Deloitte.

Addressing new automotive innovations: Synergies of cybersecurity and diagnostics

October 2024

Abstract

The automotive industry is undergoing a transformative phase characterized by increasing soft- and hardware complexity and functionality. In addition to the desired benefits, the expansion in functionality of Electronic Control Units (ECUs) and High-Performance Computers (HPCs) presents challenges, including a rise in threats and potential harm to road users caused by malicious actors.

In response, OEMs and suppliers must rethink conventional processes and develop new approaches to security solutions. Increasing cooperation between the security and diagnostic departments of OEMs appears as a viable approach, expanding the available information and processes, provided by diagnostic systems, to ensure enhanced cybersecurity while protecting diagnostic data with dedicated cybersecurity mechanisms.

As a concluding outcome of this study, an implementation strategy has been formulated for the collaborative approach. This strategy specifically emphasizes the implementation of diverse use-cases and outlines the optimal timeline for their execution. The use-cases were specifically centered around on-board diagnostic within HPCs relevant to Service-Oriented Vehicle Diagnostics (SOVD) and their seamless integration into the contemporary Cybersecurity Management System (CSMS) environment. The implementation timeline spans from the immediate future to instances requiring dedicated development resources. The formulation of the strategy was guided by an assessment of the described use-cases, and was systematically organized into correlation identification, use-case analysis, and impact evaluation.

The correlation identification focused on interfaces and combinations between security measures and diagnostic processes into potential use-cases. The analysis examined potential use-cases on measurable data, using metrics for network security applications. In the final evaluation, each use-case was systematically rated for feasibility and potential impact on the vehicle's cybersecurity. This iterative process highlighted the significance of dedicated department interfaces, underlining the benefits for the integration of cybersecurity and on-board diagnostic within the automotive domain.

The evaluation revealed a spectrum of use-cases which were transformed into the implementation strategy. The use-cases were sorted from those applicable in the near future to others requiring dedicated development resources. Short-term use-cases rely on existing information, such as freeze frames and Diagnostic Trouble Codes (DTCs). Freeze frames and DTCs' comparison can serve as potent tools for forensic purposes and detection measures. Derived from this information, the respective Threat Analysis and Risk Assessment (TARA) as well as countermeasures can be adjusted. Long-term solutions, requiring more development time, could leverage information from the on-board diagnostic system to enhance Intrusion Detection Systems (IDS) functionality or serve as additional verification measures.

In summary, the formulated strategy functions as a navigational framework tailored for OEMs, offering guidance through the challenges arising from the ongoing transformation phase. It succinctly outlines currently available use-cases and providing a strategic roadmap for the future vehicle developments, encompassing the inclusion of potential use-cases.

Contents

Table of tables

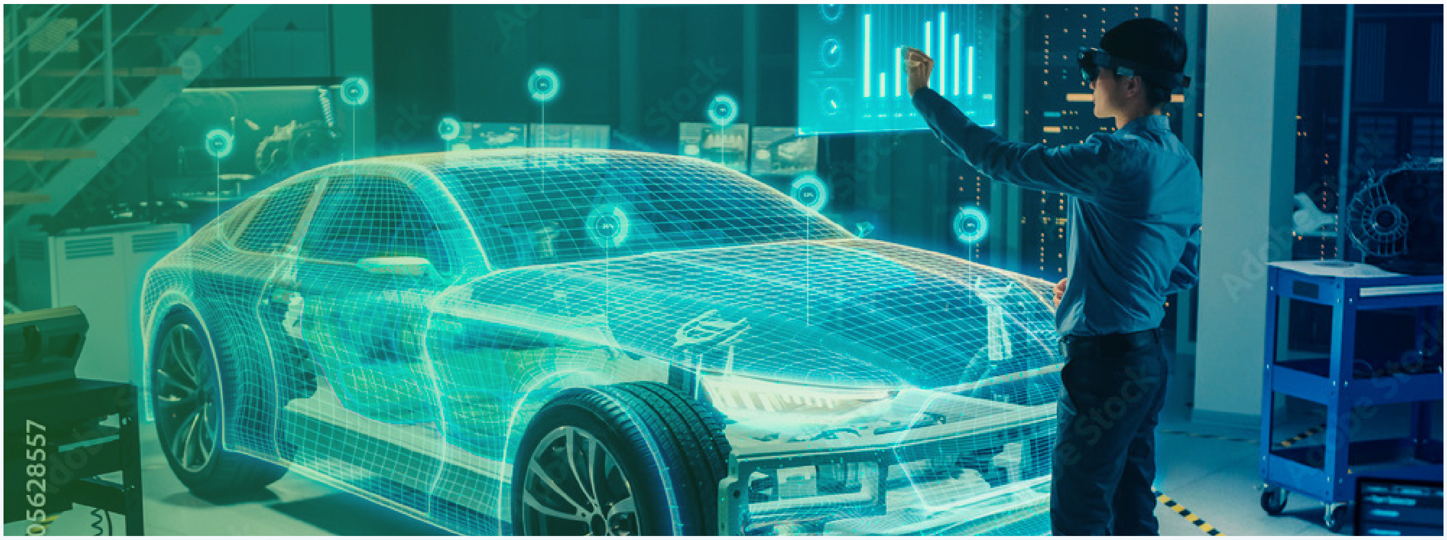
Table of figures

List of abbreviations

AI	Artificial Intelligence
ASAM	Association for Standardization of Automation and Measuring Systems
CSMS	Cybersecurity Management System
DTC	Diagnostic Trouble Code
ECU	Electronic Control Unit
GPS	Global Positioning System
HPC	High Performance Computer
IDS	Intrusion Detection System
ISO	International Organization for Standardization
OEM	Original Equipment Manufacturer
OTA	Over-the-Air
SAE	Society of Automotive Engineers
SOVD	Service-Oriented Vehicle Diagnostics
TARA	Threat Analysis and Risk Assessment

1 Introduction

As a result of current market developments, in which vehicles are increasingly networked and dependent on software-controlled functionalities, the assurance of cybersecurity within vehicles is becoming increasingly important.



The evolving threat landscape represents significant challenges.[1] This development requires proactive measures to strengthen the diagnostic capabilities of vehicles and to protect against possible misuse.
The complexity of both software and hardware is rapidly growing in the automotive industry, which is undergoing a significant transition from conventional ECUs to HPCs. This change has prompted the development of the ASAM SOVD standard, which was published in 2022.[2]
It acknowledges that "there are different aspects that are not covered by the SOVD standard, as they are specific to the implementation of a SOVD server".[2] Moreover, the standard provides examples of these uncovered aspects.

- "Prevention and quick reaction to attack(s) (...)
- Recognition of security incidents
- Maintaining the operational safety (...)
- Management of security incidents
- Load balancing of concurrent requests"[2]

Focusing on cybersecurity implementations to support the SOVD functionalities, the primary functions of "prevention and quick reaction to attacks" and "recognition of security incidents" form the cornerstone for "maintaining the operational safety (...)" and "management of security incidents".[2]

This study aims to assess potential implementations for these functions by conducting a comprehensive analysis and evaluation of various approaches.
This assessment begins by outlining the identification phase, which emphasizes re-using existing on-board diagnosis functions or creating new approaches to enhance vehicle cybersecurity capabilities. Furthermore, the analysis phase delves into the measurable data and insights gleaned from comparable scenarios in network security applications. The evaluation phase synthesizes the findings from the analysis, highlighting the strengths and limitations of each approach.

2 Assessment

2.1 Identification

The identification centered around ways to implement measures directly within the vehicle to fortify its diagnostic capabilities against potential misuse. To achieve this goal, leveraging existing on-board diagnostic functions proves essential. These functions should be used to create additional vehicle cybersecurity capabilities in HPCs, using SOVD. For this, multiple approaches were identified. These are listed in Table 1 and explained in the following chapters.

Measure	Short explanation
DTC analysis	Analyze set DTCs in legacy ECUs to identify potential tampering.
Cross-domain comparison	Compare sensor data across different domains to ensure data reliability.
Application vulnerability monitoring	Enhance software diagnostic capabilities to detect attacks exploiting potential vulnerabilities.
Update white-lists	Implement functions to authenticate updates, ensuring their authenticity.
Location verification	Use vehicle location to verify the legitimacy of diagnostic requests.
AI-based behavior analysis	Utilize adaptive learning algorithms to detect attacks by analyzing communication behavior.

Table 1: Identification - Short description of approaches

2.1.1 DTC analysis

In conventional IT systems, log analysis stands as a method for forensic investigations, aiding in the detection of anomalies or irregularities in server behavior. This involves monitoring various parameters like login attempts, file access, and system activities to flag potential security breaches or unauthorized access. Drawing from this method, a comparable approach can be applied to vehicles by analyzing DTCs and freeze frames.[3]

Traditional vehicle diagnostic and fault finding heavily depend on the accuracy of diagnostic trouble codes and proper enforcement of rules governing when to trigger a DTC. These DTCs will still be used in ECUs, that are connected to the HPC via the classic adapter.

Analyzing set DTCs and their corresponding freeze frames can help identifying issues related to bus communication and ECU availability. Moreover, by checking both the presence and absence of expected DTCs, alongside any existing DTCs, it becomes possible to identify potential tampering with data or signals. This approach holds significant forensic value, particularly in recognizing security incidents.

2.1.2 Cross-domain comparison

In modern IT systems, organizations leverage cross-domain data aggregation to compile security-relevant information from diverse sources like network devices, servers, and applications. This consolidation of data within a central repository empowers security teams to discern correlations and anomalies, thereby flagging potential security threats or attacks. Similarly, a methodology for identifying cyberattacks targeting the vehicle and, ideally, preventing them can be developed, cross-referencing sensor data from different domains.[4]

Verifying the validity of received sensor data is a standard practice in most ECUs. This verification could be extended by gathering security-critical sensor data in a central HPC and cross-referencing it with related data from other sensors, HPCs or domains. Incorporating this functionality could enable early detection of manipulated sensors or ECUs. This early detection would enhance the intrusion detection capability of a vehicle and could enhance its ability to prevent and quickly react to attacks.

2.1.3 Application vulnerability monitoring

To detect and mitigate cyber threats within applications, runtime application self-protection is use as a real-time defense mechanism. It offers monitoring and safeguards for web applications and server-side software, effectively countering prevalent exploit techniques. Through runtime analysis of application behavior, runtime application self-protection identifies and counters malicious actions, including buffer overflows, injection attacks, and other code-level vulnerabilities. This capability holds promise for integration into HPCs for both on-board diagnostic and cybersecurity purposes.[5]

The SOVD standard recognizes that the focus for vehicle diagnostic shifts "from checking hardware to checking the software functionality of applications, which corresponds to a paradigm shift".[2] As a key motivation behind the SOVD standard, the ability to diagnose software also presents an opportunity to enhance vehicle cybersecurity.[2] By implementing mechanisms capable of detecting common exploits vehicles can proactively identify attempts to breach cybersecurity measures. This proactive approach not only aids in preventing subsequent attacks but also enables swift reactions from the vehicle, thereby bolstering its overall security posture.

2.1.4 Update white-lists

File integrity monitoring solutions are used to monitor critical system files and directories for unauthorized changes or modifications. By comparing the hash values of files against known good values stored in a whitelist, FIM can detect and alert administrators to any discrepancies, indicating potential tampering or compromise. Leveraging this method can significantly bolster the resilience of the vehicle's software update process.[6]

Updating the software of an ECU or HPC is a fundamental function of the SOVD standard. To facilitate this process, two http methods, put and post, are designated for this use-case. Ensuring the integrity of these software updates is vital for the safety and reliability of the vehicle. Implementing white-lists based on the hash values of current updates can serve as an additional layer of verification and additionally enable measures for detecting attempts to tamper with the software. By storing the comparison values on an external server with a direct communication channel to the vehicle, the verification process can be streamlined without the need for additional authentication methods on the workshop side. This approach enhances the security and efficiency of software updates within the automotive ecosystem.

2.1.5 Location verification

Comparable to geofencing, location-based access controls empower organizations to manage access to network resources based on the geographical location of IP addresses. By implementing precise access policies, organizations can limit certain actions to approved locations exclusively. This guarantees that activities originate from secure and trusted environments, thereby reducing the likelihood of tampering or unauthorized access. Leveraging this approach for the vehicle software update process involves utilizing the vehicle's location as a validation checkpoint.[7]

Since the implementation and regulation of the eCall emergency system, the installation of GPS and Galileo interfaces has become mandatory in newly manufactured vehicles. These location data can serve as an additional layer of security for the software update process. Leveraging the vehicle's location as a probability indicator can help determine whether the update process is initiated in a safe or validated environment. However, it is essential to implement measures that ensure the reliability of the GPS location for this strategy to be effective. By delaying or rejecting updates based on the location data, vehicles can enhance their resilience against software tampering and detect attempted attacks. This approach strengthens the security posture of vehicles and enhances their overall protection against cyber threats.

2.1.6 AI-based behavior analysis

As an advanced protection measure for IT systems user and entity behavior analytics solutions employ machine learning algorithms to analyze patterns of user and entity behavior across network and server environments. By cross-referencing data from different sources such as logins, file access, network traffic, and system interactions, user and entity behavior analytics tools can detect anomalies in behavior that may signal potential security risks. This proactive approach aids organizations in real-time detection of insider threats, credential misuse, and other suspicious activities, thereby bolstering their overall cybersecurity stance. Looking ahead, leveraging user and entity behavior analytics techniques could offer an effective strategy for identifying and preventing cyber-attacks on vehicles.[8]

With the continual advancement of artificial intelligence (AI) capabilities, its integration into on-board diagnostic and cybersecurity holds significant promise. By leveraging ai to analyze driver and vehicle behavior over time, anomalies can be identified, provided there is a substantial amount of data available. This capability could serve as a detection system for misuse of vehicle functions by detecting sudden or abnormal changes. Such alerts could then be utilized to warn the driver and connected systems accordingly.

2.2 Analysis

The analysis focuses on measurable data, leveraging insights from comparable scenarios in network security applications. It scrutinized six key metrics, which will undergo further evaluation in the subsequent assessment phase. These metrics include the level of preparedness, the time to detect and verification as well as the support in containing and resolving the incident. They are listed and elaborated further in Table 2 for comprehensive understanding.

Metric	Description
Level of preparedness	The extent to which the identified approach enhances readiness against cyberattacks.
Time to detect	The duration required for the approach to detect a potential security incident.
Time to verification	The time taken to verify a detected potential security incident.
Measure supports containment	The duration needed to counter or contain an ongoing attack.
Measure supports mitigation	The time required to fully resolve and mitigate the security incident.

Table 2: Analysis - Metrics with description

2.2.1 DTC analysis

The DTC analysis method does not enhance preparedness against cyberattacks as its primary function is to identify security incidents. The time taken to detect such incidents relies on when DTCs are requested, whether during a workshop visit or over-the-air, depending on the diagnostic functions implemented. Confirming a security incident requires further information and testing, leading to an increase in the time to verification. Given its sole function of recognition, DTC analysis does not contribute to containing or resolving incidents. The result of the analysis is summarized in Table 3.

Metric	Description
Level of preparedness	No impact
Time to detect	Depending on the time the DTCs are requested
Time to verification	Further information and tests needed
Measure supports containment	No impact
Measure supports mitigation	No impact

Table 3: Analysis result – DTC analysis

2.2.2 Cross-domain comparison

By consolidating sensor data from various domains, cross-domain comparison enhances the detection of correlations and anomalies, thereby bolstering preparedness against cyberattacks. Operating as a function or application within the HPC, this approach enables instant detection of anomalies as they arise. However, acknowledging detected anomalies as actual incidents necessitates further investigation and testing. However, the prompt availability of information enables quick containment measures, such as deactivating specific functions or alerting the driver, depending on the targeted function. Based on the attack's nature, mitigation may be possible but necessitates additional information to prevent measures that could exacerbate rather than alleviate the situation for the vehicle. These results are summarized in Table 4.

Metric	Description
Level of preparedness	Early detection of correlations and anomalies
Time to detect	Instant
Time to verification	Further information and tests needed
Measure supports containment	Swift containment measures for specific functions
Measure supports mitigation	Further information needed

Table 4: Analysis result - cross-domain comparison

2.2.3 Application vulnerability monitoring

By integrating mechanisms capable of identifying common exploits, the level of preparedness against cyberattacks is heightened. The efficacy of promptly detecting and addressing attacks is heavily influenced by the availability of information on known attack patterns. This availability significantly affects various metrics, particularly the time to detect, verify, contain, and mitigate incidents. As a function or application within the HPC, this method facilitates immediate detection and acknowledgment of attacks. Moreover, it empowers the system to swiftly contain and ideally mitigate the incident upon its occurrence. Table 5 summarizes these results.

Metric	Description
Level of preparedness	Depending on the available information on known attack patterns
Time to detect	Instant (if attack pattern is known)
Time to verification	Instant (if attack pattern is known)
Measure supports containment	Swift containment (if attack pattern is known)
Measure supports mitigation	Swift mitigation (if attack pattern is known)

Table 5: Analysis result - application vulnerability monitoring

2.2.4 Update white-lists

Securing the update process enhances the level of preparedness against cyberattacks aiming to alter the software of ECUs or HPCs. As a measure to ensure the integrity and validity of the software, this approach enables instant detection and acknowledgment of any attempted tampering. If the validity of the update is not confirmed, the function to alter the software is blocked, thereby containing, and resolving potential attacks. This result is summarized in Table 6.

Metric	Description
Level of preparedness	Enhanced against attacks targeting ECU and HPC software
Time to detect	Instant
Time to verification	Instant
Measure supports containment	Instant containment
Measure supports mitigation	Instant mitigation

Table 6: Analysis result - update white-list

2.2.5 Location verification

Implementing location verification as an additional measure to secure the update process further enhances the preparedness level against cyberattacks targeting the alteration of software in ECUs or HPCs. This method enables the detection of potential attacks on the software by leveraging vehicle location data. The acknowledgment of such potential attacks as real incidents relies on the accuracy and reliability of the allowed location data. If the location cannot be validated, the update process can be temporarily blocked until additional information is obtained, effectively containing the attack, and partially resolving the incident. Table 7 summarizes this result.

Metric	Description
Level of preparedness	Enhanced against attacks targeting ECU and HPC software
Time to detect	Instant
Time to verification	Dependent on accuracy and reliability of the allowed location data
Measure supports containment	Temporarily blocking software update
Measure supports mitigation	Temporarily blocking software update

Table 7: Analysis result – location verification

2.2.6 AI-based behavior analysis

Utilizing an AI-based method, this approach is contingent upon the quality and quantity of data used to train the AI model. With an adequate dataset, this method holds the potential to significantly bolster preparedness levels against a wide array of cyberattacks. Instant detection and acknowledgment of attacks become feasible if the AI model can reliably identify malicious activities. The effectiveness of potential measures to contain and mitigate attacks is also contingent upon the maturity and sophistication of the AI system. Consequently, while this method boasts a high potential for impact, it also demands substantial data and technological prerequisites. The results are summarized in Table 8.

Metric	Description
Level of preparedness	Dependent on the data used to train the AI model
Time to detect	Dependent on the data used to train the AI model
Time to verification	Dependent on the data used to train the AI model
Measure supports containment	Dependent on the data used to train the AI model
Measure supports mitigation	Dependent on the data used to train the AI model

Table 8: Analysis result – AI-based behavior analysis

2.3 Evaluation

In the third phase of the assessment, the evaluation focuses on the anticipated outcomes of each approach. These outcomes are evaluated based on their potential benefits for an OEM's CSMS and risk management, while concurrently bolstering the vehicle's overall cybersecurity posture. The optimal scenario for an approach is one that can effectively detect and promptly verifying cyberattacks, while also providing mechanisms to contain the attack and mitigate its impact. To streamline the evaluation process, four categories of analysis are considered and grouped into two overarching categories. The first category, "detection effectiveness", centers on the detection and verification of a cyberattack, encompassing the metrics "time to detect" and "time to verification". The second category," impact minimization", focuses on containment and mitigation, encompassing the metrics "measure supports containment" and "measure supports mitigation". Each metric is assessed independently, and ratings are assigned based on the analysis findings, ranging from 1 to 10 points. A score of 1 denotes the lowest level of fulfillment, while a score of 10 signifies the highest level of fulfillment. For the final evaluation, the mean is calculated based on the two metrics of each category. The used formula is shown in (1), the evaluation criteria are listed in Table 9.

$$(1) \qquad EvaluationResult_{Category} = \frac{\sum \text{Metric Result}}{\text{(N(Metric)}}$$

Metric	Lowest rating	Highest rating
Time to detect	Can not detect an attack	Can detect attacks instantly
Time to verification	Can not verification an attack	Can verification every attack
Measure supports containment	No containment support	Full containment
Measure supports mitigation	No mitigation support	Full mitigation

Table 9: Evaluation - Criteria

2.3.1 DTC analysis

Due to the varying situations of requesting a DTC analysis, the detection time for an attack may extend over several weeks. This prolonged duration impacts the "time to detect" metric, resulting in a score of only 3 points. Additionally, due to the requirement for further information and testing, the mechanism lacks the ability to promptly verify an incident, earning it a score of 1 point. Further, as a pure forensic tool, the DTC analysis contributes minimally to both the "measure supports containment" and "measure supports mitigation" metrics, garnering 1 point each. The evaluation result is listed in Table 10.

Metric	Evaluated points
Time to detect	3
Time to verification	1
Measure supports containment	1
Measure supports mitigation	1

Table 10: Metric evaluation result - DTC analysis

This evaluation results in only 2 points for the "detection effectiveness" category and 1 point in the "impact minimization" category. The result for each category is depicted in Table 11.

Category	Evaluated points
Detection effectiveness	2
Impact minimization	1

Table 11: Category evaluation result - DTC analysis

2.3.2 Cross-domain comparison

The cross-domain comparison earns 10 points for detection time due to its immediate anomaly detection capability in sensor values. However, it receives only 1 point for the acknowledgment metric due to the requirement for additional information and testing. Containment measures can be swiftly initiated but are contingent upon the affected function, resulting in a decrease to 7 points. While mitigation measures are feasible in some instances, they typically necessitate additional information, warranting 3 points for this metric. This result is summarized in Table 12.

Metric	Evaluated points
Time to detect	10
Time to verification	1
Measure supports containment	7
Measure supports mitigation	3

Table 12: Metric evaluation result - cross-domain comparison

The category result calculation yields 6 points for the "detection effectiveness" category and 5 points for the "impact minimization" category. These results are detailed in Table 13.

Category	Evaluated points
Detection effectiveness	6
Impact minimization	5

Table 13: Category evaluation result - cross-domain comparison

2.3.3 Application vulnerability monitoring

The effectiveness of application vulnerability monitoring is heavily dependent upon the accuracy of identifiable attack patterns. This reliance on data quality diminishes the evaluation scores across all metrics. While the detection and acknowledgment times would ideally be instantaneous, the scores for each metric are lowered to 7 due to its dependency. Similarly, if the attack pattern is recognized, containment and mitigation measures can be promptly initiated upon detection. However, the reliance on data quality results in a reduction of points to 7 for these metrics as well. This result is listed in Table 14.

Metric	Evaluated points
Time to detect	7
Time to verification	7
Measure supports containment	7
Measure supports mitigation	7

Table 14: Metric evaluation result - application vulnerability monitoring

The category result calculation leads to 7 points for the "detection effectiveness" category and 7 points as well for the "impact minimization" category. These results are depicted in Table 15.

Category	Evaluated points
Detection effectiveness	7
Impact minimization	7

Table 15: Category evaluation result - application vulnerability monitoring

2.3.4 Update white-lists

White-listing updates based on their hash value is an ideal solution, based on the analysis results. Attempts to update an ECU with non-approved software can be detected and verify instantly if a connection with the vehicle backend is available. The containment and mitigation are also possible for these attacks.

This would result in 10 points for each metric but due to the limitation to only attacks targeting the update process reduces these points. The reduction is limited to only 2 points due to the importance of integer ECU software, resulting to 8 points for each metric. The result is summarized in Table 16.

Metric	Evaluated points
Time to detect	8
Time to verification	8
Measure supports containment	8
Measure supports mitigation	8

Table 16: Metric evaluation result – update white-lists

The calculation for the categories results in 8 points for each category, "detection effectiveness" and "impact minimization". These results are listed in Table 17.

Category	Evaluated points
Detection effectiveness	8
Impact minimization	8

Table 17: Category evaluation result – update white-lists

2.3.5 Location verification

As a location-based verification method, the detection and acknowledgment of software update attempts are immediate, with the potential for swift containment and mitigation, warranting 10 points for each metric. However, like the update white-list approach, certain limitations affect its efficacy. Location verification primarily focuses on the update process and relies heavily on the accuracy and reliability of allowed location data, leading to a reduction in points across all metrics. The restriction to the software update process diminishes points by two, while the dependence on the quality of allowed location data further reduces points by an additional one for all metrics. Moreover, the potential risk of denying legitimate and crucial updates also affects the containment and mitigation score, resulting in a deduction of 1 point. Consequently, the scores are 7 points for detection and acknowledgment and 6 points for containment and mitigation. Table 18 summarized the results.

Metric	Evaluated points
Time to detect	7
Time to verification	7
Measure supports containment	6
Measure supports mitigation	6

Table 18: Metric evaluation result – location verification

The calculation for the categories results in 7 points for the category "detection effectiveness" and 6 points for "impact minimization" category. Table 19 lists these results.

Category	Evaluated points
Detection effectiveness	7
Impact minimization	6

Table 19: Category evaluation result – location verification

2.3.6 AI-based behavior analysis

The efficacy of an AI-based approach hinges significantly on the quality of the data utilized to train the ai model. Consequently, a comprehensive evaluation becomes challenging. The potential points span a wide spectrum, ranging from 1 point in each metric due to inadequate data quality, resulting in the inability to detect and contain incidents, to 10 points for optimal data quality, leading to a highly effective system. Given this wide range and the uncertainty surrounding the quality of available data, the AI-based behavior analysis is excluded from the assessment. The result is summarized in Table 20.

Metric	Evaluated points
Time to detect	N/a
Time to verification	N/a
Measure supports containment	N/a
Measure supports mitigation	N/a

Table 20: Metric evaluation result – AI-based behavior analysis

The calculation for the categories is not possible, due to the uncertainty surrounding the quality of available data. Table 21 lists this outcome.

Category	Evaluated points
Detection effectiveness	N/a
Impact minimization	N/a

Table 21: Metric evaluation result – AI-based behavior analysis

2.4 Assessment result

In the final part of the assessment, the evaluation is summarized and set into perspective with the initial motivation. The evaluation resulted in two values for each category, with the DTC analysis scoring the fewest points and the update white-list approach the highest points. The results of the evaluation are summarized in Table 22.

Category	Detection effectiveness	Impact minimization
DTC analysis	2	1
Cross-domain comparison	6	5
Application vulnerability monitoring	7	7
Update white-lists	8	8
Location verification	7	6

Table 22: Evaluation - Result Summary

A visualization of this result in a matrix structure highlights which approach shows the highest potential for further use in CSMS and risk management systems. This visualization is depicted in Figure 1.

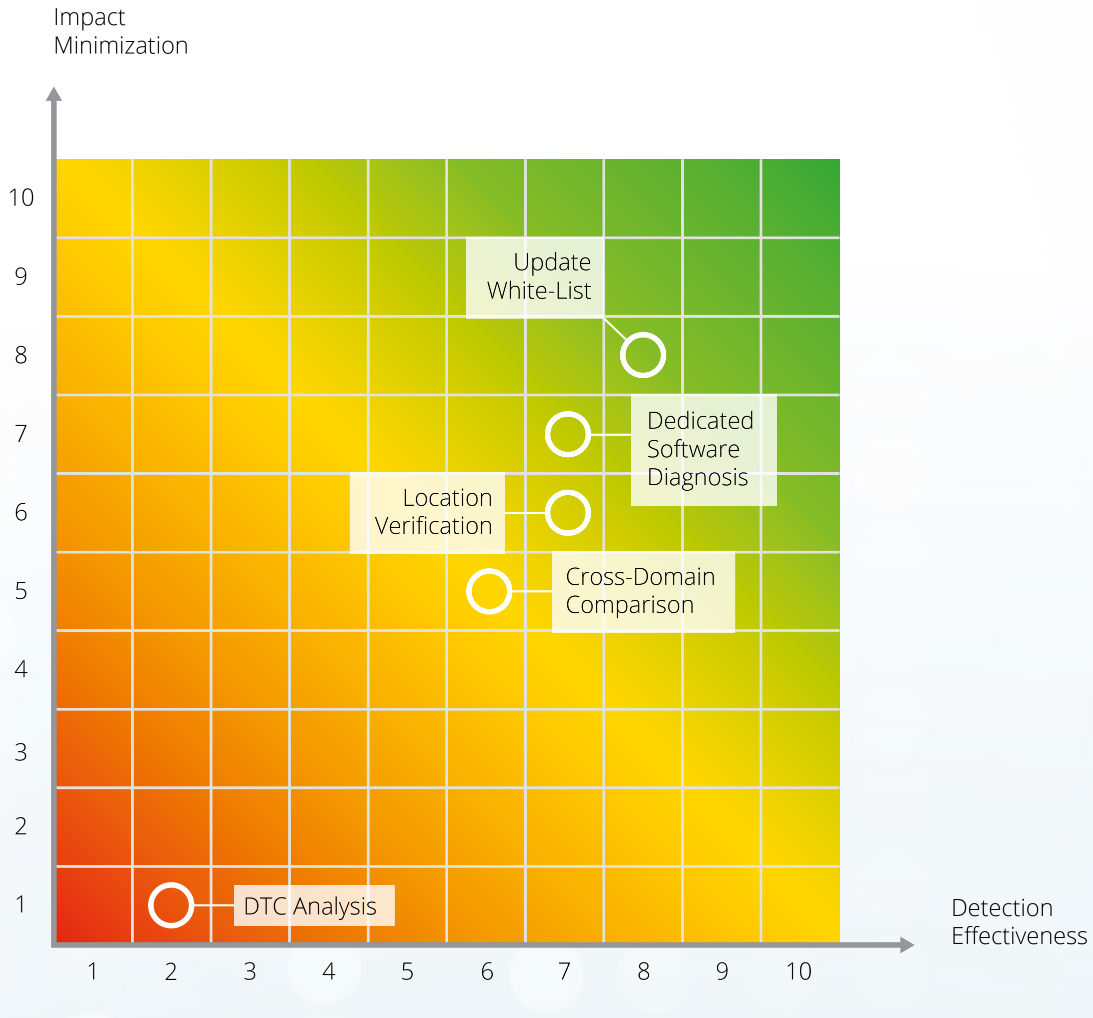


Figure 1: Evaluation Result - Visualization

The DTC analysis depicted in the bottom left of Figure 1 exhibits lower usability for a CSMS compared to the other approaches. Its reliance on modifying an existing, well-established system introduces changes that were not initially intended during its original development, thereby diminishing its usability. However, leveraging the existing DTC system, which is already operational, could result in a relatively quicker and less resource-intensive implementation compared to other approaches. While this approach may yield low overall impact, its potential for swift implementation with minimal resources could justify its adoption as a quick-win solution.

Cross-domain comparison is rated higher than DTC analysis. However, its effectiveness is tempered by its reliance on additional information to reliably verify incidents. Despite this drawback, employing cross-domain comparison systems across multiple vehicles could reveal trends in attack vectors, benefiting risk management systems. Moreover, the ability to alert drivers to potential incidents enhances vehicle safety significantly, warranting a higher rating than DTC analysis. Utilizing existing sensor data streamlines the implementation process for integrating into an HPC, minimizing development efforts. Overall, this approach offers a moderate impact and requires moderate resources, positioning it as an intermediate solution.

Position three is taken by the location verification strategy. While its effectiveness relies on the accuracy of verified location data and its constraints to the update process, it still holds potential for enhanced security. When integrated with complementary verification or security measures, it can significantly bolster overall diagnostic and update process security. Because this method utilizes vehicle data, it may not necessitate additional cryptographic security measures if location data reliability is ensured. For an OEM's CSMS and risk management system, this approach offers valuable insights into potential incidents, aiding in the identification of emerging attack trends. Location verification is adaptable, providing both incident containment capabilities and pertinent information for the OEM's risk management system. However, its implementation requires substantial resources and high-quality data. Despite this, its versatility and long-term viability make it a promising solution with significant potential impact in the future.

In second place is the application vulnerability monitoring approach. This method closely aligns with the original concept of SOVD and stands to benefit from existing frameworks for software-specific diagnostic processes. Its effectiveness, however, hinges on the quality of information regarding attack patterns, which determines its ability to accurately predict potential threats. Nevertheless, even with limited knowledge of attack patterns, this approach remains valuable. It has the capability to promptly nullify detected incidents while furnishing dependable data on identified attacks. These insights can be aggregated and refined within an OEM's risk management system, offering a comprehensive view of the prevailing threat landscape. Furthermore, incidents that escape detection by the application vulnerability monitoring can serve as a source for further updates, progressively enhancing the approach's efficiency over time. Its integration with the SOVD standard and the potential for iterative improvements result in a moderate yet consistent implementation effort, yielding incremental gains in both protection and data quality for the risk management system. This makes the application vulnerability monitoring approach a viable intermediate solution with long term effort needed to increase its maturity.

As the top-rated approach, the update white-list shows a notable advantage in safeguarding the update process against unauthorized software alterations. It not only offers robust protection against malicious software changes but also furnishes reliable data for risk management systems in scenarios involving misuse of the update process. However, a noteworthy drawback of this approach is its narrow application scope, limited solely to the update process. To ensure the effectiveness of the update white-list, constant availability of reference values for software validation is imperative, necessitating a direct connection to a back-end system and the establishment of a new data infrastructure to support the validation process. Consequently, this approach demands significant development resources and time investment, positioning it as a long-term solution tailored for the future.

2.5 Assessment conclusion

Each approach presents its own set of advantages and disadvantages. Short-term solutions may lack in usability, but their quick and easy implementation justifies their utilization. On the other hand, higher-rated approaches demand more effort to implement but offer more reliable information, thereby enhancing overall cybersecurity.

A strategic approach involves the immediate implementation of short-term solutions alongside the concurrent development of necessary systems and processes to leverage the resultant data. This approach lays the groundwork for a dynamic CSMS and risk management system. Continual refinement of these systems and processes, coupled with the integration of approaches requiring longer development times, enhances an OEM's ability to respond efficiently to cybersecurity incidents.

Considering the transformative shifts in the automotive industry, such as the rise of autonomous driving and the increasing complexity of on-board computers and over-the-air functionalities, establishing a mature and dynamic CSMS and risk management system becomes imperative for ensuring vehicle security in the future. All assessed approaches play crucial roles in this trajectory, offering valuable insights and enabling proactive responses to emerging events.

3 Conclusion

In conclusion, the assurance of cybersecurity within the automotive industry has emerged as a pivotal aspect in today's era of digitally interconnected vehicles. A careful evaluation of potential implementations to enhance vehicle software security revealed various approaches, from leveraging existing on-board diagnostic functions and whitelisting updates to utilizing cross-domain comparisons, location verification, and AI-based behavioral analysis. However, the effectiveness of these strategies varies, with each presenting its unique set of benefits and trade-offs. The challenge lies in efficiently blending quick-win solutions and implementing long-term strategies to develop a robust and dynamic CSMS and risk management system.

While short-term solutions like DTC analysis and cross-domain comparison may not provide a comprehensive security framework, they offer immediate security enhancements and valuable insights for risk management systems. Conversely, high-rated strategies such as update white-lists and application vulnerability monitoring offer substantial security benefits but require sizeable investment in terms of resources and time.

The future trajectory of cybersecurity in the automotive landscape will be heavily influenced by the continued growth of advanced technologies and the industry's transition to autonomous driving and sophisticated on-board computers. As such, there is an urgent necessity to implement a mature and dynamic cybersecurity management system, enabling OEMs to safeguard their vehicles effectively against the continually evolving cyber threat landscape. It becomes evident that optimal security can only be achieved through a combination of these approaches, offering a proactive, multifaceted security model. Through this approach, it is possible to ensure the safety and security of vehicles in an increasingly interconnected and digitized world.

Authors

Marcel Dreger
Senior Consultant
madreger@deloitte.de
Deloitte Germany

Nishant Khadria
Director
nkhadria@deloitte.de
Deloitte Germany

Ingo Dassow
Partner
idassow@deloitte.de
Deloitte Germany

Literature Review

1 TÜV Rheinland, “New cyber threats pose a risk to an automotive industry in transition”, TÜV Rheinland, Köln, https://www.tuv.com/landingpage/en/cybersecurity-trends_2024/navi/automotive-cybersecurity/, visited 18.03.2024

2 ASAM e.V, „Service-Oriented Vehicle Diagnostics“, ASAM e.V., Höhenkirchen, 30. Juni 2022,

3 Kabul Kurniawan, “Improving Cybersecurity through Semantic Log Monitoring,Analysis and Attack Reconstruction”, Universität Wien, 2023

4 Panagiotis Trakadas, Xavi Masip-Bruin, Federico M. Facca, Sotirios T. Spantideas, Anastasios E. Giannopoulos, Nikolaos C. Kapsalis Rui Martins, Enrica Bosani, Joan Ramon, Raül González Prats, George Ntroulias and Dimitrios V. Lyridis, “A Reference Architecture for Cloud–Edge Meta-Operating Systems Enabling Cross-Domain, Data-Intensive, ML-Assisted Applications: Architectural Overview & Key Concepts”, MDPI, 21. November 2022

5 David Storm, “Why runtime application self-protection is critical for next generation app security”, VASCO

6 Zhongxu Yin, Zhufeng Li & Yan Cao, “Cloud Computing and Security”, Kapitel “A Web Application Runtime Application Self-protection Scheme against Script Injection Attacks”, 4th International Conference, ICCCS 2018, Haikou, China, Juni, 2018

6 Bakil Al-Muntaser, Mohamad Afendee Mohamed & Ammar Yaseen Tuama, “Real-Time Intrusion Detection of Insider Threats in Industrial Control System Workstations Through File Integrity Monitoring”, Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Kuala Terengganu, Malaysia & College of Computer Science and Information Technology, University of Kirkuk, Iraq., 2023

7 Suresh Limkar, Nivedita Kadam & Rakesh Kumar Jha, “Signal Processing and Information Technology”, Kapitel “Access Control Based on Location and Time”, Springer, Berlin, 2011

8 Salman Khaliq, Zain Ul Abideen Tariq & Ammar Masood, “2020 International Conference on Cyber Warfare and Security (ICCWS)”, Chapter “Role of User and Entity Behavior Analytics in Detecting Insider Attacks”, IEEE, Islamabad, Pakistan, 25. December 2020

9 UN/ECE, “UN Regulation No. 155 - Cyber security and cyber security management system”, Genf, 4. März 2021

10 International Organization for Standardization, “ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering“, Genf, August 2021

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our people deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society, and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 457,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.