats. This type of protection can be implemented through the deployment on a single ECU on the network.

SafeRide – Case Study of a Multidisciplinary Cybersecurity Solution

Certain security solutions embrace a multidisciplinary approach by combining complementing security technologies to provide maximum security. An example of a multidisciplinary solution is the solution offered by SafeRide Technologies—vSentry™— offering anomaly uncovering and cyber threat prevention for connected and autonomous vehicles.

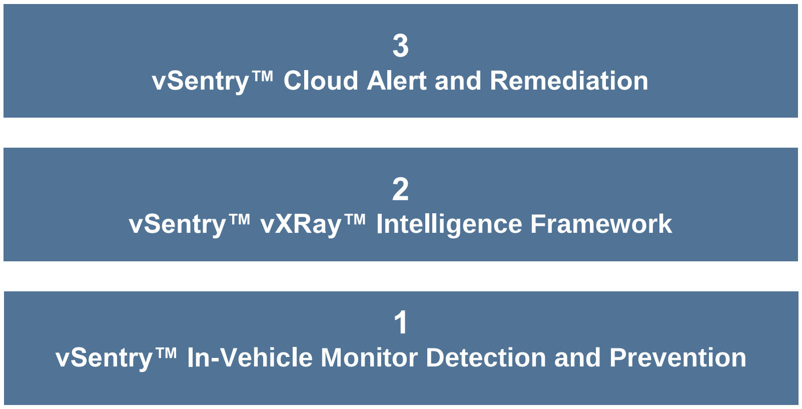
SafeRide's solution combines out of the box cybersecurity technology for the prevention of known threats with AI based operational profiling for anomaly uncovering and response for unknown zero-day threats.

The anomaly uncovering technology used by SafeRide's solution harnesses the vast amount of data and hints from seemingly disconnected sources of in-vehicle data to uncover unknown anomalies and threats to provide value-add insights systematically and at scale.

An additional advantage to SafeRide's solution is the multi-layer security approach: by securing the connectivity layer, the software and digital asset layer and the in-vehicle network layer, the software and digital asset layer and the in-vehicle layer, using a granular inbound and outbound protection scheme, the protection system provides more lines of defence for maximum protection with no single point failure.

SafeRide's solution includes 3 main software security suites.

Figure 4: SafeRide's solution


3
vSentry™ Cloud Alert and Remediation
2
vSentry™ vXRay™ Intelligence Framework
1
vSentry™ In-Vehicle Monitor Detection and Prevention

1. An in-vehicle, multi-layer security suite, including connectivity protection, digital asset protection, and in-vehicle network protection

2. An anomaly uncovering suite based on vehicle operations profiling with AI, machine learning, and deep learning technologies for detection of unknown threats and operational deficiencies

3. A cloud enablement suite for central alert and remediation through Fleet Management System and Security Operation Centre integration

SafeRide’s anomaly uncovering suite is the product of lengthy testing and training of an AI engine based on thousands of hours of recorded operational data across dozens of different vehicle models, and driving conditions.

The core capabilities that SafeRide relies on for development of the solution includes the most sought after of skills in the development of next generation solutions for the automotive industry – cybersecurity and artificial intelligence data science.

The Future of Automotive Security in an Insecure World

Connectivity heralds a seismic shift in how vehicles operate and provides enormous customer experience, safety, and commercial and societal benefits.

As we hurtle toward a more connected future these benefits will only grow, providing a landscape that will be rewarding for innovators.

The future of automotive security however remains in a growth stage. A new class of companies are beginning to launch and scale solutions that will provide the necessary layers of protection to ensure that connected vehicles’ potential is not undermined by security vulnerabilities.

In the next five years, solution maturity and complex connected cars and autonomous vehicles use cases will allow automakers to lower cybersecurity costs and, thereby, encourage wider adoption of secured solutions.

The future will bring a new level of risk thinking when it comes to connectivity. Frost & Sullivan believes that the core focus will be on implementing design processes that can produce robust products to meet market demands, best practices, and regulation.

Frost & Sullivan further anticipates that companies will look to future technologies that provide enhanced mitigation driven solutions addressing symmetric and asymmetric cyber threats.

The key to growth and prosperity in the automotive cybersecurity industry will depend on how effectively automakers and suppliers adopt suitable and scalable cybersecurity technology and systems in their designs, and culture.