International Alliance for Mobility Testing and Standardization™ Practice Report

IAMTS0003202301

Issued 2023-01-27

Automotive Cyber Security Practice Report: An Overview of Tools, Procedures, Testing Methods, and Regulations

Rationale

The UNECE's regulations R.155 and R.156 recently demand the management of cyber security risks in vehicle design and that the effectiveness of these measures is verified by testing. This mandates the introduction of automated and reproducible cybersecurity testing in automotive development processes. UNECE R.155 and its associated standard, ISO/SAE 21434, provide guidance for the implementation of a cyber security risk management system in automotive, however, there is a need for detailed implementation procedures regarding testing processes and methods in the development part of the life cycle. This report analyzes current developments in vehicular cyber security standards, regulations and recommendations, and evaluates currently used processes and tools at automotive manufacturers and suppliers.

While the global standards only recommend testing methodologies at a very high level (i.e., functional testing, vulnerability scanning, fuzz testing, penetration testing), some of the regional standards give hints on what to test (e.g., checking for exposed debug interfaces, the presence of a secure boot mechanism, usage of encryption in communications, etc.) or issued guidelines for component classes (e.g., a Japanese penetration testing guideline for ECUs).

The complexity of vehicular systems and the closedness of the automotive manufacturers, in conjunction with different standards and procedures make it infeasible to define a solid, standardized testing procedure that spans over the whole (inhomogeneous) system and over the whole life cycle. The development of standardized processes is further challenged, as each large OEM has its own established procedures from adjacent domains like functional safety testing. Therefore, this document provides a methodological framework with examples for different testing purposes, as well as a sketch process how to implement security testing.

Preface

IAMTS is a global, membership-based association of organizations that are stakeholders in the testing, standardization, and certification of advanced mobility systems and services. IAMTS brings together testing consumers and providers at a global scale to help develop a commonly accepted framework of test scenarios, validation and certification methods, and terminology.

Our mission is to develop and grow an international portfolio of advanced mobility testbeds that meet the highest quality implementation and operational standards.

Our vision is to create a global community of advanced mobility testing service providers with companies, organizations, and agencies in need of such services; to learn, develop, and share best practices to ensure consistent, replicable, and reliable testing; to maintain a global directory of physical, virtual, and cyber-physical testbeds and support and promote their audited capabilities; and to promote the rapid evolution of standards and certifications to ensure the safe deployment of advanced mobility systems and services

Introduction

With the UNECE's regulations 155 and 156, structured cybersecurity engineering of automotive systems through means of a cybersecurity management system becomes mandatory. The regulations, as well as international and regional standards, also prescribe that the effectiveness of the introduced security mechanisms must be verified and validated in a structured and replicable form through testing. The details of how to conduct testing in an adequate form are mostly left to vendors and suppliers for the sake of the general applicability of the respective standard. This document therefore aims at giving a starting point on test targets and testing methods that are mentioned in the international and regional standards, as well as the usage and applicability of such methods currently used in the wild. The structure is as follows: first the document defines the scope of its applicability and lays out the methodology of information gathering. Subsequently, an overview of international and regional standards that concern automotive cybersecurity follows, with a focus on what the examined standards outline specifically about testing and verification. Next, this document contains a survey on processes and tools, as well as common targets under scrutiny, as they are common practice among automotive security testers. Lastly, the document finishes off with conclusion and potential gaps to explore.

Table of Contents

Contents

1. Scope

The scope of the report is automotive cybersecurity verification and validation (V&V) testing and is focused on the following areas:

- International Standards and Regulations and their applicability to automotive cybersecurity V&V processes.
- Regional approaches to automotive cybersecurity V&V standards and regulations.
- Industry approaches to automotive cybersecurity V&V activities, including, processes and tools.

2. Methodology

The methodology utilized in this report included an initial overview of the international regulations and standards. Secondly, a survey of existing regulations and standards for automotive cybersecurity V&V testing in key regions, gathered from state-of-the-art, publicly available information was conducted. Lastly, a survey consisting of structured questions was conducted with IAMTS' members and other trusted organizations, to gain the industry perspective on processes and tools for automotive cybersecurity V&V testing.

3. Standards & Regulations Overview

3.1. International Regulations

3.1.1. UNECE R.155

In countries following the UNECE 1958 treaty, type approval (also referred to as homologation) is required from manufacturers prior to allowing series vehicles on public roads. The new UNECE regulations 155 [1] and 156 [2] have laid a foundation for the regulation of cybersecurity within the type-approval for several large markets (Europe, Japan, Korea, Russia, Australia, South Africa, etc.).

The new regulations R.155 and R.156 drive several changes to involved parties during the type approval process, mainly suppliers, manufacturers (OEMs) and technical services providers. For OEMs and suppliers, these are fundamental requirements of the automotive type-approval process and the development of products for their markets. In addition, specific consulting and test organizations are nominated by approval authorities to perform the technical assessment and testing of the vehicles and the manufacturer's processes for the purposes of type approval.

The UNECE R.155, from 2021 (legally binding as document ECE/TRANS/WP.29/2020/79 [3]) mandates the installment of a cybersecurity management system (CSMS - for example, as defined in ISO/SAE 21434 – see next section) to assure accompanying cybersecurity processes, to be executed during the automotive system development lifecycle. The ISO standard's stance toward cybersecurity verification is limited, however, it clearly states the requirement for testing *with adequate coverage* for vulnerabilities to cyber threats. Additionally, the OEM is required to verify the effectiveness of implemented cybersecurity measures by testing and the approval authority shall refuse the type-approval if this cannot be demonstrated (including the adequateness of the testing procedures themselves). Lastly, the authority or technical service shall itself verify the effectiveness of security measures by testing (concentrating on high-risk samples).

The UNECE R.155 Annex 5 Part B highlights a selection of commonly used systems, interfaces and processes for OEMs and suppliers to test as well as common mitigation measures. These systems, interfaces and processes include:

- Vehicle communication channels.
- Update process
- Unintended human actions facilitating a cyber attack
- External connectivity and connections
- Potential targets of, or motivations for, an attack
- Potential vulnerabilities that could be exploited if not sufficiently protected or hardened
- Data loss / data breach from vehicle
- Physical manipulation of systems to enable an attack
- Back-end servers
- Physical loss of data loss

The threats and associated mitigations are only listed as a minimum guide to follow. The testing authority needs to align these recommendations with the threat and risk assessment conducted by their own organization. For OEMs and suppliers with less mature cybersecurity testing processes, these test targets, threats, and mitigations can serve as informal input to their verification process. Details on how to verify security requirements are not outlined with the R.155 document. The presence of these requirements could be used as test targets for a verification process (as it actually occurs in practice – see Section Process and Tools Survey on p. 32). Any details on verification (what is considered as adequate testing procedures) are not specified in the regulation document.

In addition to the requirements present in R.155 and R.156, documents containing several recommendations, processes and additional requirements are usually defined at the national level by approval authorities to support the type approval process. For example, in Germany the KBA (Federal Motor Transport Authority) represents the approval authority responsible for type approval (see Section Germany).

3.1.2. International Standards

3.1.3. ISO/SAE 21434: Road Vehicles – Cybersecurity engineering

As the predominant standard for automotive cybersecurity engineering, ISO/SAE 21434 [4] also mentions verification and validation. The standard emphasizes the importance of cybersecurity testing and provides high-level guidance; however, it is not focused on providing a detailed analysis of testing methodologies, processes, and tools. Furthermore, the standard also distinguishes between verification and validation.

Verification

Verification can include:

- Review
- analysis,
- simulation and/or prototyping.

Verification considers:

- the specification,
- configuration,

- support of the intended functionality and
- guideline conformity.

Specified methods are:

- requirements-based test,
- interface test,
- resource usage evaluation,
- verification of the control flow and data flow,
- static and dynamic analysis.

The standard refers to verification by testing as an integral part of verification. Testing should be performed to uncover unidentified weaknesses and vulnerabilities. Not to test, requires, according to the standard, an appropriate rationale (e.g., a specific attack surface is not reachable).

Test derivation includes requirements analysis, equivalence classes, boundary analysis and error guessing, which should be evaluated using defined test coverage metrics (where standard metrics like statement coverage are not deemed sufficient). Suggested test methods are:

- functional testing,
- vulnerability scanning,
- fuzz testing,
- penetration testing.

Validation

Cybersecurity validation (clause 11 of the standard) consists of validating the security goals (with respect to the threat scenarios and corresponding risks) and the security claims (which are basically the accepted residual risks of a risk assessment), confirmation that the goals are achieved and that no unreasonable risks remain. The purpose is to demonstrate that the goals are appropriate and achieved. The only reference to testing within this activity is that it recommends using penetration testing for validation purposes.

As testing is not the main focus of the standard, the ISO has initiated a new standardization effort, ISO/PWI 8477: Road vehicles — Cybersecurity verification and validation.

3.1.4. ISO PWI 8477: and ISO/SAE PWI 8475

Due to the lack of testing-related details in ISO/SAE 21434 (see previous section), the ISO working group in charge (ISO TC22/SC32/WG11) proposed a new standardization project (ISO PWI 8477) for automotive cybersecurity verification and validation (V&V), which focuses on giving guidance on V&V objectives. This project is intertwined with a second project, ISO/SAE PWI 8475: Road vehicles — Cybersecurity Assurance Levels (CAL) and Target Attack Feasibility (TAF), which is dedicated to defining automotive cybersecurity assurance levels (CALs) and Target Attack Feasibility (TAF), whereby the CALs' focus lies on engineering assurance and the TAFs' on the expected strength of technical controls. These efforts have, however, not yet (as of June 2022) been started as official standards projects, so any results are therefore pending.

3.2. Survey of Regional Standards & Regulations of Automotive Cybersecurity V&V Testing

3.2.1. North America

Canada

In Transport Canada's Vehicle Cybersecurity Strategy, the Canadian Department of Transport is responsible for monitoring the work of the National Research Council Canada's Automotive and Surface Transportation Centre. The Automotive and Surface Transportation Centre engages in research and testing related to advanced vehicle technologies. Examples include examination of cybersecurity vulnerabilities in connected features, mapping and connectivity for automated driving. The testing and evaluation of cybersecurity is closely tied to applicable motor vehicle safety and data privacy legislation.

The Canada Vehicle Cybersecurity Guidance [5] provides technology neutral and non-prescriptive guiding principles for the incorporation of cybersecurity throughout the vehicle lifecycle. The guidance promotes the importance of international standards such as ISO/SAE 21434 and other related functional safety standards. The guide provides a descriptive overview of the context of cyber-attacks to vehicular systems and in particular that more advanced attacks tend to be associated with "white-hat" cybersecurity research, whilst real-world, cyber-criminal threat actors make use of the data driven ecosystem of vehicular technologies to comprise attacks on back-end systems and systems which generate and store telemetry. To this end, the guide recommends the implementation of layered security controls (known as defense-in-depth), privacy protection and information protection procedures and testing of, data security, secure external vehicle communications, identity management and access control, secure software development, secure updates, and the extended vehicle environment. Cybersecurity testing is recommended to be conducted throughout the vehicle lifecycle. Penetration testing is mentioned as an essential part of security auditing. Cybersecurity testing and validation methods are not explicit in the guidance provided by Transport Canada.

Transport Canada provides tier 1 and 2 automotive suppliers with a self-assessment tool: the Vehicle Cybersecurity Assessment Tool (VCAT). The VCAT is a self-assessment questionnaire applicable for all vehicle types with varying levels of connectivity and automated features. The self-assessment questionnaire assists with evaluating the cybersecurity performance and resilience of vehicles and vehicular components. The VCAT will provide a score, measuring cybersecurity posture, as well as recommendations for mitigations.

United States

In the U.S., National Highway Traffic Safety Administration (NHTSA) is the responsible entity under the U.S. Department of Transportation (U.S. DOT) which issues Federal Motor Vehicle Safety Standards (FMVSS) to regulate and standardize the requirements for the safety of motor vehicles [6]. With the increasing complexity and advancement of on-board computer/electronic systems in the motor vehicles; the entity undertook the responsibility of the standardization and regulation of the automotive cybersecurity [7]. Currently, there are no standards or regulations for automotive cybersecurity testing & verification which is brought by the NHTSA. However, to provide a comprehensive and systematic standardization process; the agency collaborates with the industry by encouraging them to voluntarily get involved in the standard development process and comment on the publications/reports which are published by the agency [8]. In 2016, the agency published a non-binding document describing guidelines/best practices for automotive cybersecurity, which is named as "Cybersecurity Best Practices for the Safety of Modern Vehicles". The document revised in 2020 based on the ISO/SAE 21434 draft standard and the comments on the previous version which were brought by the OEMs and various stakeholders, and a draft version has been published (2020 draft) [7]. Currently, the agency has announced a notice that it is seeking comments from the stakeholders for another revision of the document [9]. The document refers ISO/SAE 21434 standard and NIST's Cybersecurity Framework for standardizing the cybersecurity development, maintaining, and testing process. However, as the document is non-binding, the guidelines are considered as a recommendation and not obligatory for the industry. Despite the document being comprehensive and not directly related to testing & verification of automotive cybersecurity, a section related to penetration testing and documentation is provided in the document.

NHTSA's best practices document provides guidelines for automotive cybersecurity by pointing the cases under different sub-topics. One of these sub-topics includes a section on best practices for penetration testing and documentation. Those practices defined in [7] are as follows:

- Cybersecurity testing, including penetration testing should be implemented as a part of the development process.
- Qualified testers who have not been a part of the development process should be included in the testing phases.
- Identified vulnerabilities during cybersecurity testing should be analyzed; the disposition of the vulnerability and the rationale for how the vulnerability is managed should be documented.

The Automotive Information Sharing and Analysis Center (Auto ISAC[1]) is a community established by several companies from the various domains of the industry which focuses on light and heavy vehicle cybersecurity to analyze and share information across the industry. In collaboration with the Alliance of Automobile Manufacturers (Auto Alliance) and the Association of Global Automakers (Global Automakers), the community published a set of best practices document on automotive cybersecurity which points out both the technical and organizational aspects in the area [10]. Additionally, the documents are referred to by the NHTSA in the ”Cybersecurity Best Practices for the Safety of Modern Vehicles” document [7].

The series of documents comprises of 7 key cybersecurity functions. Each of the functions are investigated and best practices are discussed in a specific document [10]. The document “Security Development Lifecycle” covers the security needs and issues for the development process.

The document distributes the testing process into the different phases of development as follows [11]:

i. **Design:** This phase is where a high-level test plan can be constructed which identifies:
   - The best security verification methods (e.g. design review, manual code review, automated code analysis, component/unit testing, bench and vehicle penetration testing).
   - Needed testing tools including special build components and infrastructure support
   - An evidence sheet with details of software, hardware level, date, pass/fail status, notes on failures or unexpected behavior person running the test and approver, and others as necessary.

ii. **Implementation:** Secure implementation requires testing & verification in both hardware and software level. The methods for ensuring at the hardware level
   - Confirmation reviews or assessments
   - Penetration tests

   At the software level:
   - Code reviews
   - Automated code analysis
   - Penetration testing

iii. **Testing & Validation:** This part defines the whole process of testing through phases of the development lifecycle:
   (1). **Cybersecurity Testing:** The actual testing process is done during the implementation and post-implementation phase, which evaluates the proper working of safeguard mechanisms and identify potential vulnerabilities which leads to residual risk assessments.
   (2). **Internal Cybersecurity Sign-off Process:** The sign-off process includes the testing process which verifies the system is secure enough to withstand the previously assessed threats. Rather than assuring the system is 100% secure; it can assure the system is robust enough against previously defined attack profiles. A sign-off process should include the overall test plan, performed functional tests, penetration tests, source code audits, number of known vulnerabilities and their risk ratings, and open tests etc. If a project cannot be signed-off due to incomplete work, the overall risk should be assessed.
   (3). **Residual Risk Assessments:** Residual risk assessments can be done as a part of the development lifecycle on a periodic basis as the known residual risks evolve over time by the discovery of new attack methods or cost reduction due to newer/cheaper tools.

[1] https://automotiveisac.com

3.2.2. Asia

China

With the trend of intelligence and networking for vehicles, Chinese government ministries pay attention to the cybersecurity and data security of Intelligent and Connected Vehicles (ICVs). As a result, they issued numerous policies coping with that topic. To support these policies, corresponding standards committees are developing national standards of which the majority still are in draft version. In particular, three ministries work in the field of cybersecurity and data security of ICV: the Ministry of Industry and Information Technology (MIIT), Cyberspace administration of China (also called Office of the Central Cyberspace Affairs Commission), and the Ministry of Natural Resources.

The MIIT issued a Type approval document [12] on August 12, 2021. The type approval document covers a wide range of contents and mainly includes functional safety, safety of the intended function, cybersecurity, data security, software update and automatic driving data recording. On March 8, 2021, the ministry also issued a Standard system guideline [13], which contains 103 items. Only 12 of them are completed, 15 items are in progress and most of them are in planning. These standards involve technical requirements and management and process requirements. In the items system guideline, these standards are divided into 6 parts, including general and basic standards, terminal and facility cybersecurity standards, network communication security standards, data security standards, application service security standards and security assurance and support standards. The National Technical Committee of Auto Standardization (Abbreviated as “NTCAS”) has issued four national standards, including GB/T 40861-2021: General technical requirements for vehicle cybersecurity, GB/T 40857-2021: Technical requirements and test methods for cybersecurity of vehicle gateway, GB/T 40856-2021: Technical requirements and test methods for cybersecurity of on-board information interactive system, and GB/T 40855-2021: Technical requirements and test methods for cybersecurity of remote service and management system for electric vehicles. In GB/T 40857-2021, GB/T 40856-2021 and GB/T 40855-2021, there are two main parts: technical requirements and test methods. In the technical requirements, there are five parts: hardware, communication, operation system, application software and data. Besides, two more mandatory standards are planned: 20214423-Q-339: General technical requirements for software update of vehicles and 20214422-Q-339: Technical requirements for vehicle cybersecurity. Also, in late 2021, the MIIT has published two notices [14] [15] to address the cybersecurity requirement of connected vehicles. In these notices, it mandates that both cybersecurity and data security of connected vehicle should be fully considered before going to market. Building a complete vehicular security standard system is also prescribed to all sub-departments, organizations, and companies. Furthermore, ISO/SAE 21434 is being converted to Chinese national standards as well.

Technical Cybersecurity Requirements

For general technical cybersecurity requirements, NTCAS released the standard GB/T 40861-2021 “General technical requirements for vehicle cybersecurity” [16] October 2021, which involves the following in the scope of vehicular security:

- Software security
- electrical and electronic hardware security
- data security
- on-board communication security
- and V2X communication

Also, the authenticity, confidentiality, integrity, availability access control, anti-repudiation, auditability, and preventability should be considered to the corresponding security system if applicable. It requires that cybersecurity mechanisms in vehicles should achieve defense-in-depth, and the defense methods should not be limited to intelligence sharing, intrusion detection technology, dynamic information security policies, and collaborative measures between various information security modules to reduce the risk when abnormal behavior occurs. Compared to other standards, this standard provides the more complete technical requirements of in-vehicle cybersecurity.

There are also standards that address specific system of vehicle security: MIIT released “Security technical requirements for connected vehicle based on public telecommunication network” [17], which specified security requirement for on-board communication.

Test Practices

Meanwhile, some standards released by NTCAS focus on the technical requirement as well as test method of specified system and component. “Technical requirements for cybersecurity of electric vehicles charging system (draft for comments)” [19] addresses in-vehicle charging system and corresponding communication security. It further specifies detail test methods from hardware, software, data, and communication aspects. “Technical requirements and test methods for cybersecurity of on-board information interactive system” [20]**Error! Reference source not found.** c oncerns the security test methods for hardware, communication, operation system, application, and data. “Technical requirements and test methods for cybersecurity of vehicle gateway” [20] addresses hardware, software, communication, and data security for CAN gateway, ethernet gateway and hybrid gateway. “Technical requirements and test methods for cybersecurity of remote service and management system for electric vehicles” [21] involves on-board terminals security, communication security and platform security in the scope.

According to different kinds of cybersecurity, the Chinese standards also provide a few general best practices to test the security of:

Hardware:

- Check whether there are exposed debug interfaces and whether the interfaces have authentication mechanisms
- Check whether the PCB wiring and design are discreet
- Check whether there are any backdoors

Software:

- Check whether there is security boot mechanism, check whether the integrity of software is protected
- Check whether there are access control and integrity protection for software update
- Check whether there is log mechanism for important events
- Conduct vulnerability scan on software

Data:

- Test whether integrity is ensured by tempering data
- Test whether confidentiality is ensured by exporting data
- Check whether data is collected only after user approval
- Check whether sensitive information is well protected by security mechanisms
- Check whether integrity, confidentiality and availability are protected in data transmissions
- Check for the success of data erasure

Communication:

- Check whether authentication mechanism is applied in communication
- Check whether integrity, confidentiality, availability, and anti-reputation is ensured in communications

Management, Process and Lifecycle

Currently, the developed standards mainly focus on the technical requirements and test methods. The cybersecurity process, management, and lifecycle are not fully addressed in the current standards system. After the release of ISO/SAE 21434, NTCAS has started to convert the ISO/SAE 21434 to regional standard and the expected output is a suggestion standard to fill the gaps of the current standard system.

Data Security

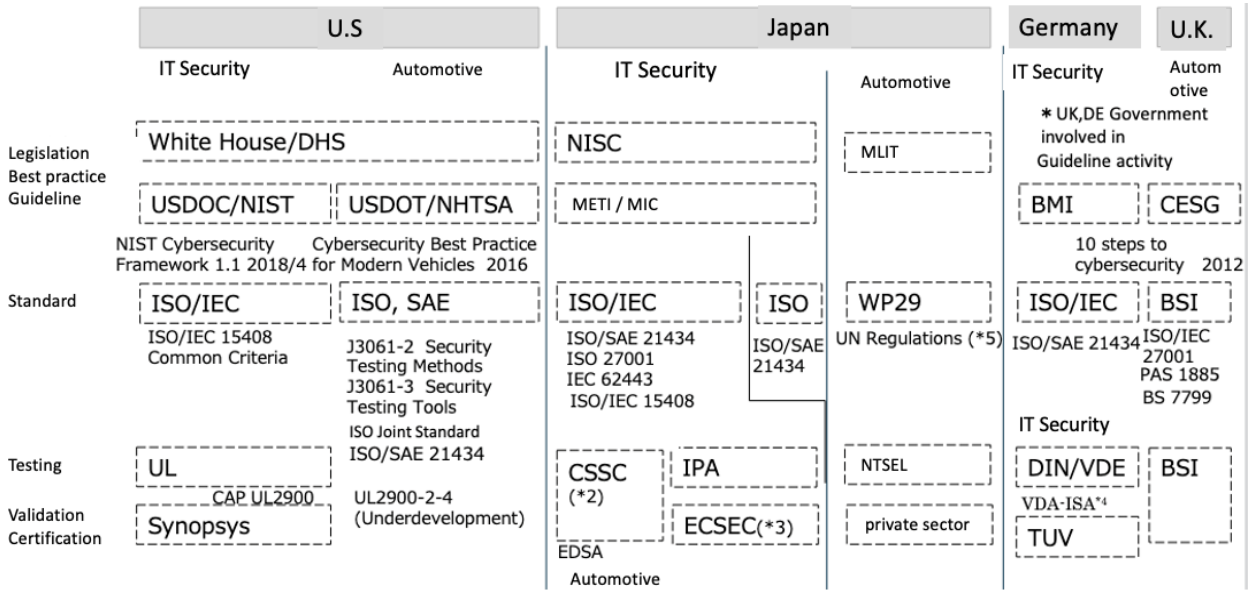
Data security is also a main concern in vehicle. A vehicle standard “Information security technology--Security requirements of vehicle collected data (draft for comments)” [20], which is dedicated for data security, was released in October 2021. Basic technical requirements for collecting, persisting, transmitting, and exporting data are listed in the standard.

Community Driven Standard

The community standard is the important supplement for the vehicle cybersecurity field, although the Chinese community standards in the vehicle field are not mandatory. The community standard is to pioneer reforms and to be supplement for national standard. China Society of Automotive Engineers (China-SAE) released "Intelligent and Connected Vehicles On-Board Terminal Cybersecurity Technical Requirements" [21], it further classified technical security requirement into 4 levels according to the different degrees of security assurance. And there are also a few other community driven standards which are put into agenda, this kind of standard will be an important part of the standard system in the future.

Japan

In Japan, cybersecurity for automotive is regulated by Japanese ministries. Based on the legislation, other governmental and industrial organizations conduct validation/certification to confirm that the produced vehicle satisfy the standards and requirements. Figure 1 displays Japan's automotive cybersecurity authorities and standards in comparison to the United States, Germany, and United Kingdom.



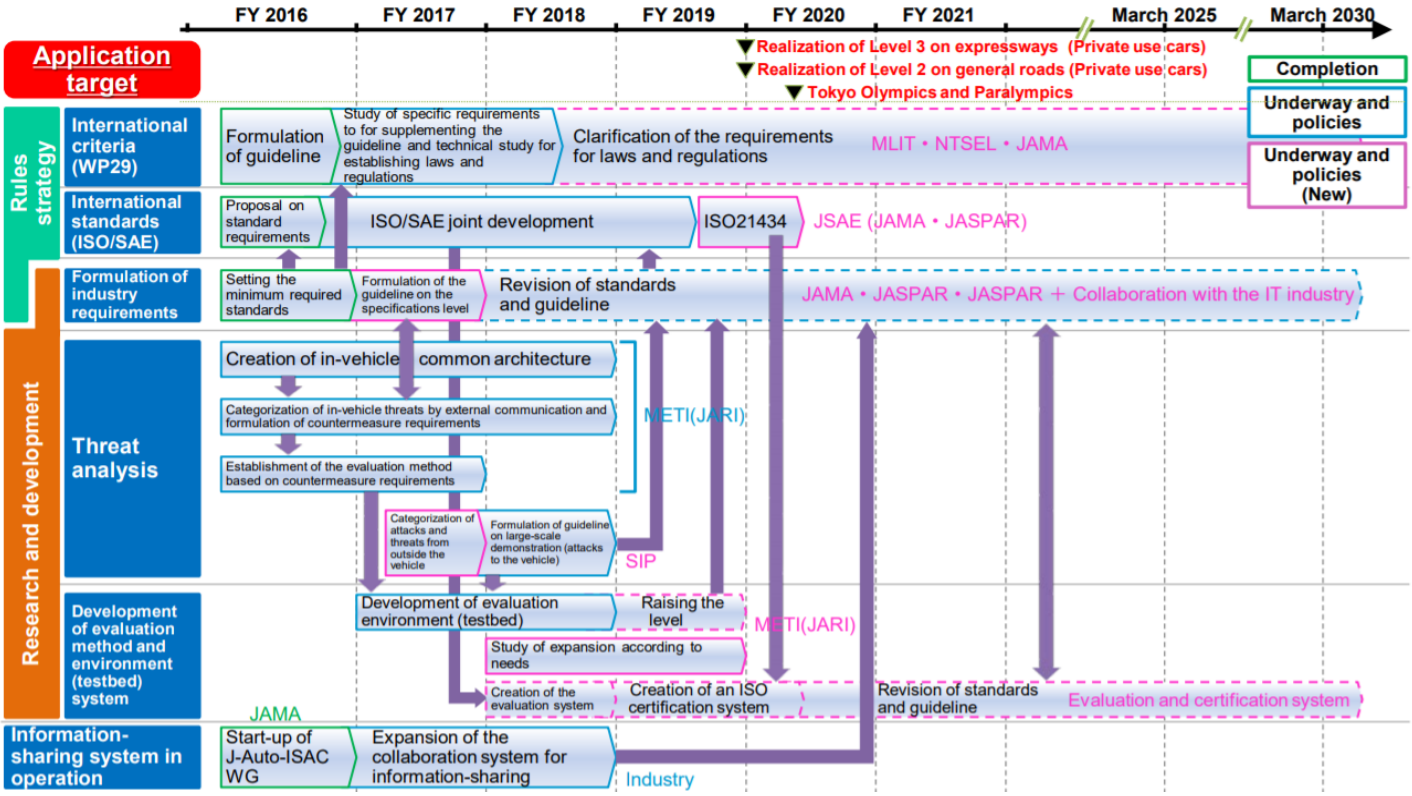
2 Control System Security Center (CSSC) – conducts research and development to handle cyber-attacks and ensure the security of control system of critical infrastructures.*
3 ECSEC Lab is an evaluation organization accredited in the field of IT products / systems and smart card (IC card) related devices.*
Figure 1: Comparison of cybersecurity automotive standards and responsible authorities[2]

Schedule for implementing ISO/SAE 21434

Japanese METI (Ministry and Economy, Trade, and Industry) published a document about cybersecurity measures for autonomous vehicles in 2018. This document describes the schedule for implementing ISO/SAE 21434. Firstly, JASPAR (Japan Automotive Software Platform and Architecture) collaborates with other countries to establish the standard while suggesting rules and policies that fit in Japanese automotive environment. While developing ISO/SAE 21434, METI and MLIT (Ministry of Land, Infrastructure, Transport and Tourism) create guidelines that describe requirements to develop and operate automotive vehicles, with some governmental organizations such as JASPAR. Besides, METI creates a more concrete guideline for testing and validation/certification of autonomous vehicles collaborating with organizations in industrial sector such as IPA (Information Processing Agency).

Until now, MLIT has published guidelines for requirements of autonomous vehicle development like [24] (Japanese). Also, IPA has published and revised more practical guidelines such as [25]. This guideline includes threat analysis and possible measures in a development cycle, namely management, planning, development, and operation.

[2] https://www.meti.go.jp/shingikai/mono_info_service/jido_soko/pdf/sanko_03.pdf



Japanese National Standards

National standards are determined by organizations such as JAPSAR, based on the international standards. The national standards describe requirements that the industry must meet in the development process against assumed security threats. Especially, they have formulated evaluation guide for ECU and hardware/software vulnerabilities. JASO TP-15002 guideline is an evaluation guideline for automotive information security analysis.

Japan Automotive Software Platform and Architecture (JASPAR) is a collaboration project of engineers from the automotive industry. The aim of JASPAR is:

"Identify common issues that will be faced in the future in the car electronics sector, and then undertake standardization initiatives aimed at resolving those issues, creating common objectives across the entire automotive industry."

The JASPAR project provides reference architectures for secure design of automotive components and verification testing. The standards are focused on areas of cybersecurity of car electronics where there are gaps in other available standards and areas which are a priority for the Japanese automotive industry. These include Software-Over-The-Air updates, ECUs, CAN-FD, secure communication, and vehicular messaging.

Table 1, from the JASPAR project details a list of standards applicable to cybersecurity testing of automotive products.

Standard Code	Standard Title	Year of Publication
TD-CST-4	ECU Penetration Testing Guide Version 1.0	2020-04-10
ST-CST-1	ECU Vulnerability Test Requirements Ver.1.1	2020-05-15
ST-OTA-09	OTA Software Update Compliance Test Specification -OTA Master Ver.1.0	2020-08-07
ST-OTA-10	OTA Software Update Compliance Test Specification -Target ECU Ver.1.0	2020-08-07

Table 1: JASPER standards and technical documents for testing of automotive electronics[3]

[3] https://www.jaspar.jp/english/standardDocumentFrom2018?select_tab=all

An exhaustive list can be found here: https://www.jaspar.jp/english/standardDocumentFrom2018 The testing standards detail the actions of the development team and the test team in each phase of the testing process. The OTA software compliance testing specifications provide more granularity, detailing the individual test cases to be implemented on the ECU or OTA Master and the testing criterion.

Republic of Korea

Two main actors in Korea for type approval and certification of vehicles are:

- Ministry of Land and Infrastructure, Transport (MOLIT)
- Korea Automobile Testing & Research Institute (KATRI)

In June 2020, MOLIT established the UNECE R.155 international standards for automotive cybersecurity as the main content for recommendations for ROK automotive manufactures. The central component being that the automotive manufacturer has a cybersecurity management system (CSMS) and demonstrate that automotive cybersecurity is managed accordingly. To integrate UNECE R.155 local laws and regulations will be amended as appropriate.

There are two regulations which pertain to the testing and evaluation of automotive:

- Korea Motor Vehicle Safety Standard (KMVSS) - Technical Regulation
- Korea Vehicle Management Act (Self-Certification system and Safety Standards for Motor Vehicles)

Strategy to improve Automotive Cybersecurity

	Y2020	Y2021	Y2022	Y2023	Y2024
National legislation and rulemaking	Automotive cybersecurity guideline	Amend 'Motor Vehicle management Act'	Amend the regulation	Issue Automotive Cybersecurity law and safety/security regulation	
Automotive cybersecurity Support and Response system	Planning	Establish/Operate Automotive cybersecurity committee			
		Build Automotive cybersecurity center with Pilot			Advancedment
			Build Automotive Cybersecurity Knowledgebase		

Figure 2: Republic of Korea Automotive Cybersecurity Regulatory Timeline

MOLIT plans to issue the Automotive Cybersecurity law and safety/security regulation in 2022. Until that time, they will have published recommendations and guidelines to fill the gap between the practice of automotive company and the requirements imposed by the registration such as Korea Motor Vehicle Safety Standard (KMVSS) Korea Vehicle Management Act. This means that they are trying to make it easy for automotive manufactures to adapt to the new scheme by publishing recommendations step-by-step.

As one of the recommendations, MOLIT announced guidelines for security of autonomous vehicles on December 15, 2020. ·The guidelines include (1) Ethical Guidelines for Self-Driving Vehicles, (2) Automobile Cybersecurity Guidelines, and (3) Level 4 Autonomous Vehicle Manufacturing/Safety Guidelines, which provide basic directions for ethics and safety.

Among that, Automobile Cybersecurity guidelines introduced recommendations for security policy directions so that automobile manufacturers, etc. can develop a cybersecurity system to prepare for the implementation of the security standards to be issued in 2022. An overview can be found as a press release from MOLIT[4].

The recommendation proposed in the guidelines are the followings:

- Security management such as a process for identifying, evaluating, classifying, and managing security threats must be established within the manufacturer's organization. and share relevant information.

[4] https://www.molit.go.kr/USR/NEWS/m_71/dtl.jsp?id=95084902

- Vehicle security threat identification, evaluation, security measures, and sufficient security-related pre-tests must be performed. Note that security measures include cyberattack detection and prevention measures, risk monitoring support measures, data forensics support measures for cyberattack analysis, etc.

The security policy direction shown in the guideline is:

> Ministry of Land, Infrastructure and Transport '22.
>
> *In July, we plan to revise the Automobile Management Act and subordinate statutes with the goal of implementing domestic standards.*
>
> *Furthermore, the government plans to build an automobile security center to test and evaluate vehicles according to security standards and monitor cyber threats.*

3.2.3. Europe

The EU has a diverse range of regulatory initiatives for cybersecurity of the digital marketplace which impact upon automotive product development. The EU Cybersecurity Act (CSA) is the predominant form of regulation for cybersecurity in the EU market. Amongst the range of important initiatives, the CSA establishes a framework for certification of ICT products for cybersecurity called the Common Criteria based European candidate cybersecurity certification scheme (EUCC). The aim of the scheme is to enable, for the consumer, transparency, and awareness of the level of assurance for cybersecurity of a digital product. The EUCC is still in development and its impact on the automotive sector is yet to be detailed.

The EU Cyber Resilience Act (CRA) is currently being developed. This regulation will focus on providing common cybersecurity rules for manufacturers and vendors of tangible and intangible digital products and ancillary services. The CRA regulation envisages a process for the digital product cybersecurity assurance where essential baseline security requirements are defined which can be applied selectively according to a risk management assessment of a device's intended use, considering the ecosystem or 'operational environment' in which the device will be placed. The products to be governed by the CRA include:

- Connected product: A finished product that is intended to communicate directly or indirectly over the internet.
- Finished product: A product usable for its intended functions without being embedded or integrated into any other product. Components of a device, such as a processor or a sensor, should be outside the scope as security functionalities need to be assessed holistically.

In the public submissions to the CRA regulation, automotive industry bodies (European Automobile Manufacturers' Association, European Association of Automotive Suppliers, TÜV Association) pointed to other existing legislation as impacting automotive cybersecurity:

- Type-approval: UN R.155 and R.156
- Radio Equipment Directive (2014/53/EU) and its delegated act (2022/30) [For Connected Vehicles]
- NIS 2 Directive (2020/0359(COD))

As the EU CSA is in policy implementation phase and the EU CRA is in policy conception phase, there is a sparsity of detail as to how automotive technologies will be validated and verified for cybersecurity.

Germany

The document "Application of the Rules for designation/recognition for technical services (categories A, B, D) for testing in the context of the KBA-type approval procedure according to UN-R 155/156" [24] was created and published by the KBA outlining binding rules and guidance for the nomination of technical services with regards to R.155 and R.156.

This document describes several procedures and rules, including specifics regarding cybersecurity testing. Note that such procedures present the minimal requirements for technical services, who are then expected to set up their own procedures and rules to interpret and implement such requirements.

Definitions:

The KBA differentiates between several types of testing:

- Functionality Test: Tests whether the security measures specified by the manufacturer meet their objective (e.g. testing a secure communication protocol regarding its suitability for software update).
- Security Test: Active attempt by a tester to circumvent security measures (e.g. penetration tests).
- Witnessing: Assessment of the performance of testers/auditors by the KBA or a body commissioned by it. The witness-assessor generally does not directly influence the activities of the tester/auditor.

Responsibilities: The technical service is responsible for the assessment and testing of the vehicle and the auditing of the CSMS/SUMS processes. However, the approval authority may at its discretion perform additional tests. Technical services must also be designated for “whole vehicle” approval in order to be allowed for the R.155/R.156 approval.

Qualifications: Authorized signatories must have several qualifications in order to be allowed to perform the required testing according to R.155/R.156, such as in-dept knowledge of testing and of vehicle, risk analysis, auditing etc. It is also allowed that technical experts support the authorized signatory in case he lacks the knowledge/skills in a specific area.

Document Review: For testing, the following documents must be submitted in addition to several other process related documents:

- Risk analysis with associated initial and test information
- If applicable, a list of CSMS/SUMS-relevant suppliers/service providers/subcontractors with their respective duties and responsibilities and an assessment of the relevant risks
- Procedures, test plans, test instructions and any other documents related to CSMS
- Overview of test results

The test report must also meet the requirements of the designation rules and include:

- Test Plan incl. justification
- Expected test results
- Test results
- Justification of any deviations accepted
- Additional peculiarities if available

General test requirements: The KBA requires at least 1 practical test per regulation (R.155/R.156) to be performed or witnessed by the technical service. It is recommended that such tests are planned based on the risk analysis/ worst case scenario, security objectives, recommendations present in the document (will later be shown).

Based on the result of this tests, additional tests are required to be carried out or witnessed by the technical service. These must focus on the most significant risks. The vehicle itself as well as the connected backend should be considered.

It is additionally required that significant claims by the manufacturer must be verified by the technical service (e.g., an update does not affect other parts of the vehicle).

Test approach requirements: The KBA does not explicitly require the execution of tests in the technical service’s laboratory. Instead, this is recommended in case the necessary test equipment is available. The manufacturer is expected to provide assistance with necessary information and tools.

Test witnessing (supervision): Witnessing begins by assessing the manufacturer’s testing capabilities and processes (can be part of the CSMS/SUMS audit). It can have a restricted focus on the essential phases (e.g., risk analysis, HW/SW, test bed etc.). The technical service is expected to define his own guidelines for test type, equipment, test environment, attack method and target etc.

Note that in case of witnessing and/or 3rd party equipment is used, the integrity of the hardware and software used must be ensured. The reproducibility of tests must also be ensured for at least 10 years after production has been discontinued.

Additional recommendations:

It is recommended for the technical service to design its own tests, and not just reproduce the manufacturer's tests. Additionally, a risk-based approach should be followed while selecting and testing the vehicle interfaces. External interfaces take priority in this selection. Random sample testing of internal components and other internal security-dependent components can be tested.

It is additionally recommended that the technical service carries the tests in its own laboratories. In all cases, the responsibility for the suitability of the equipment and methods used for testing lies solely with the technical service. Standards like ISO/IEC 17020 and ISO/IEC 17025 can support to create confidence in the work of test labs.

As for the type and level of attacks to be used: the level of attack is chosen on a case-by-case basis depending on the risk assessment. A minimum level of attack should be set factoring the available time, expertise, knowledge, and tools. White/Grey-Box test approaches are recommended for performing security tests. Additionally, it's strongly recommended for the technical service to perform independent research regarding vulnerabilities and that individually specified penetration tests are performed on vulnerable interfaces.

General Test Approach:

(1). Review manufacturer documentation: this must include the required documents by R155/R156, which are checked for completeness, accuracy, and plausibility.
(2). Define test specification and test plan: the technical service will select relevant functionality and security tests to be performed. At least one test should be chosen for the threat groups of R155 Annex 5 Table A1 if applicable. A justification must be provided otherwise. A test plan must include the expected results and the specification of test aspects including scope and coverage.
(3). Define test environment: At this stage, a suitable test environment must be chosen either at the technical service's own lab, external lab or at the manufacturer's premises.
(4). Kick-off testing and White-Box testing (optional): Here the manufacturer discloses design/interface information on the test subject.
(5). Execute tests: Tests are carried out and results are properly documented
(6). Prepare test report: results are combined in a structed test report and submitted to KBA

Note regarding R156: relevant cybersecurity and functionality tests are performed similarly to the approach described above.

Additionally, the Quality Management Center (QMC) of the German Association of the Automotive Industry (Verband der Automobile industry – VDA) issued a supplement to the process management specification Automotive SPICE (Software Process Improvement and Capability Determination), that conforms with ISO 15504 [27]. This supplement, called Automotive Spice for Cybersecurity Engineering [28], defined a set of process steps dedicated to cybersecurity engineering that is to be used in conjunction with the current Automotive SPICE process; namely:

- SEC.1 Cybersecurity Requirements Elicitation
- SEC.2 Cybersecurity Implementation
- SEC.3 Risk Treatment Verification
- SEC.4 Risk Treatment Validation, and a new management step
- MAN.7 Cybersecurity Risk Management, as well as expanding the acquisition step
- ACQ.2 Supplier Request and Selection

In particular, the risk treatment verification prescribes a specification that is suitable to provide evidence for compliance with the security requirements and the design implementation and component integration is to be tested using defined test cases (according to a verification strategy that is derived from the requirements and implementation).

The corresponding best practices provides hints on what to test:

- Requirements-based testing and interface testing on system and software level,
- Check for any unspecified functionalities,
- Resource consumption evaluation,
- Control flow and data flow verification, and

- Static analysis; for software: static code analysis e.g., industry recognized security-focused coding standards.

As well as some testing techniques (non-exhaustive):

- Network tests simulating attacks (non-authorized commands, signals with wrong hash key, flooding the connection with messages, etc.), and
- Simulating brute force attacks,
- Audits,
- Inspections,
- Peer reviews,
- Walkthroughs,
- Code reviews.

Test cases could be derived by:

- Requirements analysis,
- Building equivalence classes,
- Testing edge cases (boundary values),
- Experience-based testing.

The specification also proposes to establish bidirectional traceability between the verification activities and the system design. Analogously, the risk treatment has to be validated, which means the adequacy of the implemented measures (whereas the verification assures the compliance of the measures with the requirements). The validation includes activities to also detect previously unidentified vulnerabilities (e.g., through penetration testing), while the methodology is similar to the verification.

France

The French Ministry of the Interior (Ministère de l'Intérieur) issued a position paper on automated driving (L'automatisation des véhicules) [29] that contains an annex covering cybersecurity (Annexe 9: la Cybersécurité). Regarding testing, this annex contains the notion to use risk analyses, compliance audits and penetration tests. The Agence nationale de la sécurité des systèmes d'information (ANSSI) states in an analysis of contributions for a – generic, but also including vehicles – cybersecurity certification schemes the usage of static source code analysis tools, vulnerability scanners, automation of configuration audit and protocol fuzzers for verification [30], which is, however, a very high-level recommendation.

United Kingdom

BSI PAS 1885:2018 [31] details key principles of cybersecurity for connected and automated vehicles. Eight principles are detailed in the standards. These principles focus on; organizational management of cybersecurity risks, management of the supply-chain, 3rd parties and subcontractors and recommendations for cybersecurity design, resilience, and response measures. Principle 6 – The security of all software is managed throughout its lifecycle, proscribes a list of recommendations for testing and evaluation of vehicular software:

- 10.1.5 summary: open source or 3rd party software should be reviewed for vulnerabilities using formal code inspection reviews. Automated tools should be used to analyze the structure and security of the code.
- 10.2 summary: configuration and management control should include evidence of testing, including test scenarios and results. Also, unresolved test defects, deficiencies and anomalies should be documented.
- 10.3.3 summary: updates shall be tested and

The principles contained in the standard provide a good reference point for the management of cybersecurity risk and considerations for design of secure automotive systems.

4. Process and Tools Survey

In order to gain a picture of current practices used in the industry, we issued a qualitative survey (2022) among the IAMTS' members and trusted partners. The survey's results give a picture of which kind of testing is performed, which testing methodologies and processes are used and which tools are sensible to utilized for these purposes.

Functional security and penetration testing is widely proliferated

Two-thirds of respondents confirmed that they utilize functional testing and penetration testing within their verification and validation processes which support the entire automotive development lifecycle. Validation activities were conducted close to the end of the product development phase and before release for post-development and consisted of analysis and testing. Verification activities were conducted during the concept and product development phase and consisted of review, analysis, and multiple rounds of penetration testing. One-third of respondents have not yet adopted the cybersecurity verification and validation processes of the ISO/SAE 21434 standard.

Bias towards COTS and open source

Respondents use a diverse range of COTS, open-source, customized and in-house (internally developed) tools in their penetration testing activities. The results show a bias towards COTS and open-source tools.

The respondents also identified a number of tools which were used to test recent high-profile vulnerabilities such as BlueBorne (a well-known Bluetooth attack) and ROCA (cryptographic weakness). With the emphasis ISO/SAE 21434 places on TARA, it is apparent that automotive cybersecurity testers are agile in developing and utilizing toolsets to keep pace with the dynamic threat environment.

Tools specifically mentioned by respondents can be categorized as the following:

Tool Category	Description	Automotive Test Usage
Vulnerability Assessment	Enables performance of a scan of a device or information system to discover vulnerability of the target system to known vulnerabilities. Example tools: Nessus, Nmap	Nmap and Nessus could be used to find open communication ports on an infotainment head-unit and its vulnerabilities.
Web-Application	Enables analysis of the codebase of web-applications and mobile device applications. Example tools: BurpSuite, Android Studio	Predominantly used in the testing of infotainment systems and customer applications.
Reverse-Engineering	Used for reviewing of the codebase of the application to enable identification of vulnerabilities (Logic, Syntax etc.). Example tools: IDA Pro, Ghidra, Volatility.	Predominantly used for reverse-engineering of firmware and software-over-the-air updates (SOTA). Tools such as volatility are used for data extraction from volatile memory for analysis.
Tool Category	**Description**	**Automotive Test Usage**
Protocol Analysis	Enables analysis of the protocol (wireless, radio, Bluetooth, CAN) to understand the communication architecture and identify vulnerabilities such as weak encryption, authentication, and access control. Example tools: Wireshark, GNU Radio Companion, Universal Radio Hacker, CANoe, genymotion.	Used for automotive networks. Internal networks (CAN, LIN, MOST, FlexRay) and External networks (Wireless, Radio, Bluetooth).
Fuzzing	Used to assess the security of a system to unsanitized data input. This can either be randomized or targeted unsanitized data input. It is popularly used in software engineering to identify bugs in the codebase.	Fuzzing strategy and tools are most important for cybersecurity testing for OEMs and are therefore likely to be customized tools or in-house developed tools which have been designed for alignment with the OEM

	Example tools: OWASP ZAP, Beyond Security beSTORM, Synopsys Defensics	software development processes. Fuzzing is used ubiquitously in automotive environments from the embedded hardware ECUs to the infotainment system.

ISO/SAE 21434 is the most widely used standard

Overwhelmingly, ISO/SAE 21434 is used for cybersecurity verification & validation. Respondents also mentioned well-established, complimentary standards such as ISO/IEC 15408 (Common Criteria) and ISO/IEC 27034 (Application Security Standards).

The testing process for SUTs are mainly conducted on a case-by-case basis. The limited use of test matrix and standard test sets can be seen as due to a variety of reasons including; repeatable test processes cannot be ubiquitously applied to diverse range of automotive technologies, level of integration and architecture requires testing to be approached on a case-by-case basis, lack of development and adoption of testing metrics and criteria, cybersecurity testing is still developing and there is a lack of adoption of testing processes that support automation and repeatable testing.

OEMs conduct functional testing, vulnerability scanning, penetration testing and fuzz testing. All of these test procedures are recommendations of ISO/SAE 21434 and are essential as part of an automotive cybersecurity testing program.

Specifications coverage is the most popular method to measure and maximize test coverage of the SUT. This aligns with product development lifecycle and the focus on assurance for the intended functionality of the automotive component. Emerging methods include considerations for the requirements from UN R.155.

ECUs are the most common test target

ECUs (Electronic control units) are the most common test targets because it is the most common components in the vehicle architecture.

E/E components remain the predominant areas of focus for SUT due their importance for functionality of the vehicle. Due to the preponderance of connected vehicular technologies, communication protocols are an area of concentric concern for cybersecurity testing. Emerging SUTs include the end-to-end driving technology which supports autonomous-assisted and autonomous driving.

Third-party service providers for verification and validation are popularly used due to their existing experience of testing and certification, alignment with ISO/SAE 21434 and other standards which emphasize the use of third parties for independent verification and validation and lack of available skills for cybersecurity testing of automotive products. A majority of respondents answered that they have an established interface agreement for cybersecurity testing. Most OEMs follow a document-based audition process in their verification and validation agreement.

Model- and risk-based approaches are the state of the art

There are two principal groups of system analysis for test case derivation:

- Model-based approaches (threat modeling, attacker modeling) and
- Risk-based approaches (most prominently TARA – Threat Analysis and Risk Assessment).

a) **Model-based approaches** generally model the SUT in a form suitable for analysis. Threat modeling ordinarily involves two models:
   - An architectural model, illustrating the assets, data flows and trust boundaries of the system (e.g., a data flow diagram) and
   - A threat model defining a ruleset which kinds of assets, information flows, etc. are subject to which threats.

This yields a comprehensive (depending on the threat database), structured analysis of the threats applicable to the system, for which countermeasures can be defined which presence pose the security requirements that can be verified through testing [32].

b) **The risk-based approaches** examine the SUT in a systematic way in order to identify and prioritize threat scenarios that lead to testable requirements. Apart from the item definition, which identifies the assets the complete SUT consists of, a TARA includes [33]:

Threat analysis (Systematically, often using standardized lists, analyzing potential threats for each identified asset)

- Impact assessment (estimating the damage inferred by the respective threat; often in the form of a "traffic light" system for general comparability)
- Risk assessment (estimating the probability of occurrence and multiplying it with the impact factor)

In our survey, we saw a roughly even distribution of the two sets of approaches. Obviously, they can be combined: results from the threat/attacker modeling could serve as an input for the risk assessment.

Most test cases are generated based on requirements and specifications

There are a couple of ways to derive test cases from a performed asset/security analysis: based on derived requirements based on a model (e.g., a TARA, cf. previous section) that could also be subject to model checking; based on specifications (both standards and vendor specifications), based on the structure (i.e. the architecture – e.g. tests that verify the correctness of a security gateway's functioning), based on the experience of the respective penetration tester (i.e. trusting the right test cases to be designed to expert knowledge) or based on known faults. The respondents roughly evenly perform requirements, specification, and experience-based test derivation, while structure-based tests are significantly less (one third) used, and fault-based testing is not used at all. An additional source of information is UNECE's Regulation 155 (see above in the respective section) [3]. In its Annex 5 it defines a catalogue of countermeasures that can serve as requirements that might be verified by testing.

Regarding the testing methods, it is equally proliferated to use white box (full access to information about the SUT), black box (just the SUT "as is", with no additional information) and gray box (some information, mainly handbooks, API documentation, etc.) approaches.

Only a minority (one third) of the respondents claimed that they use a baseline for testing. This means a minimum set of tests generically issued to all of their SUTs, regardless of their nature. The relative majority of those uses testing the requirement specification followed by using prepared test plans, test cases and test data and, lastly, testing the design specification and predefined generic tests for the source code itself.

One specific test set mentioned is testing all wireless and wired interfaces (e.g., OBD) for their susceptibility to act as an entry vector into the vehicle.

When asked for specific tools during the phases of an attack test – pre-attack (scanning, CAN analysis, etc.), attack (exploit frameworks, etc.), and post-attack (reporting, life cycle management) – respondents answered with a variety of tools.

The following table gives an overview on the tools used by respondents:

Category	Tool	IP Network/ Web	Wireless	Automotive IVN	Reverse Engineering	Description
Reconn-aissance	Nessus[5]					One of the most proliferated IT vulnerability scanners. There is also an open-source variant with the Greenbone/OpenVAS[6] scanner.
	Nmap[7]					State of the art in ethernet port scanning tools.
	Dirbuster[8]					The OWASP project's web directory fuzzing tool.
	Bluescanner [9]					A reconnaissance tool for Bluetooth devices
	Wireshark[10]					Sate of the art in packet sniffing
	GNU Radio Companion [11]					GNU radios gui, used for analyzing wireless signals
	CANoe (Vector)[12]					De-facto standard tool for CAN bus message analysis
Attack tools	Ghidra[13]					Open-source tool for binary reverse engineering originally developed by the NSA
	Android Studio[14]					Android development tools (mainly used for analyzing/debugging software for infotainment units)
	Aircrack Suite[15]					WiFi network security assessment tool
	URH[16]					Wireless protocol reverse engineering tool
	Volatility[17]					Open-source memory analysis tool
	Genymotion [18]					Android debug tool
	IDA[19]					Commercial tool for binary reverse engineering, available in multiple versions (e.g. free and pro)
	Burpsuite[20]					Web vulnerability testing suite
PLC	PTC Integrity[21]					Software life cycle management

[5] https://www.tenable.com/products/nessus
[6] https://www.openvas.org/
[7] https://nmap.org/
[8] https://sourceforge.net/projects/dirbuster/
[9] https://sourceforge.net/projects/bluescanner/
[10] https://www.wireshark.org/
[11] https://wiki.gnuradio.org/index.php/InstallingGR
[12] https://www.vector.com/at/de/produkte/produkte-a-z/software/canoe/
[13] https://ghidra-sre.org/

5. Conclusion

From the review of the regional standards and regulations, the predominance of UNECE R.155 and its associated standard ISO/SAE 21434 is apparent. Regulatory reform for cybersecurity of automotive products has begun enshrining the requirements set out in R.155. Furthermore, larger markets, such as the EU, are developing approaches to increase transparency and awareness of the consumer for the level of cybersecurity of a digital product, including in the automotive sector. Government and industry are supporting the development of automotive cybersecurity through industry standardization efforts centering on cybersecurity assurance and secure-by-design architecture. Currently, guidance on how to test automotive systems is limited to specific use-cases focusing on connected and electronic/embedded systems. The requirements on OEMs and suppliers for V&V testing is aligned to the requirements of R.155, which, at its foundation level, OEMs and suppliers need to demonstrate testing according to TARA and within an overarching CSMS.

The survey on common current practices of automotive cybersecurity testing revealed that testers mostly follow the procedures of ISO/SAE 21434 in their security analyses to conduct a risk assessment- and requirements-based[22] testing approach, also relying on the recommendation in UNECE R.155's Annex 5 that describes some widely proliferated threats against systems within its scope. Apart from that, external testers often derive tests from test specifications defined by customers. Commonly, the test targets by OEM's are at the single component (ECU) level – system (full vehicle) level tests, as well as non-ECU targets (e.g., infotainment or telematics units) are less common. The survey found also that tests are ordinarily either pure functional security tests (presence and/or correctness of a certain security measure) or free penetration tests. For the tools in use, there seems to be a bias towards commercial-off-the-shelf and open-source tools, as opposed to customized and purely internally used hand-crafted tools. These results, in conjunction with the relative novelty of both R.155 and ISO/SAE 21434, hint towards the assumption that the productive industry currently concentrates on the required cybersecurity engineering and will take care of providing evidence for idem when mastering it.

A starting point for defining functional test is to segment the overall system into problem fields, e.g., testing the correct function of secure onboard communications (SecOC) and defining functional tests like manipulating the data, the message authentication code (MAC), the freshness value, etc. and determining the system's reaction (e.g., discarding the packet, etc.).

[14] https://developer.android.com/studio
[15] https://www.aircrack-ng.org/
[16] https://github.com/jopohl/urh/releases
[17] https://github.com/volatilityfoundation/volatility
[18] https://www.genymotion.com/
[19] https://hex-rays.com/ida-free/
[20] https://portswigger.net/burp
[21] https://www.ptc.com/en/products/windchill/integrity
[22] Requirements could thereby be drawn out of defined countermeasures against relevant threats identified in a TARA (threat analysis and risk assessment)

6. Contact Information

To learn more about the International Alliance for Mobility Testing and Standardization™, please visit http://iamts.org

Contact: info@iamts.org

7. Contributors

Stefan Marksteiner, AVL List

Andrew James Roberts, Tallinn University of Technology

Müjdat Soytürk, Marmara University

Berkay Yaman, Marmara University

Tomoya Tanaka, Tallinn University of Technology

Yi Yang, AVL China

Yangyang Liu, CATARC China

Mohammed Fares Abid, TÜV SÜD Auto Service

Karel Jansky, TÜV SÜD Auto Service

Christian Pahlke, TÜV SÜD Auto Service

Vladislav Kocián, TÜV SÜD Czech

Eyal Traitel, Cybellum

Marijan Jozic, OCTONX (SAE-ITC Affiliate)

Eddie Lazebnik, Cybellum

8. References

[1] United Nations Economic and Social Council – Economic Commission for Europe, “Cyber Security and Cyber Security Management System,” United Nations Economic and Social Council - Economic Commission for Europe, Brussels, Regulation 155, 2021.

[2] United Nations Economic and Social Council - Economic Commission for Europe, “Software update and software update management system,” United Nations Economic and Social Council - Economic Commission for Europe, Brussels, Regulation 156, 2021.

[3] United Nations Economic and Social Council - Economic Commission for Europe, “UN Regulation on Uniform Provisions Concerning the Approval of Vehicles with Regard to Cyber Security and of Their Cybersecurity Management Systems,” United Nations Economic and Social Council - Economic Commission for Europe / United Nations Economic and Social Council - Economic Commission for Europe, Brussels, ECE/TRANS/WP.29/2020/79, 2020.

[4] International Organization for Standardization and Society of Automotive Engineers, “Road Vehicles – Cybersecurity Engineering,” International Organization for Standardization, ISO/SAE Standard 21434, 2021.

[5] Transport Canada, “Canada’s Vehicle Cyber Security Guidance,” Transport Canada, T46-61/2020E, 2020. [Online]. Available: https://tc.canada.ca/sites/default/files/2020-05/cyber_guidance_en.pdf

[6] National Highway Traffic Safety Administration, “Understanding NHTSA’s Regulatory Tools,” National Highway Traffic Safety Administration, Washington, D.C., Report, 2017. [Online]. Available: https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/understanding_nhtsas_current_regulatory_tools-tag.pdf

[7] National Highway Traffic Safety Administration, “Cybersecurity best practices for modern vehicles (Draft Update 2020),” National Highway Traffic Safety Administration, Washington, D.C., Draft Update of DOT HS 812 333, 2020. [Online]. Available: https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/vehicle_cybersecurity_best_practices_01072021.pdf

[8] National Highway Traffic Safety Administration, “Memorandum re: NHTSA’s Cypersecurity Program,” National Highway Traffic Safety Administration, Washington, D.C., Memorandum NHTSA-2014-0071-0007, 2014.

[9] National Highway Traffic Safety Administration, “Cybersecurity best practices for modern vehicles (Draft Update 2021),” National Highway Traffic Safety Administration, Washington, D.C., Notice NHTSA-2020-0087, 2021.

[10] Automotive Information Sharing and Analysis Center, “Best Practices,” Automotive Information Sharing and Analysis Center, 2016. [Online]. Available: https://automotiveisac.com/best-practices

[11] Automotive Information Sharing and Analysis Center, “Best Practices - Security Development Lifecycle,” Automotive Information Sharing and Analysis Center, 2020. [Online]. Available: https://automotiveisac.com/best-practices-security-development-lifecycle

[12] The Ministry of Industry and Information Technology of China (MIIT), “Suggestions on Strengthening the Type Approval Management of Intelligent & Connected Vehicle

[13] The Ministry of Industry and Information Technology of China (MIIT), “Guidelines for the construction of Internet of Vehicle cybersecurity and data security standard system,” MIIT, 2021. [Online]. Available: https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2022/art_e36a55c43a3346c9a4b31e534b92be44.html

[14] The Ministry of Industry and Information Technology of China (MIIT), “Opinions of the Ministry of Industry and Information Technology on Strengthening the Management of Smart Connected Automobile Manufactures and Product Permit,” MIIT Equipment Industry 103, 2021. [Online]. Available: http://www.gov.cn/zhengce/zhengceku/2021-09/16/content_5637709.htm

[15] The Ministry of Industry and Information Technology of China (MIIT), “Notice of the Ministry of Industry and Information Technology on strengthening the cyber security and data security of internet of vehicles,” MIIT Cybersecurity 134, 2021. [Online]. Available: http://www.gov.cn/zhengce/zhengceku/2021-09/16/content_5637709.htm

[16] National Technical Committee of Auto Standardization, “General technical requirements for vehicle cybersecurity,” GB/T 40861–2021, 2021.

[17] The Ministry of Industry and Information Technology of China (MIIT), “Security technical requirements for connected vehicle based on public telecommunication network,” YD/T 3737–2020, 2020.

[18] National Technical Committee of Auto Standardization, “Technical requirements and test methods for cybersecurity of on-board information interactive system”,GB/T 40856-2021,2021

[19] National Technical Committee of Auto Standardization, “Technical requirements for cybersecurity of electric vehicles charging system (draft for comments),” GB/T, 2022.

[20] National Technical Committee of Auto Standardization, “Technical requirements for cybersecurity of vehicle gateway,” GB/T 40856-2021,2021.

[21] National Technical Committee of Auto Standardization, “Technical requirements for cybersecurity of remote service and management system for electric vehicles,” GB/T 40855-2021,2021.

[22] Chinese National Information Security Standardization Technical Committee, “Information security technology--Security requirements of vehicle collected data (draft for comments)”,2021

[23] China Society of Automotive Engineers (China-SAE), “Intelligent and Connected Vehicles On-Board Terminal Cybersecurity Technical Requirements”,2018

[24] Japanese Ministry of Land, Infrastructure, Transport and Tourism Automobile Bureau (国土交通省自動車局), “Safety technical guidelines for self-driving vehicles (自動運転車の安全技術ガイドライン),” Japanese Ministry of Land, Infrastructure, Transport and Tourism Automobile Bureau, 2018. [Online]. Available: https://www.mlit.go.jp/common/001253665.pdf

[25] Information-Technology Promotion Agency, Japan, “Approaches for Vehicle Information Security,” Information-Technology Promotion Agency, Japan, 2013. [Online]. Available: https://www.ipa.go.jp/files/000033402.pdf

[26] Kraftfahrt-Bundesamt, “Application of the Rules for designation/recognition for technical services (categories A,B,D),”Kraftfahrt-Bundesamt,2021.[Online].Available: https://www.kba.de/EN/Themen_en/Typgenehmigung_en/Zum_Herunterladen_en/BenennungTechnischerDienste_en/anwendung_Regeln_TD_R155_R156_en.pdf?__blob=publicationFile&v=4

[27] International Organization for Standardization, “Information technology - Process assessment - Part 5: An exemplar software life cycle process assessment model,” International Organization for Standardization, ISO/IEC Standard 15504–5, 2012.

[28] VDA QMC Project Group 13, “Automotive SPICE - Process Reference and Assessment Model for Cybersecurity Engineering,” Quality Management Center of the German Association of the Automotive

Industry, Core Specification 1.0, 2021.

[29] J.-F. Rocchi, P. Bodino, H. D. Tréglodé, B. Flury-Hérard, and F. Ricard, “L’automatisation Des Véhicules; Annexe N°9 : La Cyber Sécurité,” Inspection generale de l’administration and Conseil general de l’environnement et du developpement durable, Inspection Generale de l’administration 16040-R, 2017.

[30] Agence nationale de la sécurité des systèmes d’information, “Analyse Des Contributions Reçues Suite à l’appel à Manifestation d’intérêt Sur La Certification de Sécurité de Niveaux Substantiel et Élémentaire,” Agence nationale de la sécurité des systèmes d’information., Oct. 2019.

[31] British Standards Institution, “The fundamental principles of automotive cyber security - Specification,” British Standards Institution, BSI PAS 1885:2018, 2018.

[32] A. Shostack, *Threat Modeling: Designing for Security.* John Wiley & Sons, 2014.

[33] S. Marksteiner *et al.*, “A Process to Facilitate Automated Automotive Cybersecurity Testing,” New York, NY, USA, 2021.

9. Annex A: Abbreviations, Terms, and Descriptions

ANSSI: Agence nationale de la sécurité des systèmes d'information

API: Application Programming Interface (API) is an interface that defines interactions between two software entities. Usually, the goal of an API is to provide an abstraction layer that hides complexity while providing specified functionality.

BSI PAS: British Standard Institution Publicly Available Specification

CAL: Cybersecurity Assurance Levels

CAN: Controller Area Network (CAN) is a dominant serial communication network protocol used for intravehicle communication

CAN-FD: is a data-communication protocol typically used for broadcasting sensor data and control information on 2 wire interconnections between different parts of electronic instrumentation and control system.

COTS: Commercial of the shelf

CSA: Cybersecurity Act

CSMS: Cybersecurity Management System

DOT: Department of Transportation

EU CRA: EU Cyber Resilience Act

EU CSA: EU Cybersecurity Act

EUCC: EU Common Criteria

ECU: Electronic Control Unit (ECU) is an embedded system that provides a control function to a vehicle's electrical system or subsystems through digital computing hardware and associated software.

FMVSS: Federal Motor Vehicle Safety Standards

Fuzz testing: Used to assess the security of a system to unsensitized data input. This can either be randomized or targeted unsensitized data input. It is popularly used in software engineering to identify bugs in the codebase.

GNU: is an extensive collection of free software, which can be used as an operating system or can be used in parts with other operating systems.

IAMTS: International Alliance for Mobility Testing and Standardization

ICV: Intelligent and Connected Vehicles

IDA: International Development Association

IPA: Information Processing Agency

ISAC: Automotive Information Sharing and Analysis Center

ISO: The International Organization for Standardization is an international standard development organization composed of representatives from the national standards organizations of member countries.

JASPAR: Japan Automotive Software Platform and Architecture

KATRI: Korea Automobile Testing & Research Institute

KMVSS: Korea Motor Vehicle Safety Standard

LIN: Local Interconnect Network

MAC: Message authentication code

METI: Ministry and Economy, Trade and Industry

MIIT: Chinese Ministry of Industry and Information Technology

MLIT: Ministry of Land, Infrastructure, Transport and Tourism

MOLIT: Ministry of Land and Infrastructure, Transport

NISSTC: National Information Security Standardization Technical Committee

MOST: Media Oriented Systems Transport

NHTSA: National Highway Traffic Safety Administration

NTCAS: National Technical Committee of Auto Standardization

NIST: The National Institute of Standards and Technology is a physical sciences laboratory and non-regulatory agency of the United States Department of Commerce.

OBD: Onboard Diagnostic

OEM: Original Equipment Manufacturer

OTA: Over-The-Air (OTA) is a software update distribution method which uses wireless transmission.

PCB: Printed Circuit Board

PKI: Public Key Infrastructure (PKI) refers to a set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

PTC: PTC Inc. is an American computer software and services company founded in 1985 and headquartered in Boston, Massachusetts

QMC: Quality Management Center

ROCA: Return of Coppersmith's attack

SOTA: software-over-the-air updates

SPICE: Software Process Improvement and Capability Determination

SUT: System Under Test

TAF: Target Attack Feasibility

TARA: Threat Analysis and Risk Assessment

UNECE: The United Nations Economic Commission for Europe is one of the five regional commissions under the jurisdiction of the United Nations Economic and Social Council. It was established in order to promote economic cooperation and integrations among its member states.

URH: Universal Radio Hacker

VDA: Verband der Automobilindustrie

V&V: Verification & Validation

VCAT: Cyber Security Assessment Tool

Annex B: Survey Questionnaire

To better understand our methodology here are the survey questions we have send to various parties in different regions. The document is compiled based on their answers and our engineering judgment.

Question 1: What is your cybersecurity verification/validation process to support the automotive concept/product phase/postproduction phase)?
( ) None
( ) Different classes (please specify):
( ) Formalized

Question 2: What is your test type/methods/tools that you use to evaluate the respective assets and the associated items, subcomponents, sub system, interfaces and connectivity (e.g. Metasploit)? Please also categorize the tools for target type (network, binary, system level, …).
( ) COTS (please specify which):
( ) Open Source (please specify which):
( ) Customized COTS/OS (please specify which):
( ) Internal Tools

Question 3: What international & national standards are you following for verification & validation?
( ) ISO 21434
( ) ISO/IEC 15408
( ) ISO/IEC 27034
( ) IEC 62443
( ) Other (please specify):

Question 4: If you don't have a process, do you use a test matrix or a standard set of tests for certain types of SUTs?
( ) Test Matrix
( ) Standard Test Set
( ) Case-by-Case
( ) Other (please specify):
( ) N/A (using structured process)

Question 5: What types of test do you conduct?
( ) Functional Testing
( ) Vulnerability Scanning
( ) Fuzz Testing
( ) Penetration Testing
( ) Other (please specify):

Question 6: How do measure and maximize the test coverage?

( ) Line Coverage (for white box testing)
( ) Path Coverage (for white box testing)
( ) Equivalence Classes for Inputs
( ) Specifications Coverage
( ) Other (please specify):

Question 7: Which types of SUTs do you test?
( ) ECUs (e.g. HiL)
( ) Head Units
( ) IVN (e.g. security testing on the CAN bus)
( ) Protocols (implementation correctness, etc.)
( ) Other (please specify):

Question 8: (a) Do you use third-party services for V&V? (b) Is there an established interface agreement for cybersecurity testing? (c) What nature is the V&V agreement (e.g. document-based auditing, product testing, etc.)
a) yes ( ) no ( ) if yes, please specify:
b) yes ( ) no ( ) if yes, please specify:
c)

Question 9: Do you use model (threat, attacker model) or risk-based testing (i.e. TARA) approach to identify scenarios? If not, what kind of system analysis do you use?
( ) Model based
( ) Risk-based
( ) Other (please specify):

Question 10: How do you derive test cases from your analysis (e.g. requirements-based)?
( ) Requirements-based (Model-based / Model Checking)
( ) Specification-based
( ) Structure-based
( ) Experience-based
( ) Fault-based
( ) Other (please specify):

Question 11: Do you use white box, black box or grey box testing or all of them?
( ) White box ( ) Black box ( ) Gray box

Question 12:
(a) Is there some set of baseline testing for all SUTs?
(b) If so, what tests does it include?

(a)
( ) Yes ( ) No

(b)
( ) Requirement Specification
( ) Design Specification
( ) Source Code
( ) Test Plans
( ) Test Cases
( ) Test Data
( ) Product
( ) Other. Please indicate:

Question 13: What tools to do you use for
a) pre-attack (scanning, CAN analysis, etc.)
b) attack (exploit frameworks, etc.)
c) post-attack tools (reporting tools, security life cycle management)

Tools used for a):
Tools used for b):
Tools used for c):