Press Release

FEV SPORT Framework Addresses Increased Cybersecurity Risks in New Vehicles

Media Contact
Ulrich Andree
T +49 241 5689-8880
andree@fev.com

www.fev.com

Auburn Hills, Michigan, February 2021 – FEV, a leading global service provider of vehicle and powertrain development for hardware and software, has identified increased adoption of software in vehicles as a significant cybersecurity risk. FEV has created a new so-called SPORT (Strategy, Processes, Organization, Resources, and Technology) framework to enable suppliers and OEMs to act quickly and stay ahead of hackers.

FEV's SPORT framework is designed to provide a holistic approach to cybersecurity preparation. The **Strategy** part takes the OEM's or supplier's corporate vision, mission and culture into account. This step aligns the cybersecurity strategy with the corporate strategy and describes its impact on the current and future product portfolio as well as on the customer base.

The **Process** step incorporates development processes, e.g. the Security Development Life Cycle and knowledge management as well as audit and training processes, supported by a dedicated change management workstream.

Organization deals with the structure of the cybersecurity teams and develops a reporting structure with clear roles and responsibilities, while the **Resources** part defines the necessary team size, takes care of the talent acquisition and outsourcing strategies.

The **Technology** step incorporates

- A highly secured hardware and software strategy
- Technical measures (constructive and analytical)
- Available tools and infrastructure

The development of the automotive industry and the increasing incorporation of information technology into vehicles have made FEV's SPORT framework a valuable service for automakers: In 2010, a premium car had up to 100 million lines of software code, today it is close to 150 million lines. By 2030, the number of lines is expected to be >300 million. This increase in software content presents significantly more entry points for cyberattacks.

In recent years, the importance of cybersecurity has already made its way onto the financial statements of large players in the automotive and technology industries. A handful of high-profile attacks have directly resulted in a drop in stock prices, as well as a hit to the business performance and reputation. As one example, a remote attack in 2015 resulted in a recall of nearly 1.5 million vehicles. This led to estimated costs of $600 million and an estimated loss of $4 billion in market cap for this OEM.

With increasing vehicle complexity, it's likely that these events can become even more common. More consumer information will be saved and accessible through the vehicle, raising the stakes for future attacks.

"Cybersecurity will continue to play an increasingly important role for global automakers in the coming years as vehicles become more connected and automated," said Mayank Agochiya, managing director of FEV Consulting, Inc.

In addition to loss mitigation, cybersecurity measures also present an opportunity for differentiation. As vehicle owners and users are

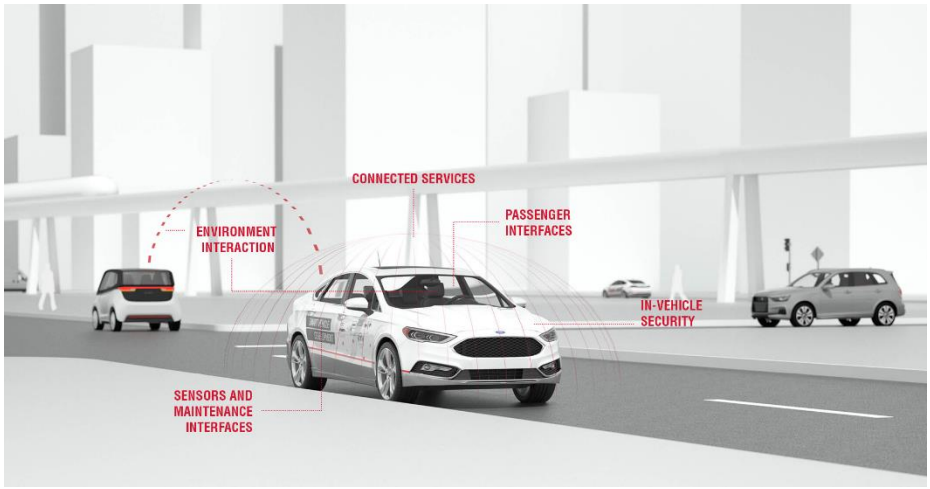
offered highly integrated connectivity features, trust will play a significant role in adoption.

With these factors swirling, the mobility industry is paying closer attention to cybersecurity. It is expected that compliance to a majority of cybersecurity regulations and standards, including ISO 21434, will be targeted for vehicles released in 2025. With UNECE WP.29 coming into place, cybersecurity will become a mandatory aspect of type approval in 54 countries even before 2025. In order to comply, OEMs and suppliers need to act now. Complex cybersecurity organizations, resources, and processes must be established and prepared by the end of 2022.

“Quick, proactive action is required for OEMs and suppliers to be ready by 2025 the latest,” said Agochiya, “To that end, we’re proud to offer support through our SPORT framework as we support our customers in the quest to develop increasingly safe vehicles.”

FEV’s methodology has already been successful in identifying and mitigating risks by acting early and utilizing a proper approach. It has proven that OEMs and suppliers in the mobility industry can both protect their finances against the risk of cyberattacks and improve passenger safety.

https://www.fev-consulting.com/en.html



FEV's SPORT framework is designed to provide a holistic view on cybersecurity preparation. It has proven that, by acting early and utilizing a proper approach, OEMs and suppliers can protect their finances against the risk of cyberattacks and improve passenger safety.
Source: FEV Group

About FEV

FEV is a leading independent international service provider of vehicle and powertrain development for hardware and software. The range of competencies includes the development and testing of innovative solutions up to series production and all related consulting services. The range of services for vehicle development includes the design of body and chassis, including the fine tuning of overall vehicle attributes such as driving behavior and NVH. FEV also develops innovative lighting systems and solutions for autonomous driving and connectivity. The electrification activities of powertrains cover powerful battery systems, e-machines and inverters. Additionally, FEV develops highly efficient gasoline and diesel engines, transmissions, EDUs as well as fuel cell systems and facilitates their integration into vehicles suitable for homologation. Alternative fuels are a further area of development.

The service portfolio is completed by tailor-made test benches and measurement technology, as well as software solutions that allow efficient transfer of the essential development steps of the above-mentioned developments, from the road to the test bench or simulation.

The FEV Group is growing continuously and currently employs 6,700 highly qualified specialists in customer-oriented development centers at more than 40 locations on five continents.

About FEV Consulting

FEV Consulting, with headquarters in Aachen, Germany, and further offices in Munich, Cologne, Bilbao, Beijing, Dubai and Auburn Hills, USA, combines top management consulting expertise with the technical capabilities and know-how of the FEV Group. The deep industry knowledge enables FEV Consulting to create pragmatic solutions to some of the most pressing and complex issues facing today's enterprises around the world.

FEV Consulting provides unique, client-oriented advisory services through years of experience in management consulting. FEV Consulting works with clients to address their most challenging business issues and employs an analytical approach, proven capabilities and – most importantly – real industry knowledge to resolve clients' problems.