+300 pages of application knowledge about vehicle security according to UN Regulation No. 155, ISO/SAE 21434 & beyond

1000 THINGS WORTH KNOWING IN AUTOMOTIVE CYBERSECURITY

The Essential Guide to ISO/SAE 21434

SECOND EDITION

Incl. all ISO/SAE 21434 requirements and work products

Reproduced with official permission of ISO

AUTOMOTIVE CYBERSECURITY

THE ESSENTIAL GUIDE TO ISO/SAE 21434

How to manage the challenges of the new automotive cybersecurity standards and regulations

CYRES CONSULTING

READING SAMPLE

CYEQT

KNOWLEDGE BASE

CYBERSECURITY VERIFICATION AND VALIDATION

9.

Chapter contents:

9. CYBERSECURITY VERIFICATION AND VALIDATION

In-vehicle software has transformed the driving experience by providing new levels of comfort, convenience, safety, and security. Increasing demand for the latest connected features and automated driving functions necessitates a sophisticated approach that includes cybersecurity in existing verification and validation. This chapter describes the implementation of cybersecurity in verification and validation (V&V) by adapting existing approaches to V&V and also by introducing new ones. This chapter also addresses various ways of verifying and validating the specification that was discussed in Chapter 5 using methods of testing cybersecurity.

9.1 V&V – Definition and comparison

Verification and validation have been common practice in the automotive and other industries for decades, but there are still frequent misconceptions. This chapter therefore begins by defining and comparing the two terms.

Verification

The purpose of verification is to provide objective evidence that an item or component fulfills its specified requirements and characteristics [311].

Verification is a process that is usually used in the various phases of development to evaluate whether an item or component meets its specifications. In other words, verification aims to prove that an item or component has been developed correctly according to the requirements and the relevant methods, techniques, standards, and rules.

The verification process can be applied to any aspect of engineering that contributes to the definition and realization of the item or component (e.g. verification of a requirement, a development plan, a test case, or the product itself) [311]. As already mentioned in Chapter 5, verification is applicable to both sides of the V-model. On the left-hand side of the "V", verification is mainly used to ensure the correctness of the work products (e.g. requirements or development documents). Peer review of the requirements is one of the most common examples of verification on the left-hand side of the "V". In contrast, on the right-hand side of the "V", verification is mainly used to check the correct implementation of the item or component, i.e. to check whether the product fulfills its cybersecurity requirements and works without errors. Furthermore, verification results can also serve as an input to validation. A few examples of verification activities are presented in the figure below [362].

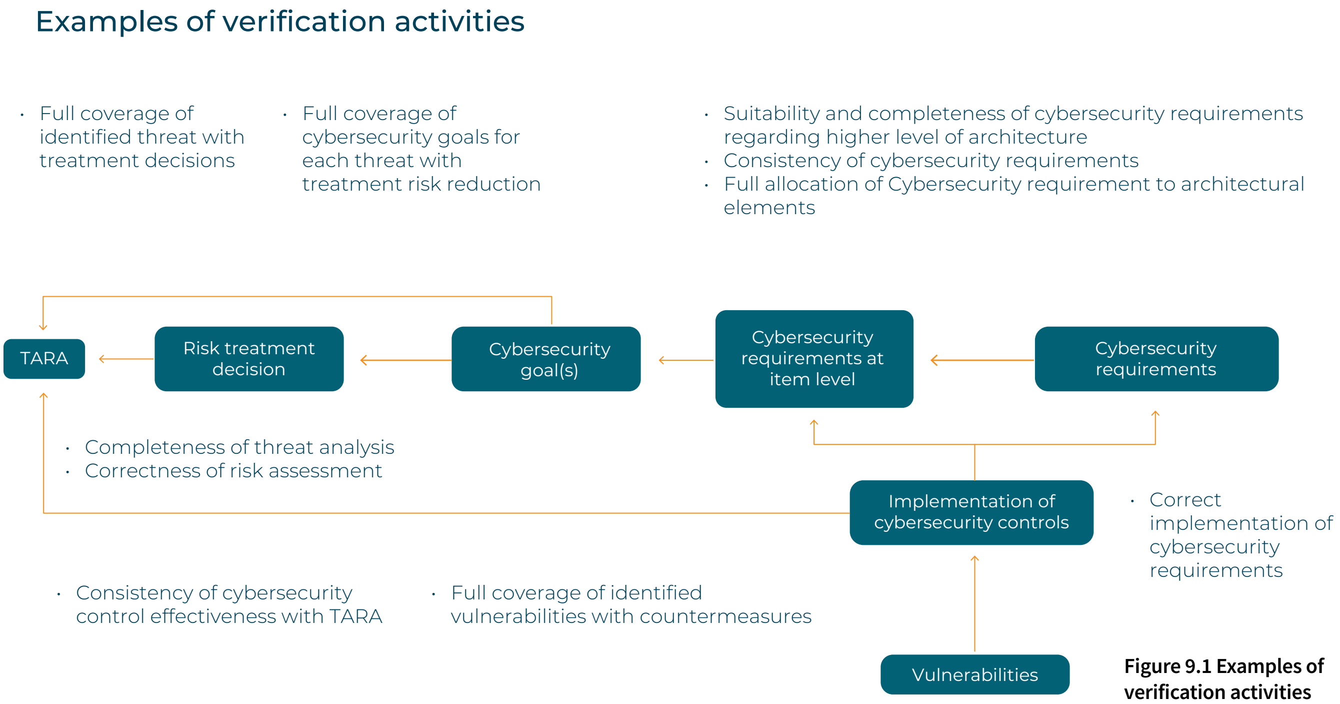
Examples of verification activities
· Full coverage of identified threat with treatment decisions
· Full coverage of cybersecurity goals for each threat with treatment risk reduction
· Suitability and completeness of cybersecurity requirements regarding higher level of architecture
· Consistency of cybersecurity requirements
· Full allocation of Cybersecurity requirement to architectural elements
TARA
Risk treatment decision
Cybersecurity goal(s)
Cybersecurity requirements at item level
Cybersecurity requirements
· Completeness of threat analysis
· Correctness of risk assessment
Implementation of cybersecurity controls
· Correct implementation of cybersecurity requirements
· Consistency of cybersecurity control effectiveness with TARA
· Full coverage of identified vulnerabilities with countermeasures
Vulnerabilities

Figure 9.1 Examples of verification activities

Validation

The purpose of validation is to provide objective evidence that the item or component, when in use, achieves its intended use in its intended operational environment and thereby fulfills its business or mission objectives and stakeholder requirements [311].

Validation is a process that is used to help ensure that the item or component meets the requirements of its stakeholders [311]. In other words, validation proves that the right system has been built for the intended use.

Similar methods are used for both verification and validation, but the two processes are not directly dependent on each other. This means that a product can be built in the right way according to its specification, but nevertheless, the validation may still fail. If the wrong stakeholders were identified or some stakeholder requirements were ignored, then the product might not be fit for its intended purpose. Validation would then be unsuccessful. For example, a language module for an infotainment system has been developed, and is available in English, German, Italian, French, and Spanish. This might fit the European market perfectly well. But if one of the stakeholder requirements states “the target market is China”, and this has been ignored, then a product has been developed which cannot be used as intended. In this case the validation fails.

9.2 V&V methods

When talking about verification and validation, it is important to keep in mind that this means more than just testing. There are other methods of V&V besides testing. It is therefore necessary to choose the right combination of methods in accordance with the circumstances of the project and the product.

The following methods are used most frequently:

- **Review** is a verification method in which a peer or another party checks the work product against certain objectives and criteria (e.g. readability, correctness, quality, etc.). Common examples include reviews of documents such as project management plans, schematic reviews of the HW that has been designed, and reviews of the software code that has been written.
- **Analysis** can be understood as a systematic investigation, based on logical reasoning, of the product or information pertaining to it. One of the most popular analysis techniques in the automotive industry is the Failure Mode and Effects Analysis (FMEA). At the hardware level in particular, Worst-Case Circuit Analysis (WCCA) is often applied. This is a systematic approach to assessing the functional performance of a circuit or system, taking into account factors such as component tolerances, environmental conditions, and ageing [361]. But the TARA is also discussed in Chapter 6 and the vulnerability analysis in Chapter 5 may also be used to support the verification and validation of a product.
- **Simulation** is a technique of mirroring the behavior of the system in real time by using various kinds of models instead of the actual physical product. For example, HIL simulation is a simulation technique that is widely used in the automotive industry. It involves mimicking a real time scenario for the system under test to verify the system’s behavior. If model-based systems engineering is applied, then state machines or architectural models can be used for simulations as well. This is a popular method when the final product is very expensive or there are few prototypes.
- **Testing** is a means of checking the performance and behavior of the real product against specific criteria. The most popular example is testing against requirements. But durability or endurance tests, stress tests, and penetration tests can also be allocated to this category.

9.3 Cybersecurity impact on V&V

The following sections discuss the impact of cybersecurity on V&V methods and activities.

9.3.1 Cybersecurity methods

It is not necessary to reinvent the wheel entirely where cybersecurity in V&V is concerned. Many ways of working in verification and validation can be reused or simply adapted. But there are also completely new methods that need to be considered. The methods of V&V used for cybersecurity can be classified as belonging to three distinct groups:

"Traditional" V&V methods

These are methods that are widely known in the automotive industry and have been used in practice for years or even decades, e.g., requirements-based testing, SW Unit testing, and integration testing. These test methods are primarily based on verification of the item, component, or element against the requirements, so no specific adaptations are needed for cybersecurity. Nevertheless, the results obtained by using these methods can be used directly to verify that an item or component has been implemented with correct cybersecurity controls according to the specified cybersecurity requirements.

Adapted "traditional" V&V methods

Well-known existing methods can be adapted to check the cybersecurity aspects of an item or component. They can be adapted in various ways, e.g. by changing the procedure of the method used, or by changing the verification criteria. The following are examples of how “traditional” V&V methods can be adapted to address cybersecurity:

- **Document reviews**: One possible adaptation is the integration of new roles for performing reviews, e.g. a cybersecurity manager who needs to examine additional project-related documents to ensure consistency and alignment with other disciplines, e.g. by checking the project management plan. Furthermore, there are new documents dedicated specifically to cybersecurity, e.g. cybersecurity plans and cybersecurity requirements, which need to be reviewed by other stakeholders. It might also be necessary to define new verification criteria for existing work products, such as system architecture, to check that cybersecurity aspects have been adequately addressed and do not interfere with functional safety or performance aspects.
- **Fault Tree Analysis (FTA):** This approach is a tool used to analyze the fault path of a system-level fault. This method can be adapted to investigate the attack path of a system-level attack vector. The adapted tool is called an Attack Tree Analysis (ATA) according to ISO/SAE 21434 and has already been discussed in Chapter 6.
- **FMEA:** This analysis is a method of analyzing potential failures early on during the development phase of an item or component. It can be adapted by extending the severity evaluation to include cybersecurity aspects, when calculating the impact of failures of the item or component. The results of this method can be compared with the TARA in order to support completeness and consistency in the analysis of cybersecurity risks.
- **Static Code Analysis (SCA):** This traditional analysis can be adapted by choosing the right database, i.e. choosing CWE and CVE as the database. Adding aspects of cybersecurity as a source in the database helps to identify the security vulnerabilities of the system. This analysis adapted for cybersecurity is also called Static Analysis Security Testing (SAST).
- **Stress Testing:** Stress testing, in the context of cybersecurity, assesses a system's ability to withstand high loads, particularly during simulated denial-of-service (DoS) attacks. These tests involve generating a large volume of requests to overwhelm or deplete system resources, e.g. network bandwidth, the central processing unit (CPU), memory, etc. [362]

V&V methods specific to cybersecurity

These are methods which are quite new to the industry, due to the need for cybersecurity. They are either reused from other industries, such as IT, or completely newly developed. Cybersecurity is still a relatively new field in the automotive sector, so there is relatively little knowledge and experience available. This lack of knowledge and experience leads to less instruction being available on how to perform these V&V methods. The following methods are therefore described in detail later in this chapter to help readers become acquainted with V&V methods that are specific to cybersecurity:

- Functional Cybersecurity Testing
- Vulnerability Scanning
- Fuzz Testing
- Penetration Testing

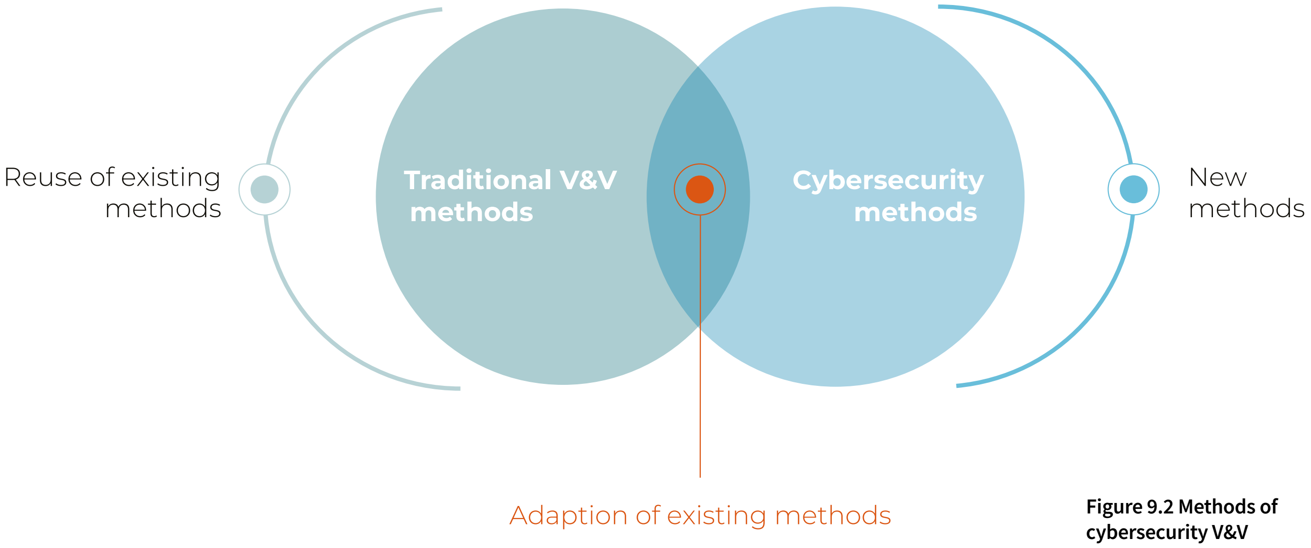

Figure 9.2 Methods of cybersecurity V&V

9.3.2 Cybersecurity activities

Cybersecurity V&V activities exist at all levels throughout the development lifecycle. They start with an initial review of specifications at the vehicle level and continue through the various levels of item or component down to the software and hardware levels. While reviewing the specifications, it is essential to examine the cybersecurity-specific elements of the product separately from the elements that are not cybersecurity-specific, in order to detect unknown or hidden vulnerabilities.

Verification on the left-hand side of the V-model entails not only a review of requirements and system architecture, but also an assessment of the performance of the item or component, in order to prove the effectiveness of the overall cybersecurity concept before spending time and money on implementation. For example, an ATA verifies that the proposed cybersecurity concept protects the item or component against the potential attack vectors which have been identified.

Interfaces often present entry points for attack. So, from a cybersecurity point of view, during specification reviews on the left-hand side of the V-model, special attention must be paid to the Interface Control Document (ICD), which contains information about interfaces between system elements, and the Hardware Software Interface Specification (HSIS), which contains information about interfaces between the hardware and software components of the system.

At the SW level on the left-hand side of the V-model, any third party libraries that have been used should be checked for their quality and compliance with relevant cybersecurity standards. Furthermore, the coding guidelines and SW design rules that have been used need to be updated to address cybersecurity. A good example of a valuable reuse of existing V&V methods for cybersecurity purposes is static code analysis. If static code analyses are executed for the complete software in a way that complies with common automotive standards such as MISRA-C, the risks associated with unknown or unused software can be reduced significantly, and additional vulnerabilities, such as backdoors in the software code, can be avoided.

On the right-hand side of the V-model, cybersecurity activities are mostly related to verification of the correct implementation of requirements and architectural elements. As already mentioned in Section 5.4, these verification activities must be performed at all levels of abstraction (not only at the product level) to fulfill the requirements of ISO/SAE 21434.

Before starting the overall validation of the product as a whole, e.g. in the form of penetration testing, the assumptions and evaluations from the early stages of development need to be verified once again, because the circumstances of the project or product might have changed. In particular, the results of the cybersecurity risk assessment (i.e. TARA) and any project assumptions which impacted cybersecurity development need to be checked again for their validity as they might have been defined as long as two years ago. For example, the probability of an attack scenario or the assumptions about the intended use-cases of the target products might change over the years of development.

9.4 Cybersecurity V&V strategy

The following sections provide an overview of why the guidance of an effective V&V strategy for cybersecurity can significantly impact a project's performance and schedule. There is also a discussion of the general V&V goals and results that need to be thought about when developing the strategy.

9.4.1 Need for cybersecurity V&V strategy

Let us begin with a simple question: What is a strategy?

According to ASPICE: "Having a strategy means that all parties involved in achieving the process outcomes have agreed on the methodological approach, on how to deal with constraints, in order to achieve these process outcomes" [305].

In other words, the V&V strategy defines an agreed way to produce a verified and validated product, taking into account the needs and constraints of the project and the affected disciplines.

Usually, different kinds of requirements address different areas of the project, e.g. maintenance and production, which impact V&V objectives and activities. A common approach to meeting these requirements must be agreed in the V&V strategy, in which attention needs to be paid to various aspects, some of which are outlined here:

- **Release planning:** The maturity of the V&V activities needs to be aligned with the planned intermediate releases and deliveries of the product. The scope and schedule of cybersecurity V&V activities therefore need to be aligned with the project planning.
- **Functional Safety (FuSa)**: Widely used methods for FuSa compliance, such as FMEA, and checkers of coding rules, such as MISRA-C, need to be taken into account when planning V&V activities. And ISO 26262 requires dedicated test methods based on the criticality level. This should be reflected in the strategy.
- **Stakeholder needs:** Diverse stakeholders are likely to have diverse interests and expectations as regards the steps in the verification of the developed products, e.g. the use of product samples for winter or desert testing.
- **Costs:** Expenditure on equipment and staffing needs to be kept in line with the overall project budget.
- **Responsibilities:** V&V activities affect different teams within a project, so a clear allocation of responsibilities needs to be defined and agreed. A typical open question is whether the cybersecurity team or the test team is responsible for specifying cybersecurity-related test cases.

Now, with cybersecurity, an additional area needs to be considered in the V&V strategy. The proof that the product is cybersecure, taking into account the new standards and regulations (ISO/SAE 21434, UN R155, R156) as well as new requirements (new tests, methods, criteria, etc.) requires that new content and aspects be added to the existing V&V strategy. But existing project needs and the aspects of the V&V strategy that have already been defined also need to be adapted, because cybersecurity has an impact on the original ideas and plans of the project. For example, penetration testing could have an impact on the estimated costs and planned infrastructure, and test results in relation to cybersecurity requirements may have to be provided to the technical service within a specific deadline.

Please note that there is no dedicated requirement that stipulates that the cybersecurity V&V strategy should be a document in its own right or, alternatively, that it should be part of the overall V&V strategy for the whole project. It is good practice to combine both viewpoints in one work product, in order to enable inter-disciplinary teams to develop a shared understanding of and approach to V&V. The figure below illustrates in broad terms how cybersecurity can be integrated into an existing V&V strategy both by amending existing areas of the V&V strategy and by adding new cybersecurity-specific aspects.

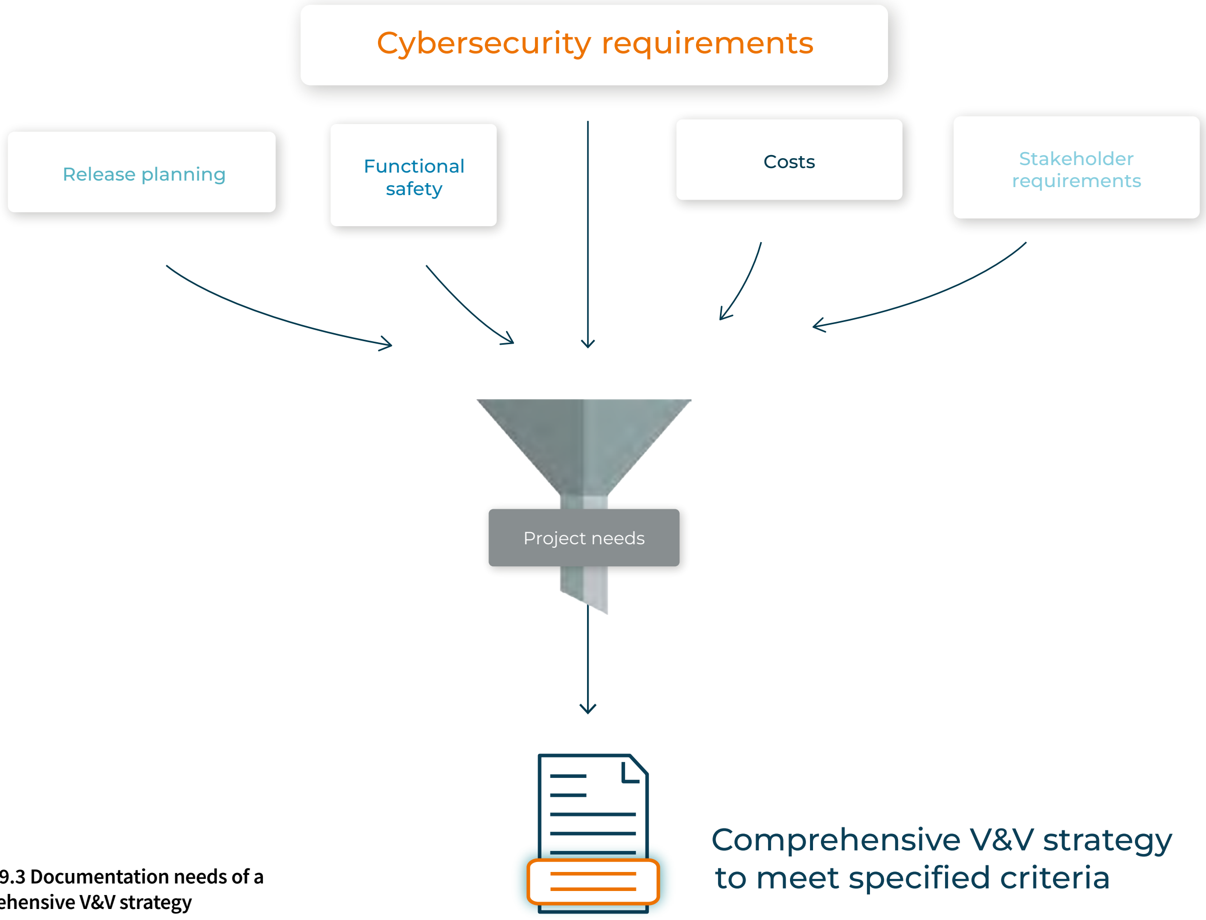
Cybersecurity requirements
Release planning
Functional safety
Costs
Stakeholder requirements
Project needs
Comprehensive V&V strategy to meet specified criteria

Figure 9.3 Documentation needs of a comprehensive V&V strategy

9.4.2 Goals of cybersecurity V&V

The goals of cybersecurity V&V activities should be the subject of agreement between project management, test teams, and the cybersecurity team, so that differing interests are combined and harmonized. This synchronization between the teams aims to ensure a shared understanding of customer expectations and the potential risks of neglecting cybersecurity V&V activities, and to cultivate awareness of the limited availability of resources and the need to follow timelines. Defining cybersecurity goals for V&V activities need not conflict with the existing goals of the V&V strategy, because the chances are high that the existing goals already address cybersecurity needs.

Two different kinds of relevant KPIs (key performance indicators) can be considered when measuring the extent to which V&V goals are being met. These are: 1. KPIs related to those requirements that specify a clearly defined approach to verification (e.g. tests, reviews, analysis); and 2. KPIs related to those requirements that are concerned with the results of verification. To aid understanding, here is some further explanation of these KPIs:

KPIs related to requirements that specify a clearly defined approach to verification

A possible target might be that 100% of cybersecurity requirements specify a clearly defined approach to verification. A verification approach indicates HOW the requirement is to be verified. This could include item or component tests, reviews, and simulations. This may be regarded as essential because ISO/SAE 21434 requires that all cybersecurity requirements shall be verified (see also **RQ-10-09**).

The approach to verification can be defined within the requirements management tool by setting an attribute that specifies the method of verification. It is good practice to set down an initial proposal regarding the approach to verification during the creation of the requirement. This can be confirmed later by the tester on the basis of peer reviews. If the tester does not agree to the methods of verification or the requirement itself, then this could be a good indication that the requirements have been misunderstood. At this stage it is possible to clarify any misunderstandings easily, and through a further iteration, make appropriate adaptations to satisfy both customer and tester expectations.

It is important to be aware that the approach to verification can vary according to the level of abstraction (e.g. vehicle, item, component, or sub-component) and the nature of the requirements (e.g. functional, physical, process, etc.).

KPIs related to requirements that are concerned with the results of verification
A possible target might be that 100% of the results of the verification tests show that the requirements have been met. If the target is less than 100%, this must be justified by an appropriate rationale.

ISO/SAE 21434 states that the test coverage shall be evaluated using defined test coverage metrics. For testable requirements, this KPI means that all requirements are related to specific tests and test results with "pass" status.

Test results can be documented in various ways, e.g. using a requirements management tool, such as codeBeamer or DOORS, or by using a consistent naming convention.

9.4.3 Rules for cybersecurity V&V

In addition to cybersecurity V&V goals, specific cybersecurity rules for the verification and validation process might also be required for the purpose of managing the impact of cybersecurity on the financial, privacy, safety, and operational aspects of a product. Potential rules for cybersecurity during verification and validation are described in this section. The rules which are to be applied need to be selected on a case-by-case basis, according to the circumstances of the project.

- **Target hardware**
  Cybersecurity tests shall always be executed on the target hardware, which means using the same hardware components that will be in the final vehicle (including the same calibration and configuration). If tests are not executed on the target HW, the potential deviations need to be analyzed to prove that changes to the HW have no impact on any cybersecurity controls and do not add new or unknown vulnerabilities.

- **Cybersecurity as highest priority**
  Cybersecurity V&V activities shall always be given highest priority by default. Due to time or resource limitations, there is always a possibility that certain verification activities may be skipped. In this case, it is necessary to ensure that cybersecurity-relevant tests do not fall victim to deprioritization.

- **Highlighting cybersecurity**
  Cybersecurity V&V test results shall be uniquely highlighted. When tests are being carried out, cybersecurity and non-cybersecurity tests are not normally conducted separately in order to ensure appropriate follow-up actions from a cybersecurity point of view. Furthermore, in the case of failed tests which are non-cybersecurity-specific, these test cases need to be clearly identified or highlighted to rule out any cybersecurity risk to the product. Depending on the tool environment, cybersecurity-specific test cases can be indicated by using a specific attribute or naming convention, or simply by highlighting the test results with a specific color. Please note that all tests that are used to verify cybersecurity requirements are automatically considered to be cybersecurity relevant.

- **Cybersecurity experience**
  Cybersecurity test cases and test results shall be evaluated by a person experienced in the field of cybersecurity. In many companies, tests are developed and carried out by in-house departments with little knowledge of cybersecurity. To ensure that such tests meet the intended purpose and fully cover the cybersecurity requirements, they should be checked by a person who is experienced in cybersecurity (see also **RQ-05-07**). Ideally, the person responsible would be the cybersecurity manager or a cybersecurity engineer working on a related project.

- **Test case coverage**
  Modified Condition/Decision Coverage (MC/DC) shall normally be reached for all requirements; Any exceptions must be evaluated. MC/DC coverage means that all the potential scenarios and combinations of a requirement are covered by test cases. To avoid any unknown vulnerabilities, all imaginable use cases and parameters - even theoretical ones - must be verified by one or more test cases.

- **Pending and failed test results**
  An impact assessment needs to be carried out on all requirements with pending or failed verification results. During product development, there are always test cases that cannot be tested as planned, or tests that fail and cannot be re-tested until the next delivery of the product. In such scenarios, the potential impact on the cybersecurity goals and requirements needs to be evaluated. If the resulting risk is acceptable, then the related argumentation needs to be added to the test results in order to approve delivery of the product.

9.4.4 Expectations and open questions

There is no commonly accepted definition of the aspects that must be covered by a cybersecurity V&V strategy. Definition of the strategy depends on the project scope, the product, and, of course, the role of the company in the overall lifecycle. The relevant criteria for a V&V strategy for an OEM are likely to differ from those for a typical ECU supplier or a SW supplier.

Nevertheless, there are some aspects which should be covered in a strategy regardless of the type of company. ISO/SAE 8477 proposes the following as a minimum:

- identification of the item or components in scope, including their references,
- definition of the purpose of corresponding activities,
- selection of methods and exposition of the rationale that justifies their selection,
- reference to a cybersecurity plan,
- reference to corresponding cybersecurity interface agreement(s) in the case of distributed development.

The exact ways in which a V&V strategy is to be defined are not specified, however. This means that there are always a lot of open questions as regards what needs to be part of a V&V strategy and how the various aspects should be integrated. Reference to various automotive standards raises a number of questions. The standards are not always cybersecurity-specific, but the following questions serve as a source of ideas for topics that could be covered by a cybersecurity V&V strategy.

- How can traditional testing and cybersecurity testing be combined?
- What is the test scope? At which system level(s) should testing be performed?
- Who is responsible for the definition and execution of cybersecurity tests? What are the required competencies in terms of cybersecurity?
- Which test methods should be applied? And which test methods are feasible in the context of the project? Which methods cover cybersecurity concerns sufficiently?
- What are the criteria for passing or failing cybersecurity verification and validation? How much testing is sufficient, especially where penetration testing is concerned?
- What tests are relevant for which sample or release?
- What test environment and which prototype are needed for the cybersecurity test? What degree of product maturity is required for the testing of cybersecurity controls?
- Which tools are needed for the execution of cybersecurity V&V activities? Are additional licenses required?
- To what extent must different tests be independent of one another?
- In what ways must the tester be independent?
- How should failed cybersecurity test cases be dealt with? What scope should be re-tested? How should regression tests be handled?

It is clearly not possible for a project team to answer all the questions immediately. Some questions will require in-depth investigation. And some may not be answered for the duration of the project. But, although the task is challenging, this should not stop the team from starting to investigate and discuss these issues. This will raise awareness and begin the process of problem solving. Even if only some of the issues can be resolved, this is a great success compared with ignoring them.

9.5 Cybersecurity testing

In order to address the open questions from the previous section and with cyberattacks becoming increasingly common, it is more important than ever before to perform adequate cybersecurity testing, in order to identify vulnerabilities and ensure iteratively that proposed cybersecurity controls are still valid. In this section, the following test methods: functional cybersecurity testing, vulnerability scanning, fuzz testing, and penetration testing are discussed in detail.

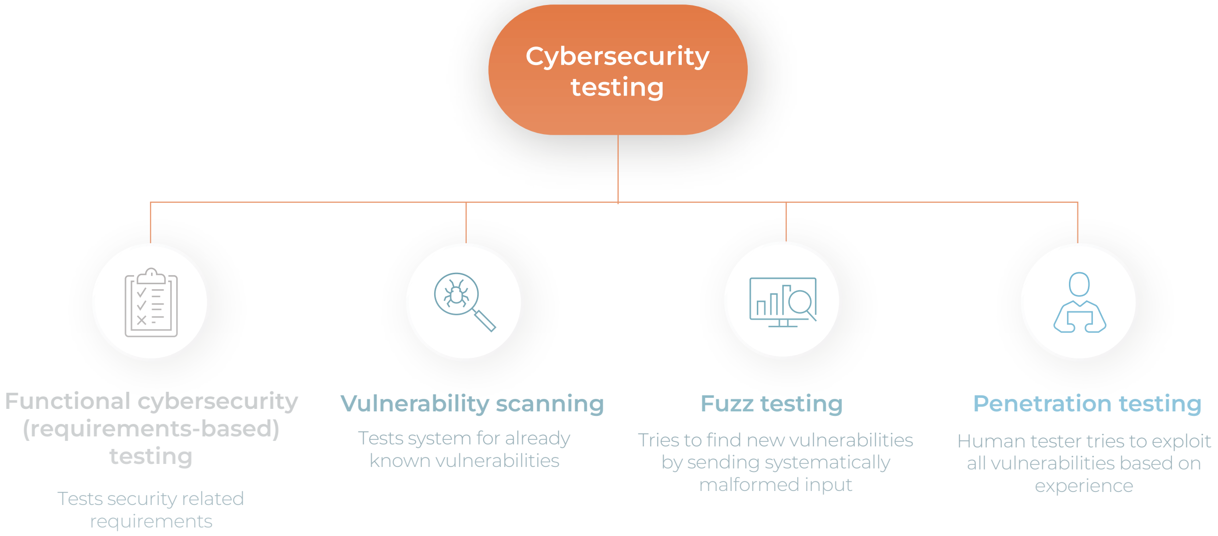
Cybersecurity testing
Functional cybersecurity (requirements-based) testing
Tests security related requirements
Vulnerability scanning
Tests system for already known vulnerabilities
Fuzz testing
Tries to find new vulnerabilities by sending systematically malformed input
Penetration testing
Human tester tries to exploit all vulnerabilities based on experience

Figure 9.4 New testing methods of cybersecurity V&V

9.5.1 Functional cybersecurity testing

+300 pages of application knowledge about vehicle security according to UN Regulation No. 155, ISO/SAE 21434 & beyond
1000
THINGS WORTH KNOWING IN
AUTOMOTIVE
CYBERSECURITY
The Essential Guide to ISO/SAE 21434
SECOND EDITION
CYEQT
KNOWLEDGE BASE

CYEQT

KNOWLEDGE BASE