#78 SPECTRUM

Dear readers,

Software plays a key role in today's mobility. In addition to sustainable propulsion technologies, software-based innovations will be crucial for the future. With our FEV.io brand, we have taken this technological trend into account and bundled our software competencies. The following pages will give you an insight into this software expertise, which we have established globally.

When it comes to automotive cybersecurity, for instance, we offer our customers a holistic approach. In this SPECTRUM, we will show you how we ensure that future vehicles comply with cybersecurity regulations and are optimally equipped against corresponding threats.

The need for updates and extensions to software-defined functions is also growing, for example in the vehicle type approval process. We present a virtual development and validation approach that enables specific homologation-relevant software updates and saves considerable time and costs.

We also give you an overview of the ADAS/AD services that we offer all year round at our test center in Morocco. In another article, we use the example of FEV.io in India to discuss the expansion of global software expertise in order to ensure the acceleration of innovations in the field of intelligent mobility.

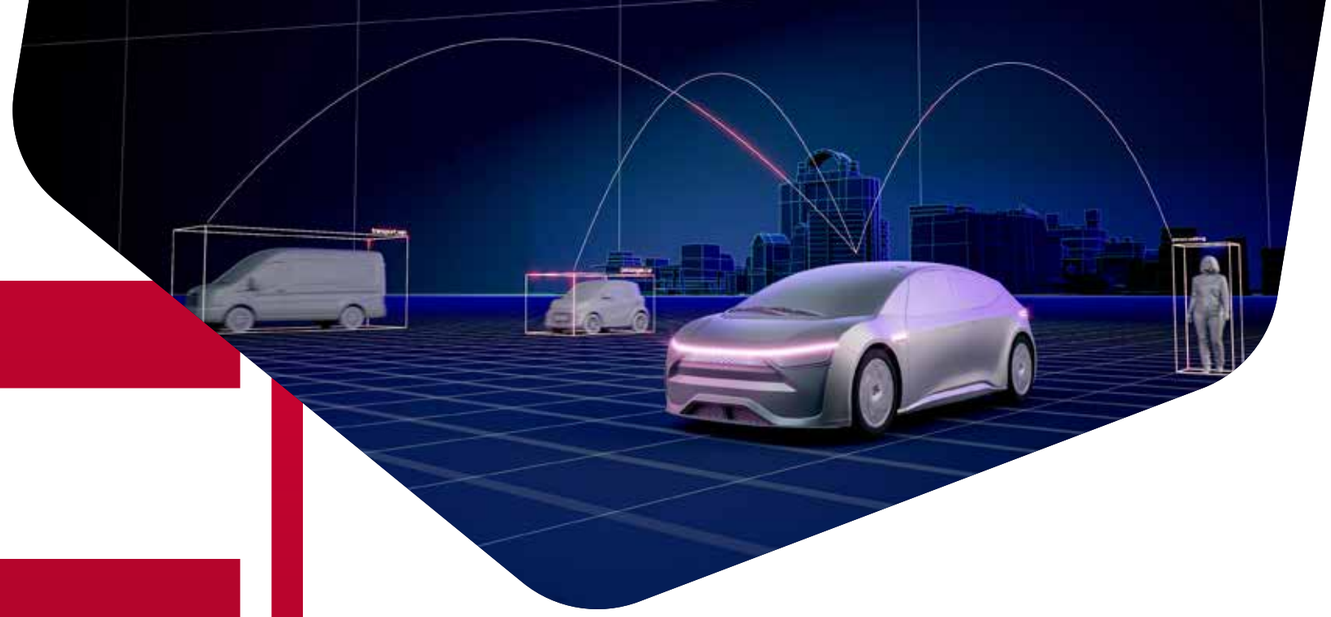
In addition to software solutions, FEV continues to stand for innovative solutions in complete vehicle development. As such, we will showcase FEV's "PD-HVX", a solution for detecting partial electrical discharge in high-voltage vehicle propulsion systems, which can prevent time-consuming and costly vehicle failures in the development process. Furthermore, we provide insights into a collaboration with Iveco, to develop a fully flexible and modular battery-electric platform for light commercial vehicles.

Finally, with the new "Proprietary Solutions" series, we underscore our "Feel EVolution" philosophy and present you with unique innovations that our experts have developed for specific current challenges.

I wish you an exciting and inspiring read.

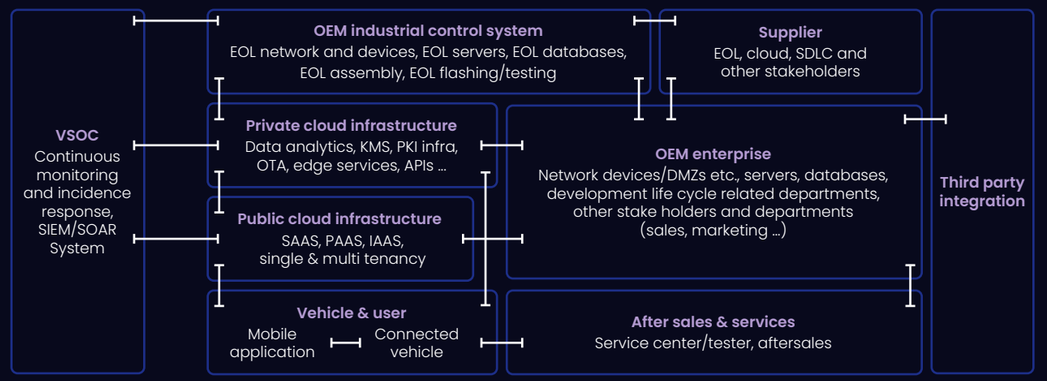
Dr. Norbert W. Alt
Chief Operating Officer (COO) and
Executive Vice President of FEV Group

CONTENT



#1 *FEV.io* – A reliable partner for *cybersecurity in the automotive industry*

The automotive industry is undergoing a transformation due to the rapid development of highly advanced technologies and complex software solutions. This transformation is particularly evident in the development of connected vehicles. Figure 1 illustrates the connected vehicle ecosystem showcasing the journey from Original Equipment Manufacturer (OEM) to user engagement. This ecosystem highlights the significance of cloud infrastructure in managing vehicle data, enabling over-the-air updates, and facilitating after-sales services. Third-party integrations extend the ecosystem's capabilities, ensuring a seamless user experience and continuous vehicle support.



1.
Automotive cybersecurity ecosystem.

»FEV.io has a systematic methodology that precisely identifies assets, threat scenarios and attack paths and evaluates potential risks.«

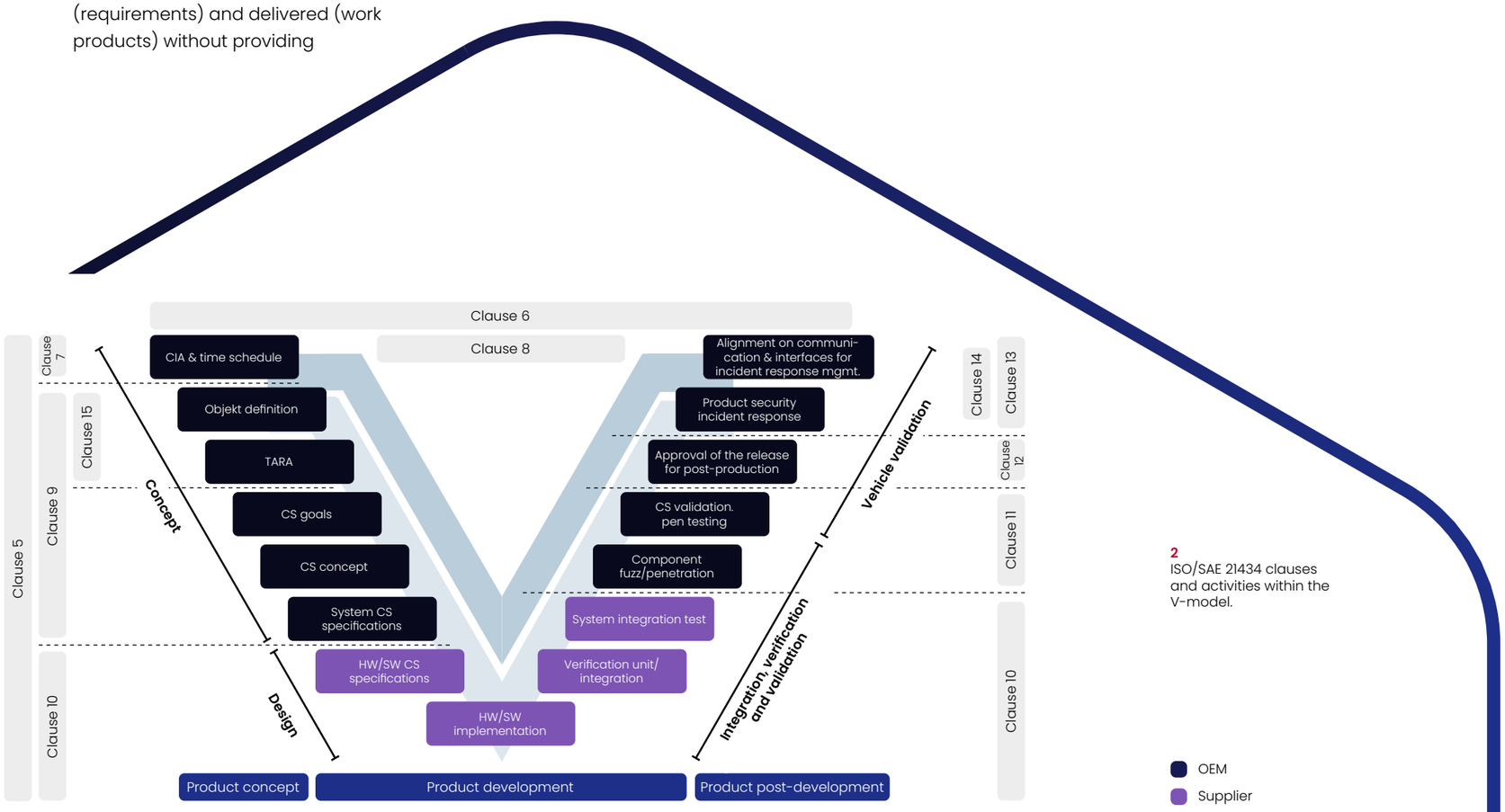
However, due to the introduction of advanced technologies and software solutions, modern vehicles have become vulnerable to threats that may compromise vehicle safety, data privacy, or the overall vehicle functionality.

Protecting modern vehicles from potential threat falls under the discipline of cybersecurity. Recognizing the need for standardized cybersecurity practices for the automotive domain, the International Organization for Standardization (ISO), in collaboration with SAE International, introduced ISO/SAE 21434 in 2021. ISO/SAE 21434 serves as one of the main references for OEMs and suppliers to comply with cybersecurity regulations, such as UNECE R155.

Implementing the requirements outlined in ISO/SAE 21434 can be challenging, particularly because the standard often specifies what shall be accomplished (requirements) and delivered (work products) without providing detailed guidance on how to do so. That's where FEV.io becomes an essential partner. With a team of experts, clients can be guided through the entire lifecycle, including performing security risk analysis, implementation of cybersecurity controls and requirements, and performing verification and validation activities.

ISO/SAE 21434 clauses and activities within the V-model

The ISO/SAE 21434 standard consists of 15 clauses describing cybersecurity activities, in terms of requirements and work products, from the concept phase to decommissioning. Additionally, ISO/SAE 21434 consists of cybersecurity management activities. Figure 2 illustrates how specific clauses and their corresponding activities from ISO/SAE 21434 are integrated into the V-model. This illustration provides a clear perspective on the distribution of cybersecurity activities across different phases and identifies the responsible stakeholders for such activities, whether OEMs or suppliers.



2
ISO/SAE 21434 clauses and activities within the V-model.

A systematic methodology for security risk analysis

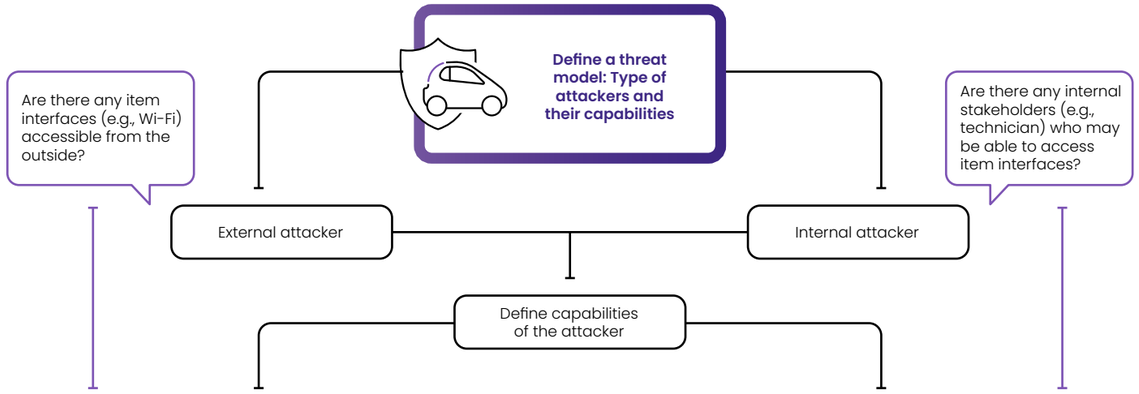
The concept phase is intricately linked with the principle of security-by-design. This principle focuses on incorporating security considerations (e.g., requirements and controls) into the system under analysis (a.k.a. item) right from the start. To this end, the concept phase consists of several activities, including performing a security risk analysis (often referred to as Threat Analysis and Risk Assessment or "TARA") of the item. TARA consists of seven activities, including identifying of

a. what needs to be protected (a.k.a. asset identification),

b. potential threats against the identified asset (a.k.a. threat scenario identification), and

c. actions performed by an attacker to realize a threat (a.k.a. attack path analysis).

Below, insights into how to carry out such activities are provided. FEV.io has a systematic methodology for performing TARA. The methodology aims to have a comprehensive set of assets. This set of assets consists of generic assets and specific assets. The former denotes assets that may be applicable to every Electronic Control Unit (ECU), such as software updates, and diagnostic routing. The latter denotes assets that are specific to the item under analysis, such as messages transmitted by communication channels relevant to the item. This process of identifying specific assets progresses from a broad, coarse-grained analysis where only a generic communication channel is identified as an asset, to a more detailed, fine-grained analysis where specific messages are identified. This fine-grained analysis leads to more practical solutions, focusing on protecting only a subset of the messages transmitted by a communication channel rather than the entire set; which could be impractical due to performance reasons.



3
Threat model-based approach.

For the identification of threat scenarios, our methodology incorporates a threat model-based approach, illustrated in Figure 3. A threat model consists of assumptions about which attackers are considered and their corresponding capabilities to compromise the item. After finalizing the threat model and obtaining customer approval, a team of experts seamlessly identifies threats and their corresponding attack surfaces from the threat model.

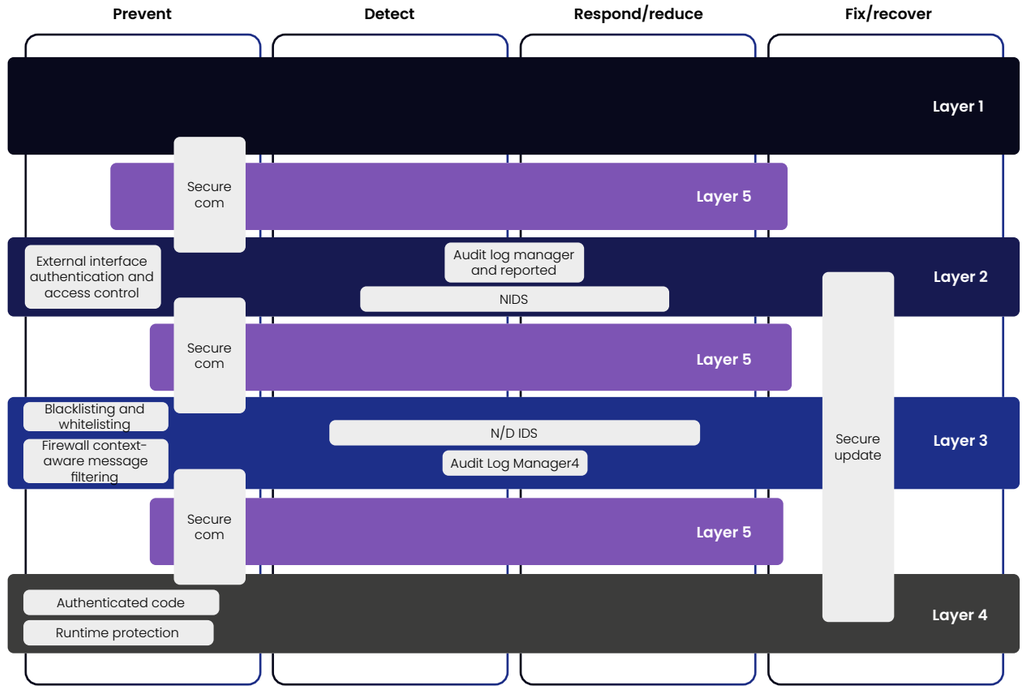
FEV.io leverages the threat model-based approach to facilitate the enumeration of attack paths for the identified threat scenarios. Based on the type of the attacker and their corresponding capabilities, we analyze the following questions by taking the system architecture as input information. The answer to such questions serves as the basis for describing the potential actions performed by an attacker.

- **How does the attacker reach the attack surface?**
- **How does the attacker proceed to reach the asset from the attack surface?**
- **How does the attacker proceed to violate the cybersecurity property of the asset?**

A significant advantage of describing attack paths based on such questions is the ability to customize recommendations for cybersecurity controls. These recommendations may be carefully deployed at one or more locations within the system architecture, such as the attack surface or any other suitable location utilized by the attacker to reach the asset.

Additionally, FEV.io proposes a Defense in Depth Strategy (DDS) depicted in Figure 4. This strategy showcases a cybersecurity architecture featuring layered defenses to protect information systems. Expertly designed, it incorporates secure communication, authenticated access, and intrusion detection to address threats. Context-aware firewalls and authenticated code execution enhance resilience, underlining the architecture's critical role in protecting against sophisticated cyber-attacks.

In summary, FEV.io has a systematic methodology for concept phase activities, which involves the precise identification of assets, threat scenarios, and attack paths. By employing this methodology, a thorough analysis is ensured, leading to the evaluation of potential risks. Consequently, FEV.io experts can make informed recommendations regarding cybersecurity goals, controls, and requirements aimed at reducing the identified risks.



4
FEV.io defense in depth strategy.

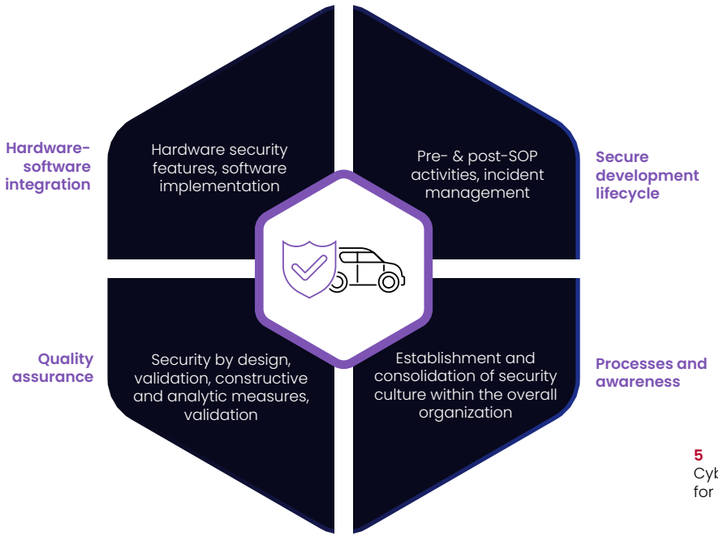
Securing the product development phase

Ensuring secure production involves the deployment of robust controls, such as secure boot and secure flashing. Secure boot utilizes cryptographic techniques to verify the authenticity of the software running on ECUs, thereby preventing the execution of any tampered software, whereas secure flashing guarantees that only legitimate and authenticated firmware updates are applied, thereby preventing spoofing attacks aimed at flashing malicious code into the item via unauthorized firmware updates. FEV.io is committed to developing such controls. For example, FEV.io has developed a unique boot mechanism using asymmetric cryptography, providing an additional layer of protection over traditional secure boot mechanisms without sacrificing the processing speed demanded by end-users of the product.

To enhance the security of in-vehicle networks and protect against potential breaches, FEV.io is dedicated to the development of robust mechanisms aimed at effectively managing the access to and usage of resources and data from the item under development. These mechanisms are often referred to as access control and usage control mechanisms. The former manages what actions users may perform and what resources they may access within the item. The latter manages how authorized users may interact with resources and data once they have gained access. The development of access and usage control mechanisms is essential to prevent several attacks, particularly usage control mechanisms prevent elevation of privileges attacks.

When it comes to the verification activities, FEV.io employs a dual approach to identify potential software issues. Firstly, statistic analysis tools are utilized to analyze the codebase without executing it, identifying potential bugs or malicious information flows. This approach is complemented with dynamic testing tools. Dynamic testing involves the execution of the software under different runtime environments, identifying potential runtime issues such as memory leaks or other issues that static testing might not identify.

FEV.io has a vast experience in performing validation activities. Customers and partners are glad to make use of several years of experience in performing fuzz and penetration testing. For example, in a former project, potential vulnerabilities were identified where fuzz testing played a pivotal role. During the testing phase, fuzz testing techniques detected a potential overflow vulnerability in a vehicle's CAN communication protocol. Upon discovering this vulnerability, corrective measures were immediately implemented, eliminating a significant liability and potential safety risk well before the vehicle went into production.



5
Cybersecurity framework for OEMs and Tier 1s.

Finally, FEV.io offers a cybersecurity strategy framework, depicted in Figure 5. It showcases the integration of hardware and software security, quality assurance through design and validation, and a secure development lifecycle. It emphasizes the importance of vigilance both before and after production, as well as the cultivation of a security-centric organizational culture.

The continuous commitment over post-product development

The FEV.io commitment to cybersecurity extends far beyond the concept and development phases. During the operation and maintenance phases, experts enable the protection of Over-The-Air (OTA) updates using encryption and digital signatures, ensuring software integrity and confidentiality. Intrusion detection systems continuously monitor the in-vehicle networks, swiftly identifying and responding to any potential threats. Regular security audits and checks ensure software continues to remain secure even after deployment.

Even during the decommissioning phase, FEV.io takes care to erase all data securely, preventing any misuse of residual private or proprietary information.

Conclusion

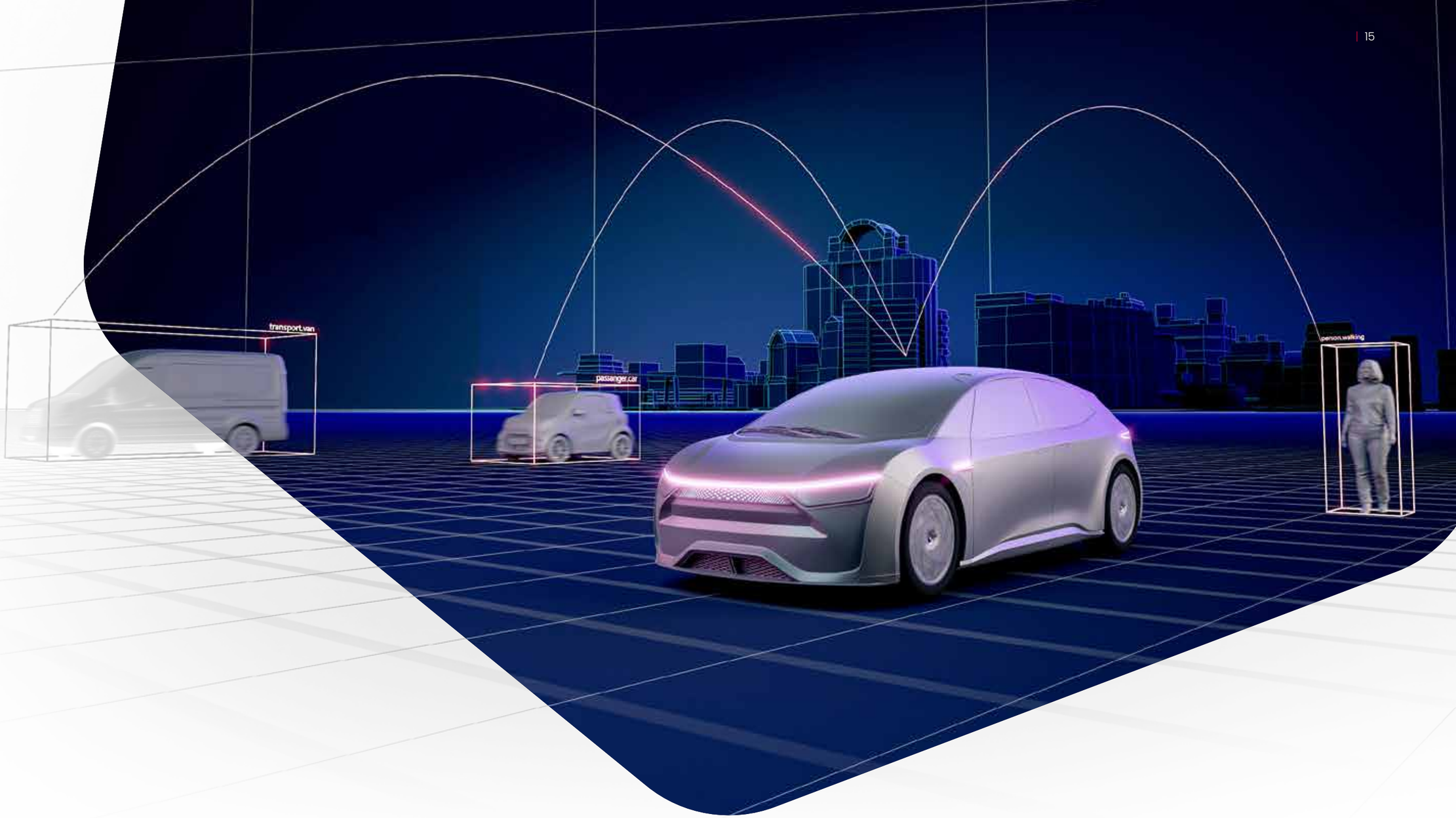
FEV.io offers a holistic approach to cybersecurity in the automotive industry, building on the company's extensive expertise across the entire cybersecurity lifecycle. This expertise, coupled with a systematic methodology and innovative developments, ensures that future vehicles not only comply with regulations, but are also optimally equipped against cybersecurity threats.

BY

Jagannath Tiwari,
tiwari_j@fev.com

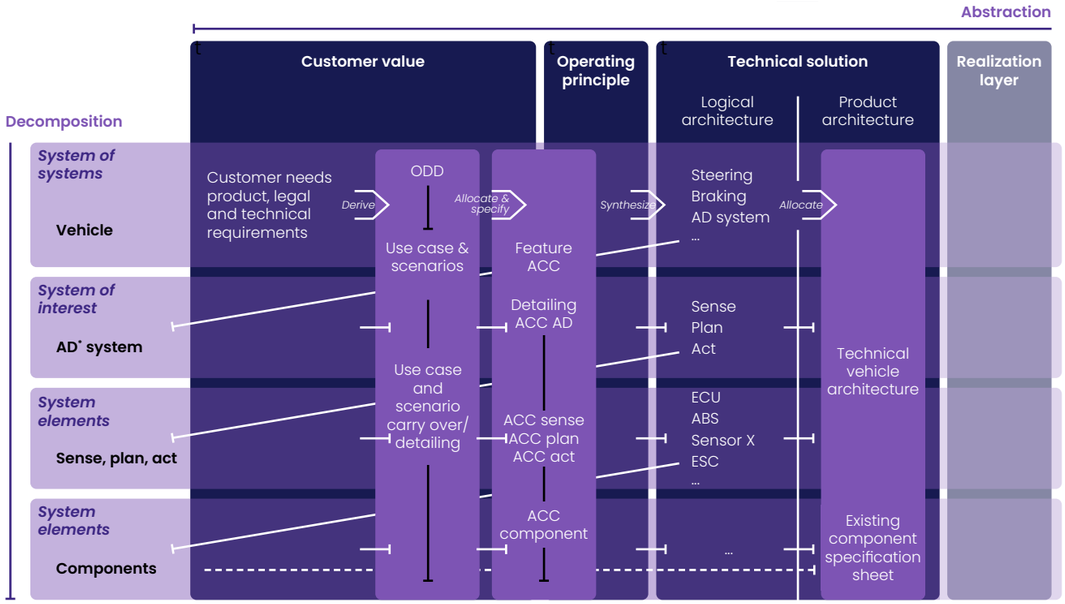
Yuri Gil Dantas,
dantas@fev.io

Matthias Rehberger,
rehberger@fev.io



#2
Acceleration of homologation-relevant ***software updates***

The growing scope of purely software-based functions in the vehicle is leading to an increasing need for Over-The-Air (OTA) software-defined function updates and enhancements throughout the vehicle life cycle. This also applies to software-defined functions that affect the vehicle type approval process. As a result, the homologation process is facing new challenges that aim to significantly reduce the high time and costs currently required to carry out software updates, especially safety-critical ones. The following describes a virtual development and validation approach that enables specific homologation-relevant software updates.



1.
FEV.io CUBE approach for model-based systems and software engineering.

* AD = Autonomous Driving

Bundled competencies

FEV.io has joined forces with Kontrol, dSPACE, TÜV SÜD, Microsoft Germany, T-Systems and Berylls to form the "Digital Loop" project group. They have set themselves the goal of developing a concept for a software-based virtual homologation process using extensive Over-the-Air (OTA) vehicle updates via mobile communications and establishing the virtual validation process as industry-wide accepted and recognized proof for the virtual homologation of software updates. This proof requires, among other things, complete traceability from the legal requirements, through the functional design, to the implemented software source code and the derived test cases for each software update. This fully digitized "digital loop" cycle offers vehicle manufacturers and approval authorities considerable advantages, as the scope of testing activities required in the real environment can be significantly reduced, saving both time and costs in type approval throughout the entire life cycle of a vehicle.

The basis of this approach is the simulation of real traffic scenarios using state-of-the-art simulation technology to achieve the required accuracy and reliability of the virtual environment for testing, validation, and approval. This virtual simulation environment is a comprehensive digital representation of the real world, based on highly detailed 3D models of roads, vehicles, pedestrians, weather conditions and other factors. The vehicle systems are stimulated with these simulations and their driving decisions are then evaluated.

Function-oriented approach

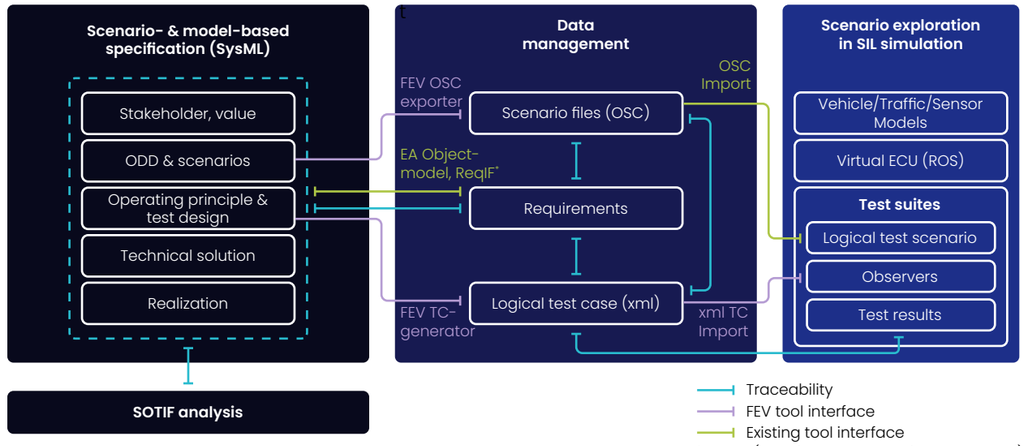
For the approval process of homologation-relevant software updates in the context of the Software Update Management (SUMS) regulation, traceability across all decomposition and abstraction levels - of all systems and subsystems, as well as across the entire development and life cycle of the product – is an essential component that can be subject to both temporal and spatial changes.

The "Digital Loop" approach addresses these requirements of the technical testing organization for this clear and unambiguous traceability of the effects of software updates on an already homologated system using the principles of Model-Based Systems Engineering (MBSE). The "Compositional Unified System-Based Engineering" (CUBE) methodology from FEV.io forms the basic framework for the requirements specification, product design, and implementation phases. The solution-neutral view of CUBE's function-driven approach fulfills the characteristics of current and future software-driven product development (Figure 1), and can be used in the development of all functional domains of the entire vehicle architecture. This is explained using an ADAS functional example in which the scenario-based development approach is also applied.

To enable scenario-based system design using MBSE, the intended Operational Design Domain (ODD) and the relevant scenarios of the ADAS function to be developed must be included in the specification model in addition to the classic requirements and use case specifications. An extension profile based on modeling languages (e.g. UML or SysML) with additional diagrams and model elements is used for modeling. Modeled scenarios must contain a machine-readable definition of the time-dependent interaction of the controlled vehicle and its environment, and include both logical scenarios with descriptions of the parameter spaces in the state space, as well as concrete scenarios for representatives of this state space.

When creating the specification model using the CUBE approach, all elements of the model are related and specified across all levels of abstraction, starting at the top decomposition level. This process is systematically repeated for the subsequent decomposition levels down to the level of the individual component (e.g. ECU) and results in an extended system and software specification. This includes more detailed traceability for all systems and subsystems, resulting in a higher degree of traceability than required by maturity models according to the V-model, such as Automotive SPICE. The tool-supported linking of requirements and scenarios into a single model ensures complete traceability of the requirements down to the software level. At the same time, the effects of a software update or the introduction of new homologation-relevant software functions on the vehicle can be efficiently analyzed and verified, which is the cornerstone of the argumentation vis-à-vis the technical testing organization, as part of the intended virtual vehicle type approval activities.

In addition, this comprehensive specification model enables the automatic generation of homologation-relevant scenarios and machine-readable test cases, including pass/fail criteria for virtual validation based on the formalized scenario specification and the behavior diagrams in CUBE. This enables not only the highest quality of test cases, but also the best traceability to the requirements, as well as the possibility of significantly reducing the validation effort. The use of standardized interfaces with other partners in the "Digital Loop" working group also contributes to the continuous integration of the simulation into the development environment.



2.
Automatic generation of verification and validation artifacts.

Simulation as proof of homologation

Another key objective of the "Digital Loop" is to establish the simulation as proof of acceptance for homologation within the verification & validation pipeline. For this purpose, dSPACE offers a cloud-based simulation and validation solution that enables data replay and scenario-based tests. In addition, all of the aforementioned development artifacts up to the virtual ECU, including the relevant test scenarios and their acceptance criteria, can be integrated automatically.

Based on a suitable simulation platform, measurement data from real driving tests must also be incorporated into the virtual validation. The relevant situations are identified by analyzing the measurement data before the actual simulation, which allows a catalog of realistic scenarios to be created. Situations with rare occurrences (edge cases) can be reproduced in detail in the simulation. It is also possible to parameterize the logical simulation scenarios, creating new variants and thus additional test cases, as well as uncovering new edge cases. This data-driven process is not only crucial for determining relevant situations, but also for validating the simulation models.

Further relevant situations can be recorded by adapting the environmental influences and external boundary conditions. This approach extends and completes the traditional homologation process by supporting the necessary proof of coverage of the relevant test and validation requirements.

In order to be able to use the simulation as an acceptance criterion, the simulation models must be verified and validated as an independent engineering artifact. This involves comparing the physical measured variables from the simulated scenario with the real measured variables in order to make any necessary adjustments to the model visible. A continuous comparison and documentation is therefore created as mandatory proof for the virtual homologation process. This can be further accelerated by documenting the results of the test execution of all relevant scenarios and monitoring the acceptance criteria within the simulation in a digital report.

Learn more about Digital Loop

BY
Sebastien Christians,
christiaens@fev.io
Elmar Börner,
boerner@fev.com

#3
Test center in Morocco:
All-year development and testing of ***ADAS/AD***

FEV operates the first test center on the African continent together with a joint venture partner. In Oued Zem near Casablanca, Morocco, the internationally recognized innovation driver offers its customers highly attractive conditions for vehicle development and testing almost all year round.

The Moroccan Mobility & Automotive Test Center (MMAC) in Oued Zem is located at an altitude of 850 meters in the Moroccan Atlas Mountains.

The site covers a total area of 500 hectares and comprises an extensive, completely newly built test area for passenger cars and commercial vehicles, which includes a total of 14 partial and individual routes, which test drives are possible.

In an optimal evironment, FEV offers its validation expertise on site in three functional areas in the field of ADAS/AD development.

Longitudinal and lateral functions (e.g. Driver assistance: ADAS road driving features) L0 to L2

- Automatic Emergency Braking (AEB)
- Adaptive Cruise Control (ACC)
- Automatic Lane Change (ALC)
- Blind Spot Detection (BSD)
- Cross Traffic Alert (CTA)
- Front Collision Warning (FCW)
- Lane Centering Control (LCC)
- Lane Departure Prevention (LDP)
- Lane Keep Assist (LKA)

Highly automated functions (AD driving features) L2+ to L4

- Traffic jam pilot/chauffeur up to 60 km/h
- Highway pilot/chauffeur up to 130 km/h

Parking functions (ADAS/AD parking features) L2+ to L4

- 360° surround view
- Parking assist
- Parking pilot/remote parking
- Automated valet parking type 1

[ADAS/AD test center]

Further information to the test center in Qued Zem, Morocco

#4
Innovation accelerator: ***Software engineering @ FEV.io India***

1.
The acceleration of innovations undoubtedly relies on building robust software engineering teams globally. Leveraging FEV's extensive expertise in software and electronics, complemented by in-depth knowledge across all vehicle domains crucial for intelligent mobility solutions, FEV delivers top-tier engineering services to its clients. Together, the company's experts continue to connect and mobilize communities worldwide.

The mobility industry is experiencing a revolutionary shift towards software-defined innovations. As vehicles evolve into digital ecosystems, the demand for skilled software engineers is rising, marking a significant transformation in vehicle design and functionality. This evolution is fueled by changing consumer preferences, regulatory requirements, and the rise of advanced technologies. From connected vehicles to autonomous driving systems, software plays an ever increasing role in enhancing safety, security, efficiency, and performance.

FEV, renowned for its expertise in mobility technology, recognizes the critical nature of software in shaping the future of mobility. The impressive growth trajectory of FEV.io brand and software development, as well as its impact throughout FEV globally, is indicative of the evolution within the mobility industry. As vehicles become increasingly digitized, the demand for advanced software solutions has surged, driving FEV to significantly expand its capabilities in this key domain.

»FEV is committed to advancing a world where safe and sustainable mobility systems enrich people's lives.«

As the company continues to evolve, FEV.io addresses the escalating demands, requirements, and rapid pace of development within the intelligent mobility pillar of the transportation sector. Their comprehensive portfolio spans across major solution lines, including: Systems Engineering, Functional Safety & cybersecurity, ADAS/AD, E-Cockpit & Connectivity, SW & EE Platforms and Integration. The FEV.io team, comprised of more than 1,400 software experts worldwide is committed to advancing a world where safe and sustainable mobility systems enrich people's lives.

FEV India's critical role in this tale of growth highlights the country's emerging talent pool and its ability to deliver cutting-edge software solutions. With a focus on innovation, and by harnessing India's expertise in software engineering, FEV is well-positioned to address the evolving needs of the mobility industry. In 2023, FEV India made significant strides by filing 27 patents across diverse fields; solidifying its role as a global center of excellence in Software Defined Vehicles, cybersecurity, E-cockpit & Connectivity, and Engineering Analytics. The company takes pride in it’s position as a knowledge partner in production programs with esteemed clients, marking a pivotal role in this transformational journey. FEV’s India campus stands out as a software powerhouse within the broader FEV Group, boasting a highly motivated team of over 600 experts. Furthermore, India's renowned status as a hub for technological innovation makes it an ideal choice for FEV to bolster its software capabilities.

2.
Mayank Agochiya’s appointment as the President of FEV Asia marks a significant development and aligns seamlessly with FEV's commitment to innovation and growth, particularly in the area of software development. His multifaceted experience and deep understanding of the mobility and energy realms will undoubtedly propel FEV to greater heights in the dynamic landscape of innovation and technology.

#5
Future mobility with FEV and SELFY: Resilience, cooperation, networking, and automation

The rapid development of connectivity and automation has driven the emergence of Cooperative Connected Automated Mobility (CCAM). The goal of CCAM is to improve transportation systems through integrated networks of vehicles, pedestrians, road infrastructures, Roadside Units (RSUs), as well as cloud services. As connectivity grows, new cyber threats emerge, and the scale of cyber-attacks significantly expands. Further challenges involve integrating data (from vehicles, infrastructures, and clouds), and utilizing AI techniques on this combined data for achieving advanced situational awareness.

Motivated by these challenges, the SELF Assessment, Protection, Healing Tools for a TrustworthY and Resilient CCAM (SELFY) project has been initiated. SELFY, a three-year project that started in 2022, is funded by the Horizon Europe research and innovation program. The project conducts research and development of a suite of tools designed to increase the resilience of the CCAM ecosystem against cyber-attacks, malicious activities, and hazards.

Within the consortium, FEV is responsible for:

- setting up the system architecture
- setting up an AI system for continuous self-assessment and diagnosis and for detecting anomalous situations
- developing security methods to protect the communication paths in CCAM from cyber attacks
- developing measures to ensure integrity, confidentiality and authenticity on the communication channels
- carrying out verification and validation tests as well as functional tests

SELFY tools aim to generate a distributed global solution, where protection, response and recovery decisions will be managed locally and globally. This article provides an overview of the SELFY key macro-tools. Three umbrella use cases defined in the project will be described. Following this, Situational Assessment Module (SAM) and the Secure Over-The-Air Software Update (SOTA), both of which are currently being developed by FEV, will be explained.

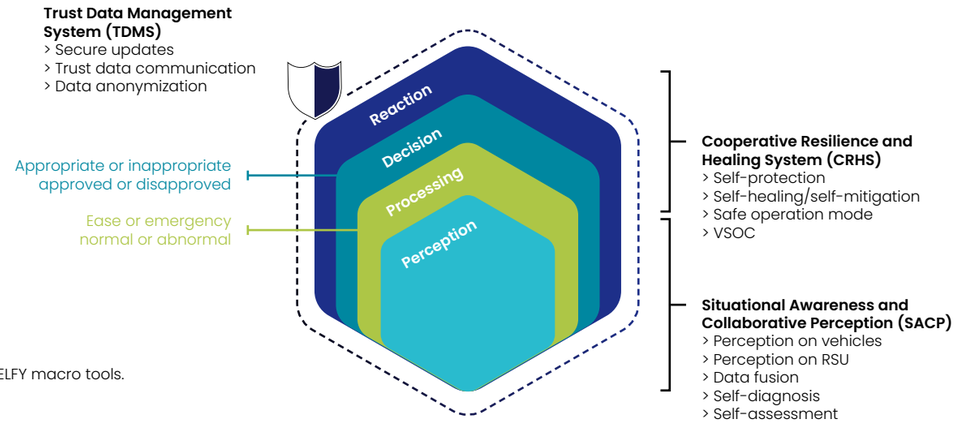
SELFY key macro tools

The SELFY toolbox performs a continuous assessment of robustness and resilience, taking advantage of a process of situational awareness achieved through collaborative perception. It offers a set of cooperative resilience services to address any compromised situations, utilizing the collection and sharing of data within a trusted collaborative framework. Figure 1 describes the key technologies of the SELFY toolbox and outlines the three macro tools into which these technologies are organized.

Situational Awareness and Collaborative Perception (SACP)
The SACP box includes a set of tools designed for a comprehensive understanding of the CCAM system's environment including different assets or devices both on the vehicle and the RSU. It consists of modules customized for interpreting the vehicle's environment by providing separate perceptions from the vehicle and the RSU, alongside a module that integrates these two perceptions. Additionally, it contains modules that detect anomalies on both the vehicle and RSU.

Cooperative Resilience and Healing System (CRHS)
The CRHS box contains tools designed to initiate self-protection actions in response to compromised scenarios involving assets, vehicles, operations, or the system itself. One such action is the activation of a safe operation mode, which is selected when necessary for vehicle safety. In this case, this tool is responsible for determining, executing, and assessing the status of the selected safe operating mode that is suitable for the detected situation. Resilience actions may be executed locally, or in cooperation with other nodes connected to CCAM framework, enabling decision-making on a global scale. Within CRHS, the Vehicle Security Operations Center (VSOC) has this global decision-making capability.

Trust Data Management System (TDMS)
The TDMS box encompasses tools designed to build a secure and trusted environment for data within a collaborative and cooperative setting, covering infrastructure and assets, as well as personal data of individuals like drivers and pedestrians. It aims at ensuring the integrity of various software components, upholds privacy, and manages secure software updates for connected and automated vehicles.



1
SELFY macro tools.

Three umbrella use cases of SELFY

The SELFY toolbox is to be validated in three different macro scenarios, corresponding to three validation environments of SELFY: real-world validation, laboratory/Hardware-In-The-Loop (HIL) validation, and simulation validation.

1

Resilient cooperative mechanisms for Vulnerable Road User (VRU) safety
The rise in automated vehicles requires improving safety measures for VRUs, such as pedestrians and cyclists. Achieving this requires smart cooperation among automated vehicles, human-operated vehicles, and VRUs. Resilient cooperative mechanisms for VRU Safety scenarios consist of perception, situational awareness, communication, and decision-making supported by risk assessment.

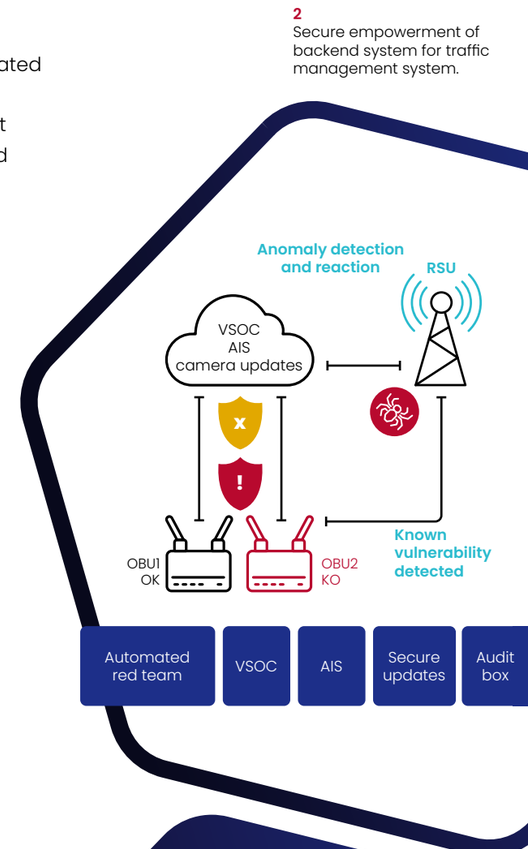
2

Secure empowerment of backend system for traffic management system
The CCAM ecosystem requires secure and robust remote data connections to cloud servers. In the future, every Original Equipment Manufacturer (OEM) will need to establish VSOCs to monitor their vehicles' cybersecurity, and report security incidents, anomalies, and hazards.

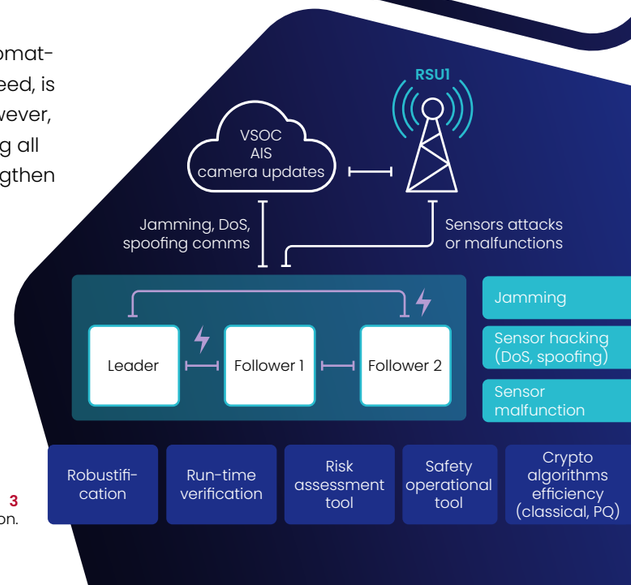
Traffic Management Systems or specific OEMs shall have the possibility to set their own parameters to the VSOC, including trust level based on the road and vehicles conditions, allowed maneuvers, reaction, or degraded modes. The VSOC is equipped with tools for system auditing and advanced algorithms for threat detection and response deployment (Figure 2).

3

Robustification of a platoon
Platooning, a technology enabling several automated vehicles to travel together safely at high speed, is representing a key cooperative maneuver. However, it requires a reliable communication link among all vehicles in the platoon. SELFY tools aim to strengthen this link, mitigating potential risks (Figure 3).

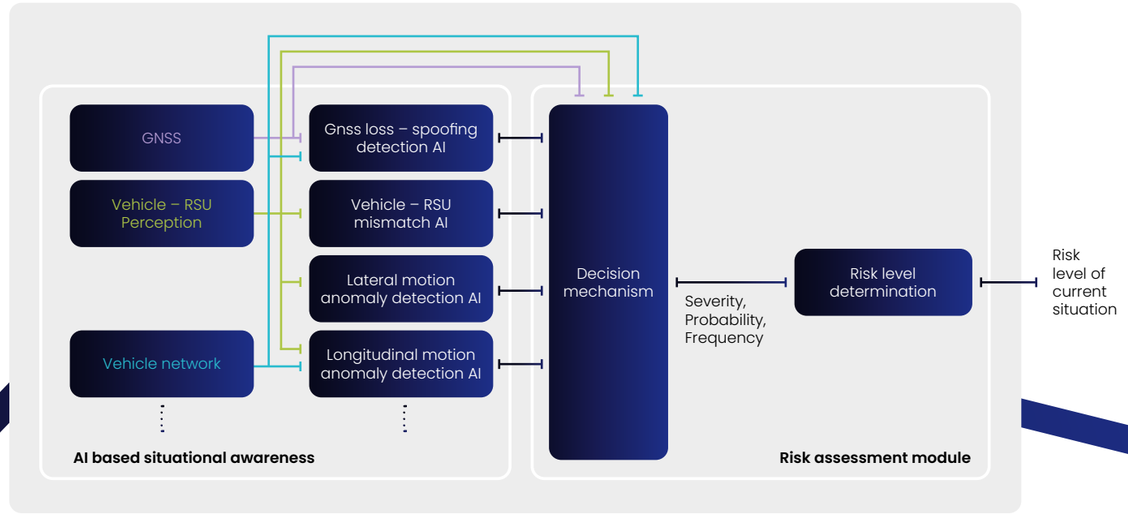


2
Secure empowerment of backend system for traffic management system.



3
Robustification of a platoon.

4
Situational assessment module.



Situational Assessment Module (SAM)

SAM is designed to enhance AI-based systems capability to detect anomalies and make decisions under different operational conditions. Using advanced AI-based techniques, SAM (shown in Figure 4) compares fused data coming from RSU and on-board vehicle sensors with ego vehicle's CAN messages to detect anomalies, misuse, and malfunctions. Based on detected anomaly, SAM determines the risk level of the current situation to be fed into the decision for selecting one of the ego vehicle's safe operation modes. For this purpose, four different AI models have been created.

The primary anomaly investigated is the phenomenon of Global Navigation Satellite System (GNSS) Loss-Spoofing. To address this issue, a distance estimation is devised to detect when GNSS data becomes unavailable for several reasons during vehicular operation. A second anomaly, RSU-Vehicle Mismatch, indicates inconsistency between RSU data and vehicle-obtained data. The detection of such mismatches signifies a loss of vehicle reliance on its perception systems and constituting an anomalous state. Further anomalies involve unexpected changes in acceleration, deceleration, and steering while the vehicle is in motion, considering factors such as the vehicle's traffic interactions and normal speeds.

During the operational phase of AI models, detected anomalies are conveyed to the decision mechanism, where calculated frequency, probability and severity values support interpreting the situation using a pre-established rule-based decision table. The risk level determination unit specifies a risk value by considering these three parameters.

Secure Over-The-Air Software Update

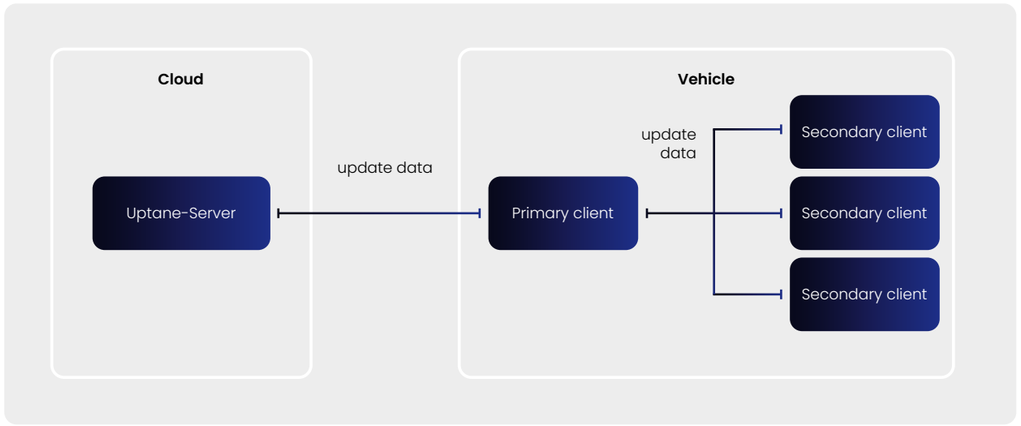
A use case illustrates the need for vulnerability detection and providing software updates and security bugfixes via a secure update mechanism. In that case the RSU detects a vulnerability/bug on the ego vehicle and informs all surrounding vehicles. Such suspicious behavior has been detected by the vehicle in front, and it has been learned that it is caused by a compromised or outdated software version. The remediation action of a software update will be transferred to the ego vehicle.

In this use case the software update is executed using a SOTA tool which is part of the TDMS macro-tool. The primary aim of this tool is to provide secure and efficient delivery of software updates to the vehicle's Electronic Control Units (ECUs) remotely. This capability is crucial for maintaining or upgrading vehicle functionalities without the inconvenience of physical dealership visits. It ensures that the latest cybersecurity measures are implemented swiftly, addressing vulnerabilities, and enhancing the vehicle's safety features. For the connected and automated vehicles, the OTA software update process will be highly significant in upcoming years and accelerate the upgrade of the vehicle software system in the mobile world.

»Secure updates are threatened by quantum advancements. The SELFY project is preparing for this by integrating post-quantum cryptographic algorithms into the SOTA framework.«

Since the OTA update requires the access to the in-vehicle communication system and enables additional attack surfaces remotely to all the ECUs which have the OTA capability, the security of the update process itself is significantly critical. Due to its importance, the United Nations Economic Commission for Europe (UNECE) published regulation R156 in 2021, to require the vehicle type approval on the cybersecurity of the software update and the software update management system. In the SELFY project, the security of the OTA software update process is the focus. The core of the SOTA tool is based on the Uptane framework, as shown in Figure 5.

- **Uptane-Server:** This server-side component is responsible for preparing secure software updates, signing them cryptographically, and distributing them to related vehicles. It is the starting point for the secure update lifecycle.
- **Primary Client:** Embedded within the vehicle, the primary client acts as the intermediate ECU, receiving updates from the Uptane Server. It verifies the updates' signatures and integrity before disseminating them to the secondary clients.
- **Secondary Clients:** These in-vehicle components (ECUs) receive updates from the primary client. Each secondary client is responsible for independently verifying and installing these updates to manage its specific vehicle function.



5
SOTA architecture.

The OTA updates require long-term security. To counter vulnerabilities discovered long after the vehicle's production, the OTA update mechanism must be secured against future threats. However, the advent of quantum computers presents significant challenges to existing cryptographic practices in vehicles. Current vehicles rely on public key cryptography for secure updates. While these methods ensure integrity and authenticity, they are at risk from quantum advancements. To be prepared for this risk, in the SELFY project, we are researching on the integration of post-quantum cryptographic algorithms into the SOTA framework.

Disclaimer
This research has been funded by the European Union, through the Horizon Europe research and innovation program, under grant agreement No. 101069748 - SELFY project. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency (CINEA). Neither the European Union nor the granting authority can be held responsible for them.

Further information on the SELFY project

BY
Burcu Oezbay,
oezbay@fev.com
Dr. Miao Zhang,
zhang_m@fev.io
Dr. Mohamed Saied Mohamed,
mohamed_m@fev.io
Ali Eren,
eren_a@fev.com

Summary and outlook

The SELFY project's vision is to become the main European provider of an agnostic toolbox for the self-management of security and resilience of CCAM ecosystems.

Moving forward, the SELFY project will continue the integration and validation of the toolbox in simulation, HIL testing, and real-world environments in accordance with its goal to provide a holistic and sustainable solution of security and resilience for all the stakeholders involved in the CCAM ecosystem including OEM, suppliers and transportation service providers.

feel evolution

FEV.io

FEV test systems

FEV propulsion

FEV vehicle

FEV energy

FEV CONSULTING

fev.com

#6
Detected: No chance for ***partial electrical discharge***

With PD-HVX (“Partial Discharge-High Voltage X”), FEV has developed the world's first solution for early detection and prevention of partial discharge (PD) in high-voltage Electric Drive Units (EDUs). PD can cause damage to the insulation in modern EDUs, which in the worst-case scenario can result in a total failure of the vehicle. FEV’s PD-HVX uses well established measuring systems with specialized sensors, which are used in EDUs for qualitative measurement. This enables customers to identify partial discharge during the development phase and take the necessary action.

PD is a local electrical sparkover that can occur at high voltages above 600 volts. It is caused by extremely small defects or inhomogeneities in the insulation material or soiled surfaces. If it remains unnoticed within an EDU and occurs repeatedly, PD leads to gradual damage of the insulation and to a premature stop of the vehicle.

PD-HVX uses electromagnetic frequency analysis, one of the most precise and reliable measurement methods for the application field of electrical propulsion systems, to measure the electromagnetic fields around the drive unit to be analyzed. The innovative software then uses the measurement results to determine whether partial discharge occurs within the EDU during operation.

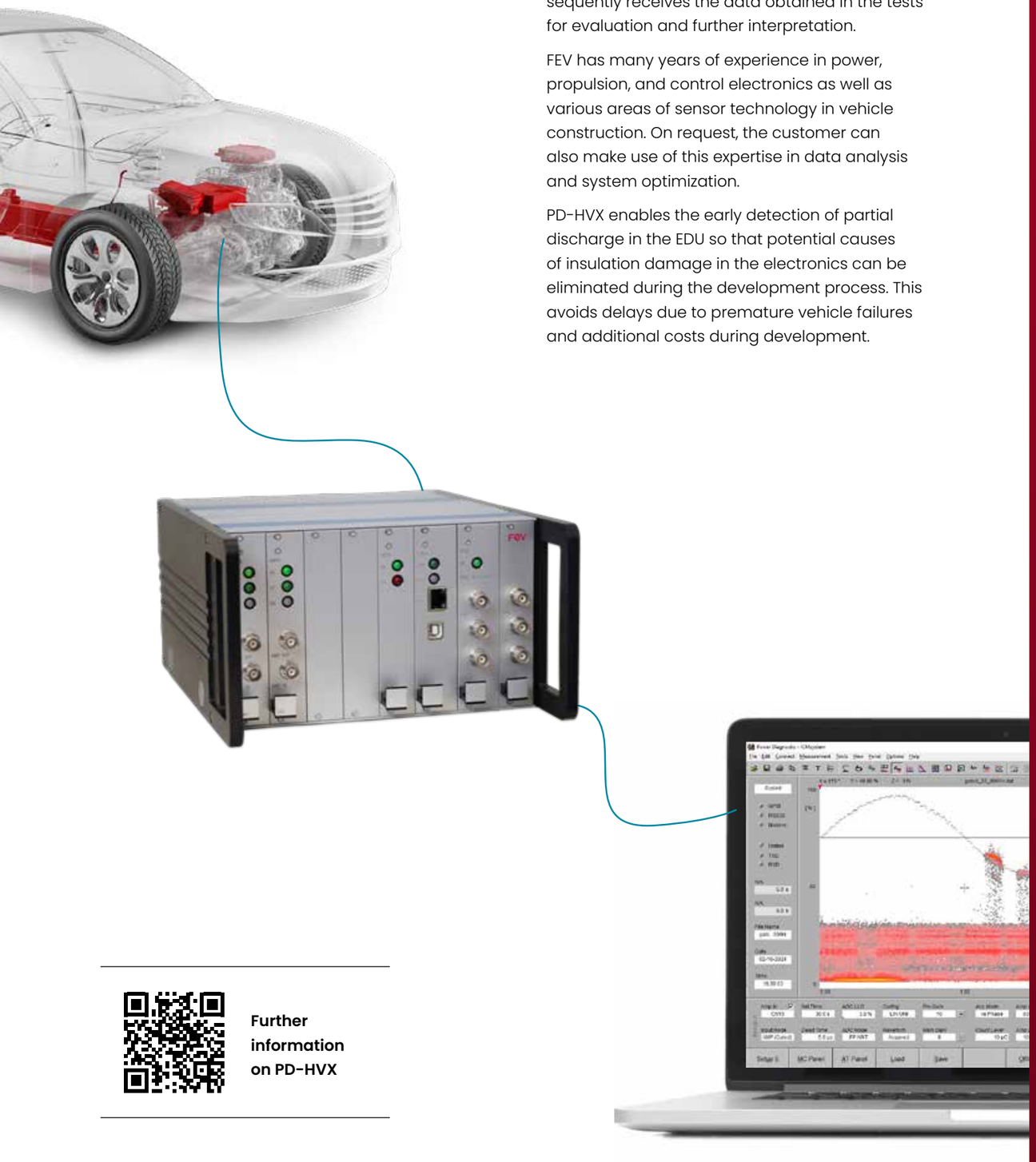
PD has been known for a long time in the field of electrical systems engineering and high-voltage transmission networks, where corresponding tests are common practice. In the automotive sector, however, the phenomenon is just gaining focus with the increasing spread of 800V batteries. Thanks to FEV’s many years of expertise in the development of EDUs, with PD-HVX the company can already offer its customers a dedicated solution for PD.

[**Partial electrical discharge**]

The solution is part of a comprehensive service package for vehicle manufacturers and suppliers. The test equipment, which is optimized for EDU operation, filters out drive-related interference signals and therefore enables significantly better measurement results for PD. The customer subsequently receives the data obtained in the tests for evaluation and further interpretation.

FEV has many years of experience in power, propulsion, and control electronics as well as various areas of sensor technology in vehicle construction. On request, the customer can also make use of this expertise in data analysis and system optimization.

PD-HVX enables the early detection of partial discharge in the EDU so that potential causes of insulation damage in the electronics can be eliminated during the development process. This avoids delays due to premature vehicle failures and additional costs during development.



Further information on PD-HVX

What makes FEV's PD-HVX solution so special?

PD-HVX is the world's first solution for measuring partial discharge (PD) that has been specially developed and optimized for use in electromobility. With PD-HVX, PD can be measured and eliminated early on in the development process.

Three questions on electrical partial discharge to the expert

Dr. Michael Stapelbroek, Vice President Electric Powertrain at FEV

The phenomenon of partial discharge has long been known in electrical systems engineering. Why is it gradually coming onto the agenda in the automotive industry only now?

The increasing use of 800V DC systems in the field of Electric Drive Units (EDUs) has multiplied the risk of PD occurring. As in all electrical systems, PD in the EDU can lead to damage to the insulation and, in the long term, to vehicle failure.

What specific services does FEV offer its customers in the context of PD?

PD-HVX is a comprehensive system solution. The combined hardware and software package has been specially optimized for use in electromobility. The overall package includes training, commissioning of the measurement technology at the customer's premises, a detailed analysis of the measurement data and the measures derived from this. With more than 25 years of experience in the measurement and elimination of PD, we advise our customers on how to eliminate them during the development process.

#7
Iveco New Daily Electric ***series development***: A successful partnership between FEV and Iveco Group

For decades, Iveco has been known as one of the most pervasive manufacturers of commercial vehicles in virtually all classes and segments. The potent "Iveco-DNA" is a highly customizable vehicle platform, with multiple variants, including special interfaces for body and coach builders. It is critical that this unique selling point be maintained while transitioning to all-electric; hence the need for a highly flexible, modular, and cost competitive electric light-duty platform.

Customized systems engineering, smart architecture and "joined forces"

Beginning with the electric Daily in 2009, Iveco had already successfully developed prototypes in very small batches using its independent core team from former Altra s.p.a. in Genova. To scale up these experiences and integrate electrification into regular series development cycles, Iveco asked FEV to provide strategy and engineering support; forging a long-term, stable partnership that has grown over time and remains highly successful today. In this article, key factors for the outstanding product and cooperation will be described.

Continuous platform evaluation and target maintenance

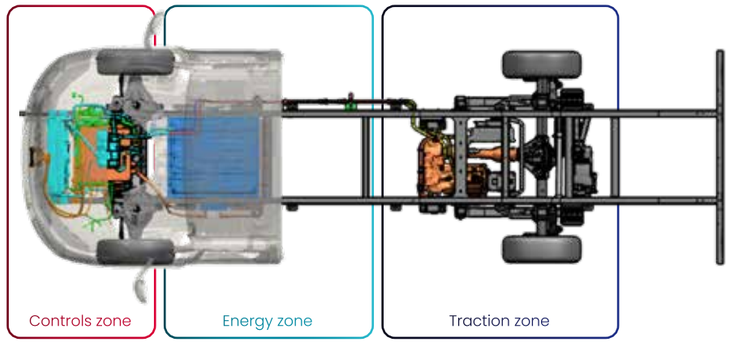
Target definition of a full platform typically takes an exceedingly long time, requiring detailed evaluation of multiple variants. To speed up this process, FEV Consulting accompanied Iveco's early phases of feasibility evaluation and concept definition for the planned "Diesel-to-BEV-conversion", evaluating both lead variants and selected targets for each development phase. Using this approach, the full platform could be continuously developed, and first key variants could be used as a baseline for the initial concept and component sizing by the engineering teams of both FEV and Iveco Group.

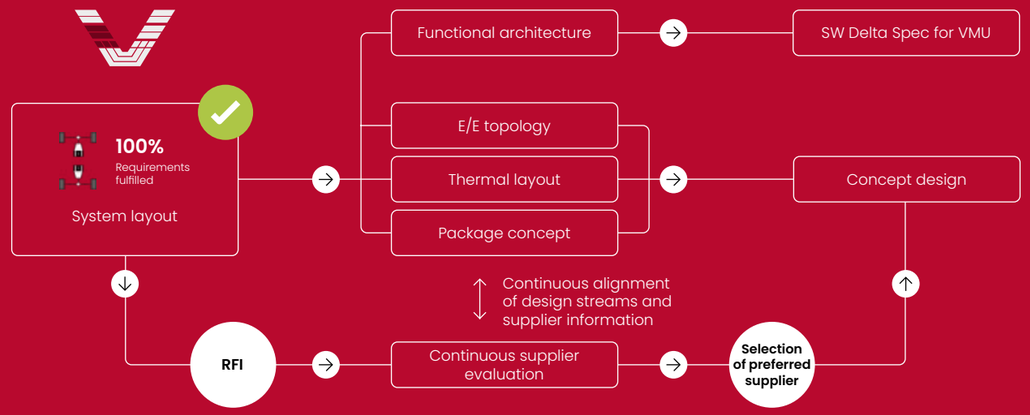
Additionally, FEV's systematic and simulation-based approach enabled the project to start with internal and external alignments much sooner than normal, allowing for full scale platform evaluation of more than 150 variants and the addition of step-by-step variant-specific use cases.

Detailed concept development was also able to be started early, leading to a fully modular approach in terms of packaging, E/E-architecture, and thermal layout, as described further below. The process was continuously challenged by cross-checks with the growing variants throughout the full concept phase. After only five months this led to robust target setting and a suitable concept design.

1.
Multiple variants of the Iveco Daily to be electrified (Cab, Van, Crew Cab (4.25t–7.2t Gross Vehicle Weight (GVW)), Chassis Cowl and Minivan (7.2t GVW)).

2.
Design zones of modular system architecture of New Daily Electric.





3.
Concept phase with parallel system design streams and synchronized supplier evaluation.

Component centric architecture definition and fast concept design
When introducing not only one vehicle variant, but a full platform, the robustness of all parts is mandatory. Hence using existing, pre-validated, off-the-shelf components is preferred. For the battery packs, however, a specific design was needed.

A continuous alignment between packaging, E/E architecture and full component technical requirements specification, as well as multiple suppliers was undertaken. The result was a very modular design, defining clear design zones for "energy", "traction" and "controls" of the vehicle (Figure 2, P. 41).

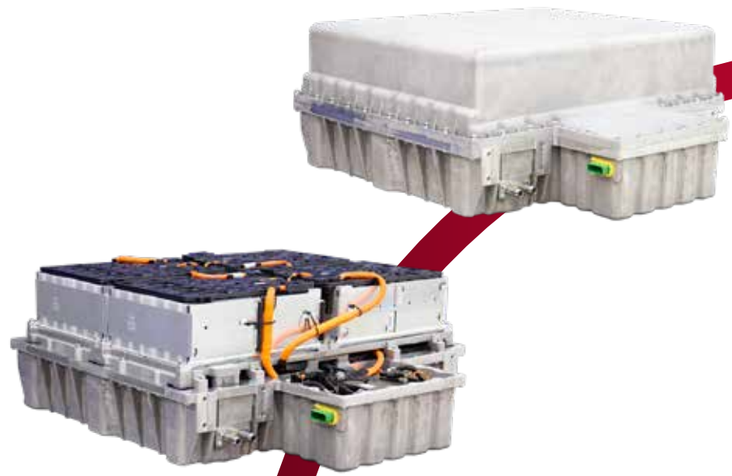
In parallel to the supplier and components evaluation, the system development and full concept design were also specified (Figure 3), incorporating the HV experience of the Iveco Genova team and their specific knowledge of Iveco's commercial vehicle platforms, with FEV's long time experience in electrification and series development of hybrid and battery electric vehicles, as well as high voltage batteries.

Tool based requirements management and early validation planning
The requirement management started with new stakeholder specifications incorporating IVG standard formats for technical requirements specification. This included the new high voltage components, in addition to standard "vehicle functions" for the system-wide functional requirements, both for modified pre-existing and new functionalities. Iveco's standard vehicle validation planning was extended with FEV's electrification knowledge, and linked together with the definitions of detailed testing demands for the new high voltage components.

eVECOp, the modular inhouse powertrain platform
To maintain an "off-the-shelf-approach" for the control unit software, a smart functional architecture was configured, defining a soft-gateway and other necessary adaptations for each of the component functions inside the in-house e-powertrain control unit, or "VMU" (Vehicle Management Unit). Although FEV offers its own e-powertrain controls platform for such instances, in this case, the Iveco in-house Software for the first Daily Electric was upscaled to a full controls platform that later came to be known as "eVECOp".

Modular FPT battery system with master BMS and customer field-test with FEV battery
The battery system consisted of multiple identical batteries, which were packaged within the ladder frame of the New Daily Electric, with all packs coordinated by a master BMS. Today's batteries are produced in-house by FPT Industrial (part of Iveco Group, based on a joint venture with Microvast). However, since the battery production and corresponding development had to be set up in parallel to the vehicle project, an intermediate solution was used in the first phase of the program. Employing cell-modules and sub-components from an existing passenger car, FEV developed a battery pack with new packaging and cooling (Figure 4). These prototype-batteries were built at FEV's development workshop; with full ECE R100 compliance testing done at FEV's state-of-the-art "eDLP", the world's largest independent development and test center for high-voltage batteries. The master BMS for the first vehicles retained FEV's multi-battery string functions, to coordinate the up to three battery packs with each other and to present them as a single energy storage system from the perspective of the rest of the propulsion system.

To collect real-life field information as early as possible, Iveco provided two mature Alpha prototype vehicles to an end customer. They were equipped with most of the target HV components, including FEV prototype batteries and the eVECOp controls together with the FEV master BMS, both running on a dSPACE MicroAutobox® ECU. These vehicles were "Single Type Approved" for the European market with prototype public road release for trained drivers and were fully integrated into the regular daily business of the customer for several months. A combined FEV/ Iveco Group team stayed closely connected to the customer for continuous data collection and analysis, as well as to perform maintenance when needed. Hence, not only were valuable insights into the real-life-use-case acquired, but also a high quality in-field-proof-of-concept could be obtained. These prototype vehicles are still reliably in operation today.



4.
By FEV developed battery pack for New Daily Electric early customer field test.

Holistic project approach
Another key to the success of the project, was the project set up itself. It included not only the technical development, but also the early manufacturing planning, training of the extended Iveco teams in the field of electrification, and the continuous parallel strategic support of FEV Consulting to keep track within the (still) volatile market environment.

Set-up and collaboration in large scale projects across dispersed teams is always a challenge. For its part, Iveco Group incorporated multiple locations, including Iveco's main site in Torino, a production plant in Suzzara, and their Electrification Competence Center in Genova. On FEV's side, experts from the headquarters in Aachen, from FEV Italy in Torino, and sites from other subsidiaries like FEV France and FEV Turkey contributed to the success of the project.

Joint success: Iveco New Daily Electric

Since April 2023, the New Daily Electric has been offered to its clients. An early program initiation with the clear target to address a wide spectrum of battery electric use cases has paid off, and the performance and the flexibility of the product have met or exceeded all expectations.

All of Iveco's standard body variants are covered, as well as the full Daily GVW range from 3.5 to 7.2 tons (t). All wheelbases from 3,000 mm up to 4,750 mm are offered as full electric versions, keeping the regular Iveco promise for high payload and cargo volume.

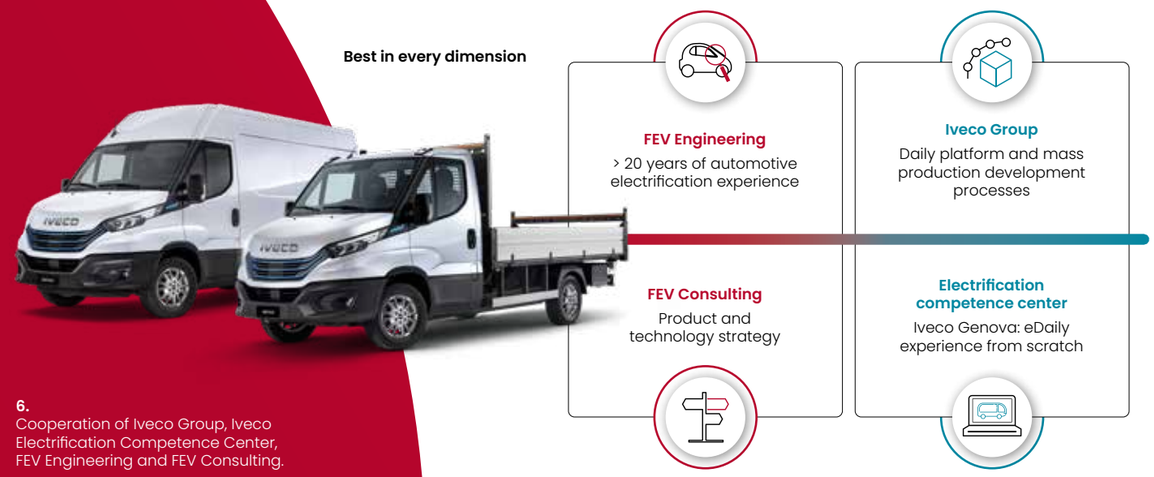
Based on the modular battery concept, produced inside Iveco Group, configurations with up to 300 kilometers (km) WLTP range and 400 km tested in real life urban conditions are available. Charging up to 22kW is possible with AC-charging and 80 kW with DC-charging, which equals up to 100 km range in just 30 minutes.

The HV architecture and its modular integration in the design zones of the chassis (Figure 2, P. 41) not only allow a choice of battery configuration, but also offers the highest flexibility for body builders. The flat and robust base chassis allows for conversions and offers three different types of electrical and mechanical PTOs (Power Take-Off), providing builders with an even larger degree of freedom than seen in diesel versions.

Finally, the 140kW/400Nm electric motor provides superior driving power and a slope startability of up to 30% and 3.5t towing capacity in combination with 2 or 3 batteries. The Iveco-typical robustness has been tested from -30°C up to +50°C.

WLTP ranges			
GVW	**1 Battery**	**2 Batteries**	**2 Batteries**
3.5t	120 km	235 km	
4.25t	110 km	200 km	300 km
5.2t		185 km	260 km
7.2t		120 km	180 km

5.
Vehicle variants with GVW, battery configurations and WLTP ranges.



6.
Cooperation of Iveco Group, Iveco Electrification Competence Center, FEV Engineering and FEV Consulting.

Outlook

This ambitious project has forged a stable, trustworthy long-term partnership between Iveco Group, FEV Consulting, Iveco Electrification Competence Center, and the FEV Engineering units. Key factors to success were the flexible architecture, state-of-the-art development processes and tools, as well as the dynamic and global project set-up – not to mention the strong, common will to find a solution for any challenge.

The future of the Iveco New Daily Electric is already being worked on today: In the meantime, a fuel cell variant has been developed, and first-level prototype vehicles are running and have been presented to the public. Updates to the New Daily Electric have already been announced and will soon be in production. The modular concept is expected to be maintained and further optimized, including a special variant with a fourth battery pack and further improved fast charging.

BY
Dr. Felix Richert, FEV
richert@fev.com
Patrick Glusk, FEV
glusk@fev.com
Alessandro Bernardini, Iveco Group
Marco Aimo-Boot, Iveco Group

#8 *Proprietary solutions*

Feel EVolution by FEV

FEV's proprietary solutions enable the company to differentiate itself in the market with unique developments and give its customers the decisive competitive advantage. In SPECTRUM we regularly present a selection of these solutions.

Further information on FEV's proprietary solutions

Vehicle Motion Control (VMC) – Software for torque management in vehicles with electric drivetrain

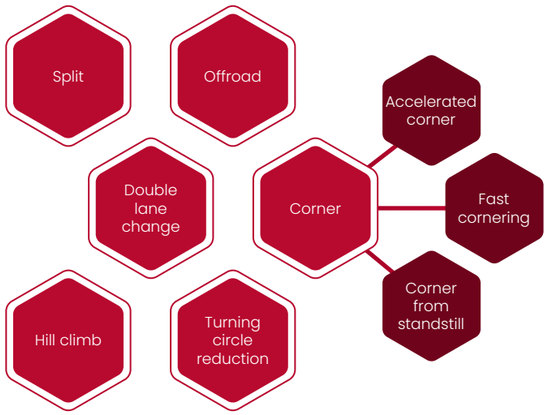
The diversity of concepts for electrified vehicles includes different drivetrain architectures, which differ primarily in the number, position and type of the machines. In addition, drivetrain control is increasingly being integrated into cross-domain Vehicle Motion Control (VMC) systems. In these cases, torque distribution is integrated into a holistic VMC to control vehicle dynamics through coordinated actuation of the brakes and powertrain.

In order to fulfill these requirements, FEV has continuously developed its software library. The modularity of the software enables simple adaptation to a wide range of drive architectures and simultaneously allows implementation of driving dynamics targets.

To achieve increased range, the drive systems must be controlled in such a way that electrical energy is utilized with as low a loss as possible. For this purpose, efficiency models of all involved drivetrain components are included in the distribution strategy of the torque software. The specific operating point selection is particularly important for architectures with different machine types, whereby the loss reduction is achieved through integrated optimization, taking existing power and torque limits into account.

In addition, the FEV powertrain software enables improved vehicle behavior and situationally increased traction by estimating transmittable wheel forces and monitoring wheel slip. In the event of an imminent loss of traction, torque is redistributed to the remaining driven wheels. These functionalities are particularly necessary for off-road vehicles where the properties of the ground can vary greatly and a loss of contact with the surface may occur.

In topologies with several machines per axle, an improvement of the lateral vehicle behavior is possible. A torque intervention is derived from the target movement of the vehicle, which influences the yaw rate and limits the sideslip angle. This results in both improved cornering behavior and increased maneuverability in evasive maneuvers. If the behavior deviates from the target movement (e.g. µ-split), the pre-control of the drivetrain intervenes in the vehicle dynamics. This pre-control has a stabilizing effect on the vehicle and reduces interventions of the Electronic Stability Program (ESP).



BY
Dr. Rene Savelsberg,
savelsberg@fev.com
Björn Krautwig,
krautwig@mmp.rwth-aachen.de

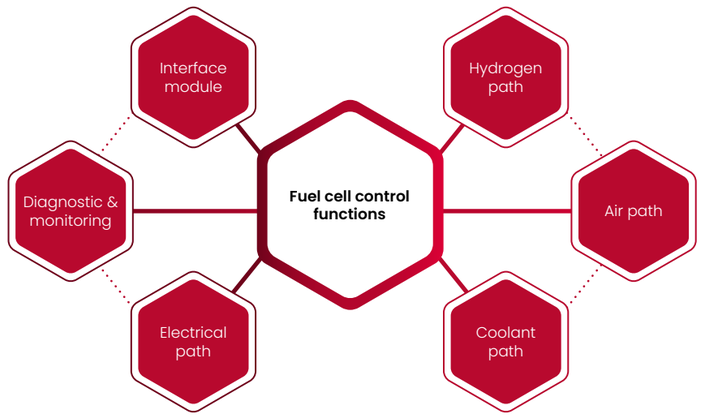
Modular fuel cell control software

To meet strict CO_2 regulations, one viable approach involves embracing hydrogen as an energy carrier to achieve mobility. Within this framework, the development of Proton Exchange Membrane (PEM) fuel cells stands out for its application in both on- and off-road mobility applications, thanks to non-existent CO_2 emissions, high-energy densities, and fast start-up times. However, the performance of these devices is closely related to the control concepts that are used to ensure high efficiency, smooth transient performance, long-term reliability, durability, and overall safety during operation.

To address these challenges, FEV has developed a modular Fuel Cell Control Unit (FCCU) software that offers the potential to be used for different P&ID (Piping & Instrumentation Diagram) configurations of fuel cell systems. The software controls and monitors the stack and the Balance of Plant (BoP) components, and establishes an optimal control coordination between different fuel cell sub-systems while communicating with the main vehicle controller. The control software features a comprehensive state-machine that manages system start-up and shut-down including freeze start, which has been coordinated with various fuel cell stack manufacturers. Essential control parameters such as temperature, pressure, humidity, and air stoichiometry, directly influencing fuel cell performance are carefully identified and regulated.

Depending on the system complexity, the modular software uses diverse strategies for mass flow, pressure, and humidity control (e.g. using throttles and bypasses). Special attention is given to optimizing the purge/drain strategy. Furthermore, the software addresses challenges arising from component deviations or aging through closed-loop power control, with particular emphasis on degradation modeling to extend the life of the fuel cell. Additionally, it enables early fault detection through comprehensive monitoring and diagnostic functions, minimizing stack damage and ensuring safe operation.

The control software has been successfully integrated into various prototype and series control units, showcasing its capabilities through testing on fuel cell test benches and vehicles. This software can be integrated with FEV's control solutions for VCU/HCU (Vehicle/Hybrid Control Unit) for supervisory control or can be paired with our customer's software. Lastly, the white-box option allows our customers to utilize FEV's solution for their own control development.



BY
Dr.-Ing. Vivek Srivastava,
srivastava_vivek@fev.com
Dr.-Ing. Joschka Schaub,
schaub@fev.com
Dr.-Ing. Marius Walters,
walters_m@fev.com

FEV Europe GmbH
Neuenhofstraße 181
52078 Aachen
Germany
P +49 241 5689-0
marketing@fev.com

FEV North America, Inc.
4554 Glenmeade Lane
Auburn Hills
MI 48326-1766 · USA
P +1 248 373-6000
marketing@fev-et.com

FEV China Co., Ltd.
168 Huada Road
Yanjiao High-Tech Zone
065201 Sanhe City
Langfang Hebei Province
China
P +86 10 80 84 11 68
fev-china@fev.com

FEV India Pvt, Ltd.
Technical Center India
A-21, Talegaon MIDC
Tal Maval District
Pune 410 507 · India
P +91 2114 666-000
fev-india@fev.com

More than 7,500 FEV experts globally

RECYCLED
Paper made from recycled material
FSC® C106855

SPECTRUM #78
Issue 01/2024

Editorial
Marius Strasdat
FEV Europe GmbH

Layout
Verena Mainz
FEV Europe GmbH

Reader service
Would you also like to receive future issues of SPECTRUM or has your address changed? Send your name, the name of your company, and mailing address to **spectrum@fev.com**

company/fev-europe

feel evolution

fev.com