CYReV

Cyber Resilience for Vehicles

Author: Peter Wirén
Date: 240307
Projects on Cybersecurity for vehicles

CyReV - Datasäkerhet för fordonssystem i en föränderlig miljö

2018-05013 & 2019-03071

Public report

Contents

Kort om FFI

FFI är ett samarbete mellan staten och fordonsindustrin om att gemensamt finansiera forsknings- och innovationsaktviteter med fokus på områdena Klimat & Miljö samt Trafiksäkerhet. Satsningen innebär verksamhet för ca 1 miljard kr per år varav de offentliga medlen utgör drygt 400 Mkr.

För närvarande finns fem delprogram; Energi & Miljö, Trafiksäkerhet och automatiserade fordon, Elektronik, mjukvara och kommunikation, Hållbar produktion och Effektiva och uppkopplade transportsystem. Läs mer på www.vinnova.se/ffi.

1 Executive Summary

The advent of autonomous and connected vehicles has brought new cybersecurity challenges to the automotive industry and put the requirement on vehicles to be designed to remain dependable in the occurrence of cyber-attacks. Furthermore, UNECE regulation 155 has identified principles for the OEMs to comply with. Following these principles provides evidence that OEMs implement cybersecurity over the lifecycle of the vehicle. Two of the key principles in the UNECE regulation are *(i)* the vehicle should be designed to be resilient to cyber-attacks and *(ii)* the vehicle should be designed with the capability to detect cyber-attacks and respond appropriately. The UNECE regulation, however, does not provide any guidance on how to comply with these principles. Therefore, in this project, we aimed to provide guidance on how to design dependable vehicles while having to comply with these principles.

This report for Cyber Resilience for Vehicles (CyReV) is an updated version of the report “CyReV Fas 1” [1] containing the results for the whole CyReV project. The addition focused on cybersecurity for automotive in-vehicle systems in a changing environment. The second phase of CyReV has contributed to the identified need by investigating and maturing (i) hybrid intrusion detection systems, (ii) defence-in-depth approaches for strong detection, (iii) forensics techniques for finding the root cause of cyber-attacks, (iv) resilience analysis of safety mechanisms, complementing the analysis of security mechanisms done in CyReV Fas 1, as well as (v) identification of metrics for evaluating resilient designs.

The project has:

- Produced a reference architecture for resilient vehicles which includes research around Architecture Design Principles for resilient vehicles,
- Identified techniques suitable for vehicular cyber-resilient designs,
- Identified principles suitable for detection, mitigation, recovery and how to create endurance over time,
- Investigated novel techniques for on-line attack analysis,
- Incorporated Machine Learning techniques for Anomaly Based Intrusion Detection Systems (IDSs) to describe normal and abnormal behaviour of traffic systems,
- Studied the Defence-in-depth strategy for the vehicle to be able to prevent and detect cybersecurity attacks,
- Investigated post-attack forensics for post-attack investigations,
- Produced a reference architecture for secure and resilient software updates and another one for automotive digital forensics,
- Conducted an interplay analysis between non-functional requirements such as safety and security when it comes to the impact of safety and security mechanisms on resilience,
- Investigated pre-injection analysis techniques with the focus on the reduction of the attack space, and
- Identified a set of metrics for developing and evaluating resilient designs.

The CyReV consortium consists of Assured, Chalmers University of Technology, Combitech, RISE Research Institutes of Sweden, Volvo Car Group, and Volvo Technology AB (VTEC), with VTEC being the project coordinator and the main applicant.

2 Background

Vehicles are now in the phase of beginning to communicate with the infrastructure around them and use information from other vehicles, roadside objects, and cloud-based resources to make decisions. For short-range communication, Vehicular-Ad-Hoc-Networks (VANETs) will be used, which typically are based on DSRC (US) or ITS-G5 (Europe) to share information about vehicle presence, status, and intentions. Typical applications in this area and often heard of are platooning and virtual traffic lights. For long-range communication and when delay is not as critical, 3G/4G/LTE/5G can be used, for example, to exchange information about weather, congestion, and road conditions. Decisions will be made by vehicles and drivers based on long- and short-range communications, and when vehicles become more autonomous, communication will govern data such as speed and distance to other vehicles. This way, vehicles will know when it is safe to overtake other vehicles and will be able to notify drivers when hidden vehicles are approaching. It is crucial that all exchanged messages are correct, and that the integrity of these messages is protected. Moreover, the information should not be shared with unauthorised users, for example the position of vehicles with dangerous or valuable goods should not be publicly available.

Vehicular systems will always be the target for hackers, thus, the ability to design for security and safety is of uttermost importance, and we must design the vehicles in such a way that they are able to deal with malicious actions from other entities. Earlier research projects such as the HEAVENS project [2] as well as ISO/SAE 21434 road vehicles cybersecurity engineering standard [3] have laid the ground for this and have defined methods for how to perform threat and risk analysis in structured ways. These methods are similar to traditional risk-based safety design processes for vehicles such as the ones defined in ISO 26262 road vehicles functional safety standard [4]. Later projects have then continued and focused on the design of secure vehicular systems, given that a risk analysis has been done. Secure reference architectures have been developed in HEAVENS and EVITA [5] projects, which guide designers in how to create structured and secure designs. Lately, projects such as HoliSec [6] have focused on increased awareness of how potential threats can and should be met with technology and required security components. These projects and the emerging standards have led to more robust, secure, and safe designs of vehicular systems.

Safety designs have always focused on building systems that are able to deal with faults (unexpected events), for example by adding redundancy and using fault-tolerant designs. In this project, we have taken a similar approach to security. In the event of a security-related incident such as a verified security breach or after an alarm indicating a potential problem, the vehicle needs to react and mitigate the threat. This work is a logical continuation of the earlier FFI projects and is a necessary component for vehicles to be able to continue to function in a malicious environment. It is not acceptable from a societal perspective that complete fleets of vehicles are grounded due to a potential security problem waiting to be investigated and, if needed, to be corrected, but they need to function albeit with a somewhat limited functionality.

3 Purpose, Research questions and Method

The high-level objectives for this project were to:

- Address the problem of how to detect and react to security incidents in vehicular systems. Working with mechanisms such as Intrusion Detection Systems (IDS) to be able to detect different types of attacks on vehicles and networks. Different solutions have been proposed in the literature, all with different characteristics, but a common problem with anomaly-based systems is the high rate of false alarms (false positives) which prevents these systems from being used in a real setting. However, employing hybrid IDS can provide enhanced visibility into security incidents by analysing data from various attack sources through diverse detection methods. Thus, a framework for a Hybrid Intrusion Detection System (HIDS) was investigated to collectively achieve a higher accuracy in detecting potential threats.
- An investigation was done into what mechanisms can be useful and how they may be deployed, whether detection should be done locally within each vehicle and/or globally using cloud-based solutions. The latter is a novel area in vehicular systems. Previous works were used, such as Alheeti *et.al.* [7] and Levi *et.al.* [8], that use data-driven methods to create either rules or neural networks-based tools to detect anomalies in vehicular networks. In particular, building on the knowledge from Rosenstatter and Englund [9] where a combination of V2V and vehicle data was combined to create a system that could be used in decision-making in the sensor fusion system of a platooning vehicle.
- Conduct research on what needs to be done when a potential security problem is detected in a vehicle or support system such as vehicular ad-hoc networks and develop methods for how to design resilient systems. Reference architectures for vehicles have been created and metrics developed, which can be used to test and evaluate real designs.
- Identify what means are necessary to enable post-event analysis and find out the reasons as to why and how an intrusion has happened. It is not enough to just detect security breaches in a timely manner, enough information needs to be available to understand why and how the situation has occurred to prevent the problem from reappearing. This work is essential in order to enable forensics. The work with resilient design and to enable forensics for vehicular systems is a new novel area that needs to be investigated. These results should be applicable not only to vehicular systems but are likely to be applicable to other Internet-connected safety-critical systems as well.
- Perform interplay analyses of the impact of the usage of safety and security mechanisms on resilience. Moreover, we use pre-injection analysis in order to reduce the time and cost needed to test system resiliency against cybersecurity attacks.

Table 3.1. WP1 - Detailing use cases

Work Package 1	Detailing Use cases
Leader	Volvo Technology AB: Use case provider
Other participants	Assured: use case provider, Combitech: use case provider, Volvo Car Group: use case provider
Description of contents	Task 1.1 Industrial needs and relevant use cases (Leader: Volvo Technology AB) State of the art investigation Automotive needs and requirements (development of the relevant use cases)
Method/approach	An interview study was performed. Subjects were selected among the participating companies based on the relevance of their experience and competence.
Delivery	D1 Industrial needs and use cases

Task 1.1 Industrial needs and relevant use cases

The goal of this task was to provide details about the use cases to be utilized in the rest of the project for other work packages. Moreover, an investigation was done on the challenges that the industrial project partners meet with regards to:

- Required components for a vehicle architecture to be able to detect and respond to cyber-attacks and their effect on the vehicle performance and each other
- Detection of anomalies in vehicular system behaviour
- Data collection and data analysis
- Interplay between safety and security and handling the conflicting requirements
- Degrading the vehicle operation during an attack/incident

Furthermore, relevant use cases were identified to illustrate situations in which:

- Anomaly detection is most needed, and where security breaches are most likely to happen
- Data useful for post-attack analysis shall be collected
- Contradictions occur between safety and security requirements
- There is the need for degrading the operation during an attack/incident

The identified use cases to be parts of bigger use cases such as:

- Fully autonomous vehicle connected through the cloud
- Remote diagnostics and Software Download over the Air
- Connection agnostic communication resilience (switch to other communication methods in the event of a loss of one connection)
- Semi-autonomous Control Tower scenario when the vehicle is connected remotely through the cloud

Table 3.2. WP2 - Development of Resilient Automotive Systems

Work Package 2	Development of resilient automotive systems
Leader	Chalmers: Resilient design and smart repairs
Other participants	RISE[1]: Security analysis and performance, Combitech: Reference architecture, principles, and performance, RISE: Security analysis and reference architecture, Volvo Car Group: Security analysis and reference architecture, Volvo Technology AB: Reference architecture, principles, and performance
Description of contents	Task 2.1 Reference architecture for Resilient Vehicles (Leader: Volvo Technology AB) Task 2.2 Principles for Resilient Vehicles and smart repairs (Leader: Chalmers) Task 2.3 Performance of resilient vehicle design (Leader: RISE)
Method/approach	Task 2.1 A reference architecture was developed, which shows possible ways to deal with security problems and continue to offer the intended service. Task 2.2 Other domains were investigated to find applicable solutions. The reference architecture was used to see how it can be used to mitigate security problems, and when necessary, it was refined. Task 2.3 Suggested designs were tested with respect to performance and usability.
Delivery	D2.1 A reference architecture for resilient vehicles D2.2 Principles for resilient vehicle and smart repair D2.3 Metrics for evaluating resilient designs

[1] *Formerly referred to as RISE Electronics, RISE Viktoria or RISE SICS.*

With the consideration that vehicles are required to be designed to be resilient to cyber-attacks, this work package has investigated what constitutes cyber security resilience for vehicles and explored the principles of designing resilient vehicles.

Task 2.1 Reference architecture for Resilient Vehicles

In this task, a reference architecture for a resilient vehicle was created, which can be used when designing and evaluating methods and mechanisms to prevent, detect and respond to cyber-attacks. We investigated the components a reference architecture shall contain and how it should be realized. The architecture is easy to use and understand yet detailed enough to be relevant for real vehicular problems and represent a real vehicle architecture.

Task 2.2 Principles for Resilient Vehicles and smart repairs

The goals for this work package were to investigate principles for building a resilient vehicle and to identify principles suitable for detection, mitigation, recovery, and how to create endurance over time. We have focused on how a resilient vehicle system can be built based on the reference architecture from Task 2.1. To do so, we identified the components necessary to be able to simulate security problems, how to limit potential impact and how to dynamically reconfigure the system when suspected security problems are detected. There may be different levels of reaction, ranging from raising an alarm that should later be checked by OEMs to enforcing stricter firewall/gateway rules, limiting or disabling some subsystem functionality, shutting down or disconnecting internal functions, disconnecting the vehicle from external communications or even initiating a complete shutdown. We have also systematically identified the threats to resilience and mapped them to the principles and mechanisms defined in this task.

Task 2.3 Performance of resilient vehicle design

The goal of this task was to study the existing metrics that have been used to measure the resilience of the system. To this end, a literature survey was conducted to find the various metrics that have been published. These metrics found used either *time*, *amount*, *score*, or *throughput* to measure the resiliency of a system. In D2.3, we present the metrics and highlight how they are used.

Table 3.3. WP3 - Defence in depth: Detection Mechanisms

Work Package 3	Defence in depth: Detection Mechanisms
Leader	Volvo Car Group: In-vehicle and cloud-based intrusion detection
Other participants	RISE: Safety and security analysis, RISE: Security improvements in the IDS infrastructure, RISE: V2X communication and data patterns analysis, Volvo Technology AB: In-vehicle intrusion detection
Description of contents	Task 3.1 V2X and cloud-based Intrusion Detection Mechanisms (Leader: RISE) Task 3.2. In-vehicle intrusion detection (Leader: RISE) Task 3.3 Interplay between error/intrusion detection/handling mechanisms (Leader: RISE Electronics) Task 3.4 Hybrid Intrusion Detection System (Leader: Volvo Car Group)

Work Package 3	Defence in depth: Detection Mechanisms
Method/approach	Task 3.1 Development of data driven models for anomaly and intrusion detection. The models are based on machine learning algorithms trained on historical or simulated data. Task 3.2 An analysis of select existing technologies from automotive and other fields and investigate a number of improvements to state of the art. Task 3.3 An analytical interplay analysis based on a layered resilience framework. Task 3.4 Development of a framework and methods for a hybrid intrusion detection system based on the data retrieved from the IVN and the related backend system
Delivery	D 3.1 Models for V2X and cloud-based IDS D 3.2 Report on feasibility of selected technologies with preliminary security and performance analysis D 3.3 Interplay between error/intrusion detection/handling mechanisms D 3.4 Hybrid intrusion detection system for cyber resilient vehicles

Task 3.1 Cloud-based Intrusion detection mechanisms

Data driven modelling techniques, capable of describing the normal behaviour of a system, as well as detecting anomalies (unexpected behaviour), were developed in this task. Since traffic behaviour is typically nonlinear, machine learning-based algorithms were used for this purpose. Anomaly detection training was done on structured historical data consisting of numerical values or simulated data when historical data was not available. The aim was to mimic the communication pattern and content described by the data using machine learning based on e.g., neural networks, support vector machines or random forest. The results were evaluated to select the model with the highest performance regarding classification accuracy and/or model complexity. Finding this trade-off is typically a challenge that has to be addressed together with the industrial partners.

State-of-the-art modelling and anomaly detection methods were investigated and adjusted for this purpose. Historical data was preferable for training and testing of the models and was used to as high extent as possible. When historical real vehicle data was not available, simulated data was used instead.

Models designed to address the Research Questions (RQs) in this task are highly dependent on defined use cases and available data. Furthermore, the activities conducted were coordinated with the activities in the rest of WP3 in order to ensure that the results are propagated to other layers in order to avoid severe incidents.

Task 3.2. In-vehicle intrusion detection

This task was focused on in-vehicle monitoring and detection mechanisms, and investigating its effect on resilient architectures and event data quality for use in WP4 for forensics and response. This work built upon existing research with different types of IDS and used the reference architecture developed in WP2, where different scenarios were simulated, although the focus was shifted to the detection of security problems and the properties of the IDS systems.

An important problem was reducing false IDS alarms to avoid triggering unnecessary or possibly dangerous actions from the vehicle. This had to be done without significantly reducing the IDS precision.

Task 3.3 Interplay between error/intrusion detection/handling mechanisms

The aim of this task was to study the layered resilience framework and investigate the safety and security mechanisms used in different layers. These mechanisms are used to increase system safety and security by detecting/handling different types of errors, including security intrusions (according to Sangchoolie *et al.* [10], security intrusions may be considered as specific types of errors that are the result of security attacks). The investigation facilitated an interplay analysis where the impact between error detection mechanisms and error handling mechanisms was studied. The interplay analysis was critical to identifying mechanisms that have potential destructive impacts on each other and on systems resilience. The interplay analysis also facilitates error removal and decreases the likelihood of ending up with catastrophic failures or system reconfigurations (safe shutdown), which are both costly. Part of the results obtained in this task was published at CARS2022 [11].

Task 3.4. Hybrid Intrusion Detection System

The main objective of this task was to propose a framework for a Hybrid Intrusion Detection System (HIDS) for comprehensive monitoring of the interconnected car system. These systems employ a mix of behavioral and misuse detection techniques to identify abnormalities, triggering alerts upon detection. Subsequently, these alerts are transferred to a Security Information and Event Management (SIEM) and further on to a Security Operations Center (SOC) analyst or a Cyber Incident Response Team (CIRT).

One of the key advantages of employing a hybrid IDS is its ability to provide enhanced visibility into security incidents by analyzing data from various attack sources. This is achieved through the utilization of diverse detection methods, resulting in collectively higher accuracy in detecting potential threats. Tasks 3.4 and 4.1 shares common ground and the outcomes will serve the objectives of both tasks. While the focus lies primarily on IDS and forensics in their respective domains, the hybrid IDS serves a dual purpose. It is employed not only for identifying cyber-attacks from a cybersecurity standpoint but also for detecting and storing events crucial for post-incident forensic investigation and fault tracing.

Table 3.4. WP4 - Forensics, Analyse, Learn, and Respond

Work Package 4	Forensics, Analyse, Learn, and Respond
Leader	Chalmers: Attack analysis and response and post attack data collection
Other participants	RISE: Attacker behaviour, Volvo Car Group: Pre and post data collection and analysis, Volvo Technology AB: Data collection and analysis
Description of contents	Task 4.1 Pre and post attack data collection and enablers for forensics (Leader: Volvo Car Group) Task 4.2 On-line forensics (Leader: Chalmers)
Method/approach	Task 4.1 Development of a data model for post-attack forensics Task 4.2 Development of live forensics techniques based on machine learning
Delivery	D4.1 Data-collection techniques D4.2 Forensics techniques

Task 4.1 Post-attack/post-event data collection and enablers for forensics

Current automotive regulations and standards, i.e., the United Nations Regulation No. 155 [12] and ISO/SAE 21434 [3], state that cybersecurity measures shall be incorporated into the design to detect and respond to potential cyber threats. It further states that data forensic capabilities shall be provided to enable analysis of attempted or successful cyber-attacks. Still, there are no details or guidelines around automotive digital forensics (ADF). In Task 4.1, we emphasize challenges, requirements, and guidelines within the field of ADF, specifically event data management and data collection. We establish the required processes and components and propose a forensic reference architecture to retain data for investigating incidents following an attack.

Ensuring the authenticity of the data is fundamental. Still, its close connection to other cybersecurity attributes, for instance, fulfillment of confidentiality and availability, is also essential to secure digital evidence. Although IDS system alarms activate robust vehicle protection measures, retaining sufficient internal and external information is imperative for a digital forensic investigation. This data facilitates forensic analysis following significant incidents, such as accidents or detecting malicious software within a vehicle.

This task's primary focus is internal and external communication, encompassing in-vehicle networks and V2X communication concerning forensically relevant data, and will consider questions such as the following.

- **RQ1:** What data is necessary to save for future analysis, and who is legally responsible for collecting the data on-site? Both w.r.t. internal and external communications and events. For example, serious events may occur due to malicious and erroneous communication from other vehicles or when others misbehave in traffic.
- **RQ2:** How can the authenticity of the digital evidence be guaranteed? How can the chain of custody be preserved, e.g., to be legally admissible in court? Post-crash data must be protected against being erased, damaged, or modified, e.g., other vehicles in the surroundings can also save data when instructed for redundancy.

Task 4.2 On-line attack analysis and forensics

The work with resilient architecture design continues with developing novel techniques that allow a vehicle (or a set of connected vehicles) to understand the root cause of an ongoing attack, once it has been identified by the IDS component. Methods are needed to make sure the problem is identified and to learn about its behaviour and avoid similar problems from being spread to other vehicles in the future. This analysis is also important to perform error handling and smart repairs.

The successful development of such analysis system requires two parts: (1) a way to instrument the software components so that they are amenable to inspection and forensics. For instance, the instrumented components are be able to flag the traversal of code sections that had never been executed before, or in an order of execution that has not been observed before; (2) a way to jointly analyse the information from the instrumented software, the IDS, the execution environment, and so on, in order to identify the location of the failure and the type of attack. The use of machine learning techniques was considered to achieve this.

Table 3.5. WP5 - Verification and Validation

Work Package 5	Verification and Validation
Leader	Combitech: Verification and validation, and PoV
Other participants	Assured: Security testing and verification, RISE: Safety and security interplay analysis, Volvo Car Group: Security testing and model provider, Volvo Technology AB: Verification and validation, safety and security interplay analysis
Description of contents	Task 5.1 Verification and validation of cyber resilient vehicles (Leader: Combitech) Task 5.2 Interplay between safety and security using experimental verification and validation methods (Leader: RISE) Task 5.3 Proof of Value (PoV) (Leader: Combitech)
Method/approach	Task 5.2 Model-implemented fault and attack injection Task 5.3 Methods identified in T5.1.
Delivery	D 5.1 Methods used for verification and validation of resilient vehicle D 5.2 Safety and security interplay analysis using fault- and attack injection D 5.3 Evaluation of use-cases

Task 5.1 Verification and validation of resilient vehicles

In this task, the aim was to identify and list verification and validation strategies that are suitable for evaluating resilient vehicles considering different layers of detection/handling mechanisms addressed by a layered resilience framework. Generic strategies as well as strategies aligned with ISO 26262 [4], the latest version of the ISO/SAE 21434 [3] and other related standards were considered.

Task 5.2 Interplay between safety and security using experimental verification and validation

The focus of this task was to study the interplay between safety and security by investigating experimental verification and validation methods, such as fault- and attack injection, suitable for testing resilient vehicles. The lessons learned from the interplay analysis were used to propose and evaluate approaches to facilitate resilience testing using attack injection. Parts of the results obtained in this task were published at PRDC2022 [13].

Task 5.3 Proof of Value (PoV)

In this task, proof of concept by means of methods and tools to demonstrate the proposed architectural principles for designing resilient vehicles (mainly derived in WP2, and T5.1) was implemented. The proof of concept was to demonstrate the usefulness for at least one use-case.

3.1 Originality and newsworthiness

The previously FFI funded projects HEAVENS [2] and HoliSec [6] have helped bring the Swedish automotive industry to the frontiers of automotive security and to reach international recognition. CyReV extended this work further by:

- Providing the Swedish automotive industry with techniques, methods and tools to maintain the safety and security of modern and emerging connected and autonomous vehicles when facing threats of evolving cyberattacks.
- Bringing together Swedish automotive players in passenger and commercial vehicles and suppliers as well as research institutes and academia to (i) identify and develop methods and technologies to support the persistence of safety and security in modern and emerging connected vehicles and (ii) improve the communication across partners of the automotive industry.
- Development of frameworks for enhancing vehicle security and resilience, a reference architecture for secure vehicle software updates, and another for automotive digital forensics.
- Developing a reference architecture for vehicles resilient to cyberattacks including principles, metrics and design requirements necessary to support resilience. Intrusion- and error handling mechanisms as well as verification and validation techniques used to support resilience will be investigated and improved which will also take the interplay between safety and security implementations and techniques into consideration.
- Aiming for at least TRL 3-4 where the technology will be trained and tested on historical as well as simulated data. Current state-of-the-art indicates that the technology is at TRL 2-3.

4 Goal

Automotive security and privacy have been addressed in several FFI-funded projects (HEAVENS [2], HoliSec [6], CASUS [14] and ThreatMove [15]). These have focused on methods and tools for in-vehicle design, development, integration, verification and validation. The CyReV project focuses on making vehicles in operation resilient towards attacks by incorporating mechanisms for detection, handling, and mitigation of attacks. This means revisiting design, development, integration, verification and validation phases, with resilience in mind.

Design for resilience: One focus of this project was to improve design processes and methods to increase vehicle resilience towards malicious attacks. In order to guarantee the safety of the vehicle, attacks need to be detected, mitigated and handled in a systematic and integrated manner (see G4 in Table 4.2), likely by reconfiguring systems, disabling some functionality and reverting to a safe and secure state until the problem has been solved. A reference architecture was created (see G1 in Table 4.2), and feasibility and performance effects of the components added in this project were tested against a future Volvo Truck architecture (see G2 in Table 4.2).

Cross-domain cooperation: In order to increase the resilience towards attacks, there is a need to investigate solutions in other domains, and to the extent it is possible to adapt them to the vehicle industry. The partners of this project have been selected in order to efficiently approach this task with their domain specific security and safety competence, as well as security competence from other domains (see O3 in Table 4.1).

Table 4.1. Connection to FFI overreaching objectives

FFI overreaching objectives	Project objective
Increasing the Swedish capacity for R&I and ensuring competitiveness and jobs in the field of vehicle industry.	**O1:** Increased resilience towards malicious attacks on vehicles in operation will increase the competitiveness of Swedish OEMs on the global market.
Developing internationally interconnected and competitive R&I environments in Sweden	**O2:** Three Ph.D. students have spent time in this project. Moreover, a Postdoctoral researcher was recruited to work in this project. These efforts increase academic competence in automotive security and privacy at a Swedish university.
• Promote the participation of small and medium sized companies • Promote cross industrial cooperation • Promote cooperation between industry universities and higher education institutions • Promoting cooperation between different OEMs	**O3**: The partners in this project were a mix of two OEMs, two SME suppliers with security competence from multiple contexts (e.g., avionics, financial sector, etc.) and two academic partners consisting of one university and one research institute.

Table 4.2. Connection to EMK topics

EMK description	Time horizon	Project goals
Cybersecurity as an integrated part of electronic architecture	Middle	**G1:** A reference architecture was created that improves vehicle resilience towards malicious attacks. **G2:** Feasibility and performance effects of the components added in this project was tested against a future Volvo Trucks architecture.
• Analysis of large data volumes in the cloud (ML algorithms used on cloud data) • Functional safety for cooperative systems (on limited use cases)	Middle	**G3:** In order to increase functional safety for cooperative systems, a proof of concept was produced for ML algorithms used on cloud data in order to detect intrusions.
Adaptive security architecture making it possible to protect against changes in the environment	Middle	**G1:** A reference architecture was created that improves vehicle resilience towards malicious attacks.
Processes, methods and technical solutions for cybersecurity adapted to make autonomous transport solutions possible	Middle	All work done in this project aims at making connected and/or autonomous vehicles more secure and thereby also safer.
Security mechanisms are a standardized and integrated part of the electrical architecture	Middle	**G4:** The interplay between error/intrusion detection/handling mechanisms was investigated.

4.1 TRL classification

The project addressed several aspects of security, from architecture, detection and mitigation mechanisms to wired and wireless technology as well as the cloud, hence it was challenging to represent the maturity of the technologies at start and end of the project by a single number. However, Table 4.3 represents estimated initial and target TRL levels to be reached by the end of CyReV. Technical validation of the technology under investigation in laboratory and relevant environments was conducted.

Table 4.3. TRL Classification

Technology and related work package	Estimated current TRL	Target TRL	Description of the maturity level to achieve
Resilient Vehicle Architecture (WP2)	2	3-4	Feasibility and performance of components of the architecture was evaluated against a future Volvo Truck architecture design.
Cloud-based Intrusion detection mechanisms (WP3)	2	3	The intention was to further investigate the data driven methods and develop models that can model normal behaviour and detect anomalies. The aim was to create a proof-of-concept that was to be trained and tested on preferably historical data and simulated when historical data was not available.

Technology and related work package	Estimated current TRL	Target TRL	Description of the maturity level to achieve
In-vehicle intrusion detection (WP3)	3	4-5	The technology was evaluated on real vehicles provided by Volvo Car Group, and it further improved the network-based IDS technology developed in the HoliSec project. The aim was to (i) improve the detection rate and accuracy, (ii) develop source detection techniques to identify the attacker, (iii) develop host-based attack detection techniques to proactively identify anomalous ECU behaviour and respond to them (proactive threat detection.) and (iv) develop log management techniques for post attack analysis.
Model-implemented fault- and attack injection (WP5)	2-3	4	The technology was used to test and evaluate Simulink models provided by the vehicle manufacturers. The fault injection part of the technology has a higher maturity than the attack injection part. The aim of the project was to improve the maturity of attack injection by enhancing the MODIFI tool [16] with more attack models and scenarios as well as adding support for pre-injection analysis techniques to facilitate verification and validation of resilience.
Collaborative attack analysis and handling (WP4)	2-3	4	The technology was evaluated via a simulation of a fleet of vehicles, based on realistic models provided by the OEMs.

5 Results and goal fulfilment

The technical work in the CyReV project was split up into five work packages, each with its own tasks, and the results were captured in deliverables. This chapter presents a summary of the deliverables that have been produced.

5.1 Deliverable D1.1

This deliverable (D1.1 State-of-the-Art Investigation) presents the results and achievements of sub-work package WP1.1 (State of the art) of the CyReV project. This deliverable provided insight into the state of current research frontiers in security and resiliency for vehicles and vehicular security. It also serves as an introduction to the issues faced in the automotive domain with an extensive reference list for more detailed studies. Finally, it can be used as background on which to base further investigations. The FFI HOLIstic Approach to Improve Data SECurity (HoliSec) project produced the deliverable "D1.2 State of the art", CyReV uses this deliverable as a baseline and extends the current state of the art with regards to resiliency. The report includes discussions about hardware and operating system level security, internal and external communication security, intrusion detection systems, secure software development, and related research projects. Many topics are discussed very briefly, since an exhaustive treatment of each would certainly be out of the scope of this deliverable.

5.2 Deliverable D1.2

D1.2 acts as input to all other CyReV work package activities. It contains the project definition of the term "resilience" ("Property of a system with the ability to maintain its intended operation in a dependable and secure way, possibly with degraded functionality, in the presence of faults and attacks").

Industry needs concerning security mechanisms have been identified as well as several use cases involving threats and security mechanisms that are to be considered within the project for further work, such as detecting an attack and recovering from it by restoring the system.

5.3 Deliverable D2.1

The deliverable describes a vehicle reference architecture that could be used when designing and evaluating methods and mechanisms to prevent, detect and respond to cyber-attacks. The reference architecture contains state-of-the-art aspects gathered from D1.1 and it has been designed to meet the needs and requirements from the use cases outlined in D1.2 Apart from giving an overview of a modern architecture with multiple security zones, the document provides descriptions of multiple electronic control units therein and how multiple use cases from D1.2 can be realized using security mechanisms within the reference architecture.

5.4 Deliverable D2.2

The work in this work package is based on the reference architecture from Task 2.1. We have investigated possible ways to react when security problems are detected and based on functionality, created a usable structure of available methods. Most techniques identified in this work are not limited to cyber-security since it often does not matter whether a deviation from normal behaviour of a component, subsystem or system, is due to a security problem or if the source is a software or hardware problem. The reactions can in many cases be the same. There may be different levels of reaction, ranging from raising an alarm to be checked by the OEM, to immediately enforce stricter firewall and gateway rules, limiting or disabling some functionality, disconnecting the vehicle from external communications or even initiating a complete, safe shutdown of the vehicle. As a result, we have gained knowledge about how to react when potential security events are detected and what mechanisms are available to dynamically reconfigure a vehicle to always offer the best possible service while guaranteeing the safety of its passengers.

We have performed a systematic literature review and identified threats to resilience, categorized and mapped them to their corresponding principles and protection mechanisms. As a result, a framework for resilient design of automotive systems, *REMIND*, has been developed.

Another framework, *Resilient Shield*, has been developed to reinforce the resilience of vehicles against security threats. Here attacks are systematically identified from which security guidelines and detailed directives focusing on security and resilience are derived. In Resilient Shield, the potential threat actors are mapped to the assets exposed by each attack, and we show which security and resilience techniques can be deployed to mitigate them. The resulting framework builds the base for designing secure and resilient systems and allows them to be easily extended in the presence of novel attacks.

Due to the ongoing legislative shift towards mandated cybersecurity for road vehicles, the automotive cybersecurity engineering standard ISO/SAE 21434 is seeing fast adoption throughout the industry. Early efforts focus on threat analysis and risk assessment (TARA) in the concept and development phases, exposing the challenge of managing TARA results coherently throughout the supply chain and life cycle. While the industry focuses on TARA, other aspects such as vulnerability and incident handling are receiving less attention. In order to better address this, we have analysed the cybersecurity engineering framework of ISO/SAE 21434 for gaps and deficiencies regarding TARA management and vulnerability and incident handling, as well as similar processes for incident handling in IT security.

We have also investigated intrusion detection systems and mechanisms for in-vehicle networks, and this work is closely related to WP5. Here we have focused on the usability with respect to resilience. A new type of intrusion detection system, *SPECTRA*, was developed, a system based on spectral analysis of CAN message payloads. It has been implemented and tested in a Volvo XC 60 vehicle and the results are very promising.

Even if vehicle-internal IDS systems are useful and necessary, it is not obvious that a vehicle can or should be trusted to evaluate its own state and decide whether it is fully functional. An internal IDS system may be failing to see the problem due to the sophistication of an attack, or the IDS system itself may be compromised. We have therefore taken a different approach to this problem to make sure misbehaving and compromised vehicles are detected and either fixed or removed from traffic. The methodology is based on peer assessment of vehicles, where vehicles assess each other after they have been interacting with each other and upload their verdicts to the cloud. This approach, "*A Trust-Based Vehicle to Cloud Anomaly Detection Framework*" makes it possible to verify vehicle behaviour and detect changes over a longer time and to follow each vehicle's behaviour. Changes do not necessarily have to do with cyber-attacks, but the system will also react to incorrect or unwanted behaviour by a vehicle that may call for software or hardware updates.

Reliable communication between vehicle and the infrastructure is essential for many functions. We have studied byzantine faults (or byzantine failures as some prefer to call it) in communication where components may silently fail or misbehave without being recognized by others. It affects for example consensus protocols and algorithms where two or more parties of components need to be in a known state. It is essential in many decisions made by communicating vehicles (V2X communication), but also inside a vehicle where decisions need to be made in a consistent way. Secure software updates can be one special case, where all or no ECUs should be updated at the same time. Other examples are fault tolerant components in the vehicle which may fail and require a, for the driver, invisible reconfiguration and reassignment of functions between ECUs and where it is essential that all involved parties agree on the change.

Having a secure software update process is essential to be able to guarantee a fully functional and resilient system design. Software updates should be possible to perform at any time using any type of network connection. We have created a unified software update framework, *UniSUF*, which should fulfil most demands for a versatile, flexible, and secure solution. We have also developed requirements for secure vehicle software updates by defining an attacker model and from there derived security requirements. The resulting framework can be used as a reference architecture to guide when designing software update systems, not only for vehicles but also for related areas such as cyber-physical systems, IoT devices and smart cities.

5.5 Deliverable D2.3

This deliverable, metrics for evaluating resilient designs, summarises the results from the activities performed in Task 2.3 Performance of resilient vehicle design. This task investigated possible metrics to quantify and evaluate the effectiveness (pros, cons, and performance implications) of a resilient vehicle design. This was done primarily by performing a literature study to find relevant metrics and measurements in use today in the context of resilience.

5.6 Deliverable D3.1

Intrusion detection is an old concept, but the security requirements vary with the increasing attack surface, especially in mobile networks involving vehicle communication. Machine learning-based intrusion detection solutions are gaining popularity because of faster detection and increased scalability for detecting intrusions. The intrusion detection solutions can be deployed as centralized, distributed, and federated solutions. To support a centralized intrusion detection solution for a fleet of vehicles, the generalizability of the ML-based intrusion detection solution is important. In this report, methods have been discussed using data pre-processing techniques to develop feature formats that can be implemented for each dataset. Also, it is identified that the frequency and time-based solutions can be useful when considering different in-vehicle network intrusion detection datasets. There are both shallow learning and deep learning models that can be leveraged to detect intrusions for vehicle networks. There is a trade-off in detection performance and the training time for different models. More complex models may perform better than less complex models, but they usually take longer to train. We have studied a number of publicly available datasets for the ML-based intrusion detection implementation. The decisions of the more complex models are also difficult to interpret and explain. There are multiple tools, such as IBM's AIX360 that provide techniques to enable interpretation of ML-based models based on data point characteristics. We have investigated some techniques to explore feature importance and sub-model importance to associate interpretability and explainability of the intrusion detection models used for vehicle networks. The methods are comparable to well-known explainable AI techniques such as LIME in terms of intrusion detection feature importance. This is an ongoing work and will be further investigated in the future with other standard techniques, such as SHAP, counterfactual reasoning to provide better interpretability of the intrusion detection models that will be deployed for V2X and cloud-based vehicular networks.

5.7 Deliverable D3.2

In this deliverable, we analysed different approaches to intrusion detection for detecting security threats within the vehicle. We investigated what types of security issues these mechanisms could detect, and where they fall short (or can be bypassed). Given that these security mechanisms may run locally inside the vehicle where resources can be limited, we also investigated how constraints on memory and computation power could affect the IDS accuracy. For this, we looked more closely at the frequency-based data aggregation approach from phase 1 deliverable D3.1. Our experiments showed that these limitations do in fact affect the accuracy of the solution, although it may be possible to find a good balance between accuracy and footprint.

The main focus has been on IDS technologies based on machine learning, and that proper training data has been recognized as a very critical ingredient. The key findings of the work can be described as follows:

- An exploration into the robustness and susceptibilities of four Machine Learning (ML) based Intrusion Detection Systems (IDSs) in automotive networks, particularly in relation to model evasion attacks executed with adversarial samples.

- Formulation of various feature selection strategies for the creation of adversarial samples, tailored to three distinct scenarios.
- An examination of the enhancement in performance and resilience against evasion attacks when ML-based IDSs are trained using adversarial samples.
- An emphasis on the existing limitations of ML-based IDSs that require attention in future IDSs, considering security and safety implications.
- Introduction of a systematic approach for evaluating intrusion detection datasets for automotive systems.
- Assessment of several available automotive IDS datasets using the proposed evaluation method.
- Identification of areas that necessitate improvements in future datasets.

Given the above findings, we conclude that the currently available solutions may not be sufficient and should be improved and augmented with other mechanisms or security technologies.

5.8 Deliverable D3.3

This deliverable reports on the work of identifying suitable resilience mechanisms for implementation in vehicular systems. An analysis has been conducted of 17 security mechanisms and 16 safety mechanisms to identify which of them that may be useful for such an implementation. Four security mechanisms and six safety mechanisms were found to be of interest; thus we assessed the general characteristics as well as dependability and security attributes of these mechanisms. The security mechanisms are (i) intrusion detection/prevention systems, (ii) virus/malicious code detection systems, (iii) Host Configuration Management (HCM) and Automated Software Management (ASM) tools, and (iv) operating systems. The safety mechanisms are (i) majority voting, (ii) software diversity, (iii) checksums/codes, (iv) substitute values, (v) reconfiguration, and (vi) reset.

As part of the assessment of the safety and security mechanisms identified, we studied and used a layered resilience framework and extended an attack–intrusion–compromised system chain model. The analysed security mechanisms can be of either protective, detective, or handling nature, and the framework and model are extended to describe these states. This model was used to identify the ten handling mechanisms which may be suitable resilience mechanisms in vehicles.

While all threat types represented by the STRIDE threat model are typically mitigated by the security mechanisms, safety mechanisms tend to mainly handle tampering threats. The analysis also shows that most mechanisms improve dependability and security, but some mechanisms also have negative impact, most notably Intrusion Prevention Systems (IPS:es) action on false positives (FPs).

5.9 Deliverable D3.4

Deliverable 3.4 introduces a framework to facilitate a Vehicular Hybrid Intrusion Detection System (HIDS). Within this framework, we have compiled a list of security events derived from prevalent technologies and services found in modern vehicles. Additionally, we have identified the components constituting the HIDS framework, detailing their communication procedures, interrelationships, and specific prerequisites. Furthermore, we have included several practical use cases to illustrate the application of the HIDS in real-world scenarios.

5.10 Deliverable D4.1

Deliverable 4.1 comprises two publications [17,18] and a master's thesis report [19]. Considering the lack of established guidelines and mechanisms in Automotive Digital Forensics (ADF), our primary focus was exploring existing literature in this field, identifying gaps and challenges, and proposing potential solutions. In the first publication [17], we addressed the following research questions.

What research exists within the field of automotive digital forensics? What is the coverage and specificity in different databases for automotive forensics search queries? What technical solutions exist concerning automotive digital evidence, and how do these solutions uphold security properties? What forensically relevant data can be derived from existing literature, and who are the stakeholders for this data?

Our investigation spanned four major databases, categorizing findings into technical solutions and surveys. We further segmented papers based on their content, linking technical solutions to their corresponding security properties. Moreover, we organized and correlated forensic data from these papers with security properties and targeted user groups. We also emphasized challenges, issues, and research gaps in this domain. Our aim was to provide guidance for ADF, assisting stakeholders such as law enforcement and automotive manufacturers. Additionally, our work aims to offer guidance for integrating forensic mechanisms into vehicle design as well as future research in this field.

In the second publication [18], we identified a threat model with the six threat actors as stated in [20]. We assume they mutually aim to execute diverse cybercrimes aimed at vehicles, potentially impacting the driver, passengers, and surrounding objects by exploiting the vehicle itself. Nevertheless, the primary goal remains concealing, erasing, or altering digital evidence, including traces of criminal activities, to impede or halt forensic investigations. We defined six high-level Automotive Digital Forensics Goals (ADFG) and mapped them to detailed forensics requirements to ensure coverage. Finally, considering the threat model, ADFG, and requirements, we proposed a reference architecture for ADF. This architecture can serve as a blueprint for designing digital forensic-enabled vehicles and similar systems.

The master thesis project [19] further investigated current practices in ADF through a literature review of digital forensics techniques and a categorization based on the Technology Readiness Level (TRL). The analysis aimed to pinpoint deficiencies in existing ADF solutions. Given the identified deficiencies, the project proposes an approach based on blockchain and CASE for ADF aligned with the stated CIANP model from [17].

Thus, in summary, deliverable 4.1 contributes to identifying the state of the art and challenges within the field of ADF via a systematic literature review [17], a reference architecture for ADF [18], and an approach for ADF based on blockchain and CASE [19].

5.11 Deliverable D4.2

Virtualisation is a vital part of many industries' software deployment. When virtualisation became popular, it was more or less synonymous with virtual machines and hypervisors. Since then, a newer form of virtualisation has surged in popularity, containers. Containers provide improvements over traditional hypervisors in several aspects, with lower overhead and short boot and shutdown times often being referenced.

Container-based virtualization supports continuous development and improves the efficiency and reliability of run-time environments. The first problem addressed in this deliverable is that different techniques have been proposed for monitoring the security of containers. However, there are no guidelines supporting the selection of suitable techniques for the tasks at hand. We have therefore worked with the selection and design of techniques for monitoring container-based virtualization environments and reviewed the literature and identified techniques for monitoring containerized environments.

Further, we have classified these techniques according to a set of categories, such as technical characteristic, applicability, effectiveness, and evaluation and further detailed the pros and cons that are associated with each of the identified techniques. The result is CONSERVE, a multi-dimensional decision support framework for an informed and optimal selection of a suitable set of container monitoring techniques to be implemented in different application domains. A mix of eighteen researchers and practitioners evaluated the ease of use, understand-ability, usefulness, efficiency, applicability, and completeness of the framework. The evaluation shows a high level of interest and points out to potential benefits.

Due to the way containers operate, they do not achieve the same level of isolation, an essential attribute in security. Containers share kernel with the host and other containers running on the host. A shared kernel means the attack surface differs from hypervisors, causing an elevated need for proper monitoring and investigation of potential monitoring techniques for detecting attacks, threats or misbehaving containers. We have performed a study that aims to understand what container monitoring techniques are available and how they operate. It explores novel container monitoring techniques providing better efficiency and coverage of the STRIDE threat model. As a result, a container monitoring technique has been created and refined over four iterations. This technique uses the Isolation Forest algorithm to detect anomalies in system call traces. The Isolation Forest algorithm enables unsupervised anomaly detection while providing multiple advantageous characteristics in terms of efficiency and detection. In order to evaluate and compare the proposed monitoring technique with other techniques, a framework was developed to support the use of different anomaly detection and feature extraction algorithms, streamlining the evaluation process. The resulting technique detects all attacks included in the evaluation while keeping an average FPR below 3%.

We have also designed and evaluated a framework for collaborative intrusion detection (CIVID) with the stated goal of increasing detection accuracy. The validation of the collaborative framework shows a marginal increase in accuracy measures through the utilization of a collaborative intrusion detection approach. However, the results also show that the implementation of CIVID yields increased time-to-detection of security events that require consultation.

5.12 Deliverable D5.1

Deliverable 5.1 consists of the findings and the analysis associated with Task 5.1. The purpose of this task was to conduct a survey on the state of the art in Verification and Validation (V&V) and to investigate the strategies suggested and/or required by different standards in several industries such as automotive, aeronautics, medical, manufacturing, etc.

In D5.1, we investigated V&V as an important step of the product development lifecycle and analysed how it relates to the V-model and the Agile methodology. After enumerating different system design metrics impacting V&V from a cost, effort, and resource perspective, we conducted a systematic literature review on the existing V&V techniques such as formal methods, fault/attack injection, simulation, testing, etc. and categorized them into two groups of test-based and non-test-based verification methodologies. As V&V is still vastly conducted by means of testing, we also studied different testing levels (unit, integration, system, and acceptance) and performed a mapping between these testing levels and the V&V techniques. In addition, we surveyed several standards and best practices in the Automotive, Avionics and Aerospace, Defence, Medical, Software development, Manufacturing industry and Critical sectors to identify their proposed V&V methods, frameworks, and guidelines. Additionally, we explored the limitations and constraints associated with each of the V&V techniques. The deliverable concluded by discussing which one(s) of the V&V techniques could be used to verify resilience in a vehicle architecture.

5.13 Deliverable D5.2

This deliverable (Safety and security interplay analysis using fault- and attack injection) presents the results and achievements of Task 5.2 (Interplay between safety and security using experimental verification and validation). The goal of this deliverable is to study the interplay between safety and security by investigating experimental verification and validation methods, such as fault- and attack injection, suitable for testing resilient vehicles. Two approaches are proposed to facilitate resilience testing using attack injection. The first approach is the exploration of multiple attack vectors by performing sequential attack injection experiments. The second approach is to use pre-injection analyses to facilitate resilience verification and validation by generating attack vectors that are more likely to explore the different resilience layers. The second approach is evaluated by analysing results from model-implemented attack injection campaigns performed on two separate automotive target systems using four different pre-injection analyses.

5.14 Deliverable D5.3

Deliverable 5.3 consists of the findings and the analysis associated with Task 5.3. The purpose of this task was to enumerate relevant security goals and requirements with respect to cyber-resilient design and implement proof of concepts by means of methods and tools to demonstrate the final proposed architectural principles for designing resilient vehicles.

In D5.3, we investigated the cyber security requirements and design principles for a cyber-resilient architecture and mapped them to different stages of ISO/SAE 21434 standard. In addition, we evaluated all the use cases by conducting threat modelling and identified their resilience attributes. Since no prototype was developed during the project and consequently there was no actual physical testing, the PoC was conducted by means of an extended and comprehensive Threat Analysis and Risk Assessment (TARA) on a selected use case (GNSS) by means of the STRIDE methodology as one of the most prominent threat modelling methodologies in the automotive industry. Lastly, we mapped the operational cycles of a vehicle (Normal, Faulty, Degraded) to different phases of cyber resilience (Prevention, Detection, Response and Recovery) and explained how a resilient vehicle transitions from one mode to another during a cyber-attack. The deliverable concluded with how a combination of Verification and Validation (V&V) techniques in addition to TARA should be used to test a resilient design and verify the fulfilment of the security requirements.

6 Dissemination and publication

6.1 Knowledge- and result dissemination

How is/will the project result (be) used and disseminated?	Mark with X	Comment
Increase knowledge in the area	X	The non-confidential publications and research are made available through AutoSec[2].
Transfer to other advanced engineering development projects	X	The consortium plans to build on the results in future projects.
Transfer to product development projects	X	The commercial partners are feeding the information back into the product development of either themselves or their customers.
Be introduced on the market		
Be used in Investigations/ Regulations/Permit matters/Political decision making		

CyReV is a part of a series of projects on **automotive** cyber security.

6.2 Publications

Most publications are also available at https://autosec.se/cyrev-results/ and at https://research.chalmers.se.

[2] https://autosec.se/cyrev-results/

- Ph.D. Thesis: T. Rosenstatter, “On the Secure and Resilient Design of Connected Vehicles: Methods and Guidelines”. Ph.D. thesis, Chalmers University of Technology, 2021. https://research.chalmers.se/publication/526019
- Ph.D. Thesis: Tuma, Katja, “Efficiency and Automation in Threat Analysis of Software Systems”. 2021. PhD Thesis. University of Gothenburg and Chalmers University of Technology, Sweden. https://research.chalmers.se/en/publication/520907
- Licentiate Thesis: K. Strandberg, “Towards a Secure and Resilient Vehicle Design: Methodologies, Principles and Guidelines”. 2022. Licentiate Thesis. Chalmers University of Technology, Sweden. https://research.chalmers.se/publication/529239
- D. Grimm, A. Lautenbach, M. Almgren, T. Olovsson. ” Gap analysis of ISO/SAE 21434 – Improving the automotive cybersecurity engineering life cycle”, 2023 IEEE 26th International Conference on Intelligent Transportation Systems (ITSC) (ITSC 2023).
- A. Lautenbach, M. Almgren, T. Olovsson. ” Proposing HEAVENS 2.0 – an automotive risk assessment model”, Proceedings - Computer Science in Cars Symposium (CSCS ’21): ACM Computer Science in Cars Symposium, 9781450391399 (ISBN)
- T. Rosenstatter, C. Englund (2017) “Modelling the Level of Trust in a Cooperative Automated Vehicle Control System”. IEEE Transactions on Intelligent Transportation Systems, 19(4) pp. 1237-1247.
- T. Rosenstatter, K. Strandberg, R. Jolak, R. Scandariato, T. Olovsson. “REMIND: A Framework for the Resilient Design of Automotive Systems”, 2020 IEEE Secure Development (SecDev),; (2020) p. 81-95
- T. Rosenstatter, T. Olovsson, M. Almgren, “V2C: A Trust-Based Vehicle to Cloud Anomaly Detection Framework for Automotive Systems”, Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 2021), (2021) p. 1-10
- K. Strandberg, T. Rosenstatter, R. Jolak, N. Nowdehi and T. Olovsson, "Resilient Shield: Reinforcing the Resilience of Vehicles Against Security Threats," 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), 2021, pp. 1-7, doi: 10.1109/VTC2021-Spring 51267.2021.9449029.
- K. Strandberg, N. Nowdehi, and T. Olovsson. “A Systematic Literature Review on Automotive Digital Forensics: Challenges, Technical Solutions and Data Collection”. In: IEEE Transactions on Intelligent Vehicles 8.2 (2023), pp. 1350–1367. doi: 10.1109/TIV.2022.3188
- K. Strandberg, U. Arnljung, and T. Olovsson. “The Automotive BlackBox: Towards a Standardization of Automotive Digital Forensics”. In: IEEE International Workshop on Information Forensics and Security 2023. 1556-6013 (ISSN)
- K. Strandberg, D. K. Oka, T. Olovsson. ” UniSUF: A unified software update framework for vehicles utilizing isolation techniques and trusted execution environments”, 19th ESCAR Europe conference 2021, pp. 86-100, https://www.escar.info/history/escar-europe/escar-europe-2021-lectures-and-program-committee.html
- K. Strandberg, Ulf Arnljung, Tomas Olovsson, and Dennis Kengo Oka, “Secure Vehicle Software Updates: Requirements for a Reference Architecture,” IEEE 97th Vehicular Technology Conference (VTC2023-Spring), 2023
- W. Aoudi, M. Almgren, N. Nowdehi, T. Olovsson. “Spectra: Detecting Attacks on In-Vehicle Networks through Spectral Analysis of CAN-Message Payloads”, Proceedings of the ACM Symposium on Applied Computing, SAC ’21, March 22–26, 2021, pp. 1588-1597, ISBN 9781450381048
- Behrooz Sangchoolie, Peter Folkesson, Pierre Kleberger, Jonny Vinter, “Analysis of Cybersecurity Mechanisms with respect to Dependability and Security Attributes,” 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), 2020.
- Conference presentation video: CyReV Videos: CyReV phase 1 and 2/WPs/WP3/Analysis of Cybersecurity Mechanisms with respect to Dependability and Security Attributes.mp4.

- Joakim Rosell, Cristofer Englund, Arash Vahidi, Nishat I Mowla, Ana Magazinius, Eric Jarpe, “A Frequency-based Data Mining Approach to Enhance in-vehicle Network Intrusion Detection”, Fast Zero´21, Society of Automotive Engineers of Japan, 2021.
- Nishat I Mowla, Joakim Rosell, Arash Vahidi, “Dynamic Voting based Explainable Intrusion Detection System for In-vehicle Network”, International Conference on Advanced Communication Technology (ICACT), IEEE, 2022.
- R. Jolak, T. Rosenstatter, M. Mohamad, K. Strandberg, B. Sangchoolie, N. Nowdehi, R. Scandariato, “CONSERVE: A framework for the selection of techniques for monitoring containers security,” Journal of Systems and Software, p.111158, 2021.
- R. Jolak, T. Rosenstatter,, S. Aldaghistani, R. Scandariato. (2022) RIPOSTE: A Collaborative Cyber Attack Response Framework for Automotive Systems. In submission to EuroMicro SEAA.
- O. Lundström, M. Raynal, E. Schiller. ” Brief Announcement: Self-stabilizing Total-Order Broadcast”, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 13751 LNCS s. 358-363, 9783031210167 (ISBN)
- R. Duvignau, M. Raynal, E. Schiller, “Self-stabilizing Byzantine Fault-Tolerant Repeated Reliable Broadcast”, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 13751 LNCS s. 206-221, 9783031210167 (ISBN)
- C. Georgiou, M. Raynal, E. Schiller: “Self-stabilizing Byzantine-Tolerant Recycling”. 25th International Symposium on Stabilization, Safety, and Security of Distributed Systems, SSS 2023, Jersey City, USA.
- L. Sion, K. Tuma, R. Scandariato, K. Yskout, W. Joosen, “Towards Automated Security Design Flaw Detection'', International Conference on Automated Software Engineering Workshop (ASEW). IEEE, 2019.
- K. Tuma, C. Sandberg, U. Thorsson, M. Widman, T. Herpel, R. Scandariato, “Finding Security Threats That Matter: Two Industrial Case Studies'', in submission to Journal of Systems and Software (JSS), 2020
- P. Folkesson, B. Sangchoolie, P. Kleberger and N. Nowdehi, "On the Evaluation of Three Pre-Injection Analysis Techniques for Model-Implemented Fault- and Attack Injection," 2022 IEEE 27th Pacific Rim International Symposium on Dependable Computing (PRDC), Beijing, China, 2022, pp. 130-140, doi: 10.1109/PRDC55274.2022.00027.
- P. Kleberger, P. Folkesson, and B. Sangchoolie. “An Integrated Safety and Cybersecurity Resilience Framework for the Automotive Domain”. In: CARS - 7th International Workshop on Critical Automotive Applications: Robustness & Safety. 2022
- A. Farooqui and B. Sangchoolie. “Towards Formal Fault Injection for Safety Assessment of Automated Systems”. In: Proceedings of Fifth International Workshop on Formal Methods for Autonomous Systems (FMAS 2023). 2023
- Book chapter: D. Dubrefjord, M. Jang, H. Hadi, T. Olovsson, “Security of In-Vehicle Communication Systems”. Chapter in Decision Support Systems and Industrial IoT in Smart Grid, Factories, and Cities, 2021, p. 162-179, ISBN: 9781799874683
- Zenden, I., Wang, H., Iacovazzi, A., Vahidi, A., Blom, R., and Raza, S. (2023). On the Resilience of Machine Learning-Based IDS for Automotive Networks. Proc of IEEE Vehicular Networking Conference, VNC, 239–246.
- Arash Vahidi, Thomas Rosenstatter, and Nishat I Mowla. 2022. Systematic Evaluation of Automotive Intrusion Detection Datasets. In *Computer Science in Cars Symposium (CSCS ’22), December 8, 2022, Ingolstadt, Germany*. ACM, New York, NY, USA, 12 pages.
- H. Lundberg *et al*., "Experimental Analysis of Trustworthy In-Vehicle Intrusion Detection System Using eXplainable Artificial Intelligence (XAI)," in *IEEE Access*, vol. 10, pp. 102831-102841, 2022, doi: 10.1109/ACCESS.2022.3208573.

- Master thesis: Desai, Deepak, and Burkin Günke. "Attacker Identification Using Low-Level Characteristics of Automotive ECUs." (2020). https://hdl.handle.net/20.500.12380/304467
- Master Thesis: RefiningCMT: Lindvärn, M., & Lundqvist, Z. “Refining Security Monitoring Techniques for Container-Based Virtualisation Environments”. Chalmers University of Technology 2021. https://hdl.handle.net/20.500.12380/302758
- Master Thesis: CIVID: Aryan, D., & Söderberg, K. “CIVID-Collaborative In-vehicle Intrusion Detection”. Chalmers University of Technology 2021 https://hdl.handle.net/20.500.12380/302485
- Master Thesis: M. Folkemark, V. Rydberg, “Performance Evaluation of a Hardware Security Module in Vehicles”, Chalmers University of Technology 2021. https://hdl.handle.net/20.500.12380/304467
- Master Thesis: E. Andreasson, I. Lyesnukhin, “Device Attestation for In-vehicle Network”, Chalmers University of Technology 2022. https://odr.chalmers.se/handle/20.500.12380/305865
- Master Thesis: J. Kristoffersson: “Zero Trust in Autonomous Vehicle Networks Utilizing Automotive Ethernet”, Chalmers University of Technology 2022.

  https://odr.chalmers.se/handle/20.500.12380/305856
- Master Thesis: Y. Dong and J. Zhang. “Master’s thesis: Digital Forensic Investigation of Automotive Systems: Requirements and Challenges”. In: Chalmers Open Digital Repository Chalmers University of Technology 2023. http://hdl.handle.net/20.500.12380/307308
- Master Thesis: E. Eriksson and L. Fahlbeck. “Master’s thesis: Investigating the Use of Honeypots in Vehicles”. In: Chalmers Open Digital Repository Chalmers University of Technology 2022. https://odr.chalmers.se/handle/20.500.12380/305879
- Master Thesis: H. Sultani and L. Han. “Master’s thesis: Indicators of Compromise of Vehicular Systems”. In: Chalmers Open Digital Repository Chalmers University of Technology 2019. https://hdl.handle.net/20.500.12380/300607
- Master Thesis: Ivo Zenden. The Resilience of Deep Learning Intrusion Detection Systems for Automotive Networks: The effect of adversarial samples and transferability on Deep Learning Intrusion Detection Systems for Controller Area Networks, 2022. https://kth.diva-portal.org/smash/record.jsf?pid=diva2:1710612
- Master Thesis: Lundberg, H. (2022). Increasing the Trustworthiness of AI-based In-Vehicle IDS usingeXplainable AI (Dissertation). Retrieved from https://urn.kb.se/resolve?urn=urn:nbn:se:miun:diva-45223

7 Conclusions and continued research

The overall goal of the project has been to identify mechanisms and solutions for building cyber-**resilient** vehicles, which has been met. We have gained new knowledge about cyber-resilient systems and have identified tools and mechanisms useful in resilient designs. An important insight is the understanding of the width and complexity of the problem, and this project has enabled us to take important steps toward a better understanding, even if more work is needed before we fully master the area. Traditional safety design for vehicles has taken many years to master. Similarly, cyber-security, which is a moving target, also needs time to reach maturity. New and more effective techniques will be developed in the coming years and the architecture of vehicles needs to evolve before we can fully deal with cyber-security threats and requirements.

Resilience is a complicated area where the right decisions must be taken by vehicles at all times. As part of WP2, we have performed extensive literature reviews and categorized mechanisms and techniques based on the problem they address. This work is an enabler for continued research in the field and is also important for engineers who need to find solutions to particular problems they face today. Moreover, we have identified a set of metrics that could be used to measure resiliency of systems.

Four security handling mechanisms were found to be useful for implementation in resilient vehicles as a part of WP3: (i) intrusion detection/prevention systems, (ii) virus/malicious code detection systems, (iii) Host Configuration Management (HCM) and Automated Software Management (ASM) tools, and (iv) operating systems. The safety mechanisms are (i) majority voting, (ii) software diversity, (iii) checksums/codes, (iv) substitute values, (v) reconfiguration, and (vi) reset.

We investigated a number of different approaches to intrusion detection and prevention systems in automotive settings in WP3 and demonstrated how such solutions can be used to detect certain security issues. However, a few shortcomings were also uncovered during this investigation, including coverage in terms of attack heterogeneity, detection performance, robustness, and explainability issues - which we plan to investigate more in the future.

Due to the increased complexity and extended connectivity in vehicles, there is an increased risk of cyber attacks and other criminal incidents, requiring more research on automotive digital forensics. Thus, under WP4, we performed a systematic literature review within this field and identified and assessed over 300 publications. Relevant publications were further categorized and provided a comprehensive overview of the forensics field to guide practitioners and researchers. A reference architecture was also proposed for automotive digital forensics for guidance, considering the architectural design of forensically enabled vehicles.

Experimental evaluation of four pre-injection analyses (inject-on-read, inject-on-write, error space pruning of signals, and error space pruning of signals and ports) to facilitate testing of resilient vehicles were performed as a part of WP5. The results show that a reduction of the attack space between 27% and 54% can be achieved. More work is needed to analyse the advantages/disadvantages of the pre-injection techniques proposed. Additional pre-injection techniques, e.g., utilizing exploration of equivalent fault- and attack classes, as well as sequential attack injection utilizing analytical methods such as attack trees and vulnerability analyses should also be investigated.

8 Participating parties and main contact points

VOLVO

Volvo Car Corporation (Kim Strandberg, kim.strandberg@volvocars.com)

RI.
SE

RISE Research Institutes of Sweden (Behrooz Sangchoolie, behrooz.sangchoolie@ri.se)

VOLVO

Volvo Technology (Christian Sandberg, christian.sandberg@volvo.com)

COMBITECH

Combitech AB (Reza Esmaeili, reza.esmaeili@combitech.com)

Chalmers University of Technology (Tomas Olovsson, tomas.olovsson@chalmers.se)

9 References

[1] Cyrev Fas 1, https://www.vinnova.se/p/cyrev-fas1---datasakerhet-for-fordonssystem-i-en-foranderlig-miljo/: 2023-12-07.

[2] FFI project HEAVENS, https://www.vinnova.se/en/p/heavens-healing-vulnerabilities-to-enhance-software-security-and-safety/, Accessed: 2024-02-26

[3] ISO/SAE 21434, Road Vehicles - Cybersecurity engineering. ISO, Standard.

[4] ISO 26262 Road vehicles-functional safety, ISO, Standard.

[5] E-Safety Vehicle Intrusion Protected Applications (EVITA), https://www.evita-project.org/, accessed: 2018-12-10.

[6] FFI project HoliSec https://www.ri.se/en/what-we-do/projects/holistic-approach-improve-data-security-vehicles, Accessed: 2018-12-05

[7] Alheeti, K. M. A., Gruebler, A., McDonald-Maier, K. D. (2016). An Intrusion Detection System against Black Hole Attacks on the Communication Network of Self-Driving Cars. In Proceedings -2015 6th International Conference on Emerging Security Technologies, EST 2015. https://doi.org/10.1109/EST.2015.10

[8] Levi, M., Allouche, Y., Kontorovich, A. (2018). Advanced Analytics for Connected Car Cybersecurity. In IEEE Vehicular Technology Conference. https://doi.org/10.1109/VTCSpring.2018.8417690

[9] Rosenstatter, T., Englund, C. (2017) Modelling the Level of Trust in a Cooperative Automated Vehicle Control System. IEEE Transactions on Intelligent Transportation Systems, 19(4) pp. 1237-1247.

[10] Sangchoolie, Behrooz, Peter Folkesson, and Jonny Vinter. "A study of the interplay between safety and security using model-implemented fault injection." 2018 14th European Dependable Computing Conference (EDCC). IEEE, 2018.

[11] P. Kleberger, P. Folkesson, and B. Sangchoolie. “An Integrated Safety and Cybersecurity Resilience Framework for the Automotive Domain”. In: CARS - 7th International Workshop on Critical Automotive Applications: Robustness & Safety. 2022

[12] United Nations. UN Regulation No. 155. https://unece.org/sites/default/files/2021-03/R155e.pdf. Accessed: 2023-12-12. 2022

[13] P. Folkesson, B. Sangchoolie, P. Kleberger and N. Nowdehi, "On the Evaluation of Three Pre-Injection Analysis Techniques for Model-Implemented Fault- and Attack Injection," 2022 IEEE 27th Pacific Rim International Symposium on Dependable Computing (PRDC), Beijing, China, 2022, pp. 130-140, doi: 10.1109/PRDC55274.2022.00027.

[14] FFI project CASUS https://www.chalmers.se/en/projects/Pages/CASUSQ-Building-Security-Assurance-Cases-in-Automotive-Open.aspx, Accessed: 2018-12-05

[15] ThreatMove, https://www.vinnova.se/p/threat-move-hotmodellering-och--simulering-for-fordons-it/, accessed: 2024-02-27

[16] Svenningsson, Rickard, et al. "MODIFI: a MODel-implemented fault injection tool." International Conference on Computer Safety, Reliability, and Security. Springer, Berlin, Heidelberg, 2010.

[17] K. Strandberg, N. Nowdehi, and T. Olovsson. “A Systematic Literature Review on Automotive Digital Forensics: Challenges, Technical Solutions and Data Collection”. In: IEEE Transactions on Intelligent Vehicles 8.2 (2023), pp. 1350–1367. doi: 10.1109/TIV.2022.3188340

[18] K. Strandberg, U. Arnljung, and T. Olovsson. “The Automotive BlackBox: Towards a Standardization of Automotive Digital Forensics”. In: IEEE International Workshop on Information Forensics and Security (2023)

[19] Y. Dong and J. Zhang. “Master’s thesis: Digital Forensic Investigation of Automotive Systems: Requirements and Challenges”. In: Chalmers Open Digital Repository (2023)

[20] K. Strandberg, T. Rosenstatter, Rodi Jolak, Nasser Nowdehi, and Tomas Olovsson. “Resilient Shield: Reinforcing the Resilience of Vehicles Against Security Threats”. In: IEEE 93rd Vehicle Technology Conference, 2021