White Paper on Cybersecurity and Smart Mobility in Catalonia

Exploring Threats, Vulnerabilities, Challenges, and Opportunities in the Pursuit of Smarter Mobility

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

Index

Index of Figures

Index of Tables

"Digitalisation and cyber are two sides of the same coin"

Excerpt from *'A Europe fit for digital age',*
by Ursula von der Leyen, President of the European Commission

Executive summary

The present white paper delves into the analysis of cybersecurity issues, stakeholders, and initiatives within the realm of smart mobility in Catalonia, aiming to understand the main elements, vulnerabilities, threats, and opportunities in this rapidly evolving sector. The research seeks to provide actionable insights for stakeholders to bolster their cybersecurity strategies and measures. The methodology involved a comprehensive review of existing literature and real-world case studies, as well as consultations with key industry experts and policymakers in the field of smart mobility and cybersecurity.

The first section of the document sets the stage of the discussion, providing a possible definition for the wide concept of smart mobility, encompassing every type of connected vehicle capable of exchanging a wealth of data with other vehicles and participants in the mobility ecosystem, and the interaction with both physical and digital infrastructures. It describes the threat landscape facing smart mobility, identifying the main actors, and revealing their possible motivations.

The second section of the white paper highlights the main threats and countermeasures identified for each of the elements introduced in Section 1.

Section 3 presents an overview of the Catalan smart mobility ecosystem, pinpointing the main stakeholder for each branch of the sector. In Section 4, the same exercise is repeated for the cybersecurity landscape in Catalonia.

In Section 5, we introduce the regulatory context both at European and Spanish level, including the main laws, regulations, and directives currently active.

In Section 6, we present the main opportunities for funding of collaborative Research and Development projects and delve into some of the most relevant projects in the field.

An overview of the international standards that apply to the transport industry in relation to cybersecurity is given in Section 7.

In Section 8, following our analysis of the sector and the most frequent threats and vulnerabilities, we give some recommendations to the stakeholders participating in the interconnected smart mobility ecosystem to bolster their cybersecurity strategies.

Finally, in Section 9 we present the conclusions.

During our research we found that the increasing integration of digital technologies in the transportation infrastructure has led to a heightened susceptibility to cyber threats. Stakeholders are advised to adhere to relevant laws and implement cybersecurity standards while fostering collaboration among industry players and experts. Regular security audits, training, and talent acquisition are also crucial. Additionally, rigorous assessment of third-party vendors and continuous monitoring of critical systems are emphasised. The establishment of a sectorial incident response plan and a Computer Emergency Response Team (CERT) is suggested. Policymakers are urged to create a national cybersecurity strategy, collaborate internationally, and actively participate in EU initiatives like the European Cybersecurity Competence Centre (ECCC) and the Joint Cyber Unit (JCU). Furthermore, the importance of 5G security, tailored cybersecurity regulations, and the need for studies combining cybersecurity and smart mobility are highlighted.

In conclusion, the whitepaper underscores the urgent need for a tailored cybersecurity strategy in the smart mobility sector to combat escalating cyber threats. It highlights the pivotal role of public administration in leading collaborative efforts, advocating for regulatory standards, and investing in research and development. The shift towards more connected and smarter mobility calls for an agile mindset and robust cybersecurity measures. Catalonia can capitalise on its strengths in smart mobility and cybersecurity, positioning itself as a significant player in Europe. Implementing these strategies will reinforce Catalonia's standing in the smart mobility domain, ensuring citizen safety and fostering secure and sustainable solutions.

1 Introduction

1. Introduction

In our interconnected and data-driven world, the convergence of technology, mobility, and evolving consumption habits has taken centre stage. This transformation has given birth to the concept of "smart mobility", a holistic reimagining of the transportation landscape facilitated by technology and digitisation.

Smart mobility encompasses traditional (but increasingly connected) private vehicles and public transport systems, along with innovative modes such as on-demand transport, ride-sharing services, car-sharing programmes, and micromobilitya, all relying on cutting-edge technologies, including big data, artificial intelligence, and IoT platforms.

This dynamic fusion of mobility and technology is reshaping the way people and goods move and revolutionising our transportation systems.

Stakeholders, including governments, cities, public transport authorities and operators, automotive OEMs, Tier 1s, technology providers, and innovative mobility start-ups, collaborate to reshape mobility. Remarkably, the global smart mobility market stood at a value of around EUR 42.77 billion in 2023 and is poised to maintain a robust compound annual growth rate (CAGR) of 21% from 2024 to 2032[1].

Smart mobility solutions represent more than just a passing trend; they provide a crucial response to the impending challenges of our era. The conventional transportation system, grappling with traffic congestion and environmental pollution, is in dire need of a substantial transformation. Smart mobility emerges as the solution, offering the promise of a cleaner, more efficient, and sustainable future for urban and interurban transportation. In this context, the transportation network transcends its traditional role as a purely physical infrastructure of roads and rails; it evolves into a connected, intelligent system.

However, this digital transformation is not without risks. As our reliance on digital systems grows, so does the potential for cyberattacks towards a sector that is considered critical and strategic for the society. In 2022, in Spain, transport operators were the second most cyber-attacked group by criminals, just behind the banking and tax sector[2]. At a European level, between January 2021 and October 2022, the monthly average of reported incidents affecting the entire transport sector increased by 25% compared to 2021, indicating a rising risk landscape. Notably, the automotive sector has experienced a troubling trend, witnessing a surge of 225% in vehicle-related attacks in 2021 compared to 2018. The public transport field also witnessed a similar trend, with news of cyberattacks to public transport authorities becoming more and more frequent. Examples include ransomware attacks targeting Barcelona Serveis Municipals (BSM) in 2021, and various waves of DDoS attacks against Transports Metropolitans de Barcelona (TMB) that had repercussions on the quality of public services[3].

The Cybersecurity Agency of Catalonia alone resolves a cyberattack every three hours. That amounts to about 2,000 cases per year. *"In some of them, the adversary succeeds, but many go unnoticed because we manage to handle them without any impact"*, explains its director, Tomàs Roy[4].

These attacks not only carry financial repercussions but also pose significant societal and safety concerns, particularly when they affect the daily mobility of thousands of citizens. Understanding these emerging trends and challenges is essential to effectively safeguard our smart mobility systems.

The new State of the Digital Decade report reveals that 75 % of Europeans emphasise the need for

[aa] For context and clarity, this white paper specifically covers the cybersecurity challenges facing land-based mobility in urban and interurban settings, thus excluding air and maritime modes

stronger cybersecurity, improved connectivity, and enhanced data protection. The hereby presented white paper serves as a comprehensive informative resource, emphasising the urgent need to address cybersecurity challenges in particular in the smart mobility sector. It analyses global developments but maintains a particular focus on Catalonia. The paper delves into the intricacies of cybersecurity within the smart mobility domain, examining the growing threats, exploring associated challenges, and proposing effective countermeasures to strengthen its related systems. While the content is intended to inform a general audience, it holds particular relevance for transportation industry professionals, including mobility service providers, administrative staff, cybersecurity experts, individuals involved in the daily operations of transportation services, and staff with decision-making responsibilities for cybersecurity in transport organisations.

1.1 Methodology

The methodology employed by Factual, an innovation and strategy consulting firm specialising in mobility, in the development of this white paper is structured to provide a comprehensive understanding of the major cybersecurity threats in the smart mobility sector. It incorporates the latest data and insights, offering a detailed description of the primary assets, vulnerabilities, threats, and countermeasures. Our research was conducted through a multifaceted approach that combined desk research and collaboration with experts from various domains, ensuring the depth and accuracy of our findings. By doing so, we aim to provide a well-rounded and informed perspective on the cybersecurity challenges in the smart mobility domain. Our intent is not only to offer an overview of the current state of affairs but also to equip stakeholders with practical insights and strategies to safeguard the increasingly interconnected and data-dependent smart mobility ecosystem.

Desk research

The foundation of this white paper rests on extensive desk research. Our research spanned a diverse array of sources, including academic journals, government reports, industry white papers, cybersecurity research papers and news articles. The aim was to gather the most recent and reliable data and insights concerning the intersection of smart mobility and cybersecurity. Throughout the methodology, we integrated relevant case studies to illustrate real-world examples of cybersecurity challenges and solutions within the smart mobility sector.

Expert collaboration

In addition to desk research, we recognised the significance of real-world expertise in comprehending the nuances of cybersecurity

within the smart mobility domain. To complement our research, we collaborated with a panel of experts comprising professionals from academia, cybersecurity agencies, and technology companies. These experts offered invaluable insights into the current threat landscape and emerging challenges in the sector.

Data synthesis

The data gathered through desk research and expert interviews underwent rigorous synthesis. We systematically organised the information into clear categories, covering aspects such as assets within smart mobility systems, known vulnerabilities, potential threats, and recommended countermeasures. The structured data synthesis enabled us to provide a coherent and comprehensive assessment of the state of cybersecurity in the smart mobility sector, with a particular focus on Catalonia.

Threat assessment

Once the data was synthesised, we conducted a thorough threat assessment. This phase involved identifying potential vulnerabilities and assessing the severity of associated threats. By categorising threats based on their impact and likelihood, we could prioritise areas that require immediate attention and offer pragmatic solutions.

Countermeasures and recommendations

The countermeasures identified are specific to the type of attack, which affects different stakeholders based on its nature. While recommendations are not only identified but are also predominantly directed toward specific stakeholders within the smart mobility ecosystem, such as public administrations, operators, or OEMs.

1.2 Smart mobility

The integration of connected vehicles, mobility data, and infrastructure and systems is the linchpin of smart mobility. The interplay between these three elements underscores an imperative demand for robust, holistic cybersecurity measures.

1.2.1 Connected vehicles

Modern buses, trains, trams, shared fleets of cars, bikes, mopeds, and kick-scooters, along with Connected and Autonomous Vehicles (CAVs), all fall under the category of 'connected vehicles'. This term encompasses any mode of transportation equipped with internet connectivity, capable of sending and receiving data. These vehicles typically incorporate sensors, radars, cameras, and communication technologies, enabling interactions with other vehicles, infrastructure, and external systems.

Connected vehicles offer a range of features and services, including real-time traffic updates, remote diagnostics, Over-The-Air (OTA) software updates, and communication with smart infrastructure, enhancing transportation safety, efficiency, and convenience, ultimately enabling autonomous driving systems.

Key elements of connected vehicles include In-Vehicle (IV) Communication and Vehicle-to-Everything (V2X) communication. In Figure 1, Figure 2, and Figure 3 the main components of the CAV's Communication framework are summarised and visualised. It is important to note that some of these components apply to all connected vehicles and not only the autonomous ones[5]. These communication components are essential for the efficient operation of connected vehicles but also present potential cybersecurity threats.

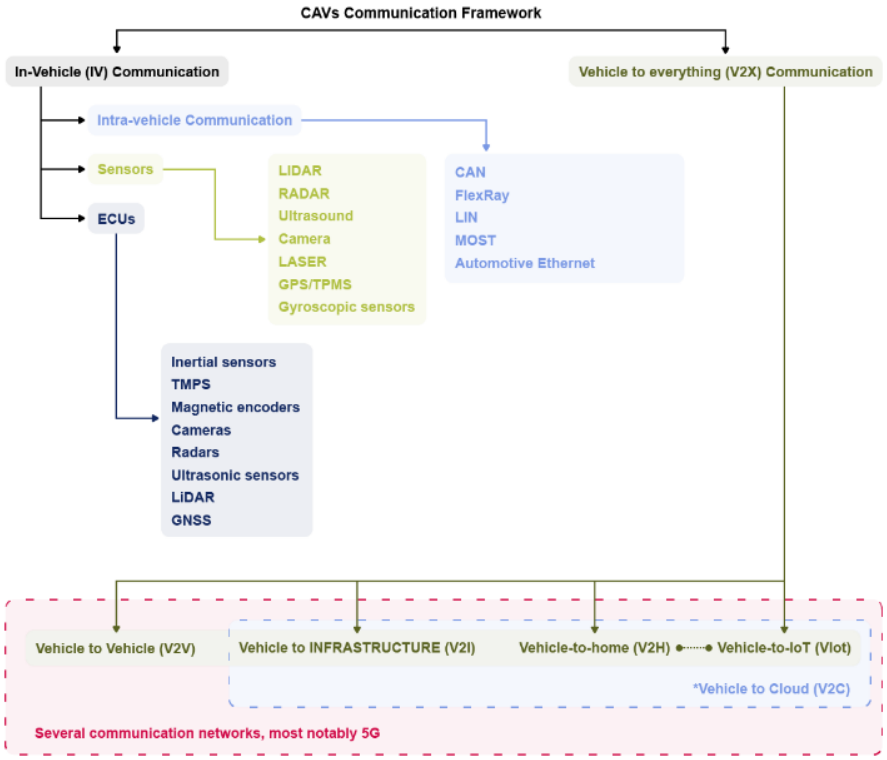


Figure 1: CAV's communication framework[4]

In-Vehicle communication: the architecture of In-Vehicle Networks (IVNs) comprises several key components, such as the Sensor Domain, the Chassis Domain, the Infotainment Domain, the Telematics Domain, the Powertrain Domain, and more. These domains communicate through protocols like Ethernet, FlexRay, Controller Area Network (CAN), and others. However, the

increasing connectivity among transportation facilities that are integrated with modern advanced technologies, such as V2X-communications, has led to the expansion of security vulnerabilities. Consequently, attackers might gain access to the in-vehicle network through these vulnerabilities[6].

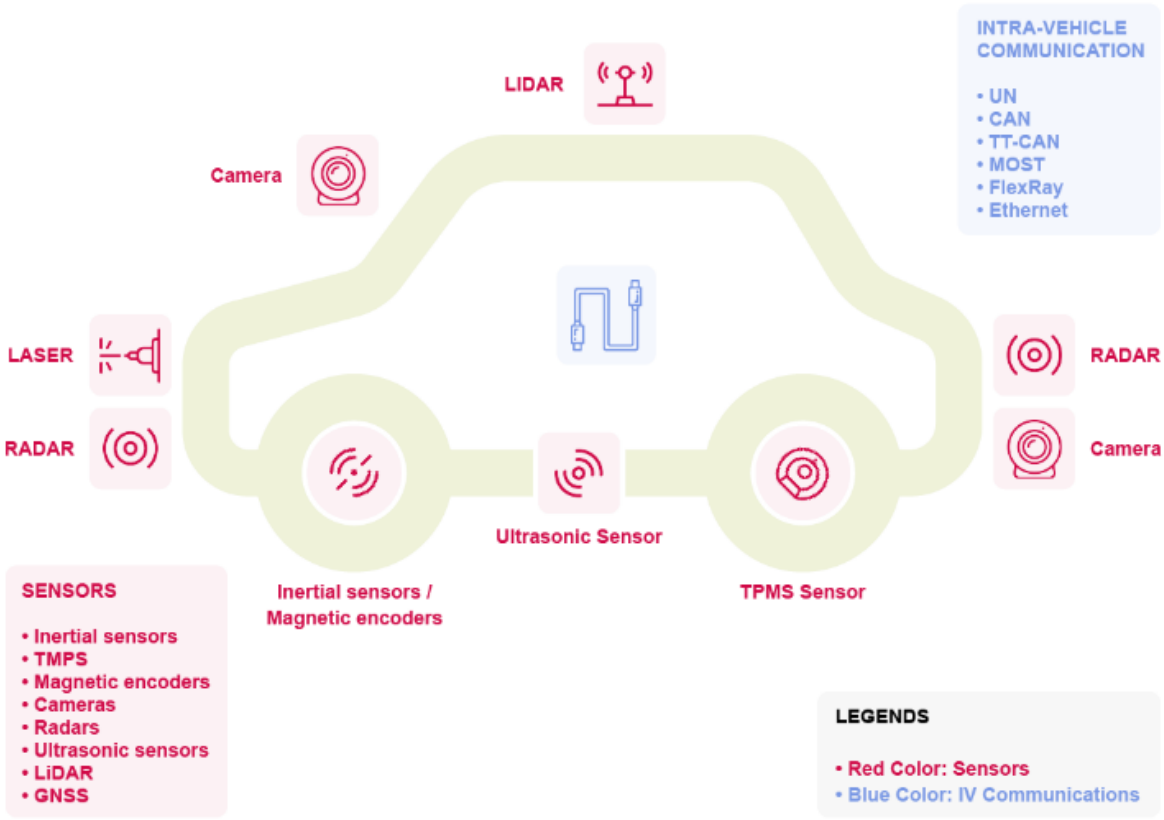


Figure 2: In-Vehicle communication[4]

Vehicle-To-Everything (V2X) communication facilitates interactions with the broader environment. It can be classified into Vehicle to Cloud (V2C) and Vehicle to Vehicle (V2V) communication4.

Vehicle-to-Cloud (V2C) communication extends to Vehicle to Infrastructure/Road (V2I/V2R) and Vehicle-to-IoT (V2IoT) interactions. Through Vehicle to Infrastructure/Road (V2I/V2R) communication, vehicles can exchange data with roadside infrastructure, including traffic lights, road signs, and other smart road components, enabling seamless integration with the transportation network. Furthermore, Vehicle-to-IoT (V2IoT) interactions enable vehicles to connect with a wide array of IoT devices, such as smart sensors, cameras, and other connected devices, enhancing the overall driving experience and facilitating the development of advanced transportation solutions[7].

Vehicle-to-Vehicle (V2V) communication enables information exchange between nearby vehicles. V2V communication operates through the use of Dedicated Short-Range Communication (DSRC) technology, allowing vehicles to communicate with each other within a range of approximately 300 meters. This technology enables the transmission of critical safety messages, such as collision warnings, emergency braking alerts, and traffic signal information, among nearby vehicles in real time[8].

Complexity of vehicle components: Cybersecurity and the principle of "privacy by design and default" have been holistically integrated into the operations of numerous manufacturers, supply chains, and delivery infrastructures. Yet, vulnerabilities persist as CAVs venture beyond the assembly line and into real-world scenarios, necessitating robust cyber resilience standards.

As CAVs become more prevalent, understanding vulnerable components is essential for developing effective cybersecurity strategies and safeguarding the future of smart mobility. Namely[9], as highlighted in this chapter, CAVs feature intricate, interlinked architectures that provide a multitude of essential services via a central gateway known as the Electronic Control Unit (ECU). This elaborate web of connections exposes CAVs to a range of potential threats, including data breaches or loss in cloud storage, system failures, power supply disruptions, software glitches, unauthorised access to vehicle controls, and identity fraud or theft.

Smartphone controls: Not only the CAV itself, but also mobile devices and associated apps play a crucial role in controlling various vehicle functions, including locks, headlights, infotainment systems, climate control, and more. These devices and apps are known to harbour vulnerabilities such as weak password requirements, coding errors, outdated operating systems, susceptibility to malware or viruses, and poor user practices. These vulnerabilities create potential avenues for cyber threats against CAVs. For example, a malicious actor may compromise a user's device and subsequently gain access to the legitimate CAV app, potentially taking control of the vehicle.

CAV payment services: CAVs incorporate multiple technologies for various payment services, such as fuel, subscriptions, tolls, parking, food, and beverages, the risk of compromising payment data is significant. This sector is expected to grow in the next decade, with the CAV payments market projected to exceed EUR 537 billion by 2030[10]. While the risk of malicious attacks and physical theft is a longstanding concern, one of the most prevalent threat vectors is financial gain through organised criminal activities.

1.2.2 Mobility data

In the smart mobility ecosystem, stakeholders can accumulate and process a diverse range of data, contingent on the services they provide and the technologies they employ. The following chapter outlines the most prevalent types of data that are frequently gathered, along with the associated cybersecurity risks they may attract:

Geolocation data[11]: encompasses information about the precise location of a user's device (such as a smartphone accessing mobility services) or an IoT platform embedded in a vehicle. However, the ubiquity of geolocation data collection raises concerns regarding its potential acquisition and misuse by unauthorised parties. Unauthorised access to geolocation data can have serious implications, ranging from privacy breaches to security threats.

One significant concern is the compromise of personal privacy. Geolocation data may reveal sensitive information about individuals, including their daily routines, frequently visited places, and even their home addresses (this is linked to the "Trip data" category below). If this data falls into the wrong hands, it can be exploited for various malicious purposes, such as stalking, identity theft, or burglary. Moreover, the misuse of geolocation data by third parties can result in invasive and targeted advertising, potentially leading to the manipulation of consumer choices and behaviours. This practice can undermine the autonomy of individuals, exploiting their preferences and vulnerabilities.

For organisations, such as public transport operators or smart mobility service providers, unauthorised access to geolocation data can compromise the safety of passengers and the security of transportation systems. Additionally, the geolocation data of shared vehicle fleets in specific city areas may unveil commercial strategies, such as identifying locations with higher demand for services. If a competitor gains access to this data, it could potentially lead to adverse business consequences.

Trip data[10]: encompasses details about a user's mobility patterns, including trip origin and destination (i.e., geolocation data), the route taken, the mode of transportation used, the trip duration, and the distance travelled. This data can extend to vehicle-specific information, such as instant or average speed, incidents of sudden braking, and emissions, among other. Shared mobility and ride-hailing operators, as well as automotive OEMs, are among those who collect and store this type of data. Cybersecurity concerns arise when considering the potential misuse of this data by unauthorised parties for malicious purposes. Unauthorised access to trip data can compromise the privacy of individuals, unveil their travel routines, and potentially lead to tracking and profiling.

Payment data[12]: encompasses details about the user's chosen payment method, which can range from credit card information to mobile payment data, along with transaction records for completed payments. This data is consistently collected by Payment Service Providers, including well-known entities such as PayPal, Stripe, Apple Pay, and Google Pay. Cybersecurity concerns come into play when evaluating the potential vulnerabilities associated with payment data. Payment Service Providers, in particular, face heightened cybersecurity risks as they store sensitive financial information. They may be targeted by various cyberattacks, including data breaches, payment fraud, and identity theft. Unauthorised access to payment data could have serious financial and privacy implications, both for the service providers and the individuals involved.

User account information[13]: comprises essential details associated with a user's account, encompassing their personal information like name, email address, phone number, and login credentials, among other. It may include information about the user's device, such as the device type, operating system, and device unique ID. This category applies primarily to account-based services, including Mobility-as-a-Service (MaaS), shared mobility, ride-hailing, and increasingly, public transport services, one notable example being the T-mobilitat.

The cybersecurity concerns regarding user account information are significant, as they involve the protection of individuals' personal data. Unauthorised access to this data can lead to privacy breaches, identity theft, and potentially malicious use of the compromised accounts. Moreover, compromised user accounts can disrupt mobility services, rendering them unusable. Service providers in the smart mobility sector, particularly those offering account-based services, need to be vigilant against cyber threats like data breaches and credential theft. Implementing stringent security measures and educating users about best practices for safeguarding their accounts is crucial in mitigating these risks.

Behavioural data[12]: encompasses details about a user's digital behaviour, including search history, application usage, and personal preferences, is of significant interest to various stakeholders in the smart mobility ecosystem. While automotive OEMs are known to collect substantial amounts of personal data from their customers, they are not the sole actors in this domain.

Other stakeholders, such as technology providers, app developers, and mobility service providers, also have a vested interest in behavioural data. They utilise this information to enhance user experiences, personalise services, and refine their offerings to align with user preferences. For example, mobility app developers use this data to suggest tailored routes and transportation options. By analysing users' search patterns and preferences, they aim to provide a more convenient and enjoyable travel experience. However, the collection and use of behavioural data must be in compliance with data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union. Non-compliance with these regulations can result in legal consequences, including fines and reputational damage.

System and security logs: include data logs with information related to the operation performance and security of the mobility systems: network activity, system usage, events, security alerts, incidents, etc. This data is essential for monitoring, maintaining, and enhancing the safety, efficiency, and effectiveness of smart mobility solutions. It may encompass data from vehicles, infrastructure, and transportation services, as well as security solutions in place to protect these systems. These various key players, such as mobility service and smart infrastructure providers, fleet operators, vehicle manufacturers, cybersecurity oversight bodies, IT services and public entities, rely on system and security logs to ensure the reliability and security of mobility services.

Algorithms[14]: smart mobility stakeholders use algorithms for various critical functions like dynamic pricing, fleet rebalancing, and route optimisation. Algorithms are also commonly used for functions such as demand prediction, traffic management, energy-efficient routing, predictive maintenance, and user experience enhancement. If these algorithms are compromised or hacked, the consequences go beyond data security and can be far-reaching.

1.2.3 Infrastructure and systems

With transportation infrastructure becoming increasingly digitised and interconnected, the threat of cyberattacks looms large. These attacks can have severe consequences, disrupting the smooth operation of transportation services and potentially jeopardizing the safety of passengers. Understanding the components of transport infrastructures that are particularly vulnerable to cyber threats is crucial for developing effective cybersecurity strategies. These vulnerable components include:

Control systems[15]: the control systems used in transportation infrastructure, such as Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, are critical targets for cyber-attacks. These systems manage and control various cyber-physical systems of transportation, including traffic signals, railway switches, surveillance cameras, and power distribution. ICS and SCADA systems in smart mobility may be targeted to disrupt critical transport infrastructures, causing significant harm, including traffic chaos, accidents, or other safety hazards.

Intelligent Transportation Systems (ITS)[16]: ITS integrates advanced technologies to improve transportation efficiency and safety. These systems include intelligent traffic management systems, electronic toll collection, and Vehicle-to-Infrastructure (V2I) communication. Cyber-attacks on ITS can disrupt traffic flow, compromise toll collection systems, or interfere with communication between vehicles and infrastructure, potentially leading to accidents or traffic congestion.

Power supply and distribution[17]: the reliable supply of electricity is crucial for the functioning of transport infrastructures. Cyber-attacks targeting power supply systems, such as substations or power distribution networks or electric vehicle charging systems, can disrupt transportation operations by causing power outages or affecting critical infrastructure components that rely on electricity.

Communication networks[18]: transport infrastructures rely on communication networks for efficient operation, including data transmission, monitoring, and control. Most notably, 5G networks, thanks to their ultra-low latency, they enable real-time interactions among vehicles and the infrastructure, making it a key component of V2X communications. Moreover, they are fundamental for the functioning of IoT systems. An emerging approach to designing Radio Access Networks (RAN) including 5G, called Open Radio Access Network (Open RAN), offers a more open, disaggregated, and standards-based architecture compared to more traditional RANs. Nonetheless, this comes with new risks that need to be addressed.

Mobile apps and web platforms: smart mobility actors employ mobile applications and/or web platforms to perform several tasks, including payments, vehicle provisioning or route planning, depending on the nature of the services provided. Their widespread use adds a layer of complexity and exposes more assets to the public internet, making them attractive targets for cyberattacks. Moreover, a successful cyberattack on mobile apps and web platforms can lead to immediate disruptions or data leaks affecting the daily lives and privacy of end users.

Internet-of-Things integration[16]: IoT applications in the field of smart mobility are mostly related to traffic control systems (more specifically for traffic management optimisation), fleet management and logistics optimisation. With regards to traffic control, the main cyber risks are linked to the disruption of real-time monitoring and data processing. Fleet management use communication protocols such as AMQP (Advanced Message Queuing Protocol) and MQTT (MQ Telemetry Transport), both of which are vulnerable to attacks. The implementation of IoT in logistics management, particularly the utilisation of the EPC global framework architecture, introduces vulnerabilities that could impact data interpretation, communication, and decision-making, potentially disrupting the integration of logistics components.

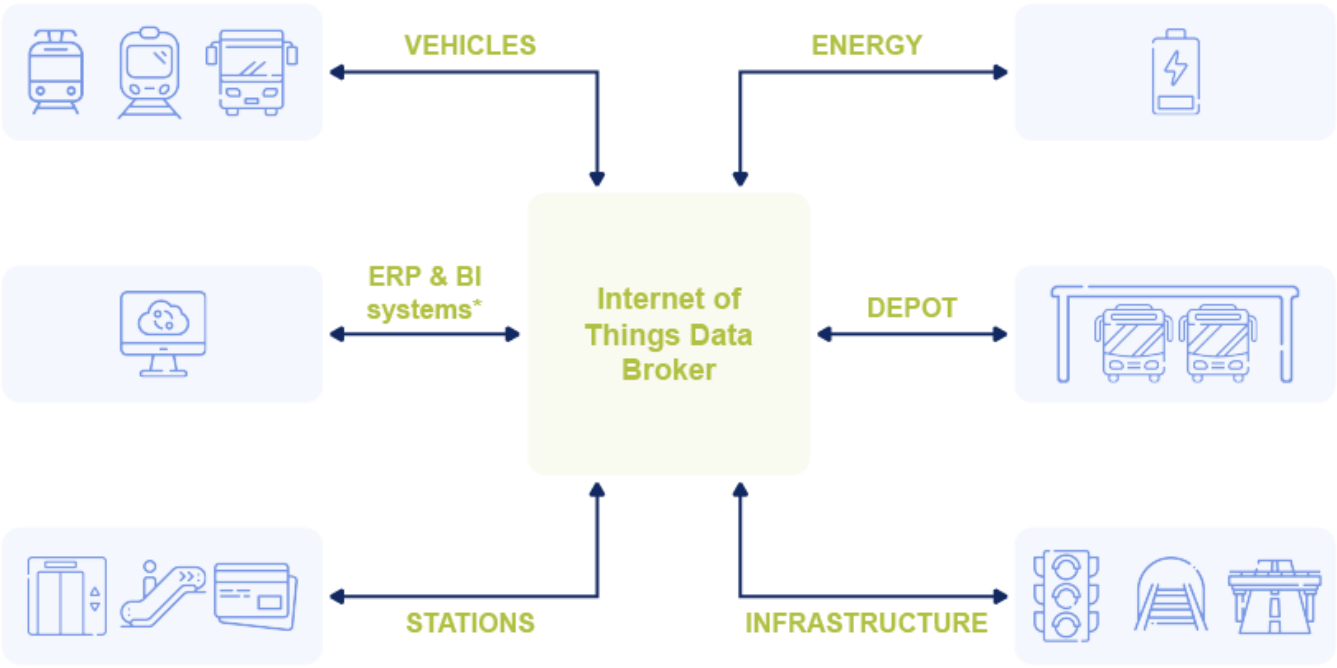


*Figure 3: Internet of Things Data Broker structure[19] (*Enterprise Resource Planning & Business Intelligence systems)*

1.3 Threat landscape

The increasing integration of digital technologies in the realm of transport and mobility brings with it a growing threat landscape that poses significant risks to the smart mobility elements outlined in the previous chapter. Take, for example, the direct connection between passenger safety and connected vehicles. A cyberattack targeting a connected vehicle can compromise its control systems, posing a significant threat to passengers' safety. Similarly, data privacy and security are closely intertwined with mobility data. This data is collected, processed, and transmitted through various interconnected systems, including those integrated into connected vehicles. Furthermore, the reliability and functionality of the digital infrastructure are paramount to the overall performance and safety of smart mobility systems. Any compromise in this infrastructure not only jeopardises public trust but can also carry significant economic implications.

A cyber incident in the smart mobility sector can result in various consequences, underscoring the need for enhanced cybersecurity. These potential impacts are outlined below:

Passenger safety: in the case of connected vehicles, cyberattacks can compromise the safety of passengers. Unauthorised access to vehicle systems could lead to accidents, as seen in instances where hackers remotely control vehicle functions.

Service reliability: any disruption or cyberattack on the infrastructure can impact the reliability of smart mobility services. For instance, an attack on the traffic management system could lead to traffic congestion, affecting the efficiency and timeliness of transportation services.

Data privacy and security: mobility data, including user travel patterns, payment information, and personal details, is at the core of smart mobility services. The mishandling or theft of this data can lead to privacy breaches, identity theft, and financial fraud, posing significant risks to users.

Economic implications: cyberattacks can result in financial losses. For instance, a ransomware attack on a transportation network could lead to a significant financial burden.

Public trust: cybersecurity incidents can erode public trust in smart mobility systems. When users are concerned about the safety and privacy of their data, they may be reluctant to adopt or continue using smart mobility services.

Regulatory compliance: the increasing focus on data privacy regulations like GDPR requires smart mobility providers to adhere to strict data protection standards. Non-compliance can lead to regulatory fines and legal repercussions.

This remainder of chapter aims to provide an overview of the prime threats to smart mobility, shed light on the threat actors with the biggest impact on the sector and understand their motivations. By capturing these threats and trends, stakeholders can better prepare and implement effective cybersecurity measures to safeguard smart mobility systems.

1.3.1 Prime threats

There are several prime threats encompassing a range of malicious activities targeting the land transport sector, that is road and railway transport combined. The data available reveals a list key threats, as visible in *Figure 4* [20]. Please note that the percentages do not add up to 100%. This is due to the fact that threats can belong to multiple categories at once.

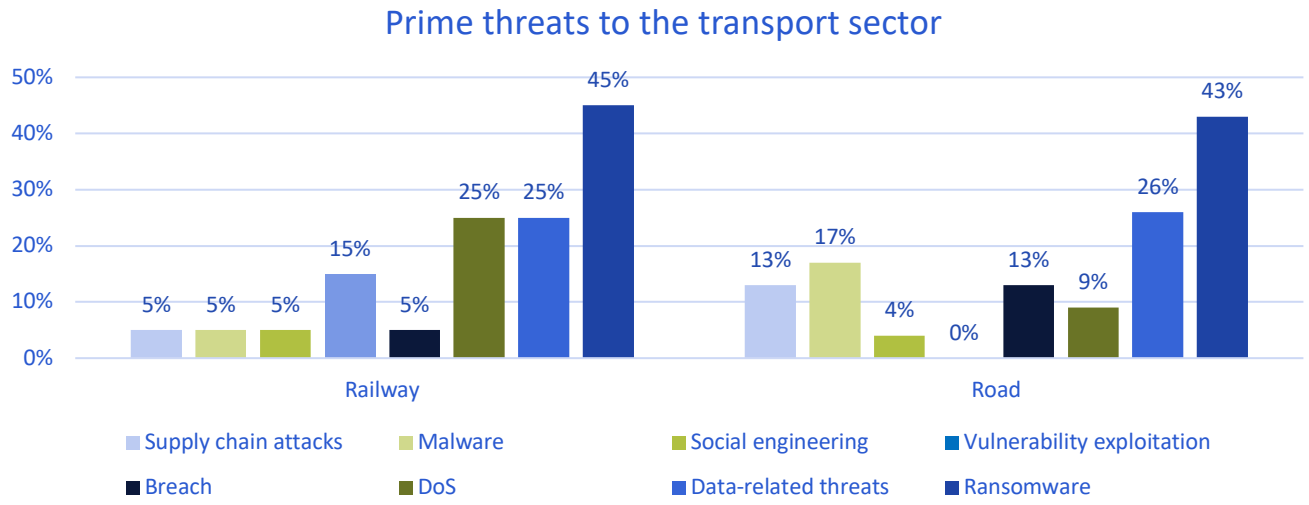


Figure 4: Prime threats to the transport sector[19] (January 2021 to October 2022)

Malware

Malware encompasses various types of software or firmware designed to execute unauthorised processes that negatively impact the confidentiality, integrity, or availability of a system. Common examples of malicious code include viruses, worms, trojan horses, spyware, and adware, among others, which infect and compromise host systems. Approximately 17% of the incidents targeting the transport sector involved the presence of malware.

Ransomware

Ransomware refers to a specific type of malware where threat actors seize control of a target's assets and demand a ransom in exchange for restoring access to those assets. In this document we distinguish ransomware incidents from general malware incidents, as they constitute a significant portion (44%) of the total attacks. These incidents often garner high levels of public attention and publicity due to their impact and consequences.

One notable example is the ransomware attack that occurred on Barcelona Serveis Municipals (BSM), a public company responsible for services like 'Bicing' (public bicycle sharing), green and blue zone parking. Although the impact was limited, it forced a temporary halt of services, including the Smou and SPRO. This had repercussions on the public bike-sharing service 'Bicing,' professional loading and unloading parking, and resident parking in the green area[21].

Data related threats

The security of data sources is being increasingly targeted, with the objective of unauthorised access, disclosure, and manipulation of data to disrupt system behaviour. Nevertheless, from a technical perspective, threats against data can primarily be categorised as data breaches and data leaks, which can serve as the foundation for many other types of attacks discussed in this report, as social engineering.

A data breach occurs when a cybercriminal intentionally breaches security measures to gain unauthorised access and release sensitive, confidential, or protected data. On the other hand, a data leak refers to an event where sensitive, confidential, or protected data is unintentionally exposed due to factors such as misconfigurations, vulnerabilities, or human errors. It is observed that approximately 30% of the incidents involve threats against the data of transport organisations.

With the launch of its testing phase in 2021, the T-Mobilitat suffered a data leak that exposed personal information of hundreds of users, a vulnerability that was swiftly detected, and addressed[22].

Denial-of-Service (DoS)

System and data availability are the focal points of numerous threats and attacks. They occur when users are unable to access essential data, services, or resources, with Distributed Denial-of-Service (DDoS) attacks being particularly noteworthy. DDoS attacks specifically target the availability of systems and data and, although not a novel threat, they play a significant role in the cybersecurity landscape of the transport sector. This can be achieved by overwhelming the targeted service and its resources or by overloading the components of the network infrastructure. The occurrence of geopolitical developments and heightened hacktivist activity contributed to an increase in DDoS attacks against transport organizations, constituting 16% of the total incidents.

On the electoral day of July 23, several institutions' websites were affected by a DDoS cyberattack carried out by the pro-Russian cybercriminal group known as 'NoName057.' The aim of this attack was to disrupt the elections due to the support of certain Spanish political parties for Ukraine. Among the targets of this cyberattack were various entities related to mobility, including the Consorcio de Transportes de Madrid (CTM), Metro de Madrid, Consorcio de Transportes de Mallorca (CTM), and Transports Metropolitans de Barcelona (TMB)[23].

Social engineering

Social engineering encompasses a wide range of activities that exploit human errors or behaviours in order to gain unauthorised access to information or services. It employs various manipulative techniques to deceive victims and trick them into making mistakes or divulging sensitive or confidential information. Within the realm of cybersecurity, social engineering tactics lure users into actions such as opening malicious documents or emails, visiting compromised websites, or granting unauthorised individuals access to systems or services. The threat landscape of social engineering primarily includes the following vectors: phishing (with its variants: spear-phishing, whaling, business email compromise, or BEC), smishing, vishing, fraud, impersonation, and counterfeiting. Within this category, the primarily observed attacks involve phishing and spear-phishing targeting transport users (10%), as well as incidents related to fraud, impersonation, and counterfeiting (6%). BEC attacks surged by 81% in 2022 and 175% over two years, yet a striking 98% of employees fail to report the threats. Particularly, transportation sector employees (16%) were most prone to respond, likely driven by the urgency of operations. Despite law enforcement efforts, BEC attacks globally yielded EUR 2.3 billion in 2021, emphasising the critical need for advanced email security measures alongside employee training[24].

As an example, in this 2023, several phishing campaigns have been detected impersonating the Dirección General de Tráfico (DGT). These campaigns involve sending fraudulent emails and SMS messages, falsely claiming unpaid fines. Victims are then lured into entering their banking information on a fake website or are encouraged to download a malicious document that can infect their device[25].

1.3.2 Threat actors

Several threat actors have been identified as having the biggest impact on the transport sector. Understanding the motivations and tactics of these actors is crucial for developing effective countermeasures.

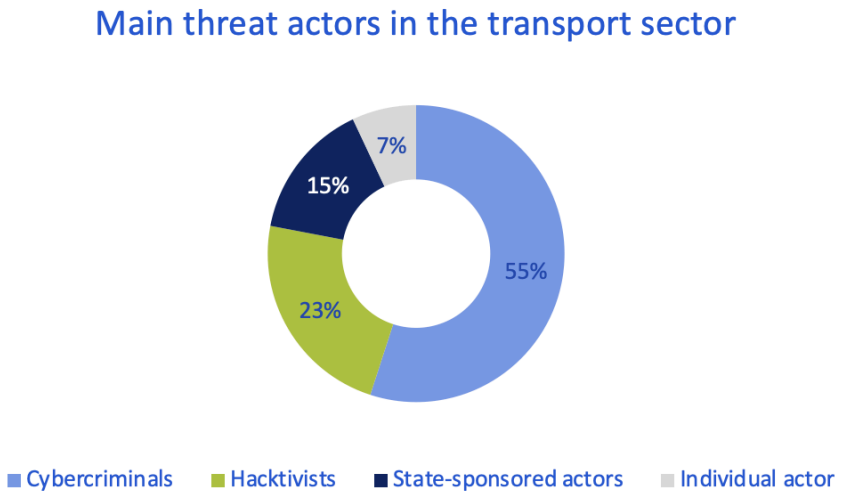


Figure 5: Prime threat actors in the transport sector[19] (January 2021 to October 2022)

Cybercriminals

Cybercriminals were responsible for the majority (55%) attacks on the transport sector, targeting all subsectors. Their motivations primarily revolve around financial gain through activities such as data theft, ransomware attacks, or selling stolen information on the dark web.

For instance, DoppelPaymer ransomware gang attacked Kia Motors America and demanded USD 20 million ransom in exchange for a decryption tool and a promise not to release stolen data. The attack resulted in a nationwide IT service disruption, affecting various aspects of Kia's operations, including mobile apps, phone services, payment systems, owner portals, and dealer-used internal sites[26].

In 2020, Adif, the Spanish state-owned company responsible for railway infrastructure, demonstrated its ability to thwart a ransomware attack, ensuring that its infrastructure remained unaffected. In a statement, the company emphasised its awareness of being the steward of critical infrastructure and considered cybersecurity as a fundamental pillar of comprehensive security. However, the cybercriminals claimed to have stolen 800 GB of data, including sensitive information related to contracts, invoices, certificates, correspondence, and customer phone numbers. They demanded a ransom to prevent the public release of this data[27].

Hacktivists

Hacktivists engage in cyber-attacks for ideological, political, or social causes. The reporting period witnessed an increased level of hacktivist activity targeting the transport sector (23%), and this trend is expected to continue. Hacktivists often employ DoS attacks to disrupt services and websites, defacement of online platforms to spread their messages, and data breaches to expose sensitive information. Their motivations can range from advocating for political change, protesting perceived injustices, or simply aiming to raise awareness about specific issues. In the transport sector, hacktivist activities have become a growing concern due to the potential for significant disruptions. They might target transportation infrastructure, such as

airports, ports, or railway systems, with the intent of causing chaos or drawing attention to issues like environmental concerns, privacy infringements, or inequality within the industry.

In October 2023, the cybercriminal group NoName057, linked to Russian Kremlin interests, successfully blocked the websites of the Granada metro (metropolitanogranada.es) and the capital's public transportation system, operated by Alsa (transportesrober.com), through DDoS attacks. This was announced on their Telegram channel, while also expressing their opposition to the European summit taking place in Granada[28].

State-sponsored actors

State-sponsored actors pose a significant threat to the transport sector (as they are behind 15% of the total threats), leveraging their resources and capabilities to carry out sophisticated and targeted attacks. Their motivations can range from intelligence gathering to disrupting critical infrastructure or achieving geopolitical goals. In a recent instance, Israeli officials have attributed a string of targeted cyber intrusions on prominent logistics and transportation firms to a group identified as Tortoiseshell, also known as TA456 or Imperial Kitten. The group, believed to be backed by the Iranian state, has been reportedly engaged in a long-term cyber campaign, deploying intricate 'watering hole' attack strategies to infiltrate and compromise Israeli websites[29].

Individual actors

Individual actors can represent a variety of cybercriminals, from a rogue employee to hackers-for-hire, criminals who sell their services to people who do not have the skills or capabilities to do so. They are responsible for 7% of the attacks.

A recent incident involving a Tesla employee who was targeted by a criminal organisation to deploy malicious software underscores the importance of fostering a robust culture of cybersecurity awareness. It also underscores the need for implementing controls to mitigate the risk of insider employees causing disruptions or harm[30].

1.3.3 Motivation

The main motivations behind these attacks are summarised in this chapter. By exploring these motivations, we gain a deeper understanding of the driving forces behind cyberattacks. This knowledge is essential for developing effective cybersecurity strategies and countermeasures to mitigate the risks posed by malicious actors. ENISA lists the following key motivations:

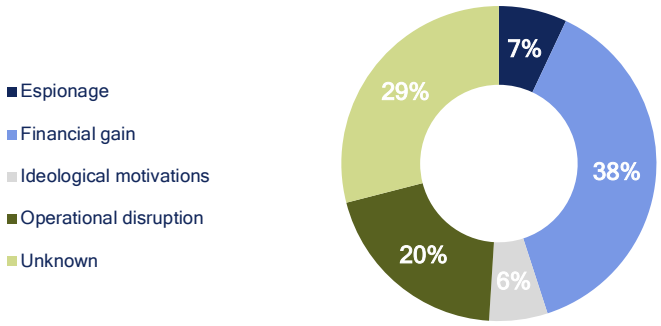


Figure 6: Main attack motivation in the transport sector[19] (January 2021 to October 2022)

Espionage

Some attacks are driven by the objective of gathering information, whether it be intellectual property or data of national significance. The attackers seek to gain access to valuable information for espionage purposes. These attackers are often state-sponsored, as for example the China-backed hacking group, Volt Typhoon. This group has been allegedly spying on critical US infrastructure since 2021, including transport, according to warnings from Microsoft and Five Eyes intelligence agencies[31].

The situation is complicated by the ongoing trade war between the USA and China, which has extended its impact to the subway car industry. A notable instance occurred in 2020 when the United States implemented legislation aimed at limiting the participation of CRRC Corporation, the world's largest train manufacturer and of Chinese ownership, in new contracts within the United States. This decision results from a combination of economic considerations and national security apprehensions, particularly the reluctance to source computer infrastructure from a nation with questionable trustworthiness[32].

Financial gain

In some cases, cyberattacks in the mobility sector are driven by financial motives, notably, those perpetrated by cybercriminals, such as ransomware attacks. Attackers carry out these attacks with clear monetary objectives in mind, which may involve fraud, extortion, or the sale of stolen data. By using different Techniques Tactics and Procedures (TTPs), cyber attackers seek to profit from their illicit activities.

In late 2022, the Chinese electric vehicle manufacturer NIO fell victim to a ransomware attack in which customer data was stolen. The attackers demanded a USD 2.25 million ransom in Bitcoin to restore the systems and prevent the stolen information from being disclosed. Shortly thereafter, as NIO refused to pay, they became aware that some of their users' data had been sold to third parties for illegal purposes[33].

Ideological motivation

Hacktivist activity often plays a role in cyberattacks, where the motivations are rooted in ideological beliefs. These attacks are accompanied by explicit declarations from the

actors, highlighting their intent and the underlying cause they support.

Shortly after the war in Ukraine began, a notable incident occurred involving Russian electric vehicle charging points situated along Russia's M-11 motorway, which connects Moscow and Saint Petersburg. These charging stations were targeted in a cyberattack, leading to their deactivation. Instead of their usual functions, the screens at these charging points displayed pro-Ukraine messages, including the phrase 'GLORY TO UKRAINE.' The suspicion is that the hacking was carried out by a Ukrainian company that had supplied components for these charging stations and potentially left a backdoor in their systems to facilitate the attack. This incident exemplifies how cyberattacks have been used in the context of geopolitical conflicts and tensions[34].

Operational disruption

Some attacks specifically target the disruption of services. Unlike cases where operational disruption is an unintended consequence of an attack, these incidents are initiated with the primary goal of causing disruptions and impairing normal operations.

Vectalia, the concessionaire operator of transportation services in cities such as Alicante, Alcoy, Albacete, Cáceres, and Mérida, fell victim to a ransomware attack. This attack resulted in the disruption of several computer systems directly linked to passenger transportation and mobility, including schedule boards, the application, and card reloading services. Vectalia implemented a special plan for in-person user information at the busiest stops in Alicante[35].

2

Threats and countermeasures

2. Threats and countermeasures

In this section of the whitepaper, we delve into the primary threats and countermeasures associated with connected vehicles, mobility data, and infrastructure and systems. While some of these threats have already materialised in real-life scenarios, others have only been demonstrated mostly in controlled environments. The latter category offers insights into potential new attacks, reflecting the rapid evolution of technology in this dynamic landscape.

The threats are evaluated based on their potential societal, safety, and financial impact, as well as the likelihood of their occurrence. For each threat, an indication of its potential impact is given by assigning a score from 1 to 5 (where 1 represents a very low impact and 5 a very high one):

Societal impact: this dimension assesses the extent to which a threat can disrupt society. It includes considerations such as the erosion of public trust in transportation systems, government entities, or other stakeholders. For instance, if a cyberattack were to compromise the safety or reliability of public transport, citizens might lose trust in these services, impacting their overall quality of life and well-being. Furthermore, the threat's societal impact could extend to the disruption of daily routines, causing inconvenience or even distress to individuals and communities.

Safety impact: this dimension measures the potential harm or danger a threat poses to people. It assesses the risk of physical harm, including injuries or loss of life, resulting from a cyberattack. For example, if the control systems of connected vehicles were compromised, it could lead to accidents or malfunctions that jeopardise passenger safety.

Financial impact: this dimension evaluates the extent to which a threat can cause financial losses. Such losses may result from various factors, including service disruptions, the need for system repairs, or compensation for damages incurred. In the context of a cyberattack on smart mobility systems, financial impacts could encompass the costs associated with addressing the attack, such as system repairs, legal ramifications, compensation to affected parties, or paying a ransom for stolen data that is critical for the functioning of key transportation systems.

For each type of attack linked to a given threat, an evaluation of the probability for this attack to occur is given. Attacks can either be labelled as low likelihood, medium likelihood, or high likelihood.

Both the impact and likelihood scores are derived from literature and experts' opinions.

2.1 Threats to connected vehicles

In 2015, a significant turning point occurred in the field of vehicle cybersecurity. Two hackers made history as cybersecurity researchers by demonstrating what could be done to a car using a computer remotely from home. The driver, a Wired journalist, experienced firsthand how these hackers took control of various car systems, including the air conditioning, windshield wipers, audio system, brakes, transmission, and remarkably, they even managed to shut down the engine. This event underscored the vulnerabilities in automotive cybersecurity and raised awareness about the need for stronger protections in modern vehicles.

In this chapter, we delve into the landscape of threats that pose risks to the safety and security of connected vehicles. Additionally, we present countermeasures that can be employed to safeguard these vehicles.

2.1.1. Alteration of vehicular sensors

Most affected:

Societal impact:

Safety impact:

Economic impact:

The alteration of vehicular sensors poses a critical threat to the security of connected vehicles. These sensors can broadly be categorised into two groups: vehicle dynamics sensors and environment sensors. In this chapter the main threats associated with these elements are presented.

Vehicle dynamics sensors

This includes sensors that provide measurements on a vehicles' state, such as:

- Inertial sensors

- Tire Pressure Monitoring Systems (TPMS)

- Magnetic encoders

Environment sensors

Environment sensors provide measurements relating to vehicular surroundings and include:

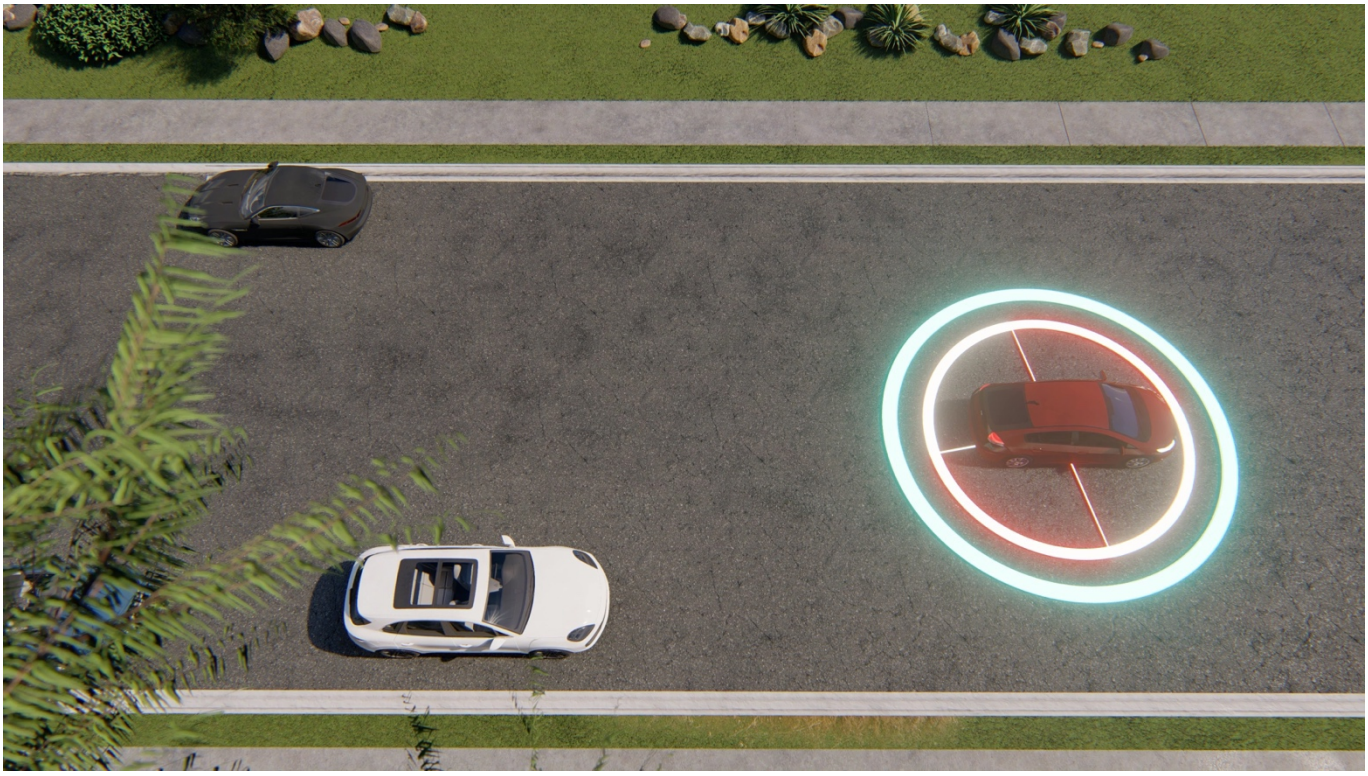
- Cameras

- Light Image Detection and Ranging (LiDAR)

- Ultrasonic sensors

- Radars

- GNSS



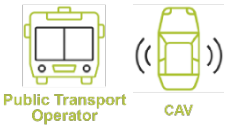
EXPERTS SAY

"Connected cars are essentially data centres on wheels, encapsulating a wealth of sensitive information and functionalities. However, this very characteristic also introduces a host of potential vulnerabilities and threats".

José Manuel Barrios
Head of Digital Transformation and Digital Solutions, Applus+ IDIADA

Inertial sensors threats

Most affected:



Inertial sensors encompass accelerometers and gyroscopes. Accelerometers gauge the acceleration experienced by the object they are attached to, while gyroscopes measure the rate of rotation around a specific axis[36].

Spoofing attack

Spoofing attacks targeting inertial sensors occur when malicious individuals employ consumer-grade speakers, transducers, directivity horns, and amplifiers to inject sound waves, thereby deceiving the sensors. These attackers can execute two distinct types of spoofing attacks by manipulating the injected analogue signals to impact the resulting digital signal. In side-swing attacks, the attackers strategically adjust the amplitude of the injected waveform to manipulate the vehicle's heading value[37]. During switching attacks, the attackers alternate between injecting waveforms of different frequencies, inducing phase pacing that leads to a continuous increase in the vehicle's heading value.

Acoustic attack

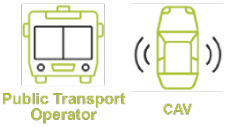
Attackers exploit spring-mass structures, such as Micro-Electrical Mechanical Systems (MEMS) gyroscopes and accelerometers, that possess a load resonant frequency, in what is known as an acoustic attack[38]. They manipulate acoustic waves, matching the load resonant frequency of the targeted cyber-physical system[39]. Researchers provide detailed information on the methodology of acoustic attacks, which involve measuring inclination parameters (roll, pitch, and yaw) and evaluating them using algorithms[40]. Researchers have demonstrated the susceptibility of MEMS-based inertial sensors to acoustic attacks, showcasing a case study that highlights how ADC converters' sampling drifts can contribute to such attacks[41]. In 2022, University of Michigan researchers used precisely tuned acoustic tones to deceive 15 different models of accelerometers to register non-existent movement. The findings question the assumption that hardware sensors can be automatically trusted by software.

Countermeasures

Researchers propose creating a physical barrier against the noise, utilising a differential comparator, and tuning the resonance frequency[42]. Other sources suggest several hardware design solutions, such as a low-pass filter, secure amplifier, acoustic dampening materials, and software defence mechanisms (e.g., randomised sampling or 180 degrees out-of-phase sampling)[43]. Researchers recommend the use of isolators and dampeners, low-pass filtering, a dynamic sample rate, and sensor fusion[29].

TPMS

Most affected:



Modern Tire Pressure Monitoring Systems (TPMS) have four pressure sensors for each tire, a TPM electronic control unit (ECU), and a receiver unit[44]. A receiver unit that may sometimes be connected to the ECU has the ability to collect packets sent by TPMS pressure sensors in or near a vehicle These packets contain information such as sensor ID, pressure and temperature readings. Normally, the TPMS ignores packets with sensor IDs that do not match any of the vehicle tires.

Spoofing attack

Faking tire pressure sensor readings lets attackers take control of the warning system in the car. This can make the warning light turn on, even if the tires are actually fine. It might even make the driver pull over unnecessarily, which can be risky, especially if on a busy road. In some cases, these tricks can affect multiple cars at once, causing confusion and unnecessary worry for drivers[34].

Reverse-Engineering attack

Attackers can conduct reverse engineering attacks on vehicle systems, where they remove and modify vehicle firmware, and expose vulnerabilities that can be exploited for future attacks[45].

Eavesdropping attack

Cyber attackers have the capability to carry out covert attacks on a car's TPMS by intercepting and analysing the sensor readings and data transmissions, thus posing a threat to the confidentiality of the system. This is because each TPMS sensor has a unique and unchanging sensor ID over its lifetime. Furthermore, TPMS are highly vulnerable to eavesdropping attacks due to the absence of robust authentication mechanisms in many TPMS electronic control units (ECUs) for verifying incoming messages

Countermeasures

Error checking, conflicting information detection, and filtering of false activation signals:

introducing simple error checking systems in the TPMS can help detect conflicting data and prevent false signals from causing issues. This can be achieved by adding a sequence number field and a cryptographic checksum without disturbing the TPMS operations. By implementing these changes, organisations can strengthen their defences against potential attacks that take advantage of weaknesses in TPMS software[34].

LFSR-based encryption:

introducing an encryption technique based on Linear-Feedback Shift Register (LFSR) to safeguard sensor IDs from potential attackers. The method utilises feedback loops to generate 64-bit encryption keys, ensuring resilience against brute force attacks. Employing XOR operations, this strategy minimises computational overhead. Consequently, Tire Pressure Monitoring Systems (TPMSs) can effectively thwart attacks aimed at compromising sensor IDs[46].

Orientation-based broadcasting:

a preventive measure against eavesdropping attacks consists in enabling signal transmission exclusively through restricted pathways, limiting the signal's reach. This strategic limitation serves to bolster TPMS defences against eavesdropping attacks, enhancing their overall security[47].

Encryption with anonymity techniques and short-term certificates:

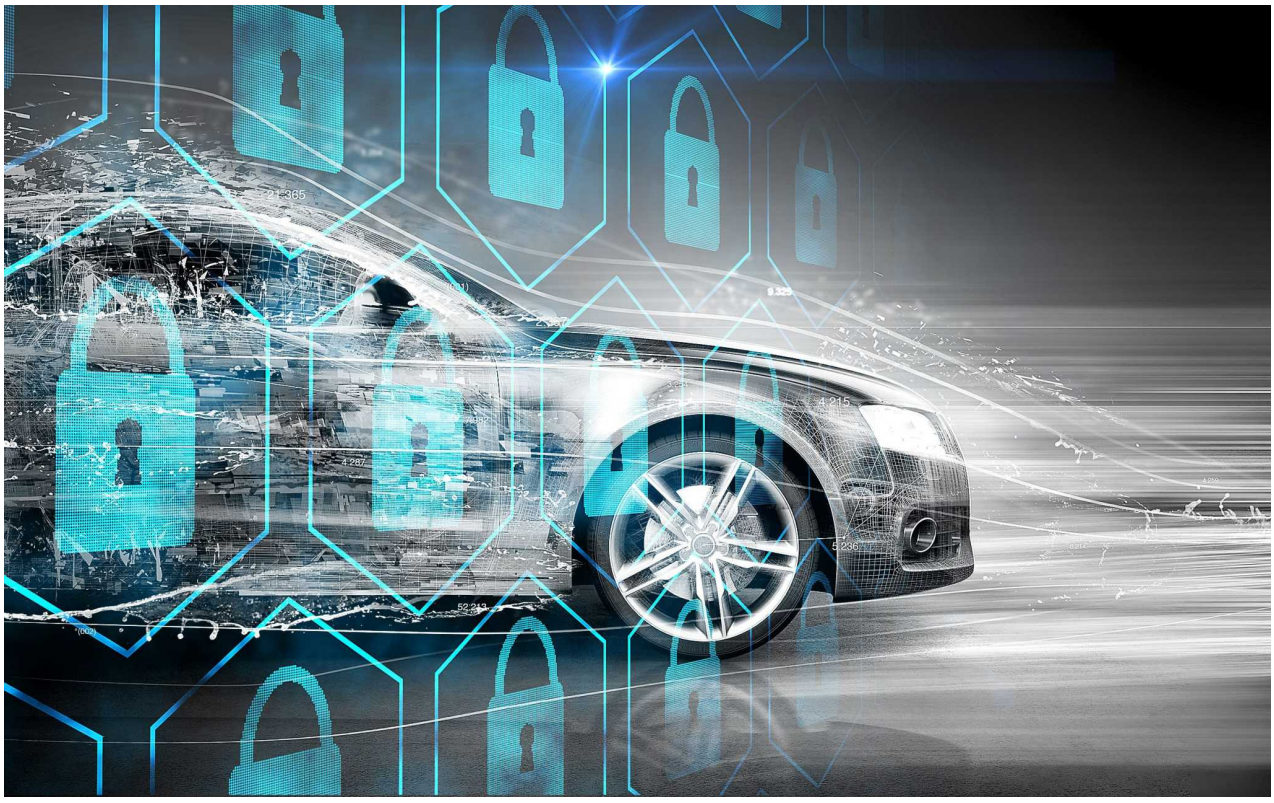
through the adoption of encryption techniques and employing anonymous methods, such as group signatures, and the implementation of temporary certificates it is possible to uphold the confidentiality of data processing and location. By leveraging these strategies, TPMS's can effectively safeguard user privacy and reinforce the security of their data storage infrastructure[4849].

Static code analysis:

static code analysis tools can be employed to detect and rectify potential ambiguities in code design[50]. These tools serve to pre-empt the exploitation of implementation bugs by malicious entities[51]. By integrating static code analysis, TPMS's can enhance their resistance to attacks that target vulnerabilities within the system's software.

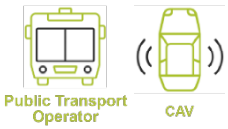
Removal of debugging symbols and error strings:

another recommendation is removing any "debugging symbols and error strings" from all code programmed in the ECU. By removing these signals and strings, it becomes harder for attackers to circumvent the code, thus improving the security of the TPMS[52].



Magnetic encoders

Most affected:



Magnetic encoders measure the angular velocity of a vehicle gear or wheel. One type of magnetic encoder is the wheel speed sensor, which measures a wheel's rotational speed using either magnetoresistance Integrated Circuits (ICs) or Hall ICs and is often used within Anti-Lock Braking Systems (ABS). Wheel speed sensors can also be used within indirect TPMSs, which use wheel speed sensors to calculate differences in rotational speeds and then estimate differences in pressure values.

Disruptive attack

During a disruptive attack, an attacker disrupts the magnetic field of the ABS's tone ring by placing an electromagnetic actuator between the wheel speed sensors, which are exposed underneath the vehicle body, and the ABS's tone wheel. Disruptive attacks are not precise since the tone ring's magnetic field still plays a large role in determining the speed sensor's output[53].

Spoofing attack

Spoofing attacks occur when malicious actors gain unauthorised entry to a system and falsify information. To conduct a spoofing attack on wheel speed sensors, an attacker must first place an electromagnetic actuator between a wheel speed sensor and the ABS's tone wheel. The attacker then shields the original magnetic field so that the malicious magnetic field will have a significant effect on the output of speed sensor[43].

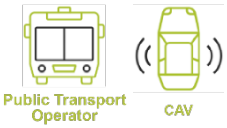
Countermeasures

PyCRA (Physical Challenge-Response Authentication):

PyCRA (Physical Challenge-Response Authentication) offers a safeguard for magnetic encoders or inductive active sensors. Unlike conventional cybersecurity methods involving query-response checks or encryption algorithms, PyCRA focuses on securing sensors before the digitization of their responses, effectively preserving the analogue signal. The transmission of the challenge occurs unpredictably, introducing a delay in the attacker's response[54]. Nonetheless, the potential bypassing of PyCRA using cost-effective microcontrollers and advanced circuitry design has been highlighted[44], especially when the attacker's sampling rate surpasses that of the victim's sensor. Recognizing the imperfections in PyCRA's security, some modifications are proposed, which involve altering phases under low signal-to-noise ratio conditions, contributing to a heightened resilience against spoofing attacks[44].

Cameras

Most affected:



Self-driving cars use cameras as their 'eyes' to understand what is happening around them. These cameras have several functions, like recognising traffic signs, spotting obstacles in the dark, assisting with parking by showing nearby objects, and collecting data about the surroundings to avoid accidents[55]. Additionally, they rely on cameras to gather information that complements data from other types of sensors.

Blinding attack

Blind collision refers to the activation of a car's camera sensors by directing a strong laser beam towards the camera, generating a loud noise, and causing the camera feed to be obstructed. Consequently, this can completely disable the vehicle's sensor system, affecting its ability to detect input controls[56]. Such interference can lead to signal distortion or even prompt the vehicle to apply emergency brakes unexpectedly[57].

Auto-control attack

The goal of an auto-control attack is to interfere with camera sensors by showing bursts of light, causing image instability and auto-controls to change[46].

Countermeasures

Multiple cameras and filters:

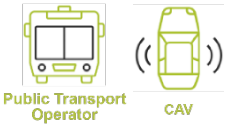
a defence strategy against blinding attacks includes the integration of multiple cameras equipped with monofocal lenses and infrared filters. These filters are designed to counteract infrared light interference specifically during daylight hours. Additionally, the adoption of photochromic glasses capable of filtering out long wave light is recommended[46].

Full environment multi-object tracking:

to reduce the impact of camera blindness, a technique that utilises a comprehensive method called "full-environment multi-object tracking (MOT) framework" is recommended[58]. This framework helps keep track of various objects over time, using a combination of early fusion and actual observed data. The early fusion gathers all instances or information about a specific object located in a blind spot at the beginning of each tracking process. These findings are then shared with the driver through the MOT system, which operates based on a technology known as Markov Decision Process (MDP) and reinforcement learning, alerting the driver whenever an object is detected.

Radars

Most affected:



Radar sensors are used in vehicles to detect nearby objects by emitting electrical signals and recording the time it takes for the signals to travel back to the radar receiver. Most radar sensors operate in the millimetre wave (mmW) frequency band. Long-range radar sensors are used for adaptive cruise control (ACC), central radar sensors are used for lane change assists (LCA), and long-range radar sensors are used for parking assistance to warn drivers of obstacles of the possibilities.

Jamming attack

Jamming attacks can interfere with radar sensors by transmitting signals in the same frequency band used by the sensors[59]. This interference can reduce the signal-to-noise ratio of the radar system, thereby increasing the ability to detect nearby objects[47].

Spoofing/Relay attack

Spoofing/relay attacks involve falsifying signals by malicious parties and persistent transmission of previously valid signals. Such an attack can be carried out using a Digital Radio Frequency Memory (DRFM) repeater that stores the signal and creates a digital duplicate for continuous retransmission Consequently, the second signal is considered valid by the radar system, allowing the attacker to attack[49].

Countermeasures

Data fusion and attack detection:

a combination of data fusion and attack detection is proposed. Data fusion requires combining information from multiple sensors to obtain an accurate estimate of the target location. That includes monitoring the operation of the radar system to detect abnormal behaviour that could indicate an intruder[47].

Filtering:

a filtering method can be used to counteract DRFM signals and prevent both jamming and spoofing/relay attacks using DRFM repeaters[60]. Dutta et al., (2018) use a hybrid filter that uses a modified Kalman filter and a Chi-squared detector to detect false data injection at random locations and reduce the impact of this data on radar sensor inputs[61].

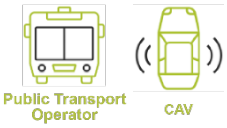
Spatio-Temporal Challenge-Response (STCR) approach:

in (Kapoor et al., 2018) the authors use a novel Spatio-Temporal Challenge Response (STCR) detection method to detect and mitigate spoofing attacks with multiple MIMO antennas and beamforming, allowing continuous surround detection our surroundings with signals in many different directions and reflected signals are detected It happens that if the reflected signal exceeds the noise limit, it is considered negative and is excluded from the distance calculation[62].

Each of these countermeasures can be used in a variety of ways to detect and mitigate radar attacks. By combining different approaches, robust and effective countermeasures can be developed that can protect radar systems from broadband attacks.

Ultrasonic sensors

Most affected:



Ultrasonic sensors can detect nearby obstacles and measure their distance from the vehicle[63]. The sensor sends an ultrasonic signal to detect nearby objects, which move toward an obstacle and bounce back to the sensor. The time lag between transmitting the signal and receiving the reflected signal can then be used to calculate the distance between the obstacle and the vehicle, these sensors are often used to assist drivers in low-speed operation such as parking.

Blind spot exploitation attack

Ultrasonic sensors in automobiles have the limitation of detecting very thin objects in their blind spot. This limitation can be exploited by attackers who are able to blindly place a flat object where a reversing vehicle, causing it to collide with the object[64].

Sensor interference attack

Sensor interference attacks can be carried out by attackers placing their own ultrasonic sensors on top of the vehicle's legitimate ultrasonic sensors, thereby hindering the accuracy of the sensor measurement. When two sensors are placed opposite each other, each sensor receives a signal from the other sensor in addition to its own reflected signal[54].

Cloaking attack

Cloaking attacks are a type of attack where attackers conceal nearby objects from ultrasonic sensors[47]. Attackers can achieve this by placing sound-absorbent materials around obstacles to prevent detection by the sensor. Objects can be concealed from ultrasonic sensors using this method[54].

Physical tampering attack

Ultrasonic sensors can be compromised by physical tampering, where attackers cover the receiver and transmitter of the sensor to disable its functionality. In a study by Lim et al. (2018), the researchers were able to render an ultrasonic sensor useless by covering it with scotch tape[54]. Attackers can use this technique to cause the sensor to fail and potentially create safety hazards. In 2019, researchers at Keen Security Lab, a division of the Chinese internet giant Tencent Keen, used stickers or paint to manipulate Tesla's Enhanced Autopilot, leading the vehicle to steer into oncoming traffic. This manipulation exploited the system's reliance on computer vision, revealing critical vulnerabilities in its driving decisions and emphasizing the need for enhanced security measures in autonomous driving technology[65].

Acoustic cancellation attack

Illegitimate signals can be used to cancel out legitimate ultrasonic signals in acoustic cancellation attacks. By transmitting a signal with a phase opposite to that of the legitimate signal, attackers can effectively reduce the signal's phase to zero[66]. This type of attack typically requires more resources and expertise than cloaking attacks and may be more difficult to execute.

Spoofing attack

There are three types of spoofing attacks: simple, random, and advanced. In a simple spoofing attack, an attacker sends a fake ultrasonic signal to an ultrasonic sensor that can reach the sensor before a valid signal is displayed, resulting in a false detection of a non-existent object[47]. In a random spoofing attack, a genuine ultrasonic signal is recorded beforehand and subsequently replayed to the ultrasonic sensor in a continuous manner. On the other hand, in an advanced spoofing attack, the attacker intercepts an incoming ultrasonic signal, eliminates the reflected signal through a cloaking attack, and replaces it with a fabricated reflected signal sent back to the ultrasonic sensor[53].

Jamming attack

Jamming attacks take place when an attacker persistently emits ultrasound pulses towards an ultrasonic sensor, resulting in the sensor becoming overwhelmed and incapable of accurately determining the vehicle's proximity to nearby objects[47]. Xu et al. (2018), in their work, successfully executed a jamming attack on a Tesla Model S vehicle operating in the self-driving Autopark and Summon modes[53]. This attack led to the vehicle colliding with obstacles that went undetected.

Countermeasures

Measures against blind spot exploitation, sensor interference and cloaking attacks:

To counter the potential risks of blind spot exploitation, sensor interference, and cloaking attacks, the following countermeasures are proposed[54]:

- Sensor Fusion and Backup Cameras: The use of sensor fusion and backup cameras can help ensure the accuracy and legitimacy of ultrasonic sensor measurements.

- Calibration of Sensors: Tampering can be prevented by balancing the sensors immediately after the vehicle is started.

- Advanced Algorithms: Advanced algorithms require a massive collection of real-time navigation data (i.e., 360-degree sensors) to train and test blind spot detection models. Models integrating 3D-CAD geometry and advanced computer vision techniques (i.e., pattern segmentation, colour edge detection, and background resolution) have the potential to improve real-time detection rates of blind spot areas.

Anti-spoofing and jamming measures:

Defence against sound cancellation attacks is limited, but many methods are presented to combat spoofing and jamming. Some of the more notable ones are:

- Physical Shift Authentication (PSA): It employs waveform randomization for the ultrasonic signal, accepting reflected signals only if they correlate

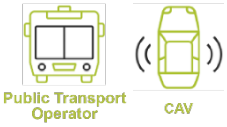
with the randomised waveform. Additionally, the frequency of the ultrasonic signal is continuously altered to thwart jamming attacks[53].

- Width-Based Signal Rejection: It employs a similar approach that involves estimating the width of incoming pulses and rejecting signals with suspicious pulse[56].

- Multiple Sensor Consistency Check (MSCC): MSCC utilises sensor redundancy to detect attackers and verify sensor measurements. In this method, a sensor shares its measurements with multiple other sensors to validate the accuracy of the measurements[53].

LiDAR

Most affected:



Light Imaging Detection and Ranging (LiDAR) systems utilise laser scanning techniques to create a three-dimensional map of the environment surrounding them. There are two types of LiDAR systems: scanning and solid-state. Scanning LiDARs employ one or more laser transceivers that rotate, while solid-state LiDARs can perform mapping without rotational components. Presently, scanning LiDARs are the primary type in use, but solid-state LiDARs are expected to dominate the market in the future. Scanning LiDARs generate a map of a vehicle's surroundings by emitting laser pulses while rotating. These pulses encounter objects in their path and bounce back to the LiDAR as echoes. If a pulse does not completely stop upon hitting an object, it may generate multiple echoes. By measuring the time between pulse transmission and echo reception and using the speed of light, the LiDAR calculates the distance to the obstacle. As the LiDAR continues to rotate, it creates a comprehensive three-dimensional, 360-degree view of nearby obstacles. This functionality is indispensable for Adaptive Cruise Control (ACC) and Collision Avoidance systems[46].

Replay attack

Attackers can intercept and capture signals transmitted by the LiDAR system. Subsequently, they can perform a replay attack by retransmitting the recorded signals to the LiDAR at a later time, intentionally misleading it into mapping objects that do not actually exist[67].

Relay attack

By extending replay attacks, malicious actors can execute relay attacks that hinder the LiDAR system's capability to accurately measure the distances of objects in close proximity. In a relay attack, attackers intercept LiDAR signals and transmit them to a receiver located elsewhere. The secondary receiver then retransmits these signals back to the LiDAR, resulting in an incorrect mapping of the nearby objects' locations[46].

Blinding attack

In a blinding attack, an external light source of the same wavelength as the infrared beam is applied to the LiDAR. This can cause saturation of the LiDAR, effectively denying the vehicle service[68].

Spoofing attack

Spoofing attacks manipulate LiDAR systems, leading them to detect objects that do not actually exist. In a research conducted in 2015 a LiDAR system was successfully spoofed, causing it to overestimate the distance to an obstacle[69]. Similarly, researchers discuss a spoofing attack on a LiDAR system, highlighting that their attack could also result in the LiDAR underestimating the distance to an obstacle[70].

Jamming attack

In this form of attack, light is directed back towards the scanner unit on the vehicle using the same frequency band as the laser[71]. Researchers highlights a cost-effective, readily available system that employs a Raspberry Pi and a low-power laser to disrupt the LiDAR sensor of a vehicle[72]. Researchers have devised a technique to manipulate lidar systems in autonomous vehicles, resulting in the removal of genuine obstacle data, prompting dangerous driving decisions. The study, presented at the 2023 USENIX Security Symposium, demonstrates the successful deletion of obstacle data and proposes potential defences, emphasizing the need for improved LiDAR and software upgrades to mitigate such attacks[73].

Denial-of-Service attack

Attackers can initiate denial of service attacks on LiDARs by introducing a substantial volume of counterfeit objects generated through jamming or spoofing techniques[57]. If the quantity of injected objects surpasses the maximum tracking capacity of the LiDAR, the system becomes unstable.

Countermeasures

Anti-spoofing and jamming measures:

- Side-channel: protection against spoofing attacks can be achieved by employing side-channel information to modulate the LiDAR laser. This approach effectively prevents attackers from injecting false reflection signals, as they lack knowledge of the secret key associated with the side channel[74].

- Multiple wavelengths: LiDAR systems could enhance their security by employing signals of various wavelengths. This measure would make it challenging for attackers to simultaneously target multiple wavelengths, adding a layer of difficulty to their malicious activities[46].

- Random probing: this technique is achieved by varying the time interval between laser pulses. By introducing this variability, attackers are unable to predict the precise moments to inject fake pulses within the interval. Random probing can also involve the skipping of certain pulses. If the LiDAR detects incoming pulses during these skipped intervals, it can infer that the vehicle is potentially being targeted by an attacker[59].

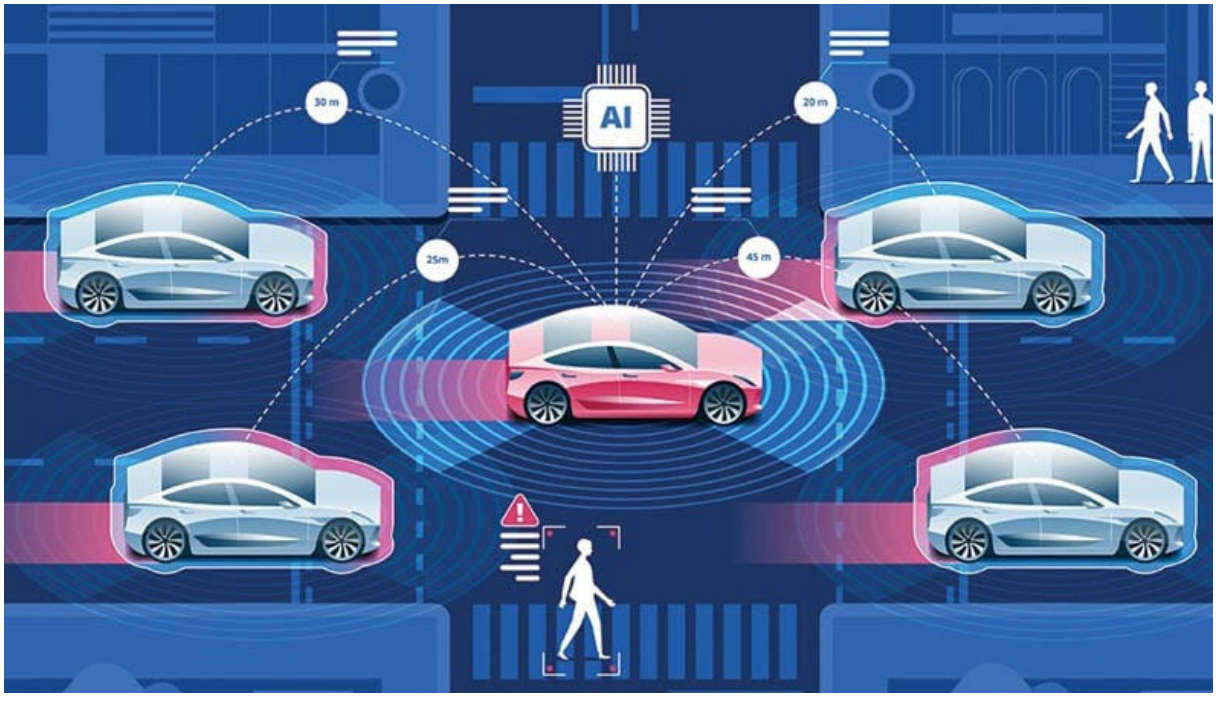
- Reducing pulse period: by reducing the pulse period, the attack window can be correspondingly shortened. Researchers demonstrated that LiDARs can perform multiple probes to detect random jamming, enabling them to decrease the pulse period and subsequently minimise the duration of the attack window[75].

Measures against replay and relay:

While there are general defences that can reduce the risk of spoofing and jamming attacks, there is a lack of dedicated research focused on preventing replay and relay attacks.

Measures against DoS attacks:

An effective measure to prevent denial-of-service attacks is to increase the number of objects that a LiDAR sensor can track simultaneously. This can be achieved by improving the hardware and software capabilities of the sensor. By increasing the number of objects that can be tracked, LiDAR can better distinguish between real and fake objects and ensure that the vehicle can operate safely even under attack[57].



GNSS interference

Most affected:

Global Navigation Satellite Systems (GNSS) such as Galileo and GPS are widely used in smart mobility for navigation, positioning and timing. Satellites transmit navigation messages to receivers on the ground, which calculate their distance from the satellites based on the transmission and arrival times of these messages. To determine their precise location, receivers need signals from at least four satellites. However, the lack of authentication and encryption in GPS signals, combined with the public availability of the spreading codes used in GPS (since it is an open standard with a transparent architecture)[59], makes GPS communication susceptible to attacks[76].

Spoofing attack

Spoofing attacks occur when malicious actors exploit the low power of GNSS signals and transmit a false one with a stronger signal strength to overpower the authentic signal, leading to compromised data integrity[62]. Attackers have two primary methods: tampering with the GNSS receiver to compute false locations and times[35] or transmitting data to disrupt the communication between the GNSS receiver and satellites, thus preventing the receiver from accurately determining its position. Spoofing attacks can serve as an initial step for carrying out subsequent attacks, such as replay and tunnel attacks[77].

Jamming attack

In a GNSS jamming attack, the signals from the sensors are intentionally disrupted to hinder the vehicle's ability to determine its location. Jamming is considered one of the easiest attacks to carry out due to the widespread availability and low cost of GPS jammers[78]. By introducing a sufficient amount of radio noise to the GNSS signal at the operating frequency (such as 1575.42 MHz), the receiver in the vehicle becomes incapable of distinguishing the authentic signal. In 2022, a GNSS spoofing attack sent several drivers from the taxi company Yandex to the same location in Moscow, causing massive traffic jams. This led to a breakdown of the taxi service and created a massive gridlock in Moscow[79].

Black hole attack

In a black hole attack, the attacker intentionally disrupts the transmission of information between vehicles in a self-organised Vehicular Ad hoc Network (VANET). These networks consist of nodes that can be vehicles or road-side infrastructure[80]. To carry out a black hole attack, attackers manipulate their GPS data and present themselves as having the shortest path to the destination node. Routing protocols like Link State Routing (LSR) and Ad-hoc On-demand Distance Vector (AODV) then allow them to respond to route request messages, as these protocols prioritise nodes with the shortest path to the destination node[81]. The malicious node subsequently discards the relevant packets, preventing the information from reaching its

intended destination. Black hole attacks can disrupt the network topology and potentially lead to its collapse. Gray hole attacks, a variant of black hole attacks, involve attackers alternating between normal behaviour and randomly dropping packets, making them particularly challenging to detect.

Countermeasures

Measures against GNSS spoofing:

to defend against GNSS spoofing attacks, several countermeasures have been proposed, such as signal encryption, drift and incoming signal direction analysis, and monitoring GNSS signals to ensure relative changes fall within a threshold. Other preventive measures include securing time tracking, reducing the lifespan of pseudonym certificates, and logging timing changes[63]. A cryptographic and military-grade implementation of GNSS is regarded as the most secure solution to spoofing.

Measures against GNSS jamming:

to combat jamming attacks, one method involves using inertial sensor measurements[64]. Another method includes using Receiver Autonomous Integrity Monitoring (RAIM) detection through both GPS and the vehicle's Inertial Navigation System (INS), which consists of inertial sensors[82]. Additionally, the authors of various studies recommend using a secondary or hybrid navigation system for GPS signals, such as Galileo or NAVIC, to strengthen the system against jamming attacks.

Measures against black hole attacks:

to prevent black hole attacks, constructing multiple routes to the destination node and utilizing Road-Side Units and associated transportation infrastructure can help to detect such attacks[67].

Vehicle theft

Most affected: 

Modern car security heavily relies on Remote Keyless Systems (RKS), which provide convenient means for locking and unlocking vehicles without the need for mechanical keys. By simply pressing a button on the car's fob or even approaching the vehicle, users can control access. However, RKS primarily employs a request-response protocol between the fob and the car's radio transceiver with limited security measures in place. Over time, various security vulnerabilities have been discovered, leading to the evolution of RKS to mitigate such attacks[83].

Jamming attack

Jamming devices operate by emitting signals within the same frequency range as key fobs, resulting in a powerful interference that disrupts the communication between the key fob and the car transceiver. When the driver exits the car and presses the lock button on the key fob, the car's locking mechanism fails to engage if an active jammer is present within a range of 30 meters. While many cars provide a visual indication of the locking action, such as blinking indicators, some individuals may not notice or pay attention to these signals. Exploiting this vulnerability, a thief can take advantage of the unlocked car after the driver has left the parking area and gain unauthorised access to the car's OBD (On-Board Diagnostics) interface, facilitating the theft of the vehicle.

Scan attack

A scan attack poses a significant threat to systems employing the rolling code technique[84]. This attack can be executed by transmitting various codes to the car transceiver, as long as the transmitted code aligns with the code of the car transceiver. This attack method is relatively straightforward. The time required to unlock the car using this attack technique varies based on factors such as the number of bits in the random challenge, the method used to generate the random challenge, and the number of attempts made by the intruder[85].

Playback attack

In this scenario, an intruder possesses a device capable of wirelessly recording transmitted messages. Subsequently, when the car driver is absent, the intruder can replay the recorded messages to the car transceiver, thereby gaining access to unlock the car[71].

Challenge Forward Prediction attack

In the Challenge Forward Prediction attack, an intruder utilises a device to capture multiple interrogation messages transmitted by the car transceiver when the door handle is pulled. Using these recorded messages as a reference, the intruder attempts to predict the next interrogation message. Subsequently, the intruder approaches the car owner and sends the predicted interrogation message to the Customer-Identification Device (CID) present in the car owner's pocket. The CID responds with a message, which is then recorded by the intruder. Later, the intruder returns to the car, pulls the door handle, and replays the recorded message from the CID[86].

Two-Thief (Relay) attack

The Two-Thief Attack is a well-known relay attack method commonly employed in Passive Keyless Entry Systems (PKES). In this attack, one thief positions themselves near the car, while the other thief stands in proximity to the car owner. Both thieves utilise signal amplification devices. The thief near the car initiates the attack by pulling the door handle, causing the car transceiver to send an interrogation message to the Customer-Identification Device (CID). The CID, which functions similar to a key fob or a credit card, is typically kept in the car owner's pocket. Since the CID is beyond the transmission range, the amplifier utilised by the thief near the car enhances the signal, enabling it to reach the amplifier employed by the thief near the car owner. Subsequently, the signal is forwarded to the CID, prompting it to respond with a valid code. This code is then transmitted back to the car transceiver via the thieves' amplifier devices[72]. It is not illegal to sell, buy or possess the technology that allows easy and quick car theft. Most of these devices are available for affordable prices on the most popular online stores, like eBay or Amazon. This is most likely the reason behind the 25% rise in vehicle thefts that occurred in the UK between 2021 and 2022[87].

Countermeasures

Key jamming

making sure that the car is actually locked is the best countermeasure against key jamming. Car manufacturer can employ several techniques in order to confirm to the owner that the car is effectively lock.

Symmetric key

Researchers developed a system[88] that utilises symmetric cryptography for encryption. It comprises a car transceiver and a key fob with a programming interface. When processing a command, such as unlocking the car, the transceiver initiates an authentication request to the key fob. The authentication process involves the key fob sending an authentication message, which is constructed using randomly selected memory locations. The car transceiver generates its own authentication message and compares it with the received Electrically-Erasable Programmable Read-Only Memory (EEPROM) message. Both the key fob and the car transceiver are assumed to have an EEPROM where shared keys are stored. The programming interface is employed to synchronise the EEPROM content between the key fob and the car transceiver. This protocol is effective against scan, playback, forward prediction, and two-thief attacks.

2.1.2 Alteration of In-Vehicle communications

Most affected: 

In this section, we analyse threats within In-Vehicle communications systems. Understanding the vulnerabilities in communication protocols and networks is vital for ensuring the security and integrity of data exchanges within connected vehicles. We also propose effective countermeasures to mitigate the risks associated with these threats.

CAN bus

- Bus off attack
- Denial-of-Service attack
- Masquerading attack
- Injection attack
- Eavesdropping attack
- Replay attack

FlexRay

- Eavesdropping attack
- Static segment attacks

LIN

- Message spoofing attack
- Header collision attack
- Response collision attack

Automotive Ethernet

- Traffic integrity attack
- Traffic confidentiality attack
- Network access attack
- Denial-of-Service attack

MOST

- Jamming attack
- Synchronisation disruption attack

CAN threats

Most affected: 

The most common protocol for in-vehicle communications is the Controller Area Network (CAN). It allows packets to be transferred between multiple electronic control units (ECUs) via interconnected buses. CAN uses a broadcast network and has many advantages including flexibility, low network congestion, and reduced wiring costs. This is because CAN uses multiple wiring architectures to eliminate the need for redundant wiring between ECUs. However, the protocol cannot provide real-time performance, which is necessary for critical security applications. It also lacks a mechanism for authentication and encryption, leaving it vulnerable to security threats[6].

Bus-off attack

Bus-off attacks occur when malicious actors deliberately send bits, including in the identifier field and other fields, in a continuous manner. This action leads to the incrementation of the transmit error counter (TEC) within the Electronic Control Unit (ECU). Once the TEC surpasses a value of 255, the affected ECU is forced to shut down as a protective measure[89].

Denial-of-Service attack

Denial of Service (DoS) attacks take place when attackers persistently transmit high priority messages with the intention of obstructing legitimate low priority messages[90]. In a standard CAN packet, the message priority is determined by the identifier segment. Attackers can designate a low value to the identifier segment of their messages to grant them a higher priority status. These DoS attacks can serve as a means to carry out control override attacks, enabling attackers to assume control of the targeted vehicle[91].

Masquerading attack

Masquerading attacks involve attackers impersonating genuine nodes within a network. There are two main vulnerabilities in the Controller Area Network (CAN) protocol that enable masquerading attacks[74,75]. Firstly, CAN frames lack encryption, allowing attackers to analyse them and identify system entry points. Secondly, CAN lacks support for message authentication, which means recipients are unable to verify the legitimacy of the message source, making it possible for illegitimate frames to be sent undetected.

Injection attack

Injection attacks involve the malicious insertion of counterfeit messages into an automotive bus system. Attackers can exploit various entry points, such as compromised Electronic Control Units (ECUs), On-Board Diagnostics II (OBD-II) ports, or infotainment and telematics systems[75]. One significant vulnerability lies in the lack of authentication for sending or receiving nodes in traditional Controller Area Network (CAN) protocols. As a result, illegitimate frames can go undetected since there is no mechanism to verify their authenticity.

Eavesdropping attack

Eavesdropping attacks occur when unauthorised individuals successfully infiltrate vehicular networks and gain access to the transmitted messages. The broadcast nature of Controller Area Network (CAN) transmissions enables attackers who have penetrated the in-vehicle network to eavesdrop on CAN communications and analyse patterns within legitimate CAN frames[75].

Replay attack

In a replay attack, attackers continually resend valid frames to impede the vehicle's real-time functioning[75].

Countermeasures

Message Authentication Code (MAC):

in the context of securing Controller Area Network (CAN) messages, various types of attacks, such as masquerading, eavesdropping, injection, and replay attacks, can occur when messages are not encrypted and authenticated. One potential countermeasure is the use of Message Authentication Code (MAC). However, incorporating MAC into standard CAN data fields, which allow for up to 8 bytes, poses challenges. As a result, researchers have explored the development of new protocols or spreading MAC across multiple transmissions.

Altered protocols for CAN message authentication:

Researchers have proposed altered protocols to address the authentication of CAN messages. Researchers evaluate these protocols based on industry-specific criteria, including cost-effectiveness, backward compatibility, vehicle repair and maintenance, sufficient implementation details, and acceptable overhead[92]. While no single solution meets all the criteria, WooAuth and VatiCAN emerge as promising options. WooAuth alters the extended CAN protocol to accommodate authentication codes, while VatiCAN emphasises backward compatibility while ensuring sufficient implementation details and minimal overhead. However, the authors also question the fundamental suitability of the CAN bus for secure communication.

Lightweight authentication framework:

one countermeasure includes lightweight authentication framework comprising two phases: ECU authentication and stream authorization. ECU authentication employs asymmetric cryptography, allowing ECUs to authenticate against a central security module[93]. In the stream authorization phase, symmetric cryptography is used to request keys for initiating message streams. This framework aims to provide secure communication while minimizing resource requirements.

Source Authentication Protocol (SAP):

Researchers introduce the Source Authentication Protocol (SAP), which utilises a one-way hash chain and a sender-based group key for authentication[94]. SAP guards against masquerading and replay attacks by accurately identifying the sender of each message. By employing a multi-class classifier, SAP can detect masquerading attacks by comparing the predicted sender with the actual CAN ID of the message.

Partial MAC protocol:

Researchers propose a protocol that defends against replay, masquerading, and injection attacks. This protocol involves sending a partial MAC in each frame, enabling tampering detection at both the individual frame and entire section levels. By incorporating this additional information in the frames, the protocol enhances the security of the CAN bus[95].

Intrusion Detection Systems (IDS):

Intrusion Detection Systems (IDS) serve as an alternative or supplement to MAC for safeguarding CAN networks. Choi et al. (2018) suggest the use of an external monitoring unit that identifies analogue characteristics of the electrical CAN signal for authentication and intrusion detection[74]. They also introduce VoltageIDS, an IDS that leverages ECU signal inconsistency for training and testing phases, detecting compromised ECUs. The IDS proposed by some researchers named Offset Ratio and Time Interval based Intrusion Detection System (OTIDS), periodically requests data frames from nodes within the CAN bus to monitor response time and offset ratio, effectively detecting denial of service, masquerading, and injection attacks[96]. Other researchers, such as, propose anomaly-based IDS that detect general anomalous behaviour rather than relying on known attack patterns[75].

Timing-based IDS:

Tomlinson et al., 2018 present an IDS that identifies attacks by monitoring timing changes in CAN traffic. For instance, increased broadcast frequency of specific CAN IDs can indicate the occurrence of an injection attack[97]. By observing and analysing timing variations, this IDS provides an additional layer of security against potential threats.

FlexRay threats

Most affected:

The FlexRay protocol uses two parallel channels to transmit data in synchronous and asynchronous modes. It can be used for time-critical applications and has reliability and fault tolerance. However, the cost of implementation is high. FlexRay handles logical errors through checksums and redundancy mechanisms.

Eavesdropping attack

Similar to CAN, eavesdropping on the FlexRay protocol refers to the unauthorised access and comprehension of FlexRay messages. FlexRay shares similar security concerns with CAN, namely the risk of security primitives leakage, network privacy compromise, and data confidentiality breaches[98].

Static segment attack

The security measures for FlexRay should primarily concentrate on the static segment, as it poses the highest risk if compromised[99]. A static segment attack refers to an attack targeting the static segment of the FlexRay communication cycle. Such attacks can encompass various types, including masquerading, injection, and replay attacks. By addressing the security vulnerabilities within the static segment, the

overall security of the FlexRay system can be significantly enhanced.

Countermeasures

In order to combat eavesdropping attacks, incorporating authentication mechanisms becomes crucial. This chapter explores various countermeasures that focus on authenticating messages within the FlexRay system's communication cycle.

Hardware co-processors for static segment security:

it is possible to enhance the security of the static segment by employing hardware co-processors. This chapter delves into the use of dedicated hardware components to authenticate and protect the messages transmitted during the static segment[83].

SAFE framework with TESLA authentication:

Researchers introduce the Security-Aware FlexRay Scheduling Engine (SAFE)[100], a scheduling framework that integrates the Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol[101]. This chapter discusses the incorporation of TESLA authentication within the FlexRay system to bolster its security against static segment attacks.

Lightweight CAN Authentication Protocol (LCAP) integration:

one solution is based on the integration of the Lightweight CAN Authentication Protocol (LCAP) within the FlexRay network[82].

FlexRay authentication and key transmission:

to secure FlexRay authentication and cryptographic key transmission, a possible solution is the utilization of FlexRay's dual-channel mode to divide message authentication codes, thereby enhancing the security of the FlexRay system against potential attacks[102].

LIN threats

Most affected: 

The LIN (Local Interconnect Network) protocol is a widely used serial communication protocol specifically designed for automotive applications. It provides a cost-effective and lightweight solution for connecting various electronic components within a vehicle, such as switches, sensors, actuators, and modules. LIN is typically used for low-speed communication tasks that require simple and reliable data transfer. The LIN protocol operates on a single-wire bus, reducing the complexity and cost of wiring within the vehicle. It uses a master-slave architecture, where a single LIN master device controls one or more LIN slave devices. The master device initiates communication by sending requests to the slaves, and the slaves respond accordingly. LIN messages consist of a header and a data field. The header contains

information about the message type, identifier, and checksum, while the data field carries the actual payload. The protocol supports different message types, including event-triggered messages, sporadic messages, and diagnostic messages. LIN provides features like message collision detection, message buffering, and automatic node configuration, making it suitable for applications that require low data rates, deterministic behaviour, and simple network configurations. It is commonly used in various automotive systems, such as body electronics, climate control, and interior lighting.

Message spoofing attack

Message spoofing attacks involve the transmission of illegitimate messages with inaccurate information to disrupt vehicular communications. LIN master-slave communications are vulnerable to message spoofing attacks due to two specific vulnerabilities[103]. Firstly, a master within a LIN network can send a message that causes a slave to go into sleep mode. Secondly, the master can manipulate the SYNC field in a LIN message to synchronise the slaves. Attackers can exploit these capabilities of the master to spoof messages, instructing slaves to sleep and effectively shutting down the LIN network. They can also tamper with synchronization by altering the SYNC field in spoofed messages.

Response collision attack

Response collision attacks occur when an attacker sends an illegitimate message simultaneously with a legitimate message. These attacks exploit the error handling mechanism in the LIN protocol, which triggers when a slave node sending a response detects a mismatch in the bus value and terminates transmission[104]. Attackers take advantage of this mechanism by either sending a false header or waiting for the master node to send a header. They then send a false response that collides with the legitimate response from a slave node. This collision alters the bus value, causing the legitimate slave node to cease transmission. If the attacker can calculate the correct checksum used in responses, other nodes will consider the false message to be from a legitimate source.

Header collision attack

Header collision attacks occur when an attacker sends a false header to collide with the legitimate header sent by the master node. The legitimate header specifies that a particular slave node should provide a response, but the attacker's collision disrupts the intended response publisher. When the new publisher node sends a response, attackers can carry out a response collision attack to inject their own false message. This manipulation of the sequence of responses within the LIN bus enables attackers to keep automated vehicle sliding doors open or lock steering wheels while vehicles are in motion[88].

Countermeasures

Countermeasures against these types of attacks can include the implementation of secure authentication mechanisms, message integrity checks, and robust error handling protocols within the LIN network. Additionally, regular monitoring and analysis of LIN bus traffic can help detect and mitigate suspicious activities or anomalies that could be indicative of attacks[88].

MOST threats

Most affected: 

The Media-Oriented Systems Transport (MOST) protocol supports synchronous and asynchronous channels for data communication. It can support GPS applications and radio. While it meets infotainment needs, it fails to provide enough bandwidth as needs peak[87].

This can cause resource consumption and performance degradation in the MOST network[105].

Jamming attack

Jamming attacks are a common threat to MOST networks. In this approach, the attacker continuously tries to destroy communication between nodes by sending misleading messages. An attacker can target a legitimate message with low priority, causing delay or loss of critical data.

In addition to issuing misleading messages, the attacker can further request data channels on the MOST transmission through the control channel.

Synchronisation disruption attack

In this attack, the attacker tries to change the synchronization of the MOST by constantly sending a fake timestamp. As a result, valid nodes in the network may lose synchronization and be unable to communicate with each other.

An attacker can use a variety of techniques to perform parallel nuisance attacks, such as continuous transmission of a spurious timetable, tampering with the sync signal, and changing the clock signal[87].

Countermeasures

The security of the MOST bus has received limited attention in research. However, some recommendations for securing general automotive bus systems can be adapted for the security of the MOST bus[89]. These recommendations emphasise the importance of authenticating senders, encrypting transmissions, and implementing gateway firewalls. It is essential for future research to explore protective measures specifically targeting synchronization disruption attacks and jamming attacks on the MOST bus. By addressing these areas, the security of the MOST bus can be enhanced.

Automotive Ethernet threats

Most affected: 

Automotive Ethernet is considered the physical layer standard in the automotive domain. Due to its capabilities, it can be used for advanced applications in vehicles such as advanced vehicle assistance systems. The main advantage is that it reduces wring costs because it supports switched network technology.

Network access attack

Network access attacks involve unauthorised access to the Ethernet network, which can facilitate other types of attacks or enable control over hosts or switches. Attackers can physically connect to unconnected ports on switches[106] or gain remote access through social engineering[107].

Traffic confidentiality attack

After gaining network access, attackers can conduct traffic confidentiality attacks, allowing them to eavesdrop on network traffic. They can analyse messages and replies to gather information about the network's structure and topology[91]. Listening devices can be attached to cables between hosts and switches or between switches to intercept network traffic. Attackers can exploit the flooding behaviour of switches to perform MAC flooding attacks, enabling them to eavesdrop on all frames[108].

Traffic integrity attack

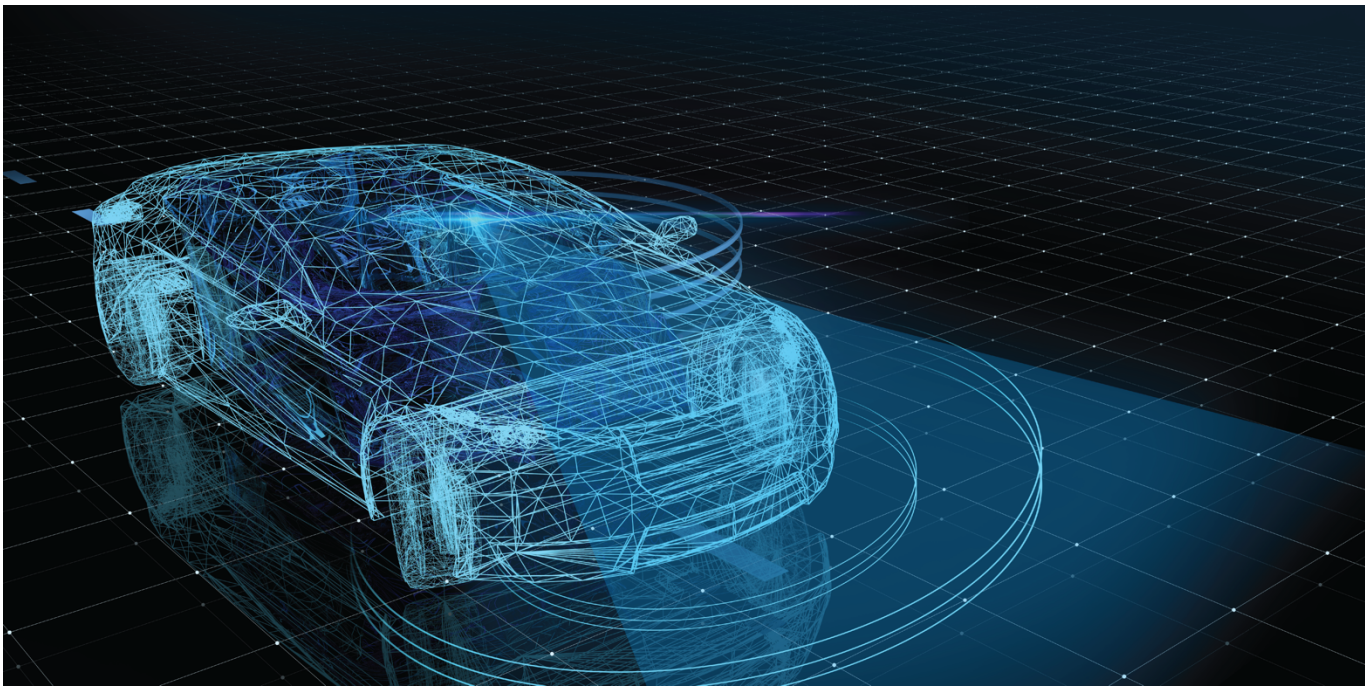
Traffic integrity attacks involve altering network traffic. Attackers can manipulate the Address Resolution Protocol (ARP) and the Dynamic Host Configuration Protocol (DHCP) to capture and control network traffic[109]. These attacks can lead to man-in-the-middle attacks, where network traffic is redirected to the attacker's node for manipulation[110]. Session hijacking attacks[111] and replay attacks[112] are other examples of traffic integrity attacks.

Denial-of-Service attack

Denial of Service attacks aim to disrupt Ethernet services by damaging physical equipment or overwhelming the system[91]. Layer 1 attacks physically damage links or circuitry, rendering the Ethernet service completely inoperable. Layer 2 attacks involve resource exhaustion attacks, where frames are continually sent to exhaust system resources, or protocol-based DoS attacks that exploit the Spanning Tree Protocol (STP) by continuously sending STP messages[95].

Countermeasures

To address these threats, various countermeasures can be implemented. Authentication methods and frame replication approaches can safeguard against traffic confidentiality and traffic integrity attacks[113]. Virtual Local Area Network (VLAN) segmentation can help prevent network access attacks. Metering Ethernet frames[114] and firewall DoS attack detection[115] are proposed as countermeasures against DoS attacks. Router-based security, access control, secure protocols, and security monitoring are also important measures to enhance the security of plain Ethernet[91].



2.2. Data-related threats

Most affected:

Data-related threats in the field of smart mobility refer to the unauthorised access, acquisition, or disclosure of sensitive information related to transportation systems. This information can include personal information, location data, payment data, and other sensitive information that can be used to track individuals, vehicles, or transportation networks.

Ransomware attack

As explained previously, a ransomware is a type of malicious software that encrypts the victim's files, making them inaccessible until a ransom is paid, typically in cryptocurrency. In the context of smart mobility, these attacks can compromise sensitive data related to user information, location tracking, or vehicle control, posing significant risks to the safety and security of individuals and the integrity of smart mobility systems. Moreover, such attacks can undermine user trust and confidence in the security and reliability of smart mobility technologies, hindering the widespread adoption of these systems. In 2022, Chinese electric automaker NIO suffered a ransomware attack in which the personal information of over 100,000 users was compromised. The breach occurred through a third-party supplier that provides data analysis services to NIO. The stolen information included users' names, mobile phone numbers, email addresses, and vehicle license plate numbers[116]. To mitigate the risks, implementing measures such as regular system updates, data encryption, network segmentation, and comprehensive security protocols, is widely considered as the best approach. Additionally, conducting regular security assessments and employee training on cybersecurity best practices can help enhance the overall resilience of smart mobility systems against ransomware threats[117].

In 2020, the Southeastern Pennsylvania Transportation Authority (SEPTA) faced the challenging task of recovering from a ransomware attack. This cyberattack forced the Philadelphia-area transit agency to suspend its real-time bus and rail information services for a duration of two weeks. The incident created considerable frustration among customers who were returning to the service's lines after a pandemic-induced decline in ridership[118].

Phishing attack

Phishing refers to a type of cyber-attack where attackers try to trick individuals into revealing sensitive information such as passwords, credit card details, or login credentials by masquerading as a trustworthy entity through fraudulent communication channels like emails, text messages, or fake websites. In the context of mobility data, phishing attacks can target individuals or organizations involved in the collection, processing, or storage of such data.

In 2023, Renfe (public operator dedicated to the transport of passengers and goods by rail in Spain) introduced several innovations to promote the use of public transportation, especially among young people. Amid these updates, some individuals took advantage of the situation to carry out scams by impersonating Renfe and advertising products that do not actually exist. This type of phishing was conducted through false advertisements on social media, which lead to another webpage

falsely claiming the existence of an annual transportation card[119]. Once on the form, all the traveller's personal information is requested, including their bank account details. To prevent such incidents, organizations should implement regular staff training, as phishing remains the most common form of data-related cyber-attack, responsible for 43% of breaches in 2021, according to Verizon's Data Breach Investigations Report[120].

Insider attack

Insider threats occur when individuals with authorised access to mobility data misuse or intentionally abuse their privileges, jeopardizing the security and privacy of such data. Insider threats can arise from current or former employees, contractors, or partners who have access to mobility data systems and may exploit their privileges for personal gain or malicious purposes.

In 2018, an Apple employee, Xiaolang Zhang, was arrested by the FBI for attempting to sell commercial secrets related to the company's autonomous driving project[121].

Unauthorised access to corporate or supply chain resources

Unauthorised access to corporate or supply chain resources in the smart mobility sector poses severe risks, including data breaches, intellectual property theft, and service disruptions.

A notable incident happened in Denmark in 2022 highlights these dangers[122]. In this case, all trains operated by DSB, the country's largest train operating company, came to a standstill for several hours. Initially assumed to be a sophisticated OT systems attack, the disruption was, in fact, triggered by a ransomware incident involving the subcontractor Supeo. Supeo's decision to shut down its servers due to the ransomware attack rendered the mobile application used by train drivers inoperative, compelling them to bring their trains to an immediate halt.

Privacy breach in cars

Researchers have discovered that car brands have insufficient privacy protection measures in place, making them the worst category of products for privacy. Many car brands excessively collect personal data beyond what is necessary for vehicle operation, and many engage in the dubious practice of deriving sensitive inferences about users. Manufacturers can then share or even sell personal data to various entities, including service providers, data brokers, and law enforcement, raising serious concerns about privacy violations and potential harm.

A recent study from Mozilla uncovers alarming privacy risks associated with modern car manufacturers. Analysis of 25 brands revealed extensive data collection practices surpassing operational needs. Concerns were raised over the widespread sharing and selling of user data, with limited user control over personal information. Inadequate security measures further exacerbate the vulnerability of sensitive data, emphasizing the necessity for stringent privacy regulations and heightened industry compliance[123].

Data poisoning in ITS systems and AI

Data poisoning is a significant cybersecurity threat for AI systems in smart mobility. It involves the manipulation of data used to train artificial intelligence algorithms to produce inaccurate or malicious results. In the context of smart mobility, data poisoning can have severe consequences,

affecting the safety and reliability of connected and autonomous transportation systems. When AI algorithms are trained on poisoned data, they can develop biased or flawed decision-making capabilities. For example, in autonomous vehicles, poisoned data could lead to incorrect perception of the environment, navigation errors, or dangerous driving behaviour. On top of this, more and more cities are equipping their traffic lights with AI sensors to optimise flows. This obviously generates exposes these systems to data poisoning threats, Data validation and quality control represents the main countermeasure to this threat. Other strategies include anomaly detection algorithms, using diverse data sources and AI model verification[124].

Formjacking attack

MEDIUM LIKELIHOOD

Formjacking is a cyberattack technique used by cyber attackers to steal sensitive information, particularly credit card details, from online forms. It involves the injection of malicious code into a website's payment processing page, which then captures and sends the entered data to a server under the attacker's control. This technique allows attackers to obtain users' credit card numbers, CVV codes, and other personal information without their knowledge.

Despite not being a case directly related to urban mobility, it is essential to highlight the data breach involving complete credit card information, including CVV, of around 100,000 customers of the Spanish airline, Air Europa[125]. This incident poses a significant potential threat to any online ticket sales service related to citizens' mobility. The cyberattack occurred through the airline's customer-facing website, using a technique known as web skimming or Magecart. The attackers successfully modified the website's source code where customers enter their credit card details for purchases, allowing this information to be transmitted to the payment gateway as well as a malicious server. As a result, customer data was collected in real-time as they made ticket purchases. This incident occurred despite the fact that Air Europa has been PCI-DSS certified since 2020.

Countermeasures

- Prepare risk analyses that identify, especially, critical processes and assets to deploy proportional prevention, protection, and response measures.

- Conduct periodic security audits and vulnerability analysis when making changes to systems or architecture to prevent information exposure due to configuration errors.

- A Private Impact Assessment (PIA) should be carried out to analyse risks and establish appropriate protective measures to ensure data security and privacy.

- In case of an incident involving personal data that could affect people's rights and freedoms, you must inform the competent authority within a maximum period of 72 hours.

Ransomware attack:

- Maintain updated and offline backups to prevent ransomware from encrypting them as well.

- Equip professional terminals with the best protection tools, such as EDR (Endpoint and Response System) for continuous monitoring of cyber threats.

- Have a business continuity plan and a disaster recovery plan and verify it through simulacres.

Phishing attacks:

- Conduct periodic educational training on security and improve practices in email usage to keep employees alert to phishing tactics.

- Provide appropriate anti-fraud training, especially for finance and procurement staff.

- Conduct phishing simulations among your employees to assess the level of preparedness.

Insider attacks:

- Limit employees' access to the minimum necessary for their tasks.

- Observe and analyse employees' digital actions for any unusual or suspicious behaviour.

Unauthorised access chain resources:

- Audit suppliers to evaluate and demand strong cybersecurity measures in their operations.

- Implement a robust vendor risk assessment program to regularly evaluate the cybersecurity posture of suppliers.

- Implement network segmentation to limit access to sensitive data and critical systems, reducing the risk of lateral movement in case of a breach within the supply chain.

Privacy breach in cars:

- Consider cybersecurity from the beginning of any digitisation project and apply the "security by design" concept.

- Consider interoperability conflicts between systems that may pose information security problems.

- Protect personal data with suitable measures (such as firewalls, dual-factor authentication access controls) and store them with secure encryption to prevent intruders from stealing them in plain text.

Data poisoning in ITS systems and AI:

- Verify the integrity and quality of input data before it is used for training or decision-making. Identify and eliminate any anomalies, outliers, or suspicious data points that could be indicative of poisoning attempts.

- Implement anomaly detection mechanisms to identify sudden deviations in model outcomes or behaviour, which could be indicative of data poisoning attacks.

Formjacking attack:

- Regularly conduct web application security tests including vulnerability assessments and penetration testing, to identify and patch vulnerabilities.

- Consider cybersecurity from the beginning of any digitisation project and apply the "security by design" concept.

EXPERTS SAY

"Securing data in the cloud can be quite complex, considering issues like where the data centres are located and who might be able to access the information. Even though companies like AWS and Google offer security tools, it's essential for the data owners themselves to make sure the data is encrypted well to prevent unauthorised access. Laws about where the data is stored can also make things tricky, highlighting the importance of protecting our data.

Alejandro Adalid Damerau
Cybersecurity Officer, Siemens Mobility

2.3 Threats to Infrastructure and systems

Most affected:

Societal impact:

Safety impact:

Economic impact:

In this chapter, we focus on the main threats that affect both the physical and digital infrastructure of transport systems and present common countermeasures.

Attack to electric vehicle supply equipment

There are several potential cyber-attacks that can target charging infrastructure for electric vehicles (EVs) or EVSE (Electric Vehicle Supply Equipment). In 2022, in an analysis of 12 electric vehicle charging systems, without specifying names, Sandia National Laboratories[126] found security flaws that exposed usernames, passwords, and credentials in an unencrypted format. Malicious cyber attackers could modify or use this information to configure certain equipment. The analysis also revealed several vulnerabilities, including credit card information skimming, similar to what occurs at conventional gas pumps or ATMs, and the potential for using cloud servers to hijack an entire electric vehicle charger network. Some examples of potential attacks to EVSE include[127]:

- EV-to-EVSE Interface Vulnerabilities: MITM attacks, data privacy risks, and malware propagation between EVs and EVSEs.

- EV Operator Interface Vulnerabilities: Vulnerabilities in early-generation EVSE infrastructure, including RFID cloning and credit card skimmers.

- EVSE Internet Interface Vulnerabilities: a. Web Services: Insecure local web interfaces and multiple web service vulnerabilities. b. Internet-Accessible EVSE Services: Publicly accessible EVSE devices with weak credentials and outdated services. c. Communications to Backend Server or Cloud Systems: Exposed EVSE backend systems, cloud communication vulnerabilities, and supply chain vulnerabilities.

- EVSE maintenance interface and hardware/software vulnerabilities: hardware and software vulnerabilities in the EVSE, including outdated Linux kernels, hard-coded credentials, and insufficient authentication mechanisms.

Attacks to control systems in railway infrastructure

Railway signalling systems, including the European Train Control System (ETCS) and the European Rail Traffic Management System (ERTMS), are vulnerable to various types of cyber-attacks. These attacks can compromise the integrity, availability, and confidentiality of the systems, leading to potentially severe consequences such as passenger safety risks, service disruptions, financial losses, and

reputational damage. The main types of attacks identified in the context of the railway signalling systems include[128]:

Passive Attacks:

- Eavesdropping Attacks: malicious actors intercept control and status information of trains, compromising the confidentiality of the Communications-Based Train Control CBTC systems.

- Traffic Analysis Attacks: attackers analyse the huge volume of transmitted information to identify vulnerabilities and exploit the weakest nodes for potential attacks.

Active Attacks:

- Denial of Service (DoS) Attacks: disrupt the proper function of the cyber-physical system, impacting the control process, data logging, and communications.

- Distributed Denial of Service (DDoS) Attacks: coordinate attacks from a distributed system of computers to overwhelm the target system and consume network bandwidth or computational resources.

- Tampering Attacks: modify, delay, or reorder legal data, potentially compromising the integrity and continuity of operations.

- Masquerade Attacks: use fake identities to gain unauthorised access and potentially cause considerable damage to the system.

- Replay Attacks: store and replay intercepted legitimate data frames to perform illegitimate functions, causing disruptions or abnormal conditions.

The railway industry employs several security protection strategies, including securing communications, encryption, authentication protocols, safety protocols, firewalls, and intrusion detection/prevention mechanisms. These strategies aim to fortify the integrity, confidentiality, and reliability of the CBTC systems and mitigate potential cyber threats. Additionally, the industry emphasises the importance of a robust security governance model, early integration of security measures during project development, and enhanced security resilience against cyber threats in rolling stock. The CYRail project, under the Shift2Rail program, is a notable initiative aiming to streamline the industry's response to cybersecurity challenges by adopting the International Electrotechnical Commission (IEC) 62443 framework and developing a unified threat landscape for standardised threat classification.

Attacks to Open RAN 5G networks

The implementation of 5G networks and Open RAN introduces cybersecurity threats such as data breaches, IoT vulnerabilities, network slicing risks, virtualization and cloud security issues, DDoS attacks, and Man-in-the-Middle (MitM) threats. Countermeasures include implementing robust encryption and authentication protocols, conducting regular security assessments, ensuring secure configuration of IoT devices, implementing network segmentation, deploying intrusion detection and prevention systems, and utilizing secure virtualization technologies.

Attacks to IoT

Cybersecurity threats associated with the Internet of Things (IoT) include botnets and DDoS attacks, data breaches, device hijacking, man-in-the-middle attacks, firmware and software vulnerabilities, insecure network communications, and physical security exploitation. In recent years, the IoT has experienced exponential growth, with 22 billion devices connected by the end of 2022, a figure expected to reach 30.9 billion by 2025[129]. The proliferation of IoT devices has expanded the cybersecurity attack surface, leading to various threats such as data theft, phishing attacks, spoofing, and DDoS attacks. These threats can result in ransomware incidents and severe data breaches, causing substantial financial and operational disruptions.

One of the most notable attacks illustrating IoT vulnerabilities is the Jeep Hack in July 2015, where researchers gained control of a Jeep SUV via the Sprint cellular network[111]. Exploiting a firmware update vulnerability, they were able to manipulate the vehicle's speed and steering, highlighting the potential dangers of insufficient IoT security measures.

Businesses using IoT devices must prioritise cybersecurity by implementing rigorous evaluation processes, seeking guidance from cybersecurity experts, conducting regular Cyber Health Checks, and developing robust Cybersecurity Incident Response Plans. Additionally, participating in Cyber Attack Tabletop Exercises, pursuing Ransomware Prevention and Protection, and obtaining Cyber Essentials certification are essential steps in safeguarding IoT networks against potential threats. With a significant portion of IoT device traffic remaining unencrypted, addressing IoT security risks is crucial to prevent potential data breaches and cyberattacks.

Attacks to applications and services

The past few years have witnessed a significant surge in vehicle connectivity. While this trend has facilitated the introduction of innovative features and opportunities, it has also heightened the reliance on APIs, making them a prime target for attacks. APIs constitute 90% of the web application attack surface, owing to their relatively accessible entry points[130]. In 2022, automotive API attacks surged by 380%, contributing to 12% of total incidents, despite the advanced IT cybersecurity measures employed by OEMs. The repercussions of these breaches extend beyond data and PII leaks, often resulting in service disruptions, fraudulent activities, erosion of trust, and potential revenue loss.

A notable case that exemplifies the ease of execution and the significant fallout of such attacks is the one occurred in mid-2022 in Moscow, already mentioned previously in this document. During this incident, hackers infiltrated the systems of the Russian ride-hailing service provider, Yandex Taxi, orchestrating a massive convergence of taxis to a single location in Moscow.

Countermeasures

- Prepare risk analyses that identify, especially, critical processes and assets to deploy proportional prevention, protection, and response measures.
- Consider the acquisition of electronic systems and devices based on cybersecurity criteria and support guarantees throughout their lifecycle.
- Maintain an asset inventory and configuration management.
- Implement segmented networks in which critical systems and services are isolated from other devices.
- Implement zero-trust models is necessary, including network segregation between operational systems and the corporate network, recurring user and device authentication and authorisation, and privilege minimization, among other measures.
- Monitor the activity of connected electronic devices, if possible, by collecting and storing logs to quickly detect and respond to potential threats or anomalies.
- Manage software vulnerabilities on devices, including monitoring, identification, and updates, as well as testing the proper functioning afterward.

- Deploy solutions to keep operating systems, firmware, software, anti-malware or antivirus, and malicious code patterns up to date.

Attack to electric vehicle supply equipment:

- Deploy strict physical controls need to be established for devices in the primary sectors located in open spaces, such as restricting physical access to authorized employees only and implementing protective measures (e.g., lockable cabinets or security sensors).

- Conduct regular security assessments, ensuring secure configuration of the equipment.

Attacks to control systems in railway infrastructure

- Deploy strict physical controls need to be established for devices in the primary sectors located in open spaces, such as restricting physical access to authorised employees only and implementing protective measures (e.g., lockable cabinets or security sensors).

- Conduct regular security assessments, ensuring secure configuration of the systems.

Attacks to open RAN 5G networks

- Protect electronic communications with encryption protocols and limit unnecessary network ports and protocols.

- Implement network segmentation, deploying intrusion detection and prevention systems, and utilising secure virtualisation technologies.

Attacks to IoT

- Deploy anti-DDoS protections for essential resources visible from the Internet.

- Conduct regular security assessments, ensuring secure configuration of IoT devices.

Attacks to applications and services

- Deploy two-factor authentication access for users and administrators.

- Keep remote access security up to date and assess it, especially RDP, VPN, and Citrix.

EXPERTS SAY

"While we have been fortunate to avoid targeted attacks on our safety systems, there remains a looming concern for potential vulnerabilities within our signalling and switching systems. We must remain vigilant, prioritizing the integration of robust security protocols to safeguard the integrity and functionality of our critical railway components."

Giorgio Pizzi
Division Director of the Directorate General of Local Public Transport
Ministry of infrastructure and Transport of Italy

3

The Catalan smart mobility ecosystem

3. The Catalan smart mobility ecosystem

Catalonia features a vibrant, multifaceted smart mobility ecosystem that is making significant strides in redefining the future of transportation through the use of digital technologies. It is home to numerous businesses focused on sustainable mobility and smart cities, including the automotive, motorcycle, and micromobility industries, the railway sector, smart mobility services, telecommunications, and infrastructures. In recent years, several new stakeholders have emerged, each playing a pivotal role in (re)shaping the mobility landscape and introducing new challenges, including those related to cybersecurity.

In this chapter, we identify and describe the key stakeholders in Catalonia's smart mobility ecosystem, encompassing both incumbents and new entrants, outlining their respective roles. These entities include public transport operators and authorities, cities, micromobility (shared mobility operators and manufacturers), ride-hailing and car sharing operators, the connected vehicle value chain, technology centres, and other relevant institutions.

Barcelona, the capital of Catalonia, tops the list of European cities with the highest car density. However, although traffic in the city is twice that of Madrid and five times that of Berlin or Amsterdam, only one in three people get around with a private vehicle, which means that two thirds of the citizens in Barcelona opt for public transport, active mobility, or other shared mobility alternatives. In fact, Barcelona ranks second among major cities in the world in terms of accessibility to public transportation, understood as the ease with which the population can access high-capacity and high-quality transportation, with an impressive 99% of residents having a metro station within one kilometre of their homes[131]. Moreover, in 2022 Barcelona was ranked as the world's 3rd and Europe's 1st smart city[132]. The implementation of Information and Communication Technologies (ICT) and innovation in smart cities has a direct bearing on the promotion of sustainable urban mobility -i.e., pursuing Sustainable Development Goal (SDG) 11- through a more convenient, fully digital, seamless-access public transport system (T-mobilitat), complemented with alternative transport modes such as electric vehicles, shared, or on-demand mobility services, the use of sustainable energies in transport, and the promotion of micromobility, that is, bicycles and other personal mobility vehicles -addressing SDGs 7, and 13. Smart parking solutions represent another means of reducing the environmental impact, since they cut down on traffic time and reduce emissions from vehicles in the city. Also, worth mentioning are sustainable solutions for last-mile deliveries, including fostering the use of electric cargo-bikes, and applications (such as AMB's 'SPRO' app) –SDG 9. Tackling traffic congestion in a holistic way is key, thus extending beyond Catalonia's capital towards its metropolitan area. Significantly, Barcelona attracts twice as much mobility as it generates, as the city receives and/or generates nearly 6,1 million trips by residents of the STI (in Catalan, 'Sistema Tarifari Integrat', that is, Integrated Fare System). Closely linked to efficiently managing traffic flows is addressing road safety and preventing accidents, where this strategic objective is closely correlated with that of reducing emissions and improving air quality.

Barcelona serves as the premier 5G hub in Southern Europe, driving the development of pilot projects for testing and validating new 5G-related technologies, which are key for the viability of advanced, smart mobility applications, such as CCAM. With its accelerated data transmission, minimal latency, capacity to interconnect myriad (moving) devices, and a reliable network infrastructure, 5G has ushered in a new era of possibilities for a diverse range of businesses and industries.

Barcelona is also the headquarters for the EIT Urban Mobility, the largest European initiative dedicated to transforming urban mobility, with substantial co-funding of up to EUR 400 million (2020-2026). EIT Urban Mobility was officially launched in January 2019. At that time, the

community already consisted of a total of 85 organizations, including city councils, companies, universities, and research centres from 16 European countries. This number continues to grow. By pooling their knowledge and leveraging their diverse skill sets, the aim is to create an open innovation community that will become a Pan-European leading force for positive change in urban mobility by 2027. EIT Urban Mobility places the challenges facing cities at the centre of all their activities, with a strong emphasis on developing and deploying solutions that address the mobility of people, goods delivery, and waste collection, prioritising sustainability, decarbonisation, equity, and accessibility. These efforts are further fortified by digitalisation, with cybersecurity playing a critical role to ensure the safety and resilience of critical transportation systems and the protection of data privacy.

Barcelona and Catalonia enjoy a very strategic location in Southern Europe, with fast and easy access to markets in the rest of Europe, the Mediterranean region, and the North of Africa. Leading infrastructures like the Port of Barcelona, the Port of Tarragona, and Barcelona's Airport ensure excellent connectivity with plenty of international routes for both cargo and passengers. A highly specialised logistics network provides any business with integrated services such as packaging, product certification, or product handling.

Overall, the mobility sector in Catalonia, comprised of the automotive sector (including passenger cars, light commercial vehicles, industrial vehicles), the motorcycle sector (including all types of Powered Two Wheelers, as well as other light vehicles, such as tricycles, quadricycles), micromobility (including bicycles, tricycles, electric motorbikes, and all types of Personal Mobility Vehicles, PMV), buses, maritime transport, and air transport, is composed of 543 companies, is worth EUR 23,397 million in turnover, and employs 52,277 people[133].

3.1 Flagship public mobility services

T-mobilitat

T-mobilitat is the new digital ticketing system in the Barcelona area offering access to the public transport network with a single rechargeable smartcard or mobile app, both using contactless technology. It introduces significant improvements in the use and management of public transport tickets, digital and online self-management, and comprehensive enhancements in transport network information. The T-mobilitat gives users access to all public transport within the 6 zones of the Barcelona's ATM Integrated Fare System. Once the T-mobilitat system is consolidated and fully deployed, the current magnetic ticket system will be withdrawn.

The T-mobilitat system's advanced ICT infrastructure, its critical role in supporting the reliable operation of public transport services, which are essential to the community, and its management of vast amounts of data, including personal information, render it an attractive target for cyberattacks.

The 'Departament de Territori' of the Generalitat de Catalunya (mobility department of the Government of Catalonia) leads the project, promoted ATM, AMB, and the public transport operators TMB and FGC.

Smou

Smou is the most comprehensive urban mobility, free app in Barcelona, provided and managed by BSM (Barcelona de Serveis Municipals), a trading company wholly owned by Barcelona City Council. It provides access to information and mobility services that facilitate getting around the city. It offers an urban trip planner including public transport and bike sharing information; it grants access to the city's public bikesharing service Bicing (including smart-card, QR, and NFC-based access), and to the BSM car parks (by the automatic number plate recognition system); it lets drivers pay for the parking meter, not only in Barcelona but also in 9 other municipalities in the Barcelona metropolitan area; it can be used to recharge an electric vehicle using the public EV charging infrastructure; it provides information about the available shared mobility vehicles in the city (bikes, mopeds, cars), and lets users hail a taxi.

Smou collects Bicing usage data (and of other services), and analyses it in an ethical, secure way in order to better manage the fleet of bikes and optimise vehicle transit. In its latest update, Smou introduced a Two-Factor Authentication (2FA) method, emphasising its commitment to cybersecurity.

AMB Mobilitat, AMBici, SPRO

"AMB Mobilitat" is a versatile, free app that lets users plan their journeys by public transport and bicycle according to their preferences. It offers Estimated Arrival Times for public transport (bus, metro, tram), personalised routes for each mode of public transport, incident alerts, and information on service alterations that affect users' favourite lines. It also provides information on the edge of Low Emissions Zones in and around Barcelona; air quality alerts; Park + Ride and EV-charging points; cycling network and safe bike parks available; information on the location of some available moped-sharing service providers. It also lets users hail a taxi and buy T-mobilitat tickets.

AMBici is the new 100% electric and high range public bikesharing service available since 2023 to cycle between 15 municipalities in the metropolitan area of Barcelona. It has been co-funded with EUR 7 million from EU Next Generation funds within the framework of the 'Plan de Recuperación, Transformación y Resiliencia' of the Spanish Ministry of Transport, Mobility and Urban Agenda. In the roadmap, the deployment of transfer stations to connect with Barcelona's Bicing is planned, enabling seamless use of public shared bikes in the whole metropolitan area. Due to their heavy reliance on ICT systems, both AMBici and Bicing proactively mitigate cybersecurity threats, including data breaches, service disruptions, financial losses, malware attacks, privacy violations, and system

downtime. If not properly addressed, these threats have the potential to impact user data privacy, operational reliability, and overall system trustworthiness, undermining active mobility as an attractive alternative to private cars.

Also developed by the AMB, the SPRO app allows last mile logistics operators to manage parking in the DUM zone (in Catalan, 'Distribució Urbana de Mercaderies', that is, Urban Freight Distribution), in Barcelona and other municipalities in the metropolitan area.

TMB App

TMB App is a free, multilingual mobile application that offers comprehensive information and services related to the public transport system in Barcelona. Managed by TMB (Transports Metropolitans de Barcelona), it enables users to handle their T-mobilitat card, purchase and validate tickets via their smartphone, and even buy tickets to be collected from metro machines. The app provides real-time data on bus and metro services, facilitates journey planning, offers scheduled arrival times, and allows users to customise it by saving preferred routes and stops. It also offers information on waiting times, service disruptions, and where to disembark. Moreover, users can utilise customer service channels and explore the JoTMBé loyalty programme. Being the most widely adopted and frequently used public transport app in Barcelona, any disruption resulting from potential vulnerability vectors could significantly impact the daily mobility of thousands of users.

FGC App

Ferrocarrils de la Generalitat de Catalunya (FGC) is a public railway company which operates several lines in Catalonia. Its official app allows users to access train schedules for all FGC lines, view rates, plan journeys, receive real-time train occupancy information, and explore additional services available at FGC stations. The app is highly customisable, enabling users to save regular journeys, access trip history, and set alarms for reaching their destination stations. It also offers the ability to report incidents.

FGC ensures that user data is not shared with third parties. The FGC app collects various data types, including precise location, personal information, in-app activity, and app performance data. Security practices involve data encryption during transmission, and users have the choice to request data removal.

3.2. Landscape of smart mobility stakeholders

3.2.1. Public transport

Rail operators: Catalonia boasts one of the most robust industrial railway sectors in Europe, comprising 190 companies with a combined turnover of EUR 6.85 billion. Moreover, an extensive rail network of almost 1,800 km connects the main cities in Catalonia with Southern Europe, including 400 km of high-speed railway lines.

Ferrocarrils de la Generalitat de Catalunya (FGC) operates metro and commuter lines in and around the city of Barcelona, tourist mountain railways, and rural railway lines in Catalonia. Notably, FGC leads one of the first 5G rail laboratories in the world, between the stations of Plaça Espanya and Europa | Fira.

Transports Metropolitans de Barcelona (TMB) operates Barcelona's metro and bus network jointly on behalf of Àrea Metropolitana de Barcelona (AMB). It reaches ten towns within the metropolitan area of Barcelona. The Barcelona metro consists of eight lines, 165 stations and 162 rush hour trains.

In addition to FGC and TMB, Catalonia's rail services encompass TRAM, a public transport business group responsible for operating Barcelona's tram network under a grant from the ATM until 2032. And Renfe, Spain's national railway company, running most regional and high-speed AVE trains, connecting Barcelona, Lleida, Tarragona-Reus, Girona and Figueres-Vilafant with the main Spanish capitals. Furthermore, since 2021 EU member states have been obligated to open up their rail markets to foreign competitors, a reform that Spain has embraced, significantly expanding the high-speed operator landscape. In a short period, Spain has tripled its high-speed operators (with the new entrants Avlo, Iryo, and Ouigo), leading to increased competition, greater availability of trains, and lower prices for travellers.

IN-MOVE by Railgrup is the cluster of sustainable mobility and multimodal logistics in Spain. A private, non-profit organisation aimed at facilitating the improvement of the competitiveness of companies throughout the sector's value chain, with nearly 130 associated organisations and a track record of more than 20 years.

Bus operators: besides TMB in Barcelona, a few other bus operators, encompassing both public and private entities, offer their services throughout Catalonia. The AMB provides its public transport services through various public (TMB) and private transport companies operating under administrative concession, namely Baixbus (Mohn and Rosanbus), Avanza, Soler i Sauret, TGO DX, TUSGSAL, UTE Monbus and Julià, UTE Julià Travel and Moventis, Monbus, Moventis, and Aerobús. Other relevant bus operators offering their services in Catalonia include TEISA, ALSA, Cots Alsina, HIFE, Autocars del Penedès, Autocorb, or Montferri.

Demand Responsive Transit (DRT) is on the rise, with a growing number of routes utilising flexible algorithms, running on mobile apps that efficiently match passengers with available buses. This approach boosts occupancy, reduces emissions, and enhances user satisfaction. Nemi is the fastest growing start-up in this domain, with their technology underpinning flexible bus services offered by AMB, Generalitat de Catalunya (Government of Catalonia), and other PTAs and PTOs across Spain, Italy, Portugal and the UK. Shotl is another prominent Catalan DRT provider, with Ioki and ByBus competing in the same segment.

Taxi and VTC services: 'Picmi Taxi' is the ride-hailing feature available in the 'AMB Mobility' app that allows users to request a taxi via their mobile phones. Users can also hail a taxi or request a VTC service (vehicle for hire with driver) through well-known apps like Cabify, FREENOW, Bolt, and Uber, present in many other cities, or Zolty for taxi in Barcelona.

3.2.2. Traffic Management and Information Centres

The Servei Català de Trànsit - SCT (Catalan Traffic Service) is responsible for regional and interregional traffic management and operates the Traffic Management and Information Centre called 'CIVICAT', Centre d'Informació Viària de Catalunya (Centre for Road Information in Catalonia). The 'CIVICAT' has the main function of informing users about traffic conditions, effectively managing critical sections of Catalonia's road network, and enhancing road safety on Catalonia's roads. 'CIVICAT' manages the traffic on the Catalan road network, and its main function is to facilitate safe mobility within the territory, minimise road incidents, and provide users with timely traffic condition information. To achieve this goal, it leverages the support of aerial resources available through the Catalan Traffic Service and various equipment, including cameras, Variable Message Signs (VMS), and vehicle counting systems, among others. Motorist information is disseminated through VMS's. They are used for advice, warnings (on traffic congestion, roadworks, accidents, adverse weather conditions, etc.), rerouting, travel times, and for itinerary recommendations. Active cybersecurity vigilance is crucial to prevent potential disruptions in 'CIVICAT' traffic management, potentially resulting in inaccurate information dissemination, and road safety impacts.

Big cities in Catalonia have their own Traffic Management and Information Centres. Barcelona, for instance, has two TMC: one is used for traffic signals and lane control for the operation of reversible lanes. The second TMC controls the ring roads ("Rondes") around the city.

3.2.3. Shared and on-demand mobility service providers

The traditional dichotomy between private cars and public transport has become outdated as plenty of alternative and complementary mobility services have thrived in recent years, especially in Barcelona and its metropolitan area. This shift has resulted in increased adoption of shared bicycles, electric mopeds, carsharing, flexible renting and subscription models, and on-demand solutions like ride-hailing and DRT in Catalan cities. Simultaneously, younger generations are exhibiting heightened awareness of climate change, thus embracing more sustainable mobility options, and a preference for flexibility, shifting from car ownership to access-based models. Shared electric mopeds are widely available and very popular, mostly in Barcelona and its metropolitan area, and are offered by the following service providers: Acciona, Cabify, SeatMo, Cooltra, Yego. Shared free-floating bicycles and e-bicycles providers include Cooltra (electric), Ridemovi (electric and traditional), Donkey Republic (electric and traditional), in Barcelona; and TIER (electric), in Tarragona, also offering shared e-scooters in this city. Shared docked bicycles and e-bicycles in Barcelona include 'Bicing', the city's popular public bike-sharing service (electric and traditional), 'AMBici', the metropolitan electric bikesharing, and Girocleta, the public bikesharing service available in Girona. Other services, like Kleta, Spinlister, Swapfiets, or Gomeep, let users flexibly rent a bike in Barcelona.

For those users in need of a car, service providers like Ubeeqo, Vamos, or Virtuo, let users flexibly access a car by hours through an app. Peer-to-Peer carsharing is offered by Getaround and Social Car. Som Mobilitat is a non-profit consumer cooperative offering electric car-sharing, with cars that can be either owned by the cooperative or by individuals, enterprises and public institutions. MEC carsharing is the pioneer electric car-sharing service provider offering their cars not only in Barcelona, but also in other Catalan cities, such as Vilafranca del Penedès. Most car-sharing operators operate under B2C, as well as B2B models. Sharing a car trip, also known as carpooling, is possible through the widespread BlaBlaCar app, Amovens, and a few other minor service providers. Car subscription models are on the rise, with novel companies like Bipi, Swipcar, or Wabi in this new space.

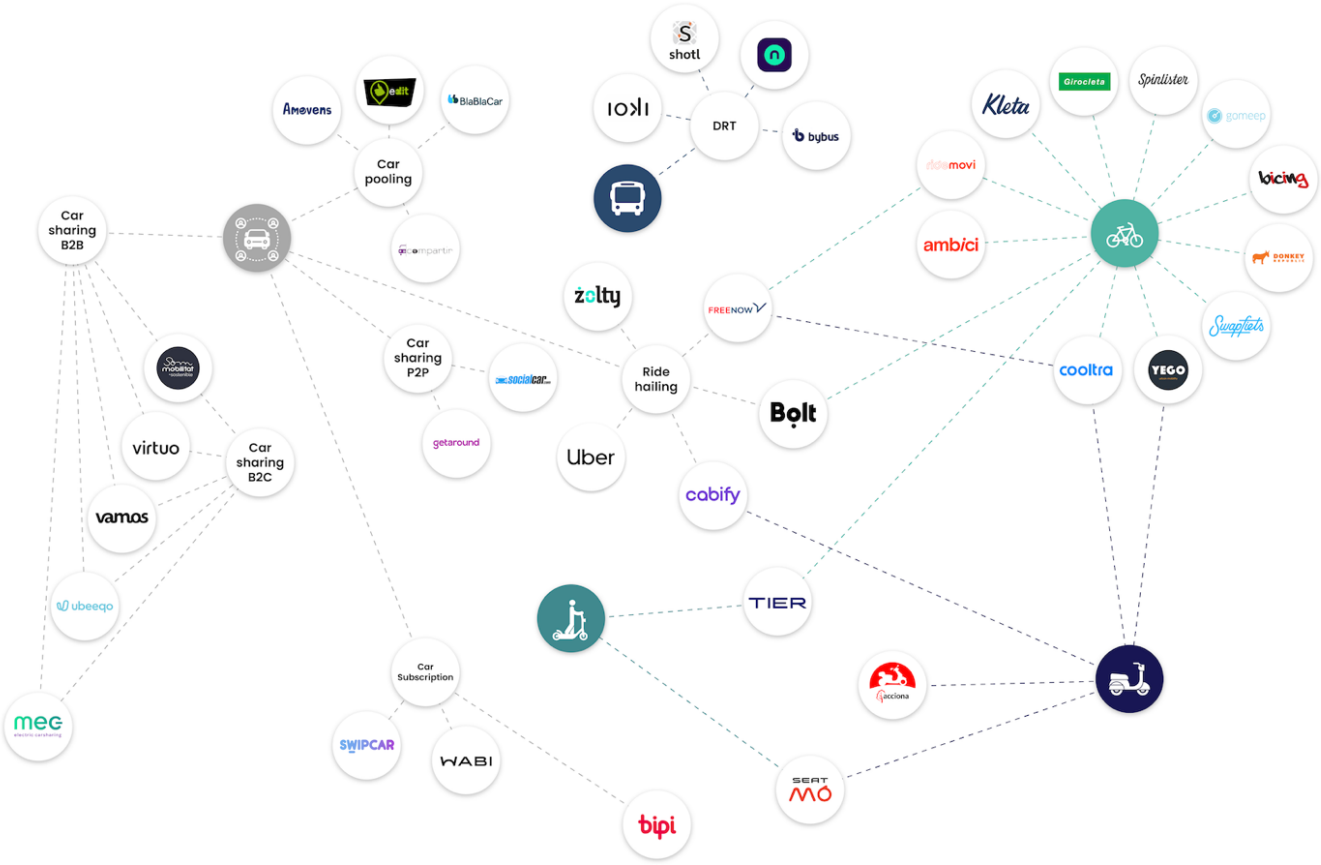


Figure 7: Map of stakeholders in Catalonia's shared and on-demand mobility ecosystem

Numerous service providers, both public and private, in Catalonia offer comprehensive Mobility-as-a-Service (MaaS) solutions. These MaaS platforms integrate various mobility services into a unified user interface, providing convenient access to a wide range of transportation options, from public transport to shared and on-demand mobility, all in one place. This approach simplifies the traveller's experience and encourages the use of diverse and sustainable mobility solutions.

In the public sector domain, in addition to the applications mentioned in section 3.1, we highlight the following mobility services:

- Clic.cat is an on-demand public transport service of the Government of Catalonia. Without predefined routes or fixed schedules, each passenger specifies their starting location and desired departure time. The system then calculates the most efficient route in real-time to meet the needs of all passengers.

- Flexitransport Catalunya is a mobility solution developed by AMTU that caters to the users' needs and simplifies daily commutes. Its flexible and adaptive system allows users to book their journey, specifying the starting point and destination, without being tied to a fixed schedule or route, both in real-time and with advance reservations.

- Dōcō, Spanish national rail operator Renfe's MaaS app that provides journey planning, payment, and ticketing for door-to-door journeys across Spain, including urban rail and bus networks, taxis, and ridesharing.

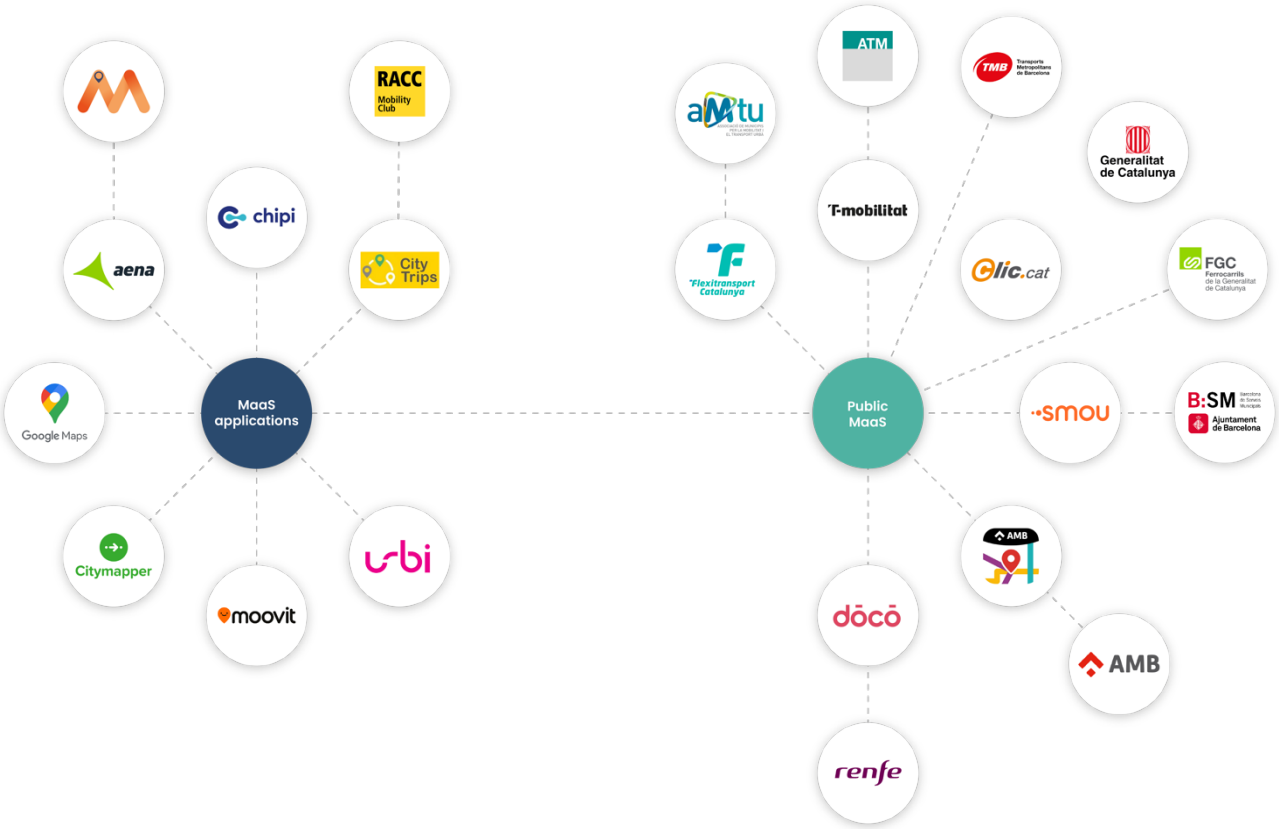


Figure 8: Map of MaaS stakeholders in Catalonia's smart mobility ecosystem

3.2.4. Automotive sector

Catalonia possesses a robust network of engineering companies and suppliers in the automotive sector. It stands out as one of Europe's leading automotive manufacturing regions, producing 1 in 5 vehicles in Spain alone. It hosts Seat, a significant automotive OEM under the Volkswagen Group. Catalonia is also home to numerous businesses focused on sustainable mobility, smart cities, and related telecommunications and infrastructures. Catalonia features advanced R&D centres and industry organisations in the automotive sector, with notable institutions such as:

Applus+ IDIADA: a global partner to the automotive industry with over 30 years' experience supporting its clients in product development activities by providing design, engineering, testing and homologation services. IDIADA's success in product development is built on a unique blend of highly experienced engineers, state-of-the-art test and development facilities, and the constant drive towards innovation. The company has more than 3.000 professionals and an international network of 56 subsidiaries and branch offices in 22 countries, ensuring its clients receive fast, customised solutions.

They specialise in comprehensive testing and validation of the latest car connectivity technologies, encompassing Vehicle-to-Network (V2N), Vehicle-to-Infrastructure (V2I), Vehicle-to-Vehicle (V2V), and Vehicle-to-Pedestrian (V2P). Their fully controlled and operable DSRC and C-V2X infrastructure ensures that communication between vehicles and infrastructure is robust and cybersecure. In addition, the testing tracks are complemented by a private 2G, 3G, 4G and 5G cellular network, providing a controlled environment capable of reproducing worldwide network configuration and conditions to develop and validate connected vehicle solutions. Overall, their advanced technology and real-world testing

scenarios help identify vulnerabilities and improve the cybersecurity of automotive connectivity.

CARNET: an open hub for industrial and academic partners from the areas of automotive and mobility research and innovation, founded by automotive OEMs Seat and VW Group Innovation, and academia, with UPC Barcelona Tech. It is based in Barcelona and works through project-based collaboration. It focuses on innovative solutions that bridge the gap between academic research and industrial innovation in urban mobility.

CARNET has developed Ona, a 6-wheeled robot capable of autonomous navigation on streets and pedestrian areas using integrated sensors. Ona is designed for efficient last-mile delivery, featuring an interior warehouse for carrying multiple packages and facilitating human-robot interaction through large screens. Expected business outcomes include a 15% reduction in last-mile delivery operation costs (when deployed in an adequate business case), a 45% decrease in greenhouse gas emissions on a life-cycle basis, improved delivery volume handling, enhanced safety, and expedited digitisation of last-mile operations.

Cybersecurity for PMRs (Public-area Mobile Robots), i.e., human-scaled robots for single destination delivery, and public-domain security or maintenance tasks is every bit as critical and important as cybersecurity for automated passenger vehicles and shuttles. While automated vehicles are larger and faster making their momentum a greater concern, maliciously redirecting the speed and direction of a vehicle is hardly the only cyber-concern. Malicious changes to contents, destination, and other actions are also concerns. All things being equal, we might expect PMRs to be a lesser concern because they are smaller and slower than passenger vehicles and shuttles. This is not so. The number of companies that will likely create small robots -because there are so many additional, specialised, and critical applications, and because their “public-safety” concerns are less apparent- is such that we are sorely in need of regulations that ensure any such device, whether automatically, partially, or remotely controlled within the public domain can be always certified and remain easily and correctly identifiable.

The Automotive Industry Cluster of Catalonia (CIAC): a non-profit association that welcomes companies associated with the automotive industry in Catalonia to engage in Research, Development, and Innovation (RDI) activities. It currently comprises over 200 companies. The primary goal of the CIAC is to enhance the competitiveness of the automotive industry, which plays a pivotal role in the Catalan economy, by promoting projects that create jobs and bolster the global standing of the Catalan automotive sector. The CIAC's Strategic Plan 2020-2024 acknowledges the challenge of cybersecurity in the automotive sector due to the increasing connectivity of vehicles. To address these challenges and find solutions, the CIAC is extending its ‘Talent Platform’ to 90 universities and training centres, recognising the importance of talent and education in tackling cybersecurity issues facing the automotive sector.

ÒPTIMA (Oficina Pública per la Transformació de les Indústries de Mobilitat i Automoció): established in January 2022, is the office for the transformation of the automotive and mobility sector, a part of the Government of Catalonia's industrial policy in the automotive and mobility industry. Its primary mission is to guide the sector's transition towards becoming a digital and sustainable industry, helping companies prepare for upcoming changes, adopt digital and sustainable practices, identify new opportunities, create a unified sector narrative, foster collaboration, support industrial policy, coordinate with key entities, and amplify public engagement in the sector. ÒPTIMA can play a major role in addressing the cybersecurity challenge in the Catalan automotive and mobility sector by promoting robust cybersecurity measures and fostering collaboration to enhance digital transformation security and resilience.

The connected vehicle sector in Catalonia is burgeoning, with a total of 71 companies actively contributing to this dynamic landscape. Catalonia has solidified its position as a thriving hub for innovation and development in this field. Notably, 70% of these companies are SMEs, highlighting

the entrepreneurial spirit driving the industry forward. Furthermore, the sector boasts a mature foundation, with 62% of companies having over a decade of experience. Notably, the sector exhibits a blend of established companies dedicating a portion of their business to the connected vehicle domain, as well as a substantial presence of entrepreneurial ventures. Start-ups make up 29% of the companies, demonstrating the dynamic and innovative nature of the industry. Approximately 20% of companies have subsidiaries abroad, showcasing their global reach and influence. Additionally, nearly half of the companies, amounting to 48%, engage in export activities, further solidifying Catalonia's position as a key player in the global connected vehicle market.

Connected vehicle manufacturers in Catalonia include Seat, Silence, Torrot, Rieju, Legend; IT and connectivity providers include Brightsight, Cellnex, Castinfo, FlexVPC, Siemens, Esi, HP, Erni, Etra, Axodel, Main memory, Idneo, Dipole; electronic parts manufacturer include LEAR, Prysmian Group, Denso, Mahle, Kostal, Marelli, Merit, Doga, Vicente Torns, Nidec, FlexNgate, J. Juan, Bitron, Escubedo, FAE, Elausa, Roquet; electronic parts manufacturers include Denso, Ficosa, Kostal, Dynacast, NTT Communications, Arcol, Advanced Automotive Antennas.

Overall, the sector generates a substantial turnover of EUR 4.1 billion and employs approximately 9,720 individuals[134].

3.2.5. Micromobility sector

In Catalonia, the micromobility sector saw remarkable growth in 2022. With 119 companies contributing, the collective turnover exceeded EUR 255 million. This year, these Catalan companies also secured a substantial investment of EUR 222 million, driving 21 investment projects and creating 372 job opportunities. Notably, a significant proportion of these companies, amounting to 88%, were based in the province of Barcelona.

The diverse landscape of the Catalan micromobility industry is evident, with approximately 40% of the companies involved in the manufacturing of micromobility vehicles such as bicycles, tricycles (manual and electric), electric motorcycles, scooters, and skateboards. Other companies are engaged in vehicle rental services (29%), shared mobility services (12%), manufacturing components and chargers (9%), app development (7%), and offering engineering services (5%).

There are several e-micromobility vehicles manufacturers located in Catalunya. Namely, for electric bikes: Megamo, Youin, Legend, Intense, Spinta, Tromber, Lobito, Batec (attachable handbikes for wheelchairs), Braih; for electric motorbikes: Silence, Rieju, Torrot, Pursang, Volta, Ray, Stark; for electric kick-scooters: Youin, Ohll, Gravity, Spinta, Lobito, Lampsy.

Light Mobility Cluster is the non-profit legal entity representing the entire value chain of two-wheeled vehicles and light mobility in Catalonia. Currently, it brings together more than 90 member companies, representing a total revenue of over EUR 900 million, with more than 5,900 employees and an export volume of 85%.

Barcelona, a key player in this narrative, is projected to witness a substantial rise in micromobility vehicle usage by 2024, with an estimated increase of 31%. To foster innovation, specific zones within the city have been designated as testing areas for companies involved in pioneering transport solutions. This initiative includes the provision of technical support and resources such as sensors, systems, and databases.

3.3. Barcelona smart mobility and cybersecurity conferences

Barcelona plays host to several international conferences that gather experts, innovators, and thought leaders to explore a wide range of topics at the intersection of technology, cybersecurity, and smart mobility. These events provide a crucial platform for discussing the latest advancements and challenges in the field, spanning subjects from the transformative impact of 5G on smart mobility to the intricacies of cybersecurity within the automotive industry. Additionally, they delve into the future of connected and autonomous vehicles (CAV) and the ever-evolving landscape of the Internet of Things (IoT). These conferences attract professionals and stakeholders from around the world, promoting knowledge exchange and collaboration, fostering innovation, and addressing multifaceted cybersecurity concerns in the context of smart mobility and related technologies. Notably, among the significant annual conferences where professionals in the smart mobility sector and cybersecurity experts convene to exchange ideas and stay updated are:

SMART CITY EXPO WORLD CONGRESS

TOMORROW. MOBILITY WORLD CONGRESS

MWC GSMA

4YFN

AUTOMOBILE BARCELONA

IOT SOLUTIONS WORLD CONGRESS

BARCELONA CYBERSECURITY CONGRESS

EUROPEAN BLOCKCHAIN CONVENTION

4

Cybersecurity landscape in Catalonia

4. Cybersecurity landscape in Catalonia

This chapter delves into Catalonia's current cybersecurity framework, shedding light on its robust network of companies dedicated to cybersecurity. It also spotlights key cybersecurity players in Catalonia, aligning with the Catalan Cybersecurity Strategy. Furthermore, we explore the strengths of the cybersecurity sector in Catalonia, with a focus on aspects such as the education system, funding achievements, and the research and innovation sector.

4.1 The cybesecurity industry in Catalonia

According to data published in 2023[135], the cybersecurity sector in Catalonia includes approximately 495 companies that provide consultancy, services, and products, with a global turnover of close to EUR 1.07 billion and employing 9,414 people. This represents a remarkable increase of 14.6% in the number of cybersecurity companies compared to the 2022. The revenue generated by these companies has risen by 17.3% and there has been a 15.0% increase in the number of workers employed.

In recent years the cybersecurity sector in Catalonia has maintained a trend of constant growth, with little impact from significant factors such as the widespread shutdown of the economy due to the pandemic and the uncertainty due to the war between Ukraine and Russia, but quite the opposite in fact, as these two factors have increased the need for professionals and solutions in the field of cybersecurity. It is expected that in the coming years this growth trend will be maintained, or become even more acute, due to the challenges we have seen above, albeit contingent on the global evolution of the economy.

Start-ups and entrepreneurship

Catalonia's cybersecurity ecosystem and entrepreneurship thrive. Of the total number of companies, 85% are small and medium and 9.5% are classified as start-ups, representing the dynamic and forward-thinking nature of the industry in Catalonia. 29.1% of these cybersecurity companies in Catalonia were founded less than 10 years ago, indicating that the growing demand for cybersecurity in recent times has spurred the birth of a significant number of companies in the sector.

Focus areas

If we make a division by the segments corresponding to the five categories with the structure of the ECSO market RADAR and bearing in mind that a company can be classified into more than one segment, we can see that 89.7% of the companies are engaged in protection, 58.7% in identification, 37% in detection, 33.6% in response and 20.6% in recovery. Although not equal, this diverse positioning ensures the availability of cybersecurity solutions in the Catalan market to contribute to local resilience against cyberattacks. Nevertheless, the cybersecurity companies in Catalonia demonstrate a strong emphasis on protection.

Catalonia's cybersecurity companies are primarily concentrated in the Barcelona region. 83.4% of the companies are situated in this area, benefitting from the strategic location and robust business environment that Barcelona offers.

Funding and investment

Barcelona stands out as the 6th city in the European Union in terms of closed funding rounds for cybersecurity start-ups. Over a period of four years (2018-2022), cybersecurity start-ups in Barcelona successfully raised EUR 103.3 million

in funding through 17 funding rounds. This remarkable achievement underscores the investment potential and attractiveness of Catalonia for cybersecurity entrepreneurs.

In 2022, Catalonia emerged as the 3rd most attractive region in Western Europe for foreign investment in the cybersecurity sector. With EUR163.6 million invested, representing 7.2% of the total foreign investment in the region, Catalonia not only benefits from financial infusion but also creates 313 new job opportunities, contributing to the growth and development of the local economy.

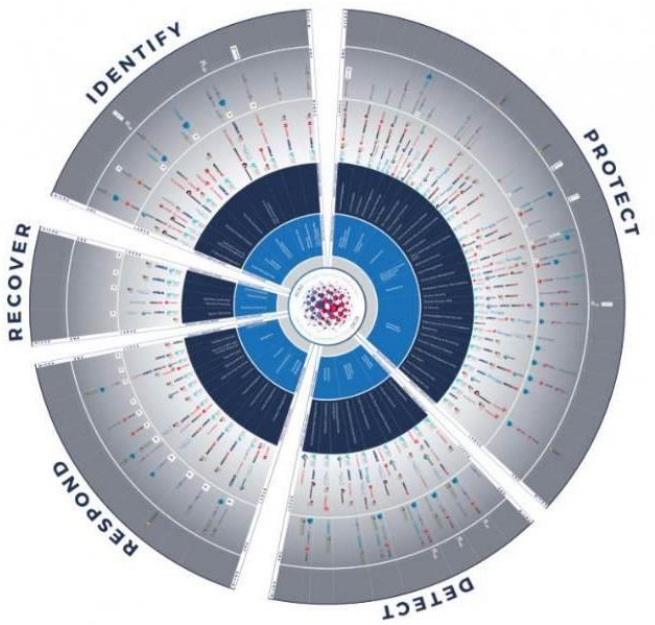


Figure 9: ECSO Market Radar[136]

4.2 Prominent cybersecurity actors in Catalonia

This chapter highlights the key players in Catalonia's cybersecurity landscape, including the Cybersecurity Agency of Catalonia, the Digital Catalonia Alliance, and the Digital Innovation Hub. It emphasises their key roles in fostering innovation, collaboration, and the development of cutting-edge technologies within the country's cybersecurity ecosystem.

Catalonia Digital Innovation Hub (DIH4CAT)

The Catalonia Digital Innovation Hub (DIH4CAT) is a regional non-profit innovation ecosystem, formed by the main support agents for the digitalisation of Catalonia, with the goal of promoting the technological transformation of small and medium enterprises (with a special focus on the industrial sector and technology suppliers), technology start-ups and public entities.

The Digital Innovation Hub for Catalonia acts as a catalyst for collaboration between industry, academia, and government entities, fostering the development and adoption of cutting-edge technologies and solutions. The technological areas of DIH4CAT are sorted into different Digital Innovation Nodes (DIN) specialised in advanced technologies and are coordinated by the most competitive centres of Catalonia. Two of them can be highlighted between others: cybersecurity and smart connectivity. For the second, DIH4CAT offers SMEs and public sectors the opportunity to work and test all those technologies that allow people, devices, cars, to connect to the networks, as well as between themselves in order to intelligently exchange, process and analyse data.

Cybersecurity Agency of Catalonia

The Cybersecurity Agency of Catalonia is in charge of implementing public cybersecurity policy and developing the Government of Catalonia's cybersecurity strategy. It is a public law entity of the Government of Catalonia that acts with complete autonomy. It acts in accordance

with Law 15/2017 of 25 July 2017 on the Cybersecurity Agency of Catalonia.

The Agency is responsible for setting up Catalonia's public cybersecurity service and works to guarantee and increase the security level of its information systems and networks, along with the public's digital trust. Being in charge of cybersecurity entails overseeing the establishment and monitoring of cybersecurity action programmes under the strategic direction of the Catalan Government, working jointly with its various public sector bodies.

Among the functions, the Agency is in charge of Collecting the relevant data from the entities that manage public or essential services in Catalonia in order to know the state of information security, inform the Government and propose the appropriate measures to carry out risk management in cyber security.

Centre of Innovation and Competence in Cybersecurity (CIC4Ciber)

In alignment with the establishment of the European Centre of Cybersecurity Competence (ECCC) and the National Centres Network (NCC), which collectively form the new European framework for bolstering innovation and industrial policy in cybersecurity, the inception of the Centre of Innovation and Competence in Cybersecurity (CIC4Ciber) marks a significant milestone. Functioning as an organic division of the Cybersecurity Agency of Catalonia, CIC4Ciber is dedicated to the coordination, consolidation, and advancement of Catalonia's cybersecurity ecosystem. With a commitment to utilising knowledge and innovation as catalysts for transformation and sectoral progression, CIC4Ciber actively promotes networking initiatives to amplify the impact of its diverse programs and projects. Simultaneously, it actively supports projects to secure funding and facilitate internationalisation efforts. Among its key areas of focus, smart transportation stands alongside healthcare, critical infrastructures, AI/RPA, 5G, and data as pillars within its strategic framework.

CATALONIA CERT®

The Cybersecurity Agency of Catalonia has an incident response team which operates under the CATALONIA-CERT® trademark as the Government of Catalonia's CSIRT, developing preventive, reactive, coordination and management measures to deal with cybersecurity incidents for the target areas associated with the Cybersecurity Agency of Catalonia, including public assets and infrastructures related to smart mobility. The coordination of cyber incidents in the smart mobility sector involves the collaboration of dedicated cybersecurity response teams, incident response centres, and regulatory authorities, aiming to mitigate the impact of cyber threats on the transportation infrastructure and the safety of the users. The CATALONIA-CERT works closely with the CCN CERT (National Cryptologic Centre CERT) and INCIBE CERT (National Institute of Cybersecurity of Spain), which are the entities to be reported depending on the nature of the incident. INCIBE CERT is more geared towards the general public and small and medium-sized enterprises (SMEs). CCN CERT is more focused on government organisations and companies in critical sectors, such as mobility and transportation, as well as others like the public administration, healthcare, finance, or defence.

Digital Catalonia Alliance (DCA)

The Digital Catalonia Alliance brings together industry leaders, research institutions, and public authorities to foster collaboration, innovation, and knowledge-sharing in the digital domain. It actively supports the growth of the cybersecurity sector in Catalonia, driving economic development and positioning the region as a global player in the field. For now, the DCA focuses on six technology communities, among which cybersecurity, the Internet of Things (IoT) and artificial intelligence stand out, which are closely related to smart mobility. However, the initiative's roadmap foresees the formation of new communities in the field of advanced digital technologies.

4.3 Strengths of the cybersecurity sector in Catalonia

Until the preparation of this report, no study had addressed the sectoral impact in Catalonia, such as turnover figures or job creation, resulting from the convergence of smart mobility and cybersecurity. Nevertheless, based on the findings presented in this white paper, expert consultations, and the contributions of various entities involved in its inception, it is evident that the development of a cybersecurity-focused smart mobility ecosystem holds significant promise as an area for application and business growth in Catalonia. Several supporting factors for this assertion are examined below.

Strong business network in cybersecurity

Catalonia has positioned itself as an attractive hub for entrepreneurial innovation in the cybersecurity industry. The region is home to 495 companies and 9,414 jobs, with 9.5% of them being start-ups. Additionally, various institutions provide support to organizations in the cybersecurity sector, serving as local counterparts to European institutions. Notable entities within this ecosystem include DIHxCAT, the CIC4Ciber, and the DCA, which are analogous to their European counterparts: the ECCC (European Cybersecurity Competence Centre) and the ECSO (European Cyber Security Organisation). Their primary goal is to support companies in their digitalisation efforts, facilitate the collection of funds for various initiatives, and promote collaboration and innovation within the cybersecurity sector.

The Cybersecurity Agency of Catalonia is another key player, responsible for developing policies within its jurisdiction and providing support to Catalan networks, systems, and companies to enhance their security measures. This multifaceted approach reinforces Catalonia's position as a regional leader in the cybersecurity field.

Education system

Education and training in the field of smart mobility are becoming increasingly important for university technology departments. For instance, UPC Barcelona Tech offers various official bachelor's and postgraduate degrees, including master's programmes related to smart mobility, urban mobility, transport, and different aspects of automotive engineering. In Catalonia, there are 11 postgraduate and master's programmes in cybersecurity offered by different universities and educational institutions, along with 37 schools providing Vocational Education and Training (VET) in cybersecurity. However, there is currently a significant gap in cross-training that encompasses both smart mobility and cybersecurity, as there are no educational programs that integrate these two knowledge areas.

Talent attraction

Catalonia, and especially Barcelona, has become a pole of attraction and demand for talent due to various factors such as the notable increase in business initiatives and start-ups, and the establishment of new operating centres of multinational companies, but also for aspects related to the quality of life, cultural and other aspects.

The report 'Digital Talent Overview 2023,' produced by Barcelona Digital Talent of the Mobile World Capital Barcelona, provides a detailed analysis of the trends related to digital talent at a global and Catalan level, with a specific focus on the Barcelona region. The report highlights that among the most demanded professional profiles in Catalonia, cybersecurity is a prominent area. This is evident in the demand for existing talent, with a 33% increase in the domain of cybersecurity in 2021 compared to 2020.

Research and innovation

Catalonia demonstrates a commitment to collaboration and research in the field of cybersecurity. 40 Catalan entities secured EUR 11.5 million in funding for cybersecurity-related projects under the Horizon 2020 programme. This significant achievement represents 1.9% of the total funding allocated to the European Union for cybersecurity projects. It highlights the country's participation in cutting-edge research and development initiatives, fostering innovation and knowledge-sharing.

Although a gap has been identified in the realm of education and training when it comes to combined studies of smart mobility and cybersecurity, the situation differs in the field of innovation. Here, some research and technology centres host well-established research, development, and technology transfer groups and units in the domains of cybersecurity, smart mobility, smart cities, and various transportation solutions. Notably, in the field of innovation and technology transfer, organisations like Eurecat and i2CAT deserve mention.

Figure 10: Agents of the cybersecurity ecosystem in Catalonia[137]

5

Policies and context

5. Policies and context

This chapter explores EU-level policies such as the General Data Protection Regulation (GDPR) and the NIS 2 Directive, emphasizing their roles in harmonizing data protection and enhancing cybersecurity resilience. It delves into the significance of the European Union Agency for Cybersecurity (ENISA) and its Transport Resilience and Security Expert Group (TRANSEEC) in fortifying cybersecurity measures within the transport sector. Additionally, it highlights the pivotal role of Information Sharing and Analysis Centres (ISACs) in facilitating information exchange and bolstering cybersecurity infrastructure. At the national level in Spain, the chapter discusses key laws and regulations including the Organic Law on Data Protection (LOPD-GDD) and the Law on Information Society Services and Electronic Commerce (LSSI-CE), emphasizing their importance in protecting personal data and regulating electronic commerce. The chapter also underscores Spain's efforts to secure critical infrastructures, particularly in the railway transport sector, aligning with the UNECE World Forum for Harmonisation of Vehicle Regulations (WP.29) framework.

5.1 EU level

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a comprehensive data privacy and protection framework that was enacted by the European Union (EU) and became fully enforceable on May 25, 2018. It replaced the Data Protection Directive 95/46/EC and represents a significant overhaul of data protection laws within the EU. GDPR aims to harmonise and strengthen data protection rules across all EU member states, providing a unified set of regulations for the processing of personal data. Its primary objective is to give individuals greater control over their personal information and to ensure that organisations handling this data do so responsibly and transparently.

NIS 2 Directive

The publication of the NIS 2 Directive in the Official Journal of the European Union as Directive (EU) 2022/2555 in December 2022 holds significant implications for entities in the transportation sector, now recognised as essential for cybersecurity. This EU cybersecurity directive aims to enhance the cybersecurity resilience of critical suppliers within the European Union. Notably, the NIS 2 Directive applies to all companies, suppliers, and organisations providing essential or significant services for the European economy and society, even those operating outside the EU. Under the NIS 2 Directive, these entities are required to implement specific cybersecurity practices by 2024 and report any breaches to the relevant authorities. Unlike the previous NIS Directive, the updated NIS 2 now explicitly includes the transportation sector, emphasising the critical role of the industry in maintaining robust cybersecurity measures.

Furthermore, the directive holds management accountable for the implementation and maintenance of risk and cybersecurity practices, accompanied by penalties for non-compliance. The directive aims to mitigate disparities in cyber resilience among Member States, recognising that such discrepancies could ultimately impact all members. Its overarching objective is to eliminate these significant divergences.

While the directive does not prescribe specific cybersecurity tools and technologies and is not explicitly tailored to mobility, it does provide a comprehensive framework for risk and cybersecurity management, endorsing the use of

conventional information security management systems.

To foster collaboration and information sharing among national authorities, the directive establishes a Cooperation Group, facilitating coordinated efforts in cybersecurity. Additionally, it mandates the creation of an EU registry for coordinated vulnerability disclosure, both overseen by the EU Agency for Cybersecurity (ENISA).

European Union Agency for Cybersecurity (ENISA)

From the perspective of the transport sector, ENISA's role under its current mandate, as initiated by the Cybersecurity Act, holds significant implications for ensuring a robust cybersecurity framework within transportation. Key tasks undertaken by ENISA, particularly relevant to the transport sector, include:

- Facilitating policy implementation: ENISA actively contributes to the implementation of cybersecurity policies, notably the NIS 2 Directive, and supports various policy initiatives integrating cybersecurity elements across sectors such as energy, finance, and crucially, transport. It aids Member States in executing specific cybersecurity aspects of Union policy and law pertaining to data protection and privacy within the transport domain.

- Strengthening cybersecurity capabilities: ENISA conducts training programmes to enhance the capabilities and expertise of EU and national public authorities in the transport sector. These efforts focus on improving incident response procedures and supervising cybersecurity-related regulatory measures, thus fortifying the sector's resilience against cyber threats.

- Addressing market-related challenges: ENISA conducts analyses of cybersecurity market trends, ensuring an effective alignment between the demand and supply of cybersecurity solutions within the transport sector. Additionally, it supports EU policy development in ICT standardization and cybersecurity certification, vital for maintaining a secure and standardised environment for transport operations.
- Enhancing operational cooperation and crisis management: with a focus on enhancing preventive operational capabilities, ENISA plays a crucial role in operational cooperation, serving as the secretariat of the CSIRTs Network. It provides critical assistance to Member States in managing cybersecurity incidents and contributes to the coordinated response to large-scale cross-border cybersecurity crises, ensuring the resilience of the transport sector in the face of emerging threats.

ENISA's Transport Resilience and Security Expert Group (TRANSEEC)

ENISA's TRANSSEC serves as an essential platform for experts within the transport sector, fostering the exchange of insights and strategies to combat cyber security threats. With a focus on air transport, rail transport, and water transport/maritime, TRANSSEC aims to identify critical security measures necessary to safeguard the sector from potential cyber risks. The group's key objectives include producing specialised work streams, contributing to policy papers on security in transport, facilitating knowledge exchange, and promoting collaboration among stakeholders. Additionally, TRANSSEC aims to prioritise participation in relevant workshops and discussions concerning the implementation of effective security measures and standardisation practices within the Transport industry.

EXPERTS SAY

"The TRANSSEC initiative has been a significant milestone, contributing to the establishment of comprehensive cybersecurity frameworks for various transport modes. Our collective efforts in collaboration with international organisations aim to bolster the resilience of our transport networks and foster a more secure environment for passengers and operators alike"

Giorgio Pizzi
Division Director of the Directorate General of Local Public Transport
Ministry of infrastructure and Transport of Italy

Information Sharing and Analysis Centres (ISAC)

ISACs serve as vital non-profit entities that act as centralised hubs for collating intelligence on cyber threats, particularly in the context of critical infrastructure. These organisations facilitate two-way sharing of crucial information between the public and private sectors, enabling the exchange of insights on root causes, incidents, and emerging threats. Additionally, they foster the dissemination of valuable experience, knowledge, and analysis among stakeholders. In numerous EU Member States, the establishment of ISACs or similar initiatives has been instrumental in fortifying cybersecurity measures. European regulations, notably the NIS Directive and the Cybersecurity Act, actively support the development of sector-specific ISACs and Public-Private Partnerships (PPPs) within the EU. The NIS Directive, for instance, delineates essential service operators across various sectors and mandates the implementation of incident reporting requirements. The formation of sectoral ISACs at the national level stands to significantly aid in the effective implementation of these regulatory provisions. As European legislation is transposed into national law, these communities can benefit from informed guidance and insights from policymakers, fostering a collaborative approach to cybersecurity management.

At the European level, several ISACs are in the pipeline, aligning closely with the realms of smart mobility, including domains such as transport, rail, cities, tourism, and automotive. These initiatives signify a concerted effort to bolster the cybersecurity posture within these sectors, emphasising the critical role of information sharing and collaboration in fortifying Europe's digital resilience.

Figure 11: 2022 Sector view and identified EU ISAC Initiatives[138]

Future developments

The EU is taking steps to advance the digitalization of transportation by focusing on key enabling technologies. These efforts are supported by funding programmes under the 2021-2027 long-term budget with an emphasis on deployment. Some of the key technologies and initiatives in this digital transformation of mobility include[139]:

Connected and Automated Mobility (CAM): The European Commission is working on a legal framework for the approval of automated vehicles and supporting research and innovation to make Europe a world leader in CAM systems and services.

Cooperative Intelligent Transport Systems (C-ITS): These systems enable information exchange among vehicles and infrastructure, enhancing road safety and traffic efficiency. Their deployment receives support from the Connecting Europe Facility (CEF) program.

5G connectivity: 5G is crucial for automated vehicles and digitalised trains. The EU aims to achieve uninterrupted 5G coverage on major transport paths by 2025, supported by financial programs and public-private partnerships.

Artificial Intelligence (AI): AI has diverse applications in transport, from automated vehicles to optimizing electric vehicle charging. The EU is actively supporting research and innovation projects that apply AI in the field.

Semiconductors: Ensuring a strong semiconductor ecosystem is essential for supply chain resilience. The European Chips Act package aims to address semiconductor shortages and mobilise significant investments.

Support for digital transformation: European Digital Innovation Hubs (EDIHs) are established to help mobility and transport companies, especially smaller ones, in their digital transformation. These hubs provide access to technical expertise and innovation services.

Digital skills: Given the transformations in the transport sector, there is a growing need for digital skills in the workforce. The EU has launched initiatives to reskill and upskill workers and equip them with the required digital skills.

5.2 National level (Spain)

At the national level, several laws and regulations have been implemented in Spain regarding cybersecurity and data protection, including:

Organic Law on Data Protection (LOPD-GDD)

It establishes the general framework for data protection in Spain, complementing the EU General Data Protection Regulation (GDPR). It is particularly important for companies that handle personal data of users.

Law on Information Society Services and Electronic Commerce (LSSI-CE)

It regulates the use of electronic commerce and information society services in Spain. This is crucial for stakeholders that carry out transactions with payment cards and other electronic services.

Royal Decree 311/2022

It establishes specific measures for the security of networks and information systems. This decree defines the minimum technical and organizational measures that entities must adopt to protect personal data, as well as the obligations of the parties involved in the processing of personal data, including the appointment of a Data Protection Officer (DPO) and the obligation to report data breaches to the Spanish Data Protection Agency (AEPD).

Royal Decree 12/2018

It addresses the security of network and information systems in Spain. This law is crucial in the context of cybersecurity, as it mandates the implementation of necessary measures to guarantee the security of networks and information systems. It outlines the essential requirements for managing cybersecurity risks and ensures the protection of critical infrastructure against potential cyber threats. Additionally, it defines the responsibilities of various stakeholders in maintaining the security of networks and information systems.

National Centre for the Protection of Critical Infrastructures (CNPIC)

The Spanish government has established the National Centre for the Protection of Critical Infrastructures (CNPIC), which is responsible for identifying, assessing, and managing risks to critical infrastructures, including those related to cybersecurity. In the railway transport sector, the Spanish Association of Railway Infrastructure Administrators (Adif) has its own Information Security Management System (ISMS) in place to protect the information systems and communication networks that support its business activities and processes and to comply with legal obligations. Moreover, the Transposition of the NIS Directive in Spain includes the transportation sector, designated as one of the strategic sectors in Annex to Law 8/2011, dated April 28[140]. The integration of this sector aligns with Spain's commitment to fortifying its cybersecurity framework and ensuring the resilience of critical infrastructures. Under the United Nations Economic Commission for Europe (UNECE) World Forum for Harmonisation of Vehicle Regulations (WP.29) framework, the R.E.3 Consolidated Resolution on the Construction of Vehicles aims to support the development of UN Regulations and promote harmonisation in the regulatory environment for wheeled vehicles. It contains definitions and guidance on the scope and requirements for the construction of vehicles, covering aspects such as active and passive safety, environmental considerations, and advanced driver assistance systems. The resolution also includes guidelines on cybersecurity and data protection.

6

Funding opportunities

6. Funding opportunities

To address the increase in cyber-attacks, the EU has prioritised the protection of digital economy, critical infrastructure, and citizen privacy, allocating funds through various initiatives. For instance, Horizon Europe's destination Increased Cybersecurity has a budget of EUR 119.1 million for 2023-2024, while the Digital Europe Programme aims to provide support for cybersecurity emergency mechanisms and coordination between civilian and defence spheres. The European Defence Fund has allocated EUR 60 million for 2023 to bolster cybersecurity solutions for defence and enhance defence systems' security. These efforts highlight the EU's commitment to strengthening cybersecurity capacities and digital technologies across the region[141].

This chapter provides an overview of the funding opportunities available under the Horizon Europe and RETECH programmes for cybersecurity applications to smart mobility. Additionally, it discusses some of the successful projects that have been funded under these programmes (and the previous Horizon 2020) in the field of cybersecurity applications to mobility, and their expected impact on the future of mobility.

Horizon Europe

The Horizon Europe programme offers funding opportunities for research and innovation projects that aim to develop advanced cybersecurity solutions for smart mobility applications. The programme provides support for collaborative projects between academia, industry, and public organisations to develop innovative technologies, policies, and best practices to improve the security and resilience of mobility systems.

EIT Urban Mobility

EIT Urban Mobility offers various funding instruments for innovators in the smart mobility sector. Annually, a 'Call for Innovation' is launched, focusing on four city challenges: active mobility, sustainable city logistics, energy and mobility, and future mobility. The thematic areas within these challenges cover a wide range of topics. For instance, projects that provide artificial intelligence solutions in mobility management applications, including complex mobility scenario predictions and applications that enhance the user journey experience, manage data protection, address cybersecurity, sustainability, and travel preferences have been highlighted as being in scope of their funding objectives in recent calls.

Moreover, the EIT Urban Mobility Accelerators consist of seven thematic EU-funded programmes to take early-stage mobility start-ups to the next level. It looks for early-stage start-up teams with business ideas that reduce congestion and increase efficiency in the transport system, innovative approaches to make commuting faster or more enjoyable, or concepts to accelerate the transition to low- or zero-emission forms of transport. Recently selected start-ups spanned from cybersecurity and software-based products enhancing connectivity and autonomy, to hardware that shapes and visually changes the public realm.

Public call for RETECH funds

The Cybersecurity Agency of Catalonia leads one of the nodes under the RETECH Fund (Redes Territoriales de Especialización Tecnológica), collaborating closely with the Valencian and Galician communities. Aiming to drive digital transformation and specialised projects, this European funding programme, overseen by the National Cyber Security Institute (INCIBE), allocates an initial budget of EUR 149 million across 15 autonomous communities. The Government will initially provide EUR 530 million of investment for this innovative initiative for the 2022-2023 period, which will have additional financing from the autonomous communities and, depending on success, could be reinforced with the funds from the addendum to the Recovery Plan. The following are the focus areas for these funds:

Culture and talent:

- Implementation of advanced cybersecurity training programmes.

- Establishment of scholarship programmes.

- Promotion of awareness among society and the business community regarding potential risks.

Development of innovation ecosystems:

- Formation of networks of sector-specific laboratories for smart technologies (automotive, aeronautical, and naval).

- Assessment of cybersecurity for various technologies and use cases.

- Standardisation of security protocols for 4.0 technologies and processes.

Support to start-ups:

- Establishment of networks of demonstration centres to foster the advancement of cybersecurity technologies and solutions.

- Provision of capacities within a network of laboratories.

- Implementation of internationalisation strategies for companies.

Deployment and acquisition of services and solutions:

- Development of tailored cybersecurity solutions.

- Creation of an observatory focused on technologies and solutions within the cybersecurity domain.

- Promotion of interoperability between business infrastructures and laboratory networks.

The Cybersecurity Agency of Catalonia oversees the governance of the funds, providing support for upcoming initiatives. The application process, started in 2023, involves the submission of ideas, subsequent evaluation of proposals, resolution of agreements and subsidies, and the eventual initiation of the projects.

6.1 Relevant projects

Research into digital security is essential to building innovative solutions that can protect Europe against the latest, most advanced cyber threats. That is why cybersecurity has been an important part of the Horizon 2020 programme and its successor Horizon Europe. In Horizon Europe, for the period 2021-2027, cybersecurity is part of the 'Civil Security for Society' cluster. Moreover, the Digital Europe Programme, for the period 2021-2027, plans to invest EUR 1.9 billion into cybersecurity capacity and the wide deployment of cybersecurity infrastructures and tools across the EU for public administrations, businesses, and individuals, addressing smart mobility, among other strategic sectors. Cybersecurity is also a part of InvestEU, a general programme that brings together many financial instruments and uses public investment to secure further investment from the private sector. Its strategic investment facility will support key value chains in cybersecurity, including transport-related projects.

Data Space Demonstration Centre (RETECH)

This initiative, led by the Catalan Agency of Cybersecurity, revolves around establishing a demonstration centre for data spaces specialising in cybersecurity services for multiple sectors, including smart transportation, health sciences, connected industry, and cybersecurity operational excellence. This centre will be established within Catalonia, the Valencian Community, and Galicia.

Participants in the Demonstration Centre will comprise cybersecurity service developers and providers, sector-specific data owners, technology infrastructure firms, data space implementation services, and prospective data space operators. Leveraging smart technologies, enhanced connectivity, and artificial intelligence, the automotive industry is transitioning toward more intelligent and eco-friendly vehicles, highlighting the growing significance of cybersecurity. A key aim within the Cooperative, Connected, and Automated Mobility (CCAM) ecosystem is the proactive application of

advanced artificial intelligence (AI) and machine learning (ML) techniques to address cybersecurity challenges in modern vehicles. Continuous efforts are being made to mitigate associated security risks. The establishment of a data space demonstrator centre aims to foster the integration of a diverse range of data sources and encourage collaboration among stakeholders in the CCAM ecosystem. This collaboration will facilitate the development of ML algorithms and threat detection technologies, enhancing the efficacy of immunisation strategies against cyber-attacks. Additionally, there is a proposal for an 'in-car anti-hacking' device, an added passive control unit within vehicles dedicated to cybersecurity functionality. This device generates integrated analysis data transmitted to the data space through a dedicated connector for storage, exchange, and processing. By consolidating this data in the data space, the ability to detect malicious attacks and unknown anomalies is significantly enhanced. This approach is projected to achieve various objectives, including improving passenger and pedestrian safety, defining minimum cybersecurity standards for smart technologies, minimising the risk of confidential data breaches, reducing accident rates, and bolstering public confidence in Connected Autonomous Vehicles (CAVs) as a rapidly evolving sector. Furthermore, the initiative emphasises the consideration of cybersecurity-related data sets across various smart technology-based mobility scenarios, encompassing not only land transport but also air and naval transportation.

SELFY (Horizon Europe)

SELFY, short for SELF assessment, protection & healing tools for a trustworthY and resilient CCAM (June 2022 – May 2025), is to develop a self-assessment and self-protection toolbox to enhance the security and resilience of Connected, Cooperative and Automated Mobility (CCAM) systems against potential cyber-attacks and malicious actions. This is at a time when around 50 million connected and automated cars are expected to be on the road in Europe by 2026.

The project seeks to be the main supplier of an agnostic to OEMs toolbox for trust data management, collaborative perception, security preservation, self-healing and resilience self-management in the industry which can be easily rolled out to provide self-awareness, self-resilience, and confidence to the end user. It will also deliver compliance with European regulations that require cybersecurity certificates for this type of vehicles.

The SELFY project tackles emerging risks and threats which call for a global, decentralised, and collaborative solution that works between static and mobile assets and CCAM ecosystem players.

To take the solution forward, the SELFY project consortium will address the kind of data to be generated, gathered, and monitored; advanced data processing to identify potential threats; developing new tools to add to the ability to adapt and cope with cyber threats by lessening their impact, and uptake and deployment of services and solutions in this field. SELFY tools are to ensure privacy, confidentiality, and integrity, as well as improve accessibility in the CCAM environment.

The solutions developed by the project will first be validated with simulation and in a lab. Three scenarios will then be built in real and controlled environments to demonstrate the toolbox's performance and usefulness in a collaborative and cooperative environment.

The SELFY project consortium is led by Eurecat, with other Catalan stakeholders involved, namely Ficosa, and Applus+ IDIADA; the Asociación Española del Vehículo Autónomo Conectado – AEVAC (Spanish Association of the Connected Autonomous Vehicle); and other partners from France, Germany, Austria, the Netherlands, Japan, Australia, and Turkey.

CitySCAPE (Horizon 2020)

CitySCAPE, short for City-level Cyber-Secure Multimodal Transport Ecosystem (September 2020 – August 2023), addressed the limitations of traditional security controls in adapting to the changing requirements and applications of multimodal transport systems. These shortcomings allowed security threats and incidents to disrupt various dimensions of transportation, posing a risk to the multimodal

ecosystem. By examining the interactions between the multimodal transport system and other critical sectors outlined in the NIS Directive (such as energy and banking), the CitySCAPE project introduced innovative risk analysis techniques and developed a series of software solutions. These solutions were integrated into an interoperable toolkit that could be incorporated into any multimodal transport system. This toolkit facilitated collaborative analysis of security and privacy threats, proactive countermeasures at potential cyber-attack entry points, comprehensive impact assessments in both technical and financial terms, and the provision of informative notifications to CERT/CSIRT. The effectiveness of the proposed solution was validated through regional-level pilots in Tallinn (Estonia) and Genoa (Italy), utilising specific use-cases carefully selected by transport operators. The insights gained from these pilots significantly influenced the development of standardisation contributions, including labelling protocols, to enhance security measures within the transportation ecosystem.

E-CORRIDOR (Horizon 2020)

E-CORRIDOR, short for Edged Enabled Privacy & Security Platform for Multi Modal Transport (June 2020 – May 2023), aimed at developing a technological framework to unleash the power of information sharing coupled with edge-based collaborative analytics for cyber protection. It involved Catalan stakeholders Factual, Pildo Labs, and AMTU, among other partners.

The framework has been tailored for multimodal transport needs by developing a set of security services based on it.

The framework allows data prosumers (producers/consumers) to easily express their preferences on how to share their data, which analytics operations can be performed on such data and by whom, with whom the resulting data can be shared etc. This entails a framework that combines several technologies for expressing and enforcing data sharing agreements as well technologies to perform data analytics operations in a way which is compliant to these agreements. Among these technologies there are data-centric policy enforcement mechanisms and data analysis operations directly performed on encrypted data provided by multiple prosumers.

The framework is mainly based on an Information Sharing Infrastructure (ISI) and an Information Analysis Infrastructure (IAI) that can be deployed in several ways and on several devices (from cloud to mobile devices). This concept extends the one developed in the C3ISP project (where several prosumers offer controlled data to a centralised analytics service) to a fully decentralised environment. Being potentially computed at the edge, the analysis process is increasingly more privacy friendly (i.e., not the raw data but only the results of the locally analysed data are provided to the upper layer). When the shared data are cyber threat information, a powerful system for creating Information Sharing and Analysis Centre (ISAC) has been obtained.

CARAMEL (Horizon 2020)

CARAMEL, short for Artificial Intelligence based cybersecurity for connected and automated vehicles (October 2019 – June 2022), aimed to introduce an innovative anti-hacking intrusion detection/prevention system for the European automotive industry. It involved Catalan stakeholder i2CAT, among other partners.

The damaging effects of cyberattacks to an industry like the Cooperative Connected and Automated Mobility (CCAM) can be very relevant. From the least important to the worst ones, one can mention for example the damage in the reputation of vehicle manufacturers, the increased denial of customers to adopt CCAM, the loss of working hours (having direct impact on the European GDP), material damages, increased environmental pollution due to traffic jams, or malicious modifications in sensors' firmware, and ultimately, the danger for human lives, either they are drivers, passengers, or pedestrians.

CARAMEL's goal has been to proactively address modern vehicle cybersecurity challenges applying advanced Artificial Intelligence (AI) and Machine Learning (ML) techniques, and to continuously seek methods to mitigate associated safety risks.

In order to address cybersecurity considerations for the already here autonomous and connected

vehicles, well-established methodologies coming from the ICT sector have been adopted, allowing to assess vulnerabilities and potential cyberattack impacts. Although past initiatives and cybersecurity projects related to the automotive industry have reached to security assurance frameworks for networked vehicles, several newly introduced technological dimensions like 5G, autopilots, and smart charging of Electric Vehicles (EVs) introduce cybersecurity gaps, not addressed satisfactorily, yet. Considering the entire supply chain of automotive operations, CARAMEL has targeted to reach commercial anti-hacking IDS/IPS products for the European automotive cybersecurity and to demonstrate their value through extensive attack and penetration scenarios.

SECREDAS (ECSEL JU & Horizon 2020)

SECREDAS, short for Cyber Security for Cross Domain Reliable Dependable Automated Systems (May 2018 – October 2021), focused on enhancing security, safety, and privacy in automated and autonomous systems. With over 70 participating organisations, including the Catalan partner Ficosa, the project successfully developed integrated solutions across various domains. Its final conference showcased more than 40 hardware and software demonstrators, emphasising the need to build consumer trust in automated systems. SECREDAS's work is notable for its cross-domain reference architecture and emphasis on mitigating external threats in autonomous driving, rail applications, and health monitoring systems.

EXPERTS SAY

"Within the Horizon 2020 project CARAMEL, an anti-hacking device was developed that can detect several cyberattacks, including defaced traffic signs, attacks to V2X communications and GNSS spoofing and respond to them. Further development of such tools can help dramatically increase the safety of CAVs".

Jordi Guijarro
Cyber Security Innovation Director, i2CAT

CYRail (Horizon 2020)

CyRail, short for Cybersecurity in the RAILway sector (October 2016 – September 2018), which received funding from the Shift2Rail Joint Undertaking, was focused on addressing the critical theme of "Threat detection and profile protection definition for cybersecurity assessment".

The main technical objectives of CYRail were:

- To select security analysis frameworks capable of assessing the most critical railway services, zones, and communications to perform an exhaustive cybersecurity assessment of the railway systems.

- To deliver a taxonomy of threats targeting rail management and control systems capable of classifying, describing, and analysing cyber-attack threats.

- To assess and select innovative rail management systems attack detection techniques.

- To specify countermeasures and mitigation strategies for improved quality levels.

- To describe resilience mechanisms for operational safety.

- To specify protection profiles with evaluation of assurance levels.

Emphasising security by design, the CYRail project developed an in-depth analysis of threats targeting railway infrastructures, pioneering innovative techniques for attack detection and alerting. Additionally, the project defined customised mitigation plans and countermeasures, taking into account their potential implications on daily operations. The project significantly enhanced the operational security level of various rail segments and bolstered the robustness of railway information, control, and signalling sub-systems.

The CYRail project recommended an alerting and collaborative incident management system that was designed as a 3-tier system, incorporating detection means (tier 1), a centralised alerting and monitoring system (tier 2), and a collaborative information sharing system (tier 3). Leveraging the latest market solutions such as SIRPs, the system aimed to enhance alerts and incident response, facilitating seamless integration with operation teams. The proposed cyber security incident response approach supported the decision-making process and enabled the involvement of public authorities, fostering a comprehensive understanding of the impacts of cyber-attacks and the associated response measures. Moreover, the system was engineered to integrate with legacy systems like IMS, allowing the reuse of detection means in specific zones and conduits, and ensuring compatibility with any SIEM available in the market.

EXPERTS SAY

"The CitySCAPE project in Tallinn involved testing multimodal solutions, particularly in the context of Mobility-as-a-Service (MaaS) integration. The project actively engaged users and strengthened the CERT's role with real-time information. The pilot included comprehensive testing of network communication integrity, last-mile connection security, and ticket validation. Various attack scenarios, including GNSS spoofing and sybil attacks, were simulated to assess system robustness.".

Liivar Luts
External Projects Coordinator, Tallin Transport Department

7

Standards

7. Standards

The integration of advanced technologies within the smart mobility sector has initiated a transformative shift in modern transportation, emphasizing the importance of robust cybersecurity measures to safeguard interconnected systems. In this landscape, adherence to internationally recognised standards and framework profiles, including those developed by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the Society of Automotive Engineers (SAE), and the National Institute of Standards and Technology (NIST), has become crucial for ensuring the resilience and security of smart mobility infrastructure.

Standards, such as those developed by ISO, IEC, and SAE, delineate the established guidelines and specifications that define quality, safety, and interoperability requirements for products and systems within the smart mobility industry. These standards provide a foundation for ensuring compliance and uniformity across various components and systems, promoting efficiency and reliability in the evolving landscape of smart mobility.

Simultaneously, framework profiles, like those formulated by the National Institute of Standards and Technology (NIST), offer tailored guidelines and recommendations specific to particular industries or sectors. Framework profiles, such as the NIST Cybersecurity Framework, provide a customizable approach for organizations to assess their cybersecurity posture and manage risks, thereby enhancing the overall security framework within the smart mobility domain.

This chapter seeks to give an overview of the most relevant cybersecurity standards and framework profiles in the field of smart mobility, emphasizing through the hereby presented table, their roles in fortifying cybersecurity practices within the smart mobility ecosystem.

Code	Description	Relevance to the smart mobility field
ISO/IEC 27001	An international standard that provides a framework for an information security management system (ISMS)	This certification ensures that the organization has a comprehensive and systematic approach to managing sensitive company and personal information, including that of customers, employees and suppliers. This is relevant in the transport industry as the industry handle sensitive information such as passenger's personal data and transactions, and the company's financial and operational data.
ISO/IEC 27005	A standard that provides guidelines for information security risk management.	This certification ensures that the organization has a systematic and proactive approach to identifying and assessing risks to information security and implementing appropriate controls to mitigate those risks. This is relevant in the transport industry as it involves the handling of sensitive information and the need to protect infrastructure, such as control systems and networks, from cyber threats.
ISO/IEC 27032	A standard that provides guidelines for cyber security in the field of communication networks and systems.	This certification ensures that the organization has a systematic and proactive approach to identifying and assessing risks to cyber security in communication networks and systems and implementing appropriate controls to mitigate those risks. This is relevant in the transport industry as it involves the use of communication networks and systems to control and monitor transportation infrastructure, such as train signalling systems and air traffic control systems.
ISO/IEC 22301	A standard that provides a framework for business continuity management.	This certification ensures that the organization has a systematic and proactive approach to identify, assess, and mitigate the impact of potential disruptions, including cyber threats, and to ensure the organization can continue to operate in case of an incident. This is relevant in the transport industry as it involves the need to protect infrastructure, such as control systems and networks, from cyber threats, and to ensure the continuity of transportation services in case of an incident.
ISO/SAE 21434	A standard that provides guidelines for cyber security in the field of connected and automated transport systems.	This certification ensures that the organization has a systematic and proactive approach to identify and assess risks to cyber security in connected and automated transport systems and implement appropriate controls to mitigate those risks. This is relevant in the transport industry as the usage of connected and automated systems is increasing in the transport sector and it's crucial to ensure the security of these systems.
IEC 62443 or prTS 50701 (CLC/TS 50701:2021)	International standard for security in industrial automation and control systems. It outlines a systematic approach to cybersecurity, encompassing various aspects such as risk assessment, policies, procedures, and technical controls tailored to industrial settings.	Relevant for securing critical infrastructure and transportation systems, such as control systems in railways, traffic management systems, and other automated transportation systems. It provides guidelines for protecting these systems against cyber threats and ensuring the safe and secure operation of transportation networks.
NIST IR 8473	Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure designed to aid organizations in managing threats to systems, networks, and assets within the Electric Vehicle Extreme Fast Charging Infrastructure (EV/XFC) ecosystem. It is an application of the Framework Categories and Subcategories in the context of the EV/XFC cybersecurity ecosystem.	Provides a comprehensive approach for assessing and communicating cybersecurity posture, facilitating cross-collaboration between industry parties, vendors, and end-users in the smart mobility field.

Table 1: Outline of main standards related to cybersecurity in smart mobility

8

Recommendations for a smarter and cybersecure mobility

8. Recommendations for a smarter and cybersecure mobility

Smart mobility stakeholders in Catalonia can play a pivotal role in safeguarding the sector's security and safety, while simultaneously nurturing the growth of a dynamic smart city industry grounded in secure technologies and innovation. To achieve this dual objective, stakeholders should actively engage in various strategic actions. These multifaceted efforts collectively not only protect the integrity of smart mobility systems but also position Catalonia as a secure technology and innovation hub, driving the region towards a key role in the smart city industry.

In this chapter we outline recommendations for each of the stakeholders identified.

For smart mobility stakeholders: service & infrastructure operators, and vehicle manufacturers

- Implementing cybersecurity standards applicable to the transportation sector, such as the ones outlined in the previous chapter, ensures a robust and consistent approach to security.

- Compliance with relevant laws and regulations is crucial and a good starting point for ensuring cybersecurity in smart mobility. The compliance landscape includes national laws such as the Organic Law on Data Protection and Digital Rights Guarantee (LOPDGDD) and the Spanish Law on Information Society Services (LSSI). If the operator deploys a public or an essential service, they are obligated to adhere to the transposition of the European Network and Information Systems Directive (NIS) in Spain, as well as the National Security Scheme (ENS). Furthermore, it is essential to adhere to the European General Data Protection Regulation (GDPR). Adhering to these regulations helps protect user privacy, secure data, and maintain the trust of customers and stakeholders.

- Implement continuous monitoring of critical systems and networks, leveraging security information and event management solutions to detect and respond to potential security incidents in real-time, thereby minimising the impact of cyber threats on the smart mobility infrastructure.

- Collaborate with cybersecurity experts and vendors to implement robust cybersecurity measures, including regular penetration testing and vulnerability assessments to ensure the secure operation of critical systems and networks.

- As the smart mobility industry undergoes transformation, employees must adapt to new working methods and acquire cybersecurity-related skills. This transformation affects various aspects of the industry, from engineering and design to sourcing, programme management, sales, and service. To prevent the risk of falling victim to social engineering attacks or insider threats, it is crucial to install a strong culture of awareness and implement rules and controls. The importance of following security policies and procedures is fundamental for the cybersecurity of the entire smart mobility ecosystem.

- The development and adherence to a comprehensive incident response plan is key to efficiently handle and mitigate cybersecurity incidents. The plan should outline the roles and responsibilities of incident response teams, the steps to contain and investigate incidents, and the procedures for reporting and communicating incidents to relevant parties. Currently, in Spain, incident responding is responsibility of INCIBE, with the Cybersecurity Agency of Catalonia providing substantial local support in Catalonia.

- Establish robust vendor risk management procedures to assess the cybersecurity practices of third-party vendors and service providers, ensuring they meet industry standards and do not pose additional risks to the smart mobility ecosystem. It is important that unbiased experts audit or assess the cybersecurity practices of vendors and service providers in the smart mobility landscape and implement robust vendor risk management procedures to evaluate their

security capabilities and ensure they meet industry standards.

- Share data on cyberattacks, IoCs (Indicators of Compromise), TTPs (Techniques, Tactics, and Procedures), and early alerts to raise awareness among other organisations or CERTs and strengthen the cybersecurity sector. Data spaces can be a suitable platform for this purpose while maintaining governance and control of one's own data.

- Collaborate with public bodies and technology centres to establish comprehensive cybersecurity testing and assessment facilities for infrastructure supporting smart mobility systems, ensuring the secure and reliable operation of critical systems and networks.

- Partner with research institutions to conduct in-depth studies on the evolving cybersecurity challenges in the smart mobility sector and devise effective strategies to address these challenges.

For public bodies:

- Create a comprehensive national cybersecurity strategy that includes specific provisions for securing smart mobility infrastructures and services. The strategy should outline objectives, responsibilities, and timelines for implementing cybersecurity measures as well as to invest in research and development efforts focused on cybersecurity innovations and technologies for smart mobility.

- In order to put the strategy into practice, the recommendation is to conduct periodic security audits and assessments to evaluate the overall cybersecurity posture of the smart mobility ecosystem. By understanding the risks, organisations can select and implement targeted security measures to mitigate the identified threats effectively.

- Ensure the enactment of cybersecurity regulations and standards tailored for the smart mobility sector, such as the ones outlined in the previous chapter, and lead the compliance of all stakeholders to these guidelines.

- Organise cyberattack simulacres to evaluate the effectiveness of the cybersecurity capabilities within companies operating in the smart mobility sector. These exercises will serve as invaluable tools for assessing the readiness and response mechanisms of these organisations in the face of potential cyber threats, ensuring the overall security and resilience of the smart mobility industry.

- Collaborate with other countries and international organisations to share cybersecurity best practices, threat intelligence, and regulatory approaches is key to improve global cybersecurity standards for smart mobility. In this regard, actively participating in the ECCC dialogues and promoting smart mobility related initiatives will create opportunities for further investing and advancing in this sector. Furthermore, engaging with the Joint Cyber Unit (JCU), a new platform that aims to strengthen cooperation among EU institutions, agencies, bodies, and the authorities in the Member States, will ensure an EU coordinated response to large-scale cyber incidents and crises, as well as offer assistance in recovering from these attacks, such as those targeting critical transport infrastructures.

- Establishing forums and platforms for sharing information, best practices, and threat intelligence can significantly enhance collective defence against cyberattacks. For example, the creation of an ISAC (Information Sharing and Analysis Centre) for smart mobility could be a solution to this objective. Additionally, participating in existing international ISACs focused on the matter would further strengthen cybersecurity efforts.

- Create a sectorial CERT would have a deep understanding of the unique cybersecurity challenges and risks faced by organisations within the smart mobility sector. This specialised knowledge would allow them to tailor their services and support to address the specific needs and threats encountered in the industry. Moreover, a sectorial CERT would serve as a central point for coordinating incident response efforts and sharing threat intelligence among organisations within the smart mobility sector.

- Capacity building is of paramount importance for all stakeholders in the smart mobility value chain, and so is capturing talent to join the cybersecurity teams and contribute to enhance resilience

against future cyberattacks. Educational programmes should include cross-thematic studies meant to boost the EU cyber workforce, especially professionals specifically trained to address the cyber-vulnerabilities of the smart mobility ecosystem.

- Support research initiatives that combine cybersecurity and smart mobility to develop effective strategies for secure and resilient integration of digital technologies into smart mobility systems.

- Create testbeds and pilot projects to evaluate the cybersecurity of new smart mobility technologies before large-scale deployment. These controlled environments would allow for identifying vulnerabilities and refining cybersecurity measures.

- In order to promote test and secure developments, it might be positive to establish and fund a European Cybersecurity Centre for Smart Mobility, similar to the EUROCYBCAR initiative, to facilitate comprehensive cybersecurity testing for connected vehicles and assess the impact of cyber threats on passenger safety and privacy.

- Developing studies that combine cybersecurity and smart mobility is essential for addressing the growing cybersecurity challenges in the rapidly evolving world of transportation and smart mobility. Such studies can provide valuable insights and help devise effective strategies to ensure the secure and resilient integration of digital technologies into smart mobility systems.

- 5G networks are planned to be rolled out across the EU, a key development for the efficient rollout of smart mobility systems, including Connected and Autonomous Vehicles (CAV). While these advanced networks promise substantial advantages, their less centralised architectural design, increased antenna density, and heightened reliance on software create additional entry points for potential cyberattacks. Leveraging the EU's 5G Toolbox outlines a set of actions aimed at reinforcing security standards for 5G networks, imposing appropriate constraints on high-risk suppliers, and promoting a diversified vendor landscape.

9 Conclusions

9. Conclusions

Our exploration of the cybersecurity landscape in smart mobility presents the following key insights and takeaways:

Cybersecurity in smart mobility as imperative

The growing surge in cyberattacks directed at connected vehicles, fleets, digital infrastructures, and end-user applications highlights the urgent need for a strong, coordinated, and tailored cybersecurity strategy within the smart mobility sector. It should consider the distinct risks and vulnerability vectors associated with the different stakeholders, allowing for more effective mitigation. To ensure the safety of the smart mobility ecosystem in Catalonia, organisations should enhance their cybersecurity measures, encourage collaboration and information sharing, allocate resources to employee training, establish incident response protocols, and regularly conduct security audits. In this regard, the European Cybersecurity Competence Centre (ECCC) aims to increase Europe's cybersecurity capacities and competitiveness, working together with a network of National Coordination Centres to build a strong cybersecurity community.

The leadership role of public administration

In the development of this holistic strategy and given the significant presence of the public sector in the smart mobility sector, the public administration (at EU, national, and Catalan level) has a central role in leading the effort towards secure smart mobility solutions. In this regard

The Cybersecurity Agency of Catalonia acts as a facilitator, bringing together industry stakeholders, cybersecurity experts, and relevant governmental bodies to devise comprehensive and adaptable frameworks that address the evolving cyber threats in the smart mobility landscape.

In coherence with this direction, actively advocating for the adoption of rigorous regulatory standards and compliance protocols will cultivate a culture of cybersecurity resilience and accountability among all stakeholder groups in the smart mobility domain.

Furthermore, the public administration should allocate resources for research and development in cybersecurity, encouraging innovation and the deployment of cutting-edge technologies that can fortify the defences of smart mobility systems. A not-to-be-missed opportunity in this regard, fostered by the Spanish government, is the comprehensive "Recovery, Transformation and Resilience Plan", through which is undertaking investments and reforms needed to transform the Spanish economy, mobilising more than EUR 69 billion until 2026, financed by transfers from the NextGenerationEU's Recovery and Resilience Mechanism. Notably including the component 15, devoted to "digital connectivity, fostering cybersecurity, and deploying 5G[142]", all aspects central to smarter, more cybersecure mobility.

Embracing a challenging shift in mindset

The legacy automotive industry is undergoing a profound transformation, shifting from traditional vehicle manufacturing to the software-defined vehicle (SDV) paradigm. This transition emphasises the significance of technical competence, including the implementation of robust cybersecurity measures, the incorporation of "privacy by design and default" principles, as well as the adoption of a more agile and start-up-like approach. Some automotive OEMs have established in-house "start-ups" to drive innovation and have highlighted the challenges of aligning traditional structures struggling to reinvent themselves, with the need for dynamic change in the face of emerging, disruptive technologies, and related cybersecurity demands. Similarly, the imperative shift in mindset applies to all other stakeholders within the smart mobility domain, including traditional public transport organisations, public authorities responsible for road management and mobility planning, and

emerging players in the urban mobility landscape, such as ride-hailing and shared mobility companies. Nonetheless, the task of adopting a cybersecurity-centric mindset is often more seamlessly embraced by new entrants in the smart mobility sector, especially those rooted in technology. These emerging start-ups possess innate agility and adaptability, as they are unburdened by the legacy structures and processes that can hinder the transformation of long-established organisations in the industry.

Opportunities for the Industry in smart mobility cybersecurity

Finally, the increasing digitisation and connectivity in smart mobility systems should also be seen as a great industry opportunity for Catalonia. The country's strengths in the mobility sector and cybersecurity infrastructure, outlined in the previous chapters, position it to capitalise on the growing trend. This presents an opportunity for innovative advancements in smart mobility solutions and continued growth in the cybersecurity sector. By embracing this synergy, Catalonia will position itself as a key player in secure and advanced smart mobility, driving economic growth and technological innovation. In this context, funding mechanisms like Horizon Europe and RETECH present significant opportunities to facilitate innovation and growth, drawing upon the extensive experience within the Catalan smart mobility stakeholder ecosystem.

By conscientiously implementing the outlined recommendations and maintaining a continuous focus on cybersecurity, Catalonia can solidify its position as a pioneering force in the smart mobility sector in Europe. These efforts will not only fortify the country's technological strengths but also ensure the safety and privacy of its citizens, ultimately paving the way for a future characterised by secure, efficient, and sustainable smart mobility solutions.

Glossary

ABS – Anti-lock Braking System

ACC – Adaptive Cruise Control

Adif – Administrador de Infraestructuras Ferroviarias

AEPD – Agencia Española de Protección de Datos

AEVAC – Asociación Española del Vehículo Autónomo Conectado

AI – Artificial Intelligence

AMB – Àrea Metropolitana de Barcelona

AMQP – Advanced Message Queuing Protocol

AMTU – Associació de municipis per la Mobilitat i el Transport Urbà

API – Application Programming Interface

ARP – Address Resolution Protocol

ATM – Autoritat del Transport Metropolità

B2B – Business to Business

B2C – Business to Consumer

BEC – Business Email Compromise

BSM – Barcelona de Serveis Municipals

CAGR – Compound Annual Growth Rate

CAM – Connected and Automated Mobility

CAN – Controller Area Network

CAV – Connected and Autonomous Vehicle

CBTC – Communication-Based Train Control

CCAM – Cooperative Connected and Automated Mobility

CEF – Connecting Europe Facility

CERCA – Centres de Recerca de Catalunya

CERT – Computer Emergency Response Team

CIAC – Clúster de la Indústria d'Automoció de Catalunya

CID – Customer-Identification Device

CIVICAT – Centre d'Informació Viària de Catalunya

CNPIC – Centro Nacional de Protección de Infraestructuras Críticas

CSIRT – Computer Security Incident Response Team

CTTC – Centre Tecnològic de Telecomunicacions de Catalunya

CVC – Centre de Visió per Computador

CVV – Card Verification Value

(D)DoS – (Distributed) Denial-of-Service

DHCP – Dynamic Host Configuration Protocol

DIN – Digital Innovation Nodes

DPO – Data Protection Officer

DRFM – Digital Radio Frequency Memory

DRT – Demand Responsive Transit

DSRC – Dedicated Short-Range Communication

ECCC – European Centre of Cybersecurity Competence

ECSEL JU – Electronic Components and Systems for European Leadership Joint Undertaking

ECSO – European Cyber Security Organisation

ECTS – European Train Control Systems

ECU – Electronic Control Unit

EDIH – European Digital Innovation Hubs

EEPROM – Electrically-Erasable Programmable Read-Only Memory

ENISA – European Union Agency for Cybersecurity

ENS – Esquema Nacional de Seguridad

EPC – Electronic Product Code

ERTMS – European Rail Traffic Management System

EV – Electric Vehicle

EVSE – Electric Vehicle Supply Equipment

FGC – Ferrocarrils de la Generalitat de Catalunya

GDP – Gross Domestic Product

GDPR – General Data Protection Regulation

GNSS – Global Navigation Satellite System

IAI – Information Analysis Infrastructure

IC – Integrated Circuit

ICFO – Institut de Ciències Fotòniques

ICS – Industrial Control Systems

ICT – Information and Communications Technology

IDS – Intrusion Detection System

IEC – International Electrotechnical Commission

IMS – Incident Management System

INCIBE – Instituto Nacional de Ciberseguridad

IoC – Indicator of Compromise

IoT – Internet of Things

IPS – Intrusion Prevention System

ISAC – Information Sharing and Analysis Centre

ISI – Information Sharing Infrastructure

ISMS – Information Security Management System

ISO – International Standards Organization

ITS – Intelligent Transport Systems

IV(N) – In-Vehicle (Networks)

JCU – Joint Cyber Unit

LCA – Lane Change Assist

LCAP – Lightweight CAN Authentication Protocol

LFSR – Linear-Feedback Shift Register

LiDAR – Light Image Detection and Ranging

LIN – Local Interconnect Network

LOPD-GDD - Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales

LSSI-CE - Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico

MaaS – Mobility-as-a-Service

MAC – Message Authentication Code

MitM – Man in the Middle

MDP – Markov Decision Process

MEMS – Micro-Electrical Mechanical Systems

ML – Machine Learning

MOST – Media-Oriented Systems Transport

MOT – Multi-Object Tracking

MQTT – MQ Telemetry Transport

NCC – National Centres Network

NIS – Network and Information Systems

NIST – National Institute of Standards and Technology

OBD – On-Board-Diagnostics

OEM – Original Equipment Manufacturer

ÒPTIMA – Oficina Pública per la Transformació de les Indústries de Mobilitat i Automoció

OTA – Over The Air

OTIDS – Offset Ratio and Time Interval based Intrusion Detection System

PCI-DSS – Payment Card Industry - Data Security Standard

PET – Privacy-Enhancing Technologies

PKES – Passive Keyless Entry Systems

PMR – Public-area Mobile Robots

PMV – Personal Mobility Vehicles

PyCRA – Physical Challenge-Response Authentication

RAN – Radio Access Network

RETECH - Redes Territoriales de Especialización Tecnológica

RKS – Remote Keyless Systems

RPA – Robotic Process Automation

SAE – Society of Automotive Engineers Society of Automotive Engineers

SAP – Source Authentication Protocol

SCADA – Supervisory Control and Data Acquisition

SCT – Servei Català de Trànsit

SDG – Sustainable Development Goals

SDV – Software Defined Vehicle

SIEM – Security Information and Event Management

SIRP – Security Incident Response Platform

SME – Small and medium-sized enterprises

SOAR – Security Orchestration Automation and Response

STI – Sistema Tarifari Integrat

STP – Spanning Tree Protocol

TEC – Transmit Error Counter

TESLA – Timed Efficient Stream Loss-tolerant Authentication

TMB – Transports Metropolitans de Barcelona

TMC – Traffic Management Centre

TPMS – Tire Pressure Monitoring System

TRANSEEC – Transport Resilience and Security Expert Group

TTP – Techniques Tactics and Procedures

UNECE – United Nations Economic Commission for Europe

V2C – Vehicle-to-Cloud

V2I – Vehicle-to-Infrastructure

V2IoT – Vehicle-to-Iot

VET – Vocational Education and Training

VLAN – Virtual Local Area Network

VMS – Variable Message Signs

V2P – Vehicle-to-Pedestrian

V2R – Vehicle-to-Road

V2X – Vehicle-to-Everything

VTC – Vehículo de Transporte con Conductor

XOR – Exclusive or

Authors

Josep Laborda, CEO & Managing Partner at Factual

Pietro Podestà, Mobility Consultant at Factual

Santi Romeu, Head of Data Science & Analytics at Cybersecurity Agency of Catalonia

Acknowledgements

We are deeply grateful to the esteemed experts who generously shared their expertise and knowledge, including Alejandro Adalid Damerau (Cybersecurity Officer at Siemens Mobility), Giorgio Pizzi (Division Director of the Directorate General of Local Public Transport Ministry of infrastructure and Transport of Italy), Jordi Guijarro (Cyber Security Innovation Director at i2CAT), Laia Pagès (Executive and Research Manager at CARNET), José Manuel Barrios (Head of Digital Transformation and Digital Solutions at Applus+ IDIADA), Liivar Luts (External Projects Coordinator at Tallin Transport Department) and Bern Grush (Executive Director and Urban Robotics Foundation). Their valuable input and perspectives have greatly enriched the content and depth of this publication. Santi Romeu, Head of Data Science & Analytics in Cybersecurity, Isart Canyameres, Head of Innovation, and Quim Vila, Responsible for Prospectives and Trends, all of them from the Cybersecurity Agency of Catalonia, also took part in the white paper elaboration with their expert insights and contributions.

ciberseguretat.gencat.cat
Cybersecurity Agency of Catalonia
November 2023

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

Developed in cooperation with:

FACTUAL

Bibliography

[1] Smart Mobility Market Size, Share, Price, Demand, Forecast 2024-2032. (2023). Retrieved October 30, 2023, from https://www.expertmarketresearch.com/reports/smart-mobility-market

[2] C logistica. (2023). El transporte, el segundo sector más ciberatacado en España. https://logistica.cdecomunicacion.es/sector-logistico/132492/transporte-ciberatcado

[3] la Vanguardia. (2021). Los servicios de Barcelona Serveis Municipals, en jaque por un ataque informático. https://www.lavanguardia.com/local/20211019/7799950/ataque-informatico-afecta-servicios-barcelona-serveis-municipals.html

[4] ACN/Redacció. (2023). Un cibercrim cada tres hores a Catalunya: la feina de l'Agència de Ciberseguretat. https://www.ccma.cat/324/un-cibercrim-cada-tres-hores-a-catalunya-la-feina-de-lagencia-de-ciberseguretat/noticia/3218755/catalunya-la-feina-de-lagencia-de-ciberseguretat/noticia/3218755/

[5] Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Chen, Y. (2020). Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. Accident Analysis and Prevention, 148. https://doi.org/10.1016/j.aap.2020.105837

[6] Rathore, R. S., Hewage, C., Kaiwartya, O., & Lloret, J. (2022). In-Vehicle Communication Cyber Security: Challenges and Solutions. In Sensors (Vol. 22, Issue 17). MDPI. https://doi.org/10.3390/s22176679

[7] Kim, H., Han, J., Kim, S. H., Choi, J., Yoon, D., Jeon, M., Yang, E., Pham, N., Woo, S., Park, J., Kim, D., & Youn, C. H. (2017). IsV2C: An Integrated Road Traffic-Network-Cloud Simulator for V2C Connected Car Services. Proceedings - 2017 IEEE 14th International Conference on Services Computing, SCC 2017, 434–441. https://doi.org/10.1109/SCC.2017.62

[8] Demba, A., & Moller, D. P. F. (2018). Vehicle-to-Vehicle Communication Technology. IEEE International Conference on Electro Information Technology, 2018-May, 459–464. https://doi.org/10.1109/EIT.2018.8500189

[9] Indi Dhami. (2020). Top 5 Threat Vectors in Connected Cars and How to Combat Them | ISTARI. https://istari-global.com/insights/articles/top-5-threat-vectors-in-connected-cars/

[10] PTOLEMUS. (2020). Connected Vehicle Payments Global Study. www.ptolemus.com

[11] de Mattos, E. P., Domingues, A. C. S. A., Santos, B. P., Ramos, H. S., & Loureiro, A. A. F. (2022). The Impact of Mobility on Location Privacy: A Perspective on Smart Mobility. IEEE Systems Journal, 16(4), 5509–5520. https://doi.org/10.1109/JSYST.2022.3147808

[12] Olifirov, A., Makoveichuk, K. A., & Petrenko, S. (2021). Cybersecurity Measures of the Digital Payment Ecosystem. https://www.cbr.ru/Content/Document/File/119960/Consultation_Paper_02042021.pdf

[13] Barth, S., de Jong, M. D. T., & Junger, M. (2022). Lost in privacy? Online privacy from a cybersecurity expert perspective. Telematics and Informatics, 68. https://doi.org/10.1016/j.tele.2022.101782

[14] Rajyalakshmi, V., & Lakshmanna, K. (2022). A review on smart city – IoT and deep learning algorithms, challenges. In Int. J. Engineering Systems Modelling and Simulation (Vol. 13, Issue 1).

[15] Ten, C. W., Liu, C. C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. IEEE Transactions on Power Systems, 23(4), 1836–1846. https://doi.org/10.1109/TPWRS.2008.2002298

[16] Mecheva, T., & Kakanakov, N. (2020). Cybersecurity in intelligent transportation systems. In Computers (Vol. 9, Issue 4, pp. 1–12). MDPI AG. https://doi.org/10.3390/computers9040083

[17] Stasiuk, A.I., Hryshchuk, R.V. & Goncharova, L.L. A Mathematical Cybersecurity Model of a Computer Network for the Control of Power Supply of Traction Substations. Cybern Syst Anal 53, 476–484 (2017). https://doi.org/10.1007/s10559-017-9949-z

[18] NIS Cooperation Group. (2022). Report on the cybersecurity of Open RAN. https://www.redhat.com/en/topics/cloud-computing/cloud-vs-virtualization

[19] UITP. (2020). A win-win: How the Internet of Things is transforming public transport. https://www.uitp.org/news/a-win-win-how-the-internet-of-things-is-transforming-public-transport/

[20] Marianthi Theocharidou, Z. S. A. D. R. D. S. F. E. T. R. N. I. L. A. M. E. (2023). ENISA THREAT LANDSCAPE: TRANSPORT SECTOR. https://doi.org/10.2824/553997

[21] la Vanguardia. (2021). Los servicios de Barcelona Serveis Municipals, en jaque por un ataque informático. https://www.lavanguardia.com/local/20211019/7799950/ataque-informatico-afecta-servicios-barcelona-serveis-municipals.html

[22] Natàlia Vila. (2021). Tube tickets' new website reveals thousands of users' data. Ara. https://en.ara.cat/society/tube-tickets-new-website-reveals-thousands-of-users-data_1_4140183.html

[23] Silvia Montes. (2023). Oleada de ciberataques contra España de los hackers rusos NoName. Escudo Digital. https://www.escudodigital.com/ciberseguridad/oleada-ciberataques-espana-hackers-rusos-noname-afectan-incluso-casa-real_56076_102.html

[24] Menghan Xiao. (2023). BEC attacks surged 81% in 2022, 98% employees failed to report threat. SC Media. https://www.scmagazine.com/news/bec-attacks-surged-81-in-2022-98-employees-failed-to-report-threat

[25] INCIBE. (2023). ¿Has recibido un correo con una multa de la DGT, donde te tienes que descargar una factura? No caigas en la trampa de este phishing | Ciudadanía. https://www.incibe.es/ciudadania/avisos/has-recibido-un-correo-con-una-multa-de-la-dgt-donde-te-tienes-que

[26] Bleeping computer. (2021). Kia Motors America suffers ransomware attack, $20 million ransom. https://www.bleepingcomputer.com/news/security/kia-motors-america-suffers-ransomware-attack-20-million-ransom/

[27] Jessica Haworth. (2020). Spanish state railway company Adif hit by REvil ransomware attack. The Daily Swig. https://portswigger.net/daily-swig/spanish-state-railway-company-adif-hit-by-revil-ransomware-attack

[28] Javier Morales. (2023). Los hackers rusos bloquean las webs del metro y los autobuses de Granada por la cumbre. Ideal. https://www.ideal.es/granada/hackers-rusos-bloquean-webs-metro-autobuses-granada-20231006125201-nt.html

[29] Alberto Payo. (2023). Israel acusa a hackers iraníes de ataques contra sus empresas de logística y transporte. Escudodigital. https://www.escudodigital.com/ciberseguridad/israel-acusa-hackers-iranies-ataques-empresas-logistica-transporte_55473_102.html

[30] Jay Vijayan. (2018). Tesla Employee Steals, Sabotages Company Data. Dark Reading. https://www.darkreading.com/attacks-breaches/tesla-employee-steals-sabotages-company-data

[31] Reuters. (2023). Chinese hackers spying on US critical infrastructure, Western intelligence says. https://www.reuters.com/technology/microsoft-says-china-backed-hacker-targeted-critical-us-infrastructure-2023-05-24/

[32] Rolling Stock World. (2022). CRRC may face new US sanctions. https://rollingstockworld.com/economy/crrc-may-face-new-us-sanctions/

[33] Insurance Journal. (2022). Chinese Electric Automaker Nio Hit by Ransomware Attack. https://www.insurancejournal.com/news/international/2022/12/22/700516.htm

[34] Erin Marquis. (2022). Russian Company Outsourced EV Chargers To Ukraine, Hilarity Ensues. Jalopnik.

https://jalopnik.com/russian-company-outsourced-the-main-components-in-ev-ch-1848603252

[35] las Provincias. (2022). Un ciberataque afecta al sistema informatico de Vectalia. https://www.lasprovincias.es/alicante/ciberataque-afecta-sistema-20220630191246-nt.html

[36] Niewels, F., Knoop, S., Jordan, R., & Michalke, T. (2013). In-Vehicle Sensors. Encyclopedia of Automotive Engineering, 1–27. https://doi.org/10.1002/9781118354179.AUTO175

[37] Tu, Y., Lin, Z., Lee, I., & Hei, X. (2018). Injected and Delivered: Fabricating Implicit Control over Actuation Systems by Spoofing Inertial Sensors. 27th USENIX Security Symposium (USENIX Security 18), 1545–1562. https://www.usenix.org/conference/usenixsecurity18/presentation/tu

[38] Nashimoto, S., Suzuki, D., Sugawara, T., & Sakiyama, K. (2018). Sensor CON-Fusion: Defeating Kalman Filter in Signal Injection Attack. ACM Asia Conference on Computer and Communica-Tions Security, 18. https://doi.org/10.1145/3196494.3196506

[39] Moller, D., Jehle, I., & Haas, R. (2018). Challenges for Vehicular Cybersecurity. https://doi.org/10.1109/EIT.2018.8500208

[40] Nashimoto, S., Suzuki, D., Sugawara, T., & Sakiyama, K. (2018). Sensor CON-Fusion: Defeating Kalman Filter in Signal Injection Attack. ACM Asia Conference on Computer and Communica-Tions Security, 18. https://doi.org/10.1145/3196494.3196506

[41] Tu, Y., Lin, Z., Lee, I., & Hei, X. (2018). Injected and Delivered: Fabricating Implicit Control over Actuation Systems by Spoofing Inertial Sensors. 27th USENIX Security Symposium (USENIX Security 18), 1545–1562. https://www.usenix.org/conference/usenixsecurity18/presentation/tu

[42] Son, Y., Shin, H., Kim, D., Park, Y., Noh, J., Choi, K., Choi, J., & Kim, Y. (2015). Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors. In Proceedings of the 24th USENIX Security Symposium. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/son

[43] Trippel, T., Weisse, O., Xu, W., Honeyman, P., & Fu, K. (2017). WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks. https://doi.org/10.1109/EuroSP.2017.42

[44] Rouf, I., Miller, R., Mustafa, H., Taylor, T., Oh, S., Xu, W., Gruteser, M., Trappe, W., & Seskar, I. (2010). Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study.

[45] Shao, X., Dong, C., & Dong, L. (2019). Research on Detection and Evaluation Technology of Cybersecurity in Intelligent and Connected Vehicle. https://doi.org/10.1109/AIAM48774.2019.00087

[46] Kilcoyne, D. K., Bendelac, S., Ernst, J. M., & Michaels, A. J. (2016). Tire Pressure Monitoring System encryption to improve vehicular security. MILCOM 2016 - 2016 IEEE Military Communications Conference, 1219–1224. https://doi.org/10.1109/MILCOM.2016.7795497

[47] Kolodgie, A., Berges, P., Burrow, R., Carman, M., Collins, J., Bair, S., Moy, G. D., Ernst, J. M., & Michaels, A. J. (2017). Enhanced TPMS security through acceleration timed transmissions. MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM), 35–39. https://doi.org/10.1109/MILCOM.2017.8170841

[48] Amoozadeh, M., Raghuramu, A., Chuah, C. N., Ghosal, D., Michael Zhang, H., Rowe, J., & Levitt, K. (2015). Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. IEEE Communications Magazine, 53(6), 126–132. https://doi.org/10.1109/MCOM.2015.7120028

[49] He, Q., Meng, X., & Qu, R. (2017). A survey on cyber security of CAV. https://doi.org/10.1109/CPGPS.2017.8075153

[50] Edwards, J., Kashani, A., & Iyer, G. (2017). Evaluation of Software Vulnerabilities in Vehicle Electronic Control Units. https://doi.org/10.1109/SecDev.2017.26

[51] Eiza, M. H., & Ni, Q. (2017). Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity. IEEE Vehicular Technology Magazine, 12(2), 45–51. https://doi.org/10.1109/MVT.2017.2669348

[52] Checkoway, S., Mccoy, D., Anderson, D., Kantor, B., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., & Kohno, T. (2011). Comprehensive Experimental Analyses of Automotive Attack Surfaces.

[53] Shoukry, Y., Martin, P., Tabuada, P., & Srivastava, M. (2013). Non-invasive spoofing attacks for anti-lock braking systems. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8086 LNCS, 55–72. https://doi.org/10.1007/978-3-642-40349-1_4/COVER

[54] Shoukry, Y., Martin, P., Yona, Y., Diggavi, S., & Srivastava, M. (2016). Attack Resilience and Recovery using Physical Challenge Response Authentication for Active Sensors Under Integrity Attacks. https://doi.org/10.48550/arxiv.1605.02062

[55] Niewels, F., Knoop, S., Jordan, R., & Michalke, T. (2013). In-Vehicle Sensors. Encyclopedia of Automotive Engineering, 1–27. https://doi.org/10.1002/9781118354179.AUTO175

[56] Petit, J., Stottelaar, B., & Feiri, M. (2015). Remote Attacks on Automated Vehicles Sensors : Experiments on Camera and LiDAR.

[57] Yan, C. (2016). Can You Trust Autonomous Vehicles : Contactless Attacks against Sensors of Self-driving Vehicle.

[58] Rangesh, A., & Trivedi, M. (2018). No Blind Spots: Full-Surround Multi-Object Tracking for Autonomous Vehicles using Cameras & LiDARs. IEEE Transactions on Intelligent Vehicles, PP. https://doi.org/10.1109/TIV.2019.2938110

[59] Lopez, A., Malawade, A. v, Faruque, M. A. al, Boddupalli, S., & Ray, S. (2019). Security of Emergent Automotive Systems: A Tutorial Introduction and Perspectives on Practice. IEEE Design & Test, 36(6), 10–38. https://doi.org/10.1109/MDAT.2019.2944086

[60] Lu, G., Zeng, D., & Tang, B. (2010). Anti-jamming filtering for DRFM repeat jammer based on stretch processing. 2010 2nd International Conference on Signal Processing Systems, 1, V1-78-V1-82. https://doi.org/10.1109/ICSPS.2010.5555517

[61] Dutta, R. G., Yu, F., Zhang, T., Hu, Y., & Jin, Y. (2018). Security for Safety: A Path Toward Building Trusted Autonomous Vehicles. 2018 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 1–6. https://doi.org/10.1145/3240765.3243496

[62] Kapoor, P., Vora, A., & Kang, K.-D. (2018). Detecting and Mitigating Spoofing Attack Against an Automotive Radar. 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), 1–6. https://doi.org/10.1109/VTCFall.2018.8690734

[63] Xu, W., Yan, C., Jia, W., Ji, X., & Liu, J. (2018). Analyzing and Enhancing the Security of Ultrasonic Sensors for Autonomous Vehicles. IEEE Internet of Things Journal, PP, 1. https://doi.org/10.1109/JIOT.2018.2867917

[64] Lim, B., Keoh, S. L., & Thing, V. (2018). Autonomous vehicle ultrasonic sensor vulnerability and impact assessment. https://doi.org/10.1109/WF-IoT.2018.8355132

[65] Keen Security Lab, T. (2019). Experimental Security Research of Tesla Autopilot.

[66] Lee, S., Choi, W., & Lee, D. (2019). Securing Ultrasonic Sensors Against Signal Injection Attacks Based on a Mathematical Model. IEEE Access, 7, 1. https://doi.org/10.1109/ACCESS.2019.2932843

[67] Stottelaar, B. (2015). Practical cyber-attacks on autonomous vehicles.

[68] Shin, H., Kim, D., Kwon, Y., & Kim, Y. (2017). Illusion and Dazzle: Adversarial Optical Channel Exploits Against Lidars for Automotive Applications. https://doi.org/10.1007/978-3-319-66787-4_22

[69] Petit, J., Stottelaar, B., & Feiri, M. (2015). Remote Attacks on Automated Vehicles Sensors : Experiments on Camera and LiDAR.

[70] Shin, H., Kim, D., Kwon, Y., & Kim, Y. (2017). Illusion and Dazzle: Adversarial Optical Channel Exploits Against Lidars for Automotive Applications. https://doi.org/10.1007/978-3-319-66787-4_22

[71] Parkinson, S., Ward, P., Wilson, K., & Miller, J. (2017). Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. IEEE Transactions on Intelligent Transportation Systems, 18(11), 2898–2915. https://doi.org/10.1109/TITS.2017.2665968

[72] Harris, M. (2015). Researcher Hacks Self-driving Car Sensors.

[73] Cao, Y., Bhupathiraju, S. H., Naghavi, P., Sugawara, T., Mao, Z. M., & Rampazzi, S. (2022). You Can't See Me: Physical Removal Attacks on LiDAR-based Autonomous

Vehicles Driving Frameworks. http://arxiv.org/abs/2210.09482
[74] Matsumura, R., Sugawara, T., & Sakiyama, K. (2018). A Secure LiDAR with AES-Based Side-Channel Fingerprinting. 2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW), 479–482. https://doi.org/10.1109/CANDARW.2018.00092
[75] Petit, J., Stottelaar, B., & Feiri, M. (2015). Remote Attacks on Automated Vehicles Sensors : Experiments on Camera and LiDAR.
[76] Narain, S., Ranganathan, A., & Noubir, G. (2018). Security of GPS/INS based On-road Location Tracking Systems.
[77] Bittl, S., Gonzalez, A. A., Myrtus, M., Beckmann, H., Sailer, S., & Eissfeller, B. (2015). Emerging attacks on VANET security based on GPS Time Spoofing. 2015 IEEE Conference on Communications and Network Security (CNS), 344–352.
[78] Petit, J., & Shladover, S. E. (2015). Potential Cyberattacks on Automated Vehicles. IEEE Transactions on Intelligent Transportation Systems, 16(2), 546–556. https://doi.org/10.1109/TITS.2014.2342271
[79] Euronews. (2022). Gridlock as hackers order hundreds of taxis to same place in Moscow. https://www.euronews.com/my-europe/2022/09/02/gridlock-as-hackers-order-hundreds-of-taxis-to-same-place-in-moscow
[80] Jadoon, A., Wang, L., Li, T., & Zia, M. (2018). Lightweight Cryptographic Techniques for Automotive Cybersecurity. Wireless Communications and Mobile Computing, 2018, 1–15. https://doi.org/10.1155/2018/1640167
[81] Raja Mahmood, R., & Khan, A. (2007). A survey on detecting black hole attack in AODV-based mobile ad hoc networks. https://doi.org/10.1109/HONET.2007.4600258
[82] Khanafseh, S., Roshan, N., Langel, S., Chan, F.-C., Joerger, M., & Pervan, B. (2014). GPS spoofing detection using RAIM with INS coupling. https://doi.org/10.1109/PLANS.2014.6851498
[83] Ibrahim, O. A., Hussain, A. M., Oligeri, G., & Di Pietro, R. (2019). Key is in the air: Hacking remote keyless entry systems. Security and Safety Interplay of Intelligent Software Systems: ESORICS 2018 International Workshops, ISSA 2018 and CSITS 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers, 125–132.
[84] Moradi, A., & Kasper, T. (2009). A new remote keyless entry system resistant to power analysis attacks. 2009 7th International Conference on Information, Communications and Signal Processing (ICICS), 1–6. https://doi.org/10.1109/ICICS.2009.5397727
[85] Alrabady, A. I., & Mahmud, S. M. (2005). Analysis of Attacks Against the Security of Keyless-Entry Systems for Vehicles and Suggestions for Improved Designs. Vehicular Technology, IEEE Transactions On, 54, 41–50. https://doi.org/10.1109/TVT.2004.838829
[86] Glocker, T., Mantere, T., & Elmusrati, M. (2017). A protocol for a secure remote keyless entry system applicable in vehicles using symmetric-key cryptography. 2017 8th International Conference on Information and Communication Systems (ICICS), 310–315. https://doi.org/10.1109/IACS.2017.7921990
[87] Daily Mail. (2018). Amazon and eBay “helping criminals” buy devices to steal vehicles. https://www.dailymail.co.uk/news/article-5645063/Car-theft-kit-sale-Amazon.html
[88] Glocker, T., Mantere, T., & Elmusrati, M. (2017). A protocol for a secure remote keyless entry system applicable in vehicles using symmetric-key cryptography. 2017 8th International Conference on Information and Communication Systems (ICICS), 310–315. https://doi.org/10.1109/IACS.2017.7921990
[89] Choi, W., Jo, H. J., Woo, S., Chun, J. Y., Park, J., & Lee, D. H. (2018). Identifying ECUs Using Inimitable Characteristics of Signals in Controller Area Networks. IEEE Transactions on Vehicular Technology, 67(6), 4757–4770. https://doi.org/10.1109/TVT.2018.2810232
[90] Liu, J., Zhang, S., Sun, W., & Shi, Y. (2017). In-vehicle network attacks and countermeasures: Challenges and future directions. IEEE Network, 31(5), 50–58. https://doi.org/10.1109/MNET.2017.1600257
[91] Xie, G., Yang, L. T., Liu, Y., Luo, H., Peng, X., & Li, R. (2021). Security Enhancement for Real-Time Independent In-Vehicle CAN-FD Messages in Vehicular Networks. IEEE Transactions on Vehicular Technology, 70(6), 5244–5253. https://doi.org/10.1109/TVT.2021.3061746
[92] Nowdehi, N., Lautenbach, A., & Olovsson, T. (2017). In-Vehicle CAN Message Authentication: An Evaluation Based on Industrial Criteria. 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), 1–7. https://doi.org/10.1109/VTCFall.2017.8288327
[93] Mundhenk, P., Steinhorst, S., Lukasiewycz, M., Fahmy, S. A., & Chakraborty, S. (2015). Lightweight authentication for secure automotive networks. 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE), 285–288. https://doi.org/10.7873/DATE.2015.0174
[94] Kang, K.-D., Baek, Y., Lee, S., & Son, S. H. (2017). An Attack-Resilient Source Authentication Protocol in Controller Area Network. 2017 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS), 109–118. https://doi.org/10.1109/ANCS.2017.25
[95] Tashiro, A., Muraoka, H., Araki, S., Kakizaki, K., & Uehara, S. (2017). A secure protocol consisting of two different security-level message authentications over CAN. 2017 3rd IEEE International Conference on Computer and Communications (ICCC), 1520–1524. https://doi.org/10.1109/CompComm.2017.8322794
[96] Lee, H., Jeong, S. H., & Kim, H. K. (2017). OTIDS: A Novel Intrusion Detection System for In-vehicle Network by Using Remote Frame. 2017 15th Annual Conference on Privacy, Security and Trust (PST), 57–5709. https://doi.org/10.1109/PST.2017.00017
[97] Tomlinson, A., Bryans, J., Shaikh, S. A., & Kalutarage, H. K. (2018). Detection of Automotive CAN Cyber-Attacks by Identifying Packet Timing Anomalies in Time Windows. 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), 231–238. https://doi.org/10.1109/DSN-W.2018.00069
[98] Mousa, A. R., NourElDeen, P., Azer, M., & Allam, M. (2016). Lightweight Authentication Protocol Deployment over FlexRay. Proceedings of the 10th International Conference on Informatics and Systems, 233–239. https://doi.org/10.1145/2908446.2908485
[99] Gu, Z., Han, G., Zeng, H., & Zhao, Q. (2016). Security-Aware Mapping and Scheduling with Hardware Co-Processors for FlexRay-Based Distributed Embedded Systems. IEEE Transactions on Parallel and Distributed Systems, 27(10), 3044–3057. https://doi.org/10.1109/TPDS.2016.2520949
[100] Han, G., Zeng, H., Li, Y., & Dou, W. (2014). SAFE: Security-Aware FlexRay Scheduling Engine. 2014 Design, Automation & Test in Europe Conference & Exhibition (DATE), 1–4. https://doi.org/10.7873/DATE.2014.021
[101] Perrig, A., Canetti, R., Tygar, D., & Song, D. (n.d.). The TESLA Broadcast Authentication Protocol. 2002. Cryptobytes.
[102] Püllen, D., Anagnostopoulos, N. A., Arul, T., & Katzenbeisser, S. (2019). Security and Safety Co-Engineering of the FlexRay Bus in Vehicular Networks. Proceedings of the International Conference on Omni-Layer Intelligent Systems, 31–37. https://doi.org/10.1145/3312614.3312626
[103] Deng, J., Yu, L., Fu, Y., Hambolu, O., & Brooks, R. R. (2017). Chapter 6 - Security and Data Privacy of Modern Automobiles. In M. Chowdhury, A. Apon, & K. Dey (Eds.), Data Analytics for Intelligent Transportation Systems (pp. 131–163). Elsevier. https://doi.org/https://doi.org/10.1016/B978-0-12-809715-1.00006-7
[104] Takahashi, J., Aragane, Y., Miyazawa, T., Fuji, H., Yamashita, H., Hayakawa, K., Ukai, S., & Hayakawa, H. (2017). Automotive Attacks and Countermeasures on LIN-Bus. Journal of Information Processing, 25, 220–228. https://doi.org/10.2197/ipsjjip.25.220
[105] Wolf, M., Weimerskirch, A., & Paar, C. (2004). Security in Automotive Bus Systems.
[106] Mitnick, K. D., & Simon, W. L. (2009). The art of intrusion: the real stories behind the exploits of hackers, intruders and deceivers. John Wiley & Sons.
[107] Kiravuo, T., Sarela, M., & Manner, J. (2013). A Survey of Ethernet LAN Security. IEEE Communications Surveys & Tutorials, 15(3), 1477–1491. https://doi.org/10.1109/SURV.2012.121112.00190

[108] Convery, S., & Systems, C. (2002). Hacking Layer 2: Fun with Ethernet Switches. http://www.atstake.com
[109] Abad, C. L., & Bonilla, R. I. (2007). An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks. 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07), 60. https://doi.org/10.1109/ICDCSW.2007.19
[110] Marro, G. (2003). Attacks at the Data Link Layer.
[111] Norris, E. (2001). Global Information Assurance Certification Paper Analysis of a Telnet Session Hijack via Spoofe d MAC Addresses and Session Resynchronization. http://www.giac.org/registration/gsec
[112] Zheng, O., Poon, J., & Beznosov, K. (2009). Application-Based TCP Hijacking. Proceedings of the Second European Workshop on System Security, 9–15. https://doi.org/10.1145/1519144.1519146
[113] Lin, C.-W., & Yu, H. (2016). Invited - Cooperation or Competition? Coexistence of Safety and Security in next-Generation Ethernet-Based Automotive Networks. Proceedings of the 53rd Annual Design Automation Conference. https://doi.org/10.1145/2897937.2905006
[114] Meyer, P., Häckel, T., Korf, F., & Schmidt, T. C. (2019). DoS Protection through Credit Based Metering -- Simulation-Based Evaluation for Time-Sensitive Networking in Cars. http://arxiv.org/abs/1908.09646
[115] Pesé, M., Schmidt, K., Zweck, H., & Dannebaum, U. (2017). Hardware/Software Co-Design of an Automotive Embedded Firewall. https://doi.org/10.4271/2017-01-1659
[116] Insrance Journal. (2022). Chinese Electric Automaker Nio Hit by Ransomware Attack. https://www.insurancejournal.com/news/international/2022/12/22/700516.htm
[117] Beaman C, Barkworth A, Akande TD, Hakak S, Khan MK. Ransomware: Recent advances, analysis, challenges and future research directions. Comput Secur. 2021 Dec;111:102490. doi: 10.1016/j.cose.2021.102490. Epub 2021 Sep 24. PMID: 34602684; PMCID: PMC8463105.
[118] Benjamin Freed. (2020). Philadelphia transit system recovering from apparent cyberattack. StateScoop. https://statescoop.com/philadelphia-transit-system-recovering-from-apparent-cyberattack/
[119] Cadena SER. (2023). "¡No piques!": Renfe advierte de una nueva estafa mediante una falsa tarjeta de regalo. https://cadenaser.com/nacional/2023/08/09/no-piques-renfe-advierte-de-una-nueva-estafa-mediante-una-falsa-tarjeta-de-regalo-cadena-ser/
[120] IT Governance Blog. (2021). Scammers impersonate U.S. Department of Transportation in phishing attack. https://www.itgovernance.eu/blog/en/scammers-impersonate-u-s-department-of-transportation-in-phishing-attack
[121] Col·legi Oficial d'Enginyeria Informàtica de Catalunya COEINF. (2018). Detingut un exempleat d'Apple per vendre secrets. https://enginyeriainformatica.cat/detingut-un-exempleat-dapple-per-vendre-secrets/
[122] SecurityWeek. (2022). Cyberattack Causes Trains to Stop in Denmark. https://www.securityweek.com/cyberattack-causes-trains-stop-denmark/
[123] Mozilla Foundation. (2023). It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy. https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/
[124] Cui, C.; Du, H.; Jia, Z.; He, Y.; Yang, Y.; Jin, M. Data Poisoning Attack Using Hybrid Particle Swarm Optimization in Connected and Autonomous Vehicles. In Proceedings of the 2022 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), Gold Coast, Australia, 18–20 December 2022; pp. 1–5. [Google Scholar] [CrossRef]
[125] El Confidencial. (2023). El "gravísimo" ciberataque a Air Europa que ha dejado al aire tu tarjeta: ¿cómo ha ocurrido? https://www.elconfidencial.com/tecnolgia/2023-10-11/aireuropa-hackeo-ciberataque-tarjetas-cvv_3751849/
[126] Sandia Energy. (2022). Sandia studies vulnerabilities of electric vehicle charging infrastructure. https://energy.sandia.gov/sandia-studies-vulnerabilities-of-electric-vehicle-charging-infrastructure/
[127] Johnson, J., Berg, T., Anderson, B., & Wright, B. (2022). Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses. Energies, 15(11). https://doi.org/10.3390/EN15113931
[128] NIS Cooperation Group. (2022). Report on the cybersecurity of Open RAN. https://www.redhat.com/en/topics/cloud-computing/cloud-vs-virtualization
[129] Cyber Management Alliance. (2022). IoT Security: 5 cyber-attacks caused by IoT security vulnerabilities. https://www.cm-alliance.com/cybersecurity-blog/iot-security-5-cyber-attacks-caused-by-iot-security-vulnerabilities
[130] The Hacker News. (2023). Smart Mobility has a Blindspot When it Comes to API Security. https://thehackernews.com/2023/03/smart-mobility-has-blindspot-when-it.html
[131] Mason, J., & Oliveira, G. (2016). People Near Transit: Improving Accessibility and Rapid Transit Coverage in Large Cities.
[132] Juniper Research. (2022). World's No 1 Smart City for 2022: Shanghai. https://www.juniperresearch.com/press/worlds-no-1-smart-city-for-2022-shanghai
[133] Acció. (2023). The automotive sector in Catalonia.
[134] Catalonia Trade & Investement. (2023). Connected Vehicle in Catalonia. https://catalonia.com/key-industries-technologies/technologies/connected-vehicle-in-catalonia
[135] Agència de Ciberseguretat de Catalunya. (2023). Creixen un 15% les empreses catalanes dedicades a la ciberseguretat. https://ciberseguretat.gencat.cat/ca/detalls/noticia/Creixen-un-15-les-empreses-catalanes-dedicades-a-la-ciberseguretat
[136] ECSO. (2022). Market Radar. https://ecs-org.eu/activities/market-radar/
[137] Acció. (2023). Cybersecurity in Catalonia 2023.
[138] ISACS EU. (2022). EMPOWERING EU ISACS OVERVIEW AND REPORT ON EU ISAC INITIATIVES.
[139] European Commission. (2023). Tecnologías clave para impulsar la digitalización del transporte. https://digital-strategy.ec.europa.eu/es/policies/technologi
[140] BOE-A-2021-1192 Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. (2021). https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-1192
[141] Zabala Innovation. (2023). Cybersecurity in Europe is a strategic priority for the coming years. https://www.zabala.eu/opinions/cybersecurity-in-europe/
[142] Conectividad digital, ciberseguridad, 5G | Plan de Recuperación, Transformación y Resiliencia Gobierno de España. (2023). Retrieved November 3, 2023, from https://planderecuperacion.gob.es/politicas-y-componentes/componente-15-conectividad-digital-impulso-de-la-ciberseguridad-y