ISSN: 2664-9640

Research on challenges and countermeasures of automotive TARA

Yihong Qin [a, *], Yanyan Han [b] and Xiong Zhao [c]

CATARC Software Testing (Tianjin) Co., Ltd, Tianjin, 300300, China

[a]qinyihong@catarc.ac.cn, [b]hanyanyan@catarc.ac.cn, [c]zhaoxiong@catarc.ac.cn

Abstract

In recent years, automotive information security incidents have occurred frequently. WP.29 has passed UN R155, the world's first mandatory regulation on automotive information security. The regulation requires that vehicle models must carry out Threat Analysis and Risk Assessment (TARA) during the conceptual design phase. However, UN R155 regulation itself does not provide clear requirements, so that OAs and consulting agencies can carry out vehicle threat analysis and risk assessment in accordance with a unified standard. The model and methodology used by TARA are determined by the Oems and consulting agencies with reference to ISO21434 and their own experience. For the automobile manufacturing industry, this uncertainty brings some difficulties to the vehicle life cycle information security management. Through the analysis process of TARA of many car companies, this paper summarizes the challenges faced by automotive TARA, and further puts forward improvement methods for part of the problems, which can help manufacturers better manage the full life cycle of automotive information security.

Keywords

UN R155, TARA, ISO21434.

1. Introduction

On January 22, 2021, WP.29 adopted UN R155 Vehicular Cybersecurity Regulation, the world's first mandatory automotive cybersecurity regulation. UN R155 regulation divides the mandatory requirements of automotive network security into two parts: one is the requirements of network security management system for automobile manufacturers; The second is the network security capability requirements for vehicle products. It corresponds to cyber security management system certification (CSMS certification) and vehicle type approval (VTA). TARA is an indispensable part of vehicle network safety type certification. The requirements in clause 7.3.3 of the UN R155 Vehicular Cybersecurity regulation make it clear that the vehicle manufacturer shall identify the key elements of the vehicle type and carry out an exhaustive risk assessment of the vehicle type and shall appropriately address/manage the identified risks.

In addition to regulations, the attack surface of automotive systems has expanded with the application of new technologies and the introduction of new functions in automobiles. Attackers can use the risks in these new technologies and functions to carry out malicious attacks, thereby threatening the information security of vehicles. Also considering the long production cycle of the car, it is difficult to make large-scale modifications to the vehicle architecture once it is determined. Therefore, vehicle manufacturers need to consider safety at the design and development stage, and adapt and improve it in future models.

2. Network security challenges and trends

Firstly, with the introduction of new features, the attack surface of cars is gradually expanding, and the application of new technologies also leads to an increase in vulnerabilities. Secondly, the strengthening of supervision and regulations puts forward higher requirements for automotive network security. In addition, once the architecture of the vehicle is determined, it will become difficult to change, and there are certain difficulties in the repair process of the vulnerability, which cannot be repaired remotely through OTA. In addition, the product life cycle of vehicles is long, and the technical vulnerabilities are endless, which brings challenges to network security. At the same time, the mobility of vehicles also increases the possibility of attacks. In addition, the complexity of supply chain and the conflict between agile development and network security are also current problems. Finally, the high cost associated with fixing bugs and recalling vehicles is also a trend of concern. In summary, vehicle cybersecurity faces multiple challenges and requires joint efforts from all parties to ensure the safety and privacy of passengers.

3. Challenges faced by TARA

Although the standard of TARA methodology is proposed in ISO21434, there are no specific provisions in the standard that clearly guide the implementation of TARA, which leads to the following difficulties in the practical application of TARA.

(1) The challenge of human assessment factors: the current automotive cybersecurity Risk Assessment (TARA) is more like an art than a science, and the assessment results are affected by the subjective judgment of the assessors and lack consistency.

(2) The traditional TARA tools face the challenges of flexibility and collaboration: it is difficult to have good flexibility and upstream and downstream collaboration, and the scalability is also poor. In contrast, Office series tools are popular in TARA activities because Office series tools are more flexible and unrestricted in their use.

(3) The challenge of obtaining accurate system description and information related to the object under Evaluation (TOE) : It is difficult to obtain accurate system description and information related to the object under evaluation (TOE), which poses a challenge for conducting a comprehensive security assessment.

(4) Engineering reuse challenges: With the service of vehicle functions, functions can be deployed on different components, or deployed and migrated arbitrarily under SOV architecture, which brings challenges to TARA engineering reuse.

(5) Decision-making challenges faced by TARA at different levels: TARA needs to be evaluated at different levels, including vehicle level, system level and component level. Different levels of TARA result in different decisions and involve different parties, such as suppliers completing component-level evaluations.

(7) Challenges of different dimensions of risk rating: establishing a multi-source attacker profile library may better help analyze the feasibility of attacks and simplify the process of risk assessment. However, the rating of the risk dimension also faces subjectivity problems, such as the difficulty of the security department to score the financial dimension, so it needs people with different backgrounds to cooperate in the evaluation.

(8) TARA process faces full lifecycle and iteration challenges: TARA needs to be used throughout the entire product life cycle, during test validation, during validation testing, and when answering the impact of new vulnerabilities in the future. In addition, TARA needs to be able to adapt to vehicles with different software and hardware configurations and be integrated with active warning functions.

4. Development direction to meet the challenges

(1) In order to deal with the challenges of human factors in the traditional TARA analysis, the use of review tools and review model library should be established. The information in the model repository, such as attack feasibility, can be scored by a professional cybersecurity team. In addition, it is difficult for the security team to evaluate the impact level, so it is necessary to participate in the scoring model of the whole industry. For example, the economic impact can be scored by the professional financial team, and the impact on the corporate image can be scored by the professional public relations team, so as to better assess the risk.

(2) Bottom-up risk assessment with vulnerability impact analysis: In addition to the traditional top-down TARA assessment, a bottom-up vulnerability impact analysis should be performed to assess the risk more comprehensively. This method can help us find potential vulnerabilities and security threats, and take corresponding measures to repair and protect in time.

(3) Enterprise Cybersecurity Assurance Level (CAL) standards: In order to ensure the safety of automotive systems, enterprises should establish their own cybersecurity assurance level standards. This can help enterprises better assess and manage risks, and formulate corresponding security policies and measures.

(4) Multi-level evaluation and participation of TARA: TARA evaluation needs to be conducted at different levels, including vehicle level, system level and component level. To reduce costs and improve efficiency, system developers, who have a deeper understanding of the vehicle system, can be involved in TARA evaluations, while safety experts can be responsible for model building and analysis.

(5) Rapid, cheap and traceable formulation of TARA: the formulation of TARA should be rapid to adapt to the rapidly developing automobile industry. Meanwhile, TARA should also be cheap to reduce the cost. In addition, TARA needs to be traceable in order to be able to trace and verify the evaluation process, ensuring the accuracy and reliability of the results.

Establish a lexical language system for entities and relations: To ensure that different people describe the same thing, we need to establish a unified lexical language system for entities and relations. This can help different teams communicate and understand better, facilitating collaboration and cooperation in the industry. In addition, in terms of reuse, we also need to further investigate the connections between different models and standards to better integrate and utilize the data.

5. Conclusion

UN R155 regulations and ISO 21434 do not provide clear requirements for TARA analysis, so that Oems and consulting agencies can carry out threat analysis and risk assessment in the vehicle concept stage according to a unified standard. TARA activities are carried out in the concept stage of vehicles. For manufacturers, the uncertainty of TARA work brings some difficulties to the design and production of vehicles. By summarizing the current status of TARA work in the industry, this paper summarizes the challenges faced by automotive TARA, and further puts forward the future development direction of TARA, which can help the industry develop better.

Acknowledgements

This paper was supported by the subject “National Key R&D Plan of the Ministry of Science and Technology (Project No: 2020YFB1600204)”.

References

[1] E/ECE/TRANS/505/Rev.3/Add.154, (2021). UN Regulation No. 155 Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. https://unece.org/sites/default/files/2021-03/R155e.pdf.

[2] ISO/TC 22/SC 32 Electrical and electronic components and general system aspects, (2021). ISO/SAE 21434:2021(E) Road vehicles — Cybersecurity engineering.

[3] Kraftfahrt-Bundesamt, (2021). 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. https://www.kba.de /EN/Themen_en/ Typgenehmigung_en/Zum_ Herunter laden_ en/ Benennung Technischer Dienste_en/ anwendung_ Regeln_ TD_ R155_ R156_en. Pdf ?__ blob = publication File&v=3

[4] Proposals for Interpretation Documents for UN Regulation No. 155 (Cyber security and cyber security management system), Dec 2020.

[5] Ekert, D. , J. Dobaj , and A. Salamun . "Cybersecurity Verification and Validation Testing in Automotive." JOURNAL OF UNIVERSAL COMPUTER SCIENCE 27(8), 850-867 (2021).