ECSO Transportation Sector Report, Cyber security for road, rail, air, and sea. WG3 I Sectoral Demand

Nina Hasratyan, Nina Olesen, Adrien Becue, Ulrich Seldeslachts, Sadio Bâ, Andrea Chiappetta, Andrei Costin, Janine Dobelmann, Christopher Henny, Pouria Sayyad Khodashenas, et al.

TRANSPORTATION SECTOR REPORT

Cyber security for road, rail, air, and sea

WG3 I Sectoral Demand

MARCH 2020

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use wg3_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

The use of the information contained in this document is at your own risk, and no relationship is created between ECSO and any person accessing or otherwise using the document or any part of it. ECSO is not liable for actions of any nature arising from any use of the document or part of it. Neither ECSO nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

This document will be continuously updated based on developments within the sector and ECSO members' input.

Copyright Notice

TABLE OF CONTENTS

Introduction

1.1 Foreword by the SWG Chairs

Cybersecurity is a complex and wide societal challenge that impacts all aspects of our current and future lives. Decades ago, cybersecurity only had limited implications for those working on personal computers that got infected with a virus. With the omnipresence of data connectivity and information and communication systems supporting almost every activity of our day to day lives, cybersecurity is a challenge for every sector and organisation and person operating in it. Cybersecurity is not limited to the dangers presented by hackers and scriptkiddies. Nation states and industrial competition, but equally so simple configuration mistakes and errors, can cause a massive effect with sometimes a direct loss of damage, sometimes collateral damage.

As we enter the second decade of the 21st century, it is becoming much clearer that the way the transport industry operates will change dramatically. Considerations of the ecological footprint, human working conditions and improved work-life balance, the sharing economy, autonomous vehicles and decision-making, ubiquitous and omnipresent connectivity and smart industrial components using sensoring technologies, capturing data and providing continuous analytical insights capable of predicting, as well as preventative measures are only some of the ongoing technological developments which are impacting the underlying transport sector. The sector itself is not particularly organised as such, but it represents a number of organisations from domains such as seaports and harbours, maritime, shipping and containers, airports, air carriers and controlling organisations, public and private authorities, railways, rail operators and infrastructure providers, road transportation, manufacturers of automotive, airplanes, rail and shipping. While the sector itself includes both public and private transport, both cargo and passenger transport, and interacts heavily with many other sectors such as logistics, wholesale – retail, security and industry, in this exercise of a “Cybersecurity for Transportation Sector Report” within ECSO we’ve tried to take a holistic approach focusing on the implications of cybersecurity on the transport sector as a whole. On the basis of various discussions and other reports and findings, we’ve tried to present this perspective in this underlying document.

In the end, the most important achievement of this report is the fact that it exists, that an effort has been undertaken in bringing various developments and thoughts together. The report collects several insights of cybersecurity on the transport sector, once more underlying the importance of the considerations and attention that need to be paid to it. The report is not intended to be exhaustive, but at least capable of bringing a holistic perspective of the domain of transport as a vertical sector both from the transport world itself and from the cybersecurity perspective. The report should serve as a baseline for further discussion and as a statement to indicate why and where improvements are needed. What we assumed early on is that the transport sector is still lacking significant cybersecurity maturity, at a moment where the sector is indicated as of strategic and national importance by the Critical Infrastructure Protection regulations and the Network and Information Security (NIS) Directive - implemented into Member States laws). With this report, the intention is also to indicate that expertise and solutions exist to further improve the level of maturity, to protect national and European interests, identify some clear and present dangers from existing gaps and experiences from other sectors, and provide some policy recommendations coming from industry concerns where self-regulation finds its limitations.

As chairs, we would like to express our gratitude to the ECSO Secretariat in producing this report, organising the various debates and sessions that have led to these insights, to the different organisations that have taken the time and effort to contribute to a better understanding of their specific industry, providing insights from experiences and best practices, participating in the discussions on getting to a better joint approach and discovering new insights on the basis of challenges not seen before, and to the European Commission and its respective agencies and DG's for their support and insights from their works and cooperation, and their efforts on making the European community cybersecure in a proactive and supporting manner.

The Chairs of the ECSO Transportation Sector SWG3.3, February 2020

Adrien Becue, Airbus Cybersecurity

Ulrich Seldeslachts, LSEC – Leaders In Security

1.2 Introduction on the report

This report is in direct continuity of several other reports that are more focused on sub-sector specificities. As such, it is worth mentioning the following:

- *Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations*, ENISA, January 2016 [1]
- *Securing Smart Airports*, ENISA, December 2016 [2]
- *Cyber Security and Resilience of smart cars*, ENISA, January 2017 [3]
- *CYRail Recommendations on cybersecurity of rail signalling and communications systems*, Shift2Rail, September 2018 [4]
- *The Guidelines on Cyber Security Onboard Ships*, BIMCO & al., December 2018 [5]
- *Aviation Cybersecurity Strategy*, ICAO, October 2019 [6]
- *Port Cybersecurity - Good practices for cybersecurity in the maritime sector*, ENISA, November 2019 [7]

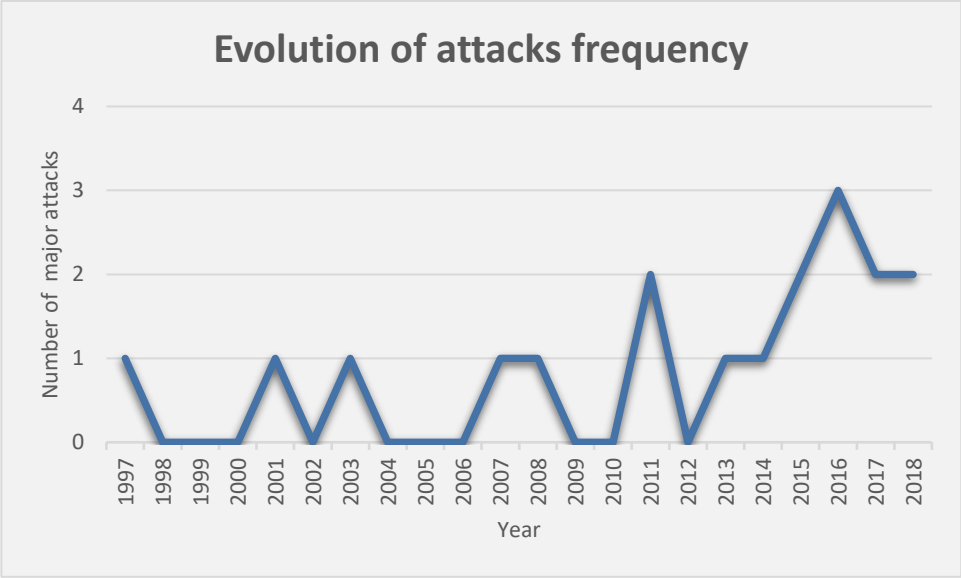
It is also worth noting that the European Commission's DG MOVE has organised a series of three workshops in Autumn 2019 respectively focusing on the maritime, rail and aviation sectors. The purpose of these workshops was to discuss with Member States representatives, as well as the industry and associations, the practicalities of the implementation of the NIS Directive and future developments in each sector.

Cybersecurity is a real challenge on many levels for the transportation sector and its sub-sectors (air, maritime, ports, road…). While some aspects remain sub-sector specific, thereby making cybersecurity issues difficult to address, this report aims to understand the landscape and come up with a horizontal and holistic understanding of the cybersecurity needs and requirements of transportation.

Most Noteworthy Cyberattacks in the Sector

The tables below provide a short overview of the most "noteworthy" known cyberattacks that have affected the transport sector at a global level, providing also a description of the attack methodology applied and the damages caused. In some cases, the resulting effects were a starting point that could have jeopardised the entire supply chain of companies, cities, Member States and the EU as a whole. It shows the need for a clear process able to guarantee that cybersecurity is playing and will play a fundamental role to "categories" if a company or even a nation is competitive and can provide a secure market. This is the challenge that Europe needs to face and a continuous battle it must overcome.

Based on the listed attacks, the chart here shows a clear growth of (known and reported) cyberattacks over the last years. Most of the incidents that have taken place have not been reported. In most countries there hasn't been any obligation, nor incentive, to report on cybersecurity. Recent regulatory changes (NIS Directive and sector specific regulations) will likely provide more insights on both attacks and other incidents taking place.



BEFORE 2000				
Year	**Target**	**Type**	**Methodology**	**Damage done**
1997	Worcester Airport	Phishing	The hacker managed to disable a key telephone company computer servicing at the Worcester Airport. In doing this, he sent a series of commands from his personal	He disabled the key services at the FAA control tower and crippled the airport for a total of six hours. In the course of the attack, services at the airport stood

			computer and disabled key services at the FAA control tower, spanning six hours long.	still and did not move, leading to massive losses and confusion.

BETWEEN 2000 – 2005				
Year	**Target**	**Type**	**Methodology**	**Damage done**
2001	Port of Houston	Denial of service attack	A teenager from Britain is said to have brought to knees all internet systems and services of a major port in the US, in an attempt to revenge on a fellow user of IRC. In doing that, he directed an attack to a fellow user in the chatroom, with the attack managing to slow down the systems at the port through a DoS. He took out the network connection of the fellow chat room user through a device he had created, only to disable the entire system at the port.	The system was running alongside other server systems, and the PING flood attack affected all the systems, but the most affected was the port system that could not work because of slowed operations. The attack made it impossible to access data (on weather, tides and water depths) at the port. Even though no physical injuries or damages were created, the actions still led to electronic sabotage.
2003	CSX US Railway	DoS	The hackers gained access into the system and disrupted the operations for some time. The system was accessed through three IP addresses, probably from another country. The company attacked was not named, neither was the country of the attackers.	System operations were derailed for quite some time before they were normalized, the attack disrupted traffic in 23 states in the eastern half of US. During the attack, trains were halted due to dark signals and delays throughout the day ranged from 15 minutes to 6 hours.

BETWEEN 2006 – 2010				
Year	**Target**	**Type**	**Methodology**	**Damage done**
2007	L.A. Traffic engineers' Strike	Hacking	The two engineers went on strike and were locked out of accessing the traffic lights control systems. However, they hacked themselves in and changed the settings back to what they were before and could easily access them.	Only system settings were changed, and it took four days to have them back to normal and operating well. No accidents were reported at the time.

			They said that their motive was protecting the system from any form of attacks.	
2008	Lodz Trams Poland	Hacking	A polish teenager is said to have derailed a tram after he attacked a train network. In doing this, he turned the tram system in the Lodz city into his personal train set, which brought about chaos and derailing a total of four vehicles in the process. He modified a TV remote control in that it could be used in changing track points. He managed to trespass the depots of the tram and collect information required to create the device. He said that he had done it only to create a prank.	Four vehicles were derailed, and a total of twelve people were injured in the process.

BETWEEN 2011 – 2015				
Year	**Target**	**Type**	**Methodology**	**Damage done**
2011	Pacific Northwest, USA	DoS	An unidentified railway company was hacked into, disrupting all its railway signals for a period of two days, December 2011. The Railway located in the Northwest of Pacific was slowed down and could not perform its operations normally.	System shutdown for two days, meaning that the operations were shut down at the railway company for two days.
2011 & 2013	Port of Antwerp	Hacking (use of Trojan horses) and phishing	A group of drug traffickers hired hackers to breach the IT security systems that controlled the location and movement of containers. The hackers began by emailing malicious software to the port's staff. They were thus able to gain access to the data through remote access, which they applied in identifying and intercepting the containers carrying drugs and cleared them. After being discovered,	Physical damage, port's physical computing equipment were taken away. At the same time, the systems were compromised, and it took time to normalise operations by neutralising the Trojan Hose used in the attack.

			the attackers physically came and broke into the port's offices and made away with the computing materials used by staff including computers, keyboards and all other materials.	
2014	Tesla Hijacking competition	Hacking	A group of Chinese researchers managed to interfere with a Tesla car by taking remote control of the Model S from a distance of 12 miles. They hacked into and interfered with the car's door locks, brakes as well as other electronic features, showing an attack that could possibly lead to hijacking and compromised Tesla cars.	The car's systems were totally interfered with. However, there were no major damages as this was for testing purposes.
2015	Sweden Airports	DoS	A DoS attack was carried out on Swedish airports in the year 2015, raising alarm to NATO and other stakeholders to come in. The attack is said to be linked to a group of Russian intelligence individuals and the system's services were totally crippled.	The systems of the airports were crippled for some time before they could be normalised.
2015	Port of LA	Ransomware attack	Maersk confirmed that a Ransomware attack had hit their services and they could not operate in all their outlets around the world. The attack meant that the LA port could not work, and it was shut down for a whole day.	Operations were stopped at the APM terminal leading to imminent closure of the port.
2015	Fiat Chrysler	Controlled experiment	Cybersecurity researchers hacked a Jeep while it was driving on a highway, gaining control over its windshield wipers, infotainment system, air-conditioning, and brakes. The car's infotainment system had a zero-day exploit which at the time had no fix.	The result of the experiment prompted Fiat Chrysler to patch over 1.4 million cars with an update to prevent this weakness from being exploited again.
2015	LOT Airlines	Sabotage	DDoS attack against the airline's flight-plan systems	Until LOT airplanes could receive valid flight plans, they

			disrupted its ability to issue flight plans.	were not be allowed to depart.

SINCE 2016				
Year	**Target**	**Type**	**Methodology**	**Damage done**
2016	Uber	Ransomware	Hackers gained access into Uber systems and obtained data of 57 million users worldwide, among those being customers and drivers. However, the attack was concealed by Uber when they paid $100,000 to the hackers and told them to delete the data and not make the breach public.	User data was obtained illegally, and Uber lost $100,000 as ransom to the users.
2016	Port of Rotterdam	Ransomware	A ransomware attack was initiated on the system and the virus crippled several businesses around the world. The businesses included Maersk and APM.	Many businesses were affected by the attack, bringing down their operations and services that depended on the affected system.
2016	US Rail	Ransomware	The attackers locked the San Francisco Municipal Transport Agency computers and demanded to be compensated with 100 bitcoins as payment to have the services back to normal. The municipal transport agency was forced to offer free rides to passengers because they could not access their systems to book the passengers and keep data. A malware called HDDCryptor was used in infecting a total of 2,112 computers and encrypted all the data.	A total of 2,112 computers were crippled and could not work. Customers were given free rides, making the agency lose a lot of revenue in the process.
2017	A.P. Møller-Maersk	Ransomware	Ransomware (NotPetya) impacted operations at Maersk terminals in four different countries, causing delays and disruption that lasted weeks. The system terminal was shut down by the attack.	The port's operations were totally crippled and could not be done normally. The system's terminal was also shut down. According to Maersk, the total cost for dealing with the outbreak

				is expected to be in the $200 to $300 million range.
2017	Deutsche Bahn	DDoS	The attackers spammed users with emails that they were tricked to open and give them access to the system. They used a ransomware called WannaCry, which later encrypted the computers and their data demanding fees of $300 and $600 to have the services reinstated back to normal.	A total of 57,000 computers were affected and could not be accessed, with the hackers only promising to reinstate them back if they paid.
2018	Danish State Rail Operator DSB	DoS	The DoS attack paralysed several operations including the communication infrastructure and ticketing system. The attackers also took offline control of telephone infrastructure and mail system. The attack was meant to destroy the entire system and bring it down to its knees but managed to slow their operations for some time before everything was normalised.	The ticketing systems were totally affected and could not work. The communication infrastructure was also damaged, and no communication could be done.
2018	Bristol Airport	Ransomware	The Ransomware attack targeted the administrative system of the airport. While the flights were not disrupted, the administrative system and screen display took more than 4 days to go back to full capacity.	A number of applications were taken offline as a precaution measure including the flight information screens.
2019	Airbus	Industrial espionage	Cyber-attack aimed at getting access to documents related to certification of airplanes. These were sensitive documents detailing many of the European giant's industrial secrets	Investigators said the attack was allegedly carried out in a manner that first targeted a contractor to reach the Airbus network. In addition, employees are suspected of having been accomplices of the hackers.
2019	Dublin Tram System	Ransomware	Attackers threatened to publish private data from the Dublin Tram System website	While a small ransom, it says a lot about possible future trends in extortion.

			unless a ransom of a single bitcoin was paid.	

Landscape

2.1 Road

The transportation sector evolves at a fast pace, with variations depending on the sub-sector. The **road sub-sector**, which includes automotive, autonomous and connected vehicles, is rapidly evolving, while others such as rail and air are encountering some sector-related challenges that prevent them from developing in a fast-paced digitalised environment.

Today, we are heading more and more towards **interconnected and autonomous vehicles** in transportation. Road vehicles, for example, are transforming from a simple mode of transport to a mobile information hub. V2X communications, telematics, in-vehicle networking as well as wireless technologies for vehicle access, Near Field Communication (NFC) and multi-standard digital broadcast reception are now integrated in road vehicles.

At the same time, mobility is becoming “greener” with the emergence of Electric Vehicles (EV). Vehicles need to be charged quickly, safely, and cost- efficiently, and at the same time to avoid overloading the electrical network. It is projected that by 2025 the number of EVs would reach €190 Million representing approximately a power of 1,330 GW. This would equate to the power yielded by nearly 2,200 large power plants. While the rise in adoption of EVs is gaining momentum, the consequences of the misuse of the infrastructure on the national and European energy sustainability can be damaging.

Modern vehicles are gradually turning into ‘green smartphones-on-wheels’, which continuously collect, process, exchange and store large amounts of data. But this connectivity also makes the car vulnerable to hackers who attack the vehicle by seeking and exploiting weaknesses in its systems or networks. In fact, several studies [9] have already warned some years ago that hacking into a car is possible, and more recently hackers have effectively demonstrated that they could gain remote control over vehicles [10].

To existing and recurrent problems such as network optimisation and security, we can now add the extreme reliance on IT technology. When it comes to autonomous vehicles, the biggest issues are both security and safety, and we need to make safety secure by distinguishing and compartmentalising the needs and requirements. In addition, unauthorised access and control of the electric vehicle supply equipment (EVSE) stations and firmware modifications should be prevented.

To avoid cyber-attacks and create trust and public acceptance, the ‘connected vehicle’ must be secured. Correct functioning of all in-vehicle systems, as well as user privacy, must be ensured. This implies a paradigm shift in the design of in-vehicle electronics. Traditionally, there has been a strong focus on *safety*, meaning that for example the brakes should function correctly under all circumstances. **Safety** will remain equally important in the future, but the increasing amount of electronics and software in vehicles will additionally require *security* to protect the vehicle against hackers. In other words, cybersecurity has become an essential element of safety, as security breaches via the interface of the vehicle are now possible. In this case, **a first suggestion** would be to design and standardise open and **generic cyber safe interfaces for vehicle evolution**. Especially since most future vehicles will be equipped with or connected to personal assistant-like

systems for voice command. This would require the safety and security of the interface between the assistant and the vehicle. In this case, encryption systems need to be designed and integrated, such as homomorphic encryption, enabling end-to-end safety of data exchange when connecting the vehicle to the cloud.

A **second suggestion** would be to **assess the system security by third parties** and use certified products, calling at the same time for an EU cybersecurity label to be recognised as "coming from a secure supply chain". Also, continuous management of the cybersecurity situation (benchmarking, monitoring…) will enhance awareness of potential breaches coming. In this sense, centralised or **edged Security Operating Centres (SOCs)** would be strongholds to protect the flow of vehicles and people from continuous attacks incoming from the cyberspace. So, vehicle-makers are encouraged to design "cyber-agile" systems, i.e. systems that can dynamically change their signature for higher side-channel attacks robustness. For the moment, open interfaces (ODB) exist for car safety audit but they are insecure as no authentication is applied.

Next, it is important to secure the automotive embedded systems, or more generally, automotive Electric/Electronic (E/E) systems. It connects and controls complex electronic systems with many functions and components in a vehicle. An automotive E/E system consists of several subsystems divided into powertrain, chassis, comfort, infotainment, and telematics domain, communicated among each other via gateways. With recent innovations in the automotive industry for connectivity, autonomous driving, and electrification, the E/E systems are no longer isolated from the outside world. The connectivity provides huge benefits, but also violates the design principles for non-remote connectivity to the vehicle bus system (e.g. CAN bus), which were true for decades. Consequently, modern cars expose a large attack surface due to many remote and local entry points such as cellular, Bluetooth, Wi-Fi, 802.11p, OBDII, Infotainment media, ZigBee radio, and third-party apps. Furthermore, automotive systems are designed, implemented and integrated in a distributed development model, involving a multitude of suppliers in the supply chain, which increases the likelihood of hidden vulnerabilities and security flaws in the deployed systems. Intrusion detection and the complementary prevention systems add another layer of defence against cyberattacks, covering the whole system from backend to the frontend. As a matter of fact, CAN-based automotive systems communicate thousands of signals (i.e. individual data packets contained within the CAN frame data field). Thus, one challenge is to correctly and timely detect attacks within the vehicle with limited on-board resources while avoiding negative impacts on critical functions and road safety. The anti-hacking device is a physical controller that is integrated into the car and acts as an attack detection device. It is connected to the busses in the car carrying the sensor data. It passively monitors the bus traffic (e.g. CAN bus frames) and extracts the raw sensor data.

In addition to the safety and security challenges, there are also **conflicting requirements** between **data privacy and regulatory constraints**, and the problem of acceptability of solutions. In many sectors, authentication of users works with shared identity group 1. In some countries, rules and regulations do not allow the authentication and identification of some workers and actors on the value chain. In general, there are not state of the art authentication techniques, not even rudimentary ones. It would be advisable to look into the possibilities of communication in work-side units. In the context of smart road transportation, the road vehicle may no longer be considered a standalone system but should be designed more with a system of system view (in connection with road infrastructure and other vehicles).

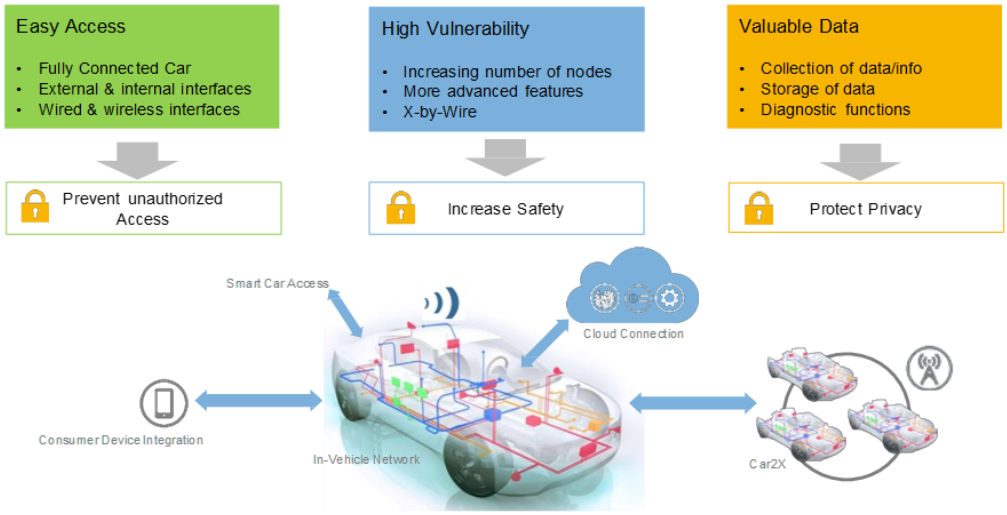
In 2015, the European Commission estimated that 135,000 people had been seriously injured on EU roads. The social cost (rehabilitation, healthcare, material damages, etc.) of road fatalities and

injuries was estimated to be of at least €100 billion per year. [11] Thus, the electronic functions mentioned above can bring beside the **important safety aspect** also **significant benefits** to the user, like e.g. increasing comfort, convenience and efficiency.

Comfort is increased because e.g. in summertime air conditioning systems to cool the cabin can be enabled remotely (shortly before driving home). Convenience can be increased because, for example, in-car entertainment systems are seamlessly synchronised with a phone and via the phone to the media connection at home. Last but certainly not least, the introduction of system intelligence, sensors and connectivity between cars and road-side units or back-end systems helps to increase safety and efficiency, for example by using information from nearby vehicles to prevent collisions, or by using information provided by road infrastructure or the cloud to reduce the travel time.

But these features **require collaboration between autonomous and non-autonomous things**, and more importantly a collaboration between autonomous things and humans. This brings into a new perspective accountability and verifiability aspects, as the liability relies in the non-deterministic behaviour. Currently in-function designed systems are thought safe against unintentional threats only. The **vehicle to machine, vehicle to vehicle and vehicle to human collaboration and communication remain very dependent on the access to data for inspection and enforcement purposes**, or to validate the assessment made by on-board units by understanding if something and what has been tampered with. This is valid both for critical infrastructure and the vehicle itself.

Lastly, the vehicles have **redundant** backing systems. Currently, a **standard (ISO-SAE 21434)** is under preparation that will create the **state-of-the-art minimum requirements of road vehicles** cybersecurity engineering.



Source: NXP Semiconductors

All these reasons make **certification difficult**, even more so when it comes to the barely breached topic of Artificial Intelligence (AI) where the traceability and explanation of received results remain an issue. In today's world, there is a greater volume of cars than of any other vehicle, which brings out these challenges of scalability and traceability. For the record, pre-existing traceability and security

measures already exist, such as the tachometer for example, but with the ongoing digitisation, there is the risk of clandestine use and traffic. Both challenges are linked to data collection, both from external sources and the inter-system communication.

Within the system itself, the communication can be differentiated. Data can be encrypted allowing for pseudonymisation up to anonymisation, given the correct implementation of it. Data generated within the system can only be about the internal management and functioning of the system. This does not raise the issue of the privacy, merely the behavioural patterns. Such is the case when it comes to the ownership of the car, where it is not the private data of the owner of the car that is at stake, but their behaviour as a driver. But this behaviour, in a specific country and specific location patterns, could be recognised and might lead back to the original driver. Human behaviour can easily be identified to its original source. However, encryption and pseudonymisation could be a solution to the reporting issue as companies are in general reluctant to report, in particular because of image and commercial sensitivities. For the data anonymisation to work within an organisation, it needs to work with all members to collect information based on trust-building.

A specificity of the road-sector is the use of **open data and applications of mobility services in transport**, which is used for all types of services, so the service providers need to fully trust the type of information they get. This helps them to integrate the loss in the cost percentage of the product instead of looking for insurance solutions. As a direct consequence, the cybersecurity environment needs to be firmly established, but above all, the trust is built by auto-assessment among the users of the systems to give their validation, thus communicating it to the central system. This in turn, raises the issue of which authority to report to and what type of data that should particularly be flagged. Raising awareness among the people involved in the sector is paramount.

On the other hand, the **inter-system communication involves more private information** for the need of understanding the threats we can have on external communication and the ones on the system itself. Linking the data to the ownership of a car can come in handy for tracking purposes, for example when an anonymous person other than the owner uses the car. This is where the segregation between operational and private data becomes tricky. To go even further, private data results can also be blurred with the new concept of car-sharing, where the driver can change constantly. This is also applied to the cargo transports, where the number of criminal incidents is increasing. As an example, there would be no way to check whether the driver of the cargo is the right person if a hacker has taken over the company computer to change the identity of the driver. Here again, reporting is extremely important because with a bigger amount of reports, it gets easier to cross-check the information.

These considerations show that today we can extract a big volume of data, more and more quickly, from different types of devices, and of communicating it to the network through the 5G. By saving the data, we are able to improve the device management, going more and more into predictive management which in some cases can also help detect threats. However, the reliance on 5G raises the major challenge of real-time communications, where most protocols are not cybersecurity secured (e.g. privacy, etc.).

Moreover, with regards to positioning data, the security aspects of authenticity and integrity of externally provided data are vital. Currently, vehicles rely on GPS and Galileo which makes them vulnerable to spoofed data. For example, an automated vehicle will drive anywhere indicated on the GPS, which raises heavy consequences on the data reliance. Additionally, when it comes to relying on external

communications, complementary security is required from stakeholders that are not necessarily part of the transportation ecosystem, mostly in terms of the resilience of the systems.

For example, Galileo, to date is considered as safe, but once finally fully available, might already be obsolete and not fit for the security requirements of future times. Furthermore, greater road safety can be achieved with state-of-the-art **traffic optimisation** algorithms and the extension to green wave practices for security interventions which would require **secure V2X** protocols.

The balance between evolution and resilience is also to be applied to other considerations such as regulation and certification. Contrary to the rail and air sectors, the concept of **imperfect redundancy** can be applied. The balance between integration and cost constraints leads to the reliance on a redundant backing system. For example, for the moment, mechanical gearing and breaking principles apply, but this may soon no longer be the case. In any case, the keeping of the manual mode remains mandatory, thus keeping a human in the loop.

Finally, a legal gap remains with regards to car data ownership and who should be entitled to collect, store and exploit the information in a given circumstance.

2.2 Rail

Historically, the railway sector has **been relatively isolated** from external influence, which has made it immune to security threats and attacks. This approach is **now outdated** due to the digitalisation of most systems, the use of wireless systems, the interconnectedness of the overall railway system, and the sharp rise of cyber threats and attacks on the transportation sector.

Initially, there were only the problems of **interoperability and safety**, to which are now added the emerging problems linked to cybersecurity. This mostly means that there is the need to keep the systems safe and secure **both in online and offline modes**. In practice, the vehicle could drive in connected mode but still have issues in the systems both in connected and disconnected modes, which can become critical.

The main cybersecurity aspects that impact the railway sector are related to its **physical components, its attached software, network and the certification** applied to it.

The cybersecurity of the **network** is one of the main aspects to consider. Aside from the consumer data privacy and confidentiality issue, **geo-localisation** must also be considered from the point of view of real-time communications. Real-time communications imply the use of satellites, yet, one source of positioning is not sufficient. At all times, experts need to make a correlation between different factors and received data, such as the GSM, the speed, the gyroscope, the accelerometer, etc. To this effect, it is interesting to mention that the European Rail Traffic Management System (**ERTMS**) [12], an industrial project developed by several UNIFE (Association of the European Rail Industry) [13] members to replace the national automatic train protections (ATP) by a **European ATP**, is based on GSM-R. The railway sector can never trust the direct information given by the network, even if the network is very good. Instead, they **check the time lapses in the information flux, cross-checking it with the maximum time lapse of information within the system to be sure to have timely information data**. Therefore, a maximum of resilience is required, because even in usual behaviour, there could be

some undetectable time lapses in the cyber network, which in themselves can cause damage and become a vector of attack. Trusting the network is bound to bring a surface attack at some point or another. Currently, there are **some experiments** being carried out at the ERTMS on the **remote control of trains** using private Long Term Evolution (**LTE**) network based on **4G**.

The cyber physical protection of electronic components scattered along the tracks and on the train should also be considered. The **distributed aspect of components** raises the access protection issue. In addition, the legacy management issue shows the discrepancy between the very long lifecycle of the physical components (more than 25 years and up to 50 years) and the **frequently needed software updates**. Finally, the **design of railway specific components is a long process**, and **if security by design is applied, the lifecycle will be even longer if there is no common reference.**

More closely linked to the physical components is the fact that the **railway network is heterogenous**, which raises the integration issue. The railway sector is divided by **zones** with each zone having its own railway specific product and its own security requirements. There is the aim to have different protection profiles for different systems, but it remains a big and largely scoped work, and to apply it on a case by case basis is very difficult. Given the longevity of the physical components, these profile protections cannot be done on a project by project basis either. To bypass this issue, several steps are taken: make assumptions on the **peripheral protection**, make security requirements that are allocated to the operational system (e.g. HMI, securitisation of the link to the identification and authentication server, etc.) and try to reduce the components in order to maximise the security. However, this **zoning by isolation system remains old school** (plain physical protection) and given the interconnectedness of the devices, is viable for barely another 5-6 years according to Shift2Rail.

The **lifecycle** between software and hardware is a key point of the qualification management. In the railway sector, it is impossible to retro-engineer systems. In vulnerability management, Commercial-Off-The-Shelf (COTS) products are still considered as the best when it comes to the connection between communication and information systems, and operating systems. For the moment, **only partial security assessments are applied for minor software evolutions.**

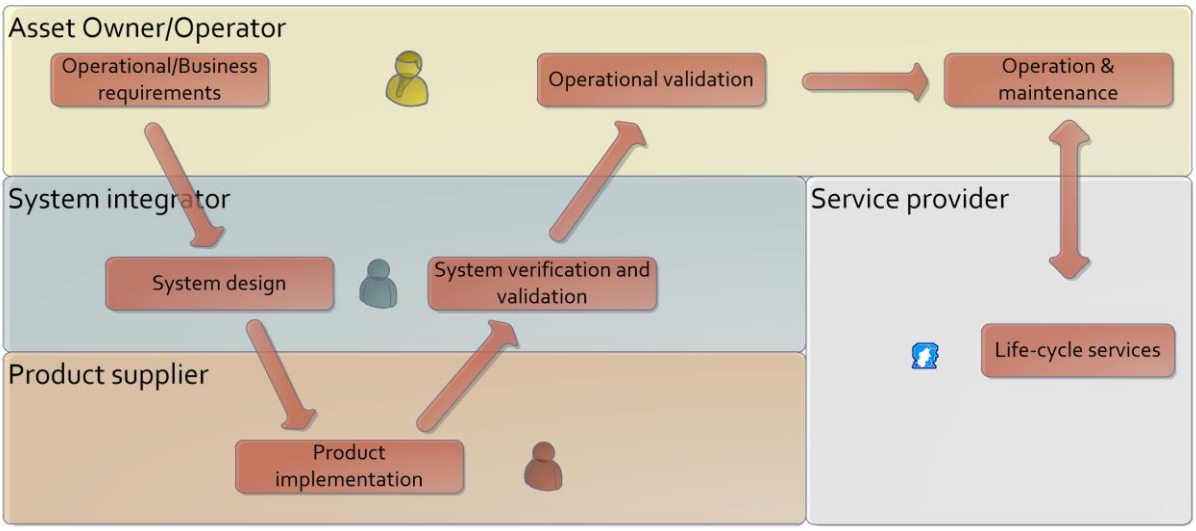
Yet, there is the need for a double-barrier protection between the hardware and software, so that tests or changes on one do not impact the other, or worse, undermine the entire system. Even changing one figure in the software takes a lot of time to be securely implemented to the rest. Today, there are **replicas of rail control centres that are used for the testing** before the deployment (mix of real and simulation), but the first trials prove to be very difficult to manage and implement. Therefore, the railway sector prefers to go towards exported approaches. If a device that is impacting the interoperability is changed, a report is made, and certifiers are consulted. Overall, the certification does not change, but the certifiers need to be contacted and consulted for safety concerns.

This leads to the last set of aspects in cyber security in railway which is the **high level of certification** applied to the railway sector. It involves the patching issue and the diversity of the supply chain and the technology in terms of the quality of both the insurance and certification.

Digital twinning technology, where there is a digital twin/replica of the device itself, is quite popular now because it can support more iterative security/safety lifecycle management. To do that, data integrity needs to be assured end to end. In general, the digital twinning technology is to be certified as little as possible in order not to invalidate the entire system. The general consensus is to **analyse how the software and the hardware relate to each other** and explore possible solutions.

There are currently two certification procedures that are applied to the railway sector, one covering the **safety aspect**, the other the **interoperability aspect**. So, if not proven immune, the system must at least be able to detect and react appropriately.

There are **designed guidelines** between the stakeholders with regards to the lifecycle of the components and systems, which are to follow a full cycle as per the following scheme:



Source: Shift2Rail

The link from the Operator to the System Integrator is with regards to the common understanding and assessment of the cybersecurity, -risks and -threats landscape and processes. The goal is to come up with a common guideline in order to reduce time and market costs. The standards covering this aspect are **IEC 62443 2-1 / 3-2 / 3-3**, as well as **NIST 800-30R1** (framework for a threats-oriented risk assessment).

The second step covering the relation between the System Integrator and the Product Supplier is about **referencing protection profiles and development processes**, as well as creating cyber certification equivalences. The protection profiles of the components are set through the definition of common rules for a security by design, i.e. a defence-in-depth implementation, a **systematic approach to develop and validate security requirements**, and a systematic approach for quality assurance assessment of cybersecurity implementation. The standards covering the component security level are IEC 62443 3-3 / 4-1 / 4-2. The equivalence of the cyber certification is set to go toward the ICCF approach, that is the European cross-certification framework for cybersecurity or security devices, in order to come up with a certification level at the cross-roads from the different certification approaches in the different sectors.

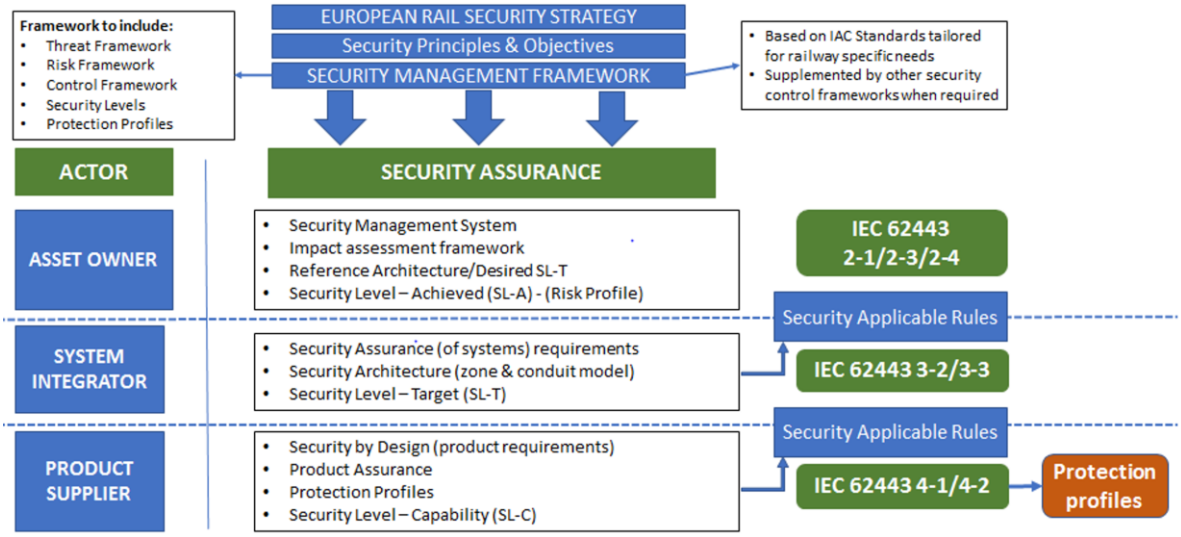
Once the product implementation has been done at the supplier level, it needs to go back all the way to the **operator**, passing again through the system integrator, for a **thorough verification and validation through common security testing methodologies**: penetration tests, vulnerability testing and integration testing. The standards covering the verification and validation are IEC 62443 4-1.

Once operationally validated, the **maintenance objectives** come into play (IEC 62443 2-4 / 3-3 / 2-3) to **provide standardised services profiles for the cybersecurity service provider, standardised**

patch management processes, as well as general requirements and processes for threat detection, prevention and response.

For the moment, at **European level**, there is a full **framework coverage for the railway sector** through actors such as **ERA** (European Union Agency for Railways) [14], **Shift2Rail** [15] (a joint undertaking between the European Commission and the railway sector, including operators, integrators, suppliers and service providers), DG HOME, DG MOVE, among others.

Shift2Rail, as representative of all the different stakeholders along the lifecycle chain as explained above, plays an important role in the cybersecurity framework for railways:



Source: Shift2Rail

They also collaborate very closely with **CENELEC**, the European Committee for Electrotechnical Standardization [16] (for a formal exchange of information and using the same standard framework IEC 62443) and European Union Agency for Network and Information Security (ENISA) [17] (in the framework of X2Rail-1 meant to start-up activities for Advanced Signalling and Automation Systems).

However, there are still aspects of the railway sector that are not covered, or are yet to be explored in-depth, such as **autonomous trains, the multimodal transportation or the discrepancy of the minimum service resilience level that varies from one country to another**.

2.3 Aviation

In the past, the aviation sector **benefited from security through obscurity**. Most states had their own custom-developed, proprietary systems, linked via point-to-point connections. Even if access were possible, interacting with such systems required rare, specialist skills. Nowadays, everyone is connecting with the Internet Protocol (IP) security because it is cheaper and more efficient. It also enables an easier data sharing globally to improve the aerospace, thus improving the cost/benefits margin. However, it also opens up to massive threats since every single aspect is put in a unique developed toolkit giving access to anything on the market, making it very appealing to attackers.

The main target is to achieve a minimum level of security for everyone. Yet, both the levels of applied security and of monitoring are completely different from one country to another, and even at the European level from one Member State to another.

In the EU, the **NIS Directive** aims for a harmonised approach in security in different sectors. However, **in aviation, it does not specifically guarantee a regular alignment**, especially when it comes to interconnected devices and maintenance. Maintenance, in particular, is a problem as its procedures are very specific to each and everyone in the world, and related costs are quite high. This heterogeneity means that the professionals are using all sorts of data from all sorts of sources which is very delicate as it means dealing closely with corporations and nation states that are not very keen on sharing it. As an example, we can point to the **unification efforts of Airbus** through its **Skywise initiative** [18], which is a big data platform for predictive maintenance and intended to be used by all major aviation players.

The other limit to EU regulations when it comes to their **local implementation is the interconnectedness of devices**. In addition, the connectedness of infrastructure will bring another level of threat. For example, if one wants to effectively hinder the activities in aviation, there is no need to attack one aircraft. Just killing or inhibiting the **signalling** would be enough (and would not even be considered as an actual attack) because the safety measures will keep all transport grounded. The implementation of regulations is also at different levels. Technically, as shown in the example, the level of security is determined by the **weakest link** (non-Air Traffic Management (ATM) systems such as BMS, power supply, HVAC, etc.). This means that if we go for a unified EU transnational network, the system will need to be heavily secured, ensuring we are ready for the worst-case scenario. On-board maintenance systems are also able to monitor a great number of physical parameters in the aircraft. They should be considered as additional cybersecurity systems. They raise alarms when detecting behavioural or structural changes that could be fed into cybersecurity systems as signatures for potential cyberattacks. Specific monitoring systems can be used to detect illegal connections on cables.

Aviation security by itself is **sub-divided into four main areas**: airspace security, air traffic management (ATM) security, airport security, and aircraft security. Each is handled by a variety of actors.

While **airspace security** is entirely under the **sovereign** control of the country, **airports** are subject to **various regulatory frameworks**, stemming from national, European and international levels all at the same time. Different services and activities of an airport must be compliant with different regulations, and the security requirements find their way through national security programmes. One of the singularities of airports lays in that they not only deal with aviation: they also provide other services – military, industrial, civil, commercial or business activities (hotels, real estate, parking lots, etc.), and of course including passenger security checks when entering an airport's gate areas.

In the traveller-centric applications, airports do not see cybersecurity as a new topic, but a new one coming to the aviation domain. An airport already listed as a critical infrastructure becomes, with the adoption of the EU NIS Directive 1148, subject to a move from "protecting the State" to "protecting the European Union market and essential services (EU key sectors including the transport industry); and will be subject soon to another transformation that is to "protect aviation". One of the main challenges therefore remain in the articulation between the State sovereign driven areas with those driving essential services under the Term of NIS Directive (OES & DSP) but also in the short term with those pertaining to aviation security and safety. The cybersecurity responsibilities, management and risk impact

vary from one airfield to another. **Not all the airports are critical infrastructures or operating essential services. But most European airports will be subject to protecting aviation**.

In the same way, not all airfields have the same maturity level of threat landscape. Quoting one former ACI expert in cybersecurity, Mr. Domenic Nessi, ”most large airports have made at least some efforts to secure their data and systems (a subset of which have made extensive inroad into cybersecurity), while many small and medium sized airports are aware of the threats but not sure what to do and where to start”.

In civil aviation, according to the International Civil Aviation Organization (ICAO) [19], two categories of risks can be considered:

- **Indirect facilitation-vector** to a subsequent act of unlawful interference
- **Direct disruption** – business continuity (rather than conventional aviation security and safety)

A holistic approach is necessary in the risk assessment, requiring the collaboration and information sharing between the national authorities and the industry. This fits into the bottom-up feeds from operators and the top-down intelligence from the States. Operators should be made aware of the threat picture pertinent to their activities from a national threat assessment standpoint.

A special focus should be given to the **ATM** (Air Traffic Management) security which is about safeguarding the ATM systems themselves, and also enabling collaborative support to national and pan-European aviation security incident management.

Protecting ATM system assets requires a multi-faceted approach to the protection of service provision in terms of performance (e.g. maintaining airspace capacity, minimising delays), of physical assets (communications/navigation/surveillance (CNS), ATM centres, air navigation service provider (ANSP) facilities), staff (operational, engineering, IT, etc.), information (operational or historical data), and of organisational assets (financial, safeguarding the reputation, etc).

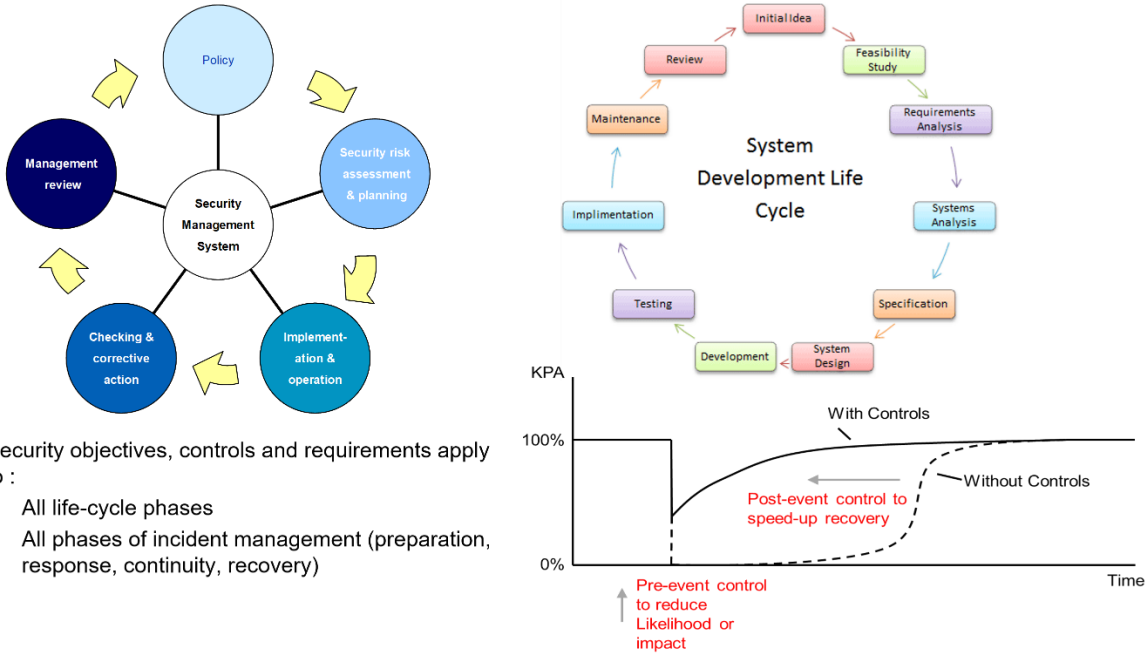
The impact of a security event on ATM tends to increase as more systems become interconnected and more data is shared. In addition, as more systems developed with COTS products and open standards are integrated with legacy systems, the likelihood of a security event also increases. Consequently, as the ATM system evolves, the risk (a function of impact and likelihood) are likely to increase. In order to address this trend, it is necessary to take a systematic approach to security risk management.

Several of the protocols used in CNS systems were developed before (cyber)security became a concern, and some are vulnerable to certain exploits, such as jamming and spoofing. ADS-B (Automatic Dependent Surveillance-Broadcast) is an example of such a protocol, and research is ongoing to address known vulnerabilities. GNSS (global navigation satellite systems) are also vulnerable to jamming. Fortunately, ATM can usually resort to other systems if there are problems with CNS. For example, potential issues with ADS-B are mitigated by the presence of ground radar systems which are typically not vulnerable to threats impacting ADS-B.

In aviation, **trade-offs** must be made regarding safety and security. Prior to a modified ATC (Air Traffic Control) system being brought into operation, extensive, time consuming **testing** must be carried out to ensure that changes to the system do not adversely affect system performance and potentially affect safety. Consequently, **ATC system changes are deliberately infrequent**.

This is in contrast to the approach applied to typical information technology systems. Generally, if a new vulnerability is discovered, such a system will be updated as quickly as possible to mitigate the risk to the system. By employing best practice in quality management, and following good engineering practices, such updates are relatively straightforward to perform, and there is no safety risk involved.

Compare that with ATM. In order to install a security patch, a **rigorous process** must be followed to ensure that the systems remain safe. The frequency at which patches can be applied is therefore somewhat limited.



Source: EUROCONTROL

Consequently, there is a **need for a new approach to ATC system design**, which may imply a new architecture which will allow quick system changes for security purposes without requiring the system to be, essentially, re-certified.

Other challenges include the **lack of security harmonisation** from one state to another and the challenge of developing trust between neighbouring states, which, although they conform to ICAO and EC regulations, may have achieved compliance via different means.

Safety culture is well developed and fairly mature in Europe, However, the development of a security culture of a similar level of maturity will take time and effort. The sector is trying to develop a holistic approach to security, addressing people, technology, and procedures together, with awareness development and training as key drivers in maturing security culture.

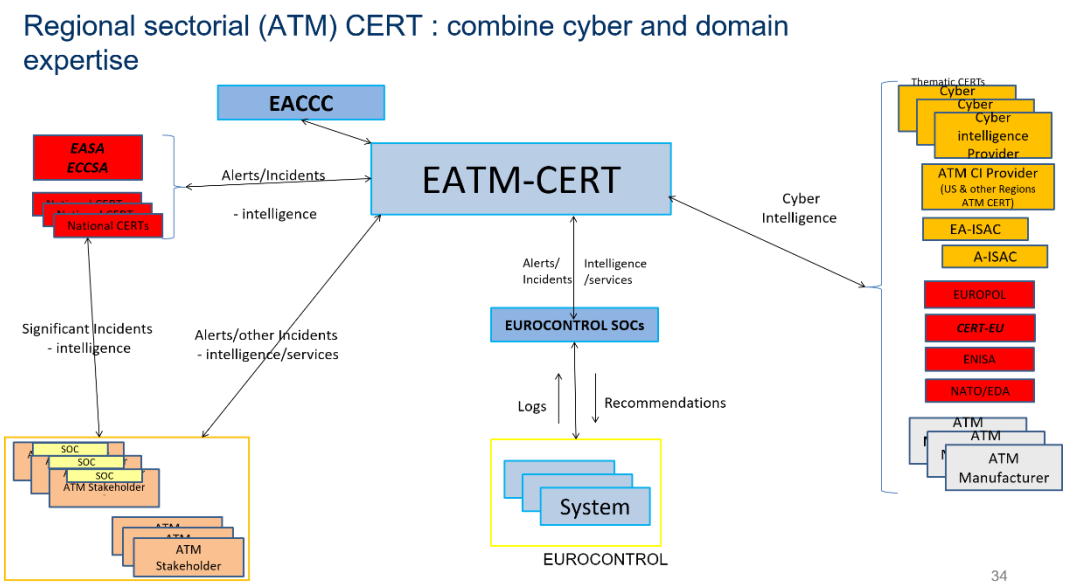
Security certification is an area which has been addressed for aircrafts and is still evolving, however, until recently there was a gap regarding ground systems, such as those in ATM/CNS. A recent publication (ED205) has addressed this gap. Aviation certification is based on deterministic behaviour – not a repetitive but an adaptative behaviour (which also conflicts with artificial intelligence).

Though aviation still needs interoperability in its ATM cybersecurity processes, there is coordination at European level between different stakeholders and bodies. **Cyber-attacks not only target the national level, but also the overall aviation network**. Several bodies exist at the European and international level, such as **EASA – the European Aviation Safety Agency** [20] that has a regulatory role, or **EUROCONTROL** [21] which is a technical authority and acts as a bridge between the European Commission and the 41 countries that are part of it. At the international level, it is worth mentioning the establishment of the ICAO Cybersecurity Task Force in November 2012 [62], that was a direct consequence of a demonstration given by Dr Andrei Costin in July 2012 of the weaknesses in the ATC systems coming into use. During the demonstration, he showed that with just a $ 2,000-worth of store-bought electronics, an ADS-B beacon could be spoofed to show that a non-existent aircraft was arriving to land. This 'Ghost Plane' presentation was possible because of ATC systems had no way of verifying where messages were coming from. [63]

Information sharing is therefore essential and has been implemented at several levels. EASA's **ESCP** (European Strategic Coordination Platform) has implemented the STORM Work Stream which is a Shared Trans-Organisational Risk Management working group. The SESAR project also launched the System Wide Information Management - SWIM Common PKI & Trust Network (SDM). SWIM ensures unified information network for ATM and access control for multiple stakeholders. [22] The EACCC – the **European Aviation Crisis Coordination Cell** [23] has been established in common by EUROCONTROL and the Commission, and given a legal basis by the latter (Commission Regulation (EU) No 677/2011 of 7 July 2011) to be "actively engaged in ensuring an improved level of preparedness in Europe for any kind of crisis potentially having an impact on air traffic". [24]

There are several lessons to be learned from the EACCC. In cybersecurity, the main concern remains the **CERTs**, the lack of coordination and the lack of a clear role distribution among the different stakeholders. The national CERTs, while established or under development as per the implementation of the NIS Directive, in most cases do not yet have links with aviation and/or ATM. In the same line, it is advised that selective flight protections (SFPs) and air navigation service providers (ANSPs) should also establish links with their national CERTs. The roles and responsibilities of already mentioned stakeholders (CERT-EU, ENISA, EASA, ECCSA, etc.) should be defined and clarified through a **gap analysis** to be performed at EU level for cyber-related attacks. In terms of coordination, the relations between the different entities have improved, especially at CERT level, even if internally the bigger member states remain predominant. However, there is still a gap when it comes to risk assessment. This also means that a specific pan-European CERT for aviation (including ATM) should be established.

EUROCONTROL has recently implemented its **EATM-CERT** (European Air Traffic Management Computer Emergency Response Team). It is in its early stages and they are currently trying to build-up a user base and connections in Europe. Its purpose is, inter alia, to collect, generate and distribute ATM relevant cyber intelligence within EUROCONTROL's Member States (41+2) and on a voluntary basis to EUROCONTROL Stakeholders (ANSPs and Airport Operators). For the moment, they are using standard tools, such as the Malware Information Sharing Platform (**MISP**) but are also in the process of developing their own environment. EUROCONTROL/EATM-CERT is a founding member of **EA-ISAC** which is being set-up by industry actors and facilitated by ENISA.

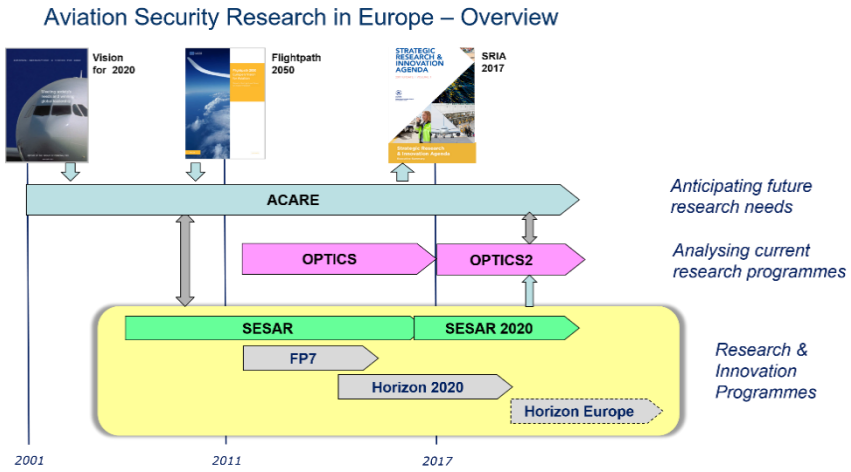


Source: EUROCONTROL

EUROCONTROL also provides several **training courses** for the ATM community, covering Security Management Systems, Risk Assessment, Cybersecurity, and Security Oversight amongst others. EUROCONTROL also provides support to states, ANSPs, and national CERTS, to help Member States to conform with regulatory requirements.

There is also a lot of research being done, by, for example, ACARE [25], the Aviation Council for Aeronautical Research in Europe, which is trying to define the R&I needs for the future, plotting a path towards meeting the goals of **Flightpath 2050**. Meanwhile, the **OPTICS2** project is analysing past and ongoing research projects in Europe and in EU Member States, assessing how these projects are developing the necessary enablers, and identifying gaps and overlaps.

The **SESAR** and **SESAR2020** projects have been carrying out research which will be deployed in the short term.



Source: EUROCONTROL

2.4 Maritime

Maritime transport and ports play a crucial role in **world trade and are part of the economic and strategic interests of Europe as a whole**. A threat to ports and ships can have impacts on the trade flows between nations, damage corporations and jeopardise the supply chains of several sectors. All maritime stakeholders are possible targets and need to consider this threat as concrete, and at EU level the cyber domain is now a priority. While there is no clear standard definition of cyber-space, it can be referred to as the domain of **information flow and communication between computer systems and networks and includes physical as well as purely virtual elements**. Cybersecurity, in this context, refers to the domain of systems playing a pivotal role in the prevention or response to threats to critical operations and indicates prevention of or reaction to deliberate and malicious acts undertaken via the cyber-space to compromise a system directly or indirectly.

Connected ports and devices in ports can be easily hacked through bypassing the security of one of the devices. In transportation, safety is strongly intertwined with security and cybersecurity. Incidents such as the recent increase in irregular migrants entering Europe through the Mediterranean coastal areas as well as smuggling of illicit goods requires increased protection of the Critical Infrastructure such as port operations. Software systems that support **Critical Infrastructure operations** are becoming more and more attractive to outside cyber-attacks from cybercriminals interested in wreaking havoc on cyber environments. Not only sensitive data needs to be protected from any malicious intentions, but if the overall control that these software systems have on the operational aspects in Critical Infrastructure is harmed, then negative results with high risk, impact and visibility can arise. Innovative physical and cybersecurity mechanisms must be created to be able to prevent and respond to all potential threats to these Critical Infrastructures.

In the maritime sector, there are several parameters to be monitored like GPS, and similarly to aviation, several of the protocols were developed before (cyber)security became a concern. Some protocols such as AIS (Automated Identification System) are vulnerable to certain exploits, such as jamming, snooping, spoofing, and research is ongoing to address known vulnerabilities. [64] Hull opening, hull stress, radar, ship speed, fuel and machinery temperature and so on, from landside SCADA[1] allows the control of Surveillance system until cargo handlings systems. In recent years, Cloud Computing and Internet of Things (IoT) have been rapidly advancing as the two fundamental technologies of the “Future Internet” concept. Different IoT systems are designed and implemented according to the IoT domain requirements, typically not taking into consideration issues of openness, scalability, interoperability, and use case independence. This leads to a variety of new potential risks concerning information security and privacy, data protection and especially safety, all of which need to be considered in unison. IoT is just beginning to emerge with exploits reported at a steady pace and suggesting that information security and operational security are already major challenges. Such security threats are broad and have the potential to undermine IoT systems and/or significantly alter their intended operation. Since the IoT ecosystem can often have critical infrastructure components, it will inevitably be a

[1] SCADA means supervisory control and data acquisition; the first use was started in the 1960s to monitor and control remote gear grew that is part of the Control Systems family, that includes ICS (Industrial Control System), DCS (Distributed Control Systems), PCS (Process Control System), etc. Early systems were built from mainframe computers and required human oversight to operate. When the technological development became automated, it reduced the involvement of human control. These systems are used to monitor and control a plant on industries in many different sectors like energy, transport, waste control, etc.

target for attack and espionage, as well as vulnerable to denial-of-service and many other types of cyberattacks. [26]

Currently, the **shipping industry** has an estimated 65,000 commercial ships and 5,000 ports, and only half of the ports understand or are aware of their problems and vulnerabilities concerning cybersecurity. It is most likely that all of them have at least been hacked once by now, though none of them have ever reported any incidents.

Beyond the cloud, the maritime sector is subject to huge amounts of threats, mostly due to the interfaces of systems that see enormous differences of architecture and generations between the IoT and IT devices. The systems are connected to networks each in a different way and in reality, a lot of work is put into connecting the systems between themselves despite the differences (e.g. monitoring, transmission, etc.). It is highly advised to work on open standards and develop protection and mitigation techniques with many fields of application, that is beyond the maritime sector-specific applications.

Currently, a **majority of the systems are autonomous**, and it is anticipated that in the future autonomous ships will require enhanced cybersecurity. The ever-increasing digitisation in the maritime sector has resulted in an increased exposure to attacks, and even more so for fully autonomous ships. Cybersecurity is therefore a key factor in securing autonomous ship operations and will require a specific approach towards system design, including internal and external threats. Potential vulnerabilities of various ship systems (such as propulsion and engine management, power control, bridge, communications, cargo management and access control systems) should be addressed.

Because of these discrepancies, it is important to note that **basically all systems could be hacked** on a ship, thereby showing that the maritime sector has a much lower security culture compared to the other transportation sub-sectors. Each ship contains **an estimated 300 entry points for hackers**, without even addressing the criticality of ship to shore information exchange. Recently, the most attacked systems have been the navigation systems, for example because of crew members charging their phones on USB ports or loading something infected, the safety systems, and the power systems.

As a consequence, the threat-scape covers a wide range of vulnerabilities. Most ships are still operating on **extremely outdated Windows systems**; there are multiple systems from multiple manufacturers; and in general, a lack of awareness and bad procedures being carried out. **Phishing** remains a major issue (at least 70% of the problem) with malwares invading the system on a matter of weeks while the response from the regulators takes months, if not years. The threat level percentage skyrockets from one year to another and could effectively ruin a business model.

Phishing immediately raises another issue, the one of cyber **awareness** among the crew and in general, all involved individuals in the maritime sector. Individuals need to realise the impact of digitalisation, especially on a ship where most systems are not cyber protected. It is currently estimated that the maritime industry lacks 50 to 100,000 trained people in cyber. It is also important to note that there is a general confusion in the distinction between cyber experts and IT experts. Currently, the average ship has one IT expert. Most ships do not get hacked remotely, rather they get hacked when in port, or the problem of vulnerability is simply internal. With such a lack of qualified effectives, if a problem appears, it is not noticed by the crew on board since most systems have a manual back-up. It is advised that the effort to raise the flag and send it when something is not working correctly needs to be included directly in the system.

As already mentioned, **insurance** is a very big part of the maritime sector. Generally speaking, there are the Protection and Indemnity Clubs, aka the P&I Clubs, centralised by the International Group of P&I Clubs [27] that is **insuring the shipowners' liabilities**. The members of the Club share their large loss exposures between themselves. That also means that when the International Group is defining the contracts of the ships, it also judges their **seaworthiness**. If a ship is not deemed sea-worthy, then it is not covered by the insurance. On the other hand, the International Association of Classification Societies [28] that gathers 13 classification societies, i.e. NGOs or groups of entities in the shipping industry, works on establishing and maintaining technical standards for the construction and operation of the ships, thus classifying and validating their seaworthiness [29]. The new concept that has been recently introduced in the shipping industry is the **'cyber seaworthiness'**, since insurance is a real problem in shipping due to the major costs that it entails. There is an extreme difficulty to quantify the risk, and even to the best of ability, the cost of a small hack on a ship is estimated to result in up to hundreds of millions of dollars of damage.

Beyond the insurance aspects, sharing information in the maritime sector is considered as a dramatic failure. Contrarily to the relatively centralised air sector, **maritime is very fragmented**. There is a lack of transparency with regards to the actual stakeholders to whom to report to and in general, reporting is not made anonymous which can have damaging consequences such as bad press for the company, the captains seen as whistle-blowers and losing their "non-event sailing bonus", etc. This would be a recommendation for the EU to create a safe, confidential and anonymous reporting centre for the maritime sector. Currently, the CSO Maritime Alliance – Chief Security Officer Alliance [30] is an example of an attempt to implement the reporting of cyber incidents, though the membership remains extremely low to concretely feed into the system.

There is a lot to be learned from reporting, though it needs trust, and regulators and national administrations working together. The greatest challenges remain in the difficulty of defining **one applicable law with a diversity of legal environments and conditions – the law of the country of the ship? the captain? the sailing area? the freight? the shipbuilder? on shore, territorial or international waters?** - and the existence of too many codes of conduct with no universally agreed upon standards and guidelines. A first step was made in January 2016 with the publication by shipping companies of a recommendations guide to cybersecurity on board of ships, since updated to version 3 in 2018. (cf. [5])

A quote that is representative of the current state of the art in the maritime sector was mentioned by Chris Henny during a workshop organised by ECSO in July 2019: "airlines once taking off have a limited time to stay in the air. It is quite different for the ships. Imagine a vessel with a Ukrainian captain with a Filipino crew, operating partially in national and international waters all around the world under a Liberian flag – Libera does not have any CERT, SOC or reporting capabilities – that gets a cybersecurity incident. Then whom do they report to? This is where the real weakness is as there is no recourse, no way of finding where the real hacker is or where to get a concrete picture of the scale of the problem."

2.5 Cross-sectoral Security Considerations

Unfixed vulnerabilities are the biggest vector of attack possible. It has to be considered and enforced. Ultimately, that means that we need a safe and security aware design of everything that is supposed to be connected and this applies to all of the sub-sectors.

Some cross-sectoral security elements to consider are:

- Avoid single supplier situations.
- Deployment of COTS needs to go along with daily vulnerability management.
- Problem of scalability to big heterogeneous data: abundant data increases the risk but also may feed into more accurate anomaly/attack detection systems.
- Need to identify and apply distinct measures to privacy/IP-sensitive vs time/safety-critical data.
- Some data such as geolocation data may be both critical and sensitive. Countermeasures against GPS jamming and spoofing are urgently needed: law enforcement, shipping, airlines, power stations, smartphones, and anything else dependent on GPS time and location synchronisation are vulnerable to GNSS hacking.
- Conflicting hardware / software lifecycles – need for dynamic requalification processes. The link between the cyber and the physical layers and the interdependencies remain an issue from the technology point of view.
- Apply extensively approaches such as Secure Software, Secure SDLC, Secure by Design, DevSecOps. Regardless of sector or technology (i.e. GPS, GNSS, ADS-B, AIS), it is a matter of some critical software processing potentially untrusted input (e.g. spoofed/fuzzed by hackers) for possibly mission-critical and life-depending decision-making.
- Is there a conflict or possibility of continuum between State sovereignty and safety?
- Existing segregation between the cybersecurity training platforms, i.e. cyber ranges, and the requirements for visualisation that a non-expert trainee would have.

Overall, an **entire cybersecurity culture** needs to be introduced within companies, starting with the CEOs and going down the hierarchy chain to create awareness. Special training needs to be provided according to the roles and responsibilities, even if it will take time to make it happen. The reporting is a huge part of the awareness training as well, for the individuals to know what should be flagged, where to report and to whom to report. As mentioned, some companies refrain from reporting in particular because of image and commercial sensitivities. In this sense, the anonymisation of the information and of the reporting could be a solution to build trust and encourage good practices. All these elements require both sector-specific and cross-sector trainings and approaches. This is where, at the European level, the European Commission is encouraged to take action for a legitimate standing in order to have the appropriate authority approving the cyber hygiene training packages according to the different constituencies.

The issue of reporting is also an area where the European Commission could take action to provide for a centralised and harmonised approach in reporting. Beyond the global international aspect of transportation (especially aviation and maritime), European countries need to tune in their approaches for a common understanding of standard operating procedures. The reporting, whether anonymised or not, is even more crucial beyond the sub-sector approach as is the case in multimodal transport where the different sub-sectors are interrelated, meaning a cybersecurity incident could potentially affect the whole ecosystem.

The last issue, the **anonymisation of data** in reporting, needs to also be carefully considered as it can lead to reduced accountability. Indeed, the European Commission is encouraged to take on a centralising role for coordination purposes first between Members States but also between the European Union and the rest of the world. However, there are levels of incident reporting that simply cannot be anonymised. A solution would be for the **industry operators to create clusters**, as in trusted communities, to encourage information and intelligence sharing among peers. This again excludes the area of information sharing with the larger public – panic-inducing, bad publicity, etc. – which still should be mandatory if the right effort is made for the sharing to have a positive

impact. A platform worth mentioning in this respect is ECSO's own Users Committee (UC), a hub that gathers a network of C-level executives from Users and OES to discuss and share intelligence on a voluntary basis in all trust and confidence. The UC intends to have a supra-national European and cross-sector approach to also allow best practices learning from one sector to another and from one country to another. Cyberattacks do not have borders or limits and thus, nor should cybersecurity.

User Engagement

In the transport sector, several actors play a key role for cyber security. From Original Equipment Manufacturers (OEMs), Tier-1 and Tier-2 suppliers to public transport and infrastructure operators to consumer associations – they all have specific cybersecurity requirements and discuss that topic from different angles.

The following stakeholders should be consulted and/or considered:

Drivers / passengers: Car drivers and users of rail / ship / air services (also businesses) are the main target group of intelligent transport solutions. Trust and acceptance are a prerequisite for the roll-out of those technologies. It is important to understand their needs and expectations, also in terms of cybersecurity. Two essential aspects must be taken into account for transport: safety - in terms of resilience of connected vehicles and services - as well as privacy of personal data.

OEMs: Original Equipment Manufacturers provide components to the supplier-manufacturers. These include sensory, actuators, digital platforms, and other components of technologies that will be integrated together by a technology provider or supplier-manufacturer.

Manufacturers: Manufacturers of cars, airplanes, ships, trains and space applications are confronted with new, even disruptive technological opportunities. Their products are becoming more complex with more electronics inside, being able to be connected to other devices via the Internet. These “everything can be connected with everything” developments result in new safety (incl. cybersecurity) and privacy requirements for manufacturers.

System Integrators and Technology Services Providers: Facilitating the integration and additional day to day support on operations.

Tier 1 / Tier 2: Suppliers of components are more and more confronted with specific cybersecurity demands by their customers (OEMs). In addition, value chains are changing. New players are entering the market (e.g. telecoms) and typical business relationships are breaking up, e.g. meaning that Tier-2 suppliers are now directly involved with OEMs.

Public transport / infrastructure operators: Railway, harbours as well as road operators have identified the opportunities in terms of efficient traffic management, CO2-reduction and safety coming with digitalisation. But since cyber-attacks and data theft are still a severe risk, a lot of them stay reluctant when it comes to investments in smart technologies. Airports remain an exception in this case.

Regulators and certifiers: The work of other regulatory groups, especially the Homologation, shall be considered as well to prevent duplication or contradictory regulatory approaches. However, not all transportation sectors are easily certified or regulated.

—

On the other side of the spectrum, the following should also be considered:

Criminal actors: The emerging criminal actors (hackers, attackers, etc.) are forcing stakeholders to collaborate with different governmental actors to monitor the individual profiling and understand the motivation of different attackers. Countering criminal actors requires an understanding of the field, both at the technical and psychological level.

State Actors: Nation state sponsored criminal actors, aiming to interrupt, or cause direct and environmental damage to other nation states or organisations.

—

The stakeholder groups and associations to be consulted include (non-exhaustive list):

Road Sector:

- ACEA (European Automobile Manufacturer's Association) [31]
- CLEPA (European Association of Automotive Suppliers) [32]
- CORTE (Confederation of Organisations in Road Transport Enforcement) [33]
- ETSC (European Transport Safety Council) [34]
- IRU (World Road Transport Organisation) [35]
- ITF (International Transport Forum) [36]

Air sector:

- ACI Europe (Airports Council International – Europe) [37]
- ASD (Civil Aviation Task Force)
- EASA (European Aviation Safety Agency) (cf. [20])
- ECAC (European Civil Aviation Conference) [38]
- EUROCONTROL (European Organisation for the Safety of Air Navigation) (cf. [21])
- ICAO (International Civil Aviation Organization) (cf. [19])

Rail and public transportation sector:

- ERA (European Union Agency for Railways) (cf. [14])
- ERRAC (European Rail Research Advisory Council) [39]
- LANDSEC (Expert Group on Land Transport Security)
- RAILSEC (EU Rail Passenger Security Platform)
- Shift2Rail (Joint Undertaking) (cf. [15])
- UIC (International Union of Railways) [40]
- UNIFE (Association of the European Rail Industry) (cf. [13])

Sea sector:

- BIMCO [41]

- CIRM (The International Association for Marine Electronics Companies) [42]
- CSO Maritime Alliance (Chief Security Officer Alliance) (cf. [30])
- IACS (International Association of Classification Societies) (cf. [28])
- ICS (International Chamber of Shipping) [43]
- IMO (International Maritime Organisation) [44]
- International Group of P&I Clubs (cf. [27])
- MARSEC (EC DG MOVE Maritime Security Expert Group)

Sector Specificities

Based on the assessment of the ECSO SWG 3.3 on transportation and following two separate workshops, the following sector specificities have been identified:

3.1 Risk management – framework for cyber risk, integration with domain

There is a **clear need to manage the current and future risks properly**. Identifying the risks through analysis of validated methodologies and translating them into corresponding cybersecurity requirements (starting from the design, thus laying the grounds for a security by design approach) is a must, also including cyber risk in the safety analysis. For example, ISO is working on a standardised and internationally accepted method of cybersecurity and privacy risk assessment for road vehicles.

Also, **passenger safety** is one of the most important concerns in the road vehicles domain. Especially with the evolution towards connected vehicles and automated driving, cybersecurity risks may immediately induce safety risks, which makes cybersecurity and safety concerns of same importance. Lifetime for road vehicles is typically 10-15 years, such that changes in the risk profile have to be expected and taken into account.

The biggest cybersecurity risk for a product is to not understand the cybersecurity implications of its development and use. Therefore, instead of quickly jumping to mandatory cybersecurity feature conclusions, the manufacturers and the road vehicle / automotive industry as a whole first have to further improve their capability to identify and assess cybersecurity risks and to select, implement and quality-assure appropriate risk management controls – up- and downstream the value chain and across the whole product lifecycle. An important step in this direction is the ISO-SAE 21434 standardisation activity "**Road vehicles - Cybersecurity Engineering**".

The development of **data centric business models** on top of the pre-existing transportation services can be a solution for a better risk management. However, limitations remain in this respect, mainly compliance with GDPR requirements, the issue of competitiveness for the European players, and the implication of massive anonymisation techniques which are incompatible with attack attribution techniques. Anonymisation has indeed been advised earlier in this report when it comes to reporting, but massive anonymisation of data at all levels would be counter-productive to actual risk management.

Finally, transportation itself has **disruptive elements** in its present and future evolution from traditional air/sea/road/rail sub-sectors, such as flying cars, UAV-based package delivery, etc. These new means would operate in little, if not at all, regulated environments. Here again, converging standards and security measures will be required for an optimised risk management.

3.2 Everything that can be hacked will be hacked – design to fail (securely)

It is important to manage and implement the different phases of the cybersecurity process: bootstrap, update and recovery (coming back to secure conditions even in the case of successful attacks).

At the same time, functional safety and cybersecurity principles may contradict each other: While it is good practice to disconnect and isolate compromised nodes from an enterprise network, it **may be safer not to "shut down"** a potentially compromised autonomously driving car, but to go to a fail-operational mode that still provides essential functionality until a safe "shut down" is possible.

As seen in some transportation sub-sectors, such as aviation, a shutdown is out of question, and software fixing cycles are taking a very long time to be implemented without endangering or destabilising the entire system. The digital twinning technology, in this aspect, may be a solution. Digital twins are quite the fashion now because they can support more iterative security/safety life-cycle management. To do that, data integrity needs to be assured end to end.

Digital twins are used in different environments: engineering, R&D and, especially rail and air (traffic control). There is a digital twin of the device of itself. From an operator's perspective, you cannot even make the difference between the virtual digital twin and the actual operating system. The digital twin may effectively address software security problems and check if the hardware security is also effectively addressed. However, for product security, a digital twin only works so far, not being useful at all in case of a blend of software and hardware.

Digital twin environments may support enhanced training of autonomous driving algorithms, but the influence of environments conditions might not be duly reflected by the digital twin. Engineering designs are made in functions, shaped in a nice, elegant and efficient manner. But engineers do not think in reverse of how the functions can be attacked, and functionalities exploited in the end. If cyber-physical attacks are happening on the properties of the hardware, one would be reluctant to use any data.

To enhance **resilience** and make it more difficult to attack, there is the need for different platforms (operations, communications, etc.) at all levels, though this remains quite expensive.

3.3 Safety issues/aspects weaved with cybersecurity

In transportation, safety is strongly intertwined with cybersecurity. The problem is the two evolve at dramatically different speeds. Safety risks in traditional road vehicle systems primarily originate from unintentional hardware and software failures that can be modelled by well-understood stochastic processes. Security risks, on the other hand, originate from intentional behaviour of self-interested, incentive-driven human threat agents, who have to be approximated with game-theoretic methods. The incentives of such threat agents are subject to change, e.g., due to changing political environments, market conditions, etc., and so are the attacks to be expected from them.

To try and mitigate this dualism, we propose in the first place to apply **least privilege and separation of duties, differentiating connected systems and critical systems.** Securing on board communication is also a measure to be implemented, to maintain the integrity of the information exchanged within the vehicle and avoiding external breach that would make the vehicle behave inappropriately.

Autonomy is also very much sought after, as well as the supporting infrastructure to achieve this – for example the V2X: car-to-car and car-to-infrastructure services to support assisted driving and autonomous driving. This is an area to be carefully safeguarded together with efforts in standardisation.

Another point is that **almost no practically used security mechanism has a formal security proof**. Our trust in these mechanisms is based on the fact that they have been examined by many experts for many years without considerable findings. There is no guarantee that what is believed to be secure today will not turn out to be entirely insecure tomorrow. Moreover, security mechanisms typically rely on the hardness of certain computational problems. Their strength therefore already decreases with increasing computational power available to attackers, leading to a "natural security wear-out" over time, similar to the wear-out of mechanical parts.

Another issue with a broad scope is **cybercrime**. It **does not stop at national borders**: this is especially true for remote attacks on connected products via the Internet, which may be carried out from virtually anywhere in the world, while the exact origin of the attack is often impossible to determine.

In summary, security risks are much more subject to change than traditional safety risks and are often largely connectivity-induced, which has to be accounted for in the security risk management strategy.

Considered as a best practice of security, **cryptography** is seen as an easy solution, i.e. any kind of authenticity and integrity could be handled by means of encryption and signature. A common misunderstanding relies in the fact that cryptography is not a general solution as it merely addresses a need in confidentiality and implies reliance on data not always free to use, while it is preferable to have more data to analyse and correlate than one would usually use. But for some sectors of activity, such as ATM, data integrity and availability are more important than confidentiality. Risk assessment and impact analysis are required prior to deciding which controls to implement. The concrete implications of applying cryptography solutions are that it needs to be in place in real-time (for critical communication) and to rely on solid infrastructure. Thus, there is not one single solution by a single supplier, and usually COTS deployment makes attack cost/effectiveness greater. Moreover, encryption may not always meet time sensitivity requirements.

On the other hand, **object-based encryption** can be advised on a case by case basis. This solution can come with several other recommendations such as assessing/sharing economy and cloud to cloud services. Secure cloud-based platform service providers are required with trust-enabling technologies, based on reputation, rating/scoring, blockchain and indeed object-based encryption.

3.4 Strong defence to side-channel attacks & cyber-physical

With the long lifecycle of road vehicles and their components, and the inherent dynamics of cybersecurity described above, it will be prohibitively **expensive**, if not impossible to prevent cybersecurity incidents thinking from a cyberspace perspective only. We need to remember, though, that every system will be deployed in the field, and as such will be susceptible to being attacked from its physical side, in the so-called side-channel attacks. To mitigate this aspect, we propose to assess system security by third parties and use certified products, calling at the same time for an EU cybersecurity label to be recognised as "coming from a secure supply chain". Also, continuous management of the cybersecurity situation (benchmarking, monitoring…) will enhance awareness of potential breaches coming. In this sense, centralised or edged SOCs will be strongholds to protect the flow of vehicles and people from continuous attacks incoming from the cyberspace.

Lastly, to be more forward-looking, enforcing wherever possible – maybe just in **the safety-critical sections of the code – a formal analysis approach** (that is EAL6/High Assurance per se) coupled with a binding to some hardware root of trust (like physical unclonable functions), while expensive, could grant a more resilient ground to build a safe and secure platform.

3.5 Patch agility and reach – OTA security vs regulation

Speed has a different meaning in cyberspace. While deploying a safety patch once every 5 years would seem exaggerated, deploying a security patch every 5 days is the minimal cyber hygiene. Again, safety and security play two radically different roles. Sending software update **Over The Air (OTA)** will update vehicles remotely and avoid having cars returned to service points to update software. At the same time, how will it be possible to still grant safety? By isolating functionalities and activities of systems, such as a dedicated safety and security system, this is currently being implemented. This will be an issue to be addressed in a new wave of standardisation. Finding a balance between patch agility and cybersecurity/quality assurance, especially when cybersecurity vulnerabilities are identified for products in the field, will mean finding a trade-off between patch distribution speed and security/quality assurance for the patch. Especially Regulation has to ensure that the roll-out of patches is not overly delayed by, e.g., time-consuming (re-)certification. This could lead to a longer period of exposure of vehicles in the field or the temporary abandonment of vehicles, which regulation originally had intended to avoid.

3.6 Always have a human in the loop

Keeping a human in the loop currently remains highly recommended, especially when it comes to spoofing in aviation and rail or the manual mode in the automotive sector. Human assessment and vigilance remain key factors in spotting inconsistencies.

Fault attribution and the accountability gap that is being created with regards to machine decision-making are an entirely predominant aspect in the field of autonomous vehicles. There are still drivers, operators, software editors, etc. operating in that field, and with the increased attribution of decision-making to machines comes an increased risk of negligence and loss of vigilance due to cognitive underload. However, adversarial AI, spoofing of sensor data, mobile data jamming, etc. remain high-target risks in case of attack and human vigilance is required. Therefore, a clear line should be drawn between the human and machine decision-making with a clear separation of roles.

A final aspect covers the **stringent need for training**, raising of awareness and risk quantification. All members of a team, whether with technical or non-technical profiles, must be cyber-aware and have an impeccable cyber hygiene. The transportation sector involves the transport of goods but also of humans whose lives can potentially be targeted in case of an attack or malfunction derived from an attack. Several solutions can be envisaged, such as the support from **cyber ranges** for the training or AR/VR exercises (augmented reality/virtual reality), and the digital twinning technology for the secure transition between software and hardware.

3.7 The role of firmware security

The challenges of smart devices belonging to the Internet of Things ecosystem (but also legacy systems including PLC's and SCADA) are increasingly present. However, technology companies producing these evolved systems tend to underestimate the potential risks to which they are exposed since these devices are continuously connected to the Internet. The greatest danger is caused by the manufacturers themselves who tend to release firmware updates too infrequently and sometimes, fortunately only in extreme cases, the updates are not even released. This behaviour allows hackers to take advantage of a huge amount of potentially vulnerable devices. [45]

The firmware, an expression consisting of the terms firm (baked into the device, considered as stable) and ware (component), is a software programme present within most electronic components. Its fundamental role is to start the functioning of the same component allowing it to communicate with further integrals or cards present in the device in which they are installed. The amount of shared information allows us to determine the importance it has to release firmware updates. Otherwise, it may happen that an IoT device, updated and therefore safe at the time of the purchase, becomes dangerous for the consumer when cybercriminals discover a vulnerability in the system. This event usually occurs when the manufacturer decides to allocate its internal resources to the production of a new product to be proposed on the market, effectively stopping the development and release of updated firmware versions for already existing and marketed products.

Most device manufacturers are building on already existing components, taking existing technologies including software to be fitted to serve the integration, to reduce cost and to easily work on capabilities for integration with existing (internet) technologies. No considerations are being paid to potential vulnerabilities in these (sometimes) open source components, and they are simply integrated and forgotten about. More efforts will be paid later on to the web application / application interfacing and network protection, with the adverse effect that the basic technologies are still largely vulnerable.

Consequently, the most significant risk for the consumer (transportation organisation in this case, an operator or even an airplane pilot) is to be hacked due to obsolete and potentially dangerous hardware. The failure to update the software is not always attributable to the choices of the manufacturer; in this sense, the end user also plays an active responsible and sometimes harmful role. Often, due to personal inexperience or lack of knowledge of the technological product being used, the consumer does not check for updates and does not install the firmware versions later released and recommended by the manufacturer. To overcome this specific situation and reduce as much as possible the risks related to the security of software platforms, the most advanced devices, including computers, are programmed to perform automatic updates without the need for customer intervention. Unfortunately, protecting and updating the security features of the systems belonging to the Internet of Things world doesn't happen automatically, and is not yet completely automated, and for this reason, it will not be trivial to implement solutions oriented towards this purpose. Companies' commitment to firmware security is increasing and should become a priority.

To achieve a high level of security for IoT devices, it is necessary to introduce a shared standard that can guarantee a common methodology during the design, development and above all the issue of updates. As an example, ARM Holdings [46], a company specialising in the technological development and known on the market to be the manufacturer of processors based on the ARM architecture, Huawei, and Intel are engaged in the launch of the process that will lead to the approval of a standard for the IoT. While only a few IoT and other internet-connected devices have been equipped with ARM-processors, ARM Holdings has already released a formal document called "IoT Firmware Update Architecture" [47] demonstrating the commitment placed in the firmware security field. The paper presents a set of rules that all smart system manufacturers should follow during the implementation steps of the **firmware update mechanism** of the implemented devices. The most necessary prescriptions contained in the document are the following:

- Use of end-to-end encryption;
- Prevention of cyber-attacks;
- Facilitate the distribution of updates with different modes (USB, Bluetooth, Wi-Fi, etc.);
- Maintaining the same file formats for the firmware.

While intended for developers using ARM architectures, the method presented is a starting point for the achievement of a concrete (IETF) standard. However, the document shows some aspects that need to be deepened and improved to make it valid in all its parts. Achieving the goal of introducing a constructive standard for smart systems would allow to mitigate the numerous security flaws in the connected devices. The updating of the firmware of the devices is a critical operation since for some years there have been search engines specialised in identifying the services exposed by devices connected to the Internet. Unfortunately, there are no recommendations for service operators, integrators, or security services providers. As a result, many challenges remain unresolved and vulnerabilities, known or unknown, are open to future discoveries of weaknesses.

A very well-known search engine is shodan.io through which specific searches can be made to obtain a list of smart systems belonging to the vulnerable Internet of Things ecosystem. This portal can be used by anyone, therefore also by any hacker willing to find targets for their cyberattacks. However, to avoid facilitating the task for the bad guys, registration is scheduled on the website, and in any case, only little information is provided free of charge. Fortunately, the portal can also be used consciously by company personnel to monitor the level of security of their business

devices. Thanks to this web service it is possible to carry out targeted scans to detect vulnerabilities and intervene promptly to secure your work environment.

Trends, cross-sector & transversal issues impacting transport sectors

4.1 Digitalisation & Digital Servitisation

Transportation by itself refers to movement, and therefore, the habits of people. The impact is tremendous with the increasing number of passengers who are using transport data for suggestions on their smartphones' applications thereby showcasing their patterns and habits.

Digitalisation of transport is a process that already started years ago, and that is happening both within the infrastructure and on the services levels. The transport nodes are being equipped with different sensors, technologies collecting and transmitting data, digital platforms showing passengers and customers the whereabouts of the transport mechanism using satellite navigation information. Traffic systems have been connected in order to optimise the traffic flows, reduce congestions and reduce the impact on the environment. Number plate recognition systems support smart cities and allow for improved intelligent transport systems. In cars, telematics are continuously monitoring the status of road transport, but equally allow for improved maintenance of railroad and planes. Mobile connectivity allows for the end users to continuously interact with their services providers, tracking packages from all over the world.

With the digitalisation of the transport sector, there are many new opportunities but also new challenges, including some related to IoT (Internet of Things) and industry 4.0, the circular economy, horizontal and vertical integrated systems and cyber-physical systems, the multimodal transport, the autonomous vehicles, robots, and the emergence of new modes of mobility such as drones, e-scooters, etc. These new modes were not available before but certainly do include a cyber element now that cuts across the traditional ways of transport.

With the digital servitisation, new forms of technology, but also of the economy, appear. The sharing economy approach, sometimes referred to as "uberisation", is the perfect example of the new techniques happening thanks to the digitalisation of the sector.

Privacy challenges can already be identified here, and the first step in transportation should be to make the differentiation between cybersecurity and access to data. Access to data is very often asked by authorities, for law enforcement purposes which requires more and more recordings, while privacy pushes towards the exact opposite. A suggestion here would be that the industry could give the data to the authorities, i.e. the law enforcement, on a voluntary basis. Here again, another distinction should be made between cybersecurity, that is roughly the solving of incidents happening, and cyber attribution in the case of organised crime for example.

The issue of privacy is equally raised in data-centric business models. The liability between the one paying for the data and the one using it, which is not always the same person, is a big issue for regulators, especially in the case of fraudulent activities.

"Uberisation" is not only an example of the new mobility services but also of the new business model of the new sharing and accessibility approach of the economy where data needs to flow in an open way. Concretely, uberisation is about shaping the model by usage, with the constant change of users, the behaviour of individual stakeholders, the use of disruptive technologies, such as the concept of having partially autonomous vehicles being shared, and working different transport models, under the same brand. There are different actors in uberisation, and the

cybersecurity implications are enormous which is also stretching the parameters of scope of existing legislation.

The collaborative approach should be applied to all aspects of the sector. For example, collaborative technology is extremely important in the field of autonomous vehicles and robotics. However, there are still levels of autonomy to be considered implying the necessity of an operating crew for optimisation purposes. This raises the problem of accountability though with regards to which human with which position should oversee the autonomous vehicle. Even the degree of human intervention should be carefully monitored. A data overload would overwhelm the human operators with too much information, not knowing the degree of reliability of the information to analyse. On the other hand, the issue of underload questions our degree of trust in the vehicle's sensing and alerting capacities to perform good driving, thus decreasing the level of attention of the humans. There are AI mechanisms that have algorithms that detect patterns, and there are humans to apply reason for a selective processing from experiences. Interfering with either of the two could be dangerous.

Equally dangerous is the trend of the cyber-physical systems. Those are the mechanisms that are controlled or monitored by computer-based algorithms. Such interactions between the AI and the machine should be flawless which would bring a higher efficiency and reliability to the systems in the transportation sector. However, any friction could create an incident.

Finally, a trend that is worth mentioning is the case of multimodal transport and multimodal transport operators, aka MTO. This concept denotes the transportation of goods by the same carrier, the MTO, using different modes of transportation. Even if the MTO is legally responsible for the entire process and the goods, the actual transportation and the different steps are undertaken by different actors, the sub-carriers. The multiplicity of actors involved increases the number of systems used, the legal implications of liability and the passage from one critical infrastructure operator to another. All these in turn increase the cybersecurity implications across systems and networks (snowball effect).

4.2 Critical Infrastructure Protection & OES

There is the need to have a holistic approach to security. If you miss out on just one crucial and asset-dependent topic in your risk assessment plan, there is the danger of leaving a gap in the security of your supply chain. Often the security of industrial systems is as good as the weakest link, and sometimes the security of the management system. For instance, while physical access management in a factory can be quite a challenge, in transportation, because of the road-side units, scattered infrastructure, and distributed systems, it will be even more of a challenge to supervise and secure. But at the same time, having facial recognition systems on board the vehicle, allowing multifactor authentication and decentralised access management and authentication, allows for an improved level of security. No system should be allowed to operate without proper credentials and authorisation. In addition, all the actions and events can be recorded, tracked and traced, or used for supervisory controls and monitoring of activities.

Critical infrastructure does not come from one single aircraft, train station, etc. By merely attacking the signalling (air traffic management, information centres, etc.), it would be possible to reach the full system, i.e. the enabling service, in order to disable the entire traffic. This implies that targets have different levels of criticality.

If we are heading towards more network transportation, we need more protection of infrastructure, meaning having common regulation and requirements on security. However, it remains tricky to have sectorial and cross-sectorial regulations. Duplication is a burden, but gaps are worse.

4.3 Regulations and Regulatory Developments

Regulation in the transportation sector is extremely fragmented at national, European and international level, and between the transportation sub-sectors themselves. For operators and manufacturers, the level of regulation is causing a burden for development and stifling innovation.

But equally so in operations. In the overlap between Members State and the European level, there are potential conflicts between the **GDPR** implementation and security requirements with regards to unique identity and user monitoring in some countries. In some cases, the GDPR itself can turn privacy against the security purposes. For Airbus, for example, there is an overload of procedure with regards to the specific implementation of GDPR in research projects, and their projects themselves become unmanageable time- and cost-wise. Such kinds of situations create a serious disadvantage for European companies in comparison with US companies that have a freer access to data.

The road transportation sector has its own specificities with regards to cybersecurity and data privacy as they consider that both are tightly interlinked. The abstract approach between vehicle data and data ownership raise questions on the usage of the data, for what purposes and by whom, and above all how to protect it in terms of GDPR. However, these considerations should not undermine GDPR. We need protection to create strong and secure systems, but the balance between the privacy and security objectives should be better calibrated.

National laws on **critical infrastructure protection** and/or essential services occasionally duplicate with pre-existing sectoral regulations as well. In the same vein, national laws on critical infrastructure protection tend to be a bit elitist and do not enforce minimal security level for all economic players. In France, for example, the ANSSI (French National Cybersecurity Agency) [48] has a national law that addresses transport sectors and is implementing the **NIS Directive**, though only for critical infrastructure (not taking into account aircrafts or railways for example). For the automotive and mobile sectors, they do not have any regulation for the moment.

These considerations create a weaker link which in a systemic perspective is enough to paralyse an economy. It also creates niche markets that do not enable economies of scale for the European industry, making a competitive disadvantage in comparison with other international actors such as the US.

For a homogenous European approach, a first cross-sector consensus would be to start with the identification of the operators of essential services (OES) and their scope for the application of regulations. Therefore, the NIS Directive is a good start as a high-level principle. Even more so, the NIS Directive and many national laws were released before the public-private exchange was initiated. This is a positive point, though also augments the risk of mismatch between the regulatory requirements, operator constraints and industrial capacities.

One important aspect to highlight is that the NIS is a Directive and not a Regulation. It guides every European Member State in transposing its requirements, such as the creation of their cybersecurity response teams or the identification of OES, in the best way possible. For the transportation sector, the NIS community is not exchanging with the transport community while at the same time it is up to each Member State to designate their OES. The transport community is not being concretely approached and remains in tiny clusters, working in silos.

From the European Commission side, several actions are being undertaken by the Directorate-General for Mobility and Transport (**DG MOVE**), the Directorate-General for Communications Networks, Content and Technology (**DG CNCT**) [49], and **ENISA**.

Aviation is likely the most regulated transportation sub-sector, while road appears to be the least developed. Thanks to DG MOVE, the European Commission adopted in September 2019 the Implementing Regulation (EU) 2019/1583 amending Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures. DG MOVE is also currently working on a draft legislation on preventive cybersecurity measures for the aviation sector, targeting both authorities and stakeholders. Recently, DG MOVE has also started to address the maritime sector which is drawing from lessons learned from the aviation sector. For the general transportation sector, DG MOVE had launched a call for tender to prepare a cybersecurity toolkit for all sub-sectors as well as Member States. They are now selecting the best offers to kick off and begin working from 2020.

DG MOVE is also working with ENISA to identify the different OES for the transportation sector and a thorough analysis should be completed by May 2021. For the moment, ENISA is in the process of addressing conflicts and complementarities in the regulation of the sectors. It is also closely following the NIS implementation by the Member States. The list of national public administrations, authorities and legislations can be found on the ENISA website [61].

At the **international level**, no general transportation regulation exists. It is rather driven by sub-sector specific international organisations with the aviation sector being the most developed. The ICAO is working to address the cybersecurity issue by encouraging authorities to take preventive measures. In 2018, they upgraded their recommendations to standards in an effort to move towards regulation. In this case, every contracted member of the ICAO, that is all 191 of them, must implement the rules, obliging players to identify their critical networks, systems and data, and set up the means to protect them. But not all of the important topics are covered, such as vetting and clearance issues, and not all contracting members are on the same level of strength. Nevertheless, the ICAO is approaching the cybersecurity issue from different angles and currently in the process of preparing a global aviation cybersecurity strategy, even if the criminal or individual aspects from operators are not considered. This could be an interesting example for the EU which is an observer at the ICAO.

Regulation in the **maritime sector** is extremely fragmented to the point that shipowners are lost in the number of rules coming from different regulators. These include the national legislations, the local inspections that vary from one harbour to another, the International Safety Management Code (ISM) [50], the International Maritime Organization (IMO), the CIRM (International Association for Marine Electronics Companies) or even the best practices issued by BIMCO, the international shipping association representing shipowners.

The ISM is currently upgrading its safety management for operating a ship to include the cyber component and the port management systems. The upgrade is under revision at the IMO. Even if most ships choose to comply with the IMO, there is complementarity coming from the ICS - International Chamber of Shipping that will make, as of 2021, the cybersecurity requirements mandatory for ships with regards to international shipping trade.

Reporting, or rather non-reporting or non-taking the duty of care of systems, is another issue in the maritime sector, which can cost up to 40% of the annual income for shipping companies. With the

data flow of information from the ship to the shore (e.g. notices of arrival, data on the crew, etc.), it is time to have general and enforceable rules and to put them as a best practice. With the multiplicity of stakeholders, a mixed governance structure would be advisable.

Market Study

The increasing risk of cyber-attacks has prompted the adoption of cybersecurity solutions among large companies. In 2017 only, the average cost of cyber-attacks rose by 11%. The use of smart logistics, IIoT, and other modernisation initiatives have further increased the risk by creating a wider attack surface from enormous systems. Any disruption in the operations of transportation and logistics companies can cause substantial downtime and loss of revenue. [51] The global cybersecurity market is expected to reach a worth of over $ 300bn by 2024 while the transportation market is expected to grow at a CAGR (Compound Annual Growth Rate) of over 15% over the projected timespan [52]. In 2017, Europe accounted for a 26.1% share of the cybersecurity market and this number will keep growing due to the rising public-private partnerships and government investments, though North America remains the leader in the share percentage of the global cybersecurity market. [53]

The global aviation cyber security market is expected to grow at a CAGR of 7.4% during the period 2017 to 2025. Despite the constraints, this high growth, that is to reach an estimated US$ 4,759.3 mn by 2025, is due to the mergers and acquisitions between big global players (such as Thales) but also to the increasing number of airports that make connectivity feasible and the entry of small players in the aviation sector. High investments are needed to deploy cybersecurity systems across any airport. Small players or new entrants may face difficulties to get them up and running into their system though [54].

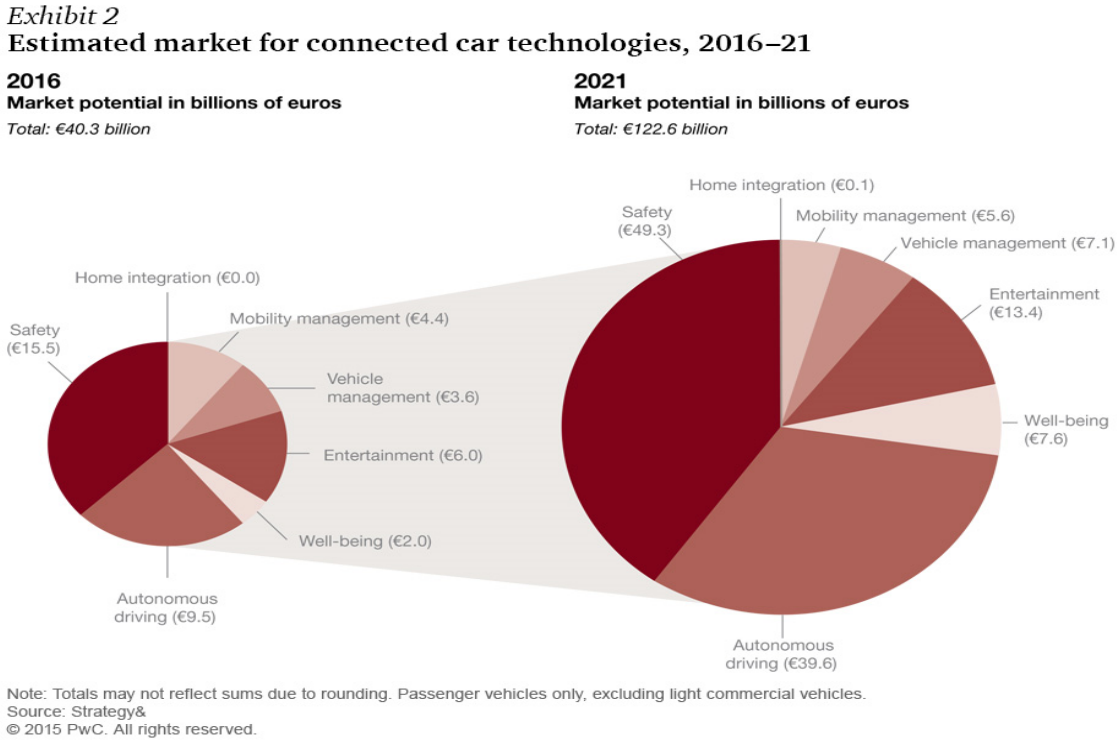
According to the ICAO, airlines spend an average of 7% of their overall IT budget on cybersecurity, compared to a higher airport investment at 10%. However, cybersecurity costs were estimated at 9% and 12% respectively in 2018. This reflects the rising importance of protecting data and systems from unauthorised access showing that regulatory compliance and data privacy regulation are among the highest priorities. A recent shift in trend also shows growing investment towards detection and response. When tackling cybersecurity, the air transport industry faces similar challenges to other industries: a lack of resources, budget and skills [55].

In the railway sector, increasing digitalisation and a growing number of smart railway systems will drive the demand for infrastructural railway cybersecurity across the globe. The global railway cybersecurity market is estimated to grow at a CAGR of 9.8%, from USD 6.0 bn in 2019 to USD 12.6 bn by 2027. Adoption of IoTs and automation technologies to enhance the efficiency in the optimisation of the sub-sector, as well as the increasing number of government and PPP-model initiatives are among the biggest drivers of the railway cybersecurity market. Other factors include the increase in the user preference for urban transportation and the growing demand for convenient transport. Major European actors for railway include Siemens, Nokia, Thales, Alstom due to their long-term supply contracts with leading service operators and are involved in the development of strategies and new products, acquisition and collaborative partnerships, etc. to get a grasp of the railway cybersecurity market. [56]

Data on the maritime industry remains scarce. However, according to a study carried out in the US maritime industry, the maritime industry has a well-established and impressive safety record. But when it comes to cyber threats, the study found that, especially among SMEs, there is a considerable gap between possessing the information (knowing) and taking concrete actions on it (doing). The industry is not as prepared as it must be to prevent and address damaging cyber-attacks. Currently, cybersecurity budgets are small, with the majority of companies spending 1 to 2 percent

of their overall budget on cybersecurity. There is only a small portion of industry stakeholders in the maritime sector that are actively engaged in cybersecurity collaboration and information-sharing programs. [57]

In the road sector, the number of cars connected to the internet keeps growing rapidly. The estimated global market for automated vehicles is 44 million vehicles by 2030. [58] The total market size and potential of connected passenger vehicles is forecasted of € 122.6 billion in 2021, three times of what was estimated for 2016. The highest market opportunities are coming from safety and automated driving.



Source: PwC

According to a study from STRATEGY& PWC, the market of connected vehicles will grow from 31,87 billion € to 115,2 billion € between 2015-2020 worldwide. This market will be driven primarily by safety considerations. The safety segment alone is expected to grow from 12,18 billion € in 2015 to 47,37 billion € by 2020. [59]

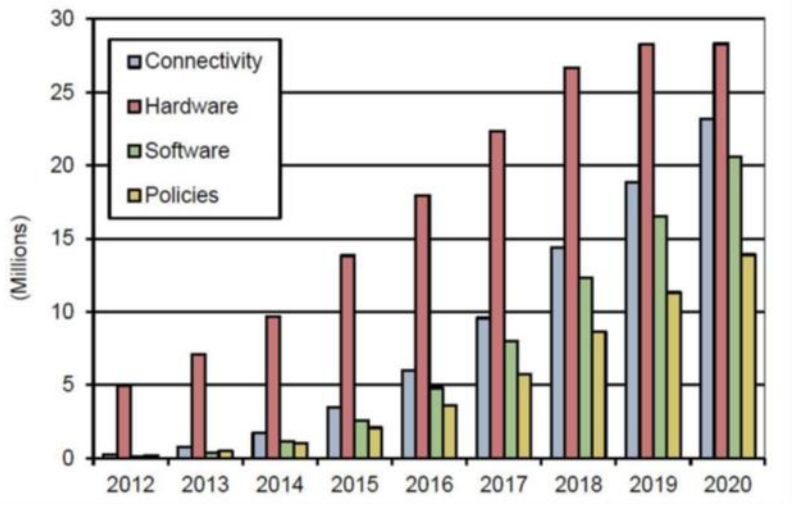
Buyers remain reluctant to use connected car services due to concerns regarding privacy and security. A survey has shown that 37% of the respondents were concerned due to privacy reasons, 54% regarding security. [60] Hence, security and privacy are seen as key enablers for the market uptake of connected solutions in vehicles.

According to a market study of ABI Research on “Connected Car Cybersecurity” (February 6, 2014), new vehicle shipments with integrated security applications will be equipped with four types of security technology:

- Connectivity: VPN, encryption, authentication
- Software: Virtualisation, sandboxing, on-line monitoring

- Hardware: Separation (firewalls), locks, secure memory
- Policies: Security auditing and risk management

The number of vehicles shipped worldwide with security technology until 2020 is expected to grow annually by 15% to 53%, depending on the type of security technology used. In Europe, growth is expected to be slightly higher (17% to 55%). Hardware separation will remain the dominant security technology, connectivity and software-based security and security policies were predicted to become mainstream by the end of 2020.



Conclusion

The diversity of the transportation sector as a result of differences in the way its sub-sectors of road, rail, air and maritime are organised is very representative of the state of cybersecurity this sector is currently in. While some car manufacturers take cybersecurity very seriously, Air Traffic Management are trying to develop industry standards, and maritime ports are organising cyber physical exercises, there are giant gaps between and within the sub-sectors.

The eagle-eye-perspective on the high-level state of affairs of the transportation sector this document represents clearly identifies two major developments. First, there are people, organisations, operators and manufacturers aware and actively working on cybersecurity measurers, trying to organise ways to mitigate potential risks by identifying and taking proactive measures in order to avoid major incidents.

But all these actions, effort, energy, time and other resources turn pale when put into the context of legacy systems and operations, sloths and traditions. The cybersecurity components being put in place are shimmering lights in a blue sky, targeting pin-point actions but mostly only a drop of water on a hot plate. Notwithstanding, these efforts should be further applauded and used as reference for the whole industry to carry along.

While transportation - like any other sector - is confronted with societal challenges linked to the ecological footprint, circular and sharing economies, digitalisation and fragmentation, its infrastructures sometimes date back to the 19th century. However, from a sectoral perspective, there are key things to learn from both the sub-sectors and other sectors when considering cybersecurity. A sub-sectoral approach continues to be needed, by starting to push for a can-do approach and ensuring the implementation of policies that consider cybersecurity for all operations. This risk-based approach should lead to a better understanding of the risks but will also help identify major and minor risks per subsector, where possible solutions might already exist.

The challenge identified throughout the report that safety and security come first before any other operation, clearly stifle the potential for innovation. While the approach can be applauded, the sector will need to consider a more agile approach on all levels. Recent incidents with rail (Belgium, Buizingen 2010, Wetteren 2013), cars (GPS in 2019, remotes in 2019, BMW, Hyundai, 2019, Jeep 2015, Tesla 2019, …), airports (Gatwick, 2018), and airplanes (Boeing 737 Max, 2019) have shown that these security and safety measures can also be circumvented, misled, and provide false senses of safety and security. Sometimes human errors can lead to major incidents, sometimes the lack of interactions and communication could cause adverse effects.

Apart from this, there continue to be many cybersecurity challenges which are also prevalent for any other industry. Vulnerabilities both for cybersecurity and privacy protection from new technologies are omnipresent, but they are being considered. Vulnerabilities can be managed. Methodologies, best practices and other technologies exist to prevent, detect, mitigate and remediate potential breaches and incidents. This active cyber defence approach, which is already being applied in various transportation sectors, should be considered sector wide. Standards and standard operating procedures allow for discussion and debate and allow visions to converge over time. But these standards must be supportive of an agile, proactive approach to cybersecurity.

An overall policy recommendation for the transportation sector and its sub-sectors is missing, including the required oversight mechanism that continuously assesses and judges the approaches taken on the overall management and actions being taken. Such policy recommendation, with clear and direct objectives, should be taken up by the European Commission, Member States and the various sectorial representations and respective boards of the transportation sector bodies. In this respect, policy has a significant role to play, as many of the infrastructures (sea, air, road, ports, traffic management, …) are being managed by the Member States and include multiple supervisory bodies. The skills they require can be supported by the industry skills, calling for independent cybersecurity advisors. This might well be an addition to the challenging security and safety aspect and can also lead to a weighted and balanced approach, but it should at least become transparent and dealt with. Beyond Critical Infrastructure Protection and Essential Services, transport is one of the core elements of our societal and economic fabric. Without electrical power, there will be reduced service and massive road chaos. Without data infrastructures, there will be complete service disruption and lack of safety. But without transportation, there won't be supplies for energy, data infrastructures, food and waste. An active cybersecurity policy should be taken up by organisations and companies servicing and providing products to transport, considering their small contribution to cybersecure means of transportation. They should be held responsible when not being able to provide a significant means within their realms, and they should be rewarded when they do provide it. These continuous small steps will finally light up the whole sky and help provide a more cybersecure transportation sector.

While in this 21st century we are making progress in transport to Space, we seem to be stuck with systems from the past in other transportation means. But both innovation and new approaches can be used to improve the current means and identified challenges can be handled with intelligence and best practices from other sectors. While this document is a state of the current affairs, it calls for continuity in order to provide further transparency, share best practices and means, provide insights in new and upcoming challenges, and support in bringing various stakeholders around the table that otherwise would not happen at all. The results of these discussions can lead to policy recommendations, contributions to cybersecurity standards which can become cross-sectorial and calls for new cybersecurity research developments.

This document considered the main transportation nodes road, rail, sea and air, and tried to highlight the cybersecurity aspects specific to the domain by considering:

- Domain specific risks and framework for cyber risk, integration with domain
- The secure-to-fail design (Everything that can be hacked will be hacked) philosophy
- That safety issues/aspects are continuously weaved with cybersecurity
- That more than in other sectors stronger defence is needed towards cyber-physical (and side channel) attacks
- The absolute necessity of patches and firmware agility
- Ensuring human involvement, which is crucial in the complexity of infrastructures and outdated systems.

Many policies and procedures exist, many standards and standard operating procedures exist and have a significant impact if they are implemented properly and when organisations and people are being held accountable for them. Transportation and many other sectors are served in the first place with a recommendation towards personnel on all layers, with all organisations involved in the sector to set out a "light" policy. Its weight should not be considered because of its impact, but

thanks to sticking to the following 5 major guidelines, people not dealing with information technology but acting as the responsible employee or business partner in trying to make their sector more cybersecure, will be better placed to tackle today's challenges:

1. Consider cybersecurity in all day to day operations and activities and report about concerns and considerations for improvements, even with limited in depth understanding of cybersecurity
2. For all new developments, ensure cybersecurity is being considered and at least debated; ensure there is a design plan template that considers cybersecurity and privacy
3. Identify a series of risks and potential vulnerabilities from your perspective, document them and consider them periodically for updates. Ask yourself if progress is being made.
4. Take a preventative measure and document it. This can be as small as notifying that access control should be improved, not allowing everybody using the same username and password. You can help by removing the post-it notes with passwords from your colleague's screen.
5. Share cybersecurity intelligence and consult with your peers. Share the previous experiences with other divisions and organisations, exchange ideas and best practices, and support people in doing so.

Following these recommendations in both legacy and high-tech domains and applications in the sector will allow for small, but sometimes first steps, in a change process that could take some time, but at least where progress is being envisaged.

Over time it is likely that more procedures and regulations will follow, that harder and stronger measures will be required and that more cybersecurity challenges will appear. It won't be wise to stop innovation and digital transformation or any of its future forms of evolution, as it will be hard to stop the evolution of the transportation sector and all its sub-sectors. Slowing it down could even cause more adverse effects than anticipated. But it will be wise to consider at least the positive effects of cybersecurity throughout the process and value chains, and to continuously improve all – even the small – steps.

We must understand and acknowledge that all of our transportation means are genuinely not cybersecure, and that a lot of efforts will be needed to improve its cybersecurity. Measures are needed, where exactly to focus on first is the topic of another series of studies, but at least on the top and the bottom of the organisation, by integrating it in any new development taking place, and by using the state of the art cybersecurity technologies of the moment, organisations will be on the right path.

For ECSO, SWG 3.3 Chairs, February 2020

References

[1] ENISA, “Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations” (January 2016). https://www.enisa.europa.eu/publications/good-practices-recommendations

[2] ENISA, “Securing Smart Airports” (December 2016). https://www.enisa.europa.eu/publications/securing-smart-airports

[3] ENISA, “Cyber Security and Resilience of smart cars” (January 2017). https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

[4] Shift2Rail, “CYRail Recommendations on cybersecurity of rail signalling and communications systems” (September 2018). https://cyrail.eu/IMG/pdf/final_recommendations_cyrail.pdf

[5] BIMCO & al., “The Guidelines On Cyber Security Onboard Ships” (December 2018). https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=20

[6] ICAO, “Aviation Cybersecurity Strategy” (October 2019). https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf

[7] ENISA, “Port Cybersecurity - Good practices for cybersecurity in the maritime sector” (November 2019). https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

[8] Directorate-General for Mobility and Transport (DG MOVE), European Commission, https://ec.europa.eu/transport/home_en

[9] CAESS (2017) “Comprehensive Experimental Analyses of Automotive Attack Surfaces”; August 2011. http://www.autosec.org/publications.html.

[10] WIRED (2015), “Hackers Remotely Kill a Jeep on the Highway - With Me in It”. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway & Dr. C. Miller and C. Valasek (2015), “Remote Exploitation of an Unaltered Passenger Vehicle”. http://illmatics.com/Remote%20Car%20Hacking.pdf

[11] European Commission – Press Release (2016), “Road Safety: new statistics call for fresh efforts to save lives on EU roads”, accessible online: http://europa.eu/rapid/press-release_IP-16-863_en.htm

[12] ERTMS - European Rail Traffic Management System, http://www.ertms.net/

[13] UNIFE – The Association of the European Rail Industry, http://www.unife.org/

[14] ERA - European Union Agency for Railways, https://www.era.europa.eu/

[15] Shift2Rail, https://shift2rail.org/

[16] CENELEC - European Committee for Electrotechnical Standardization, https://www.cenelec.eu/

[17] ENISA - European Union Agency for Network and Information Security, https://www.enisa.europa.eu/

[18] Airbus, Skywise, https://www.airbus.com/aircraft/support-services/skywise.html

[19] ICAO – International Civil Aviation Organization, https://www.icao.int/

[20] EASA - European Aviation Safety Agency, https://www.easa.europa.eu/

[21] EUROCONTROL, https://www.eurocontrol.int/

[22] "SWIM – System Wide Information Management", CMAC CNS Technical Leaflet #10, EURO-CONTROL Directorate Air Traffic Management (https://www.eurocontrol.int/sites/default/files/publication/files/201704-swim-civ-mil-leaflet_0.pdf)

[23] EUROCONTROL, EACCC – the European Aviation Crisis Coordination Cell, https://www.eurocontrol.int/articles/european-aviation-crisis-coordination-cell-eaccc

[24] European Commission, European Aviation Crisis Coordination Cell – EACCC. https://ec.europa.eu/transport/modes/air/single_european_sky/eaccc_en

[25] ACARE - Advisory Council for Aviation Research and innovation in Europe, https://www.acare4europe.org/about-acare

[26] Chiappetta A. (2017). HYBRID PORTs: the role of IoT and Cyber Security in the next decade; Journal of Sustainable Development of Transport and Logistics, 2(2), 47-56. doi:10.14254/jsdtl.2017.2-2.4.

[27] International Group of P&I Clubs, https://www.igpandi.org/

[28] IACS - International Association of Classification Societies, http://www.iacs.org.uk/

[29] Classification Societies, http://maritime-connector.com/wiki/classification-society/

[30] CSO Maritime Alliance – Chief Security Officer Alliance, https://csomaritimealliance.com/

[31] ACEA - European Automobile Manufacturer's Association, http://www.acea.be/

[32] CLEPA - European Association of Automotive Suppliers, http://clepa.eu/

[33] CORTE - Confederation of Organisations in Road Transport Enforcement, http://www.corte.be/

[34] ETSC - European Transport Safety Council, http://etsc.eu/

[35] IRU - World Road Transport Organisation, https://www.iru.org/

[36] ITF - International Transport Forum, https://www.itf-oecd.org/

[37] ACI Europe - Airports Council International – Europe, https://www.aci-europe.org/

[38] ECAC - European Civil Aviation Conference, https://www.ecac-ceac.org/

[39] ERRAC - European Rail Research Advisory Council, https://uic.org/research/european-rail-research-advisory-council-errac/

[40] UIC – International Union of Railways, https://uic.org/

[41] BIMCO, https://www.bimco.org/

[42] CIRM – The International Association for Marine Electronics Companies, http://www.cirm.org/

[43] ICS - International Chamber of Shipping, https://www.ics-shipping.org/

[44] IMO - International Maritime Organization (IMO), http://www.imo.org/fr/Pages/Default.aspx

[45] H2020 project Cognitive Heterogeneous Architecture for Industrial IoT Deliverable 1.4 CHARIOT Design Method and Support Tools.

[46] ARM Holdings, https://www.arm.com/

[47] ARM Holdings (2018), "A Firmware Update Architecture for Internet of Things Devices", https://tools.ietf.org/id/draft-moran-suit-architecture-01.html

[48] ANSSI - French National Cybersecurity Agency, https://www.ssi.gouv.fr/en/

[49] Directorate-General for Communications Networks, Content and Technology (DG CNCT), European Commission, https://ec.europa.eu/info/departments/communications-networks-content-and-technology_en

[50] ISM - International Safety Management Code, http://www.imo.org/en/OurWork/HumanElement/SafetyManagement/Pages/ISMCode.aspx

[51] MarketWatch, "At 12% CAGR, Cybersecurity Market Size will reach 300 billion USD by 2024", 13 February 2019, https://www.marketwatch.com/press-release/at-12-cagr-cybersecurity-market-size-will-reach-300-billion-usd-by-2024-2019-02-13

[52] PR Newswire, "Cybersecurity Market Worth Over $300bn by 2024: Global Market Insights, Inc.", 16 January 2019, https://www.prnewswire.com/news-releases/cybersecurity-market-worth-over-300bn-by-2024-global-market-insights-inc--863930577.html

[53] Global Market Insights (January 2019), "Cybersecurity Market Trends - 2024 Industry Statistics Forecast", https://www.gminsights.com/industry-analysis/cybersecurity-market?utm_source=prnewswire.com&utm_medium=referral&utm_campaign=Paid_prnewswire

[54] Bloomberg, "Aviation Cyber Security Market Worth US$ 4,759.3 Mn by 2025; Technological Advancements to Make the Market Fly High – TMR", 17 May 2019, https://www.bloomberg.com/press-releases/2019-05-17/aviation-cyber-security-market-worth-us-4-759-3-mn-by-2025-technological-advancements-to-make-the-market-fly-high-tmr

[55] SITA, 2018 Air Transport Cybersecurity Insights (2018), https://www.icao.int/NACC/Documents/Meetings/2018/CSEC/D12b-AirTransportCybersecurityInsights2018-SITA.pdf

[56] Research and Markets (June 2019), "Railway Cybersecurity Market by Type (Infrastructural and On-board), Solutions and Services, Security Type (Network, Application, End Point, System Administration, and Data Protection), and Region - Global Forecast to 2027", https://www.researchandmarkets.com/reports/4774865/railway-cybersecurity-market-by-type?utm_source=CI&utm_medium=PressRelease&utm_code=7x2dh9&utm_campaign=1267309+-+Global+%2412.6+Bn+Railway+Cybersecurity+Market+to+2027+-+Major+Players+are+Thales%2c+Alstom%2c+Siemens%2c+Bombardier%2c+and+Nokia+Networks&utm_exec=chdo54prd

[57] Jones Walker LLP (2018), "Maritime Cybersecurity Survey", https://cdn2.hubspot.net/hubfs/4386046/Collateral%20-%20Whitepapers/2018%20Jones-Walker%20LLP%20Maritime%20Cybersecurity%20Report.pdf

[58] ERTRAC (2015), Automated Driving Roadmap. http://www.ertrac.org/uploads/documentsearch/id38/ERTRAC_Automated-Driving-2015.pdf

[59] PWC (2015), Connected Car Study: Racing ahead with autonomous cars and digital innovation, accessible online: https://www.strategyand.pwc.com/media/file/Connected-Car-Study-2015.pdf

[60] McKinsey (2014), Connected Car Consumer Survey.

[61] ENISA (2019, NIS Directive Tool, accessible online: https://www.enisa.europa.eu/topics/nis-directive/nis-visualtool

[62] ICAO, “Twelfth Air Navigation Conference: Cyber Security for Civil Aviation” (November 2012) https://www.icao.int/Meetings/anconf12/WorkingPapers/ANConfWP122.1.1.ENonly.pdf

[63] Costin, Andrei, and Aurélien Francillon. "Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices." *Black Hat USA* (2012): 1-12. https://media.blackhat.com/bh-us-12/Briefings/Costin/BH_US_12_Costin_Ghosts_In_Air_WP.pdf

[64] Balduzzi, Marco, Alessandro Pasta, and Kyle Wilhoit. "A security evaluation of AIS automated identification system." *Proceedings of the 30th annual computer security applications conference*. 2014.

Acknowledgments

This report was initiated in 2018 and completed in December 2019. Its publication has been possible thanks to information provided by different contributors in the context of the ECSO SWG3.3 “Transportation” and through workshops organised by ECSO in February 2017, February 2019 and July 2019.

MAIN EDITORS - ECSO Secretariat	
Nina HASRATYAN	Policy Manager
Nina OLESEN	Senior Policy Manager

MAIN CONTRIBUTORS – ECSO Members	
Adrien BECUE	AIRBUS (SWG3.3 co-chair *by interim* for 2018-2019*)*
Ulrich SELDESLACHTS	LSEC (SWG 3.3 co-chair *by interim* for 2018-2019)
Sadio BÂ	ANSSI (French National Cybersecurity Agency)
Andrea CHIAPPETTA	ASPISEC
Andrei COSTIN	University of Jyvaskyla / binare.io
Janine DOBELMANN	NXP Semiconductors
Christopher HENNY	AIRBUS/Maxess SPRL
Pouria Sayyad KHODASHENAS	I2CAT Foundation
Gabriele RIZZO	Leonardo
Rémy RUSSOTTO	CORTE
Jayant SANGWAN	CORTE
Eva SCHULZ-KAMM	Siemens (formerly NXP Semiconductors)
Lorraine WILKINSON	EOS

Thorsten WOLLWEBER	AIRBUS APSYS

MAIN CONTRIBUTORS - External partners	
Athanasios DROUGKAS	ENISA
Christophe GRANSART	IFSTTAR & ERRAC
Hana GUYAUX-PECHACKOVA	DG MOVE, European Commission
François HAUSMAN	Shift2Rail
John HIRD	EUROCONTROL
Dennis KUTSCHKE	Continental Automotive
Jérôme MORANDIERE	ACI Europe
Francisco PASTRANA	Shift2Rail
Markus TSCHERSICH	Continental Automotive

> JOIN ECSO

10, RUE MONTOYER - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE: WWW.ECS-ORG.EU - TWITTER: ECSO_EU