

Report of June 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](mailto: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

- ❑ A new DevSecOps platform launched to tackle security vulnerabilities in Software-Defined Vehicles (SDVs) by integrating threat analysis, code security management, and automated testing functionalities.
- ❑ To comply with the UNR 155 regulations, companies are collaborating to develop the cybersecurity solutions for vehicles such as vulnerability management, API security, encryption keys management and software signing.
- ❑ Multiple inventions are patented to protect the vehicle's internal network from cyber attacks for example, time-based packet analysis, periodic packet sampling, and packet filtering algorithms.
- ❑ A patent application describes a secure way to perform over-the-air (OTA) software updates using Blockchain technology.
- ❑ One of the prevention techniques published as a patent application is the use of honeypots (simulation of vehicle systems in real-time) to protect vehicles from cyberattacks.
- ❑ A recent patent application unveils an AI-based intrusion detection system that analyzes sensor data for anomalies using learned patterns.

# DevSecOps Platform

## **Argus Launches New DevSecOps Platform to Accelerate and Secure Automotive Software Development Cycles**

Argus Cyber Security, a leader in automotive cybersecurity, launched a DevSecOps platform to address the security challenges of developing software-defined vehicles (SDVs). This platform integrates various security technologies throughout the development lifecycle to find and fix vulnerabilities early, reducing costs and speeding up development. The platform offers features like threat analysis, code security management, and automated testing, making it easier for manufacturers to implement security by design and comply with regulations.

Source

[argus-sec.com](https://argus-sec.com)



# Vulnerability Management

## **ESCRYPT CycurRISK meets ONEKEY: A Joint Solution for Effective Vulnerability Management in Software-Defined Vehicles**

A joint solution from ONEKEY and ESCRYPT CycurRISK tackles challenges in managing vulnerabilities for software-defined vehicles mandated by UNR 155 regulations. ONEKEY automates SBOM creation and prioritizes vulnerabilities, while ESCRYPT CycurRISK aids in threat analysis and risk assessment. This collaboration streamlines the process by providing developers with a focused list of critical vulnerabilities to address, improving development efficiency. The future looks to integrate vulnerability feedback into risk assessments and expand the solution with other cybersecurity tools for a more comprehensive approach.

Source

[www.etas.com](http://www.etas.com)



# API Security

## **VicOne Partners With 42Crunch to Deliver Uniquely Comprehensive Security Across SDV and Connected Vehicle Ecosystem**

VicOne partnered with 42Crunch to enhance security for application programming interfaces (APIs) in software-defined vehicles (SDVs) and the broader connected vehicle ecosystem. This collaboration benefits car manufacturers (OEMs) and suppliers by providing them with quicker detection of API security vulnerabilities, identifying potential threats during operation, and improving overall risk assessment. The partnership aims to eliminate security blind spots created by the growing attack surface due to the increased reliance on APIs in SDVs and cloud technologies. This improved security will help OEMs comply with evolving cybersecurity regulations.

Source

[www.vicone.com](http://www.vicone.com)



# EV Cybersecurity

## **Vietnamese company aims to conquer cybersecurity for Chinese e-vehicles**

VinCSS (Vietnam) and GoGoByte (China) joined forces to develop and deploy cutting-edge cybersecurity solutions for EV makers. With the growing complexity of EV software, the need for strong security is rising. Together, they will develop advanced security solutions for Chinese and Vietnamese EVs, potentially expanding to other markets. This will protect connected car systems from cyberattacks and ensure new technologies are developed with security in mind. Their solutions will comply with international regulations, keeping EVs safe and meeting global standards.

Source

[www.gogobyte.com](http://www.gogobyte.com)





# Partnership

## **Ford Trucks, Irdeto announce cybersecurity partnership**

Ford Trucks has partnered with a cybersecurity company called Irdeto to improve the security of their trucks. This will help them meet new regulations and protect their vehicles from cyberattacks. Irdeto will manage the encryption keys and software signing for Ford Trucks, making it easier and more secure. This partnership allows Ford to focus on making great trucks while Irdeto handles the complex security side of things.

Source  
[irdeto.com](https://irdeto.com)





PATENT

The editor's shortlist

# Patents of the month

## Patents of the month

Published in Jun 2024

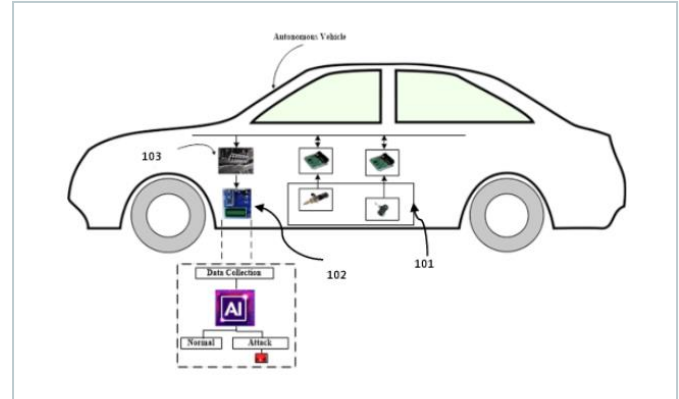


### Shortlisted and summarized by our analyst

- [IN202441033688A](#) - An artificial intelligence-integrated online intrusion detection system in connected and autonomous vehicles  
Assignee: [École Centrale School of Engineering - Mahindra University \(MU\)](#)
- [US11985005B2](#) - Method for detecting CAN bus intrusion of vehicle-mounted network based on GMM-HMM and system  
Assignee: [China Automotive Innovation Co Ltd](#)
- [US11991195B2](#) - Real-time cybersecurity monitoring of inflight entertainment systems  
Assignee: [Thales Avionics Inc](#)
- [US11985150B2](#) - Cybersecurity on a controller area network in a vehicle  
Assignee: [Securethings US Inc](#)
- [US2024152607A1](#) - Detection device, detection method, and detection program  
Assignee: [Sumitomo Group](#)
- [EP4367828A1](#) - A method and system for validating security of a vehicle  
Assignee: [Continental Automotive Technologies](#)
- [EP4109816B1](#) - Context-based response to attacks against autonomous systems  
Assignee: [Intel Corp](#)
- [EP3373553B1](#) - System and method for providing cyber security to an in-vehicle network  
Assignee: [Argus Cyber Security](#)
- [CN117997582A](#) - Attack detection system  
Assignee: [Toyota Motors](#)
- [CN118034736A](#) - Intelligent automobile OTA security upgrading method, system and application based on blockchain technology  
Assignee: [East China Normal University](#)

《 IN202441033688A

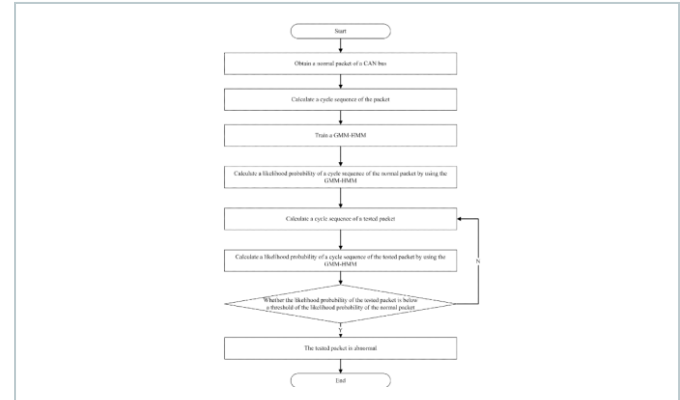
## An artificial intelligence-integrated online intrusion detection system in connected and autonomous vehicles



The patent describes an online intrusion detection system (OIDS) for autonomous vehicles. The OIDS is an external device that monitors sensor data within the vehicle for anomalies. If the OIDS detects an anomaly, it can take actions like alerting the driver or taking control of specific vehicle functions to prevent accidents. The OIDS uses artificial intelligence (AI) to analyze the sensor data. This AI model is trained on normal driving data and data with potential intrusions. The trained model continuously analyzes incoming sensor data and compares it to the learned patterns to detect any anomalies. If an anomaly is detected, the OIDS can take steps to mitigate the threat.

《 US11985005B2

# Method for detecting CAN bus intrusion of vehicle-mounted network based on GMM-HMM and system



This patent proposes a method to detect intrusions on a vehicle's Controller Area Network (CAN) bus. This method relies on a Gaussian Mixture Model-Hidden Markov Model (GMM-HMM) to analyze the timing patterns of messages on the CAN bus and figure out if there are any strange or suspicious activities happening. By analyzing how often certain types of data packets show up and how they relate to each other, this system can catch things like fake messages being sent or repeated attacks on the network. This helps keep vehicles safe from cyber-attacks that could harm drivers or passengers.

Company name China Automotive Innovation Co Ltd

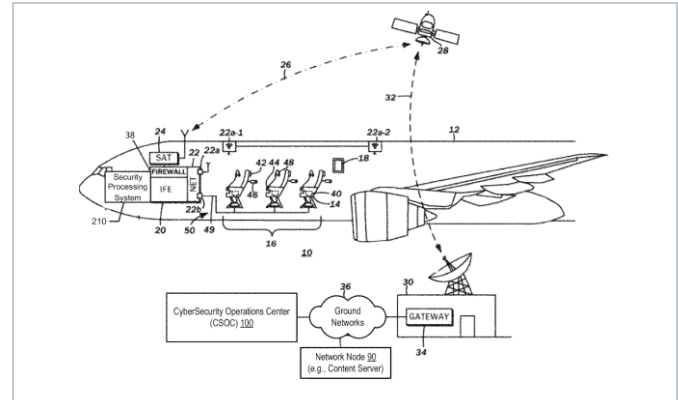
Inventors Hu Heng,  
Hu Hongxing,  
Cheng Wendong,  
Huang Huibin,  
Yu Tao,  
Liu Hong

Priority date 02-Nov-2021

Publication date 14-May-2024

« US11991195B2

# Real-time cybersecurity monitoring of inflight entertainment systems



The patent is about a system that monitors and protects the entertainment systems on airplanes from cyber attacks in real-time. Traditional methods involve collecting large log files during flight and then analyzing them later on the ground. This new system processes the logs (data collected from various components of the entertainment system) on the airplane in real-time, sending only a smaller, summarized version of the data to a ground-based security center. The ground-based center can then detect security issues and send commands back to the airplane system for remedial actions if needed.

Company name Thales Avionics Inc

Inventors Sumien Arnaud

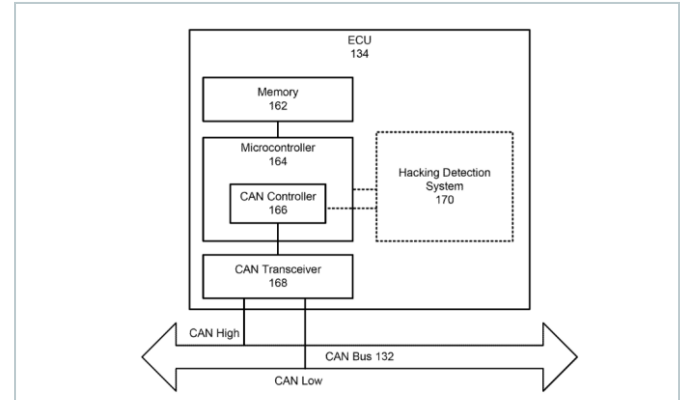
Priority date 08-Sep-2021

Publication date 21-May-2024



《 US11985150B2

# Cybersecurity on a controller area network in a vehicle



This patent describes detecting and mitigating hacking of ECUs within a vehicle. It uses hacking detection software modules on each ECU that communicate with each other. During an initialization stage, the modules identify each other and learn the normal patterns of CAN bus messages. Then, during a detection stage, the modules monitor the CAN bus for signs of malicious activity, such as unexpected messages or changes in message patterns. The system can also respond to detected hacking attempts by taking actions such as preventing an operation, discarding a message, or initiating an alert to the driver.

Company name    Securethings US Inc

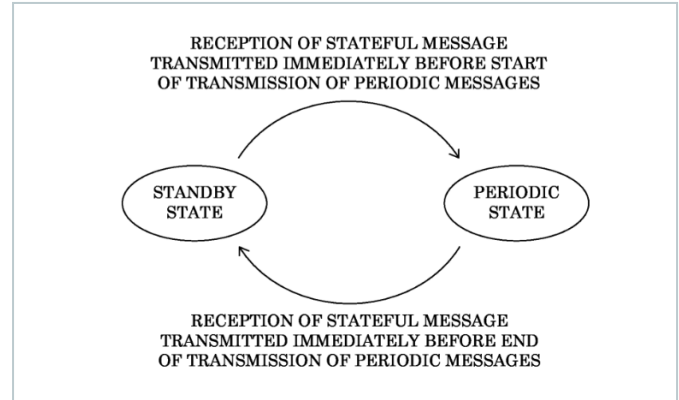
Inventors        Vishal Bajpai

Priority date     25-May-2018

Publication date  14-May-2024

《 US2024152607A1

## Detection device, detection method, and detection program



This invention describes a system for detecting unauthorized messages on a car's internal network. Existing systems rely on comparing message contents to a predetermined list of criteria. The proposed system looks for patterns in the timing of messages. The system has two main parts: one part checks the type of messages being sent to see if they are normal periodic messages, and the other part analyzes how often these periodic messages are received to spot any unusual activity that might indicate an unauthorized message. If it finds something suspicious, like a message with the wrong timing or content, it can alert or even block that message from reaching its destination.

Company name Sumitomo Group

Inventors Yoshida Keigo,  
Tsukamoto Hiroyuki,  
Kamiguchi Shogo,  
Ueda Hiroshi

Priority date 14-Jan-2021

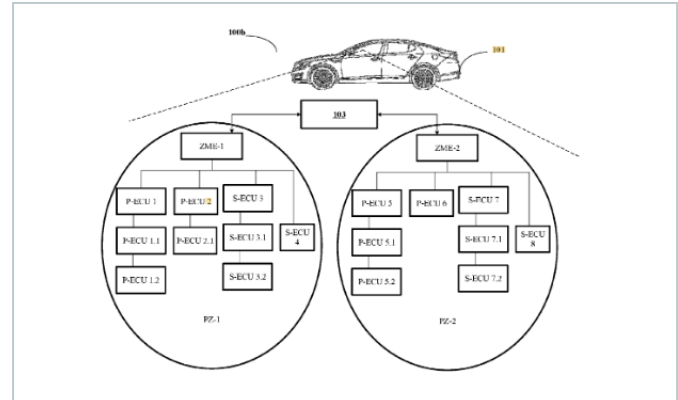
Publication date 09-May-2024





《 EP4367828A1

# A method and system for validating security of a vehicle



The patent describes a method for verifying the authenticity of Electronic Control Units (ECUs) in a car during startup. It divides the car into different zones and uses special codes to check if each part of the car is real and not tampered with. This system works quickly and all at once, instead of checking each part one by one, making sure the critical parts are secure first. By doing this, it helps start the car faster and keeps it safe from any potential threats.

Company name Continental Automotive Technologies

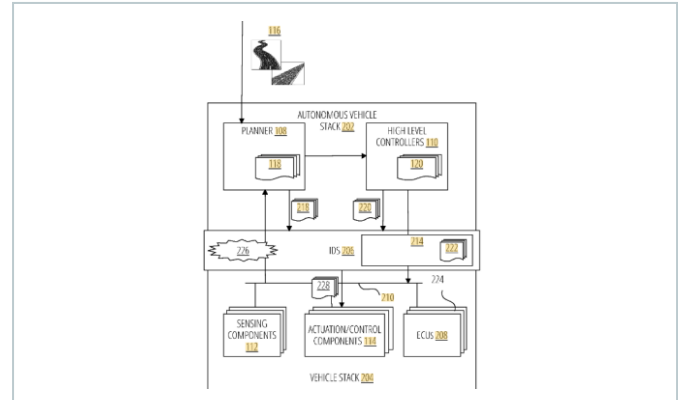
Inventors Wang Yi,  
Suriyakumar Vijayaraj

Priority date 09-Jul-2021

Publication date 15-May-2024

« EP4109816B1

# Context-based response to attacks against autonomous systems



The invention describes a safety system for self-driving cars in case their main control system is compromised. It equips the car with a separate intrusion detection system that monitors the car's behavior and learns its normal operation. This system also stores information about expected actions in different situations. If the main control system gets hacked or malfunctions, the intrusion detection system can recognize this as an attack. Based on the pre-determined contract, it can then decide. This command is then sent to a secondary control system in the car, allowing it to take over and hopefully keep the car safe. In essence, this is a backup plan to ensure the car's safety in case its main computer is hacked.

Company name Intel Corp

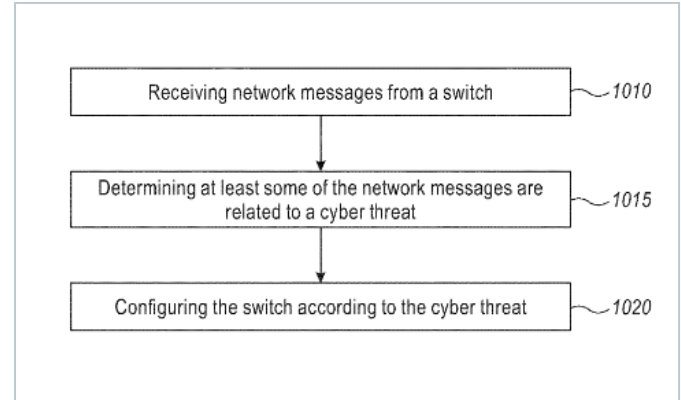
Inventors Juliato Marcio,  
Ahmed Shabbir,  
Gutierrez Christopher,  
Lesi Vuk, Sastry Manoj,  
Wang Qian

Priority date 24-Jun-2021

Publication date 15-May-2024

《 EP3373553B1

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



The patent describes a method for protecting the network inside vehicles from cyber-attacks. The system includes a switch and an intrusion detection and prevention system (IDPS) that work together to detect potential threats in the network messages. The IDPS unit monitors messages traveling on the network and can identify signs of cyber threats and takes action to secure the network accordingly. The IDPS unit is designed to update security rules dynamically, block suspicious packets, and log detected attacks for further analysis. By using advanced filtering mechanisms, it can identify anomalies in network traffic that may indicate a cyber threat.

Company name Argus Cyber security

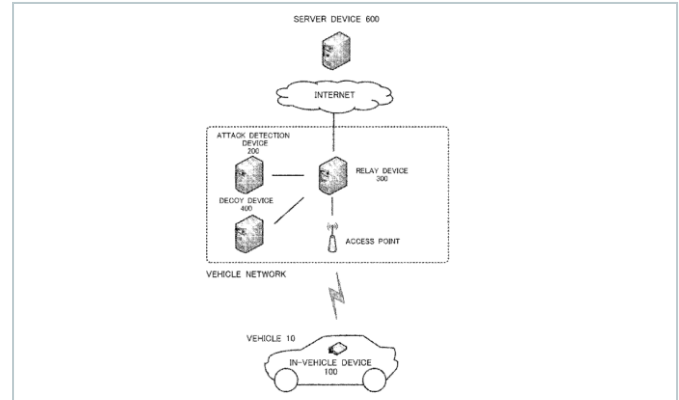
Inventors Matan Atad  
Shiran Ezra  
Gilad Barzilay  
Yaron Galula

Priority date 09-Mar-2017

Publication date 08-May-2024

《 CN117997582A

## Attack detection system

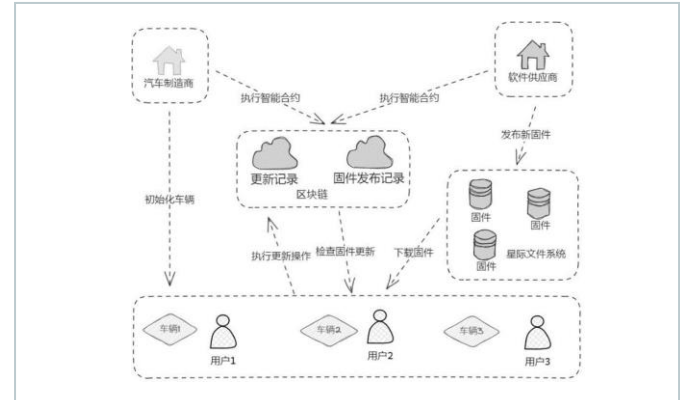


The patent describes a defense system for cars (first vehicles) against cyberattacks. The car continuously monitors its network traffic for signs of attack. If a suspicious device (attack source) is detected, the car takes two steps. First, it instructs a separate device (second device) to activate a honeypot server. This honeypot pretends to be the car's computer system. Second, the car reroutes all communication from the attacker to the second device instead of itself. The second device, equipped with the honeypot server, can then safely process the attacker's messages without putting the car at risk. This approach not only shields the car from the attack but also allows the honeypot to gather information about the attacker's tactics for further investigation.

Company name	Toyota Motor
Inventors	Kazuya Tomita
Priority date	07-Nov-2022
Publication date	07-May-2024

《 CN118034736A

# Intelligent automobile OTA security upgrading method, system and application based on blockchain technology



The patent describes a secure an intelligent automobile OTA (Over-The-Air) security upgrading method based on block chain technology. The system uses tamper-proof blockchain to store information about each car and the software versions it has. When a software update is available, the car can download it and verify its authenticity using blockchain before installing it. This approach ensures that only authorized updates are installed and that the update history cannot be tampered with.

Company name East China Normal University

Inventors Wang Jiangtao,  
Li Zhiyuan,  
Wang Zhenhui,  
Wang Gaoli

Priority date 19-Feb-2024

Publication date 14-May-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](http://www.dennemeyer.com) to find out more about us.

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

 North & East India  
**+91 79831 15166**  
South & West India  
**91 88266 88838**

