McKinsey&Company

Shifting gears in cyber security for connected cars

Advanced Industries February 2017

Authored by:
Corrado Bordonali
Simone Ferraresi
Wolf Richter

ABSTRACT

Connectivity has the power to transform but is not without its risks. In automotive, cyber security threats are real, OEMs are facing a unique level of challenge given the increasing complexity of the product (e.g., the exploding amount of ECUs, lines of code, and level of connectivity), an extremely fragmented supply chain, and the integration of all these systems that can compromise any specific countermeasure.

The solution in such a context comes only with a **holistic approach that acts on two fronts.** On the first front, the specific cyber security solutions address the design of the product, how it is developed, and the maintenance and response architecture. On the second front, OEMs must focus on the automotive environment at industry level (e.g., to establish effective cooperation programs), with the regulatory bodies, and on the final users who are directly involved as active players in protecting their cars (e.g., keeping software updated). In parallel, the approach should prioritize at all times innovation, user experience, and product cost competitiveness.

A product can only be secured if it is **designed with security in mind. "Quick fixes"** on top of an unsecure product do not only add complexity, cost, and sometimes weight, but **can also be easier to circumvent** as they may not structurally solve the vulnerability challenge (e.g., on architectural issues) – **conducting so-called "penetration tests" can only be a temporary solution.** Other industries (e.g., aviation, trains, critical infrastructures) started adopting a set of different **design approaches – not just technologies –** as the **silver bullet solution simply does not exist.** Future car design must be "cyber security native," integrating security solutions into the earliest stages of product design.

Secure design, while necessary, is not sufficient to guarantee full product security over time. **Solutions are effective only when they are consistently implemented** and the components – both software and hardware – used to implement the design are optimally quality controlled. This requires a sound and managed development process, including reinforced collaboration between the product security team and the company IT security team. Accordingly, **OEMs must implement and enforce strict development guidelines** effective in minimizing the chance of bugs and unintended software security gaps and in making it easier to modify or patch as necessary. In doing so, they should manage security as a single extended product-enterprise perimeter in order to boost synergies on the protection effectiveness and cost sides.

Security is not static and OEMs are learning that what is considered secure today most probably will not still be secure in the **future threat landscape. Over-the-air (OTA)** updates have recently become available on some cars (although only for limited portions of their software) and they are **clearly a "must have" of any connected system.** This functionality allows for quick responses to attacks and enables manufacturers to eliminate particular vulnerabilities before they are exploited. These benefits come with a price, as OTA implementation costs are high on both the car and the back-end infrastructure. Hence, **effectiveness and area of focus need to be carefully traded off,** considering the design and the development approaches for each module and at the overall system level.

OEMs as the sole customer interfaces and most often final system integrators **are the ones to ultimately deal with the integration risk and would bear responsibility** for ensuring that secure, stand-alone systems do not become vulnerable when connected. This means that on one side they need to **ensure that security practices are consistently**

implemented within the full value chain (i.e., including suppliers) and on the other side they should **play an active role in shaping the future industry standards** (as related to regulations as well as to best-practice guidelines).

Many industries (financial services, oil and gas, aviation) have established **alliances,** which allow open sharing of threat intelligence and vulnerabilities both internally among OEMs and suppliers and externally with relevant entities (e.g., regulatory bodies, media) within a secure space. As this approach makes it easier for each participating company to benefit from the collective threat intelligence and also facilitates the prompt response to novel threats, **automotive companies should further move in this direction adding to the first alliances that are being set.**

OEMs' best efforts in cyber security will be effective only insofar as **users** are aware of the importance of cyber security, take responsibility for their **role in security,** and avoid behaviors that can facilitate the threats. Recent research shows that despite the resonance in the automotive community, **current user awareness of cyber risks for cars is relatively low.** As end users will represent a wide range of security savvy, **it will be critical for OEMs to consider a variety of tools that increase user awareness.**

Although an increasing number of **regulatory bodies** globally is starting to focus on the cyber security aspects of automotive, the definition of formal rules is still at a preliminary stage. For the mutual interest of setting effective and realistic guidelines, **OEMs and relevant suppliers** should engage in a **continued collaborative discussion with regulators** (e.g., leveraging on the industry alliances) to provide the most complete set of inputs.

Bringing it all together, to minimize waste in terms of investments and time to market and to preserve the security of their products, OEMs should follow a specific process to **select and implement the adequate set of cyber security solutions** for each subsystem of each vehicle, via an holistic approach in

- **Assessing** the acceptable **risk profile** (i.e., the areas/components that are vulnerable to cyber threats from a customer, company and regulator perspective)
- **Understanding** the cyber **risk exposure** (i.e., the gaps versus the risk profile on organizational processes and capabilities from product resiliency standpoints)
- I**dentifying the solution set** (i.e., trading off the different solutions versus cost, time to market, user experience, product innovation)
- **Defining** the **implementation** strategy and **key enablers** needed (i.e., designing the implementation road map, sourcing capabilities, managing relationships with key stakeholders).

Shifting gears in cyber security for connected cars

Digital is changing the way companies across all industries do business. From production to sales to customer care, all aspects of the value chain across industries are affected by digital's potential, and the automotive industry is no exception. With opportunity, however, comes risk; and one of the risks of digital in automotive is the threat of a purposeful attack on the organization, the production, and the product.

CYBER ATTACKERS AND THEIR AUTOMOTIVE TARGETS

Today's cyber threats come from a wide array of potential attackers, which range from highly sophisticated state-sponsored adversaries to insiders helping external hackers or initiating their own incursions. They can be suppliers seeking advantages in negotiations or litigation, criminals looking for customer data, disgruntled employees or former employees, or competitors attempting to disrupt business. The attackers' targets are broad, and attackers can hit OEMs on three different, overlapping fronts:

The organization. A first battlefield – in common with most large corporations – involves the automaker's organization, where attackers' targets include intellectual property, strategic plans, employee and customer information, and other sensitive data.

Production plants. A second battle takes place in highly automated production plants where increasing levels of connectivity in the wake of the Industry 4.0 revolution expose a growing number of product manufacturers to further cyber risks as interference with production activities (e.g., damaging equipment and parts up to harming the integrity of the end product).

Connected cars. A third battle is happening on the connected-car front. In this battle-ground, hackers work to get access to cars' internal networks and, step by step, hijack the electronic control units (ECU) that control everything from infotainment and the climate control system to the engine, brakes, and steering.

The cyber security risk for connected cars is of particular importance. A breach that allows external access to a car's network cannot only compromise the privacy of a driver's data, but there is much more at stake; the cyber security threat in connected cars is a matter of life and death and threatens the industry's road map towards autonomous vehicles. Within current car architecture, where connections between systems follow more practical considerations rather than security ones, an attacker can potentially gain access to all aspects of the car including its vital systems. Hackers have the ability to attack systems to steal personal data, compromise infotainment/navigation GPS units, and neutralize vehicle alarm systems. What is worse, they can threaten drivers' physical safety with the potential to hijack the systems directly related to the car's safe operation. Not only does this kind of attack risk the lives of drivers and pedestrians, a successful attack would likely have dramatic consequences for the industry. Recent incidents have shown how quickly regulators, customer advocacy groups, and the court of public opinion can act if an attack on an electronic device is instrumental in causing the death of a person. A single cyber attack that exposes a systematic weakness rather than a user error will cause a critical setback to the connectivity efforts and progress made over the last years.

OEM READINESS AND UNIQUE CHALLENGES

Recent McKinsey research suggests that most OEMs consider cyber security a real concern. When it comes to proactively addressing the threat, however, less than half have operational cyber security units. Compared to other industries, automotive – namely OEMs and suppliers – are behind the maturity curve when it comes to cyber defense capabilities. Even among those with up-and-running cyber security units, less than half of OEMs and suppliers are confident in the capacity of their units to fully handle the threat. In addition, in many cases these units are shells of what they ought to be to address the aforementioned threats through capabilities like, for example, red teaming and blue teaming[1].

Part of the challenge of being fully prepared to address the cyber security threat in automotive is the industry's unique set of challenges:

Increasing complexity. The number of potential points of attack in a car is already high enough to make a full-scale defense a tall order. In the coming years, the number of an OEM's potential targets is expected to dramatically increase. One reason is the number of vehicle nodes (ECUs) keeps increasing to support the demand for additional functionalities. Today, an average vehicle may contain around 30 units, and complex vehicles can be comprised of up to 100 units. Adding to this the fact that each unit embeds dedicated operating software, the multiplier effect can mean that a single vehicle's systems contain hundreds of millions of lines of code[2] – a complexity that even the best programming methods will not be able to produce without vulnerabilities.

Multiple stakeholders. The automotive industry is characterized by having established one of the most fragmented supply chains of all industries. Development of countermeasures is made difficult by the multiple players involved, each producing to their own standards and patch specifications. OEMs are faced with significant integration risks and have so far not established sufficient integration testing capabilities to mitigate this risk. The 30 to 100 control units per vehicle can be supplied by more than 20 different suppliers. A high number of components developed and manufactured by multiple suppliers means an increased risk of compromised cyber security. Specifically, regardless of the strength of the individual components, poor integration can result in a vulnerable network of interconnected elements. Recent successful cyber attacks on cars leveraged the peculiar vulnerability that can result from an interconnection in which individual components are reasonably secure on their own but the door to cyber attacks gets opened when integration under diffuse authority leads to a compromised system.

Supplier vulnerability. OEMs are used to getting support from their suppliers in areas like quality or product innovation. Unfortunately, when it comes to cyber security, suppliers appear to be even less prepared than OEMs. In our recent survey, only 10 percent say cyber security ranks high on top management's agenda compared to 35 percent of OEMs, and around 45 percent consider the cyber security of external partners (i.e., subsuppliers) as being important to very important, compared to more than 60 percent of automakers.

1 One group of security pros – a red team – attacks an asset, and an opposing group – the blue team – defends it (originally, the exercises were used by the military to test force-readiness)

2 More than last generation fighter jets

SECURITY ISSUE AREAS TO BE ADDRESSED BY THE INDUSTRY

In our investigation of the cyber security issues facing the automotive industry, we understand the matter as two sides of a single coin. One side is the product itself and the design, development process, maintenance and operations procedures that make up the product's life cycle. The other side is the role of the operating environment, i.e., the automotive industry, the government/regulatory bodies, and, especially, the users and the driving environment. Each side poses multiple questions that players must consider in shaping their approaches to cyber security (Exhibit 1).

Exhibit 1

Automotive cyber-security questions

Space of solutions		Environment	
Design	▪ Which is the most effective set of design principles? ▪ To what extent can design/architecture by itself ensure security?	**Industry**	▪ Who is the ultimate owner of cyber security for the final product? ▪ How to orchestrate cooperation along the supply chain?
Development process	▪ What is the role of development processes and standards in strengthening product security? ▪ What is the required level of collaboration between the product security team and the company IT security team?	**Government/ regulatory bodies**	▪ What is the role of governments and regulatory bodies? ▪ What would be the relationship with industry players?
Maintenance and response	▪ How to preserve the product security along its life?	**Users**	▪ What is the role of user behavior to achieve cyber security? ▪ What is the impact/trade-off on user experience?

How to trade off solutions versus cost and time to market?

In finding the set of answers that make the most sense for their particular organizations, OEMs must consider at least three implications and how to optimize the solutions across them:

Cost, i.e., the effort required to develop and implement each solution, plus and versus the cost of maintaining security over time (continuous updates, no software is forever secure), plus the eventual recovery cost related to risk of cyber failures – all of those related to the maturity level of the target vehicle.

Time to market, i.e., the implementation timeline of each solution versus the product lifecycle/ maturity stage and its impact on market competitiveness (e.g., possible delays in releasing a new generation of a vehicle).

Strategic approach, i.e., how the set of solutions selected fits with the strategic direction of the company and its position with customers: internal know-how vs. relying on supply chain partner, be more aggressive or more reactive in mitigating threats, technical maturity of the customer base and what they are willing to allow, importance of security as part of the brand image, etc.

Failing to choose the optimal cyber security strategy can result in serious recall/brand damage costs when an OEM is underprotected and wasted money and time in the development and go-to-market plan when overprotected.

STRATEGIC SOLUTIONS TO AUTOMOTIVE'S CYBER SECURITY CHALLENGES

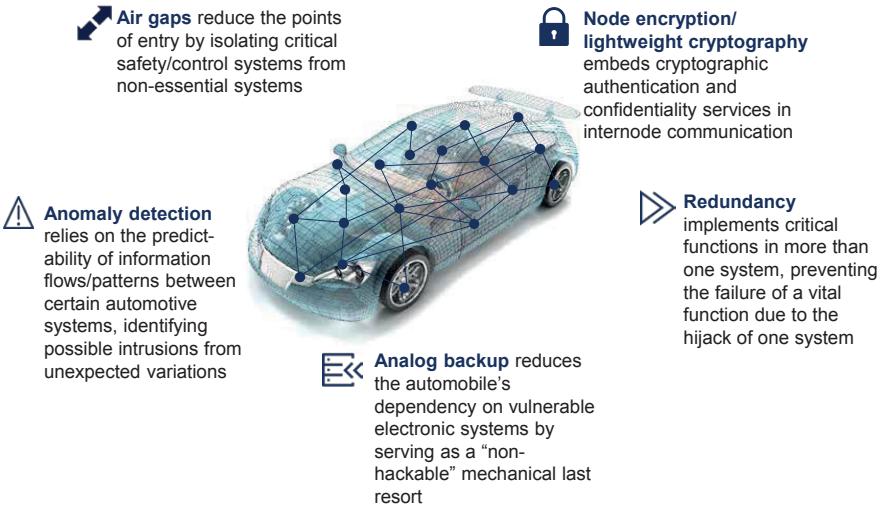
In the following, we discuss six specific cyber security solution areas for strategic consideration; the first three – design, development, and maintenance – concern the lifecycle of the product, while the other three – OEM-supplier alliances, end users, and government agencies – address the ecosystem in which OEMs are operating.

Design

There are several approaches that other industries have successfully deployed to increase security of their products. We identified five design patterns that we have seen working effectively each with its own set of trade-offs that OEMs need to evaluate (Exhibit 2):

Exhibit 2

Design solution patterns



Air gaps. The concept here is to isolate the most critical systems from the most exposed networks within the car. Confirmed by its application in aviation *(see Text box 1: "Cyber security in action"),* physically separating the infotainment/connected devices from the critical control systems (e.g., braking, steering) enhances security and reduces the risk of external attacks that threaten the physical safety of the driver and passengers. While air gaps are considered a key element of a secure architecture, they can have a significant impact on cost if the original system had a high level of integration (more cables, connections, controllers, etc.). Hence – for the current generation of vehicles – this approach should be applied only to core critical systems for vehicle and user safety.

As redundant parts create additional cost and increase the potential cost of the solution, the target level of architectural separation (e.g., full air gap, hybrid air gap with single interconnection, unique network without gaps) should be optimized based on the specific vehicle characteristics.

A hybrid solution limits to a single point the interconnection between the critical and non-critical networks, providing it with additional protection features (e.g., node encryption, "read-only" data flows, deep package inspection).

A more lightweight alternative is to keep only the information separate by implementing encryption at the nodes and overlay the bus infrastructure with a virtual private network.

Text box 1:

Cyber security in action: Design solutions from aviation and power generation

Given that automotive is in its cyber security infancy and that there is no identical industry, automotive leaders should look at best practices from a variety of industries as they begin to draw their own cyber security road maps. The security solution of "air gaps" – protecting the most critical systems by isolating them – is a prime example of how automotive can look to how other industries have successfully implemented cyber security measures.

Air gapping in aviation. Isolating the passenger entertainment network from the navigation systems is considered a key element of a secure architecture in aviation. In recent cases for long-range civil aircrafts, US regulatory bodies (Federal Aviation Administration and Government Accountability Office) established that mere firewalls were insufficient to protect air traffic control systems from potential attacks coming from passengers' network, and are actively pushing for air gaps.

Detecting anomalies in power generation. Power production plants are increasingly Internet connected. The sector is not as regulated in this area as aviation is but the threat is no less real. The sector is characterized by the large amounts of "precyber" legacy technologies, and the cost of total upgrades would be prohibitive. Network monitoring can recognize and intercept the exchange of anomalous data – whether or not the data is already known to be a worm, virus, or other threat – , recognize changes in the operating pattern of the systems, and proactively provide a defense against external attacks on plants' control systems in ways that firewalls or encryption systems might not be able to.

Node encryption. Embedding cryptographic authentication and confidentiality services in internode communications is another defense against cyber attacks. This security solution has been widely adopted in automation systems – from building automation to next-generation energy production systems – but it is not yet fully established in the automotive space. Managing, updating, and continuously verifying cryptographic keys over a very large installed base is a complex endeavor. However, it could be effectively applied to select key interconnections between critical and non-critical systems (provided that the involved components/networks support encryption).

Looking forward, the automotive community (OEMs and tier-1 suppliers) is currently discussing the possibility of developing a new generation of CAN-BUS architecture with native support for encryption. Multiple solutions are technically available at the moment; however, the industry has not yet agreed on a new, shared standard.

Redundancy. In cyber security, redundancy is the concept of linking critical functions to more than one system and eliminating single points of failure. If one system is hijacked by an external attacker, other systems are still able to support the function the hijacked system was responsible for.

Redundancy is an expensive solution given the additional weight and cost of the redundant components. It is standard practice in the aviation and defense industries, where safety

factors often require two to four redundant systems. It is starting to be introduced in the automotive space with safety-critical systems, for example, by installing double drive-by-wire steering ECUs. Experience from high-speed train control systems highlights an additional critical element coming from CPUs redundancy. In order to switch from a CPU to its backup, we need to know in real time when the CPU is compromised (not simply shutdown), and it is clearly a responsibility that we could not pass to that CPU by itself. In such context, redundancy (double or triple in best practices) is primarily a way to detect an anomaly and requires all redundant CPUs being active and a complex "voting" algorithm to establish CPUs' role and priorities in taking safety decisions, e.g., activating brakes.

Analog backup. Maintaining or reintroducing some basic analog control in an increasingly digital environment is another security solution. One function may be supported, for example, by three redundant electronic control systems and a mechanical one.

This non-hackable, last-recovery approach is beginning to be introduced in automotive for safety-critical systems only on the drive-by-wire/electric actuation solutions, to maintain basic turning/braking ability even on power shutdown. Specifically, indirect electronically-actuated steering systems have a backup mechanical drive for the steering wheel. Even in the remote case that a hacker manages to take control of all the ECUs, he or she will never be able to take control of the direct mechanical drive. Implementation requires that the analog backup system has the "final authority" to overwrite the digital unit signals – another relevant principle from a safety perspective that needs to be balanced and traded off.

Anomaly-based intrusion detection. Adopted in power generation, complex network monitoring and data traffic analysis detect intrusions and performance anomalies, alert operators, and trigger countermeasures *(see Text box 1: "Cyber security in action").* Unlike the other cyber security solutions, there are no known applications of anomaly detection in automotive yet, but opportunities exist to retrofit automotive systems with this function. As in power generation, the information flows/patterns between certain automotive systems is predictable.

One example of anomaly detection in automotive might be on tire pressure monitoring systems (considered to be vulnerable to remote attacks). Since the system should transmit fairly consistent pressure readings, a data monitoring system would allow threat detection, sending out alerts and triggering countermeasures (e.g., disconnecting the attacked system from the core network).

Many cyber countermeasures can become a vehicle of attack, and anomaly detection does not make an exception, as it can be leveraged with the purpose of blocking the normal functionality of a system by just injecting some "noise" in the network, aimed to raise continuous alarms.

Anomaly detection can also be supported by a stronger identification of the traffic "author". A recent paper aims to demonstrate that it is possible to "fingerprint" an ECU via the tiny timing errors on the CPU's clock. The advantage of this technique is that it relies on the clock skew[3], which is nearly impossible to replicate.

3 See https://www.google.co.uk/search?q=clock+skew&oq=clock+skew&aqs=chrome..69i57j0l5.1552j0j4&sourceid=chrome&ie=UTF-8

In addition to these approaches, there are also some new emerging solutions. One example for open networks with distributed nodes (e.g., vehicle-to-vehicle connectivity) is blockchain. A blockchain is a cryptographic or encoded distributed ledger, comprising a digital log of transactions that is shared across a public or private network. Although the development of blockchain technology is still in an early stage, new business cases are likely to evolve as soon as the technology further evolves and proves feasible. In the case of car cyber security, blockchain could allow an efficient validation (in terms of security, speed, convenience and cost) of transmitted information from a network of distributed nodes as opposed to a central administrator. In an autonomous driving environment, this would allow the reliable validation of the flow of position, speed, and route data exchanged between vehicles and traffic infrastructures (vital information to avoid collisions) and increase the data security. In addition, the potential application of blockchain in cars could also be utilized for automatic micropayments through smart contracts.

Development

Design by itself needs to be secure as a base, but it is not enough by itself to guarantee full product security over time. The design solutions described above are only effective when they are consistently implemented and the components – both software and hardware – are used to implement the design are quality controlled; this requires a sound and managed development process. Strict development guidelines are effective in minimizing the chance of bugs/unintended security gaps in the software and making it easier to modify/patch as necessary.

Development guidelines, certified developers, and regular reviews and security tests will improve software quality. Suppliers must be held to a common standard, helping avoid situations in which suppliers neglect security in their efforts to save cost. In any case, each component received from a supplier needs to be quality-assured and security-tested. This will not only impact sourcing processes but also transform the organization, with (among others) procurement executives having to learn to negotiate cyber security features as rigorously as other component features.

In aviation, strict development guidelines apply to all electronic elements and their related integration in the aircraft systems *(see Text box 2 “Development guidelines in aviation”).*

Text box 2:

Development guidelines in aviation: A cyber security cost-optimization lesson for automotive

The DO178 guideline in aviation standardizes code modeling, documentation, and testing and was recently integrated by DO326 with specific indications for interactions between safety and cyber security during integration phase.

Benchmarks from aviation show up to 70 percent additional development cost for certified aviation software vs. standard current automotive software. Considering this cost, it would be important for players in the automotive sector looking to establish development guidelines to find the level of requirements/depth of guidelines appropriate for this sector and decide which nodes/ECUs should be prioritized.

The argument could be made that safety requirements in aviation are different from those in automotive. A navigation/communication system failure, for example, has a different impact on a plane flying at 950 km/h at 12,000 meters versus on a car driving at 50 km/h on an even road. However, the impact of a major cyber security attack on the automotive industry could be just as severe if we consider the number of potentially affected cars, which could result in a disaster on a massive scale if all cars of the same popular brand start to behave abnormally at once or if a single car is connected to dozens of other cars following it in self-drive mode.

Certified development should not only be applied to safety-critical software/modules (e.g., ABS, stability control). Instead, a systematic view of the risk that the individual component introduces into the system should be considered when deciding where to prioritize application of certified development. The certified areas must be cordoned off from the rest of the car systems and be connected only when needed through few and clearly defined access points. General development guidelines enforcing basic security standards must be applied to the full car.

In this context, it is also crucial to reinforce collaboration between the product security team and the company IT security team as cars become "endpoints on the enterprise network" for multiple purposes related to car connectivity (e.g., preventive maintenance, updates/upgrades, and digital remote services). For managing security as a single extended product-enterprise perimeter can boost synergies on the protection effectiveness side (e.g., through scaling up crossed controls, improving consistency in the level of protection, and ensuring faster coordination and reaction) and on the cost side (e.g., through preventing duplications and overlaps as well as fostering joint development of technologies and solutions).

Maintenance

Designing security solutions under rigorous development guidelines sets the foundations. However, security is not static, and OEMs are learning from software developers that keeping the ball rolling (and up to date) is just as important because what cyber security needs to protect against today won't be what the threat landscape will look like tomorrow.

The development timeline of a vehicle and/or its subsystems ranges from two to five years on average, hence any current cyber security architecture would be mostly designed for a set of soon-to-be outdated threats. All security solutions should include update features (both pre-emptive and corrective) capable of responding to the evolution of the threats.

Today, automotive OEMs are managing these update processes in a variety of ways. The first is a "traditional" approach, in which software is updated when the car is brought in for regular maintenance or service. Manufacturers may also send USB drives to owners. In this case, the owner is responsible for initiating the update (usually for critical issues/recall actions).

So far, a few OEMs are enabling continuous, over-the-air (OTA) software updating. This functions similarly to the way modern smartphone operating systems are updated about once a month. Financial services mobile applications are another example of OTA maintenance, where each update maintains the app's compliance with tight, ever changing certification protocols.

The benefits of OTA make it a cyber security must-have feature for automotive systems. Having this functionality allows for quick responses to attacks and enables manufacturers to eliminate particular vulnerabilities before they are exploited. These benefits, however, come at a price. The cost of implementing OTA updates is significant (e.g., establishing content delivery infrastructure, updating and testing the code, etc.), but recent research indicates that this cost is quickly offset by benefits over the product lifetime (just think of the cost and risk of a massive recall). Security of the update process/infrastructure is also very important as, otherwise, this would represent an additional (and preferred) remote attack surface (e.g., installing malicious patches, allowing external intrusions).

OTA is a crucial lever for quickly deploying software patches as a reaction to identified vulnerabilities or successful attacks. Efficient OTA updates can be an additional layer of system security on top of the intrinsic robustness of the initial architecture.

The elements of design, development, and maintenance described above pertain to the product side of the automotive cyber security question; the environment in which players operate is the other dimension to consider. In the following we will explore some of the ways in which automotive players are addressing the roles of the various stakeholders within the cyber security ecosystem.

OEM-supplier alliances

The traditional allocation of roles between OEMs and tier-1/2 suppliers lets OEMs design the end product and specify exactly what they expect the suppliers to produce. This model seems to be broken when it comes to cyber security as OEMs' specifications have so far only vaguely specified cyber security requirements and do not mandate the use of specific frameworks or standards. On the other side, suppliers so far have been hesitant to establish standards by themselves, as they fear risking their investment if the OEM eventually mandates a different one.

Reflecting on the role of the OEM as the master architect and the integrator of parts, OEMs would be in the better position to mandate a security architecture for their suppliers in the absence of cross-industry standards.

OEMs as the final systems integrators are the ones to ultimately deal with the integration risk and would bear sole responsibility for ensuring that secure, stand-alone systems do not become vulnerable when connected. This means that OEMs need to:

- Develop security integration testing capabilities
- Define standards for duty of care/negligence with respect to cyber security in cooperation with authorities and insurance companies
- Strive to agree on minimum standards on, for example, coding practices and documentation of security requirements in the specification.

One factor critical to success in cyber security is up-to-date knowledge of current threats and the effectiveness of mitigating solutions. Moreover, as such knowledge on threats and solutions is distributed along the fragmented supply chain, there is a need to support cross-industry information sharing, involving both OEMs and suppliers. Many industries (financial

services, oil and gas, aviation) have established alliances, which allow open sharing of threat intelligence and vulnerabilities among OEMs and between OEMs and others (e.g., regulatory bodies, media) within a secure space. This approach makes it easier for each participating company to benefit from the collective threat intelligence and also facilitates the prompt response to novel threats.

The automotive industry is still in the process of establishing secure, information-sharing alliances; one example is the Information Sharing and Analysis Center (Auto-ISAC), which launched in the US in late 2015 under the leadership of the Alliance of Automobile Manufacturers and the Association of Global Automakers, in cooperation with NHTSA and SAE. ISAC has been structured on the model of similar institutions in the financial services and the oil and gas industries and currently involves 22 companies (OEMs and tier-1 suppliers from the US, EMEA, and Asia) focusing on tracking cyber threats and developing joint industry solutions to address the security issues (in June 2016, they published a first set of best practices guidelines for cyber security). For this alliance to be successful, it is important to define the appropriate set of information that should be shared and the level of protection the information is granted by the authorities. The density of information (e.g., details on cyber attacks carried out, on solutions developed, etc.) should not be limited by individual player competitiveness (and at the same time should not damage the players themselves).

End users

The active participation of the end user is paramount in the success of cyber security solutions. Even with OTA as a maintenance mode, users themselves are a key link in the cyber security chain. Recent research shows that despite the resonance in the automotive community, current user awareness of cyber risk to cars is relatively low. User awareness peaks in the immediate aftermath of a serious security breach but fades away within a few months. According to data presented during the March 2016 RSA conference, the percentage of US consumers aware of actual automotive hacks that occurred in the previous year went down from 72 percent to 25 percent just eight months after the last public security break in 2015 (a week after the conference, the FBI issued a public service announcement with NHTSA and US DoT to warn drivers about the threat of cyber attacks on cars and trucks).

The role of the user in cyber security is not only to keep their automobile's software systems up to date but also to not install unsafe software on their mobile phones, which connect to their cars and potentially open the door to vehicle system cyber threats. In order to cultivate a culture of cyber security awareness among users, OEMs will need to look at a number of interventions *(see Text box 3: "Driver guidance").* Importantly, manufacturers will need to be aware that not all interventions will have equal impact, as the range of users – from tech savvy to very traditional – is wide. From on-screen, in-car security guidance to systems that automatically disable the ignition when unknown devices are connected to in-person orientations upon driver license renewal, manufacturers should be strategic about their approaches to user awareness.

Text box 3:

Driver guidance: Helping end users in their critical cyber security roles

OEMs have significant cyber security responsibility from the design of security products to the active monitoring of threats to the continuous updating of security features. OEMs' best efforts, however, will be effective only insofar as drivers are aware of the importance of cyber security, take responsibility for their role in security, and don't do anything to unknowingly add to the threat. End users will represent a wide range of security savvy, so it will be important for OEMs to consider a variety of tools that increase user awareness:

In-car screen guidance. From the driver's seat, users will be directed to the vehicle's screen and prompted to follow key security steps/perform key checks (e.g., confirming the list of devices connected to the car, highlighting recent changes in security/privacy settings). These steps and checks might be initiated, for example, upon every connection of an external device to the system, displaying detailed information on risks from data exchanges enabled by the different apps/devices), similar to smartphone/ICT practices.

Functional inhibitors. Functional inhibitors serve as roadblocks in suspect cases. For example, if an uncertified external device is detected, pairing might be disabled or warning/error messages might be sent to the registered user or to the back office for further analysis.

In-person education. Despite digitization, several physical touch points still exist for drivers. Cyber security briefings or modules as part of, for example, licensing exams at a government motor vehicles office or car purchase at the dealership, can serve as important orientations to the topic of cyber security. Modules could be structured on three areas: what are the cyber security risks (e.g., different potential consequences of hacks), which are the main attack techniques (e.g., review of remote attack surfaces and relevant cases of car hacks), what should the user do to be protected (e.g., selecting hard passwords, regularly updating the car, verifying and rejecting connections from unknown devices). Tests can be administered following these briefings to demonstrate user understanding, and evidence of a satisfactory level of knowledge in the area can be required before the user is able to activate a vehicle's connectivity functions.

Best-practice security behaviors also have different impacts on users based on their experience and profile. For example, informative messages and OTA update procedures (similar to those of smartphones and other connected devices) would be familiar to tech-savvy and "millennial" users but not to other "traditional" users, who might need time to get used to the advanced connectivity features. Additionally, security procedures and functional inhibitors may disrupt a smooth user experience (e.g., long setup times before being able to connect a new system, reiterated and complex identification procedures, etc.), and recent research shows that user satisfaction for connected car systems is highly driven by the user-friendliness of the interfaces.

The impacts of "security" behavior and procedures on user experience should be managed carefully, aiming to keep the interaction process as smooth and simple as possible. This should be done by integrating cyber security into user experience design and customer testing and applying the automotive industry's own best practices in design to the cyber area.

Government agencies

Most automotive regulatory bodies still have not concretely defined an approach to cyber security issues.

After the recent security breaches, some governments have started to require regulatory bodies to define and deploy a set of guidelines/rules for the industry on this topic, in order to keep the threats under control. Despite some of these early efforts, the industry currently is still mostly unregulated with regard to cyber security. Industry self-organization is occurring slowly with the first alliances on the topic being established only now. It is still unclear if the governments will take on roles as strict, top-down regulators or just leave the content leadership to industry institutions.

While industry self-regulation is only materializing slowly, governments and regulatory bodies need to watch carefully that the environmental parameters are established to allow the industry itself to find solutions to the security challenges. Without clear boundaries the widespread adoption of connected cars and assisted-driving vehicles will be hampered by security risks and unaffordable insurance premiums.

The government has three main roles. First, it must balance the interests of the public with those of the industry in protecting consumers from the potential harms of vulnerable products and services while protecting the industry from liability claims if a set standard of security and a known set of due diligence requirements are being maintained. Second, the government can facilitate greater collaboration within the industry and step in early if the industry struggles to come up with a solution. For example, in banking, a similar approach in giving direction to the banking institutions/associations has helped reduce transaction costs. Finally, governments should establish and ensure a safe information-sharing environment, giving incentives to disclose failures and liabilities within information-sharing organizations (e.g., if Company X shares the issues it has suffered, it will not get penalized).

Governments and their regulatory agencies will play a key role in ensuring that public and environmental safety are not compromised in the implementation of these security solutions. In turn, these regulatory bodies will protect the industry from liability claims as long as players follow standards and meet their due diligence requirements.

HOW TO OVERCOME THIS COMPLEXITY

As said, there is a broad range of automotive cyber security solutions that differ in applicability and effectiveness, and each uniquely impacts the efficacy and the complexity of the whole system. The scenario is complicated also on the front of the automotive ecosystem: there is a number of stakeholders involved in the supply chain (the OEM as system integrator, tier-1 and tier-2 suppliers and technology providers), the regulatory environment is still evolving (most main regulatory bodies are in the Request for Proposals stage for their guidelines), and finally the user has to take a full role in ensuring system protection, making user experience all the more important (e.g., because of potential trade-offs on available functionalities).

Moreover, given the natural continuous evolution of threats, there is no definitive “silver bullet” solution, implying that **OEMs should establish a culture of cyber security in the whole product development lifecycle,** from concept through continuous update and maintenance.

Wide variability in individual contexts and needs means that **each solution should be optimized** with respect to cost (recurrent and non-recurrent), time to market, user experience, and innovation. Finding the optimal cyber security strategy for an OEM would then require a **holistic approach based on four main steps.**

Step 1: Preliminary definition of acceptable risk profile

The specific context has to be analyzed to get a preliminary understanding of the possible cyber threats and their related risks based on the implications from the user, company, and regulation dimensions.

On the user side, OEMs should determine the tolerance level of target consumer groups for the different types of risk and the acceptability of eventual compromises on user experience due to cyber security measures (e.g., countermeasures should not make autonomous driving too burdensome for the user), eventually leveraging lab research[4]. On the company side, OEMs should discern which events would cause the brand identity or the strategy to suffer. On the regulations side, they should consider the impact of current and expected inputs related to cyber issues (e.g., guidelines for security, definition of stakeholder liabilities).

Step 2: Assessment of actual cyber risk exposure

Once the risk profile has been defined, understanding the gap versus the starting point is crucial to drive an appropriate selection of the solutions and a suitable definition of the implementation steps. This would be done through a holistic assessment of organization processes and capabilities (e.g., product development practices and procedures, high-level architecture principles, incident management and response readiness, existing cyber capabilities and culture, level of supplier involvement) and product resiliency (high-level analysis of the whole product portfolio, eventually with selected deep dives and penetration tests on key vehicles/systems, resilience of the adopted and planned technologies).

The resulting risk exposure map enables measurement of the actual gaps versus the risk profile for each product. Such gaps are operatively prioritized based on the volumes involved (number of existing and planned units per each product) and the product lifecycle road map (product maturity level, future planned technological evolutions, etc.).

Step 3: Identification of solution set

Based on the prioritized gaps resulting from the risk exposure map, a set of solutions should be identified at both the organizational level (e.g., new development processes) and the product level (e.g., specific hardware/software choices per each vehicle in the product line). The output would be the result of an optimization along the following main dimensions:

Costs. OEMs will need to evaluate the total cost effectiveness of the specific cyber security solutions with respect to product development, product cost itself, and maintenance cost:

- Product development cost involves the non-recurring cost of designing the chosen solution (e.g., effort spent for design and testing, for system integration)

4 E.g., McKinsey – ClickFox joint research

- Product cost includes the additional cost of the cyber security solution for a specific vehicle (e.g., hardware, software licenses, installation and physical testing effort)
- Maintenance cost has to be considered over the vehicle lifecycle and mainly concerns coding (updating/rewriting the software), secure version management (maintaining and supporting releases over time), testing (for any change of code and/or environment, e.g., testing system security when a new device is added), and update infrastructure (e.g., servers, clouds, and transmission infrastructures for OTA updates, USB-pen drive distribution, etc.). The cost structure could also be benchmarked against relevant industries (e.g., smartphone/ICT).

Based on the profile risk chosen for the specific vehicle, the optimization should balance the overall cost of the secure solution versus the eventual recovery cost related to the risk of cyber failure.

Time to market. Each solution has its own implementation time and impacts the possibility of putting a specific feature on the market at a specific point in time. Each solution also has consequences for market competitiveness, implementation costs (already covered), and risk exposure (with risk of prolonged exposure in case of delay of a solution, implying a higher probability of facing the cost of a recall action). More broadly, the time to market of the solution should also be consistent with the maturity level of each product, to maximize the return on the investments. For example, the solution for a system or product at the end of its lifecycle with no reuse opportunities is likely to be different from the one for a new product with seven years of useful market life and with the possibility of reuse on other products.

User experience. Most solutions have an impact on customer experience, which could eventually turn into a top-line issue if customers decide that security issues make their car less appealing if must-have or nice-to-have features are disabled or limited in an effort to reduce the risk of an attack (e.g., disabled Internet connectivity on the infotainment system). Similarly, cyber security solutions that place significant demand on users (e.g., frequent system updates to be performed by the user via PC-downloaded files on USB drive) may be perceived as too burdensome, creating another top-line issue.

Innovation. Each solution should be assessed in terms of its implications on the future evolution of the product. If not managed adequately, some levers could in fact put sand in the gears of innovation, constraining the creative environment from both the technology and process development point of view (e.g., choosing not to support a certain protocol or platform).

All these dimensions influence the overall value of the “cyber-secure” product: the actual cost of adding a feature, the realistic time to market, the accessibility and usability of the product, the level of innovation.

Step 4: Definition of implementation strategy and key enablers

As a last step to operationalize the solution set and ensure smooth execution, the OEM should, among other things:

- Define a detailed product implementation road map (considering both product and technology views and making sure the steps are aligned and shared with the supply chain)

- Put in place organizational levers as identified during the assessment phase to address gaps in both capabilities and processes (e.g., source know-how) through acquisitions or technological partnerships, install “cyber-secure” product development processes)
- Build relationships with other stakeholders (e.g., establish working alliances with peers, suppliers, and technology providers, cooperate with regulators).

□ □ □

Given the size of the challenge, the effort from the individual OEM in setting up its own secure strategy needs to be complemented at a higher level. The industry as such needs to develop new modes of collaboration and interaction to secure their products across the whole supply chain to prevent adverse customer reactions or regulatory burdens that could impede the road map towards the car of the future.

AUTHORS

Corrado Bordonali is an Engagement Manager in McKinsey’s Rome office.
corrado_bordonali@mckinsey.com

Simone Ferraresi is an Expert Associate Partner in McKinsey’s Rome office.
simone_ferraresi@mckinsey.com

Wolf Richter is a Partner in McKinsey’s Berlin office.
wolf_richter@mckinsey.com

The authors especially want to thank Garrett Bray, Associate in McKinsey’s Perth office, Marc Sorel, Engagement Manager in McKinsey’s Washington DC office, Dominik Wee, Partner in McKinsey’s Munich office, and James Kaplan, Partner in McKinsey’s New York office, for their valuable contributions and sharing their perspectives.

Advanced Industries Practice
February 2017

Design contact: Visual Media Europe
www.mckinsey.com