Automotive Security Testing

An overview of compliance and best practices in automotive security testing

Filippo Capocasale | Director,
Filippo.Capocasale@nttdata.com

Lorenzo Sicignano | Senior Cybersecurity System Engineer,
Lorenzo.Sicignano@nttdata.com

Francesco Gozzoli | Cybersecurity System Engineer,
Francesco.Gozzoli@nttdata.com

Security Business Service Line
NTT DATA Italia

Index

Abstract

This white paper explores the emerging topic of "Automotive Security Testing", providing a detailed overview of the methodologies and techniques used to assess and improve cybersecurity in automotive systems (components, vehicles and the connected ecosystem).

The paper focuses on recommendations coming from guidelines, standards and regulations, as well as the description of testing methodologies typically applied in the automotive domain. The ambition is to provide an overview of this important topic and even a practical guidance for better organize structured testing campaigns to guarantee a proper level of cybersecurity in modern automotive systems.

The document is structured as follows:

1. The first chapter gives a general introduction and background that highlight the importance of security testing for automotive systems.
2. In chapter two there is a description of domain specific guidelines, standard and regulations where security testing is involved.
3. The third chapter describes the types of vulnerabilities and threats and the concept of security testing.
4. The fourth chapter describes the frameworks used for the exhaustive performance of security testing. The basic steps for a structured execution of testing activities are also explained.
5. In the fifth chapter, an overview of the different possible techniques for security testing is given, highlighting the different types and their direct link to compliance with Annex 5 of UNECE Regulation R.155. This chapter also reports NTT Data's approach to the different types of security testing illustrated.
6. In the sixth chapter there is a general recap leading to final considerations about security testing and their prospects.

1 Introduction

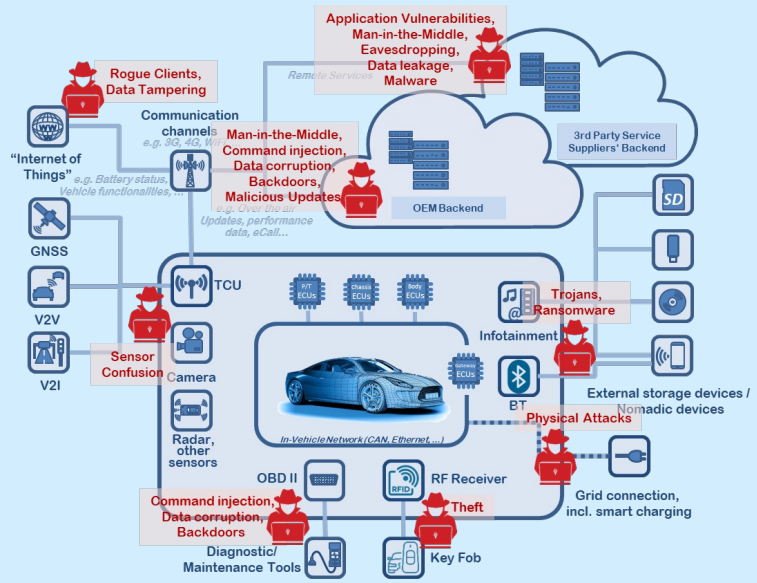
1.1 Overview on Automotive Security Testing
1.2 The importance of Security in the digital era

In the recent decades we observed a great evolution in the automotive domain: the introduction of more and more electronics and advanced technologies to support new features, the advent of connected vehicles and the prospect of autonomous mobility, are radically transforming the automotive industry. These innovations offer countless benefits in terms of comfort and performances, but at the same time introduce cybersecurity-related challenges.

As vehicles become increasingly interconnected to take advantage of an entire connected ecosystem of services and facilities, cyber-threats may put at risk vehicles, the infrastructure, user's privacy and even the safety of drivers, passengers and all road users.

Modern vehicles are equipped with a wide range of electronic components and software, which may be vulnerable to cyber-attacks. It has been practically demonstrated[1] that a compromised vehicle might be subject to remote control by hackers, putting the safety of the people on board at risk. Moreover, with the increasing adoption of autonomous driving technologies, automotive security becomes even more critical. An autonomous vehicle must be able to make quick and safe decisions, ensuring maximum reliability to avoid traffic accidents. Automotive security is also essential to protect sensitive data collected by connected vehicles. This data includes personal information, geo-location data and other sensitive information that must be treated with the maximum security and confidentiality.

Figure 1 - Attack Surface of connected vehicles



1. IOActive, "Remote Exploitation of an Unaltered Passenger Vehicle", https://ioactive.com/wp-content/uploads/2018/05/IOActive_Remote_Car_Hacking-1.pdf

2 Standards, Regulations and Guidelines for Security Testing

There are several recognized guidelines, standards and regulations in the automotive industry specific for cybersecurity: most of them highlight the importance of security testing to demonstrate and guarantee an appropriate level of cybersecurity in automotive systems. In these chapter an overview of these documents is provided.

2.1 Guidelines

Several entities have published guidelines about automotive security: such guidelines are documents that offer guidance and recommendations for ensuring the security of vehicles and their associated electronic systems. There are guidelines covering several key areas, including risk management, security testing, data protection, and compliance with industry regulations.

Domain specific best practices aim to ensure that vehicles - and, recursively, all their subsystems and components - are designed, developed, operated and updated in a secure manner, reducing the risk

We report hereafter some best practices recommendations:

Integration of security into software design and development

In the ever-evolving automotive ecosystem, the integration of security into the embedded software development process, referred to as security-by-design, has become a key cornerstone. The increasing complexity of embedded systems in vehicles requires a holistic approach to security, in which information protection and data privacy aspects are considered early in the development cycle. Incorporating security considerations from the outset not only helps identifying and resolving vulnerabilities in a timely manner, but also helps reduce the costs and risks associated with late fixes. This proactive approach requires active involvement of developers and security engineers throughout the process, ensuring that software development best practices and security guidelines are applied at every stage, from design to software deployment.

Continuous testing and DevSecOps

The adoption of continuous testing practices, in synergy with the DevSecOps approach, plays a crucial role in managing security challenges. Implementing a continuous testing process enables early identification of emerging vulnerabilities and potential security gaps. Collaboration between development and operations teams through the DevSecOps model ensures that testing is performed automatically and regularly, seamlessly integrating into the software development and deployment phases. This synergy facilitates timely detection and resolution of security issues, promoting an approach to cyber threat management in the automotive industry.

Vulnerability and bug management

Effective management of vulnerabilities and bugs is a key element in ensuring the security of automotive systems. The rapid identification, assessment, and mitigation of vulnerabilities is essential to prevent potential security breaches. A structured process for vulnerability management involves recording and classifying detected vulnerabilities, determining their potential impact, and establishing appropriate action plans.

Security training and awareness

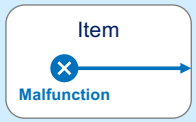
Security training and awareness play a crucial role in ensuring that everyone involved in the development, production, and usage of automotive systems understands the importance of cybersecurity. Awareness of cyber threats and security best practices is critical to preventing human error and risky behaviour. Organizing regular training programs and disseminating relevant security information helps to maintain a high level of awareness and involvement of all stakeholders, thus contributing to the creation of a safer environment for connected and autonomous vehicles.

Among several guidelines published on the topic of automotive cybersecurity, the ISO 26262 had great relevance as it was the first attempt to cover domain-specific safety aspects in a comprehensive and structured way. After this document, a more specific one was written in cybersecurity aspect, the SAE J3061.

2.1.1 ISO 26262

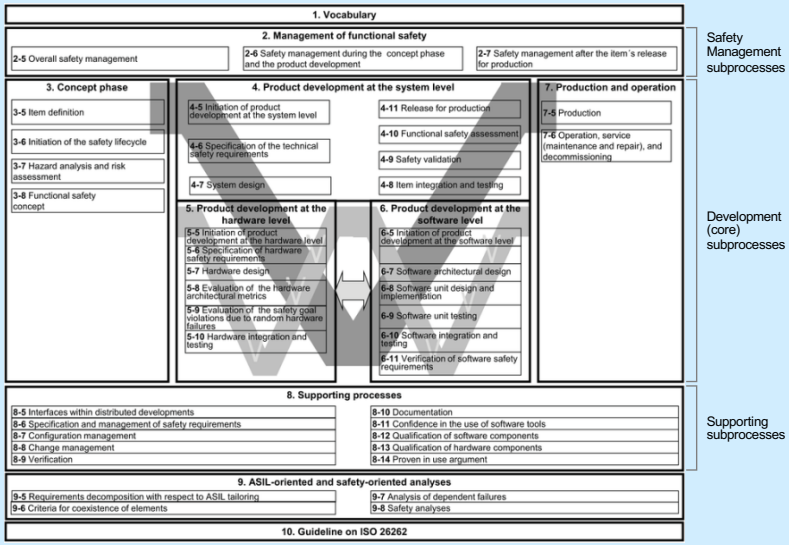
ISO 26262 “Road Vehicles Functional Safety” is an automotive-specific international standard dealing with functional safety of on-board electrical and electronic systems. It is mainly focused on safety-critical systems, on possible “malfunctions” in an “item” which may lead to a “hazard”:

Figure 2 - Focus of ISO 26262



The Functional Safety of a system is related to its robustness, resiliency and correct responses to input, taking into account possible hardware faults, software errors, interaction with humans and the external environment. The approach to functional safety is intrinsically end-to-end in scope since the function of a component or subsystem has to be considered as part of the function of the whole system. ISO 26262 provides recommendations that should be applied throughout the entire product lifecycle, from conceptual development to final decommissioning. ISO 26262 is based upon a system-development V process model.

Figure 3 - ISO 26262 process framework



2.1.2 SAE J3061

Since Cyber-Security is not sufficiently addressed in ISO 26262, the Vehicle Electrical System Security Committee (VESSC) at the International Society of Automotive Engineers (SAE) has published, on purpose, the new J3061 Standard, in January 2016. Strictly speaking, SAE J3061 is a “Cyber Security Guidebook for Cyber-Physical Vehicle Systems”, containing a set of high-level guiding principles for Cyber Security as it relates to automotive cyber-physical systems. SAE J3061 is “built upon” ISO-26262, and inherits the main characteristics of its approach, but it focuses on “threats” to a “feature” and their related “risks”:

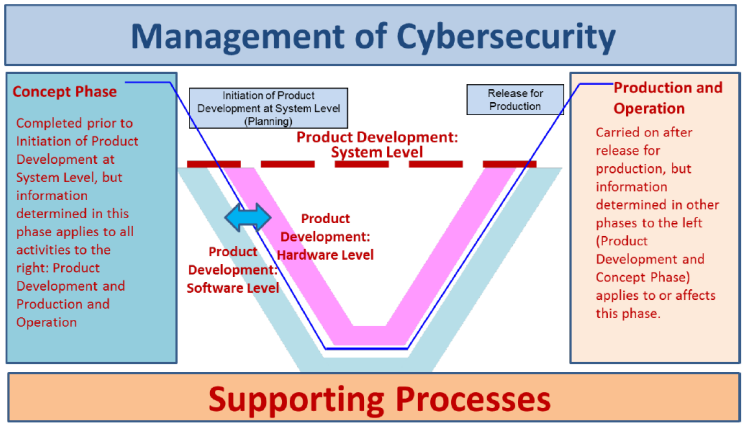
Figure 4 - Focus of SAE J3061

The scope of Cyber-Security is somehow broader than the one of Functional Safety:

- all safety-critical systems are cybersecurity-critical systems, but not all cybersecurity-critical systems are safety-critical;
- cyber-security takes also care of aspects (such as privacy) that are not directly related to safety.

According to SAE J3061, a comprehensive and effective Security approach must be applied during the whole lifecycle of a vehicle (and its parts): from the initial concept phase, through product development, and then production, operation, service and decommissioning.

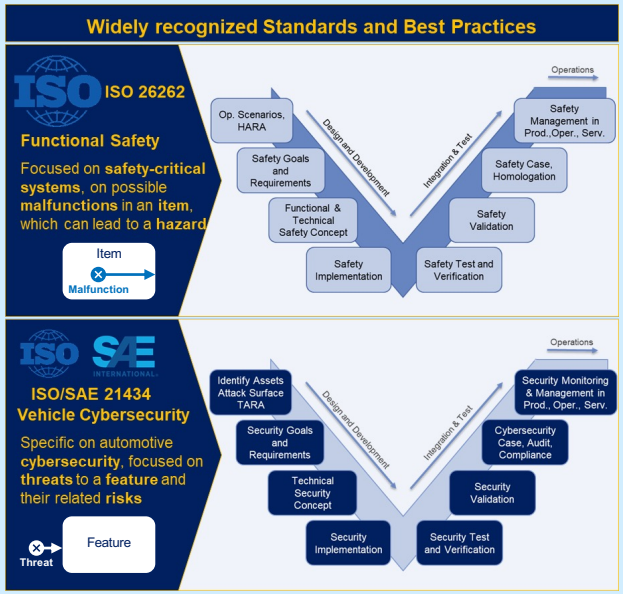
Figure 5 - Overall cyber-security process framework of SAE J3061



2.2 Standards

The main standard regarding Automotive Cybersecurity is the ISO/SAE 21434, that is a refinement and evolution of the SAE J3061 and a harmonization with the ISO 26262.
It establishes criteria and procedures for assessing, identifying and mitigating cybersecurity-related vulnerabilities and threats in electronic and connected vehicles; it also provides a structured and methodological framework for conducting in-depth security testing of vehicle systems, components and networks to ensure data protection, confidentiality, integrity and availability of systems, as well as safety of passengers and road users.

Figure 6 - Safety and Security Automotive Best Practices



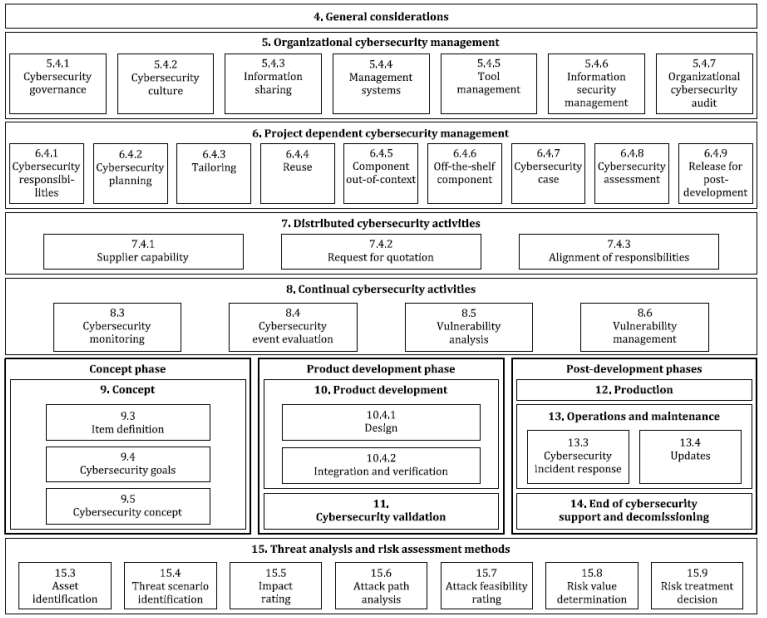
2.2.1 ISO/SAE 21434

Two guidelines, ISO 26262 and SAE J3061, have deeply influenced the creation and content of ISO/SAE 21434. Recognizing the intricate relationship between functional safety and cybersecurity, this standard elegantly integrates concepts from both ISO 26262 and SAE J3061.

ISO/SAE 21434, known as "Road vehicles - Cybersecurity Engineering," is the first real standard that sets principles and guidelines tailored for cybersecurity engineering concerning road vehicles. This standard, widely recognized in the automotive sector, testifies the growing attention on cybersecurity in a domain that increasingly relies on software-driven components, complex electronics and connected functionalities.

ISO/SAE 21434 delineates embedding cybersecurity measures from the very beginning. This pre-emptive approach ensures that security is an intrinsic part of the development and not a later task. The document highlights the importance of aligning security objectives throughout the entire lifecycle of the vehicle, starting from the conception phase, progressing through design and production, up to the post-production phase which includes maintenance, updates, and eventual decommissioning.

Figure 7 - ISO/SAE 21434 Framework

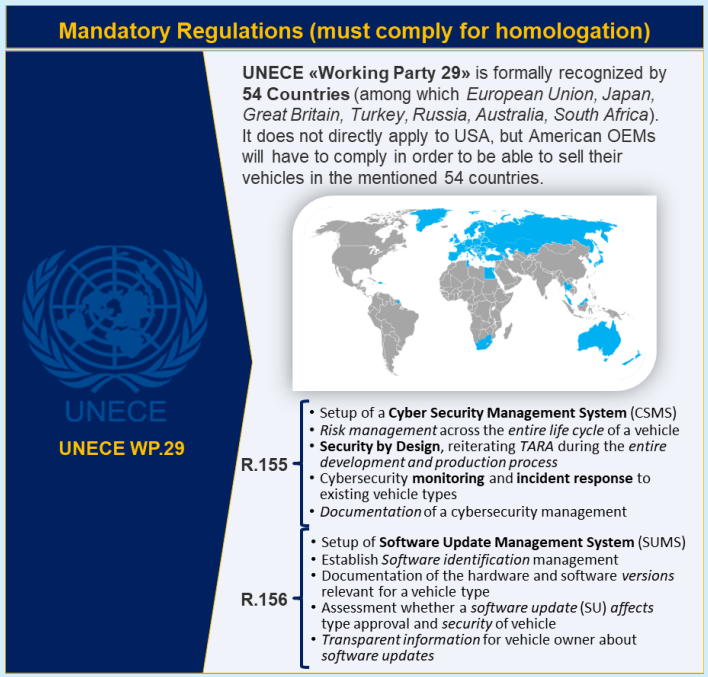


This holistic approach, supported by ISO/SAE 21434 ensures that potential vulnerabilities are not only identified but also addressed in a timely and efficient manner.
The standard provides a comprehensive, versatile and multifaceted testing regime. By endorsing methodologies such as penetration testing, it allows organizations to simulate real-world attack scenarios to measure their defences. The emphasis on static and dynamic code analysis underscores the necessity of an in-depth examination. Furthermore, the standard acknowledges the interconnected nature of hardware and software components and promotes rigorous testing regimes for both to ascertain that they do not introduce vulnerabilities when working in conjunction.
Lastly, the inclusion of vulnerability and risk assessment procedures in the standard testifies to its comprehensive nature: by guiding entities to evaluate the severity and likelihood of potential threats, ISO/SAE 21434 helps in prioritizing mitigation efforts, ensuring that resources are allocated effectively.
ISO/SAE 21434 is not just a standard—it's a roadmap for the automotive industry to navigate the intricate and critical realm of cybersecurity, ensuring the safety and trust of its stakeholders.

2.3 Regulations

Government organizations and regulatory authorities have issued directives and laws, in order to ensure high safety and cybersecurity standards in road vehicles.
The UNECE regulation entered into force from June 2022; at the time being, car manufacturers must demonstrate that they have integrated cybersecurity aspects into the framework of their processes, to obtain the “type approval” (homologation) for new models; from June 2024 they will have to demonstrate and document the effective application of the cybersecurity framework in their development processes to proceed with the registration of new cars.

Figure 8 - UNECE wp.29 R155 and R156 Overview



2.3.1 UNECE R155

"UNECE Regulation No. 155 on the Safety of Connected Vehicles" is a normative issued by the United Nations Economic Commission for Europe (UNECE) that focuses on the security of connected vehicles, including autonomous vehicles. This regulation establishes requirements and procedures for the approval of connected vehicles with respect to security aspects. In addition to this, it mandates the establishment of a Cyber Security Management System (CSMS) to ensure continuous monitoring and management of cyber security threats. For what is about the security testing, the Approval Authority or the Technical Service shall verify by testing of a vehicle of the vehicle type that the manufacturer has implemented the cyber security measures they have documented. Tests shall be performed by the Approval Authority or the Technical Service itself or in collaboration with the vehicle manufacturer by sampling. Sampling shall be focused but not limited to risks that are assessed as high during the risk assessment. The CSMS is integral to this process, as it provides a structured approach for managing cyber security risks throughout the vehicle's lifecycle. The “type approval” won’t be granted if the OEM is not able to demonstrate proper testing on the implemented security measures and the effective operation of their CSMS.

2.3.2 UNECE R156

UNECE R156 is a normative concerning uniform provisions for the approval of vehicles with regards to software update and the implementation of a Software Update Management System (SUMS). When an update or modification is performed, it is important that this does not make the vehicle less secure. The SUMS is crucial as it oversees the safe deployment of software updates, ensuring that they do not compromise vehicle integrity or customer safety. Every modification on the vehicle type which affects its technical performance and/or on the documentation required in this Regulation must be notified to the approval authority. The approval authority may then either:

- Confirm that the modifications made still comply with the requirements and documentation of prior type approval; or
- Require a further test report from the Technical Service responsible for conducting the tests. In this context, the SUMS is instrumental in providing documented evidence that software updates have been managed according to the established procedures, thus maintaining compliance with the regulation.

3 Security Testing Concept

Security testing concept requires a strategic and methodological approach to assessing and ensuring the security of electronic systems and software used in vehicles. This involves a series of planned and structured activities designed to identify, analyse and mitigate potential security vulnerabilities and threats that might affect vehicle components and systems.

3.1 Security Testing definition

After an analysis of the documentation and the characteristics of the item under consideration, the Security Test Definition is aimed to:

- Check if the functionalities are implemented with proper mitigation of possible vulnerabilities;
- Check if all the interfaces are properly secured;
- Check if the item behaves as expected, also in case of maliciously forged input.

3.2 Types of threat and vulnerability

With the increased adoption of complex technologies, car manufacturers have been able to improve comfort and performance, but – as a side effect - the "attack surface" and the possible threats and vulnerabilities have growth more and more.
Some of the major threats are:

Remote Attacks	Hackers might exploit wireless or cellular connections to access the vehicle remotely, taking control even of critical systems such as the engine or braking systems;
Vehicle Theft	Vulnerabilities in security systems and electronic keys might be exploited for vehicle theft or unauthorized door opening;
Infotainment Intrusions	Internet-connected infotainment systems might be subject to attacks to compromise drivers' privacy by stealing sensitive data or tracking driving habits;
Data Manipulation	Hackers might modify data from vehicle sensors, such as speed or orientation data, leading to unexpected or dangerous behaviour;
Attacks on Bluetooth Connection	Hackers might exploit vulnerabilities in the Bluetooth connection to gain access to the vehicle and steal personal information or take control of connected devices;
Attacks on the OBD-II Port	The On-Board-Diagnostics port, typically used for vehicle diagnostics at the service, might be exploited by hackers to gain access to vehicle systems and change its behaviour;
Attacks on ECUs	Electronic control units (ECUs) can be vulnerable to attacks that might affect vehicle functions, or to intentional tampering;
Navigation System Attacks	Hackers might interfere with navigation and positioning systems, causing incorrect directions or loss of accuracy;
Attacks on Connected Infrastructure	Connected Road infrastructure may be subject to attacks that affect road signs or cause security problems by deceiving a multiplicity of vehicles;
Vehicle Fleet Attacks	Corporate vehicle fleets might be targeted by attacks aimed to affect multiple vehicles simultaneously, compromising business operations.

Proper security testing should be applied to reduce the risk associated to all these threats.

4 Security Testing in the context of a comprehensive Cybersecurity Framework

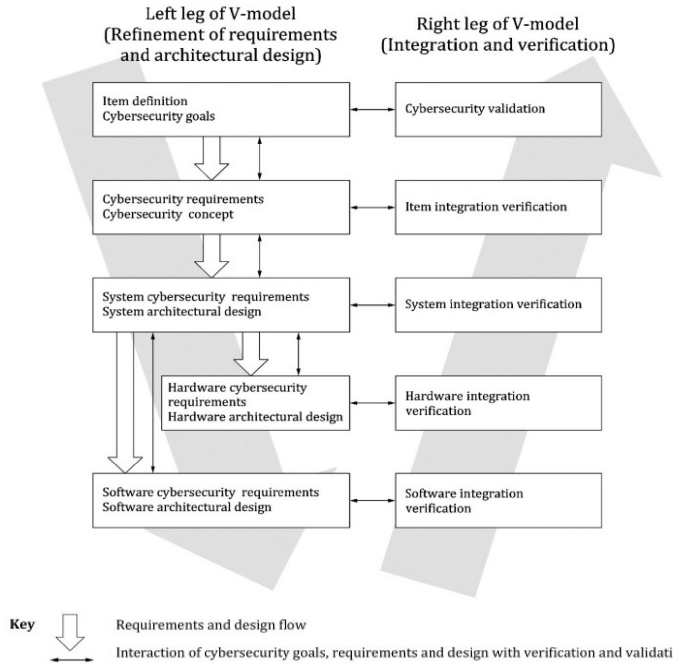
The ISO/SAE 21434 standard provides a comprehensive framework for Automotive Cybersecurity, that is a structured set of processes, procedures and models to address security challenges in vehicles and connected systems.
Such framework enables automotive companies to:

- Identify potential threats;
- Evaluate the associated risk;
- Design, refine and implement robust security measures to mitigate the cyber-risk;
- Execute proper tests to verify the correct implementation and validate the effectiveness of security measures;
- Re-evaluate the risk, keeping into account the applied measures, and the possible newly identified threats.

4.1 ISO/SAE 21434 V-model

The security framework defined in the ISO/SAE 21434 is built on top of the so-called V-Model, that is widely applied in the automotive domain to represent the multiple phases of the overall lifecycle of an automotive product (component, system, vehicle).

Figure 9 - Example workflow for product development



The main phases of the ISO/SAE 21434 V-model are:

1	**Item Definition and Cybersecurity goals**	The main product functionalities (items) are identified and related security objectives are established. The operational context, potential threats and related protection objectives are also defined.
2	**Cybersecurity requirements and Cybersecurity concept**	Here, security requirements are developed and defined starting from the objectives established in the previous phase. A high-level security concept is also developed that addresses these threats and goals.
3	**System cybersecurity requirements and system architectural design**	At this level, the security requirements for each individual system are detailed. The system architecture is also designed to meet these requirements, considering interfaces, modules and components.
4	**Hardware cybersecurity requirements and Hardware architectural design**	Specific requirements for hardware security are defined and the hardware architecture is designed with these requirements in mind, identifying key components, connections and other relevant elements.
5	**Software cybersecurity requirements and software architectural design**	In this phase, the security requirements for the software are outlined and the software architecture is defined to satisfy these requirements. This includes the definition of modules, interfaces and data flows.
6	**Software integration verification**	Once the different software modules have been developed, they are integrated and tested together to verify that they function correctly and safely as an overall unit.
7	**Hardware integration verification**	Similarly, hardware components are assembled and tested to ensure that they meet safety requirements and function as intended.
8	**System integration verification**	In this phase, hardware and software are integrated together at system level and tested to ensure that the entire system meets the established security requirements.
9	**Item integration verification**	Each 'item' or product is examined as a complete entity, verifying that all systems, hardware and software, are correctly integrated and work together safely.
10	**Cybersecurity validation**	Finally, it is validated that the entire product meets the originally established security objectives. This is a final verification that ensures that all security measures have been implemented and are working correctly.

Compliance with the requirements of ISO/SAE 21434 can also be demonstrated without following the development approach indicated by the V-Model, although this is probably the best model to use in the context of compliance with current regulations.

4.1.1 Agile V-Model

The V-model has historically been applied to the waterfall methodology, but at the same time it can be applied to the Agile methodology that is also increasingly used in the automotive sector. This approach, based on short development cycles, is suitable when rapid adaptation to change and close collaboration between multidisciplinary teams are necessary.
The Agile method and V-Model can be used together:

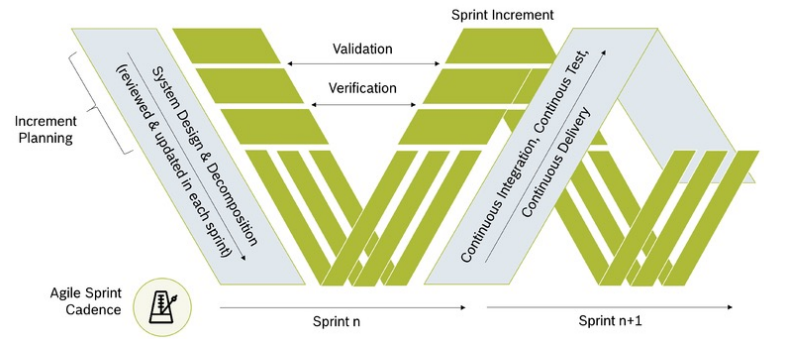
- On the left side of V-Model are story maps, used by the Agile methodology for logical decomposition;
- On the right side of V-Model are the Continuous Integration / Continuous Testing / Continuous Delivery processes, which by their nature fit well with the Agile methodology.

In this 'Agile V-Model' approach, the basic assumption is that the V-model is used not as a cascading model, but that the sprints of the Agile methodology fit the V-Model. Likewise, the V-Model must repeat itself and integrate multiple iterations depending on the sprints that occur.
In particular, two options can be used to realise the Agile V-Model:

- Each sprint includes both development and integration/testing phase and involves the entire iteration of the V-Model;
- Each V-Model iteration comprises two sprints: one development sprint and one integration/test sprint.

The first option is preferable for most projects, but for projects with a high level of complexity and dependencies, that is, when there are many components developed by different organizations, the second option that alternates the development and integration phases is preferable.

Figure 10 - Agile V-Model Process Diagram



4.1.2 V-Models Alternative

Models other than the V-Model could be used, the most important of which are:

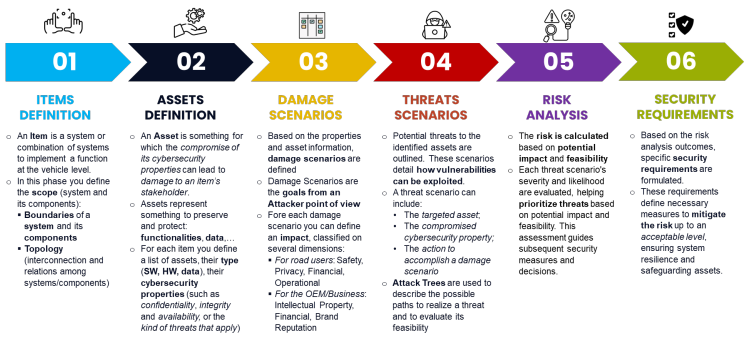
The Spiral Model	a Model that involves iterative development cycles, each one including risk assessment phases. These phases can be integrated to assess and mitigate cybersecurity-related risks iteratively during development.
The incremental model	a model that involves progressive product development in small increments or iterations. This approach can be adapted to meet cybersecurity standards by introducing continuous testing and validation practices during each Agile iteration to ensure standards are met.
DevSecOps	a combination of development (Dev), security (Sec) and operations (Ops). This approach integrates cybersecurity into the DevOps workflow, enabling continuous detection and correction of vulnerabilities.

In any case, to be compliant with standards and regulations, it is necessary to use a model and to document vulnerabilities and threats, their identification, and related countermeasures applied.

4.2 TARA

An important process involved in the initial phases of the V-model is the TARA. TARA, which stands for Threat Analysis and Risk Assessment, is a fundamental cybersecurity process that aims to identify and evaluate potential threats and associated risks within a given system or context. In the "Item Definition and Cybersecurity goals" phase, the system's components and functionalities are defined, and the associated cybersecurity objectives are established. In this iteration, TARA is applied to analyse potential threats and assess the risks tied to each system component or function, subsequently helping to shape precise cybersecurity goals for each item. As the process advances to the "Cybersecurity requirements and Cybersecurity concept" phase, the threats and risks identified through TARA guides the derivation of specific cybersecurity requirements and their prioritization. The resulting cybersecurity concept is then crafted, considering these requirements, outlining how each will be met in terms of security solutions and measures. In essence, TARA is deeply embedded in the V-model's initial phases, ensuring a systematic and comprehensive approach to security from the outset of system development.

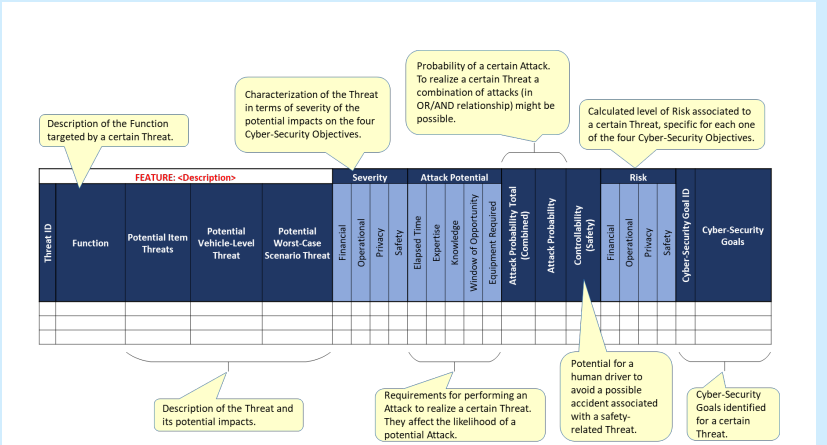
Figure 11 - Stages in the TARA Process



4.2.1 EVITA Model

Is it possible to choose among several models to conduct a TARA. One of the most accurate has been proposed in the EVITA Project.

Figure 12 - EVITA Model



The TARA process identifies the critical components of the system under test, those that could have a significant impact on cybersecurity. Following the EVITA model, once these components are identified, the functions targeted by a certain threat and the potential impacts are analysed. After that, the threat is examined from the point of view of severity, i.e., the potential impact on the 4 cyber-security objectives (Financial, Operational, Privacy, Safety) and from the point of view of Attack Potential, i.e., the requirements needed by an attacker to accomplish a certain threat (time, expertise, knowledge, etc.). Then the Attack Probability is calculated based on the Attack Potential and finally for each of the 4 cyber-security objectives the Risk Level is calculated. As a final step for each of the identified threats, security levels from SL1 to SL4 are identified and based on the assigned level, Cyber-Security Goals are established.

4.2.2 The importance of the TARA

The TARA is important for multiple reasons:

- First, the vehicle nowadays is a complex system, having a complex network composed by multiple interconnected ECUs;
- Cyberattacks on automotive systems, such as brake systems or engine control, can have direct physical consequences for the passengers, but also for other road users;
- Standard and regulation require a TARA, such as ISO/SAE 21434 and UNECE R155;
- Cybersecurity incidents in vehicles can seriously damage brand trust and loyalty, potentially leading to lost sales;
- TARA allows organizations to take a proactive stance, identifying potential risks before they become actual issues;
- Cyber threats are continually evolving. Adopting TARA ensures that organizations regularly review and update their assessments to account for changes in the threat landscape.

4.2.3 Goals of TARA

Here listed the main goals of doing the TARA:

Identify Vulnerabilities	The primary goal of Automotive TARA is to identify potential vulnerabilities and weaknesses within the complex electronic systems of connected vehicles. This includes analysing software code, hardware components, communication networks, and interfaces to uncover potential points of exploitation.
Assess Threat Landscape	Automotive TARA aims to assess the ever-evolving threat landscape in the automotive industry. By understanding the latest cyber threats and attack vectors, stakeholders can develop tailored security strategies to counter emerging risks effectively.
Enhance Vehicle Safety	By conducting TARA, manufacturers can implement robust cybersecurity measures to protect critical safety systems within the vehicle. This helps prevent potential cyberattacks that could compromise vehicle control, safety features, and the well-being of occupants.
Protect Customer Data	Modern vehicles collect and process a significant amount of personal data. TARA helps safeguard customer data from unauthorized access, data breaches, and privacy violations.
Optimize Resources	Resources are allocated efficiently for risk mitigation.

4.2.4 Stakeholder Involvement

An important point for a proper TARA execution is the stakeholder involvement:

- It is important to involve automotive cybersecurity experts who have knowledge of vehicle systems and architecture, so that they can identify potential vulnerabilities and assess the feasibility of implementing security measures. Their expertise significantly increases the effectiveness of TARA;
- The TARA process is a collective effort, involving multiple stakeholders working together towards a common goal: improving cybersecurity and ensuring vehicle safety;
- Stakeholder involvement is not limited to the initial TARA process but extends to continuous improvement. Regular engagement with stakeholders ensures that the TARA remains up to date with evolving threats and technological advancements;
- TARA is a shared responsibility of all stakeholders. Collaborative engagement promotes a proactive and holistic approach to automotive cybersecurity, contributing to a safer and more secure automotive ecosystem.

4.2.5 NTT DATA Approach and benefits using C2A EVsec TARA tool

In our research for robust cybersecurity solutions, we have refined an approach to threat analysis and risk assessment (TARA) that harnesses the power of our partner C2A's advanced automation tools. By doing so, we've addressed some of the most significant challenges that organizations typically face during this crucial process.

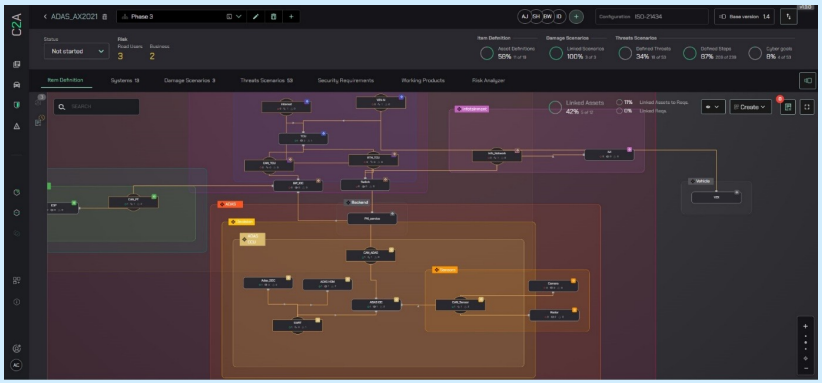
One of the features of this tool is its ability to foster seamless collaboration. Whether it's inter-departmental work, teamwork, or even engagement with external suppliers, the tool's intuitive design and capabilities facilitate smooth delegation and real-time cooperation. This is a game-changer, particularly in the rapidly evolving landscape of cybersecurity, where collaboration is not just a benefit but a necessity.

Another advantage lies in the tool's capability to reuse prior work. This not only ensures consistency but also dramatically reduces repetitive tasks, optimizing the TARA process in terms of both time and resources.

The tool comes equipped with a rich set of templates, catalogues, and libraries. What's even more impressive is that these resources are not fixed; they offer extensibility, allowing for customization based on the unique needs and nuances of any given project.

Our chosen TARA tool is designed to be intuitive. It streamlines and simplifies activities, with automation features that reduce manual input and margin of error. This ensures that even the most complex tasks become more manageable and less prone to human error.

Figure 13 - Example of Item Identification on C2A TARA tool



Another cornerstone of our approach is accountability and compliance. With evolving cybersecurity norms, it's imperative to have a system in place that can demonstrate adherence to both industry standards, like ISO/SAE 21434, and global regulations, such as those published by UNECE WP.29. Our tool produces tailor-made reports that prove compliance, facilitating audits and reviews of operations.

Finally, recognizing the importance of agility in modern software development and operations, this tool is built to fit seamlessly within a DevSecOps environment. This ensures that cybersecurity considerations are not an afterthought but an integral part of the development lifecycle, right from ideation to deployment.

4.3 Structured execution of Testing Activities

One of the elements that guides test execution is TARA. In other words, tests must be structured, planned and prioritized according to the risks that have been highlighted during the TARA phase.

4.3.1 Selection of testing tools

The identification of testing tools, techniques and technologies is a crucial step in ensuring the effectiveness and coverage of security testing. This may include static code analysis tools, vulnerability scanning tools, penetration testing platforms, and attack simulation software. The choice of tools depends on the specific needs of the project, budget and the type of testing to be performed.

4.3.2 Creation of test plans

Creating well-defined test plans is an essential step in ensuring the structured and systematic execution of security tests. Detailed test plans define test objectives, procedures to be followed, test cases to be performed and criteria for acceptance of results. Each automotive component and system involved requires a specific test plan that takes into account the unique characteristics and associated potential threats.

4.3.3 Execution of tests and results analysis

Test execution is the phase in which specific tests are carried out to assess the security and the resilience of automotive systems or components. These tests are related to specific vulnerabilities and may include:

- Tests to verify the fulfilment of security requirements;
- UNECE wp.29 R155 compliance test (R.155 Annex 5);
- Fuzz Testing;
- Penetration Testing: Black-box, Gray-Box, White-Box.

After the tests execution, the results are analysed to identify any flaws, vulnerabilities, or abnormal behaviour. This step is essential to detect potential vulnerabilities and assess their impact as soon as possible.

4.3.4 Reporting and documentation

Reports and documentation serve to communicate the results of the tests and analyses conducted. Test results, detected vulnerabilities, and recommendations for corrective actions are documented in detail. This documentation will support risk mitigation decisions and help provide a clear picture of the state of system security. Well-structured test reports are essential for transparency, regulatory compliance, and to demonstrate commitment to cybersecurity.

5 Main security testing techniques

Security testing techniques in the automotive field are varied and aim to identify vulnerabilities and potential threats to the integrity, confidentiality and reliability of systems.

5.1 Automatic and manual Security Testing

The testing process to increase automotive cybersecurity involves two main approaches: automated testing and manual testing. Both are important in ensuring that vehicles and automotive products are protected from cyber threats, but they differ greatly in their methodologies and capabilities. Below, we will introduce both aspects of automotive cybersecurity testing.

5.1.1 Automated Security Testing

Automated security testing involves the use of automated tools and software to identify vulnerabilities and security issues in software, communications, and vehicle interactions. These tools perform static and dynamic code analysis, explore communication interfaces and protocols for potential threats, and leverage fuzzing techniques to discover vulnerabilities.

Benefits of Automated Testing	• Efficiency	Automated tests can analyse large amounts of code and data in relatively short periods of time;
	• Scalable Coverage	They can be used to test a wide range of scenarios and configurations;
	• Repeatability	Tests can be run multiple times to ensuwre consistency of results;
	• Rapid Discovery	They allow known vulnerabilities and potential problems to be quickly identified.
Disadvantages of Automated Testing	• Limited Knowledge of Context	Automated tools may not be able to fully understand the specific operating context of the DUT (Device Under Test);
	• Lack of Creativity	They cannot identify new vulnerabilities or scenarios as ingeniously as a human tester.

5.1.2 Manual Security Testing

Manual security testing involves careful analysis and exploration of the system by security experts who simulate targeted attacks, assess behaviours in critical situations, and use their knowledge to identify complex vulnerabilities. This approach requires advanced technical skills and detailed analysis of system interactions.

Advantages of Manual Testing	• Creative Approach	Human testers can think creatively and identify innovative attack scenarios;
	• Understanding Context	Security experts can evaluate the system by considering the specific context/characteristics and implement ad-hoc testing scripts.
Disadvantages of Manual Testing	• Cost and Time	Manual testing requires more time and resources than automated testing;
	• Possible Subjectivity	Results may vary slightly depending on the testers' skills and perspective.

Both automated and manual security testing are crucial in automotive security. While automated testing allows for efficient, large-scale assessment, manual testing offers deep analysis of complex threats and vulnerabilities. Often, a hybrid approach combining both methods can maximize the effectiveness of vehicle security assessment.

5.2 Vulnerability scanning

In the automotive field, vulnerability scanning is a technique used to identify vulnerabilities and possible security holes in vehicle electronic systems and components. This methodology involves the use of specialized tools to analyse the software, firmware, communication protocols and other components of the vehicle's electronic architecture to identify potential weaknesses that could be exploited by cyber-attacks. The vulnerability scanning process in the automotive environment helps to ensure that vehicles are protected from cyber threats, enabling developers and engineers to mitigate risks and improve the overall security of systems embedded in vehicles.

One crucial element of this process is the analysis of the Software Bill of Materials (SBOM) and Hardware Bill of Materials (HBOM). The SBOM provides a detailed inventory of all software components used in the vehicle's electronic systems, while the HBOM offers a comprehensive list of hardware components. Thorough assessment of potential weaknesses at both the software and hardware levels. This holistic approach ensures that vulnerabilities are identified and addressed comprehensively, contributing to the overall security of the embedded systems within vehicles.

5.3 Tests to verify the fulfilment of security requirements

Based on the risk analysis outcomes, specific security requirements are formulated. These requirements define necessary measures to mitigate the risk up to an acceptable level, ensuring system resilience and safeguarding assets. Once the mitigations have been implemented, it is necessary to proceed to test their effectiveness by verifying the absence of the previously associated vulnerabilities through appropriate security tests.

At this point the TARA can be modified by entering the new information to recalculate and possibly lower the risk level of the system under test.

5.4 UNECE (R.155 Annex 5) Compliance Testing

UNECE is the Economic Commission for Europe that recently has published two regulations in the automotive field, one of them is the R155 which establishes a comprehensive framework for automotive cybersecurity. The regulation mandates that vehicle manufacturers, before their products hit the road, ensure that they have identified potential cyber threats, assessed the risks, and implemented robust cybersecurity measures to mitigate these risks. Manufacturers are required to continuously monitor, report, and respond to any new vulnerabilities or threats that emerge after the vehicle has been sold. From the Annex 5 of the UNECE R155 it is possible to deduct some tests in order to show the compliance with the regulation.

Annex 5 of UNECE R.155 consists of 3 parts:

- Annex 5 Part A describes the baseline for threats, vulnerabilities and attack methods;
- Annex 5 Part B describes the mitigation measures for threats inside vehicles;
- Annex 5 Part C describes threat mitigations for areas outside of vehicles, such as IT backends.

Figure 14 - Annex 5 Part B links the part A in-vehicle threats with their mitigation

Part B. Mitigations to the threats intended for vehicles

1. Mitigations for "Vehicle communication channels"

Mitigations to the threats which are related to "Vehicle communication channels" are listed in Table B1.

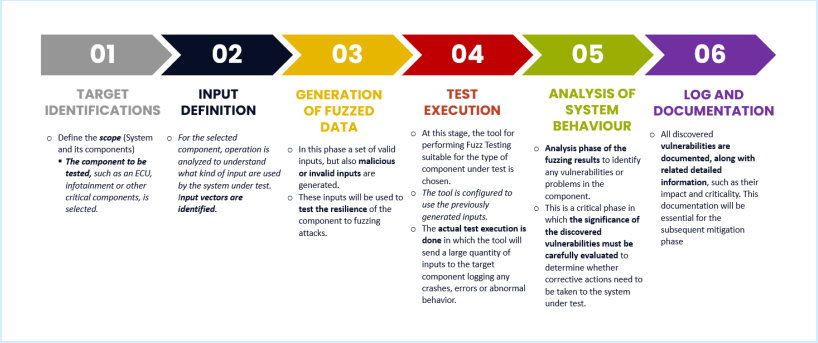
Table B1
Mitigation to the threats which are related to "Vehicle communication channels"

Table A1 reference	*Threats to "Vehicle communication channels"*	*Ref*	*Mitigation*
4.1	Spoofing of messages (e.g. 802.11p V2X during platooning, GNSS messages, etc.) by impersonation	M10	The vehicle shall verify the authenticity and integrity of messages it receives
4.2	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)	M11	Security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules)
5.1	Communication channels permit code injection into vehicle held data/code, for example tampered software binary might be injected into the communication stream	M10 M6	The vehicle shall verify the authenticity and integrity of messages it receives Systems shall implement security by design to minimize risks
5.2	Communication channels permit manipulation of vehicle held data/code	M7	Access control techniques and designs shall be applied to protect system data/code
5.3	Communication channels permit overwrite of vehicle held data/code		
5.4 21.1	Communication channels permit erasure of vehicle held data/code		
5.5	Communication channels permit introduction of data/code to vehicle systems (write data code)		

5.5 Fuzz testing

Fuzzy testing is a security testing technique used in the automotive industry to assess the robustness and reliability of electronic systems and software within vehicles. This methodology involves introducing pseudo random inputs into systems in order to explore unusual or unexpected scenarios that could lead to errors or crashes. Fuzz testing can be performed on a wide range of objects and components, in the automotive field the elements that benefit from fuzz testing are: Communication protocols, ECUs, Infotainment systems, Sensors, Embedded Libraries, Diagnostic Interfaces, etc.
This technique can help detect programming errors, security problems or unforeseen situations that might arise in real-life usage scenarios or caused by malicious actors. Fuzzy testing thus helps to improve the resilience and security of vehicle systems, enabling developers to detect and correct potential risks before they can be exploited by external attacks.

Figure 15 - Fuzz Testing steps



5.5.1 NTT DATA Approach using C2A Attacker tool

We have integrated a state-of-the-art fuzz testing tool into our cybersecurity framework, which has several advantages that make the testing operation simpler and allow us to achieve excellent results.
What sets our approach apart are the advanced features of the C2A Attacker Tool. the Tool has the ability to take input binaries (as well as other file types) and perform an automatic analysis of the component under analysis. In addition, C2A Attacker Tool can do automatic and semi-automatic design of the input range to be used in the fuzz campaign. Automation allows a more exhaustive code analysis, examining the program instruction by instruction. Given the vast array of possible input combinations, the proportion of these combinations that is actually tested is what constitutes the test coverage.
A notable challenge in fuzz testing is the vastness of the test space, which can make the process time-consuming and less efficient. Maximum coverage is achieved by C2A Attacker Tool identifying the most critical input types and ranges for the component under test. Again, with the aim of maximising coverage and increasing security, the tool has a semi-automatic guided mode that uses binary files to carefully analyse “corner cases”, i.e. those situations that occur outside the normal operating parameters, in addition to achieving high coverage rates, the features just described allow for significantly increased fuzzing speed, which in some cases can be truly time-consuming. While total automation leads to a significantly acceleration of the process, the semi-automatic component allows for a targeted focus, favours precision and reducing the possibility of oversight.
Ultimately, one of the key points of our tool is the intelligent ability to identify input-related validation checks. In this way, it guarantees two main results: a further reduction of the test space and a consequent increase in coverage. This means that we not only run tests faster, but also ensure a high level of coverage and corner cases. In this way, an in-depth analysis of potential vulnerabilities is carried out.

5.6 Static code analysis

Static code analysis is an analysis and evaluation technique used in the automotive field to examine the source code of software embedded in vehicle electronic systems. This methodology focuses on analysing the source code without actually running the program to identify potential vulnerabilities, programming errors and security flaws.
During the static code analysis process, specialized software tools are used to analyse source code for patterns, common errors, potential security problems, vulnerabilities and inconsistencies. These tools can identify various types of problems, such as buffer overflows, unauthorized access to sensitive data, security holes, and other vulnerabilities that could be exploited by cyber-attacks.
There are also some tools such as the “Polyspace”, “Vector PC-Lint”, and others which allows you to check the compliance of the code under analysis with the MISRA rules, i.e. a set of software development guidelines for computer programming language C developed by MISRA (Motor Industry Software Reliability Association) with the aim of facilitating the safety, portability and reliability of embedded systems, particularly those developed using ISO-C as programming language.

5.7 Dynamic application security testing (DAST)

Dynamic Application Security Testing, or DAST, is a methodology used in the automotive industry to assess the security of software and applications implemented in vehicle electronic systems. Unlike static code analysis, which focuses on source code, DAST focuses on dynamic application execution to identify potential vulnerabilities and security risks.
In the automotive context, DAST involves the active execution of the application within a controlled test environment. During this process, typical activities and interactions that might occur during vehicle use are simulated. The main purpose is to detect real-time vulnerabilities, such as possible security holes, exposures of sensitive data, and potential weaknesses in the application while it is running.
DAST solutions use a variety of techniques, including inputting malicious or manipulated test data to identify possible vulnerabilities, monitoring application responses, and analysing data flows and communications between components. This dynamic approach provides a realistic assessment of the actual robustness of the application against potential threats and attacks.

5.8 Threat modelling

Threat Modelling is a methodology used in the automotive industry to identify and assess potential threats and vulnerabilities within vehicle electronic systems. This technique focuses on the design and analysis of possible threats that could compromise vehicle security and integrity, as well as the evaluation of possible attack scenarios. There are different threat modelling frameworks but in the cyber-physical domain the most used is the STRIDE. Threat Modelling is included in the TARA and it typically involves several activities, including:

1 System Description	Initiate the process with a detailed overview of the automotive system under analysis. This overview should encapsulate its core functionalities, intricate interfaces, and dynamic interactions with external systems. Recognize and document the assumptions surrounding the system's operational environment and anticipated threat actors. As the realm of cyber threats advances, it's paramount to periodically revisit and adjust these assumptions to remain aligned with emerging risks.
2 Model Creation	Construct a representation of the automotive system, emphasizing potential points of interaction, data flow, and external dependencies. This model serves as a visual aid, facilitating a structured analysis of the areas susceptible to threats.
3 Threat Identification	Systematically identify and catalogue potential threats to the automotive system. This encompasses a wide range of risks, from cyber-attacks, physical tampering, and unauthorized access to potential system misuse. Recognizing these threats requires an understanding of the system's design, its operational context, and potential adversaries' capabilities and motivations.
4 Mitigation	After identifying threats, tailored strategies are developed to mitigate each risk. This might involve introducing specific technical countermeasures, adjusting system architectures, implementing software updates, or adopting procedural changes. It should be ensured that each mitigation strategy is in line with the system's operational and performance requirements.
5 Validation	In this final phase, validate the effectiveness of the proposed mitigation strategies. Employ a combination of testing, simulations, and expert reviews to ascertain that the measures, once implemented, will adequately address the identified threats without introducing new vulnerabilities or adversely impacting system performance.

5.9 Penetration testing

Automotive penetration testing is an advanced security testing methodology that aims to assess the robustness and resilience of computer systems and electronic components within vehicles. This technique involves carrying out controlled and simulated attacks toward the system to identify possible vulnerabilities and weaknesses that could be exploited by real attacks. Penetration testers use sophisticated techniques and tools to perform intrusion tests and analyse how the system reacts to various cyber threats. The goal is to detect potential security holes, assess their impact and likelihood, and provide recommendations for strengthening vehicle protection against cyber-attacks. Penetration testing is an essential element in automotive security strategy to ensure that vehicles are resilient to attacks and that sensitive data and driver privacy are preserved.

The penetration test can be performed in various ways that allow for a broader assessment of risks and attack paths, which can differ greatly depending on the attacker's knowledge of the system. The 3 types of penetration testing used in automotive are: Black-Box, Gray-Box and White-Box.

5.9.1 Black-box Security Testing

Black Box Security Testing is a testing methodology that involves analysing and evaluating a system or application without knowing the internal details of its operation or source code.

In the context of automotive security, Black Box Security Testing involves performing security tests on an embedded system or electronic component within a vehicle without having access to detailed information about its architecture or internal design. Testers focus on how the system responds to inputs, how it handles data, and how it reacts to possible attacks or threats from outside.

5.9.2 Gray-box Security Testing

Gray Box Security Testing is an intermediate approach between Black Box Testing and White Box Testing. In this method, testers have partial knowledge of the inside of the system or application, but do not have complete access to the source code or internal architecture.

In the context of automotive security, Gray Box Security Testing requires that testers have limited knowledge of the vehicle or system components and their interactions.

5.9.3 White-box Security Testing

White Box Security Testing is a methodology that involves detailed, in-depth analysis of a system or application, with full access to internal information, including source code, architecture and operating logic.

In the context of automotive security, White Box Security Testing involves the in-depth examination of an embedded system or electronic component within a vehicle, analysing its code, data flows and interactions between various modules.

5.9.4 NTT DATA Approach

Usually, combinations of the three types of penetration testing just described are used. In fact, these approaches are most effective each at a different point in the product life cycle. The white box approach is most useful in the early stages of development to detect and fix vulnerabilities specific to some component. The gray box type is more useful in the middle stages of development to test existing parts of the system, particularly when developers do not have all the internal details. Finally, the black box approach is most useful when testing a system in the final stages of design and in continuous post-launch security monitoring.

6 Conclusions

6.1 Summary of the main considerations

Security testing in the automotive environment plays a crucial role in ensuring the security of vehicles and their occupants in the digital age. Not only does this process help identify and mitigate cyber vulnerabilities that could be exploited by malicious attacks, but it also brings several essential benefits to the automotive industry.

First, security testing enables strengthened protection against increasingly sophisticated cyber threats, ensuring that automotive systems are resilient to malicious attacks and intrusions. This results in safer and more reliable vehicles for end users.

In addition, security testing addresses the growing needs for compliance with automotive industry standards, regulations, and guidelines. Adopting security testing practices recommended by recognized organizations, such as ISO, SAE and UNECE, not only enhances the company's reputation, but demonstrates a commitment to providing vehicles that meet stringent safety and security requirements.

In addition to protecting vehicles and occupants, security testing promotes safe innovation in the automotive industry. It provides a structured approach to evaluate and continuously improve the security of systems, encouraging the development of advanced technologies that meet both mobility needs and security standards.

Performing security tests from the outset allows vulnerabilities and risks to be identified earlier and mitigated (shift left), so changes are made earlier and more costly interventions (e.g. machine recalls) are avoided.

Ultimately, automotive security testing is a key investment for the modern automotive industry. It ensures the protection of vehicles, passengers and sensitive information, providing a higher level of confidence to both manufacturers and end users.

6.2 Future prospects for security testing

Continuing technological developments and the ever-increasing interconnection of vehicles will require increasingly sophisticated approaches to ensuring security.

Here are some key perspectives on the future of security testing:

Security-by-Design	The security-by-design approach will be increasingly adopted at the early stage of vehicle development in according with the “Shift Left” strategy. This will ensure that security measures are integrated from the start, step by step, and not only at the end of the design phase, significantly reducing the cost and complexity, as well as the probability, of late intervention;
Regulatory Compliance	Increased regulations in the automotive industry will require more emphasis by the OEM and Tier1 on security testing to ensure compliance with standards and regulations;
Continuous Security Testing	Adoption of DevSecOps practices will promote continuous security testing throughout the vehicle lifecycle, allowing vulnerabilities to be identified and resolved promptly as they are discovered;
Training and Awareness	Ongoing security training and awareness will be critical for software developers to ensure a thorough understanding of threats and countermeasures;
Intelligent Automation	The integration of artificial intelligence and machine learning will enable the development of more advanced and automated security testing tools. These tools will be able to recognize and address threats in real time, improving the responsiveness and robustness of security systems;
Electric Vehicles and Charging Infrastructure Security	With the rise of electric vehicles, is important to protect not only the vehicle itself but also the charging infrastructure. The software controlling electric vehicle batteries and managing charging stations must be safeguarded to prevent potential cyberattacks, making cybersecurity a critical concern in this evolving landscape;
Artificial Intelligence Security	With the increasing adoption of artificial intelligence-based systems in vehicles, security testing will also focus on protecting algorithms and machine learning models from malicious attacks;
Autonomous and Connected Cars	The growing number of autonomous and connected vehicles will require high-level security that extends far beyond the vehicle itself, involving the communications infrastructure and roadside infrastructure;
Emerging Threats	The future may bring new automotive-specific cyber threats, such as attacks targeting autonomous vehicles or vulnerabilities related to emerging technologies, such as 5G networks;
Shared Responsibility	Vehicle security will be a shared responsibility among manufacturers, component suppliers and software developers, requiring unprecedented collaboration to ensure maximum protection.

Ultimately, security testing will continue to be a key pillar of automotive security in an increasingly interconnected and digitized future. Innovation in security testing will help create vehicles that are safer, secure, more reliable and able to meet emerging challenges in the world of mobility.