

# Cybersecurity in Mobility

## Recent Developments – January 2024

Published by: Denne Meyer India Private Limited  
Contact : Parag Thakre  
pthakre@denne Meyer.com



scan me

# CONTENT

## □ Latest News

- curated and summarized, with reference link to the external source

## □ Latest Patents published in December 2023

- relevant patents shortlisted and summarized, in simple language



# LATEST NEWS

(Curated and summarized by analyst)



## ThunderSoft selects C2A Security along with 18 other companies to create new vehicle OS

The vehicle operating system DISHUI OS, will be powered by C2A Security, a cybersecurity company that focuses on risk management. Designed for central computing, the DISHUI OS incorporates several technologies, such as multi-domain convergence, container virtualization, large language models, cybersecurity, and SDV middleware. Further, it integrates with the automotive industry ecosystem so as to provide users with a more effective, and safe travel experience.

Source: [c2a-sec.com](https://c2a-sec.com)

## LG and Cybellum to introduce cybersecurity management system cockpit

In 2021, [LG acquired Cybellum](https://www.lg.com). They are collaborating on developing the CSMS Cockpit platform, which identifies security vulnerabilities and takes preventative measures to mitigate threats as soon as possible. Automakers can identify and address hardware security threats rapidly using the CSMS Cockpit, an integrated control center for product security monitoring and management.

Source: <https://www.lg.com>



## Cybersecurity robustness solution developed VERZEUSE™ for runtime integrity checker strengthen in-vehicle cybersecurity measures

Panasonic Automotive Systems Co., Ltd. has developed VERZEUSE for Runtime Integrity Checker to ensure the safety and reliability of automated driving functions and network services.

Source: [news.panasonic.com](https://news.panasonic.com)



## ProvenRun participates to secure on-board communications on Ampere's future SDV platforms

ProvenRun's cybersecurity IP, co-developed with Ampere software & systems teams, protects onboard communication on future Software Defined Vehicle (SDV) Platforms. ProvenRun emphasizes the use of top-tier security tools like Rust programming language and ProvenCore operating system to bolster SDV security.

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

## Argus Cyber Security unveils groundbreaking aftermarket product to prevent cyber vehicle theft

Argus Cyber Security developed a product [vDome](#), an anti-theft solution focused on protecting vehicles from CAN injection attacks. It is a patented AI-powered solution that proactively detects and neutralizes malicious devices in under 200 microseconds.

Source: [www.prnewswire.com](https://www.prnewswire.com)



## AUTOCRYPT releases polarion-based cybersecurity TARA template for the automotive industry

[AUTOCRYPT](#) released "TARA Template for Automotive," a project management tool for conducting Threat Analysis and Risk Assessment (TARA), a process crucial to the development and maintenance of automotive software. It greatly reduces the complexity and increases the accuracy of TARA activities.

Source: [www.prnewswire.co.uk](https://www.prnewswire.co.uk)

# INTELLECTUAL PROPERTY

## LATEST PATENTS

(Shortlisted and summarized by analyst)



Patent

- ❑ [WO2023220615A3](#) - Systems, methods, and apparatus for cyberattack mitigation and protection for extreme fast charging infrastructure
- ❑ [US20230401317A1](#) - Security method and security device
- ❑ [CN117152708A](#) - Spoofing attack detection method, device, equipment and storage medium
- ❑ [CN114844721B](#) - Attack detection method and system, vehicle and computer readable storage medium
- ❑ [WO2023241954A1](#) - Method for indicating an attack
- ❑ [CN117319069A](#) - Intrusion detection method, intrusion detection device, computer equipment and storage medium
- ❑ [CN117201101A](#) - Unmanned aerial vehicle CAN bus intrusion detection method based on enhanced GAN model

# WO2023220615A3 - Systems, methods, and apparatus for cyberattack mitigation and protection for extreme fast charging infrastructure

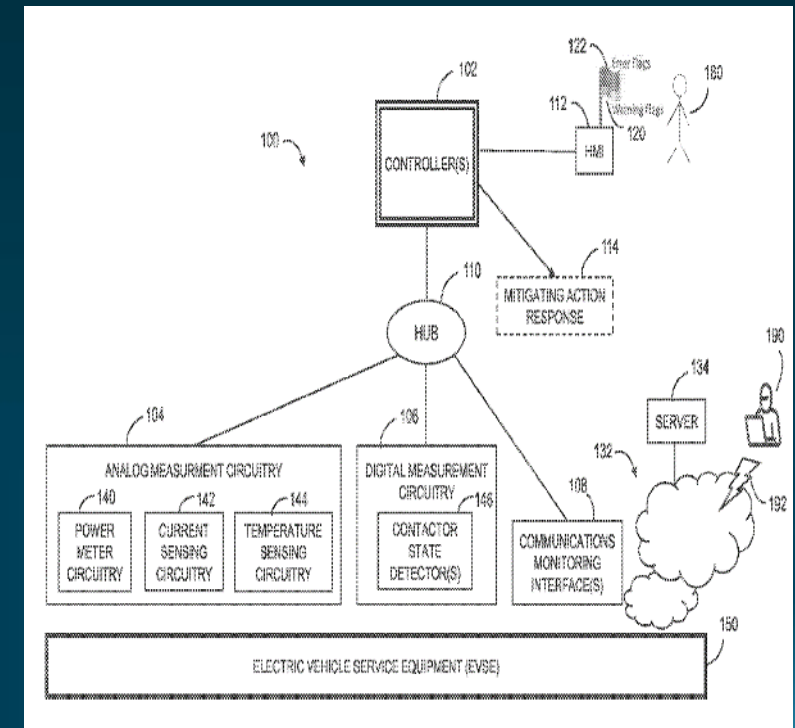
🏠 **Assignee** Battelle energy alliance LLC

👤 **Inventors** Rohde Kenneth; CARLSON Richard;  
Salinas Sean; Crepeau Matthew

📅 **Dates** Priority date: 10-May-2022  
Publication date: 16-Nov-2023


## 🗨️ Summary

The invention relates to a system for cyberattack mitigation and protection for electric vehicle supply equipment (EVSE) i.e., an EV charger. The system has controllers that determine the anomaly condition (indicative of a cyberattack, cyber manipulation, cyber tampering, and so on) based on the analog signal associated with the charger and communication signals associated with the operations of the charger. Once the anomaly is determined, the controller takes the mitigation action.






# US20230401317A1 - Security method and security device

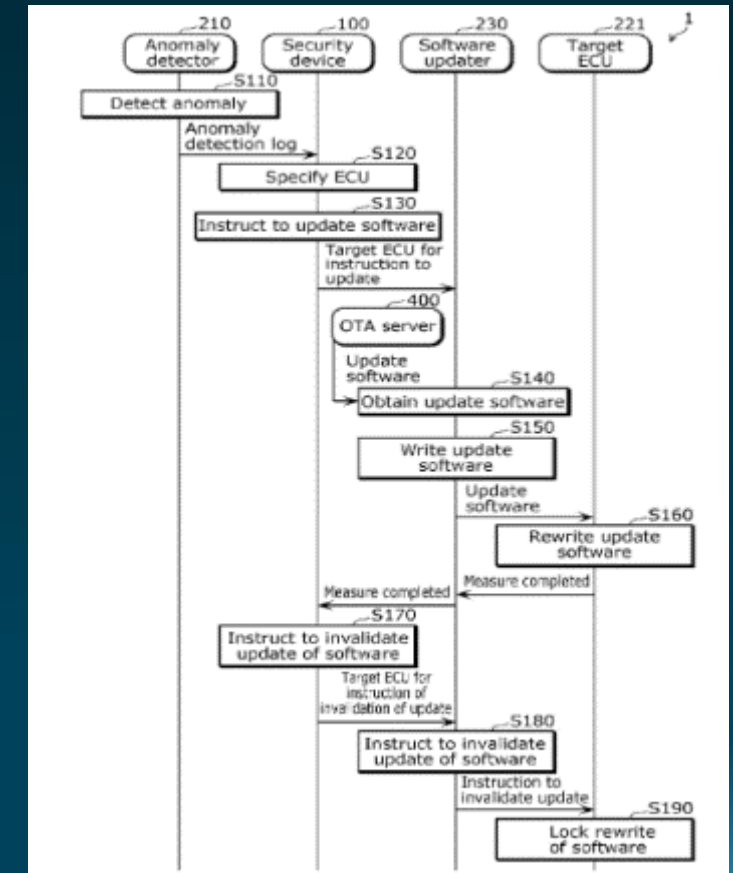
 **Assignee** Panasonic Intellectual Property Management Co Ltd

 **Inventors** Kaoru Yokota

 **Dates** Priority date: 04-May-2023  
Publication date: 14-Dec-2023


## Summary


The invention discloses a device to restrain controls of a vehicle when an attack against the vehicle is detected. When an anomaly is detected in the in-vehicle communication network or the CAN bus, the device determines which ECU (Electronic component unit) is compromised. The device then responds instantly by updating the software security patch for that ECU, without restraining the driving functions. For this reason, even when a vehicle is attacked, a measure can be taken against the attack without restraining the driving functions of the vehicle. Thereby, for example, the driver can drive the attacked vehicle to evacuate to home or can drive the vehicle to a service center for recovery from troubles.



# CN117152708A - Spoofing attack detection method, device, equipment and storage medium

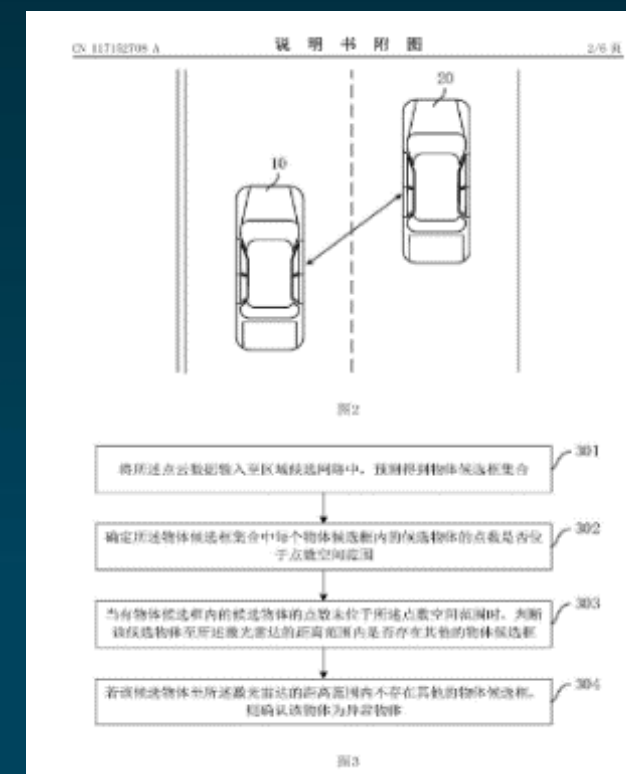
 **Assignee** City University of Hong Kong City

 **Inventors** Fu Weiwei; Zhang Jindi; Zhang Yifan; Wang Jianping

 **Dates** Priority date: 24-May-2022  
Publication date: 01-Dec-2023

## Summary


The invention relates to detecting a spoofing attack against a LiDAR in autonomous driving vehicles, specifically in multi-vehicle scenarios. When multiple autonomous vehicles are close to each other, the corresponding multiple LiDAR can collect partially overlapping driving environment data, and then collaboratively identify whether the LiDAR is subject to spoofing attacks. For example, when any autonomous vehicle identifies an abnormal object in the point cloud data collected by its own LiDAR, it can broadcast that data and its position to the surrounding vehicles. Further, based on the response from the surrounding vehicles, the spoofing attack is determined.



# CN114844721B - Attack detection method and system, vehicle and computer readable storage medium

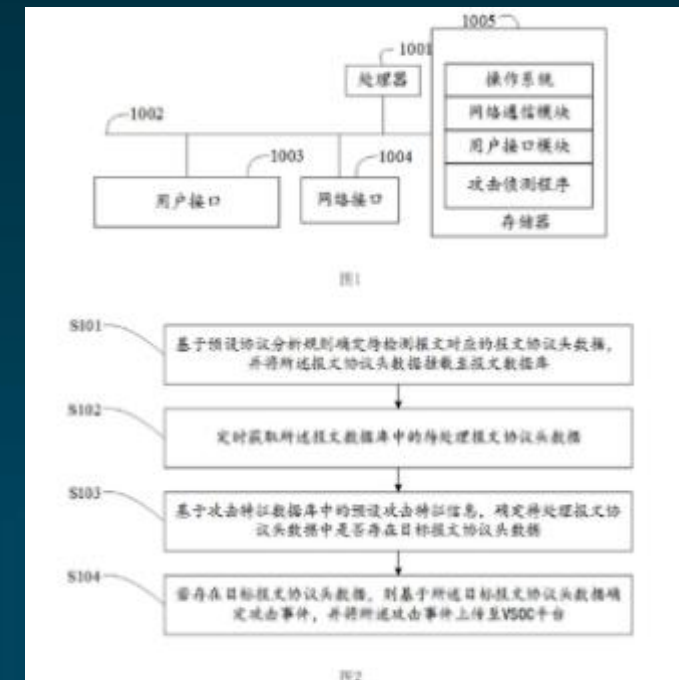
 **Assignee** Zhaoqing Xiaopeng New Energy Investment Co Ltd Guangzhou Branch

 **Inventors** LI Xuefei; Yi Shengbi; Bell Stone

 **Dates** Priority date: 06-Jun-2022  
Publication date: 29-Dec-2023


## Summary


The invention relates to the field of vehicle information security. The vehicle has an attack detection device that regularly performs the attack detection on the protocol header data of the message received from the cloud (or outside world). The device uses preset attack characteristic information of each attack type, to determine whether the protocol header data satisfies the attack characteristic information. If an attack event is determined; it is uploaded to the VSOC (Vehicle Security Operation Center) platform for further analysis.



# WO2023241954A1 - Method for indicating an attack

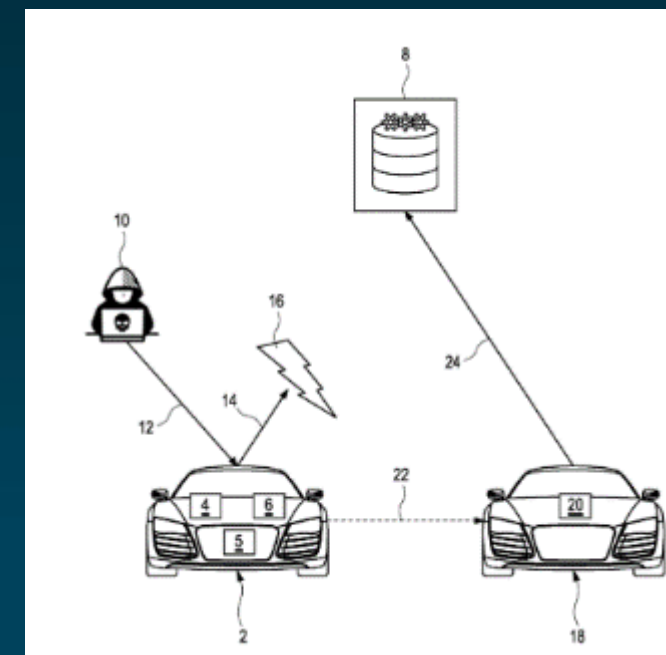
 **Assignee** Audi Ag

 **Inventors** Christopher Corbett, Schmidt Karsten


 **Dates** Priority date: 13-Jun-2022  
Publication date: 21-Dec-2023

## Summary


The invention determines a cyber attack on the hardware/software of a vehicle computing unit. The vehicle has an anomaly detection sensor to detect the attack, it also has an encryption unit that encrypts a main message with the attack information. The encrypted main message is then sent to a third-party vehicle via electromagnetic waves to further decrypt the message and report an attack.



# CN117319069A - Intrusion detection method, intrusion detection device, computer equipment and storage medium

 **Assignee** China Automotive Innovation Co Ltd

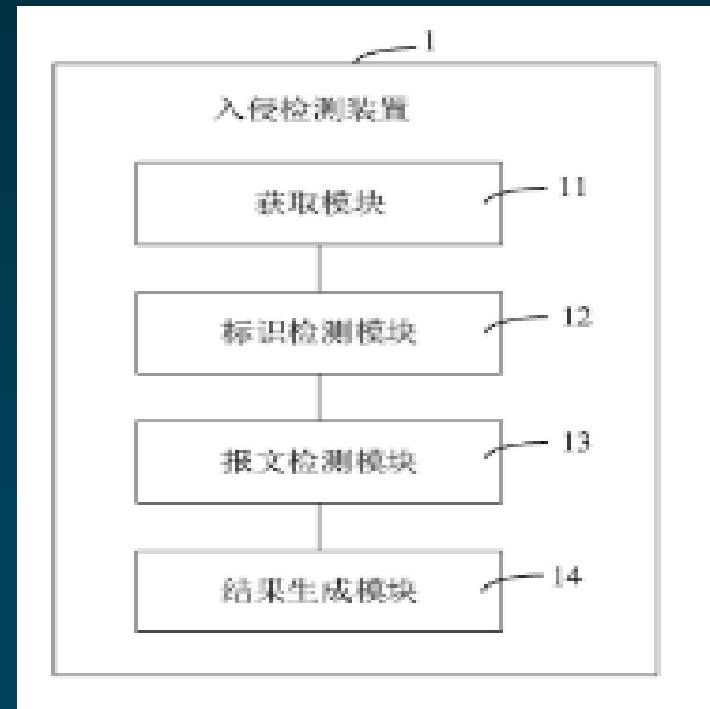
 **Inventors** Zhang Qiangqiang, Ju Shichao, Wang Wenxuan, Qu Hongda, Yan Kuangcheng, Ling Jinwen

 **Dates** Priority date: 25-Oct-2023


Publication date: 29-Dec-2023

## Summary


The invention relates to an intrusion detection system (IDS) for vehicle-mounted communications technologies. An IDS monitors network transmissions in real time such as monitoring the received messages based on the message identifier and content identifier rule. Whenever a suspicious transmission is detected, the IDS alerts or takes proactive action to ensure the safety.



# CN117201101A - Unmanned aerial vehicle CAN bus intrusion detection method based on enhanced GAN model

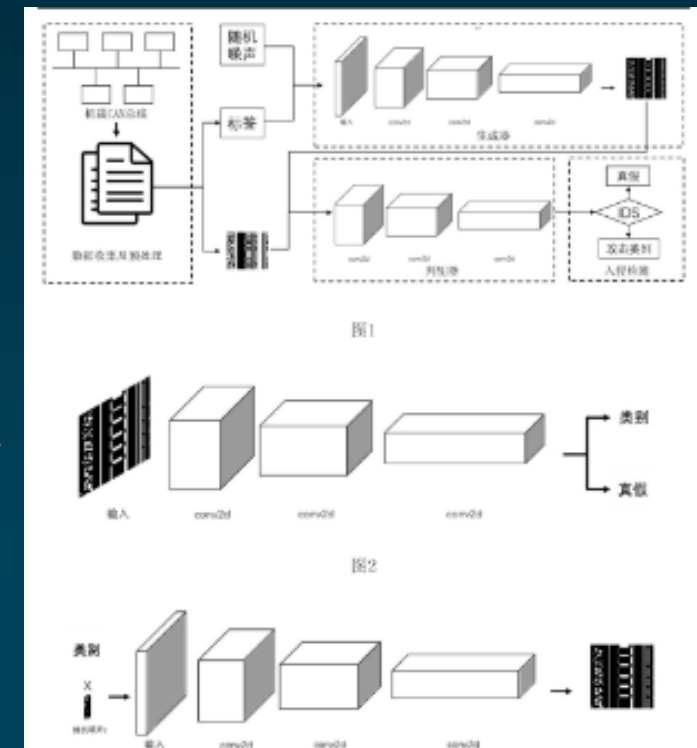
 **Assignee** Xi'an Lianfei Intelligent Equipment Research Institute Co Ltd, Xidian University

 **Inventors** LI Teng; ZHAO Chengnan

 **Dates** Priority date: 25-Oct-2023  
Publication date: 29-Dec-2023

## Summary

The invention relates to CAN bus intrusion detection in an unmanned aerial vehicle by using an enhanced Generative Adversarial Networks (GAN) model. The GAN model solves the problem of difficult deployment, insufficient training data, and poor detection accuracy of existing models. From the available attacked and unaddressed data a training set and testing set is created. Then constructing an enhanced GAN model which has a generator and a discriminator. Generators are used to generate images similar to real samples, while discriminators judge whether the generated images are true or false. Further, training the GAN model and deploying the discriminator of the GAN model to identify the intrusion.



# Thank You

To know more about us please visit

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

Contact us at

**Dennemeyer India Private Limited**

North & East India: +91 79831 15166

South & West India: +91 88266 88838

DISCLAIMER: This report, including external links, is generated using databases and information sources believed to be reliable. While effort has been made to employ optimal resources for research and analysis, Dennemeyer expressly disclaims all warranties regarding the accuracy, completeness, or adequacy of the information provided. We do not control or endorse the content of external sites and are not responsible for their accuracy or legality. The information provided in this report should not be construed as legal advice, and users are strongly advised to consult with qualified legal professionals for specific legal guidance.