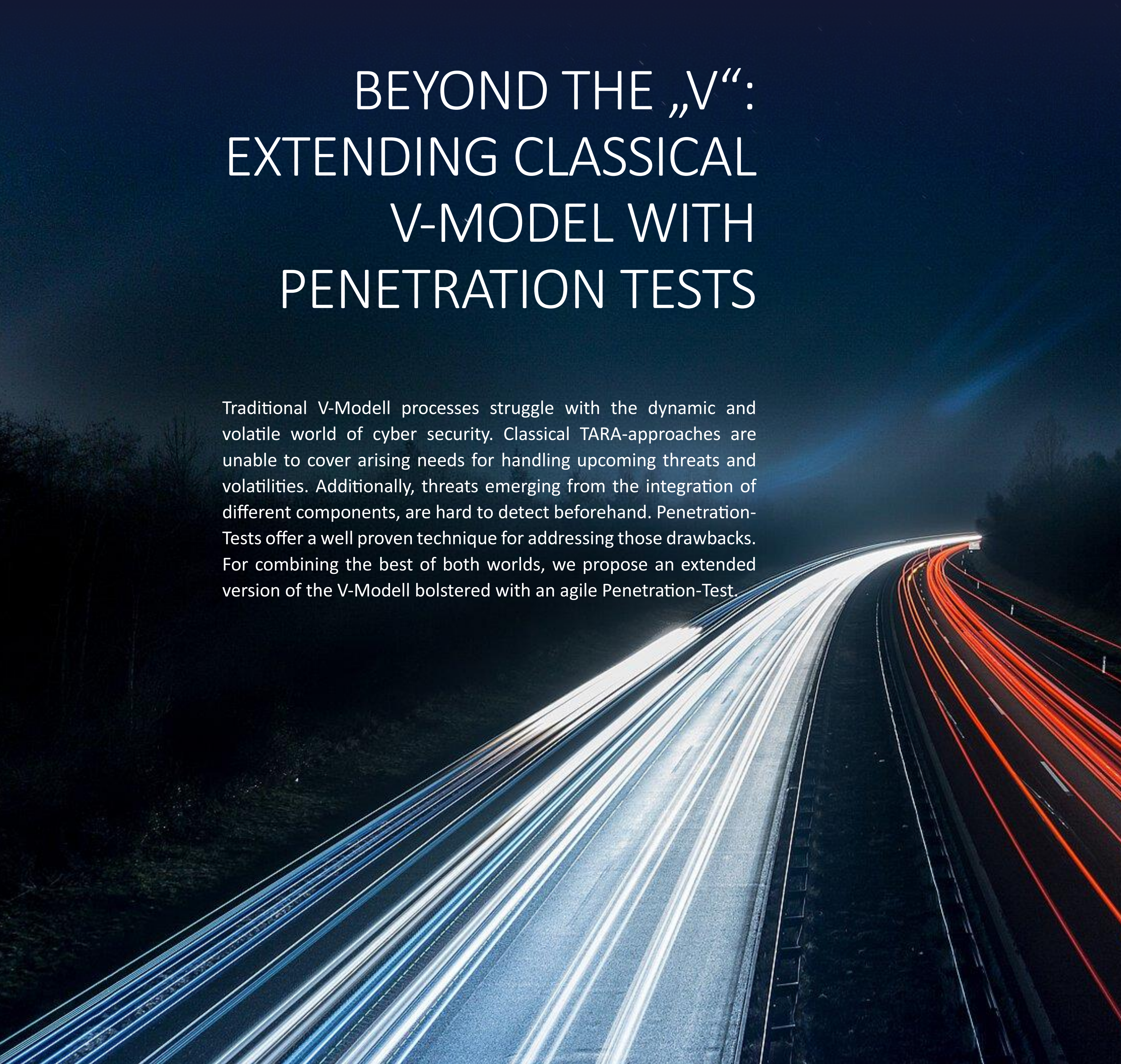
INCYDE

BEYOND THE „V“: EXTENDING CLASSICAL V-MODEL WITH PENETRATION TESTS

Traditional V-Modell processes struggle with the dynamic and volatile world of cyber security. Classical TARA-approaches are unable to cover arising needs for handling upcoming threats and volatilities. Additionally, threats emerging from the integration of different components, are hard to detect beforehand. Penetration-Tests offer a well proven technique for addressing those drawbacks. For combining the best of both worlds, we propose an extended version of the V-Modell bolstered with an agile Penetration-Test.



About the authors

INCYDE

As experts in IT/OT we support you through the end-to-end project process and apply security-by-design within the operation life cycle. Analyzing your system's maturity, verifying IT/OT security concepts, and performing risk assessments as well as KRITIS audits. Moreover, we develop and specify future security standards, manage the security project as well es set the IT/OT security strategy.

Huawei is making strides in the automotive industry through innovative technology, particularly in smart vehicle solutions. Its emphasis on connectivity, autonomy, and electrification signals a promising direction for the future of transportation.

HUAWEI

AVL

With over 75 years of automotive innovation, AVL offers a comprehensive engineering portfolio and advanced software tools for automotive security. Trusted by OEMs, Tier 1 suppliers, and engineering firms worldwide, AVL is leading the way in shaping the future of secure mobility.

We have been developing pioneering digital software solutions together with our customers and partners since 2003. Artificial intelligence, deep learning, natural language processing, the Internet of Things, autonomous mobility, digitalized processes, revolutionary products.

itemis

Special Thanks for Collaboration and In-Depth Discussion

Bundesamt
für Sicherheit in der
Informationstechnik

The Federal Office for Information Security (BSI) is a German federal authority within the portfolio of the Federal Ministry of the Interior and Home Affairs based in Bonn, which is responsible for IT security issues.

DEKRA is one of the world's leading expert organizations. Around 44,000 employees work in more than 50 countries on all five continents. On the road, at work and at home - DEKRA's experienced experts create greater safety in all key areas of life.

DEKRA

Also, special thanks for discussions and feedback to Ms. Samaras-Frühwirt and her team from Mercedes Benz Tech Innovation GmbH, Team Automotive Cyber Security.

Release: 21. Mai 2024 Version 1.0

CONTENTS

1. Introduction

The proliferation of connected vehicles has ushered in a new era of mobility and convenience. However, it has also introduced new challenges in the form of cybersecurity threats. An important step to address these threats has been taken by introducing UNECE Regulation 155 making a Cyber Security Management System (CSMS) mandatory for type approval. The defined requirements can be addressed by following ISO/SAE 21434 "Road Vehicles – Cybersecurity Engineering". This is the only international standard by now, that was developed to provide a systematic approach to automotive cybersecurity management systems. It is specifically tailored to the complex and safety-critical nature of vehicles on the road.

ISO/SAE 21434 encompasses a range of guidelines, processes, and best practices, aiming to ensure that automotive systems are designed, developed, and maintained with security at their core. It introduces a structured methodology for assessing, managing, and mitigating cybersecurity risks associated with road vehicles. The standard emphasizes a lifecycle approach, recognizing that cybersecurity is not a one-time effort but a continuous process that evolves alongside technological advancements and emerging threats.

The ISO/SAE 21434 V-model is a framework used for managing cybersecurity in road vehicles. It spans the entire vehicle development lifecycle, including requirements, specification, design, implementation, verification, production, operation, and end-of-life phases. One of the fundamental principles of ISO/SAE 21434 is that cybersecurity must be considered at all stages. This structured approach ensures that cybersecurity is integrated into every aspect of a vehicle's development, safeguarding it against potential cyber threats throughout its life cycle.

A Threat Analysis and Risk Assessment (TARA) is performed during the early stages of the V-model before detailed component lists are available. It involves identifying potential threats and vulnerabilities to the vehicle's cybersecurity. By systematically assessing risks and defining cybersecurity requirements, TARA informs the subsequent stages of development, ensuring that security considerations are integrated into the vehicle's design and implementation. Current executions of TARAs are prone to lack collaboration, standardization and do not factor into account the dynamic nature of threats. Assumptions are an integral part of the threat assessment process and bear the risk of incorrect security measures if not regularly validated.

Penetration testing usually takes place during the verification and validation phase, focusing on evaluating the effectiveness of implemented cybersecurity measures. Penetration testers simulate real-world attacks to identify vulnerabilities and weaknesses in the vehicle's security controls. This hands-on testing helps to ensure that the implemented security features can withstand actual threats and attacks. They also make threats and risks claimed by the TARA more tangible, since they are based on realized attacks. However, they do not confirm the absence of vulnerabilities.

In this whitepaper, we propose to add additional security assessments and penetration tests which should be conducted early in the V-model, during the pre-TARA or TARA phase. In our opinion, penetration testing, by all stakeholders, as a proactive measure, should play a significant role in the pre-TARA phase. It acts as a precursor to TARA by actively identifying vulnerabilities and weaknesses in the system or parts of it, before the complete threat landscape is understood. This proactive approach ensures that potential risks are uncovered early in the development process, allowing for timely mitigation, and strengthening the overall cybersecurity posture of the vehicle. We discuss the different viewpoints of regulation, Original Equipment Manufacturers (OEMs), and suppliers and highlight the different scopes of testing performed by each stakeholder.

With this approach, automotive manufacturers can gain valuable insights into their systems' security, facilitating informed decisions about security controls, design modifications, and risk management strategies. The synergy between penetration testing and TARA is a proactive step toward securing the next generation of connected vehicles.

The need for strong security measures in the ever-evolving field of automotive technology is emphasized in this whitepaper. With the increasing evolution of vehicles towards connectivity, autonomy, and electrification, there is a rising need for comprehensive security throughout the automotive development lifecycle. The study examines how penetration testing, when informed by TARA principles, may revolutionize end-to-end security while adhering to ISO 21434 and UNECE Regulation 155 standards. Penetration testing is becoming an essential tactic to proactively detect, evaluate, and mitigate security risks as the automotive sector moves from traditional structures to software-driven platforms. The section showcases the advantages of integrating penetration testing approaches throughout the automotive development lifecycle and its role in building a strong security framework.

2. Requirements for a Secure Development Process

The multifaceted nature of ISO/SAE 21434 introduces complex requirements. From federal authorities responsible for type approval to OEMs, suppliers, security professionals, and tool providers, a comprehensive approach to cybersecurity is vital for ensuring the safety and integrity of modern road vehicles in the face of evolving cyber threats. Collaboration, innovation, and commitment to these complex standards are essential for the success of the automotive industry in this ever-evolving landscape. End-users benefit from increased security and trust in their day-to-day vehicle operation. In the following, we discuss the different requirements of these stakeholders.

Regulators

Regulators take a security-focused approach defined by UNECE R 155, which may be implemented by ISO/SAE 21434. They evaluate financial, legal, market, and reputational aspects related to implementing cybersecurity in the automotive sector. Regulators understand the importance of investing in security to mitigate development risks and enhance market competitiveness. Compliance with data protection and cybersecurity regulations is enforced to maintain trust and reputation This approach empowers stakeholders to make informed decisions about ISO/SAE 21434 compliance, balancing costs, and benefits in an ever-evolving security landscape.

OEMs

For OEMs, ISO/SAE 21434 brings the challenge of seamlessly integrating cybersecurity measures into the vehicle development process. They must consider not only safety and performance but also the intricate details of securing vehicle components and systems. This approach requires a shift in traditional development processes and closer collaboration with suppliers. OEMs also assess the long-term financial implications, recognizing that upfront security investments can reduce the total cost of ownership. Legal and long-standing contractual obligations may put OEMs in a difficult spot to execute ad-hoc penetration tests. Changing supplier contracts often incorporates difficult negotiations.

Suppliers

Suppliers in the automotive industry are tasked with meeting the cybersecurity demands set by OEMs in accordance with ISO/SAE 21434. This requires a substantial enhancement of security measures and product adaptation to fit within the secure ecosystem of the vehicle. Close collaboration with OEMs becomes pivotal to satisfy the complex requirements and ensure that the supplied components align with the heightened cybersecurity standards. By addressing these demands, suppliers contribute to the overall security of vehicles and help maintain the industry's competitive edge in the face of evolving cybersecurity threats.

3. Background Information about Penetration Testing

This section will describe the requirements and basis of penetration testing for vehicles as part of the pre-TARA assessment. A penetration test, often referred to as "ethical hacking", is conducted to identify vulnerabilities and weaknesses in vehicle systems and connected networks and backends. To ensure a successful penetration test, several key requirements and best practices should be in place, which will be outlined in this section.

A key problem inherent in all penetration tests is the complex problem of assessing the quality of the executed tests, which will be discussed in Section 5 of this whitepaper.

3.1 Cyber Security Threats against Vehicles

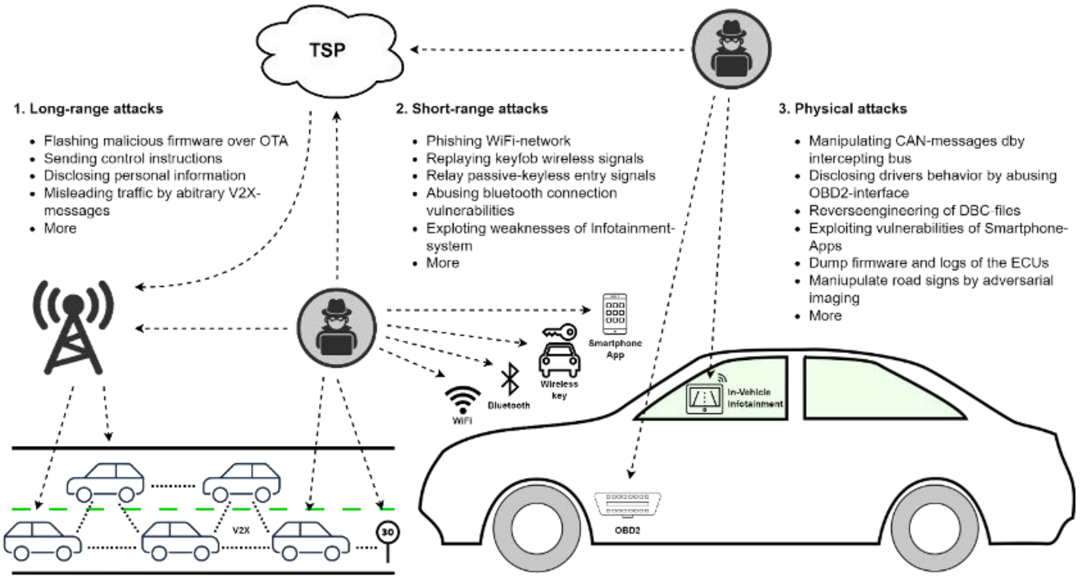

TSP
1. Long-range attacks
• Flashing malicious firmware over OTA
• Sending control instructions
• Disclosing personal information
• Misleading traffic by abitrary V2X-messages
• More
2. Short-range attacks
• Phishing WiFi-network
• Replaying keyfob wireless signals
• Relay passive-keyless entry signals
• Abusing bluetooth connection vulnerabilities
• Exploting weaknesses of Infotainment-system
• More
3. Physical attacks
• Manipulating CAN-messages dby intercepting bus
• Disclosing drivers behavior by abusing OBD2-interface
• Reverseengineering of DBC-files
• Exploiting vulnerabilities of Smartphone-Apps
• Dump firmware and logs of the ECUs
• Maniupulate road signs by adversarial imaging
• More
Smartphone App
Wireless key
Bluetooth
WiFi
In-Vehicle Infotainment
OBD2
V2X
30

Figure 1: Overview of attack vectors and possible threads of a vehicle.

In the digital age, vehicles have evolved into complex networks of software and hardware, offering enhanced safety and convenience. However, this connectivity also introduces significant cybersecurity threats (see Figure 1):

- Remote hacking is of paramount concern since successful attacks can have large-scale effects. Cybercriminals can exploit software or communication vulnerabilities to access a vehicle's systems, potentially controlling critical functions like braking and steering, jeopardizing safety. With internet access, V2X communication, and new wireless interfaces, the attack surface is expected to grow. Fleet management as utilized by major OEMs today also widens the threat landscape.

- Over-the-Air (OTA) updates, which have a security baseline with the introduction of UNECE Regulation 156, can be manipulated by attackers to inject malicious code into a vehicle's software, compromising its security and safety.
- Data Privacy is a major concern in modern vehicles. They gather vast amounts of data, including location and personal information, which can be intercepted or stolen, raising privacy and security risks.
- Supply chain attacks, targeting component and software suppliers, can compromise vehicles through compromised parts, making detection and mitigation challenging.
- Denial of Service (DoS) attacks can disrupt essential systems, rendering them temporarily inoperable, posing safety risks. Inadequate security protocols, especially in legacy systems, leave vehicles vulnerable to known exploits and vulnerabilities.
- Human error and social engineering are often underestimated threats, with drivers or personnel inadvertently disclosing sensitive information or falling victim to phishing attacks. This might also open the possibility for ransomware attacks on vehicles.

This non-exhaustive list of threats showcases that all components of a modern vehicle are prone to attacks. Real world attacks often combine multiple threats, hence a clear distinction is difficult (also refer to Annex 5 of UNECE-R 155). Physical attacks on CAN (Controller Area Network) interfaces, used for ECU (Electronic Control Uni) communication have been realized multiple times. They partly rely on DBC (CAN Database) files which need to be reverse engineered before successful attacks.

To mitigate these threats, the automotive industry must enhance cybersecurity measures, conduct regular security assessments, and invest in research and development. A collective effort is essential to maintain the safety and security of connected vehicles, while it is rather hard to persuade the consumer "behaving secure" or supporting security measures. If threats are successfully executed against vehicles, it has already been demonstrated that unauthorized access to vehicle data leads to privacy breaches and theft of intellectual property and further enables various (cyber-)crimes. Therefore, the main responsibility and load for securing a vehicle (and all supportive digital infrastructure) should be at OEM side.

3.2 Penetration Test Planning and Execution

The process how a penetration test is planned, scoped and critical and interesting components are identified is visualized in Figure 2.

In the realm of vehicle security testing, it is essential to begin by setting clear objectives, which include identifying vulnerabilities, evaluating security measures, and assessing overall vehicle security. Next, prioritize specific vehicle systems for testing, considering factors like their criticality and potential impact on vehicle safety. Finally, establish measurable success criteria, such as identifying and mitigating critical vulnerabilities or demonstrating the ability to compromise specific vehicle functions or access levels within the vehicle's electronic systems.

In the context of vehicle penetration testing, it is imperative that the scope of the test is clearly defined, distinguishing what is within its scope and what is excluded, thereby averting misunderstandings, and ensuring focused efforts by the testing team on critical areas. Certain systems or data may be excluded due to legal or operational constraints. Additionally, technical and environmental constraints that demand awareness by testers should be specified; for example, testing may be confined to pre-production hardware or software without the full set of functionalities. Furthermore, due consideration should be given to regulatory and compliance requirements that could impact the scope, ensuring alignment with industry-specific standards and regulations like ISO/SAE 21434, GDPR, or the EU Cybersecurity Act.

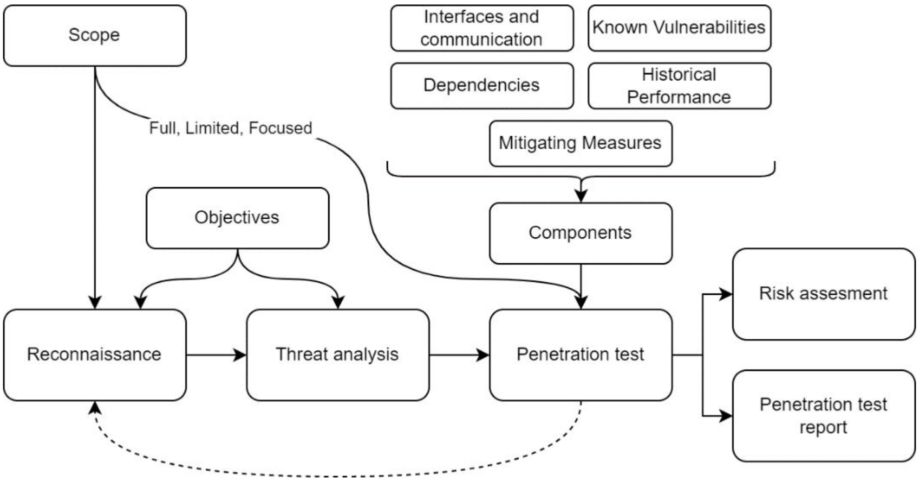


Figure 2: Penetration test planning and scope defining process.

To solve the critical part of scope definition, a quick and inexpensive process is required. Even though the operational environment may not be fully defined yet, components and information about supplier parts are readily available most of the time. To quickly create a list of components for pre-TARA penetration testing various factors that contribute to the overall system functionality and security need to be considered:

- Interfaces and communication systems used are one of the main denominators for scope definition and criticality. External interfaces, such as those connecting to the internet or third-party systems, may introduce additional vulnerabilities that could be exploited by attackers. In contrast, internal interfaces within a controlled network environment, most of the time, have a reduced attack surface (see Section 6).
- Dependencies refer to the interconnections between different components or systems, where the functionality or performance of one relies on the proper operation of another. Understanding and managing dependencies is vital for assessing the potential impact of disruptions. Assets with connections to highly critical systems inherit a higher inherent risk.
- Known Vulnerabilities refer to known weaknesses or flaws that could be exploited by attackers to compromise security. Identifying vulnerabilities is crucial to decide whether an asset should be penetration test and often involves reviewing regular assessments, patches, and security updates that mitigate potential risks.
- Historical performance involves analyzing its past incidents, outages, and security breaches to gauge its reliability and resilience. This retrospective examination provides valuable insights into the component's track record and informs decision-making regarding its ongoing management and potential attacks.
- Mitigating measures involve the implementation of proactive strategies and safeguards to reduce the impact or likelihood of potential threats or vulnerabilities. These measures may include the deployment of firewalls, encryption protocols, regular software updates, trust frameworks, and disaster recovery plans, collectively aimed at fortifying the asset against

risks and ensuring prompt response in the event of a security incident.

The development of a comprehensive test plan is essential, encompassing critical elements such as objectives, scope, methodologies, testing techniques, and timelines. This document serves as a roadmap for the testing team and offers a clear understanding of the tasks to be undertaken. Furthermore, obtaining buy-in (i.e., rules of engagement) from relevant stakeholders within the organization, including senior management, IT, and engineering, is crucial. Their approval should be actively sought, ensuring that the purpose and scope of the test are well understood by all. It is important to manage the expectations of each of the involved parties to allow for a focused approach to the TARA assessment that will be conducted later.

While it is crucial to define clear objectives and scope, it is equally important to remain flexible to be able to include changes to the scope and the criticality of assets. Cybersecurity threats evolve, and new vulnerabilities may emerge unexpectedly. Preparedness to adjust the scope, if necessary, to address emerging risks should be maintained.

Suppliers can significantly support OEMs in the automotive industry by offering penetration testing services for components used in car manufacturing. These services provide a crucial layer of cybersecurity assessment and assurance throughout the supply chain. Suppliers often possess specialized expertise in cybersecurity, allowing them to conduct comprehensive and customized penetration testing of components. This testing encompasses the identification of vulnerabilities, evaluation of attack vectors, and assessment of the component's resilience against cyber threats. This information is a valuable input for the OEM conducting a TARA as they can be used to identify attack graphs and damage scenarios.

To assess risks of known threats, the Common Vulnerability Scoring System (CVSS) serves as a globally adopted standard. CVSS primarily concentrates on assessing the severity of vulnerabilities within software systems and networks. Its metrics, including base, temporal, and environmental components, allow for the quantification of characteristics such as exploitability, impact, and ease of remediation for identified vulnerabilities. CVSS is widely applicable across various industries and is commonly employed in incident response to prioritize and address vulnerabilities based on their severity and potential impact. The release of CVSS 4.0 has made safety assessments an integral part of the CVSS scoring system and makes an adoption for automotive industries more tangible.

ISO/SAE 21434 introduces the concept of security levels, categorizing the cybersecurity requirements of connected vehicles based on their criticality and potential impact. One key difference lies in the scope and context of its application. While CVSS is versatile and broadly applicable, focusing on vulnerabilities in software and networks, ISO/SAE 21434 is tailored for the automotive industry, ensuring that cybersecurity risks associated with connected vehicles are effectively managed throughout the product development lifecycle.

For the evaluation of the penetration test, a score based on the attack feasibility of each attack path (according to ISO 18045) should be determined. In addition, the impact of a successful attack across the four dimensions: Safety, Financial, Operational, and Privacy (according to ISO/SAE 21434) needs to be evaluated. Finally, the risk level based on the risk rating matrix can be obtained as defined in a simple scoring mechanism included in ISO/ISA 21434.

3.3 Scoping of Penetration Tests

In the pursuit of building resilient and secure automotive systems, the strategic deployment of penetration testing across distinct phases of development is paramount. This section explores the dynamic evolution of penetration testing scopes, adapting to the changing landscape of automotive development. Beginning with early-stage component testing, the focus is on scrutinizing individual elements to establish a robust foundation. As development progresses, the scope broadens to system integration testing, evaluating the security implications of interconnected components. Finally, in the late stages, penetration testing extends into the operational environment, simulating real-world conditions to ensure comprehensive security assurance throughout the vehicle's lifecycle and recursively improve pre-TARA assumptions for future tests. By implementing this, knowledge of the professional penetration testers can be utilized more precisely as all components are tested by separate teams.

Early-Stage Component Testing

In the nascent stages of automotive development, penetration testing takes on a targeted approach, zeroing in on individual components and subsystems. This early-stage testing delves into the foundational elements of the vehicle's software and hardware, scrutinizing components for potential vulnerabilities. By adopting this focused strategy, security experts can identify and rectify issues at the grassroots level, ensuring that each building block of the automotive system is fortified against potential threats. Early-stage penetration testing, with an emphasis on component testing, lays the groundwork for a resilient and secure foundation upon which subsequent development phases can build.

Intermediate System Integration Testing

As the development progresses and various components converge to form a cohesive system, penetration testing expands its scope to encompass system integration. This phase involves testing the interactions and interfaces between different components to identify vulnerabilities that may arise from their integration. Security assessments at this stage simulate real-world scenarios, providing insights into how potential threats may exploit the interconnected nature of automotive systems. By adopting an intermediate focus on system integration, penetration testing ensures that the amalgamation of components does not introduce security weaknesses, and the system functions securely as a unified whole.

Late-Stage Operational Environment Testing

In the latter stages of automotive development, penetration testing extends its reach to the operational environment defined during the development process. This comprehensive testing phase simulates real-world conditions, mimicking the operational scenarios the vehicle is expected to encounter. Testing in this environment allows security experts to evaluate not only the security of individual components and their integration but also the resilience of the entire system under realistic conditions. By executing penetration testing in the operational environment, organizations can identify and mitigate potential threats specific to the vehicle's intended use, providing a robust layer of security assurance for end-users.

Continuous Testing in Post-Deployment

The cybersecurity landscape is dynamic, and threats evolve over time. To address this reality, penetration testing should not be viewed as a one-time event but as an ongoing process. Continuous testing post-deployment allows for the identification of emerging threats, the validation of security measures, and the application of updates and patches as needed. By adopting a proactive and iterative approach to penetration testing, automotive systems can adapt to the evolving threat landscape, maintaining a high level of security throughout their operational life.

4. Concept of Pre-TARA Penetration Testing

Using penetration tests from the pre-TARA phase as foundational input for a TARA in the automotive industry offers a multitude of advantages. Perhaps the most compelling of these is the early identification of vulnerabilities. Penetration testing actively detects vulnerabilities in automotive systems prior to integration, enabling a proactive approach to risk management. By doing so, it allows for the mitigation of potential threats at the crucial design and development stages, substantially reducing the likelihood of encountering security issues in the final product. Moreover, the results of penetration testing offer a real-world simulation of attack scenarios, providing practical insights into potential risks that may not be apparent through theoretical assessments. This realism ensures that the TARA process is grounded in verified data, which is instrumental for evidence-based risk analysis. Also, penetration tests tend to identify previously unknown weaknesses, hence including them early in the development lifecycle eases the mitigation throughout the development. In the context of TARA, this evidence facilitates more informed decision-making regarding the implementation of security controls and strategies for risk mitigation. Penetration testing results also enable the prioritization of identified risks based on their likelihood and potential impact, a crucial aspect of risk management. This ensures that resources are allocated effectively to address the most critical vulnerabilities. Furthermore, addressing security issues early, as indicated by penetration testing, is often more cost-effective than dealing with them post-deployment. TARA leverages these findings to make cost-effective decisions for mitigating risks, optimizing resource allocation. The utilization of penetration testing results also aligns TARA with industry standards and regulations, such as ISO/SAE 21434, ensuring that the analysis meets compliance obligations. It also supports a culture of continuous improvement in cybersecurity by applying lessons learned from testing to enhance security controls and practices over time. Ultimately, this approach builds trust and confidence in the safety and security of automotive systems among stakeholders, including regulators, consumers, and partners. It demonstrates transparency and a commitment to cybersecurity, fostering faith in the products and the manufacturer's dedication to safeguarding the integrity of connected vehicles.

In Figure 3 the general concept of the development-cycle penetration testing is shown.

Initially, the OEM, supported by security professionals, defines the critical assets of the product and the dependencies between them (see Section 4.1). During the supplier-phase a supplier develops a product, which will be evaluated by a TARA and verified with further penetration test (see Section 4.2). The results of this evaluation will be considered for the requirements and objectives of the OEM. In the pre-TARA-phase (see Section 4.3) all insights gathered from the asset management and the supplier-phase are cumulated and used for focusing the penetration tests. In the TARA-phase (see 4.4) the insights obtained by the penetration-tests are combined with the assets and the information provided by the supplier for adapting and improving implementation guidelines and requirements. The analysis-results and the implementation are passed to the verification-phase (see 4.5) for (optionally) running a last penetration test of the whole integrated system and verifying all requirements of the TARA are met.

In the following sections the phases of the contributed extended TARA-concept are proposed.

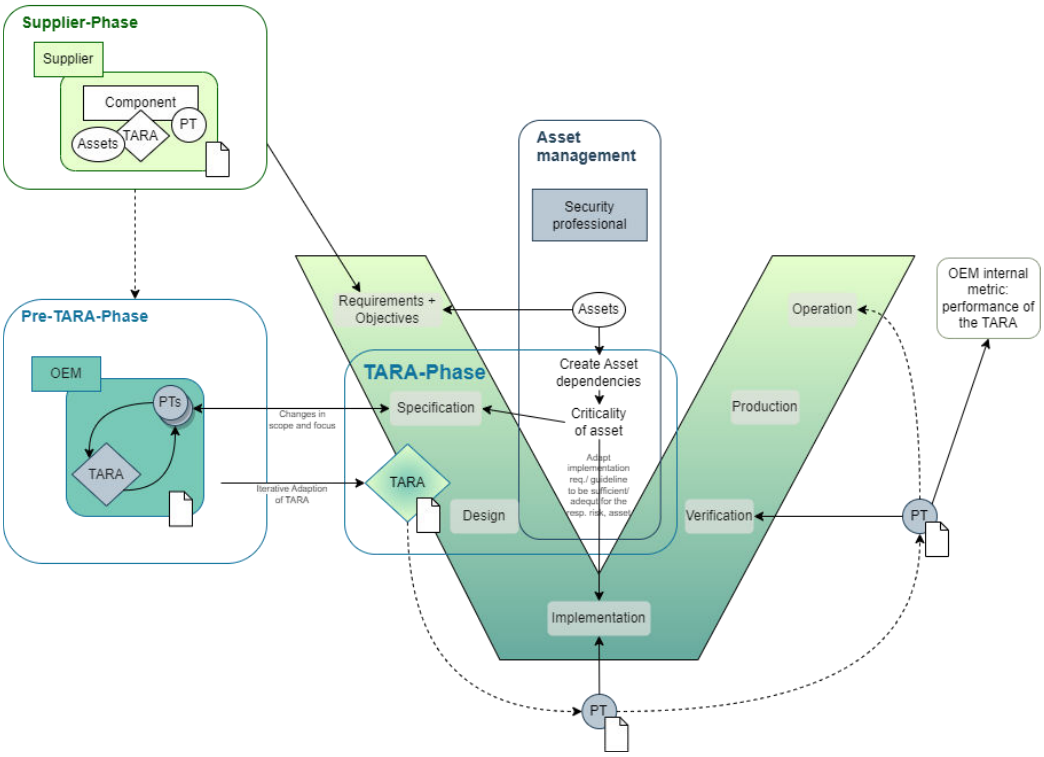

Supplier-Phase
Supplier
Component
PT
TARA
Assets
Asset management
Security professional
OEM internal metric: performance of the TARA
Requirements + Objectives
Assets
Operation
Pre-TARA-Phase
OEM
PTs
TARA-Phase
Create Asset dependencies
Criticality of asset
Specification
Changes in scope and focus
Production
TARA
Iterative Adaption of TARA
Adapt implementation req./ guideline to be sufficient/ adequt for the resp. risk, asset
TARA
Design
Verification
PT
Implementation
PT

Figure 3: Concept of agile penetration test during the development cycle.

4.1 The Asset Management

Asset management within our security framework is overseen by security experts and the OEM, ensuring comprehensive coverage of both security and functionally relevant assets. The primary objective is to systematically identify assets and maintain their organization in an updated and well-structured manner.

In adherence to the initial V-Model, the asset identification process aligns with the first stage of defining requirements and objectives. However, this approach may pose the risk of overlooking crucial or emerging assets, consequently omitting them from consideration in the TARA phase.

Recognizing the interconnected nature of assets, their dependencies serve as a basis for deriving attack paths, pinpointing core or exposed assets, and assigning a criticality rating to each. This criticality assessment becomes the cornerstone for crafting specifications and delineating the scope of Penetration Tests in the pre-TARA phase, a concept to be explored further in Section 4.3.
A granular understanding of assets is achieved through identification stages encompassing the supplier phase, pre-TARA activities, and the TARA phase itself. This comprehensive approach ensures that assets are not only identified but also appropriately classified, laying the groundwork for robust security measures throughout our operational landscape.

4.2 The Supplier-Phase

The supplier-phase represents a comprehensive and self-contained stage conducted exclusively by the supplier. This pivotal phase encompasses all essential tasks preceding any involvement of the OEM. It involves not only the development of the proposed component but also simultaneous activities such as evaluation, penetration testing, and risk management. Crucially, this phase operates independently of the OEM's processes but is strategically positioned to conclude prior to the commencement of the OEM's development phase. Ideally, processes are aligned with OEMs to accelerate the development.

All pertinent information, including assets, risks, and technical specifications, is meticulously compiled during the supplier phase. This data serves as the foundation for two crucial initiatives: the initiation of asset management and the pre-TARA phase. Specifically, this information is instrumental in delineating the parameters for penetration tests.

The OEM plays an active role in motivating and supporting the supplier to undertake a comprehensive TARA analysis. The OEM should encourage the suppliers to create component TARAs and penetration tests that can be used throughout the OEMs own risk assessment. A cybersecurity interface agreement (CIA) could be utilized to define responsibilities between the involved parties. Emphasis is placed on ensuring that these penetration tests and security analyses adhere to universally applicable guidelines, ensuring comparability and interoperability.

To optimize the advantages of collaborative efforts, it is recommended that TARA information be shared among stakeholders throughout various stages. One possible solution for this purpose is the usage of the openXSAM format. XSAM, an acronym for eXchanging Security Analysis Models, constitutes an open format and data model designed for the exchange of risk-related information within the automotive industry. Based on XML file format, XSAM facilitates the representation of TARA information in a structured data format. The format is already used in the industry. XSAM is structured into four modules: Item Definition, Security Risk Analysis, Catalogue and Method Configuration and allows to easily design dependencies between those modules.

4.3 The Pre-TARA-Phase

The initiation of the pre-TARA phase is orchestrated by the OEM after the identification of the initial iteration of assets. The execution of penetration tests and the subsequent formulation or adjustment of the TARA is undertaken by seasoned security experts.

Within the pre-TARA phase, penetration tests are systematically conducted across various assets and scopes. The findings derived from these tests play a pivotal role in shaping the TARA. The methodology allows for the possibility of conducting multiple, independent penetration tests tailored to diverse scopes, components, or different assumptions, such as varying attacker capabilities. This approach enhances the robustness of risk estimations within the TARA, rendering them more reliable and empirically validated. It is imperative that these penetration tests comprehensively cover all critical assets as defined by Section 4.1.

There may be a necessity to modify the scope or assets earmarked for testing, potentially requiring a rerun of the penetration tests. Moreover, such adaptations can exert an influence on the assets themselves. This may manifest in the emergence of new, previously overlooked assets, alterations in the criticality rating, or the identification of new attack vectors. Consequently, these changes can lead to a shift in the interdependencies between assets. Efficient cybersecurity strategies entail the identification of unnecessary components within a system, streamlining the attack surface by eliminating non-essential elements. Additionally, components with similar risk profiles enhance the effectiveness of security measures, allowing for a more focused and cohesive defense against potential vulnerabilities.

The comprehensive documentation of all results serves as the bedrock for the subsequent TARA phase. This meticulous documentation captures the intricacies of the testing process, providing a foundational framework for informed decision-making and risk mitigation strategies.

4.4 The TARA-Phase

The TARA-phase is meticulously overseen by the OEM and bolstered by the expertise of security professionals. The outcomes derived from the pre-TARA phase serve as pivotal inputs for the formulation of the product's TARA. This process involves the comprehensive collection and assessment of assets, drawing upon information supplied by vendors, initialization efforts led by the OEM and security experts, and the findings from penetration tests conducted during the pre-TARA phase.

Penetration test results play a crucial role in shaping attack paths and attack surface by identifying vulnerabilities, prioritizing exploits based on severity, mapping potential pathways, detailing successful exploitation techniques, and guiding attackers to adapt their strategies based on the effectiveness of defensive measures.

The insights gathered from the TARA hold significant implications beyond risk assessment. They provide valuable data for the refinement of implementation guidelines and processes. This adaptability ensures that guidelines and processes are tailored to be more fitting and responsive to the dynamically evolving landscape of estimated risks, thereby enhancing overall security measures.

4.5 The Implementation and Verification Phase

In the pursuit of implementing functionally relevant components, guidelines, and processes, particularly those pertaining to security- or safety-critical aspects, play a pivotal role in supporting developers to yield satisfactory outcomes. While many conventional techniques often introduce additional time, personnel, or expertise overhead, our proposed asset-oriented approach offers a tailored solution for refining processes, ensuring their appropriateness for the respective working item or asset.

A judiciously applied supervisory mechanism, such as peer reviews or pair programming, proves especially appropriate for highly critical assets, where meticulous scrutiny is imperative. Conversely, items of lesser significance may not necessitate such rigorous oversight. The choice of the supervision mechanism can be directly informed by the risks identified through the TARA.

This nuanced approach strikes a balance between functionality, security, safety, and the associated overhead, thereby facilitating a harmonized implementation. The ultimate validation of the implemented solution is indispensable, ensuring that the end result aligns seamlessly with all stipulated requirements. This comprehensive process underscores our commitment to delivering outcomes that are not only functionally robust but also adhere to the high standards of security and safety.

4.5.1 TARA as Input for Verification Phase

A conducted TARA can then also be used as input for the penetration test during the verification phase. For example, identified threat scenarios with a high risk can be tested more thoroughly in a penetration test than those with a low risk. If resources for a penetration test are limited, the TARA can be used to define the test scope. This would also share the workload between the stakeholders as specific penetration tests can already be executed by the supplier.

The results of a TARA can be useful in several stages of a penetration test. In an (optional) “planning and preparation phase”, TARA results can be used to define the overall goal of the penetration test, e.g., testing all components and communication interfaces with an associated high-risk threat scenario.

A TARA requires a lot of documents such as specifications which can support in an “information gathering phase”. Depending on the technical depth of the TARA, these documents can be the basis for the discovery of information of the concrete implementation. For example, an Electronic Control Unit (ECU) datasheet can help in the identification of specific information such as used Operating System (OS), libraries etc.

The gathered information is then usually analyzed in an “analyzing information phase” to define the concrete targets for the active intrusion attempts. The results of the TARA can be used to define and prioritize the test targets in the following “active intrusion attempt phase”.

The results of the “final analysis and report generation phase” of a penetration test (as described in figure 2) can then be used to verify whether the TARA has been conducted with realistic assumptions and that the estimated risk values are realistic. A performance metric of the TARA can be derived from the results of the penetration-test. This metric provides insights on how well the initial TARA performs, compared to the iteratively generated one during the pre-TARA-phase and results given by the verification step.

As TARAs yield structured lists of threats usually stemming from an underlying architecture model, identified threats can be concentrated using structural information. This yields a kill chain or an attack path (or tree from multiple part overlapping and part complementary paths) from a certain entry point (as an exposed interface) towards a certain attack target (as critical components). These attack paths can be labelled with certain actions to take when traversing using a formalized rule set. Each attack path then yields a generic description for an attack that can be converted to an executable test case when concretized with details in the implementation phase. This method of test generation has two benefits: a) efficiency, as two CSMS steps converge and b) effectiveness, as specifically the security goals and requirements are tested because this way they derive from the same source as the test cases.

4.5.2 Feedback to TARA and Pre-TARA

As TARA comprehensively assesses a system for threats based on a model, the quality of the latter should also be assessed. This means that underlying (intrinsic) assumptions made during the modeling process must be verified. For instance, a component using a certain communication protocol will mostly be used in way that presumes that the protocol implementation complies with the respective standard(s) or other common requirements and guarantees certain properties or behaviors. This should also be scrutinized using comprehensive test methods assessing particularly these assumptions. If they are not met (i.e., the specifications are violated), the impact on the overall system must be included in the model, reiterating the TARA process.

5. Evaluation and Recommendations

In the following section, we will evaluate the proposed pre-TARA penetration testing methodology against the already existing and well-established classical V-Modell approach. Afterwards, we will give some recommendations for the real-world implementation.

5.1 Advantages stakeholders

In the preliminary phase of the evaluation, we will explain and highlight the benefits for each stakeholder as part of our analysis.

Regulatory Advantages

Requiring penetration tests for car components, UNECE R 155 serves as a strategic advantage for regulatory authorities such as the KBA and BSI. Firstly, it ensures an active and systematic identification of vulnerabilities within components and finished products, aligning with ISO 21434's mandate for a comprehensive cybersecurity framework for automotive systems. The validation of security controls through these tests demonstrates a commitment to upholding the highest industry standards and reinforces the importance of cybersecurity in the design and implementation of automotive components. Fostering penetration tests not only ensures compliance with ISO 21434 but also establishes these organizations as leaders in the promotion of robust cybersecurity practices. It serves as a proactive measure to address potential threats, aligning with the dynamic nature of the automotive cybersecurity landscape. This requirement encourages continuous improvement in security measures and strategies, positioning KBA and BSI at the forefront of emerging cybersecurity challenges. Furthermore, penetration tests provide tangible insights into the security posture of components, enabling these organizations to refine and enhance overall cybersecurity goals for the industry.

OEMs

In the dynamic realm of automotive cybersecurity, OEMs navigate the imperative of fortifying vehicles against advanced threats. Conducting penetration tests prior to TARA presents a spectrum of pivotal advantages for OEMs committed to elevating the cybersecurity resilience of their vehicles.

The value of penetration testing extends to its provision of a practical examination of potential threats. This delivers a tangible understanding of how attackers might exploit vulnerabilities in specific automotive systems. Such real-world insights enrich the subsequent TARA by incorporating dynamics and nuances derived from simulated attacks.

Insights from penetration testing serve as a cornerstone for informed risk prioritization during the TARA process. This ensures that remediation efforts are strategically directed toward addressing the most critical and impactful threats, aligning seamlessly with ISO 21434's risk-based approach to cybersecurity. Conducting penetration tests, in accordance with ISO 21434, not only demonstrates a commitment to industry best practices but also positions OEMs to meet compliance requirements. This adherence to standards contributes to the development of a robust cybersecurity framework, instilling confidence in stakeholders and end-users.

OEMs can leverage the expertise of their suppliers by incorporating penetration testing requirements into procurement contracts. By collaboratively engaging suppliers in joint penetration testing initiatives, OEMs can ensure a holistic evaluation of the entire supply chain, fostering a comprehensive approach to automotive cybersecurity. An advantage that helps reduce the resource requirements during the verification phase of the ISO 21434 development lifecycle.

Suppliers

Executing penetration tests for their components in accordance with ISO 21434 provides suppliers with critical advantages. This proactive measure allows suppliers to identify and rectify vulnerabilities in their products, ensuring a robust cybersecurity stance. If suppliers decide to collaborate, giving practical insights into potential threats and attack scenarios, suppliers contribute to informed risk assessment, enhancing the overall cybersecurity resilience of their automotive components. Moreover, the validation of security controls through penetration testing aligns with ISO 21434's emphasis on a comprehensive and effective cybersecurity framework, positioning suppliers as essential contributors to industry standards and best practices. This approach not only fosters compliance but also establishes suppliers as proactive and reliable partners in the dynamic landscape of automotive cybersecurity.

By conducting penetration tests for components suppliers showcase a practical understanding of potential threats, thereby enriching the TARA-process of OEMs. The insights gained from these tests enable suppliers to contribute to a more comprehensive and informed TARA, ensuring a thorough evaluation of cybersecurity risks and reinforcing the resilience of automotive systems as per ISO 21434 standards. Ultimately, suppliers will gain a unique selling point by assisting OEMs in an end-to-end secure development process.

Security Professionals

Executing penetration tests on components before executing a TARA provides security professionals with several pivotal advantages. Firstly, it allows for the active identification of vulnerabilities within the components they oversee, offering a hands-on approach to understanding potential threats and attack scenarios. This proactive engagement enhances the efficiency of the TARA process, facilitating a more comprehensive evaluation of cybersecurity risks. The validation of security controls through penetration testing reinforces ISO 21434's emphasis on establishing a robust and effective cybersecurity framework for automotive systems. This approach ensures compliance while also fostering a culture of continuous improvement in security measures. This proactive stance is essential in the dynamic and ever-evolving landscape of automotive cybersecurity, ultimately bolstering the overall security posture of the industry.

5.2 Challenges for conducting pre-TARA penetration testing

In the next step we draw up the challenges which might come with the implementation of the proposed methodology. Therefore, we focus on aspects which might accompany the real-world realization.

Collaboration and Dependencies

Within the collaborative landscape of suppliers and OEMs, the inclusion of regulators and security professionals adds an additional layer of complexity and importance. Regulatory compliance and security considerations are paramount in industries where precision and reliability are critical.

Regulatory bodies play a crucial role in shaping the landscape within which suppliers and OEMs operate. Adherence to industry standards and regulations is not only a legal requirement but also fundamental to ensuring the safety, quality, and reliability of products. Collaborative efforts must, therefore, include a proactive engagement with regulatory frameworks, with transparent communication to address compliance issues, and a commitment to upholding the highest standards.

Simultaneously, the involvement of security professionals is vital in safeguarding sensitive information, particularly in the context of Intellectual Property (IP) and proprietary technologies. Establishing robust cybersecurity protocols, secure data-sharing mechanisms, and a shared commitment to protecting against potential threats are integral aspects of a comprehensive collaboration strategy. This proactive approach helps build trust and confidence among all parties involved, fostering a secure and resilient collaborative environment.

The interplay between suppliers, OEMs, regulators, and security professionals underscores the need for a holistic and inclusive approach to collaborative endeavors. By integrating regulatory compliance and security considerations seamlessly into the collaborative framework, a more resilient and adaptive partnership emerges—one that not only meets industry standards but also anticipates and mitigates potential challenges effectively.

In summary, for penetration testing, the collaboration between suppliers and OEMs takes on added significance with the inclusion of regulators and security professionals. Proactive engagement with regulatory frameworks and robust cybersecurity measures are essential components in navigating the complexities of collaboration, ensuring not only legal compliance but also the security and reliability of the collaborative efforts. By addressing regulatory and security considerations with diligence, collaborative partnerships can thrive, delivering enduring value to all stakeholders involved.

Quality Assessment of the Penetration Test

Assessing the quality of penetration tests poses significant challenges rooted in several key aspects of the testing process. The first hurdle lies in the meticulous definition of the test's scope. A poorly articulated scope can lead to incomplete assessments, potentially overlooking critical areas that require scrutiny. Clear and precise delineation is essential to ensure that the penetration test provides a comprehensive evaluation of the organization's security posture.

The second critical factor is the expertise and skill level of the penetration testers. The effectiveness of a penetration test is intricately linked to the capabilities of the individuals conducting it. Disparities in skill levels among testers can result in inconsistent evaluations, as the ability to identify and exploit vulnerabilities may vary. A thorough assessment demands a team of skilled professionals who can navigate complex systems and simulate real-world attack scenarios effectively.

Simulating realistic attack scenarios forms the third challenge. The quality of penetration tests relies heavily on their ability to replicate genuine threats that an organization might face. If the scenarios are not reflective of actual risks, the test may fail to identify vulnerabilities that could be exploited by determined adversaries. Realism in testing scenarios is pivotal for ensuring the relevance and accuracy of the assessment.

The depth of testing, the fourth consideration, involves determining the extent to which testers delve into the system to uncover vulnerabilities. Striking the right balance between a comprehensive evaluation and resource constraints is challenging. Since (penetration) testing employs empirical methods, achieving meaningful test coverage is the most important factor for success.

Quality is further influenced by the clarity and completeness of documentation. The fifth challenge revolves around the adequacy of reports and findings. Incomplete or unclear documentation can hinder a comprehensive understanding of identified vulnerabilities and the subsequent remediation steps. Effective communication of the findings to stakeholders is crucial for driving necessary security improvements and mitigating risks.

Lastly, effective communication is indispensable in conveying the significance of identified vulnerabilities to stakeholders. While technical accuracy is vital, communicating the risk in a clear and understandable manner is equally important. Failure to articulate the implications of vulnerabilities can impede the organization's ability to prioritize and address security concerns effectively. In navigating these challenges, organizations can enhance the overall quality and utility of penetration tests in bolstering their cybersecurity defenses.

6. Example: Risk Analysis of Brake-Control- and Gateway-ECU

In this section, we want to visualize the developed concept of combining an agile penetration-test within a V-Modell process. Therefore, we consider the simplified connection between a safety critical Brake-Control ECU and a Gateway ECU (see *Figure 4*). The ECUs are connected as shown in the image. The use case is oriented on state-of-the-art automotive architecture.

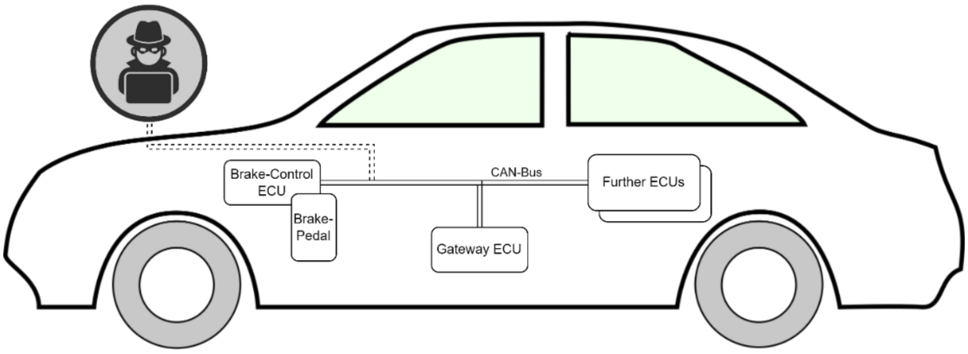


Figure 4: Simplified connections inside a car between different ECUs with possible physical attack vectors.

The *asset management* focuses on the integrated system (resp. the vehicle). The *safety of passengers* is assumed as the primary asset. For preventing an adversary injecting malicious commands, the *integrity and authenticity* are required.

During the *supplier-phase*, the supplier creates a set of assets of the respective component (Brake-Control ECU, Gateway ECU). Based on the asset analysis, the supplier creates a targeted TARA, underpinned with a penetration test. The TARA might contain following aspects:

Assets	Possible Threats	Severity	Feasibility	Risk
Brake-Control ECU				
Message Integrity and Authenticity	Message injection through physical MitM	High: safety critical	High: exposed, accessible without unlocking vehicle	High
Gateway-ECU				
Message Integrity and Authenticity	Message injection through physical MitM	High: safety critical	Low: physical encapsulated	Low - Medium

In the *Pre-TARA-Phase*, the OEM utilizes the knowledge gained from the supplier phase about risks and their estimated impact. It is the goal enabling the OEM to analyze the integrated systems, the impact of sub-systems (resp. ECUs) to each other and the actual impact of risks considered as "acceptable" by the supplier.

An - from supplier-perspective - acceptable risk (e.g. Physical Man-in-the-Middle (MitM) on CAN-bus) might become non-acceptable - from OEM-perspective - by the integration. The penetration test helps to understand and estimate the actual impact.

In the *TARA-Phase* of the regular V-Modell, the findings and resulting risks are considered. The risk of arbitrary CAN-message injection regarding the Gateway ECU is considered "low" resp. "acceptable", since the CAN-bus is not exposed. The Break-Control ECU is assumed to be exposed against attackers and might become target of a physical MitM easily. By this, the feasibility of such an attack for the Gateway ECU increases drastically.

These results can be treated during the *implementation*, while sharpening the assets to be protected. For preventing unauthenticated participation on the CAN-bus, the messages can be cryptographically protected (e.g. with SecOC). By this, any unallowed access by an (MitM-) attacker becomes less feasible, while introducing additional overhead like the need for a key management.

During the *verification phase*, the implementation is evaluated while focused on the findings of the suppliers, the OEM and the identified assets and risks. In this example we have focused on arbitrary message injection. The verification step must check if the cryptographical algorithms are vulnerable (e.g. by side-channel attacks), if the key generation and management is secure against assumed adversaries (e.g. enough entropy, keys stored in secure hardware storages, secure key distribution securely). By clearing possible attack vectors, the risk of unallowed message injection can be reduced.

After all tests are passed, the implementation receives the clearance for *production*.

7. Outlook

The relationship between ISO 21434 and TARA, the practical integration of real-world penetration testing into the planning and implementation phases emerges as a pragmatic next step. In the foreseeable future, the automotive industry can anticipate a more refined and responsive approach to cybersecurity, one that draws upon the tangible insights gained from penetration testing throughout the development lifecycle.

The forthcoming evolution in TARA methodologies is poised to be grounded in the realities uncovered by penetration testing at critical junctures. By incorporating these insights early in the planning phase, organizations can proactively address vulnerabilities, minimizing the risk landscape associated with automotive systems. Furthermore, integrating penetration testing into the implementation phase allows for a continual validation of security measures, aligning the theoretical strengths of TARA with the practical realities uncovered by penetration testing.

This outlook envisions a methodical fusion of ISO 21434 TARA principles with the pragmatic inputs derived from penetration testing. As organizations increasingly recognize the need for a more iterative and adaptive cybersecurity strategy, the refinement of TARA with real-world penetration testing data represents a tangible and actionable way forward. By embracing this approach, the industry can fortify its cybersecurity posture, ensuring that the principles outlined in ISO 21434 are not only met but surpassed in the face of evolving cyber threats.