STRATEGY ANALYTICS
Celebrating 25 Years of Insights

Keeping Vehicles Safe in the Age of Software

August 2021

Report Snapshot

Car makers are facing a cybersecurity challenge unmatched by any other industry. Yet cyber security resource needs still not fully understood. As automotive OEMs struggle to get on top of the challenge, an automated solution is necessary as a force multiplier to help OEMs cope with exponentially increasing complexity.

Contents

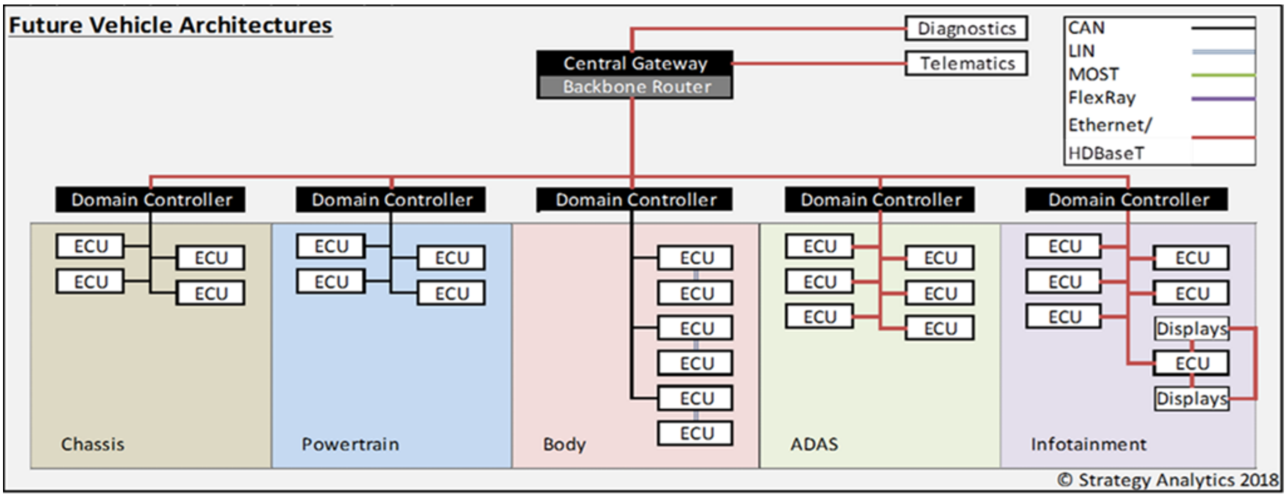
1. Software on wheels – A new threat landscape

The digitalization of the automotive industry has introduced the concept of the software-defined vehicle. From safety systems to powertrains and infotainment, software stands at the core of vehicle development and design.

Software now stands at the core of vehicle development and design.

The rise of software has coincided with the proliferation of vehicle connectivity and the pursuit of automated driving. Managing and securing software is suddenly a requirement for vehicle design with requirements quickly being defined by regulators.

Connectivity is increasingly leveraged by carmakers to enable automated driving and car-sharing applications along with traditional vehicle diagnostics and supporting fleet electrification. More onboard software has dictated a reconsideration of vehicle electronic architectures and cybersecurity.



The evolution and expansion of vehicle software have contributed to the growing complexity of the supply chain with automakers increasingly dependent upon hundreds of new firmware suppliers large and small, to a stage where regulators demand manufacturers have software updating capabilities and detailed cybersecurity plans.

With more software auto makers face growing complexity of the supply chain

The United Nations Economic Commission for Europe (UNECE) adopted a new international automotive cybersecurity regulation in June 2020. The regulation establishes performance and audit requirements for cybersecurity and software update management for new passenger vehicles sold in the European Union and dozens of other countries.

UNECE's WP.29 is the name of the World Forum for Harmonization of Vehicle Regulations. The new WP.29 regulation took effect in January 2021 and applies to passenger cars, vans, light trucks, and buses, and other light vehicles. It applies to 54 countries that participate in the 1958 UNECE Transportation Agreements and Conventions but also calls for compliance from any non-participating countries (i.e. U.S., Canada, and China) seeking to sell into those 54 markets.

Additionally, the Biden Administration in the U.S. issued Executive Order 14028 in May of 2021 which stated: "The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace."

While the order applies initially to "all Federal information systems," it also calls for greater collaboration between the Federal government and the private sector. Among its provisions, the Order emphasizes the implementation of automated systems for detecting cybersecurity vulnerabilities.

The new WP.29 regulation orders implementation of automated systems for detecting cybersecurity vulnerabilities.

The Federal government and international authorities have good reason to be concerned. The average vehicle comprises millions of lines of software code; multiple operating systems, multiple networks, and processors; a complex and expansive supply chain; a years-long product development cycle; a regional and global regulatory landscape; and existential liability exposure.

Car makers are not only responsible for their cybersecurity measures they are accountable for the cybersecurity stance of a complex supply chain. Last year's attack on German body component supplier Gedia exposed this reality as a ransomware attack resulted in supply chain disruptions to multiple automaker customers of the firm and a release of sensitive data.

Car makers are accountable for their own cybersecurity measures as well as for the cybersecurity stance of a complex supply chain.

Shortly before the Gedia attack, the FBI had sent a warning to prominent companies in the automotive industry warning that malicious hackers and state-sponsored actors were targeting the sector. CNN reported at the time that the FBI warned of efforts by hackers to compromise industry computer systems taking advantage of network vulnerabilities. The report noted that attacks had already resulted in ransomware infections, data breaches and the exfiltration of personally identifiable information, and unauthorized network access.

The wave of software-defined systems and the introduction of connectivity more than two decades ago exposed the industry's vulnerability. Hackers from around the world, including state actors, are attacking cars, the organizations making them, and their suppliers.

Suppliers expressed a variety of concerns regarding OEM responses to cybersecurity:

1) Regulation – Suppliers say: “OEMs are not on top of this at all, including little understanding what this means in detail pertaining to their product design. This includes WP.29 as well as various ISO regulations that are even specific to cybersecurity. Advisory regulations coming in as part of other specifications such as on EV charging where there are cybersecurity requirements hidden away in the specification. This will drive a lot of change over the next 3 – 4 years.”

Suppliers say: “OEMs are not on top of this at all”

2) Security – Suppliers say: “It’s a new domain for Tier1s and they are used to responding to OEM RFQs. But T1s do not understand what exactly OEMs are trying to achieve as the OEMs are not always clear about the strategy as well as the details. There is a gap between what OEMs are requesting and what they mean or need (a lot of OEMs do not know how to express their requirements properly, hence requires a lot of interpretation by T1).”

Suppliers say: “There is a gap between what OEMs are requesting and what they mean or need”

3) Human skills (access to talent) – Suppliers say: “Cybersecurity is a small world and automotive is not what the best people first think of, i.e. they’d rather work for big tech companies.”

4) Monetizing cybersecurity – Suppliers say: “T1s are constantly challenged already and squeezed for value by OEMs. The separation of hardware and software poses a major business model challenge to T1s, and security is seen as part of BOM rather than an enabler of future revenue streams or higher-level service. T1s do not position it properly and OEMs don’t focus on making security central to their messaging, i.e. consumers won’t want to use connected services if not perceived safe (e.g. banks very much worked security into their online customer services and messaging, none of this happens in Automotive today). At the same time, nobody seems to want to pay for security including OEMs and their consumer customers (e.g. banks offer free antivirus software).”

Suppliers say: “OEMs don’t focus on making security central to their messaging to consumers”

1.1 Digital cyber risk is still not prominent enough

Topping these issues is the perception of cybersecurity as purely a cost center. Rather than being viewed as loss prevention or cost mitigation, it is seen as an obligatory activity from which it is difficult to derive a resalable value proposition to the consumer.

Said one supplier: *“OEMs see cybersecurity as something they must do and a cost, rather than a platform for enhanced services and value. It will take a few years and probably some serious attacks before they fully wake up*”.

Another recent quote also includes this question from the security team of a top 10 OEM: *'Why would we need to encrypt the vehicle network? "*

Strategy Analytics spoke to multiple carmakers and supplier executives to get a sense of the psychic landscape and the organizational measures that have been taken to confront the cybersecurity threat. What emerged from the interviews is an ominous picture of an evolving response still unequal to the task of protecting cars from attack.

According to one supplier, quoted earlier, *"OEMs are willing to pay for safety but have not brought that mindset to security yet. Hence, they always seem to want it for free (for safety nobody wants to be the guy who saved $5 on BOM and cost lives, but for security, they still fail to fully grasp the risks and potential damage). This will require 3 – 5 years of education and possibly some serious attacks"*

One supplier said: "OEMs are willing to pay for safety but have not brought that mindset to security yet"

"It costs money to write secure code, and OEMs are willing to do it in functional safety (e.g. working in AUTOSAR), but not for the wider vehicle. There is no OEM today that has aligned everywhere with regards to all the functions and a security strategy of the organization."

The result is the creation of a highly vulnerable mobile device with dozens of attack surfaces created by an organization comprised of multiple product design teams dedicated to individual vehicle functions or components. While every industry must mitigate cybersecurity vulnerabilities across their enterprise, distribution, and manufacturing operations, the automotive industry is uniquely tasked with orchestrating a cybersecurity strategy across a landscape of hundreds of hardware, software, and service partners.

For automakers, safety is the highest priority. The time has arrived to equate safety risk with cyber risk. This is the most important conclusion.

For OEMs, the time has clearly arrived to equate safety risk with cyber risk.

"Our greatest cybersecurity challenge derives from managing our product development process," said a senior cybersecurity executive for a large, global auto manufacturer. For this car company, managing cybersecurity has meant the creation of multiple teams, working in and across multiple geographies, and coordinating with multiple internal cybersecurity layers of management.

1.2 Cybersecurity resource needs still not fully understood

Just as it takes a battalion of electrical, mechanical, and software engineers to design a vehicle, increasingly there are multiple platoons of engineers seeing to the cybersecurity demands of the process as part of existing teams or as discrete organizations unto themselves. The problem is, as we have been told by car makers and their suppliers, “vehicle complexity grows exponentially, while internal resources expand linearly.”

The automotive industry is struggling to get a handle on the requirements of cybersecurity. No longer reliant on so-called security by obscurity, automakers have been forced to take an organized and systematic approach to take on cybersecurity concerns.

> **“There is exponential rise of risk due to the digital transformation of the industry.”**

1.3 UN Cybersecurity and Software Update Regulation Changes All

The aforementioned UNECE WP.29 regulations that took effect in January require that measures be implemented across 4 distinct disciplines:

- **Managing vehicle cyber risks;**
- **Securing vehicles by design to mitigate risks along the value chain;**
- **Detecting and responding to security incidents across vehicle fleet;**
- **Providing safe and secure software updates and ensuring vehicle safety is not compromised, introducing a legal basis for so-called “Over-the-Air” (O.T.A.) updates to onboard vehicle software.**

Thanks to this regulation and standards including ISO 21434 cybersecurity is now a requirement for vehicle design and carmakers have set aside board-level positions of responsibility and division-level commitments of resources.

Yet perceptions of OEM inaction persist. Said a Tier 1 supplier executive: *“The IT team understands large data and cloud… let them handle it”* is a typical OEM attitude. The problem with leaving it to IT departments is that they are used to building/bolting on security around (existing) hardware and software. But WP.29, in effect, requires software to be designed securely from day one which is a completely different requirement and challenge.”

Slow-moving OEMs appear to be the exception. Multiple interview subjects identified emerging OEM leaders taking on cybersecurity. Chief among those named as in the forefront of taking on cybersecurity concerns were General Motors, Ford Motor Company, BMW, Daimler, Toyota, and Volvo.

2. Key OEM Challenges

Car makers and their suppliers described the challenges to Strategy Analytics in stark terms. Said one OEM: *"There is an exponential rise of risk due to the digital transformation of the industry."*

"We face an operational challenge in new development while having to monitor what occurs after the start of production, along with new vulnerabilities emerging in older car lines. In addition, we have regulatory challenges, the need to comply with WP.29, for example".

Every car maker has confronted the cybersecurity challenge in its way. Said one: *"We have gone through this safety issue and built internal departments to handle regulation and compliance, but there is an existing gap regarding an adequate supply of executives with cybersecurity knowledge."*

Every car maker has confronted the cybersecurity challenge in its own way

Said another: *"There are different models. Some OEMs place this responsibility under a CISO (Chief Information Security Officer). OEMs have always had IT or corporate security, but this new domain is product cybersecurity. Now they need to decide how to handle this."*

2.1 No established OEM model for responsibility

Even after multiple vehicle cyber-attacks, many car companies have remained in a reactionary mode as far as cybersecurity is concerned until very recently. "Each OEM needs to utilize the resources they have. This means they use standard IT processes, e.g. build an exact asset inventory of all software they have to create a secure development lifecycle. Each OEM needs to adapt these practices to their automotive engineering environment. If I am a vendor, I need to look at what their processes are."

"There are huge variations not just between OEMs, but also between projects within a company. OEMs tend to take systems from T1s and hence place responsibility onto the T1. OEMs still just specify the architecture and leave most details (including security) to the T1."

The executives on the front line of the cybersecurity struggle say visibility into the supply chain is a complex issue. Understanding exactly what software is in all the ECUs is a challenge by itself, as there are many car lines, models, versions, and geographies.

OEMs say they are upping their cybersecurity requirements for suppliers. For leaders in the space, cybersecurity is not an afterthought. It is an essential element of every design and product management process. It's not optional.

For leaders, cybersecurity is not an afterthought but an essential element of every design and product management process. It's not optional.

WP.29 regulations now require a complete application software inventory. This is not possible without the legal consent of the T1 and could amount to illegal reverse engineering of the code. It is a complex challenge requiring a complex solution.

3. Benefits of an automated solution

For much of the industry, it is a numbers game – piling on personnel. Increasing headcount, though, is typically an inadequate response to the demands of the task at hand. Auto industry cyber executives say the tip of the vulnerability spear lies in product management and the only means for meeting the challenge is augmenting human resources with software tools and automation.

Cybellum is one such platform and automation provider. Cybellum's solution is to combine several layers of protection to the key point of vehicle vulnerability: the product design and development process. Because of the complex nature of the automotive supply chain, carmakers are forced to orchestrate and integrate software from multiple sources using multiple operating systems. This is where Cybellum enters the picture.

The process of certifying code continues to become more complex. Cybellum seeks to break that process into discrete steps delivered via an integrated platform.

"Ensuring that software is secure is the biggest challenge," said a senior cybersecurity executive for a car maker. *"We can't see the source code. We have to trust the suppliers".*

> **"Ensuring that software is secure is the biggest challenge. We have to trust the suppliers"**

The urgency of this task has meant that many car makers have sought to address the issue with internal resources. As standards and regulations have come into play, though, the industry has inevitably turned to third-party solution providers.

Cybellum's portfolio includes:

- Automatic detection of vulnerabilities in binary code
- Compliance with security policies, standards, and regulations
- Continuous coverage throughout the vehicle lifespan
- Proactive mitigation of relevant risks with OTA (over-the-air) integration
- Deployable offboard solutions, cloud, and on-prem

3.1 Addressing Key Vulnerability Sources

At the heart of Cybellum's offering is the focus on supply chain protection – the point that carmakers and suppliers agree is the key source of most vulnerabilities. The objective is to deliver a vehicle that can operate safely.

The wave of software-defined systems and applications and the introduction of connectivity more than two decades ago began to expose the industry's vulnerability and hackers from around the world, including state actors, are attacking cars – including the organizations making the cars and their suppliers.

The introduction of connectivity, anti-lock brakes, electronic stability control, and power steering opened the door to the prospect of remote vehicle control along with everything from denial of service to ransomware attacks. The car has officially arrived as a ripe and tantalizing target for hackers.

The car has officially arrived as a ripe and tantalizing target for hackers.

3.2 Cars are now awash with attack surfaces

It wasn't just the introduction of cellular wireless connectivity to cars that created vulnerabilities. The industry came to see that cars were awash in attack surfaces from embedded cellular modems and wireless tire pressure sensors, to Bluetooth, satellite connections, Wi-Fi, and RDS-TMC reception.

Tackling cybersecurity now requires an organizational commitment encompassing the entire vehicle development effort and impacting the entire supplier ecosystem. The recognition of the nature and scope of this challenge has spurred automakers to engage cooperatively in a manner not previously seen. As one auto exec remarked: *"We compete on product. We don't compete on cybersecurity."*

The cooperative spirit gave rise to the Auto-ISAC which was initially only open to automakers, but that ultimately welcomed suppliers and now has dozens of members encompassing all corners of the supplier value chain along with auto and truck manufacturers themselves.

The key to the Auto-ISAC's success has been the need for car companies to come together to combat vehicle vulnerabilities. Of necessity, carmakers must interact with and are exposed to the varying cybersecurity hygiene of every partner supplier. Significantly, each supplier has multiple OEM customers, which requires the industry-wide sharing of intrusion incidents information.

Said a Tier 1 supplier executive: *"In the next 1 – 2 years OEMs will start to implement cybersecurity operation centers, as they become more sophisticated.*

In the next 1 – 2 years OEMs will start to implement cybersecurity operation centers

This will also involve the concept of digital twins which will allow mass testing and avoid the expensive way of testing on real vehicles."

Just as they have been applied in other areas of product management and design, digital twins are being applied to cybersecurity. Digital twins are core elements of the Cybellum solution.

4. The Digital Twin Solution

Saying that "Vehicle security is challenging" is an understatement - It requires relevant talent, processes, and technologies to be accomplished. Most importantly, it's not a one-off effort, but rather a continuous process that spans the entire vehicle lifespan (recognized by the latest industry standards and regulations).

Vehicle security must be a continuous process spanning the entire vehicle lifespan

Digital Twins - A virtual replica of a FW physical product (a device or a component of it) - are increasingly used to introduce transparency and speed to decision making and to determine the impacts of changes without the cost, time, and risk needed to be spent on analyzing the actual system.

Digital Twins are already used in the automotive industry, so it makes sense to apply the Digital Twins concept to automotive cybersecurity as well. An automotive manufacturer can generate an updatable "cybersecurity twin" of a vehicle's software and use it for multiple security-related tasks, including:

1. Aggregating all underlying software metadata in one place, including versioning and configuration - C-BOM/S-BOM.
2. Creating a normalized output that can be shared with approved 3rd parties.
3. Simplifying enforcement of cybersecurity requirements and policies across the supply chain.
4. Managing vulnerabilities lifecycle including detection and traceability that identify dependencies on a specific system and/or vendor.
5. Providing a single platform by which all vehicle systems can be continually assessed for security issues pre-and post-production.

By analyzing product binary code, Cybellum's Cyber Digital Twins platform reveals the underlying composition and characteristics of automotive software, including S-BOM, package versions, licenses, hardware architectures, operating systems, configurations, control flows, API calls, encryption algorithms and keys, hardening mechanisms and more – generating an accurate digital replica - a Cyber Digital Twin - of every vehicle component in the backend.

Cybellum's Cyber Digital Twins platform generates an accurate digital replica - a Cyber Digital Twin - of every vehicle component in the backend.

Subsequently, the platform runs threat analysis and monitoring solutions to detect and remediate potential cyber risks and regulatory/policy violations.

4.1 Cybersecurity concerns have transformed the industry radically in the past 10 years

For OEM product development teams, cybersecurity concerns have spurred the creation of dedicated teams focused on individual function areas such as API security, embedded security, and connectivity security. For most car makers cybersecurity within the product-management is separate from enterprise security. It is a dedicated internal function usually operating out of multiple global locations and with compartmentalized teams and functions.

Not all suppliers and OEMs are entirely on board. Said one supplier: “Many OEMs are preparing their strategy for WP.29 but are not communicating this whilst requests for quotes are going out to suppliers for SOP 2024 vehicles. The worst-case could be OEMs unable to sell these cars as these may not fully meet WP.29 requirements.”

Perhaps more important, though, is OEMs need to recognize that cybersecurity ought not to be seen as part of the unit cost of the vehicle but rather attributable to the security or IT budget. Today, OEMs are looking for a “single pane of glass” through which they can view the functioning of all products and systems and identify and mitigate vulnerabilities before they emerge.

4.2 Incident Response

The ideal operating environment for the carmaker is to detect and mitigate vulnerabilities before they manifest. The recent past, however, has shown that OEM responses typically start with an incident which can come in various ways (an email indicating a problem, system detecting a breach); a triage effort to determine severity: an impact assessment; and the creation of an incident response team to deploy a fix.

Today OEMs still typically respond to an incident, rather than detect and mitigate vulnerabilities before they manifest

Having proper cybersecurity protocols and systems in place is essential for being able to rapidly trace vulnerabilities and intrusions to their source. Cybellum’s platform is intended to fulfill this function as well. Its Cyber Digital Twins enables on one hand proactive security monitoring of vehicles and components post SOP so that relevant risks can be mitigated ahead of any exploit, while on the other hand, when an incident occurs, it facilitates root-cause analysis and impact assessment across assets in development and on the road.

5. Conclusions

The automotive industry faces an existential crisis in meeting the challenge of mitigating the risk of mounting cybersecurity exposure. Standards setting bodies and regulatory agencies have risen to the task with new standards and new regulatory requirements. The industry is still in the early stages of adopting and adapting to these new protocols.

The point of greatest industry vulnerability is the complex automotive supply chain and years-long product development process. Car makers have taken on hundreds of cybersecurity executives, created new divisions and operational teams, and escalated cybersecurity response to a board-level responsibility.

Still, the scope of the threat continues to grow – requiring external support from third parties. The complexity of vehicle design continues to grow, contributing to an exponential growth in the complexity of the cybersecurity task. This is where solutions such as Cybellum can be applied to identify and remove risks and vulnerability in the vehicle design process and preserve cybersecurity throughout the life of the vehicle.

Suppliers and OEMs universally acknowledge they need help in meeting regulatory and standards-related requirements, integrating hardware and software from hundreds of suppliers, and sharing incident data and resources with competitors. Meeting the cybersecurity challenge is a shared endeavor across the complex automotive supply chain. Thankfully solutions like Cybellum are available to act as a force multiplier to address this industry-wide effort.

6. Analyst Contacts

The authors of this Report can be reached at:

Roger Lanctot, can be reached at **rlanctotkendall@strategyanalytics.com**, or by using the following telephone number: **+1 617 614 0714**.

Andreas Koehler can be reached at **akoehler@strategyanalytics.com**, or by using the following telephone number: **+44 1908 423 631**

Get help from Strategy Analytics

Working with Strategy Analytics gives you the knowledge you need to succeed.

Understand your customer

Business opportunities abound. But which ones are right for you and your customers? Which will give you the advantage?

Optimize your user experience

Optimize your product to give your users the best experience and you the market advantage.

Analyze the market

Understand the size of the opportunity and where your product fits using our unrivaled knowledge and world-class data analysis techniques.

Explore your future

Working with us will focus you. With our insight and forecasting expertise you'll make confident strategic decisions that drive success.

Please contact us at custom@strategyanalytics.com with any questions and for further details and solutions on how we can work with you on creating a custom solution to address your specific needs.