

Report of July 2024

Cybersecurity in mobility

Recent developments

Curated and summarized - Industry and Patent news

Published by Denne Meyer India Private Limited

Parag Thakre (pthakre@dennemeyer.com)

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.

Key Insights

- ❑ Cybersecurity firms are increasingly collaborating with software companies to integrate security measures at the outset of a car's software development lifecycle. This collaborative approach emphasizes the "Shift-Left" approach, which prioritizes proactive security integration from the earliest stages of development.
- ❑ Automakers are recognizing the need to work with cybersecurity companies to secure their entire supply chain, not just their software development processes.
- ❑ New standard (IS 18590: 2024 and IS 18606: 2024) has been introduced to enhance the safety of Electric Vehicles in India.
- ❑ A recent patent application reveals a novel feature called a 'boarding determiner' which analyzes cyberattacks and notifies users about the safety of entering their vehicle.
- ❑ Innovative security solutions have been patented as electronic control units (ECUs) become more vulnerable to cyberattacks. These solutions leverage advanced encryption and authentication techniques to safeguard ECU software, firmware, and inter-ECU communication. Additionally, methods for identifying software vulnerabilities are being developed to further bolster overall vehicle network security.

Strategic collaboration

Argus Cyber Security Collaborates with Microsoft to Redefine Next Generation Automotive Security

Argus Cyber Security has partnered with Microsoft to develop a next-generation platform for securing connected vehicles. This "Argus Vehicle Security Platform" combines Argus' existing security solutions with Microsoft's software development and security tools. This collaboration focuses on a "shift left" approach, where security is integrated early in the development process of car software. This aims to improve overall software quality and security, while also speeding up development and reducing costs. The platform consists of two parts: Automotive Shift-Left Security and Automotive Security Lifecycle Management.

Source

argus-sec.com



Threat Intelligence

Revolutionizing Automotive Cybersecurity, VicOne & ASRG Team Up for Unrivaled Coverage of Automotive Threat Intelligence

VicOne has partnered with the Automotive Security Research Group (ASRG) to launch a new database called AutoVulnDB. This database focuses upon existing sources of vulnerabilities provided by NVD (National Vulnerability Database) and MITRE CVE (Common Vulnerabilities and Exposures) to uniquely provide enhanced contextual and situational data that is specific to the automotive industry. AutoVulnDB integrates with existing bug bounty programs to provide comprehensive coverage of potential security weaknesses. With the growing number of connected cars on the road, the need for robust cybersecurity is crucial.

Source

<https://vicone.com/>



ISO 21434 certification

QNX Certified to the Latest Automotive Cybersecurity Standard

QNX, has received ISO 21434 certification, a major achievement in automotive cybersecurity. This certification ensures QNX's development processes meet the highest security standards, allowing them to better support car manufacturers who need to comply with regulations like UNECE WP.29. By following these practices, QNX not only strengthens the security of their own software but also helps automakers build secure vehicles. This benefits both sides: QNX customers gain a secure foundation for their automotive systems and car manufacturers can streamline compliance and ensure the safety of their vehicles in an increasingly connected world.

Source

<https://blogs.blackberry.com/>



EV Security Boost

Leading EV Manufacturer BYD Selects Karamba Security to Meet Global Automotive Cybersecurity Regulations

BYD, has chosen Karamba Security's VCode software to secure its supply chain and comply with cybersecurity regulations. VCode automatically creates a Software Bill of Materials (SBOM) for BYD's electronic control units (ECUs), identifying potential vulnerabilities and ensuring secure software. This allows BYD to keep pace with the growing EV market while meeting regulations and protecting customers from cyberattacks. VCode integrates seamlessly with existing development processes and offers a comprehensive view of potential security risks within the software.

Source

<https://www.karambasecurity.com/>



Standards for EV

Bureau of Indian Standards introduces 2 new standards to enhance safety, quality of Electric Vehicles

The Bureau of Indian Standards (BIS) has introduced two new safety regulations IS 18590: 2024 and IS 18606: 2024 to improve the quality and safety of electric vehicles (EVs) in India. These standards apply to L, M, and N category. The new rules focus on stricter safety requirements for a critical EV component: the powertrain (motor and battery system). This aims to ensure EVs are built more securely and are less prone to accidents. With these new standards, India now has a total of 30 specific regulations for EVs and their accessories, signifying a major push for safer and higher quality electric vehicles in the country.

Source

<https://auto.economicstimes.indiatimes.com>





PATENT

The editor's shortlist

Patents of the month

Patents of the month

Published in Jun 2024

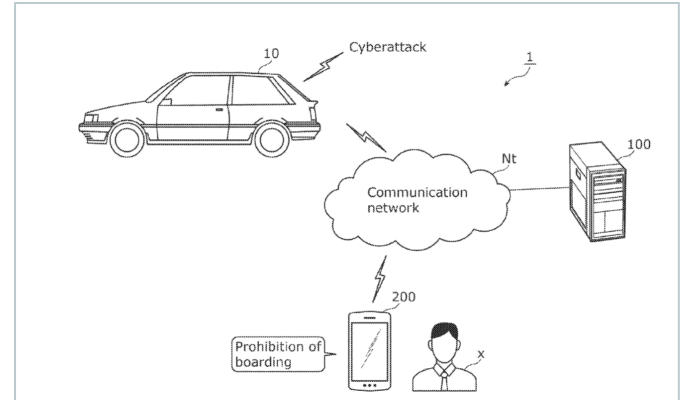
Shortlisted and summarized by our analyst



- [US2024195822A1](#) - Security apparatus, security method, and recording medium
Assignee: [Panasonic IP Management CO LTD](#)
- [US11999364B2](#) - Systems and methods for intrusion detection in vehicle systems
Assignee: [Intel Corp](#)
- [US12001553B2](#) - Detecting vehicle malfunctions and cyber attacks using machine learning
Assignee: [Red Bend Ltd \(Samsung Group\)](#)
- [US12010518B2](#) - System and method for securely defending against collusive attack under internet of vehicles
Assignee: [Xian Univ Of Posts & Telecom, Xian Anmeng Intelligent Tech Co Ltd](#)
- [US2024195813A1](#) - Secure communication between In-vehicle Electronic Control Units
Assignee: [Nagravision SA](#)
- [EP4381402A1](#) - Software vulnerability analysis
Assignee: [Continental Automotive Tech GMBH](#)
- [EP3547191B1](#) - System and method of generating rules for blocking a computer attack on a vehicle
Assignee: [AO Kaspersky Lab](#)
- [DE102023120706A1](#) - Security system for electronic devices connected to a vehicle
Assignee: [GM Global Technology Operations LLC](#)
- [WO2024119401A1](#) - Anomaly detection method and apparatus, and vehicle
Assignee: [Huawei Technology Co Ltd](#)
- [CN118175536A](#) - Safety state analysis method and system for vehicle
Assignee: [General Motors CO, SAIC General Motors Corp Ltd](#)

《 US2024195822A1

Security apparatus, security method, and recording medium



This patent tackles a critical gap in existing car cybersecurity systems: the lack of user support during cyberattacks when the user isn't present. This invention proposes a novel security apparatus, It features a "boarding determiner" which analyzes the cyberattack and decides if it's safe to enter the vehicle. The system then communicates this decision directly to the user's smartphone or other external device. If boarding is unsafe, the system can suggest alternative transportation options, further aiding the stranded user. Additionally, it can take countermeasures against the attack itself, like preventing the car from starting or restoring altered programs.

Company name Panasonic IP Management CO LTD

Inventors Iguchi Akihiko

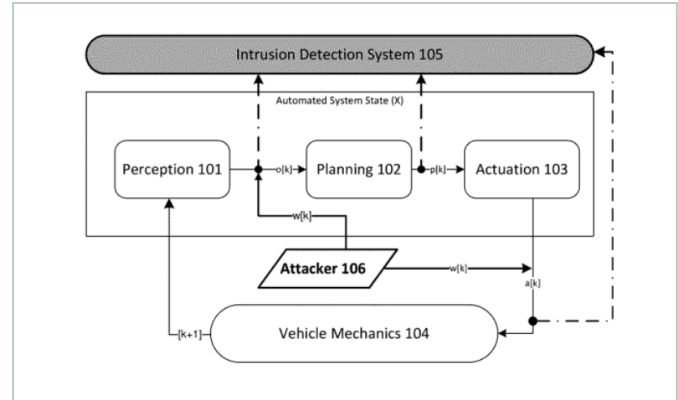
Priority date 07-Dec-2022

Publication date 13-Jun-2024



« US11999364B2

Systems and methods for intrusion detection in vehicle systems



This patent focuses on safeguarding automated vehicles from cyberattacks that target communication within the vehicle control system (VCS). The proposed solution involves an Intrusion Detection System (IDS) integrated within the VCS. The IDS anticipates a vehicle's expected behavior based on incoming messages from various control units. It then calculates a "reachable set" that considers potential uncertainties in the environment. Any significant discrepancies between the expected behavior and the reachable set indicate a potential intrusion. It can also pinpoint the source of the attack and its criticality based on predefined safety models.

Company name Intel Corp

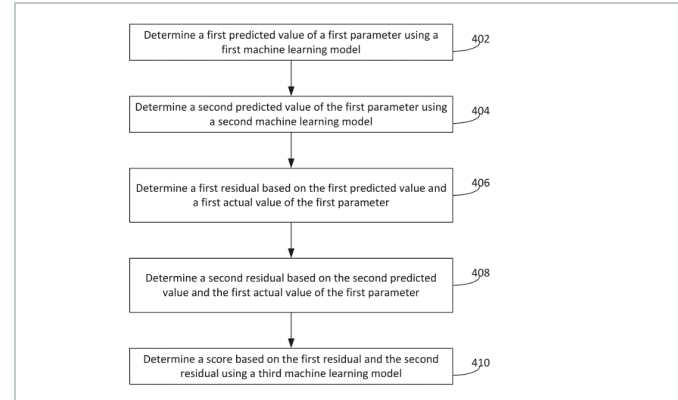
Inventors Alvarez Ignacio J,
Elli Maria Soledad,
Felip Leon Javier,
Turek Javier Sebastian,
Gonzalez Aguirre David Israel

Priority date 23-Dec-2020

Publication date 04-Jun-2024

« US12001553B2

Detecting vehicle malfunctions and cyber attacks using machine learning



This patent proposes a new method to combat the growing threat in connected cars. It uses machine learning models to detect anomalies or cyberattacks in vehicles. It's unique because it employs a multi-layered approach. The first layer uses multiple models (like time series and regression) to predict normal vehicle behavior based on various operational parameters. The second layer then analyzes the differences between the predicted and actual values to identify suspicious activity. The proposed machine learning method for vehicle security offers a powerful defense against cyberattacks. By combining multiple models and using a layered analysis, it makes robust predictions and adapts to new threats without needing frequent updates.

Company name Red Bend Ltd (Samsung Group)

Inventors Cohen Dror,
Kreines Alexander,
Mendelowitz Shachar

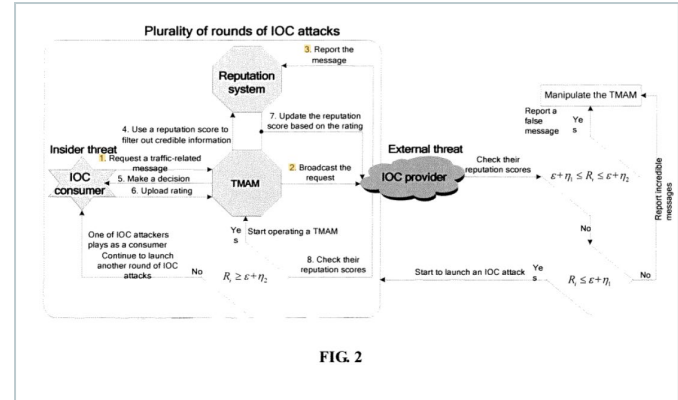
Priority date 20-Aug-2020

Publication date 04-Jun-2024



US12010518B2

System and method for securely defending against collusive attack under internet of vehicles



This patent tackles collusion attacks on the Internet of Vehicles (IoV) where attackers manipulate traffic information. The solution involves a system that analyzes how reputations fluctuate to identify suspicious activity and remove malicious actors. This "Reputation Fluctuation Association Analysis" (RFAA) helps prevent the spread of misinformation and ensures reliable communication within the IoV network, improving overall traffic safety and efficiency.

Company name Xian Univ Of Posts & Telecom,
Xian Anmeng Intelligent Tech Co Ltd

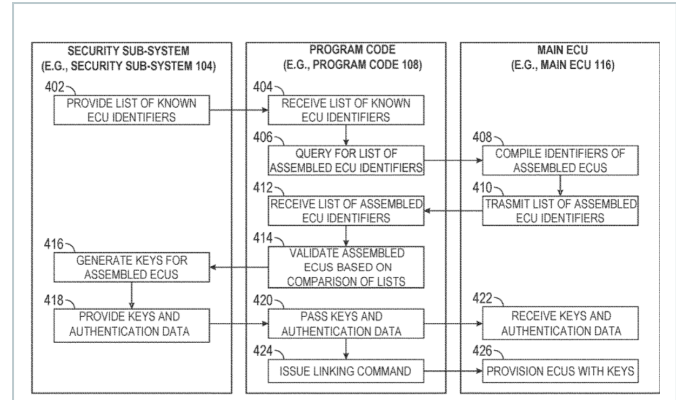
Inventors Zhao Feng,
Feng Jingyu

Priority date 20-May-2019

Publication date 11-Jun-2024

《 US2024195813A1

Secure communication between In-vehicle Electronic Control Units



This patent tackles the growing problem of cyberattacks targeting vehicles with multiple electronic control units (ECUs). The solution involves a system where a central ECU securely distributes encryption keys and unique authentication data to each ECU. This data includes details like valid timeframes for messages and permitted operations, ensuring only authorized communication occurs. Additionally, the system enables secure over-the-air firmware updates for ECUs by utilizing digital certificates. Overall, this patent improves in-vehicle communication security by implementing robust encryption and authentication measures.

Company name Nagravision SA

Inventors Buffard Christophe,
Sehgal Sanjeev

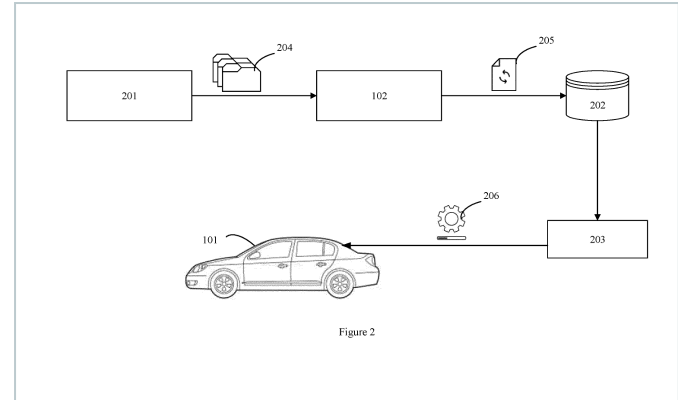
Priority date 29-Jan-2018

Publication date 13-Jun-2024



《 EP4381402A1

Software vulnerability analysis



This patent talks about the growing risk of software vulnerabilities in modern vehicles, which can cause critical system failures or make cars susceptible to hacking, potentially leading to accidents. The proposed solution involves an automated system that analyzes software applications used in vehicles. This analysis considers various factors, including automotive safety standards and known security threats. The system identifies vulnerabilities, updates security databases to reflect new findings, and provides patches to fix the issues. This method offers several improvements: automation for faster detection, real-time updates for better threat protection, and comprehensive analysis using multiple data sources to ensure a thorough evaluation of software security in vehicles.

Company name Continental Automotive Tech GMBH

Inventors Xiong Siyang,
Habib Sheikh Mahbub,
Wang Yi,
Dehm Mathias

Priority date 05-Aug-2021

Publication date 12-Jun-2024



《 EP3547191B1

System and method of generating rules for blocking a computer attack on a vehicle

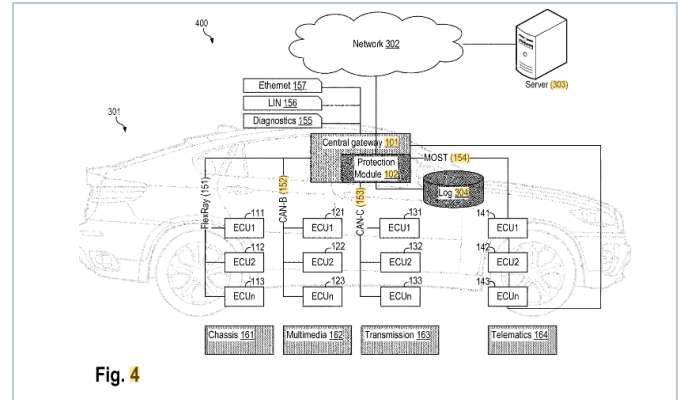


Fig. 4

This patent tackles the rising threat of cyberattacks targeting Electronic Control Units (ECUs) in vehicles, which can cause accidents. Current systems struggle to detect these complex attacks. The solution proposes a system that analyzes intercepted messages during security incidents. By identifying malicious messages and their intended ECU targets, the system generates specific rules to block or alter future communication attempts. This method offers several improvements such as targeted defense, active protection and adaptive learning. Overall, this patent provides a more comprehensive and adaptable approach to vehicle cybersecurity by leveraging real-time analysis and targeted rule creation.

Company name AO Kaspersky Lab

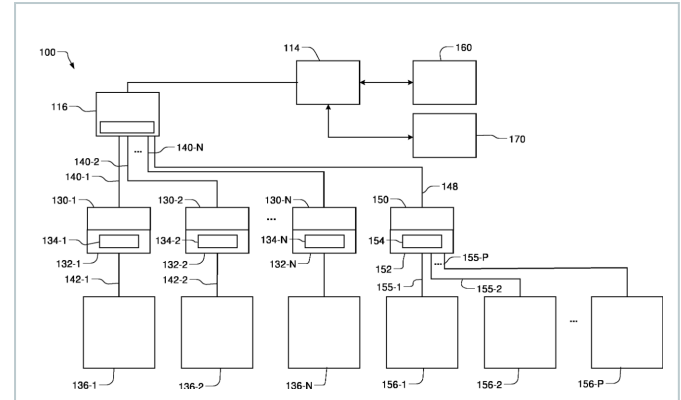
Inventors Dyakin Pavel V,
Shadrin Alexander V,
Kulagin Dmitry A

Priority date 30-Mar-2018

Publication date 05-Jun-2024

« DE102023120706A1

Security system for electronic devices connected to a vehicle



This patent focuses on improving car safety by ensuring all connected devices are authenticated. Current systems struggle with aftermarket parts that might not meet safety standards. The solution involves a security system embedded within the connector itself. This system verifies the legitimacy of the connected device before allowing it to function. If authentication fails repeatedly, the car's systems can take action, potentially impacting drivability. By guaranteeing only authorized components operate within the vehicle, this patent aims to enhance overall safety and reliability.

Company name GM Global Technology Operations LLC

Inventors Lowe Infane,
Winger Lyall Kenneth

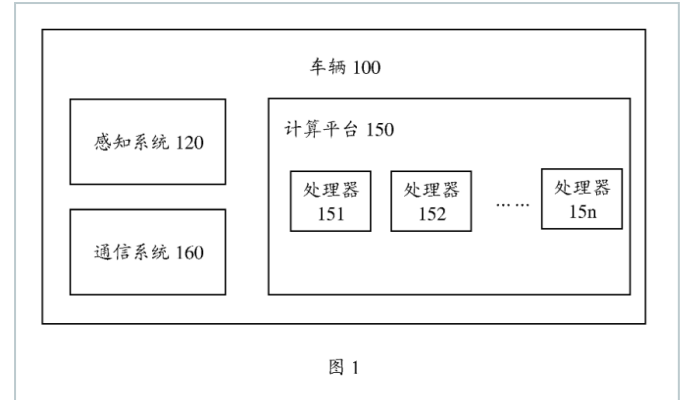
Priority date 19-Dec-2022

Publication date 20-Jun-2024



《 WO2024119401A1

Anomaly detection method and apparatus, and vehicle



This patent tackles the challenge of pinpointing anomalies in vehicles, especially those with advanced driver-assistance systems. The solution involves a real-time method that analyzes a vehicle's motion data (from sensors and potentially external sources) to detect and locate problems. This method doesn't require large amounts of training data and can pinpoint the exact source of the anomaly, whether it's a faulty sensor, an internal communication issue, or even an external network problem. This offers a versatile and efficient way to identify problems within various connected vehicles.

Company name Huawei Technology Co Ltd

Inventors Yang Tianci,
Feng Xiangbing,
Wei Zhuo,
Yao Hanbo

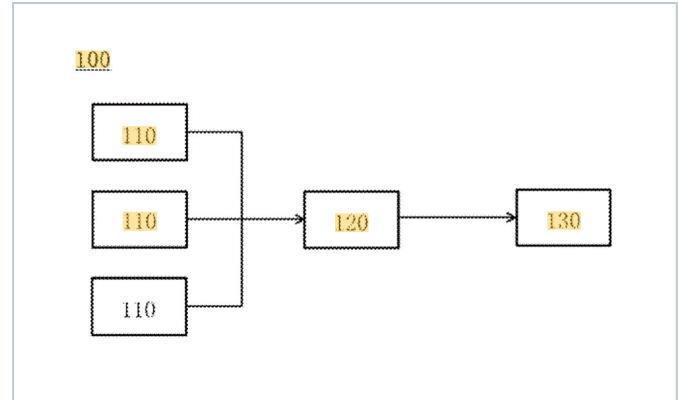
Priority date 07-Dec-2022

Publication date 13-Jun-2024



《 CN118175536A

Safety state analysis method and system for vehicle



This patent tackles the critical issue of ensuring robust network security in vehicles by promptly detecting and responding to threats across various electronic modules. It provides a system that gathers detailed security information from these modules, including specific error codes and environmental context. This data is then packaged and transmitted to a central location for ongoing analysis. This method offers several advantages: detailed alarm messages pinpoint the exact issue, repeated problems are tracked due to cumulative recording, and packaged data ensures continuous monitoring for timely threat detection.

Company name	General Motors CO , SAIC General Motors Corp Ltd
Inventors	Bi Xiaodong, Feng Haitao, Gu Xiaoli, Liu Min, Tong Fei, Wang Meng
Priority date	01-Dec-2022
Publication date	11-Jun-2024



We are now in India

Your global full-service IP partner

With **60 years of experience** and **23 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 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
Vargarda, SE
Warsaw, PL
Woking, UK
Zagreb, HR

Talk to us now


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


- Patent Renewals
- Trademark Renewals
- Trademark Filing
- Recordals
- PCT Nationalization
- European Patent Validation
- DIAMS IP Management Software
- IP Analytics



Visit us

at www.dennemeyer.com to find out more about us.

 Denнемeyer India Private Limited
Bengaluru
info-india@dennemeyer.com

 North & East India
+91 79831 15166

South & West India
91 88266 88838

