

Special Edition – June 2025

# Cybersecurity in Mobility

Recent developments

Curated and summarized - Industry and Patent news

Published by Denne Meyer India Private Limited

Parag Thakre ( [pthakre@denne Meyer.com](mailto:pthakre@denne Meyer.com) )

Himanshu Varun ( [hvarun@denne Meyer.com](mailto:hvarun@denne Meyer.com) )

This report is subject to copyrights and may only be reproduced with permission of Denne Meyer.

# Subscribe now



Scan the QR code to receive this monthly report via email in your inbox.

# Preface

The rise of connected cars and software-defined vehicles has revolutionized the automotive industry, but it comes with a surge in cybersecurity threats. Thus, cybersecurity becomes paramount for the OEMs, suppliers and users.

This monthly report is focused on “Cybersecurity in Mobility” including applications in Electric Vehicles, Autonomous Vehicles, Software Defined Vehicles, UAVs, Drones, Aircrafts, Fleets, etc. This report is a free resource for anyone working in this domain including technologists, innovators, Intellectual Property (IP) managers, strategy makers, etc. The report contains curated insights and summaries of the latest news and key patents published in the last one month, including the latest products, business updates, collaborations, new innovations, etc.

In this special edition, we explore the future of EV charging, with a focus on Extreme Fast Charging (XFC) and the cybersecurity challenges it brings.

# Special Edition

In this special edition of our monthly report, we take a closer look at the future of Electric Vehicle (EV) charging with a spotlight on the Extreme Fast Chargers (XFCs). As EVs become more common, faster and smarter charging is becoming essential. This special edition explores how EV charging is getting faster, the risks that come with it, and what companies are doing to keep these systems safe.

This month's report includes the following content:

- [The Future of Secure Extreme Fast Charging \(XFC\)](#)
  - [Global EV Charging Speed Race](#)
  - [XFC Threatscape: Why It's an Attractive Target](#)
  - [Companies Working to Secure XFCs](#)
- [Industry news](#)
- [Patents of the month](#)

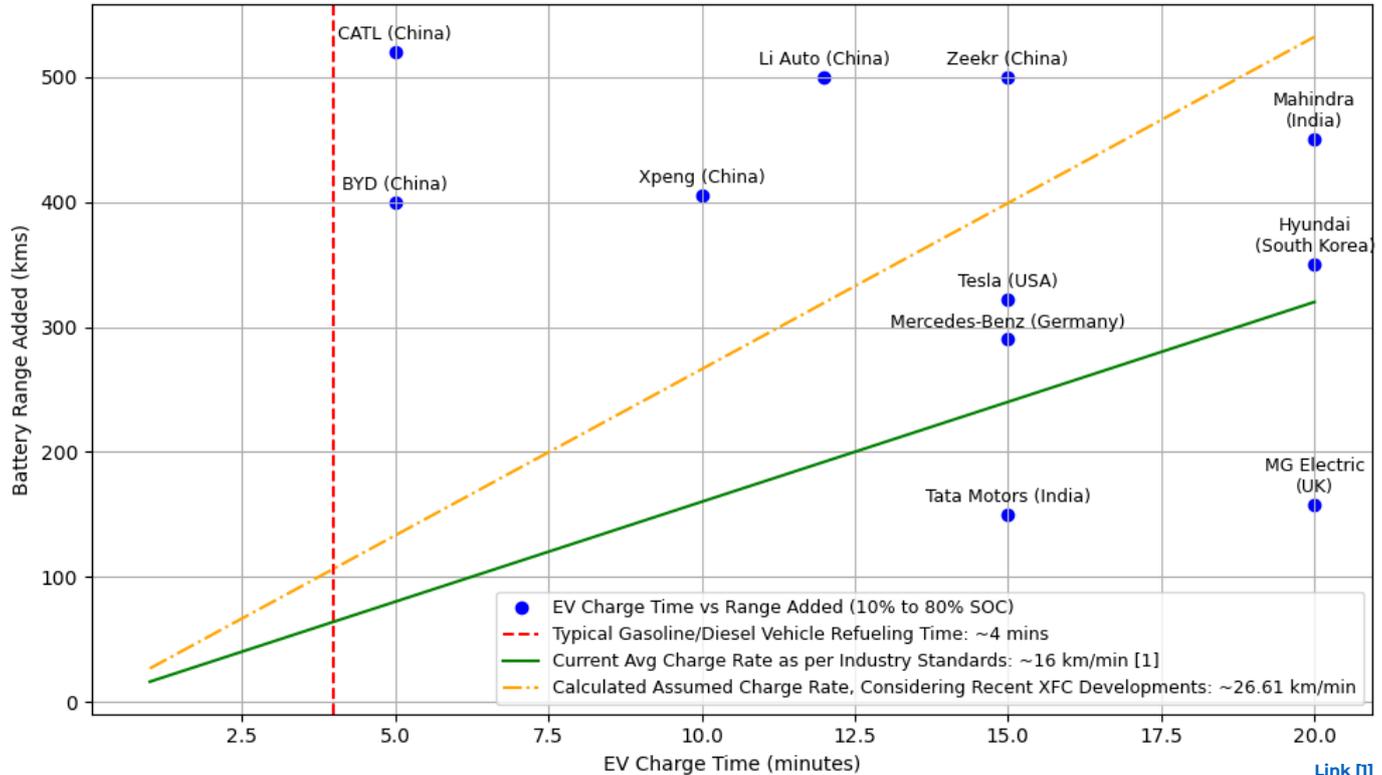
# Key Insights this month

- ❑ As Extreme Fast Chargers (XFCs) begin to rival traditional refueling times, they are set to become more widespread, shifting consumers' expectations toward instant charging convenience. This shift is expected to reduce range anxiety, accelerate EV adoption, and encourage greater investment in charging networks. As demand rises, infrastructure expansion into previously underserved areas will further reshape market dynamics.
- ❑ As high-power chargers adopt more complex digital controls for load balancing, diagnostics, and remote updates, their expanding attack surface will invite more sophisticated cyber threats. This will push stakeholders to prioritize security-by-design frameworks & industry-wide collaboration to safeguard XFCs and, in turn, preserve grid stability.
- ❑ As EV adoption grows, it will be crucial to see how the industry tackles battery degradation from high-rate charging. A lack of standardization across vehicles and chargers may hinder seamless integration, while grid readiness for XFCs, especially in rural areas, remains a major hurdle. Overcoming these will define the pace of XFC's success.
- ❑ Recent flaws in Volkswagen's connected car app allowed hackers to access owners' data simply by taking a photo of the Vehicle Identification Number (VIN) and bypassing the app's OTP system using a simple code. Such incidents highlight the critical importance of protecting sensitive vehicle and user data against evolving cyber threats.
- ❑ Patents published last month emphasize on adaptive behavioral modeling to enhance vehicle cybersecurity by leveraging real-time context, fleet-wide learning, and layered detection to distinguish genuine threats from anomalies, ensuring accurate, efficient, and context-aware responses.



# ◀ The Future of Secure Extreme Fast Charging (XFC)

Fast Charging Comparison for EVs (10% to 80% SOC) vs Fuel Filling & Avg Charge Rate



[Link II](#)

- As charging times approach conventional refueling speeds, EV adoption is expected to accelerate globally.
- The growing reliance on digital systems in extreme fast chargers for power management, safety controls, and efficiency optimization, makes EV charging infrastructure more vulnerable to cyberattacks.

### Higher Power = Higher Risk

XFC systems exceed 350 kW, which heightens the risks of physical harm, equipment damage, and grid instability if compromised by a cyberattack.

**Attack Instance:** [MaDEVloT Attacks, 30MW load shift risks blackout events.](#)



### Real-Time Monitoring Requirements

XFC systems require real-time anomaly detection due to high-speed charging using methods like side-channel monitoring and redundant sensors to counter spoofing, such capabilities are absent in standard chargers.

**Attack Instance:** [EV chargers injected with false grid data](#)



### Thermal Management Vulnerabilities

XFC relies on active thermal management (e.g., liquid-cooled cables). Disabling or spoofing the cooling systems can lead to overheating, a lesser risk in lower-power chargers.

**Attack Instance:** [Change in current to cause physical damages & overheating](#)



## Extreme Fast Charger (XFC) (350 kW+)



### Complexity of Control Systems

XFC systems use advanced control logic like coordinated power electronics, liquid-cooled cables, and complex standards and protocols (ISO 15118, OCPP) which expand attack surfaces and complicate anomaly detection.

**Attack Instance:** [Autel, ChargePoint, and JuiceBox EV Chargers hacked at Pwn2Own](#)



### Lack of Safety Instrumented System (SIS) Integration

By adapting SIS frameworks from critical infrastructure sectors such as nuclear energy, we can introduce industrial-grade safety, real-time diagnostics, and automated shutdown protocols to extreme fast EV charging systems.

**Attack Instance:** [Autel, ChargePoint, and JuiceBox EV Chargers hacked at Pwn2Own](#)



### High Consequence Events (HCEs)

HCEs are events that may trigger grid instability, cause personal injury, or lead to equipment failure. Due to their high-power density and complexity, XFC systems are more vulnerable to such incidents.

**Attack Instance:** [Simulation of HCE attacks by U.S. Department of Energy \(DOE\)](#)

In the coming years, cyber-physical threats will become one of the primary risk vector in high-power EV infrastructures

**Charger-EV  
Sync  
Sequence**

**Cybersecurity Risks**

**Interesting Patents  
& Players working  
in this domain**



Plug-In &  
Handshake

Unencrypted Controller (PLC)  
communication allowing  
eavesdropping & spoofing attacks

[EP4289156A1](#) (Eve Energy  
Ventures Inc),  
[EP4219225A1](#) (Hyundai  
Motors Co)



Authentication

Weak or reused keys extracted  
from non-volatile memory

[US20220063429A1](#) (Cisco  
Technology Inc),  
[US11321482B2](#) (Hyundai  
Motor Co, Kia Corp)



Power  
Negotiation

Manipulated negotiation causing  
overcurrent or battery drainage

[US11305665B2](#) (General  
Electric Co),  
[US11884177B2](#) (Atom Power  
Inc)



Charge  
Session

Firmware corruption via PLC; data  
sniffing during sessions

[US20240291859A1](#),  
[US11336662B2](#) (ABB E-  
mobility B.V.)



V2G  
Communication

Grid Injection attacks; false  
metering; unauthorized access

[US11305665B2](#) (General  
Electric Co),  
[US10833509B2](#)  
(ChargePoint Holdings Inc)



Session  
Termination

Tampering with billing data or  
session hacking

[US20230401613A1](#) (Zeco  
Systems Pte Ltd),  
[WO2022170333A1](#) (Eve  
Energy Ventures Inc.)



## ◀ Industry news

# VicOne's Cybersecurity Upgrade

## **VicOne's Next-Level xAurient Automotive Threat Intelligence Platform Enables Streamlined and Tailored Threat Response**

VicOne has introduced xAurient, a new cybersecurity platform that helps OEMs and suppliers detect and respond to cyber threats early. It delivers tailored threat intelligence, showing how attacks might happen and how to stop them. Unlike basic tools that just collect data, xAurient uses AI trained on decades of information and scans the dark web and social media to identify and prioritize serious risks. It can integrate with existing vehicle security systems or work independently, reducing manual effort for cybersecurity teams by automatically flagging the most critical threats. Designed for modern, software-driven vehicles, xAurient is scalable, cost-effective, and already proven useful, with VicOne having uncovered over 100 major flaws in connected cars and EV chargers.

Source

<https://vicone.com/>



# Partnership

## **Xiphera Partners with Siemens Cre8Ventures to Strengthen Automotive Security and Support EU Chips Act Sovereignty Goals**

Xiphera, a provider of hardware-based cryptographic solutions that protect critical systems like ECUs and telematics from hacking, has partnered with Siemens Cre8Ventures to boost cybersecurity in the automotive industry through the Digital Twin Marketplace. With the rise of quantum computing, Xiphera's solutions helps future-proof vehicle security. Their cryptographic IP also helps automakers meet global cybersecurity standards like ISO/SAE 21434 and regulations like UNECE WP.29. This partnership makes it possible for OEMs and Tier 1 suppliers to integrate Xiphera's cryptographic solutions directly into their virtual car (digital twin) models on Siemens' PAVE360 platform, enabling early-stage security implementation, ensuring vehicles are secure by design.

Source

<https://xiphera.com/>



# Trusted UGV Certification

## AUVSI Launches "Trusted UGV" Cybersecurity and Supply Chain Certification at XPONENTIAL 2025

AUVSI, a global nonprofit that promotes safe and ethical use of uncrewed systems, has launched the Trusted UGV certification, focused on cybersecurity and supply chain safety for uncrewed ground vehicles (UGVs). Developed with Neya Systems, a division of Applied Research Associates specializing in autonomous systems. This certification addresses growing cyber risks as UGVs become more common in defense, logistics, and infrastructure, where their reliance on software and connectivity makes them vulnerable to attacks. Trusted UGV sets a new standard to ensure UGVs are secure, reliable, and ready for critical missions. It evaluates product security, remote operations, and supply chain integrity, while supporting both commercial and government applications & aligning with federal cybersecurity policies.

Source

<https://www.auvsi.org/>



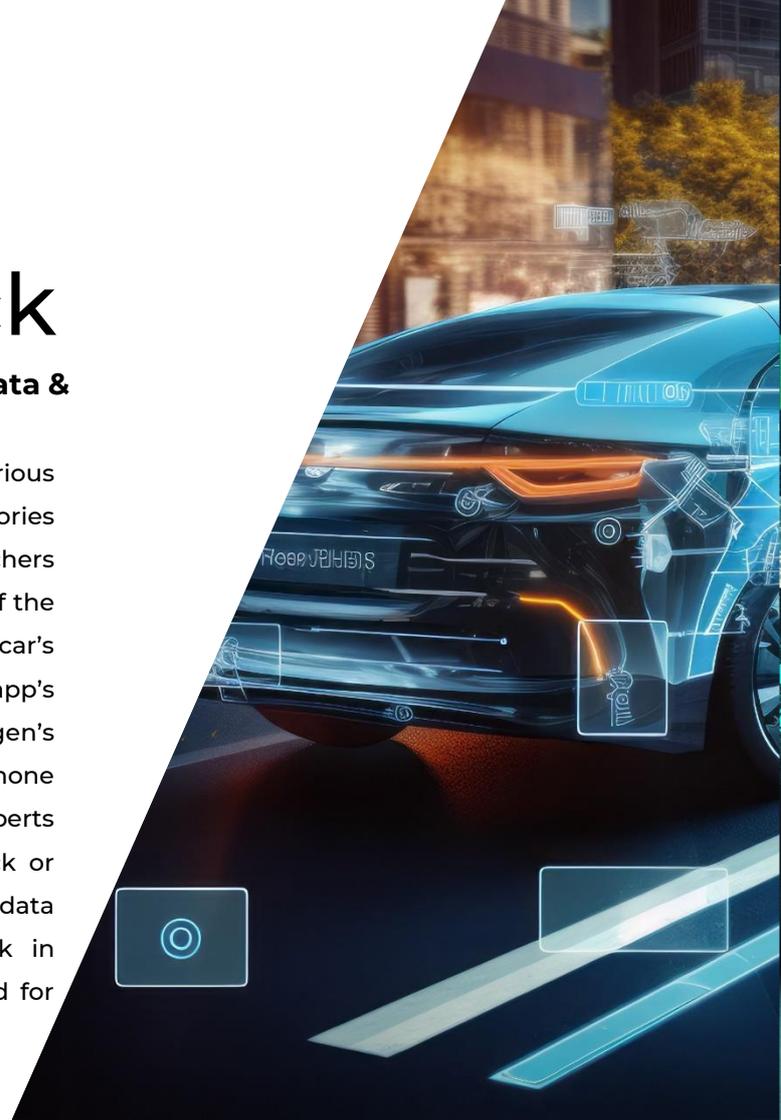
# Volkswagen Hack

## Volkswagen Car Hacked – Owner’s Personal Data & Service Details Exposed

Volkswagen’s connected car app was found to have serious security flaws that exposed personal data and service histories of vehicles worldwide. The issue allowed security researchers to access sensitive information by simply taking a photo of the Vehicle Identification Number (VIN) visible on the car’s windshield. A simple code was then used to bypass the app’s OTP system, revealing multiple vulnerabilities in Volkswagen’s APIs. The leaked data included names, addresses, phone numbers, vehicle locations, and engine statistics. Experts warned that such access could enable criminals to track or target individuals. This marks Volkswagen’s second major data breach in six months, following a cloud storage leak in December 2024. The incident highlights the urgent need for stronger cybersecurity in connected vehicles.

Source

<https://cybersecuritynews.com/>



# Securing Autonomous Minibuses

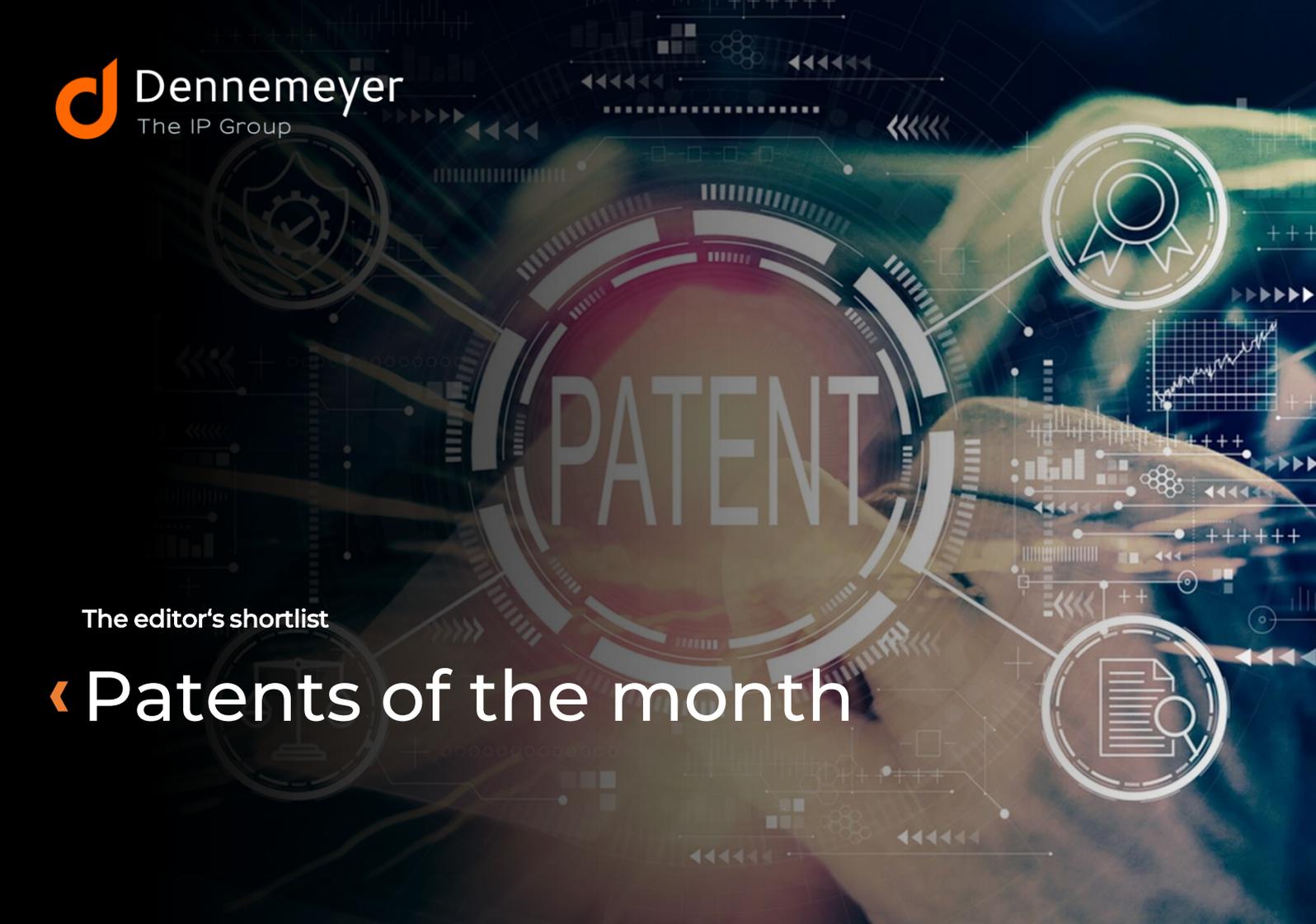
## **TIER IV Selects PlaxidityX to Provide Cyber Security Expertise for The Japanese Airport Autonomous Bus Project**

PlaxidityX has partnered with TIER IV, a company known for its open-source self-driving vehicle software, to ensure their technology is safe from cyberattacks and meets global safety rules. TIER IV was selected for a Japanese government project to deploy self-driving minibuses at airports, which required compliance with the UN-R155 regulation and ISO/SAE 21434 standard. To support this, PlaxidityX conducted a cybersecurity gap analysis and timely delivered reports on threat assessments. Additionally, TIER IV later engaged with PlaxidityX to implement a Cyber Security Management System, highlighting the growing importance of cybersecurity in self-driving vehicles.

Source

<https://plaxidityx.com/>





PATENT

The editor's shortlist

# ◀ Patents of the month

## Patents of the month

## Published in May 2025

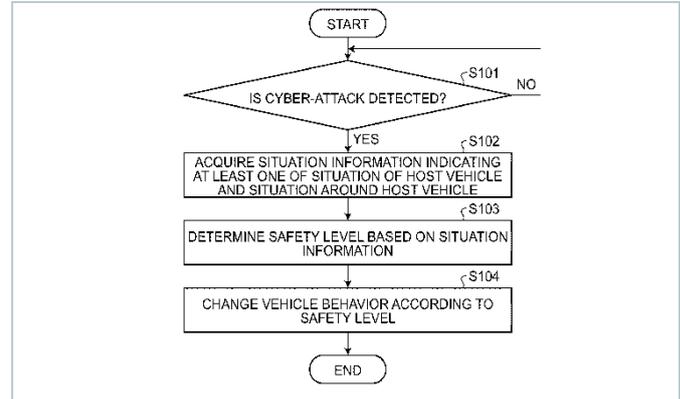


### Shortlisted and summarized by our analyst

- [US2025145182A1](#) - Vehicle Behavior Control Method And Vehicle Behavior Control Device  
Assignee: [Panasonic Automotive System Co Ltd](#)
- [US12301591B2](#) - System and method for connected vehicle cybersecurity  
Assignee: [Upstream Security Ltd](#)
- [US12309184B2](#) - System and method for providing security to in-vehicle network  
Assignee: [Hyundai Motor Co; Kia Corp](#)
- [EP4561022A1](#) - Vehicular control unit comprising a partitioning system for at least one security-relevant network line due to a cyber-attack and related road vehicle  
Assignee: [Ferrari Spa](#)
- [IN202421034487A](#) - Intrusion detection system for connected vehicles  
Assignee: [Matter Motor Works Pvt Ltd](#)
- [WO2025103243A1](#) - Intrusion detection method and apparatus, and vehicle  
Assignee: [Shenzhen Yinwang Intelligent Tech Co Ltd](#)
- [DE102024131322A1](#) - Test procedure and test system for testing the security of a vehicle against cyber attacks  
Assignee: [FEV Group GMBH](#)
- [JP2025075389A](#) - Vehicle security analysis system, vehicle security analysis method, and program  
Assignee: [NTT Security Japan Corporation](#)
- [KR20250072196A](#) - CAN communication security method for detecting CAN bus attacks, recording medium and CAN communication device for performing the same  
Assignee: [AY Innovation Co., Ltd.](#)
- [CNT19995974A](#) - Unmanned aerial vehicle Internet of things DDoS attack detection method based on neural network  
Assignee: [Jinan Univ](#)

◀ US2025145182A1

# Vehicle behavior control method and vehicle behavior control device



This patent describes a way to safely manage vehicle behavior during cyber-attacks, particularly in self-driving vehicles. Upon detecting a cyber-attack, the system gathers real-time data on the vehicle's condition and surroundings to assess the situation. Based on this information, it determines a safety level and selects an appropriate response to the threat. This approach helps prevent sudden braking, stops or distracting alerts that could endanger passengers and other road users. By tailoring actions to the current driving context, it enhances both threat detection and response, ensuring safer handling of cyber risks in both manual and self-driving scenarios.

Company name Panasonic Automotive System Co Ltd

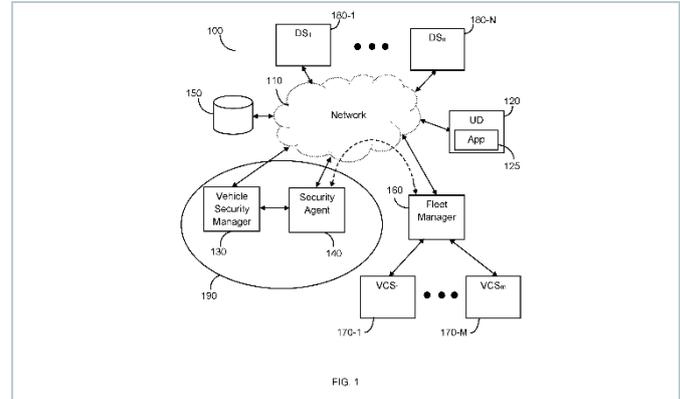
Inventors Fukumoto Satoshi

Priority date 02-Nov-2023

Publication date 08-May-2025

◀ **US12301591B2**

# System and method for connected vehicle cybersecurity



This invention presents a way to protect connected and self-driving cars from cyberattacks by learning what normal behavior (behavior modeling) looks like. A remote system collects operational data from a group (fleet) of vehicles and builds a normal behavior model for each vehicle and its sub-fleet based on past information and events. These models help spot unusual behavior by comparing new data against expected patterns. When something suspicious is found, the system decides how to respond and stop possible threats. This approach allows for real-time threat detection using machine learning and adapts security policies based on the nature of the threat. It helps keep the cars safe by quickly reacting to cyberattacks in a smart and organized way across a hierarchical fleet structure.

Company name Upstream Security Ltd

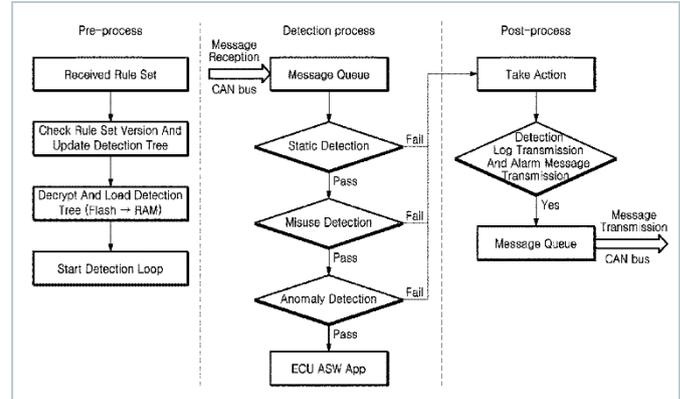
Inventors Appel Yonatan,  
Levy Yoav

Priority date 27-Jul-2017

Publication date 13-May-2025

US12309184B2

# System and method for providing security to in-vehicle network



This invention describes an electronic device that helps protect the car's internal network, which is increasingly at risk due to the growing number of Electronic Control Units (ECUs) connected via both wired and wireless systems. The device has a small computer that monitors network messages using a message queue and a set of rules. These rules use a layered detection approach, including checking for known problems, unusual behavior, and applying threat detection techniques to identify potential threats. It updates its rule set from a backend server and stops further checks once a threat is detected, improving efficiency. This system can be added to existing vehicle components or operate as a separate unit, offering flexible integration and faster threat detection while conserving resources.

Company name Hyundai Motor Co; Kia Corp

Inventors Park Seung Wook,  
Kim Seil, Cho Aram

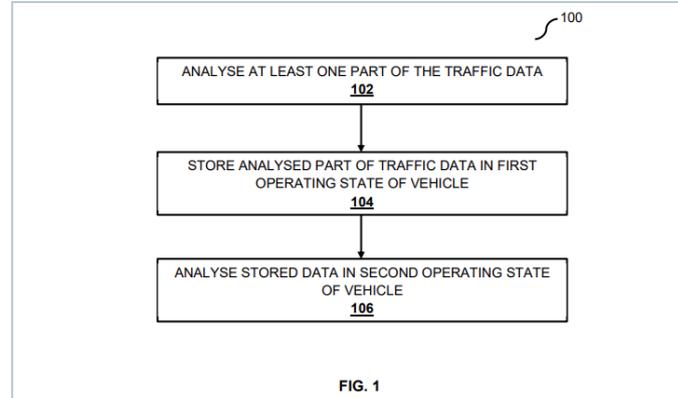
Priority date 23-Jan-2018

Publication date 20-May-2025



◀ IN202421034487A

## Intrusion detection system for connected vehicles



This patent introduces an intrusion detection system (IDS) designed to enhance the security of connected networks in vehicular systems. Instead of just protecting data with encryption, it also monitors how data moves around and looks for unusual behavior or timing problems that might indicate something is wrong or someone is attacking. This system addresses that gap by collecting data, analyzing it, and spotting faults through real-time communication monitoring. It compares current activity with past records to detect anything suspicious. If threats are found, the system assigns threat codes to suspicious packets, enabling quick isolation of malicious activity. This layered setup helps find problems faster, keeps the car's network running smoothly, and ensures that all connected devices can communicate safely.

Company name Matter Motor Works Pvt Ltd

Inventors Kumar Prasad Telikepalli,  
Satish Thimmalapura,  
Pankaj Kumar Bharti

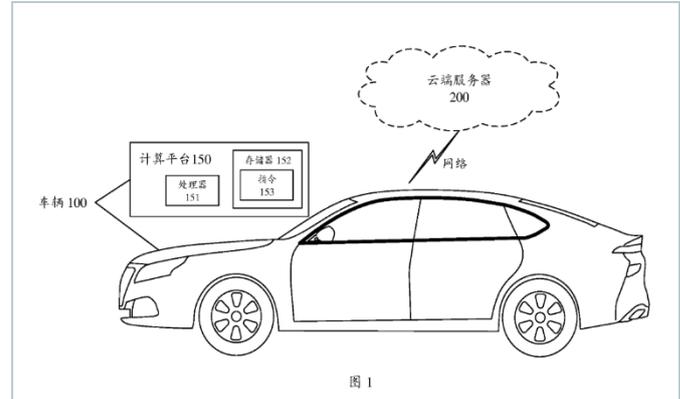
Priority date 01-May-2024

Publication date 09-May-2025



WO2025103243A1

# Intrusion detection method and apparatus, and vehicle



This patent talks about protecting self-driving vehicles from hackers trying to fool the car's location system, which could lead to dangerous driving decisions. The system works by collecting two types of data: one about things that don't move, like signs and buildings, and another about things that do move, like other cars and people around the car. It then uses a set of detection rules to compare this real-world data with expected environmental information to spot any inconsistencies that may signal an intrusion or threat. By relying on multiple sensor inputs instead of just GPS, the method becomes more resistant to spoofing attacks. This multi-layered detection approach allows the vehicle to identify threats in real time and maintain safe navigation even under potential cyber threats.

Company name Shenzhen Yinwang Intelligent Tech Co Ltd

Inventors Lv Qi,  
Liu Shenglin

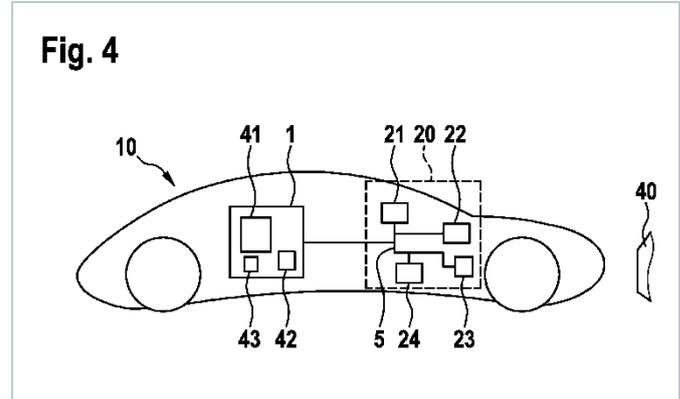
Priority date 14-Nov-2023

Publication date 22-May-2025



◀ DE102024131322A1

## Test procedure and test system for testing the security of a vehicle against cyber attacks



This patent tests how secure a vehicle is against cyberattacks by using a specialized test system that automates the process. The system first selects a specific vehicle component using a selection module, then simulates a cyberattack on that component using a simulation module, and finally observes the effects of the attack. This approach allows for efficient and targeted testing of vulnerabilities in different parts of the vehicle. By automating the selection and simulation steps, the system reduces the need for manual work and speeds up the testing process. It also enables testing multiple attack scenarios quickly, making the overall security assessment more thorough and effective.

Company name FEV Group GMBH

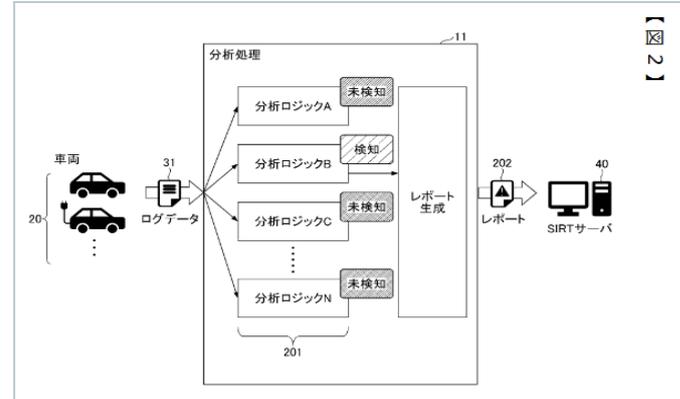
Inventors Mateusz Dedo

Priority date 17-Nov-2023

Publication date 22-May-2025

◀ JP2025075389A

# Vehicle security analysis system, vehicle security analysis method, and program



This invention discloses a vehicle security analysis system that collects sensor data from in-vehicle devices and checks whether the data is related to normal vehicle behavior or a potential cyber-attack. It uses information about what the car is doing currently to decide if an alert is a false alarm or a real threat. A special device manages and estimates the vehicle's condition using either the sensor data or information from the vehicle or an external server. If it is found that the suspicious data doesn't match any real cyber-attack activity, it marks it as a false positive and ignores it. This helps reduce unnecessary work for the system and improves the accuracy of detecting real cyber threats. The invention improves vehicle cybersecurity by filtering out harmless events and focusing only on genuine risks.

Company name NTT Security Japan Corporation

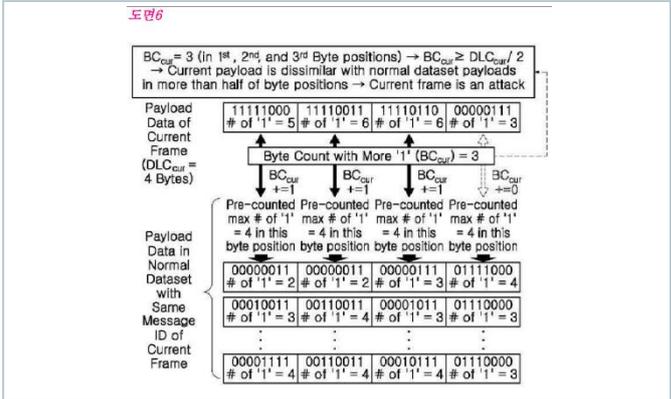
Inventors Yasunobu Chiba,  
Manabu Nakamura,  
Wataru Ueno,  
Masashi Tanaka,  
Kensuke Nakata

Priority date 31-Oct-2023

Publication date 15-May-2025

**KR20250072196A**

# CAN communication security method for detecting CAN bus attacks, recording medium and CAN communication device for performing the same

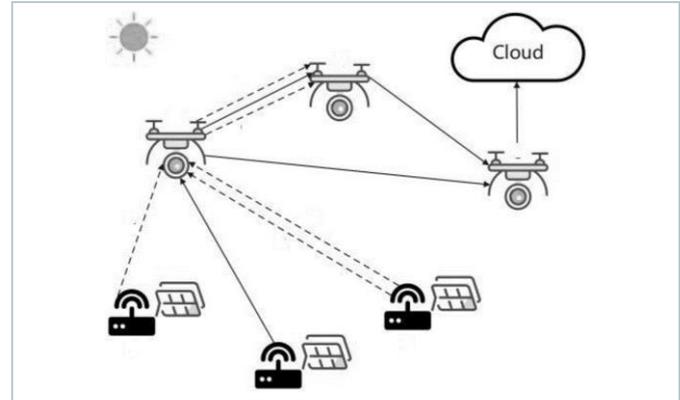


This patent improves the detection of cyberattacks on Controller Area Network (CAN) systems used in vehicles. It works by first analyzing CAN data frames using a trained IDS to identify possible attack types like Denial-of-Service (DoS), spoofing, or sending confusing data (fuzzing) attacks. Then, it applies a set of rules to recheck and confirm these results more accurately. For example, even if a message seems normal at first, it may still be flagged as an attack if it appears too often or has unusual message IDs or data patterns. The system also considers how much the data changes over time to detect fuzzing attacks. This approach helps catch attacks that might slip past the initial detection and reduces false alarms by using real-world attack patterns.

Company name	AY Innovation Co., Ltd.
Inventors	Lee Sung-Su, Lim Hyung-Cheol
Priority date	16-Nov-2023
Publication date	23-May-2025

◀ CN119995974A

# Unmanned aerial vehicle Internet of things DDoS attack detection method based on neural network



This patent is about protecting drones that use the Internet to communicate with each other from being overwhelmed by cyberattacks called Distributed Denial of Service (DDoS) attacks. These attacks flood the system with too much traffic, making it hard for the drones to work properly. Current methods to stop these attacks don't work well when many drones are attacked at once. This invention uses a neural network that monitors the data coming from the drones, spots harmful traffic, and blocks it. The system keeps learning and improving over time, adjusting to changes in the environment. It also helps avoid false alarms and ensures the drones use their energy and resources wisely. This makes the whole drone network safer and more efficient.

Company name	Jinan Univ
Inventors	Wen Jinming, Zheng Mingrui, He Tengjiao, Chen Benyu, Tan Zhihe
Priority date	05-Feb-2025
Publication date	13-May-2025

# We are now in India

## Your global full-service IP partner

With 60+ years of experience and over 20 offices worldwide, Dennemeyer Group is committed to being the first choice partner for the protection and management of Intellectual Property (IP) rights globally.

Our India office is your gateway to the world of IP, offering a single point of contact and full-service IP management solutions to support you throughout your IP life cycle.



IP consulting



IP law firm  
services



IP maintenance  
services



IP management  
software



Octimine patent  
analysis software

## By the numbers



Founded in  
**1962**



**180**  
jurisdictions  
covered worldwide



**~2 Million**  
patents maintained



**~1 Million**  
trademarks managed



**>60**  
years  
of experience in IP



**>20**  
global offices



**>900**  
employees and  
associates

## Global presence



Abu Dhabi, UAE



Beijing, CN



Bengaluru, IN



Brasov, RO



Chicago, USA



Dubai, UAE



Howald, LU



Johannesburg, ZA



Manila, PH



Melbourne, AU



Munich, DE



Paris, FR



Rio de Janeiro, BR



Rome, IT



Singapore, SG



Stockport, UK



Taipei, TW



Tokyo, JP



Turin, IT



Warsaw, PL



Woking, UK



Zagreb, HR



Zug, CH

## Talk to us now

Find out how we can support you  
in these services and more.

- International Patent and Trademark Renewals
- International Patent and Trademark Filings
- European Patent Validation
- PCT Nationalization
- Recordals
- DIAMS IP Management Software
- Patent Search & Analysis



# Visit us

at [www.dennemeyer.com](http://www.dennemeyer.com) to find out more about us.

 Denne Meyer India Private Limited  
Bengaluru  
[info-india@dennemeyer.com](mailto:info-india@dennemeyer.com)

 North & East India  
**+91 9818599822**

South & West India  
**+91 88266 88838**