ISSN: 1813-4890

Thoughts on the landing of UNECE R155 related detection activities

Hao Shan [a], Yanyan Han [b] , Kexun He [c], Xuebin Shao [d]

CATARC Software Testing (Tianjin) Co., Ltd, Tianjin, China

[a]shanhao@catarc.ac.cn, [b]hanyanyan@catarc.ac.cn, [c]hekexun@catarc.ac.cn, [d]shaoxuebin@catarc.ac.cn

Abstract

With the official implementation of UNECE R155 regulations in Europe, OEMs with export requirements for new models to EU 58 treaty countries need to obtain a VTA certificate by July 2024. In order to obtain a VTA certificate, type testing is an essential part. From the perspective of a third-party testing institution, this paper analyzes the links of testing activities during the actual implementation of R155 regulations, the characteristics of each testing activity, the influence of test input and output on the upstream and downstream links, and the matters for attention during the landing of testing activities. The sample space based on this paper includes 3 consulting agencies, 4 certification agencies, more than 10 OEMs certification models.

Keywords

Thoughts , landing of UNECE R155.

1. Introduction

The intellectualization and network connection in the four modernizations of modern automobile make the automobile no longer a single information island in the past, but a new intelligent traffic cabin equipped with advanced sensors, intelligent systems, vehicle, road, cloud and network integration. At the same time, the information security of automobiles has become more and more important, and automobiles have even become potential targets [1-2]. Automobile network security has become a part of automobile basic security, causing widespread concern [3-6]. In order to cope with the risks that may be caused by automobile network security, the International Organization for Standardization issued the standard ISO 21434[7] in 2021. The standard is related to the whole life cycle of vehicles and studies automobile network security engineering from four aspects, including risk assessment management, product development, operation and maintenance, and process audit. The goal is that products designed, produced and tested by this standard have certain network security protection capabilities [8]. Based on ISO 21434, the United Nations World Forum for the Coordination of Vehicle Regulations (UN/WP.29 for short) has issued important regulations UNECE R155[9], unified regulations for cybersecurity vehicle approval and cybersecurity management system. This regulation applies to member countries under the 1958 Agreement (the number of Contracting parties to the 1958 agreement of UNECE has increased to 54, including all EU countries and other OECD countries). Although China is not in the 1958 Agreement, automobiles produced in these countries must pass relevant certification as long as they are sold in these countries.

2. Test stage in R155

First of all, we need to clarify the detection link in R155 regulation [10].

ISSN: 1813-4890

According to ISO 21434, based on the classic V-shape development process, in the concept stage of the vehicle, through the vehicle level threat analysis and risk assessment (TARA) report, the vehicle level network security statement, and network security objectives. According to the network security goal, then customize the corresponding truck-level network security requirements to achieve the corresponding network security goal. As the responsible party, the OEM will properly allocate the network security requirements of the whole vehicle. Part of the network security requirements will be undertaken by the service providers such as network suppliers, and part of the network security requirements will be transferred to the corresponding parts suppliers. Through the realization of the network security requirements of parts, the network security requirements of the whole vehicle can be met. After obtaining the network security requirements assigned by the OEM, service providers or component suppliers need to conduct customized analysis and integrate the network security implementation solutions that meet the network security requirements into the existing development architecture.

After the product is developed by the service provider or component supplier, the first test step in R155 regulation is the network security requirements verification test stage at the component level. In this stage, component suppliers need to verify the network security scheme implemented in the development stage. Firstly, they need to verify that the scheme has been implemented, and secondly, they need to verify that the scheme can achieve the expected purpose. This part of the test needs to be led by the parts supplier, which can do it by itself or assign it to the testing institution. We need to note that this part of testing is only related to network security, and functional testing that has nothing to do with security is not included in our discussion.

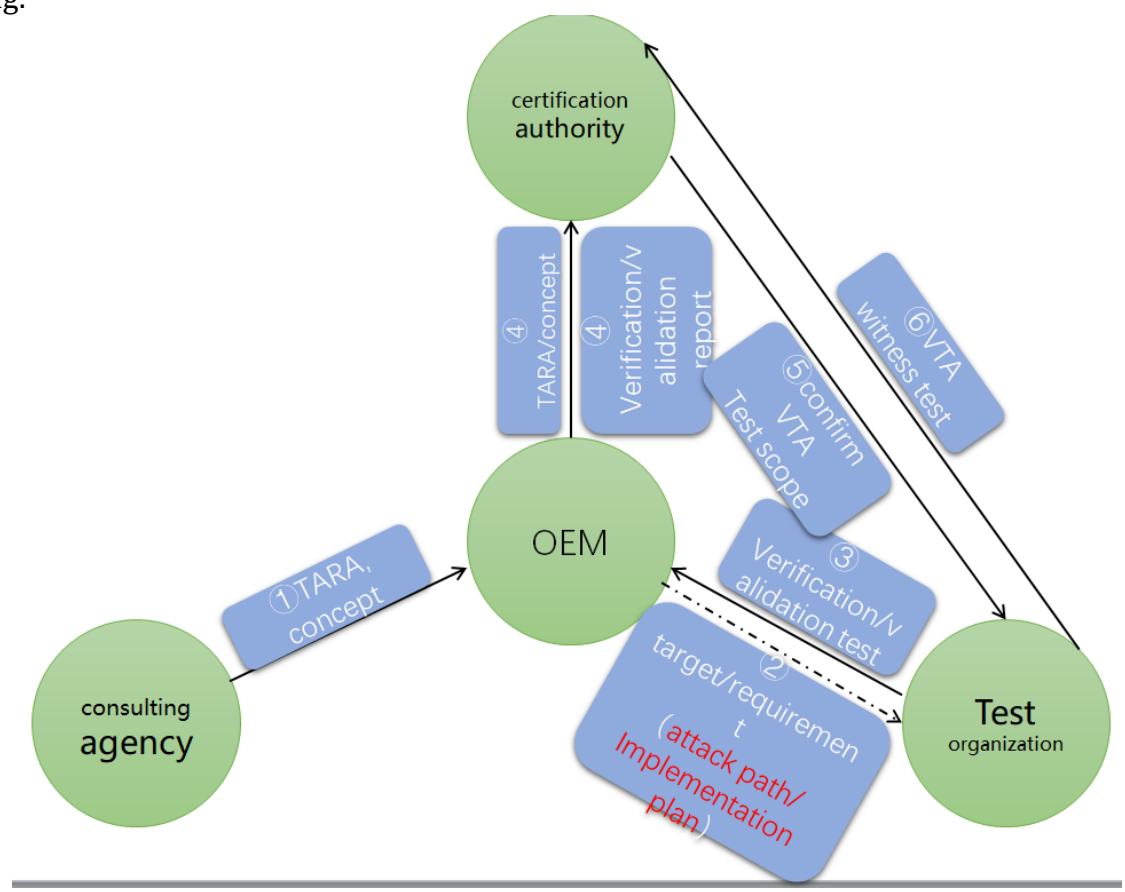
After the component-level cybersecurity verification tests are done, it's time to test at the vehicle level. At the vehicle level, the test is divided into two types, one is the network security verification test at the vehicle level, the other is the network security confirmation test at the vehicle level. Let's first talk about the network security verification test at the vehicle level. The purpose of the test is to verify whether the subsystem or the vehicle achieves 100% of the product design scheme and meets the network security requirements in TARA analysis. Again, the verification test focuses only on the parts related to network security. The purpose of the whole-vehicle network security confirmation test is to confirm the validity of the security objectives in TARA analysis, that is, the security objectives are fully realized. From the perspective of testing, penetration testing, fuzzy testing, vulnerability scanning and other means are used to try to attack and penetrate according to the attack path obtained by the tested object in TARA analysis, so as to confirm that all attack paths end in failure, and the sensitive information or permission of the vehicle cannot be further obtained.

Finally, we come to the VTA witness trial. As the name implies, witness test is the certification body with eyes to see the testing body to do the experiment, in order to confirm the effectiveness, authenticity, integrity of automotive product information security. The general procedure for this process is that the certification body reviews all the materials submitted by the OEM (including CSMS, concept reports, cyber security activities during the development phase, etc.) and then selects the scope for testing. The testing method can be specified by the certification body or output by the testing body. When these are confirmed, the VTA eyewitness test can be conducted. It is worth noting that during the testing process, the testing personnel of the testing agency need to explain the testing methods, and the teachers of the certification agency can also ask questions about the testing links, which will make the final test report issued more convincing. Another point to note is that in some cases, the European representative of VTA Eyewitness testing certification body will attend an online meeting, resulting in testing work from 2pm to 10pm in China time.

ISSN: 1813-4890

3. Landing verification, confirmation, VTA witness test, and matters need attention during them

Above, we have outlined the links that need to be detected during the implementation of Regulation 155. Next, we have reviewed the whole process of R&D and VTA witness test in order to see the upstream and downstream of each detection stage, so as to have a deeper understanding of the position and significance of the detection stage. According to ISO 21434, the network security activities of automobile products start from the network security concept made by the consulting agency. The concept stage uses TARA analysis method, and the output to OEM related to the test is "network security objective, network security statement". Based on network security objectives, OEMs formulate network security requirements and delegate them to component suppliers and service providers. When parts suppliers and service providers formulate technical specifications according to network security requirements and implement the scheme, it is necessary to carry out network security verification and confirmation testing, which can be further subdivided into parts level testing and vehicle level testing.



After the network security verification and confirmation test is completed, the report will be summarized to the OEM department. The OEM will integrate the concept report, CSMS management system documents, and all the test reports to the certification agency. The certification agency will determine the scope of the final VTA witness test based on the submitted materials. Certification bodies will select their own accredited testing agencies to perform the final eyewitness test.

The above is the classic process of 155 regulation test execution, but the actual execution process is full of many variables, such as: 1. The output materials of each organization are different when each link is implemented, which leads to some variables when they are connected with each other. 2. In the whole certification process, the duration is long, there are many institutions involved, and there are more interwoven places, which will also produce

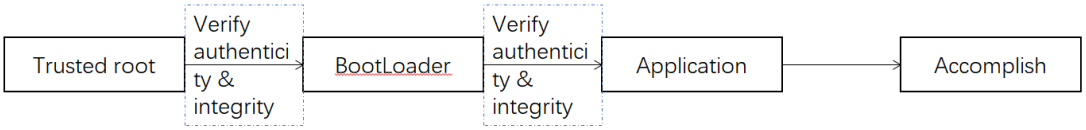
ISSN: 1813-4890

certain variables. Generally, the behavior of passing the certification will involve the certification applicant and the certification body, while the test link of 155 regulations involves at least four parties.

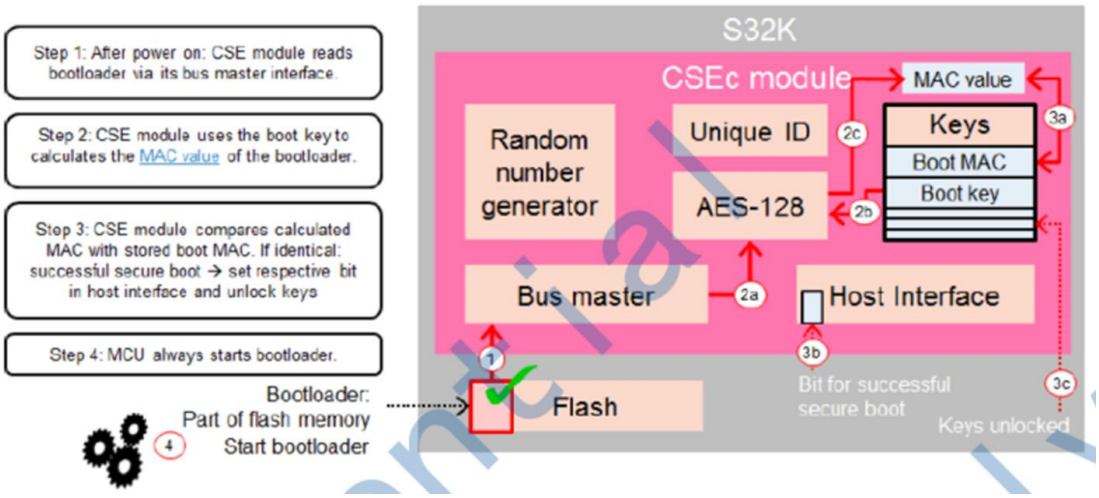
Next, this article discusses the impact of these variables on detection activities. For example, where there may be variables, what impact these variables will have on the detection work, and how to deal with these variables in the detection process to ensure the smooth progress of the detection work. The sample for this report includes 3 consulting agencies, 4 certification bodies, and more than 10 OEMs.

In order to facilitate understanding, three concepts in the process of verification testing are introduced first: security requirements, technical specifications, and implementation schemes. If these concepts are not clearly distinguished, subsequent tests will be affected. Security requirements are derived from the TARA report to meet the network security objectives set out in the TARA analysis. A typical network security requirement might be "Firmware tampering should be prevented by a secure boot mechanism." The technical specification is a general normative document for the product formulated by the product implementer in order to achieve the network security requirements. It will generically describe what kind of technical means and what kinds of process are used to achieve what kind of function. For example, the implementation specification of "safe startup" is as follows:

The procedure of secure boot is: power on the ECU, firstly run the trusted root, which will verify the authenticity & integrity of BootLoader, the run the verified BootLoader, which will verify the authenticity & integrity of Application, at last run the verified Application.



The implementation scheme is a way of landing the technical specification. It will introduce the implementation and execution of the scheme step by step in detail, including the actual architecture, data flow, execution timing:



Secondly, it introduces the two concepts of security target and attack path during the confirmation test. If the first three concepts are similar, these two concepts are relatively easy to distinguish and have a great impact on the subsequent detection work. The security goal is the highest level requirement in TARA analysis, which needs to address the corresponding risks and threats. The attack path is for the security target of the attack tree analysis, to the security attribute of the asset in the security target as the analysis object, the use of a variety of threat

ISSN: 1813-4890

models (such as STRIDE model) to analyze may affect the asset security attribute of the possible situation, finally implemented to the executable level.

Let's analyze the impact of test input conditions on validation and validation tests, as shown in the following table. What we need to verify in the verification test is the landing plan of the safety requirements. Therefore, what we actually need to input is the implementation plan provided by the OEM parts supplier or service provider, which will clearly specify the implementation method, so that we can get the most appropriate verification test method. However, some OEMs are not very familiar with this and will send us security requirements. There are many ways to achieve security requirements. Which one is it? It cannot be located by security requirements alone. If the OEM input only safety requirements, then when we do the actual verification test, we can first understand the actual solution of the real vehicle environment, and then write the corresponding test method according to this solution and test. If the OEM only input technical specifications, then we do the verification test method is similar to the above situation, we can first understand the actual solution of the real vehicle environment, and then write the corresponding test method according to this solution and test. In short, the verification test scheme we make should be consistent with the actual situation. Is there no problem in the follow-up test after the implementation plan is given by OEM? In fact, for implementation schemes, there is an implementation scheme that is specifically designed for specific security requirements, so such input materials will be very suitable for us to test, such as the above example of security start-up. However, some implementation schemes are not a separate and special scheme, but achieved through some basic protection means, such as access control of the system itself to manage permissions. In this case, our test method is sampling test. For example, we can log in users of different roles and different permission levels in the system to check their access control and permissions, to demonstrate the realization of security requirements.

What we need more for validation testing is the attack path derived from the TARA analysis so that we can try to attack the assets we need to protect from various angles. However, some OEMs only exported security targets to us, such as protecting the availability of a certain part. As for the attacks that can be launched against the availability, we do not know from the input. If this happens, we need to rely on the penetration test case library we have accumulated and select use cases from it to test that might launch attacks against the availability, such as DOS attacks, firmware tampering, etc. As for the attack paths exported by OEM, we cannot accept them as per the order. We need to conduct a round of analysis and screening before implementing them. For example, if there is an attack path that is unreasonable, theoretically impossible or incorrect, for those attack paths, we need to organize an expert review to make sure that the path does not pose a risk. There are also attack paths that are not controlled by the OEM, such as communication base stations, carrier networks, etc. Such attack paths also need to be reviewed and excluded from the final test items.

Based on this, we summarize the thinking in the process of verification and validation testing. There are the following points: 1. OEM needs a person who knows the whole process to connect, coordinate, and ensure that the input and output materials (implementation plan, attack path) connected to the upper and lower lines are available and reliable! Otherwise, it is easy to be led by the nose by others, and cannot get the appropriate input, resulting in poor project execution; 2. Requirements related to verification testing are only limited to those related to information security, not functional. That is to say, the verification test here only focuses on security attributes, and does not test at the functional implementation level (for example, security protection is achieved through IDSP, PKI and other means, we do not need to verify the functions of IDPS, PKI and so on). 3. Some projects need to be assigned to departments other than the lead department (IT, etc.) or delegated to parts suppliers. The department that leads the OEM project needs to have the right to make overall planning and ensure that there are no

ISSN: 1813-4890

dead corners in task allocation (the secret key of vehicle and cloud communication stored in the cloud may become a zone of neglect).

Let's talk about the VTA sightings that you're most interested in. For example, if the previous tests were a long school career, this eyewitness test is the real deal. So the first thing you're going to be interested in is how do you get the questions? Based on our Tianjin inspection Center has done about 10 witness tests, we have analyzed some of the patterns. The first is the scope of selected test items in Appendix V of R155 regulation. Basically every category in Appendix V will be selected (except "threats to vehicles caused by unconscious human actions"):

and back-end servers are connected to the vehicle related to the threat

about the threat of vehicle communication channel

threats about vehicle update process

threats about vehicle external connections

threat to vehicle data/code

if not fully protect or strengthen, may use the potential vulnerability The choice is reasonable and can fully cover all aspects of risk faced by the vehicle.

The second point of use case selection is the doubts found in the process of document review or the early test report. For example, the scheme materials that should be provided were not obtained during the document review. In order to confirm the actual situation, it is also put into the final witness test. For projects with insufficient verification and confirmation testing process in the early stage, the certification body may have doubts about the test method and environment, and may also arrange such test items to witness tests for final confirmation.

The next thing to note is that although R155 is a full-vehicle regulation, there may still be component-level testing even after the VTA eyewitness phase. Such as the need to open additional debugging interface, safe startup, safe startup and other projects, these projects require more input, and is tested on the parts. So that's a feature of the VTA eyewitness test.

The last point is that the resources that are difficult to coordinate in the early testing, such as OTA testing, will be put into witness testing in many times, because OTA testing coordination resources are relatively large, IT and other departments need to cooperate, but usually the leading department does not have so much power, so certification agencies think this place is a security risk. Therefore, OTA testing programs are specially arranged in witness trials.

Let's talk about some of the characteristics of VTA eyewitness testing, which means that it's only happening to individual certification bodies so far, but it can happen to others as well. First of all, VTA witness trials sometimes involve foreign reviewers, so the review time needs to be synchronized with the European side, so sometimes it lasts from afternoon to 10pm. Second, generally speaking, the test items are selected by the certification body, but some certification bodies indicate a testing direction, for example, from the point of view of risk, the core expects to attack the CAN bus, the detection body free play test items, to the audit body to show the detection body's security detection ideas, and check whether the vehicle can resist the relevant attacks. Third, if the quality of the early verification and confirmation test is not high, the audit agency thinks that the hidden danger is relatively large, it will arrange more test items to VTA witness testing, resulting in a relatively large pressure of witness testing. Generally speaking, the cycle of the eyewitness test is 2-3 days, and the test items are generally about 10. However, some OEM pre-test quality is not high, resulting in the certification body VTA eyewitness test selected nearly 50 use cases, resulting in very nervous eyewitness test. Fourth, certification authorities have doubts about whether the tools used for testing can achieve the desired results (what tools? Please provide the source code). This problem occurred when we assisted another testing company to complete the eyewitness test. Maybe the foreigner was not sure about the ability of the whole laboratory, which led to many problems in the VTA. It was the only VTA eyewitness test that lasted more than a week at present.

In view of this, the thinking in the process of VTA eyewitness testing is as follows: 1. OEM needs to select qualified laboratories and experienced teams, which will reduce a lot of unnecessary trouble for subsequent detection; 2. 2. Because the scope of the VTA witness test is not limited to the previously performed test items, the certification body may select any item terms for the test, so it needs to be fully prepared; 3. There are some test projects without a clear test basis (interference, there is no standard clearly states how much power, frequency to do interference), it is best not to put in the early test projects, so as not to be pumped, pumped words cannot be explained with the certification body.

4. Summary

Based on the certified models of 3 consulting agencies, 4 certification agencies, and more than 10 OEMs as samples, this paper analyzes the testing links involving UNECE R155, analyzes the influence of the input and output of upstream and downstream links on testing activities, and summarizes the points for attention in each testing link. Finally, based on the experience of R155 regulation verification test, confirmation test and VTA witness test, I have the following deep feelings:

OEM: the main responsibility is to the whole process, the scale is the point; The lead department needs to be able to coordinate the resources needed

consultancy in upstream link in the entire process, has a great influence on subsequent work

inspection agencies have credibility, reduce subsequent may cause unnecessary trouble

As time goes by, each organization do more and more well, mutual grinding degree is more and more high, the whole industry level is higher and higher, more and more standard, for our country automobile products go out of the country contribute their strength. We should be confident to get the VTA certificate!

References

[1] Chen.C, Han.WL, Wang.X; VANET overview of security technology[J]; A small microcomputer system, 2011,32(5):896-904.

[2] Suchen Jiang, Research on the development trend of intelligent automobile enterprises[J]. engineering technology: The full version, 2016(11): 00318-00318

[3] Tian.M, Wang.S, Cai.L, Research on vehicle network security protection[J], Computer knowledge and technology: academic exchange, 2017, 13(6): 72-75.

[4] Miller C, Valasek C. Adventures in automotive networks and control units[J]. Black Hat USA, 2013, 21: 260-264.

[5] Miller C, Valasek C. A survey of remote automotive attack surfaces[J]. Black Hat USA, 2014.

[6] Miller C, Valasek C. Remote exploitation of an unaltered passenger vehicle[J]. Black Hat USA, 2015.

[7] ISO/SAE DIS 21434 Road vehicles — Cybersecurity engineering, ICS: 43.040.15 Car informatics. On board computer systems.

[8] CESI. White paper on standardization of automotive electronic network security (2018 edition). http://www.cesi.ac.cn/201804/3790.html, 2018-04-16.

[9] UN Regulation No. 155, Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system.

[10] Han Yanyan, Automotive cyber security test method for UN-R 155 regulation. Conference | [P] . Volume 12457, 2022. PP 124571F-124571F-5.