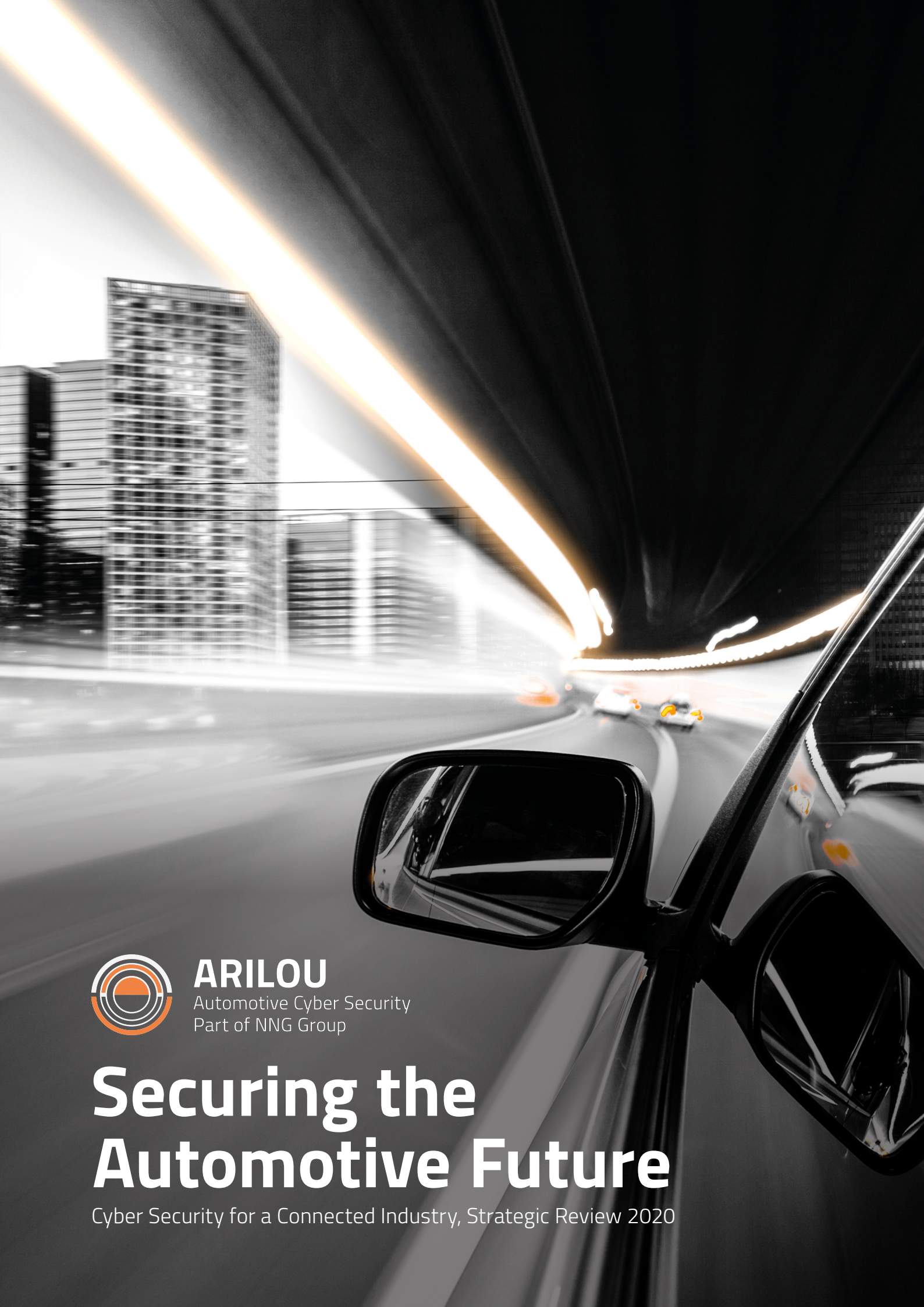


ARILOU
Automotive Cyber Security
Part of NNG Group

Securing the Automotive Future

Cyber Security for a Connected Industry, Strategic Review 2020

UNDERSTANDING THE THREAT

The Automotive landscape

Cyber Security threats emerge from a convergence of trends

The automotive industry is currently experiencing a convergence of multiple trends. Ubiquitous connectivity, increasing levels of vehicle automation, co-operative intelligent transportation systems, new regulations, shifting business models, and the development of new ecosystems to support them, are coming together to change the shape of the industry forever.

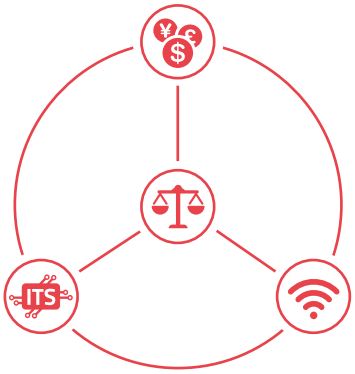
These trends, as part of the evolution of the internet of things (IoT), are born of the connected technologies adopted by automotive manufacturers that are intended to both solve a variety of societal, environmental, and economic challenges, as well as to differentiate their products in a competitive marketplace.

Now the proverbial genie is out of its bottle, and the adoption of connectivity in the vehicle is creating a positive feedback loop further accelerating adoption rates. In 2019 alone, there were approximately 51 million connected vehicles sold globally, with annual sales figures projected to exceed 76 million by 2025[1] .

This feedback loop is also encouraging the steady development of automated vehicles; from current advanced driver assistance systems (level 1), all the way through to the dream of fully automated vehicles, able to drive without any human interaction at all (level 5)[2] . While still evolving, the potential economic and safety benefits of vehicle automation are driving its journey from science fiction to reality. Other business opportunities driven by the software industry, such as Mobility as a Service (MaaS) are radically overhauling the way we look at the automotive value chain. These opportunities in turn, in effort to maximize market share and profitability, are driving innovation and investment in new connected and automated ecosystems to support them.

With such a broad range of opportunities to connect, and such a large impact on our daily lives, it's no surprise that mobility and the automotive industry have fallen firmly under the gaze of government regulators. Early guidance, drafted to address vehicle safety[3] and environmental concerns[4] , has also driven adoption of connected technologies. The range of sensors and analytical data these systems provide will boost the effectiveness of emergency features, as well as aid emissions reduction and range optimization for electric vehicles.

However, connectivity at this level, with links to other vehicles and infrastructure, presents a significant risk to public safety. In recent years, regulation and legislation[5] has begun to appear to address the fear of threats[6] , not only to personal, but also national safety. It requires not only detection and response but active prevention of cyber-attacks. This development has given rise to the need for cyber security solutions, to protect both the connected vehicle and its passengers, as well as the ecosystems that have arisen to support them. Never has the automotive industry faced such a radical convergence of trends in such a short period of time.



Connectivity in the Vehicle

Enhances driver safety and provides convenience and competitive differentiation.

Evolving Value Chain

New business models affect the priorities of the industry, providing opportunities for innovation and investment.

Intelligent Transport Systems

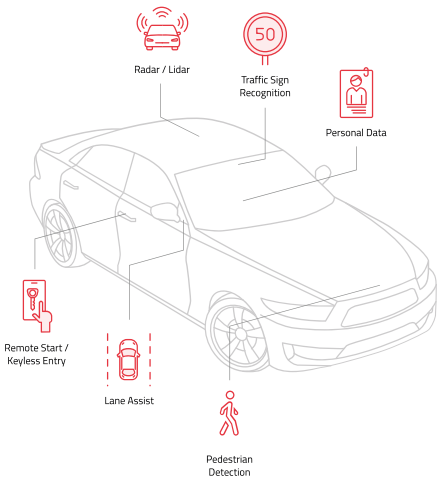
Connected and automated ecosystems are driving the need for standardization and encouraging further investment in connectivity and automation technologies.

Socio-Political Factors

Safety and environmental legislation are accelerating the adoption of connected technologies, in turn leading to the emergence of personal and national-level cyber security threats.

Connectivity in the vehicle

Connectivity opens the whole vehicle to attack



The In-Vehicle Network and ECUs

The threat to the vehicle stems from the architecture of the in-vehicle network (IVN) over which all the connected components, or electronic control units (ECUs), communicate. In most of today's vehicles, the dominant IVN is the Controller Area Network (CAN) bus[7] , a low cost, low bandwidth communications protocol developed in the 1980's.

Designed in a time before wireless connectivity was a realistic consideration for the car, there is no inherent security, and connected ECUs communicate freely with each other across the CAN with no authentication. Before remote-connected ECUs arrived on the market this wasn't a problem. Now however, with a vast array of connectivity options, one compromised ECU can open the entire IVN to attack by malicious actors.

Any connected feature is potentially hackable[8] , but the most common connected ECUs [9] include those that receive data from remotely hackable advanced driver assistance systems (ADAS), telematics ECUs, tire pressure monitoring systems (TPMS), and infotainment systems.

A newly emerging technology, due to replace the CAN bus, is automotive Ethernet. This IVN brings new functionality but also new vulnerabilities, many carried over from the IT industry. These vulnerabilities will need to be addressed before Ethernet becomes the primary IVN or it too will become a means of staging cyber-attacks.

Advanced Driver Assistance Systems

ADAS systems can include but are not limited to; adaptive cruise control, electronic stability control, electronic power steering, airbag control systems, as well as cameras, LIDAR and RADAR systems, providing collision avoidance, lane departure warning systems, automatic parking, and traffic sign recognition.

Infotainment

Infotainment ECUs share inputs with telematics units and are housed in the vehicles head unit, dash, central console, and driver facing instrument cluster. These ECUs control a variety of functions including climate control systems, digital radio, and GPS navigation. Additional features include USB, Bluetooth, and data connectivity, enabling Wi-Fi LAN in-car internet, SMS-texting, and handsfree calling.

Tire Pressure Monitoring System

TPMS, mandatory in all new US vehicles since September 2008[10] , includes air pressure sensors in each tire which feed data back to the main TPMS unit via wireless transceivers. The TPMS in turn, feeds data back to the vehicle control module, which aggregates it with other data to manage fuel economy, exhaust emissions, and a host of safety features.

Telematics and V2X

Telematics units transmit data between the vehicle and telematics service providers (TSPs). This includes diagnostic data, and the reception of over-the-air (OTA) updates and remote commands. It features a GPS unit providing location data, two-way communications via a mobile/cellular unit, and can provide remote access via GPRS and Wi-Fi bearer protocols. Future vehicle-to-everything (V2X) ECUs, and specific use-cases of more recent safety systems such as the EU's eCall[11] , may connect or be integrated with telematics systems.

V2X poses a special concern since it consists of remote, uncontrolled sensors which can influence vehicle behavior. Furthermore, it is a major component in co-operative driving, this technology will need special attention due to its potential for devastating impact if it were to become compromised.

What is eCall?

An initiative by the European Union, eCall is a vehicle safety monitoring system similar in concept to an aircraft's black box. In the event of an accident, eCall collects and relays relevant data (location, road conditions, vehicle status) to the nearest public safety answering point (PSAP). It does this by calling 112 (the EU emergency number), establishing a voice channel connection, and transmitting the data in a similar manner to the old dial-up internet modems. The PSAP can then relay the data or dispatch emergency services to the vehicle's location.

Evolving Value Chain

New business models and new technologies bring new threats

The value chain is changing. Shifts in consumer demand, and new entrants bringing new technologies to the marketplace, are radically changing the product development and launch cycle. This in turn is raising a variety of new cyber security challenges.

The Value and Supply Chain

The automotive sector, an industry fragmented over a complex structure of original equipment manufacturers (OEMs) and tier suppliers, has traditionally been a slow-moving entity. However, consumer awareness of new technologies, and the growing amount of software in the vehicle, are forcing OEMs to reassess their priorities.

The automotive industry is seeing a clear trend towards shorter production and launch cycles. Findings from as early as 2018[12] indicate that many OEMs have reduced production cycles to within two years. With 76% of surveyed OEMs adjusting their production cycles to compete with new entrants.

This swift, constant, development and turnover of software is increasing the amount of code in the vehicle (the average new model now contains over 100 million lines of code[13]), and with large amounts of code inevitably come bugs[14] .

Bugs, or defects in code, especially in devices or software not designed for security, bring unwelcome vulnerabilities into the vehicle. In addition, changes to the supply chain mean that secure development and production practices need to be reviewed to rule out the potential generation of Zero-Day threats[15] ; threats in which a malicious actor with access to (or involvement in) development may leak pre-existing (or even create new) vulnerabilities within the product itself.

Mobility as a service

With the growth in popularity of peer-to-peer ride sharing services such as Lyft and Uber[16] (and the resulting fall in cost-per-ride), consumer tastes in urban areas are moving away from vehicle ownership to shared ownership models. This will likely remain true despite the impact of the Covid-19 crisis[17] .

As one of the many new ways in which vehicles are becoming part of the burgeoning mobility-as-a-service (MaaS) market, this trend has also led to the rise of vehicle sharing services which offer the use of a private vehicle on a cost-per-mile or timed basis. These services hold personal financial data in apps on mobile devices, which are then used to connect to cars directly, functioning as remote keys[18].

Connectivity and publicly accessible vehicles present a huge opportunity for skilled hackers to take advantage of unsuspecting users. As an example, malware could be placed on publicly shared infotainment systems, and personal data stolen. In addition, company fleets could also be held to ransom[19], with services effectively halted until a bounty is paid to the hacker.

Data Services

Navigation and infotainment are already well-established services in the automotive industry, and although they may see some change in the way they exist within the vehicle as the industry moves towards critical MaaS[20], they are key enablers of the connected vehicle and we will continue to see innovation in these technologies.

vehicle usage data is set to reach an estimated market value of

USD 750 billion by 2030

Arising from these technologies is the new (to automotive) market of data analytics. In addition to telematics and other car data, navigation and infotainment usage data are becoming valuable commodities, with vehicle usage data in general set to reach an estimated market value of USD 750 Billion by 2030[21].

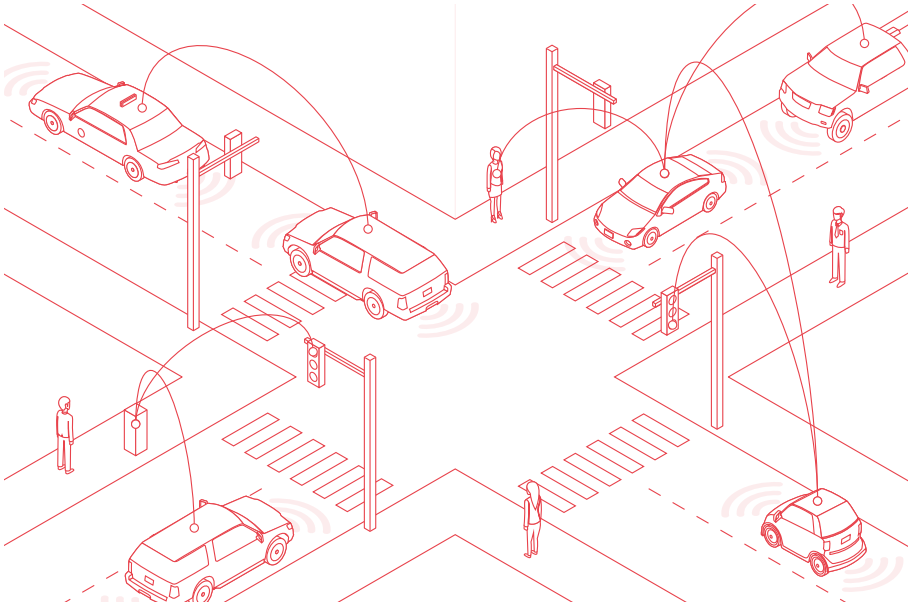
Useful for refining vehicle and technology design, this data can also be used to fine tune marketing profiles and provide more relevant services. But as a commodity, data also becomes the target of theft, and with global cybercrime's estimated value set to climb to over USD 8 Trillion by 2022[22], unsecured data in the car provides a tempting target.

Intelligent Transport Systems

A wider connected landscape opens new avenues of attack

Intelligent Transport Systems (ITS) encompass a wide array of applications for connected technologies, from the safety related (eCall, telematics) to the more commercial (e-Toll, public transportation and infrastructure).

As more vehicles become connected and the services that support them collect more usage data, that data in turn will be used (in what is now known as Traffic Management 2.0) to examine journey patterns, allowing city and transport planners to optimize their designs and networks. This has already seen some success in cooperative intelligent transport system (cITS) projects such as SCOOP[23], a joint program between France, the Netherlands, Germany and Austria, among others, which explored vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) applications.



This type of innovation could, in the future, create wider connected infrastructure to which vehicles can connect, allowing them to join a vehicle platooning service operated by specialized traffic management centers or purpose-built AI[24]. This connectivity, called vehicle-to-everything (V2X), combines V2V and V2I, and is enabled by the multitude of communication systems and sensors that are now common in modern connected vehicles.

Vehicle to Everything

V2X systems will greatly widen the attack surface available to hackers, providing opportunities to take control of unsecured connected vehicles, and in turn provide potential access to wider connected infrastructure, potentially putting tens of millions of people at risk.

Socio-Political Factors

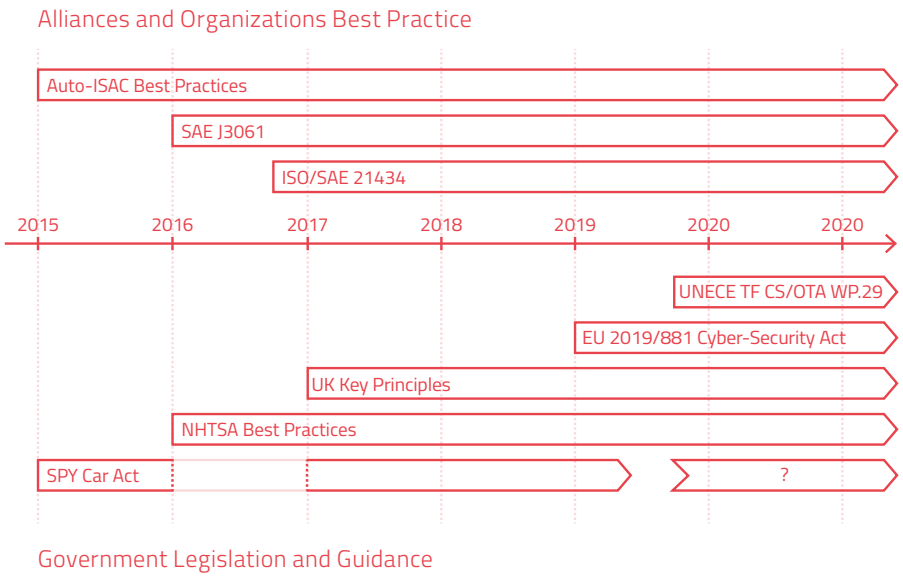
Cyber security is about more than just the vehicle

With such a wide variety of opportunities for attack, an infinite number of vectors, and a confusing array of technological obstacles, the industry needs to work together if it is to overcome the cyber security threat. This makes it about much more than securing the vehicle.

> **"...the industry needs to work together if it is to overcome the cyber security threat."**

The technology is important, and for the automotive industry, naturally, the vehicle is the best place to start. But we also need to be aware of the wider picture and make sure that we build in a level of future proofing to avoid preventable incidents as technologies evolve. This includes working closely with governments to make sure that all legislation is adhered to, and that a delicate balance between innovation, safety, and security is met.

Careful analysis and consideration is required, and cooperation at a level that goes beyond the simple OEM/Tier chain. Alliances and organizations such as the ISO[25] and SAE[26], Auto-ISAC, AUTOSAR and JASPAR are already making headway into this territory, with the goal of outlining best practice and standards for ITS systems, software development frameworks, and network architectures that allow for modularity and interoperability.



Awareness and Legislation

The hardest part of achieving effective, industry-wide cyber security, is developing awareness, and making sure that those in a position to make the necessary changes see a real need. Connected services, ITS, and V2X promise convenience and exceptional opportunities for economic growth, but with the current political climate raising concerns regarding the threat of terrorism or clandestine state action, connected vehicles and related infrastructure could become a real vulnerability.

In the USA, the NHTSA[27] has released guidelines for cyber security in the vehicle, as has the UK Department of Transport[28]. In 2004 the EU formed ENISA[29] to study cyber security vulnerabilities, and in 2013 relaunched[30] the agency as the true scope of the threat was realized. The UNECE is attempting to harmonize this globally but unfortunately not all countries are committed to it. When viewing these events in combination with the reintroduction of initial US legislation such as the SPY Act[31], it's clear that international government is playing a key role in driving automotive cyber security forward.

"...with the current political climate raising concerns regarding the threat of terrorism, connected vehicles and related infrastructure could become a real vulnerability."

Best Practice

Best practice can help streamline processes and procedures, enable efficient use of resources and make sure that common mistakes are avoided. Auto-ISAC[32], formed in 2014 is an alliance of global automakers who have formed a community to share insights and analysis of current and emerging cyber security threats. In 2016 SAE presented their first best practice guidebook[33], which in turn led to an ongoing cooperation between SAE and ISO[34] on standards for road vehicle cyber security engineering[35].

Standardization

Common development methodologies and layered architecture will enable OEMs and Tier suppliers to combine software and components from a variety of sources. The Automotive Open System Architecture (AUTOSAR)[36], is a global partnership formed in 2003 which works towards this goal. As does JASPAR[37], founded to address the Japanese market. Interoperability will not only enable ITS, but also provide a standardized vehicle network architecture, which is easier to secure, and most importantly can be designed with security in mind.

ATTACKS AND COUNTERMEASURES

Motivations

Understanding how and why the vehicle and network can be attacked is the first step to protecting it

There are a multitude of motivations for launching a cyber-attack against a connected vehicle, but they can be grouped into three loose categories: economic, political, and sociological.

Economic

Monetary gain is the key motivator in this category, and can include both malicious attacks, such as industrial espionage (reputation/brand damage, theft of trade secrets, data mining), criminal enterprise (grand theft auto, ransomware, denial of service). As well as the benign, such as academic or corporate research, and ethical hacking or penetration (PEN) testing.

Political

Strategic or tactical gain is the key motivator in this category, with political espionage (manipulating infrastructure to generate unrest), cyber warfare (disabling key transport links), and cyber terrorism (terror threats, loss of life).

Sociological

Fame or generating public awareness are the usual motivators in this category, with desire for renown (Script Kiddies, or 'Skiddies', trying to develop a reputation), and hacktivism (pushing for social awareness or change using hacking, e.g. Miller and Valasek's Jeep Cherokee hack[38]) being the most common.

Methods

Hacking

Attackers use knowledge of coding and hacking techniques to access their intended target. Some examples include MAC Spoofing, which involves changing factory assigned MAC addresses via vulnerabilities in driver software; SQL injection, which uses vulnerabilities in an application's database to inject malicious code; memory based attacks such as the Buffer Overflow (BOF) attack which cause a program to 'overflow' and overwrite adjacent memory locations; and Denial of Service (DOS) attacks, where a hacker attempts to overwhelm a network with fake or malicious messages, making usual operation impossible.

Social Engineering

Hackers can use psychological profiling to understand their intended target, map their behavior, and use this insight to discover potential exploits. Examples include, bin-diving (searching outgoing trash/garbage for sensitive data, e.g. passwords, employee, and customer data), phishing (using psychology to manipulate customers/employees), and spear-phishing (targeting specific customers/employees using collected data).

Physical Access

Although emphasis is placed on remote threats, vehicles and their networks are still vulnerable to traditional physical attacks. Attackers can gain access to the vehicle cabin using a variety of means, including breaking and entering or cloning key remotes[39]. Once inside, connecting simple tools to the vehicle's OBD-II diagnostics port gives direct access to the CAN bus. Alternatively, time-delayed malware can be placed on the infotainment system via USB. It should also be noted that an ECU could be compromised during firmware development, with malicious actors deliberately introducing vulnerabilities into the code.

OBD-II Port

The on-board diagnostics port has been standard in new model vehicles since the late 1990's in the US and the early 2000's in the EU. Connecting directly to the CAN bus the port allows diagnostic engineers to connect tools for maintenance purposes. The port is also used to attach third party connected modules such as driver behavior monitors advocated by many insurance companies.

Although being gradually phased out in favor of telematics units the OBD-II port is still present in many new cars.

Attacks

The attack surface of a vehicle is composed of all available vulnerabilities and threats.
As more connected features are added the attack surface of the vehicle grows.

ADAS

THREAT	ATTACK	
Remote Control of the Vehicle or Denial of Service (DOS)	Spoof ADAS sensors to produce aberrant vehicle behavior. The attack requires proximity to the vehicle as sensors are short range.	SEVERITY: HIGH PROBABILITY: LOW

Infotainment

THREAT	ATTACK	
Remote Control of the Vehicle and DOS	Place a FM transmitter and send hostile messages to the car stereos RDS, gaining entry to the infotainment system, ultimately gaining access to the CAN bus. Deliver hostile media to the vehicle via the infotainment web browser[40]. Place hostile media files on a victim's personal computer. Use a connected mobile phone (USB, Bluetooth) to transfer hostile media files to the infotainment system. Place a Bluetooth transceiver to hack a vulnerable infotainment systems Bluetooth connection[41]. Hack the driver's mobile using a compromised application, or alternate method, and use the Wi-Fi link to hack the Infotainment stacks Wi-Fi connection.	SEVERITY: HIGH PROBABILITY: MEDIUM
Data Privacy	Using the above channels, user data (navigation, location, personal data) can be stolen.	SEVERITY: MEDIUM PROBABILITY: HIGH
Ransomware Deployment	Vulnerabilities of the infotainment system can be used to deploy ransomware. Impact of the attack can be limited if the IVN is protected and malware is restricted to the infotainment system only.	SEVERITY: MEDIUM/LOW PROBABILITY: HIGH

TPMS

THREAT	ATTACK	
Remote Control of the Vehicle and DOS	Transmitting hostile messages to the TPMS receiver, taking control of it, enabling message sending over the CAN bus. Use a standard TPMS transmitter (which is usually installed inside the tires) with an amplifier to brute-force any protection the TPMS receiver may have and gain access to unprotected software layers.	SEVERITY: HIGH PROBABILITY: LOW
Data Privacy	TPMS radio frequency (RF) codes from a vehicle can be recorded, and with a network of RF sensors it would be possible to locate a vehicle with a good degree of accuracy.	SEVERITY: LOW PROBABILITY: MEDIUM

Telematics and V2X

THREAT	ATTACK	
Remote Control of the Vehicle and DOS	Call the vehicle telematics ECU directly using the integrated cellular/mobile connection. Then use predefined capabilities or find a vulnerability and exploit it. Use the exploit to send messages over the CAN bus. Infect the telematics server via the internet and then infect other vehicles. Infect the telematics server via a vehicle and then infect other vehicles. Place a 'time-bomb' or other triggered type of bridgehead.	SEVERITY: HIGH PROBABILITY: MEDIUM
Data Privacy	Compromised telematics and V2X units can collect data from the IVNs they are connected to and then leak it to the attacker.	SEVERITY: MEDIUM PROBABILITY: HIGH
Remote Control of the Vehicle and DOS	Take possession an authorized V2X ECU and use it to send false data causing the vehicle to exhibit programmed behavior at incorrect times. Use the predefined capabilities of a compromised but authorized V2X ECU to communicate with and/or exploit a vulnerability of a victim V2X ECU within the vehicle, enabling the hacker to send messages over the CAN bus.	SEVERITY: MEDIUM PROBABILITY: HIGH

Countermeasures

Security solutions should be considered at a holistic level

Choosing a Security Solution

Selecting countermeasures for the various attacks that pose a threat to a vehicle requires consideration of the full lifecycle of a vehicle – from assembly line all the way through to maintenance. How can we make sense of the large variety of options available on the market? Which solution is the right one?

The automotive cyber security market is new, and the supplier environment is fragmented with as many solutions available as there are connected components in the vehicle. When deciding on which solution is the best fit, it is important to consider these key areas:

Transparency
Is it clear what the solution offers?

Reliability
Can the solution offer proven and tested results, including validation from leading research institutions such as UMTRI[42] or governmental transportation departments?

Scalability
Is the solution future proof, offering security for the full vehicle lifetime? In addition, can the supplier provide the necessary expertise to respond and adapt to emerging threats as the industry landscape changes?

Performance Criteria

Not all solutions are suitable for the complete vehicle environment. Network overhead and component design play a key role in the allocation of resources across the vehicle. When assessing a system, these 5 key performance criteria should inform selection:

Connectivity Requirements
Does the solution require a mobile data connection to function? Some solutions can be cloud based or require regular over the air updates to operate correctly. Consideration should be given to both online and offline performance, especially as this can raise latency issues if not addressed correctly.

Latency
Speed of detection – the difference in time between the moment the attack happens and the moment that the security system identifies it as a malicious attack.

Deployment and Integration
How complex is the security solution, and how much time does it take to deploy and integrate with the vehicle and the lifecycle process? While part of the production stage, this is still a key area to consider when assessing whether the solution is suitable for business needs.

Overhead
The network or system resources the solution requires to operate. A security solution that creates significant overhead can dramatically reduce the performance of the network or ECU to which it is deployed.

Accuracy
Accuracy can be broken down into two areas, precision and recall. Precision is the ability of the solution to identify malicious attacks with the least possible false alarms (false positives). If a security solution fails in this area it means that it falsely considers normal events in the car to be hacking attempts. Recall, or the true positive rate, represents the actual amount of malicious attacks identified. A solution's low performance in this area means that it fails to detect hacking attempts.

Multi -Layered Security

A security solution should encompass all touch points of the industry. The automotive value chain is incredibly fragmented, and as such there are many potential vulnerabilities to be considered. With such a wide array of avenues for attack, it is very difficult to guarantee 100% protection. However, with a multi-layered solution a very high level can be reached. These 6 layers should be considered for a holistic security approach:

Secure Development

Design for security at the production level, using techniques that include configuration of inherent security features, static code analysis, and secure coding standards and best practice.

Supply Chain Management

Make sure all vendors involved in the supply chain follow secure working methodologies and procedures, and that all organizations involved, be they Tier suppliers or OEMs, adopt a security mindset and operational culture.

In-Vehicle Network Protection

Use intrusion detection and prevention systems (IDPS, IDS) and network management techniques to harden the IVN against attacks, restricting a malicious actor's movement. Utilize sender authentication/source detection, deep packet inspection, context analysis, and interception techniques.

ECU Hardening

Make ECUs harder to infiltrate and less attractive to hackers. Use endpoint protection mechanisms to monitor ECU software, harden the operating system, and use software authentication mechanisms (e.g. secure boot) at a hardware level. This will become even more important as the growing trends of consolidation and virtualization add more complexity[43], and therefore more potential defects to the ECU, raising the potential number of vulnerabilities.

Backend Cloud and OTA Security

Over-the-air (OTA) updates via the cloud are vital to the swift management of security breaches and threats. It is also important that the backend and the delivery channel (the connection between the OEMs security operations center (SOC) and the vehicle), whether cloud based or not, be secured to avoid manipulation, snooping, and interception attacks.

Security Architecture and Systems Engineering

Security must be a consideration at the design level, making sure that both critical vehicle systems, and the cloud and OEM hosted solutions that support them, are optimized and ring fenced appropriately to minimize damage in the event of an attack.

Security Solutions

There are many different solutions which can be used to secure the various parts of the automotive value chain. Having a clear idea of the pros and cons of each type of defense solution can help make decisions about which is the best fit for specific needs and scenarios. They can be loosely broken down into network and host solutions, some of the most popular are below:

Host Based Solutions

End Point Protection Mechanisms

As connected ECUs are the first target of attackers trying to access the vehicle, they should be hardened in a way that will make it more challenging to breach their security and exploit them. There are many ways to harden a system, starting from using only the necessary parts of the operating system or software (minimizing the number of bugs and security holes in the system due to fewer lines of code), to using special host-based security mechanisms that constantly monitor the ECU.

Host-based security mechanisms come in two forms, signature-based antiviruses, and their more advanced counterpart, anomaly detection-based host intrusion detections systems (IDS). The latter constantly monitors the hosts behavior, running tasks and analyzing the memory access and control flow of the code. As the name suggests, these two solutions function only at host level, not across the full network, and as such can also create additional overhead, reducing host performance.

While a viable solution, especially for ECU hardening, relying solely on host-based security is risky. There are many hosts (ECUs) in the vehicle, each comprised of individual components that may themselves be vulnerable. These components are supplied by a vast array of vendors, over which the OEM has little or no control, and as such can open a variety of potential vectors for attack.

Network Based Solutions

Cryptography

Encrypting (signing) and decrypting (validating) data that flows between ECUs over the in-vehicle network can ensure the authenticity of data. However, it can create significant overhead in low bandwidth networks such as the CAN bus. To enable the sending of messages and the authorization of received messages, cryptographic solutions require each ECU's firmware to support key storage and cryptographic operations. This can drain resources, significantly reducing network performance.

However, cryptography is a mature and widely used solution in other domains and will certainly have applications for high bandwidth networks, V2X technologies, and cloud security. It should be noted that although a robust technology, integrated cryptography needs to be managed due the significant key management overhead and production lifecycle complexity.

Intrusion Detection and Prevention Systems

IDPS solutions provide, as the name suggests, detection and prevention of attacks on the network. They can be either software or hardware solutions, or a combination of both. IDPS monitors the communication in the network, detects anomalous traffic and reports potential attacks to the security operations center (SOC) for further review. Prevention mode can also be toggled on and off manually. Automatic prevention is also possible with high precision solutions, ensuring the security of the network and the ECUs connected to it.

In-Vehicle Network Secured Management

Ethernet, a new high bandwidth IVN, is fast becoming a network of choice for media rich applications. It raises interesting new challenges and while it has some inherent security protocols not found in other IVNs, it requires the decoupling of the network communication functionality, and security services such as firmware updates, intrusion detection, deep packet inspection, encryption, and configuration management to provide the most effective protection.

Connectivity Security

In our modern environment there are many communication channels connecting different systems. It is vital to make sure these communication channels, whether between the vehicle and the cloud, or between the backend and other sources of data, are properly secured.

DEVELOPING A CYBER SECURITY STRATEGY

Defining a strategy can help combat emerging threats

Effectively securing the vehicle is the key concern of the industry, however, to be truly effective any solution needs to be part of a wider, holistic approach. Having a clearly defined strategy not only allows for advanced planning, but also aids in defining a clear chain of response, so that key stakeholders know how and when to respond, and whom to report to in the event of a breach. Some key areas to consider include:

Responsibility

Before spending the time and resources to develop a plan, it's important to assign who is responsible for cyber security strategy and management within the OEM. To design an effective strategy at a companywide level there needs to be someone in charge who not only has a wide understanding of the ecosystems of the business, but, because cyber security solutions integrate at a very low layer of the lifecycle process, also possesses the requisite technical understanding. They must also be able to communicate and fight for cyber security issues at the highest level of management. Buy-in and support from the executive suite is an imperative.

Risk Assessment

Assessing areas of vulnerability within the vehicle, the organization, and the supply chain requires a thorough audit of technological limitations, as well as procurement processes and procedures. This includes data handling procedures companywide, IT security, incident response, and compliance activities. It is also recommended to consult with professionals in various relevant fields to ensure no important areas are missed.

Prioritization

It's important to assess the probability and severity of an attack and assign values to the threats the risk assessment has established.

Mitigate Existing Threats

Assess and implement available solutions to secure the vehicle, and any other at-risk areas.

Create a Response Plan

A crisis response plan helps understand and manage events if a breach occurs. Create a clear chain of command and a checklist of scenario appropriate actions.

Crisis Response

Establish a security operations center (SOC) from where trained staff can remotely monitor and manage detection and protection systems. Alternatively consider whether 3rd party, automated or cloud solutions are more suitable.

Customer Service

Consider how to address customer expectations in the event of a crisis. How will the event be managed, how will communication be handled, and what level of detail will be shared?

Reporting to Authorities

How will communication with authorities be handled in the event of an external, or even internal breach? What internal processes are relevant to specific scenarios?

Commit to Progressive Improvement

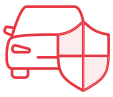
Conduct regular training and bring staff and management onboard by developing a security mindset. In addition, regular penetration (PEN) testing and assessment of security solutions and response capabilities are a must.

Building healthy relationships within the security community, including cyber security companies and professionals, can be highly beneficial when trying to understand threats, assess preparedness, and respond with speed and accuracy to attacks or breaches.

THE FUTURE OF AUTOMOTIVE CYBER SECURITY

Working Together

Cooperation in a complex industry is essential for effective cyber security



Connected vehicles, shared mobility, and current advancements in automated technologies have changed the way we look at the automotive environment. Risks now go well beyond the usual cost of recall and temporary brand damage. It is no longer a question of if an attack will happen, but when.

Current and future cyber security vulnerabilities pose a significant threat to personal safety, both at the individual vehicle and fleet level. Additionally, cyber-crime has the potential to affect privacy and data security, threatening the larger connected ecosystems that are evolving to support the future markets that vehicle-to-everything (V2X) and autonomous technologies promise.

Yet connected technologies and remote attacks are not the only challenge. The potential for physical attack remains, and threats to the automotive industry extend beyond the vehicle. We also need to consider the human factors, the who and the why, including the institutional and organizational vectors, examining the processes and procedures within our industry that can also prove to have vulnerabilities. We need to learn to identify them and discover how to turn them from threats into opportunities.

Automotive is a unique industry with a complex, deeply fragmented supply and production chain, and cyber security is vital to its evolution. It is time to think about where responsibility for protecting the customer lays and how we can work together to defend our business.

Protecting the future of the automotive industry starts now.

At Arilou we are constantly working toward building new partnerships to solve new challenges. With our experience and knowledge, we can help you take control of connected vehicles. If you would like to know more, please reach out us at Ariloutech.com/contact

Israel-based Arilou, part of NNG Group, is the leading provider of pioneering cyber-security solutions for the automotive industry, and first to introduce CAN and Ethernet in-vehicle network security.

Winner of Frost & Sullivan's 2019 Technology Innovation award, and independently tested by UMTRI, with perfect results, its Sentinel-CAN (CAN-bus) and Sentinel-ETH (Ethernet) IDS/IPS solutions offer supreme detection and prevention rates with zero false alarms. Additional product in the portfolio include CANpress: CAN-bus data compression, with authentication and encryption options.

With its holistic approach and low-cost multi-layered solutions, Arilou is making full protection for vehicles a reality.

ENDNOTES

[1] "Global Connected Car Market Outlook 2019." Frost and Sullivan, https://store.frost.com/global-connected-car-market-outlook-2019.html

[2] "When does a car become truly autonomous? Levels of self-driving technology explained", April 2017, Burgess, Matt, WIRED, https://www.wired.co.uk/article/autonomous-car-levels-sae-ranking

[3] "Principles of cyber security for connected and automated vehicles." August 2017, UK Department of Transport, et al, https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles

[4] "Government launches Road to Zero Strategy to lead the world in Zero emission vehicle technology", July 2018, UK Department of Transport, et al, https://www.gov.uk/government/news/government-launches-road-to-zero-strategy-to-lead-the-world-in-zero-emission-vehicle-technology

[5] "UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles.", June 2020, UNECE.org, https://www.unece.org/info/media/presscurrent-press-h/transport/2020/un-regulations-on-cybersecurity-and-software-updates-to-pave-the-way-for-mass-roll-out-of-connected-vehicles/doc.html

[6] Security and Privacy in Your Car Act (SPY Car Act) of 2015, Senators Markey and Blumenthal, https://www.markey.senate.gov/imo/media/doc/SPY%20Car%20legislation.pdf

[7] "Understanding Automotive Cyber Security – The In-Vehicle Network", February 2018, NNG/Arilou Cyber Security Blog, https://blog.nng.com/understanding-automotive-cyber-security-in-vehicle-network-ivn/

[8] "Nissan Leaf app contains cyber vulnerability, researcher says", Feb 2016, Bigelow, P, Autoblog.com, https://www.autoblog.com/2016/02/24/nissan-leaf-app-cyber-vulnerability/

[9] "Understanding Automotive Cyber Security – Electronic Control Units", April 2018, NNG/Arilou Cyber Security Blog, https://blog.nng.com/understanding-automotive-cyber-security-electronic-control-units-ecu/

[10] "Federal Motor Vehicle Safety Standards; Tire Pressure Monitoring Systems; Controls and Displays", April 2005, National Highway Traffic Safety Administration (NHTSA), https://one.nhtsa.gov/cars/rules/rulings/tpmsfinalrule.6/tpmsfinalrule.6.html

[11] "The interoperable EU-wide eCall." European Commission Mobility and Transport Website, https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en

[12] "Automotive Industry Trends Point to Shorter Product Development Cycles", January 2018, Morley, C, Jabil.com, https://www.jabil.com/insights/blog-main/automotive-industry-trends-point-to-shorter-product-development-cycles.html

[13] "Many Cars Have a Hundred Million Lines of Code", Dec 2012, Zax, D, MIT Technology Review, https://www.technologyreview.com/s/508231/many-cars-have-a-hundred-million-lines-of-code/

[14] "Ratio of bugs per line of code", Mayer, D, Mayerdan.com, https://www.mayerdan.com/ruby/2012/11/11/bugs-per-line-of-code-ratio

[15] "Automotive Cyber Security – A Glossary of Terms", Ariloutech.com, https://ariloutech.com/news/automotive-cyber-security-glossary/#Zero-Day

[16] "Uber powered four billion rides in 2017. It wants to do more – and cheaper – in 2018.", Jan 2018, Bhuiyan, J, Recode.net, https://www.recode.net/2018/1/5/16854714/uber-four-billion-rides-coo-barney-harford-2018-cut-costs-customer-service

[17] "Why shared mobility is poised to make a comeback after the crisis", July 2020, Andersson, Lennart et al. McKinsey & Company, https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/why-shared-mobility-is-poised-to-make-a-comeback-after-the-crisis

[18] "Car2go turns your smartphone into carsharing key with Mobile Access", Nov 2014, Blanco, S, AutoBlog.com, https://www.autoblog.com/2014/11/24/car2go-turns-your-smartphone-into-carsharing-key-mobile-access/

[19] "WannaDrive? Feasible Attack Paths and Effective Protection Against Ransomware in Modern Vehicles", 2017, Wolf, Lambert, Schmidt, et al, https://www.escrypt.com/sites/default/files/documents/Ransomware-against-cars.pdf

[20] "Mobility-as-a-service and overcoming the issues to get Critical MaaS", March 2017, Taylor, A, ITS-UKReview.org, http://www.its-ukreview.org/mobility-as-a-service-and-overcoming-the-issues-to-get-critical-maas/

[21] "Monetizing car data New service business opportunities to create new customer benefits", September 2016, McKinsey & Company, https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Monetizing%20car%20data/Monetizing-car-data.ashx

[22] "Cybercrime to cost global business over $8 Trillion in the next 5 years", May 2017, Juniper Research, https://www.juniperresearch.com/press/press-releases/cybercrime-to-cost-global-business-over-$8-trn

[23] Project SCOOP, French Ministry of Environment, Energy and the Sea, http://www.scoop.developpement-durable.gouv.fr/en/

[24] "How an Automated Car Platoon Works", July 2017, US Department of Transportation, Volpe Center, https://www.volpe.dot.gov/news/how-automated-car-platoon-works

[25] ISO/TC204 – Intelligent Transport Systems Working Group, International Organization for Standardization (ISO), https://www.iso.org/committee/54706.html

[26] Vehicle Cybersecurity Systems Engineering Committee, SAE International, sae.org, http://profiles.sae.org/tevees18a/

[27] "Vehicle Cyber Security", US National Highway Traffic Safety Administration (NHTSA), https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity

[28] "The Key Principles of Cyber Security for Connected and Automated Vehicles", August 2017, UK DoT, UK CPNI, UK Centre for Connected and Autonomous Vehicles, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/661135/cyber-security-connected-automated-vehicles-key-principles.pdf

[29] European Network and Information Security Agency (ENISA), 2004, now the European Union Agency for Network and Information Security, 2005, https://www.enisa.europa.eu/

[30] Regulation (EU) No 526/2013, May 2013, Official Journal of the European Union, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF

[31] "Senators reintroduce a bill to improve cybersecurity in cars", March 2017, Hall-Geisler, K, Tech Crunch, https://techcrunch.com/2017/03/23/senators-reintroduce-a-bill-to-improve-cybersecurity-in-cars/

[32] Auto-ISAC, automotiveisac.com, https://www.automotiveisac.com/

[33] "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems", January 2016, SAE J3061, https://www.sae.org/standards/content/j3061_201601/

[34] "Status of Work in Progress on ISO/SAE 21434 Automotive Cyber Security Standard", 2018, Barber, A, SANS Institute, https://www.sans.org/summit-archives/file/summit-archive-1525889601.pdf

[35] "ISO/SAE AWI 21434 Road Vehicles – Cybersecurity engineering", ISO, https://www.iso.org/standard/70918.html

[36] General Information About Autosar, autosar.org, https://www.autosar.org/about/

[37] About Us, JasPar, jaspar.jp, https://www.jaspar.jp/en/about_us

[38] "Hackers remotely kill a Jeep on the highway – with me in it", July 2015, Andy Greenberg, WIRED, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[39] "Just a Pair of These $11 Radio Gadgets Can Steal a Car", April 2017, Andy Greenberg, WIRED, https://www.wired.com/2017/04/just-pair-11-radio-gadgets-can-steal-car/

[40] "Chinese Researchers Hack The Tesla Model X So Hard They Make It Do A Lightshow", July 2017, Torchinksy, J, Jalopnik.com, https://jalopnik.com/chinese-researchers-hack-the-tesla-model-x-so-hard-they-1797333548

[41] "BlueBorne: Bluetooth Vulnerabilities Exposes Billions of Devices to Hacking" Sept 2017, TrendMicro Security News, https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/blueborne-bluetooth-vulnerabilities-expose-billions-of-devices-to-hacking

[42] University of Michigan Transportation Research Institute (UMTRI), http://www.umtri.umich.edu/

[43] "Rethinking car software and electronics architecture", February 2018, Ondrej Burkacky et al, McKinsey & Company, https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/rethinking-car-software-and-electronics-architecture

---

Editor: Daniel Harrison Design: Mátyás Sólyom Contributors: Ziv Levi, Michael Orlovsky

BENEFITS OF WORKING WITH US:

- **Efficiency.** Our solutions work on low-cost hardware, and even when the automobile is offline.
- **Lifetime care.** We know that cybersecurity solutions must be updated and maintained for the life of the vehicle..
- **Independent product.** We are not tied to big supply chain networks and can work with any platform.
- **Cost saving.** Not only does our product reduce the risk of expensive recalls, it also requires fewer resources.

NNG Kft.
Szépvölgyi út 35-37.
1037 Budapest HUNGARY
Tel. +36 1 872 0000
Fax +36 1 872 0100
[47°31'43.21"N 19°2'1.44" E]
sales@nng.com

Arilou Technologies Ltd.
Sapir Tower, 40 Tuval St.
Ramat Gan ISRAEL

[32°05'05.6"N 34°48'06.6"E]
contact@ariloutech.com

@ArilouTech
ariloutech.com/LinkedIn
ariloutech.com

ARILOU
Automotive Cyber Security
Part of NNG Group

NNG

V2020_09