Journal of Electronics and Information Science (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/jeis.2023.080615
ISSN 2371-9524 Vol. 8 Num. 6

Research on the requirement decomposition and test verification for vehicle data security

Yujia Li[1,a], Xianzhao Xia[1,b], Hanbing Wu[2,c], Lei Liu[1,d], Rui Zhao[1,e]

[1]CATARC Automotive Test Center (Tianjin) Co., Ltd., Tianjin, China
[2]China Automotive Technology and Research Center Co., Ltd., Tianjin, China
[a]liyujia@catarc.ac.cn, [b]xiaxianzhao@catarc.ac.cn, [c]wuhanbing@catarc.ac.cn,
[d]liulei2021@catarc.ac.cn, [e]zhaorui@catarc.ac.cn

Keywords: Vehicle data security, requirement decomposition, test verification

Abstract: While data is considered as new production factors in various scenes of the automotive industry. The data interaction of vehicles also raises a significant amount of data security risks and issues. The vehicle development process needs to be considerate of satisfying data security requirements. The main objective of this paper is to investigate a method for decomposing vehicle data security requirements so that they can be met at different levels of the system during development. A principle of data grading is proposed in this paper, enabling the quantitative classification of vehicle data. Meanwhile, the process of test verification on basis of decomposing requirements is also the subject of this paper. Tests can be derived directly from the requirements at the finest level. The coverage analysis of requirements is explored integrating the impact of data classification, requirements decomposition and test results. This paper is useful for vehicle developers to conduct development and test verification for data security requirements.

1. Introduction

Under the influence of technological changes in the electrification, intelligence, networking, and sharing of vehicles, the current stage of vehicle development and production has been different from that of traditional automobiles, which involve more and more functions of data interaction. With a massive amount of data, complex data types, extensive data access, and diverse data processors in the connected vehicle environment, a variety of data security issues have received widespread attention worldwide. Addressing these data security issues necessitates the implementation of data security technologies in vehicles, which makes it necessary to take data security requirements into account during vehicle development. On the one hand, the vehicle development cycle is prolonged and the process is more complicated, and on the other hand, there are multiple systems involved in vehicle data processing and data security, rendering the fulfillment of data security requirements require more efforts. Therefore, introducing automotive data security requirements early in the development process and breaking them down into modules and components will help reduce the cost and effort caused by automotive data security. However, there has been less studies focusing on the application of the requirement engineering for data security. A new approach is therefore needed for the decomposition of data security requirement in the field of vehicle, especially the intelligent and connected vehicle.

The main objective is to investigate methods for improvement of the importing data security requirements into the vehicle development process and test verification based on the decomposed requirements.

Section 2 describes the basic theoretical background on requirements engineering. The third section introduces a method to define assessment. Section 4 presents the concept for the requirement decomposition and the data classification for vehicle data security. The test verification is presented in Section 5, which involves a method addressing the requirement coverage analysis proposed in this paper. The Section 6 draws upon the paper by giving a brief conclusion and a short outlook on future research.

2. Requirement Engineering

2.1 Requirement and Requirement Engineering

Requirements are defined as the documented statements that translate or describe the need and their associated constraints and conditions. Requirements refer to the need that a particular design, product or process aims to meet and they can be divided into different levels in the system structure [1].They are considered as the base for development process and define what the stakeholders including users, customers, suppliers, developers, businesses desire to achieve from the new system, and what the system must have in order to meet the need [2].

Requirements engineering is the creation of services and functions for a stakeholder-requested system, and gives limitations for system operation and development. The purpose of the requirements engineering is mainly to establish the system requirements documents that can be used for knowledge sharing[3]. The final output of requirements engineering is the requirements specification, which have the following characters:

1) Correctness: Correctness is the most fundamental property. Each requirement should describe what is really needed [4].

2) Unambiguous: There should be a single, common understanding of requirements by all parties involved [2].

3) Completeness: All required information should be covered [4].

4) Verifiable: Each statement in the requirements should be accompanied by a method to examine whether the designed system satisfies the requirements [4].

5) Consistency: There should be no obvious and implied inconsistencies in the specification [4].

6) Understandability: Not only the specification authors and programmers, but also the users and customers are able to understand the requirements specification.

2.2 Requirements and Testing

Requirements engineering has influence on every phase development process, not only at the very beginning of the development. The V-Model in Fig.1 demonstrates the corresponding concerns of different layers and shows the relationships between testing and requirements at each layer.

Testing can be understood as the activity that aims to detect or prevent the defects in the system being designed, where defects are deviation from requirements. Testing activities involve reviews, inspections, analysis through modeling and the tests of components, subsystem and systems that are implemented. Any kind of testing as well as the resolving of detected problems can lead to great costs for design changes and even rebuilds if these testing activities begins until the system is almost completed. As a result, these activities should be planed and conducted as early as possible. The earliest activity is performed during the system design, and includes requirements reviews, design inspections, and various forms of analysis based on system models [2].

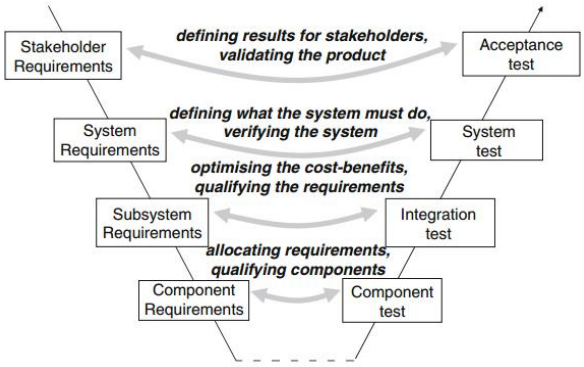

Figure 1: Requirements engineering in layers [2].

2.3 Requirements and Architectures

In a development process, requirements describe what the system should do, whereas the architectures show how the system does. A pattern named "ZIGZAG Pattern" can be undertaken as a method to depict the relationships between the requirements and architectures. It starts with the solution-free requirements, on the basis of which a system architecture is designed as solution to fulfill these requirements. This step is named as "Zig", from requirements to the system architecture. The architecture results subsequently in new requirements on the next abstraction level. These requirements bases on a designed architecture and are solution-free from the perspective of their level while they involve aspects of the solution on the upper level. The step from the architecture to the requirements is "Zag". Again a corresponding architecture can be derived from those new requirements, and so on. Thus, the "ZIGZAG Pattern" between requirements and architectures is formed in such way [5].

Moreover, the zigzag pattern also presents the interactions between different requirement types and architecture kinds. As shown in Fig.2, it covers the left side of the V-Model. The stakeholder requirements on the top level in a project describe the requirements from stakeholders' viewpoint and serve as fundamental to design a logical architecture that includes the technical concepts without technical details. That architecture results in system requirements that specify the requirements from the engineers' perspective and then the system architecture containing technical details of the system level is built based on these requirements. On the next level, components requirement and component architecture are generated according to the developing steps above.

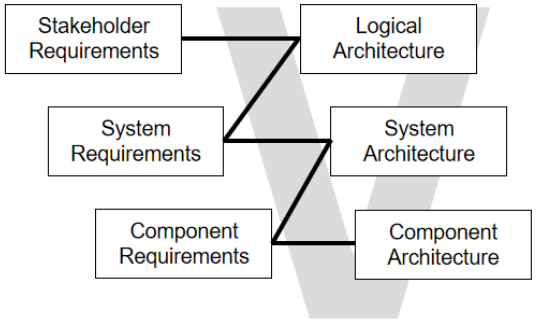

Figure 2: Requirements engineering in layers [6].

2.4 Requirements Decomposition

The concept of requirements decomposition is derived from the V-model of systems engineering

development and design, which is widely used in vehicle development process as well. Since the vehicle as a complex system is made up of many subsystems, each of which can be divided into further subsystems, they constitute a hierarchical relationship in terms of composition. In the context of vehicle system development, the conceptual, analytical, design and requirements work for the whole system can therefore be decomposed into parallel conceptual, analytical, design and requirements work for individual subsystems. The decomposed subsystem is simpler in structure and function, and the decomposed requirements make it easier to find a solution that meets the requirements, thus increasing the efficiency of system development [7].

3. Assessment definition

There are various approaches for the definition and execution of assessment in the research field of testing, addressing different test contexts and test instruments. In this paper, a concept of automated function assessment proposed by King [8] is utilized.

This concept enables the assessment and the scenario or test case description to be separated. As depicted in Fig.3, the assessment is partitioned into the activation and the actual test, and it utilizes activation and test conditions. These conditions are not only able to be generated with raw information from the vehicle bus and simulation, but also can be determined using derived additional information from the simulation. Hereinto, the test conditions start to be evaluated only if all activation conditions are satisfied and end when the activation conditions are either not met or predetermined period has passed. Each violation of the test condition is recorded [8].

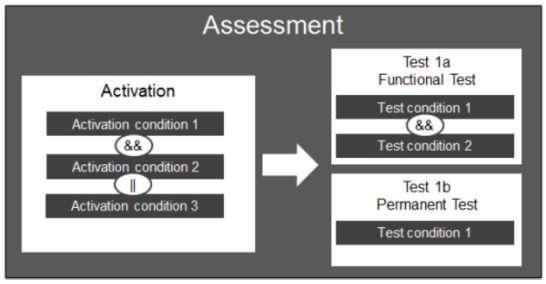

Figure 3: The structure of an assessment [8].

4. Vehicle data classification based on Requirement decomposition

4.1 Requirements Decomposition

Similar to other vehicle security requirements, vehicle data security requirements can be decomposed so that they are addressed through vehicle systems and their interactions. A decomposition method for vehicle data security is proposed in this paper.

Security requirement decomposition typically starts with security goals. The purpose of vehicle data security is to protect the data in each processing stage of the whole life cycle of data security, and data processing and vehicle function scenarios are associated, so the decomposition of vehicle data security requirements can be based on the scenario-based security goals to start. Vehicle data processing does not merely involve the vehicle itself, as there also exists data interaction between the vehicle and other terminals, such as cloud platforms, mobile apps, etc. Therefore, data security goal can be further decomposed into data security requirements of vehicle level, data security requirements of cloud platform level, etc. Then, based on the vehicle system architecture, vehicle data security requirements can continue to be broken down into different system requirements. According to the full data life cycle, those vehicle data security requirements can be divided into requirements on data collection systems, data storage systems, data processing systems, data usage systems and data

transmission systems. The data collected inside and outside the vehicle via the collection system is utilized or further processed by other systems for the operation of the relevant vehicle functions, some of the data is transferred outside the vehicle via the transmission system. Therefore, there exists the flow of data and interaction of functions between these systems. Each system requirement can be further decomposed into sub-system requirements, for example, the requirements on data collection systems will be decomposed into requirements for various collection devices, including cameras, microphones, radars, etc. The process of decomposing the vehicle data security requirements as described above is illustrated in Fig.4.

An example is shown below to explain the process of requirements decomposition process more explicitly.

As shown in Fig.5, one data security goal in the scenario operating in sentinel mode is that sensitive personal information is protected. When this security goal is decomposed to the vehicle level, one security requirement that can be decomposed is that the sensitive personal information in the collected data should be anonymized before the vehicle transmits those data. Another security requirement of the vehicle level is that vehicle should protect the stored sensitive personal information from unauthorised access.

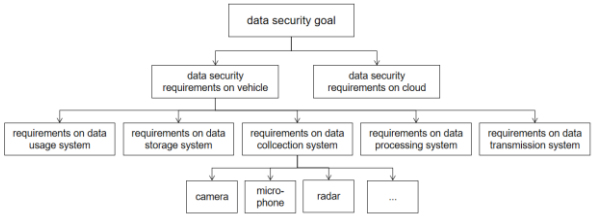

Figure 4: Requirements decomposition for vehicle data security.

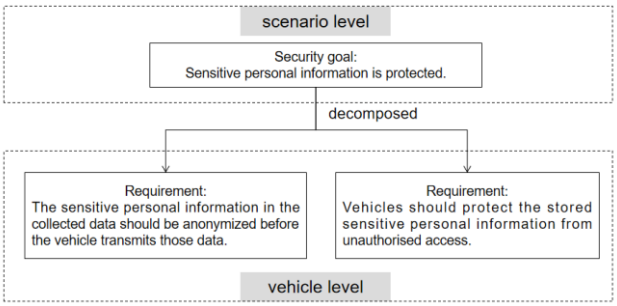

Figure 5: An example of the requirements decomposition from security goal to the vehicle-level requirement.

These two requirements on the vehicle level can be further decomposed into requirements on the system level. The data processing system plays an essential role to fulfill the requirement about the anonymisation can be further broken down into requirements on the data processing system, which plays an essential role to fulfill that requirement. For instance, one decomposed requirement is that face and licence plate targets in the video and image data should be anonymized before the transmission out of the vehicle ,since the face and licence plate belongs to the sensitive personal information, leakage of this information may result in threats to the subject of the personal information. Another decomposed requirement address the interaction with the data transmission system, as shown in Fig.6.

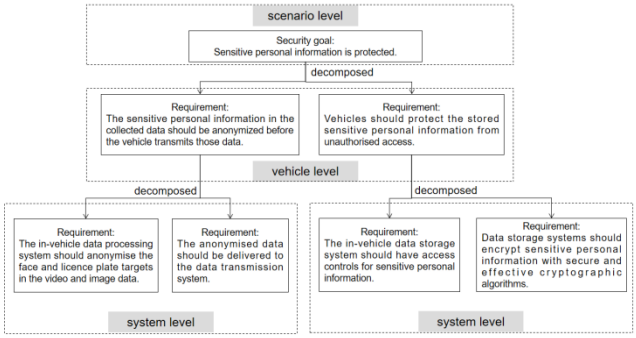

Figure 6: An example of the requirements decomposition from the vehicle-level requirement to system-level requirement.

In addition to data transmission, the requirements for data storage on the vehicle level are mainly realized through data storage systems. When decomposing data security requirements at the vehicle level, on the one hand, the data storage system is required to implement access controls for sensitive personal information. On the other hand, there is also a requirement for data security in respect of the encryption of sensitive personal information in data storage systems (see Fig.6).

As the decomposition of data security requirements continues, the system level requirements are divided into subsystem levels, which the expected functionalities are actually realized. An example of the anonymisation requirement in depicted in Fig.7, the requirement on the data processing system is further decomposed into requirements addressing the target detection rate and false detection rate for anonymisation module as one of the subsystems.

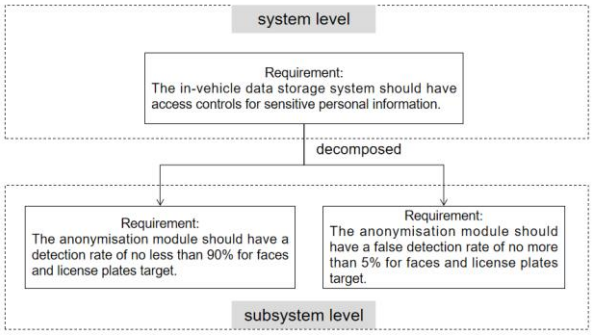

Figure 7: An example of the requirements decomposition from the system-level requirement to subsystem-level requirement.

4.2 Vehicle Data Classification

Compared to other security and safety requirements such as functional safety and information security, the classification of vehicle data is crucial to the assessment of the coverage of vehicle data security requirements. The grounds are that data classification is the starting point of data life cycle security management, and the data with the level determined by data classification has the possibility to implement security control measures in each step of its life cycle, as well as different levels of data are subject to varying security risks. A principle to grading vehicle data quantitatively is presented below.

The vehicle data is classified in terms of three factors: severity, controllability and importance. A major classification factor is severity, that is, the degree of harm caused by a security event such as data tampering, destruction, leakage, or illegal access. Vehicle data that has the potential to cause a more severe data security hazard requires a higher level of protection measures to be imposed, and therefore that data has a higher degree of severity. Controllability is intimately related to the extent to

which vehicle data can be disseminated. The more widespread the data is transmitted implies that it can be processed by more vehicle data processors, with less control available in the event of a security incident with that data. Importance measures the significance of vehicle data to data processors, taking into account the various costs invested in processing the data, as well as the expected benefits of processing the data.

The classification degrees for those three factors are as follows. The minimum severity situation is where a data security incident causes no harm, so the lowest severity degree is defined as 0. When data is processed solely in the vehicle, the potential data security risk is in general controllable, so the controllability degree is set to 0. Since data processors need to contribute to the cost of processing vehicle data with the expectation of benefits, the importance degree is calculated starting from 1.

Severity - S

– S0: causing no impact on individuals and data processors

– S1: causing limited minor negative impact on individuals and data processors

– S2: causing a certain harm to legitimate rights and interests of the individual's personal information subject, or causing serious harm to the corporate rights of data processors

– S3: causing harm to national security, social rights and interests, or serious harm to the legitimate rights and interests of the individual's personal information subject

• Controllability - C

– C1: data in the vehicle

– C2: data out of the vehicle and controlled by single data processor

– C3: data controlled by more than one data processor

– C4: data controlled outbound

• Importance - I

– I1: few additional costs required for data processing and no benefits from the data

– I2: a certain amount of cost required and limited benefits from the data

– I3: higher cost required and greater benefit from the data

– I4: enormous cost required and huge benefit from the data

As the grading of vehicle data necessitates consideration of the combined effect of these three factors, vehicle data can be classified based on the sum of these three factors. The vehicle data is divided into four levels, and the vehicle data is defined as the highest level when the degree of all three factors reach maximum. This type of vehicle data will demand the most stringent protection. This is due to the fact that the occurrence of a data security incident can result in significant harm, hindering data processors from achieving their original goals and potentially incurring massive cost losses, and the difficulty of controlling the impact of the data security incident is exacerbated by the presence of data controlled or processed offshore. TABLE 1 demonstrates the correspondence between the sum of the three factor degrees and the four data levels. Data Level 4 (D4) refers to the highest data security level while Dara Level 1 (D1) represents the lowest.

Table 1: Correspondence between Factor Degree and Data Level

Factor's degree sum	**Vehicle data classification**
11	Data Level 4 (D4)
10 or 9 or 8	Data Level 3 (D3)
7 or 6 or 5	Data Level 2 (D2)
4 or 3 or 2	Data Level 1 (D1)

To evaluate the vehicle data level, the three factor degrees S, C, and I are first identified in terms of the situation in which the data security accidents related to the data occurs, as well as the cost and benefits for the data processor. Following that, the data level can be determined by combining the three

degrees, using the correspondence principle stated in 0.

So as to be capable of directly identifying the level of the vehicle data, the relationship between the degree of the three factors (S, C, I) explained above and the data level (D) is summarized in the figure (Fig.8) below.

Severity - S	Importance - I	Controllability - C			
		C1	C2	C3	C4
S0	I1	D1	D1	D1	D2
	I2	D1	D1	D2	D2
	I3	D1	D2	D2	D2
	I4	D2	D2	D2	D3
S1	I1	D1	D1	D2	D2
	I2	D1	D2	D2	D2
	I3	D2	D2	D2	D3
	I4	D2	D3	D3	D3
S2	I1	D1	D2	D2	D2
	I2	D2	D2	D2	D3
	I3	D2	D2	D3	D3
	I4	D2	D3	D3	D4
S3	I1	D4	D4	D4	D4
	I2	D4	D4	D4	D4
	I3	D4	D4	D4	D4
	I4	D4	D4	D4	D4

Figure 8: Vehicle data classification.

5. Test Verification

Under the idea of V-model and requirements engineering, the test verification for the designed system should be derived from the corresponding requirements. The decomposed requirements facilitate the test verification at different architecture levels. An approach to derive tests from decomposed vehicle data security requirements is accounted for in this section. Moreover, the principle addressing determination of the requirement coverage is explored based on the decomposition and test results.

5.1 Test derivation

Tests can be derived with using decomposed requirements, which also illustrates the correspondence between requirement and verification. The test definition on the concept mentioned in section 3, in which assessment is separated into activation conditions and test conditions.

The activation and test conditions are checked whether they are met or not with the support of various signals. The Fig.9 demonstrates that the signals in the conditions are defined based on the factors in the related requirement. Factors can be interpreted as variables contained in the data security requirements, such as the switching status of the sentry mode, the number of face targets detected, or the storage address of the data.

Fig.10 shows the test derived according to the requirement that “the anonymisation module should have a detection rate of no less than 90% for faces and license plates target”. The three factors extracted from the requirement are assigned to the variables of the activation condition and the test condition. As the requirement focuses on the sensitive personal information in the collected video and image data, the assessment is activated when the data type is video or image. For the test condition, the test is passed when the detection rate of both face target and license plate target reaches 90% or above.

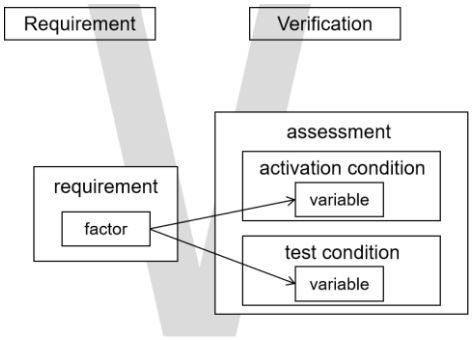

Figure 9: Test derivation from requirement.

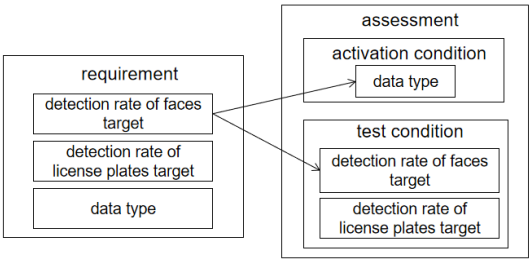

Figure 10: An example of the test derivation based on one the requirements decomposition.

Based on the requirement of false detection rate, activation conditions and test conditions can be derived in a similar way. The assessment activation conditions and test conditions corresponding to these two decomposed subsystem-level data security requirements are summarized in TABLE 2.

Table 2: Derived assessment

Assessment	Activation condition	Test condition
1	data type=video or image	detection rate of faces target >=90% and detection rate of license plates target >=90%
2	data type=video or image	false detection rate of faces target <=90% and false detection rate of license plates target <=90%

5.2 Test execution

Tests addressing the anonymisation are carried out, in order to verify the decomposed requirements at the subsystem level presented in Fig.7.

In the test procedure, the anonymized out-of-vehicle collected video is acquired and then random frame sampling is performed to extract 500 images as test data. Therefore, the activation condition of the assessment in TABLE 1 is fulfilled. To evaluate whether the test passes or fails, the detection rate and the false detection rate need to be calculated.

The calculation of the detection rate requires measuring the number of positive detections and the number of deserved detections. The ratio of the number of false detections to the number of detections is the false detection rate. The detection number refers to total amount of anonymized objects marked as face target. The number of deserved detections is the number of targets that should be subject to anonymization. Through image labeling and target comparing, the detection rate and false detection rate of face target and license plate target are calculated (see TABLE 3).

According to the test conditions defined from the requirements, the detection rate and false detection rate of the face target and license plate target passed the test. The corresponding decomposed requirements can be verified to be satisfied.

Table 3: Test results

Target type	Face target	License plate target
Positive detection number	36	347
Deserved detection number	37	349
False detection number	0	7
Detection number	97	773
Detection rate	97.31%	99.43%
False detection rate	0.00%	0.91%

5.3 Coverage analysis

The coverage analysis is executed in order to determine the requirement coverage degree, which can be used to represent the extent to which the requirement is fulfilled by the designed system. The coverage degree of one requirement can be decided based on the results of test verification, which include not only assessments derived from that requirement, but also the requirements at its sub-levels. As a result, when constructing a method to determine the coverage degree, the data level of the vehicle data involved should be also taken into account. The test assessment addressing the vehicle data with greater data level has more impact on the satisfaction of the requirements since such vehicle data is more vital to the overall data security. Therefore, such test assessment is designed to weight more while determining the coverage degree, and the coverage degree of the requirement can be assessed with combined consideration of the test result and the data level.

A mathematical formula (1) is devised to calculate the coverage degree of a data security requirement in order to evaluate the compliance of the requirement quantitatively. In the formula, D stands for data level, P for the proportion of passed results in all test results for one test assessment such as the derived assessment in TABLE 2, and n for the number of the test assessments involved in the calculation. The weighting is determined as the proportion of individual data levels in the additive value of data levels of all related requirements, which can also reflect the data level's influence on the evaluation of requirement coverage.

$$\text{coverage degree} = \frac{D_1}{\sum_{i=1}^{n} D_i} \times P_1 + \frac{D_2}{\sum_{i=1}^{n} D_i} \times P_2 + \cdots + \frac{D_n}{\sum_{i=1}^{n} D_i} \times P_n \quad (1)$$

As an example, the video or image data of face and license plate in the anonymisation requirement belongs to sensitive personal information, thereby its severity degree can be defined as S2. Since the data anonymisation process is carried out in the vehicle, the controllability is C1. The anonymization process takes additional algorithm development, and there is a cost for the vehicle-side module to carry the anonymization algorithm, the importance refers to I2. The data level is thus D2, according to the previous principle shown in Fig.8. During the coverage degree determination for this requirement, the test results for the anonymisation of face target and license plate target need to be taken into account.

6. Conclusion and outlook

The paper set out to develop a method for the requirement decomposition as well as a process for the test derivation based on decomposed requirements, in order to better deal with the fulfillment of vehicle data security requirements. The theoretical background surrounding requirements engineering

is introduced, covering the association between requirements and testing, requirements and architecture, and the significance of requirements decomposition, as an important foundation for the concept development in this paper. This paper proposes a method for decomposing data security requirements, from security goals on the basis of data processing scenarios to vehicle-level requirements, and then refined to the data security requirements of diverse systems, and finally to the sub-system level. In this regard, the system level is classified along various data processing activities and the subsystems serve as functional modules for the realization of requirements. The vehicle data security requirement decomposition for the protection of sensitive personal information is presented and analyzed as an exemplary case in order to explain the concept of requirement decomposition more visually. The vehicle data can be classified into four levels considering the combined effect of severity and controllability after data security accidents, and the importance for the data processor.

Test verification has been a key part of vehicle development. Tests are derived from decomposed requirements, which reflects the relevance of requirements and tests. The decomposition of vehicle data security requirements facilitates vehicle developers to more explicitly deploy data security technologies into specific functional modules, while making it easier to perform test verification activities. The calculation formula for coverage degree developed in this paper takes into account the impact of vehicle data level and test results. The data level is utilized as the weighting for the test result for each test assessment which is relevant to the requirement.

In future work, researching the requirement decomposition into more refined subsystems according to the development demands might prove important, since the vehicle data processing is increasingly complicated. In addition, it would be of great significance if the traceability of requirement decomposition and test verification could be implemented using automatic tool.

Acknowledgment

Over the course of my researching and writing this paper, I would like to express my thanks to all those who have helped me. I also express my appreciation to the company for the support during the test data collection and testing implementation.

References

[1] Zhang L , Xing X , Chang X ,et al.Research on Data Segmentation Technology of Grid-Connected Test System for New Energy Plants[C]//Student Conference on Electrical Machines and Systems.2020.
[2] E. Hull, K. Jackson, and J. Dick, "Requirements Engineering", 3rd ed., Springer-Verlag London, 2011.
[3] A. Lucia, A. Qusef, "Requirements Engineering in Agile Software Development", Journal of Emerging Technologies in Web Intelligence. 2, doi: 10.4304/jetwi.2.3.212-220, 2003.
[4] Y. Chen, H. Miao, "Integrating object-oriented methods and formal methods for requirement engineering", Journal of Harbin Institute of Technology (New Series). vol. 11, 2004, pp. 295-299.
[5] T. Weilkiens, J. Lamm, S. Roth, and M. Walker, "Model-based system architecture", Wiley, 2016.
[6] G. Madzar, "Anforderungen vs. Architektur - Das SYSMOD ZIGZAG Pattern", url: https://medtech-ingenieur.de/anforderungen-vs-architekturdas-sysmod-zigzag-pattern (visited on 02/02/2023).
[7] X. Zhu, H. Xue, "Study on Domain Ontology Model Based on Requirement Decomposition", Journal of Computer Applications, 2003(06).
[8] C. King et al., "Automated Function Assessment in Driving Scenarios". In: 2019 12th IEEE Conference on Software Testing, Validation and Verification (ICST), doi: 10.1109/ICST.2019.00050. 2019, pp. 414–419.