

Special Edition – October 2024

# 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) )

# Subscribe now



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

# Special Edition

In this special edition of our monthly report, we are exploring the multifaceted landscape of cybersecurity. October is the Cybersecurity Awareness month, which provides an excellent opportunity to highlight the importance of promoting cybersecurity best practices within the community. Taking the recent incident in Lebanon as an example, it emphasizes the devastating impact that cyber threats can have on cyber physical assets, demonstrating the need to prioritize cybersecurity. The severity of this attack serves as a warning that even tangible infrastructure, such as vehicles, is vulnerable to cyber manipulation.

This month's report include the following content:

- [Cybersecurity awareness month](#)
- [Lebanon pager attack – special coverage](#)
- [Industry news](#)
- [Patents of the month](#)

# 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 this month

- ❑ The recent pager attack in Lebanon demonstrate the devastating impact that cyber threats can have. It is a reminder that even tangible assets, like vehicles (which are equipped with a larger battery), can be compromised through cyber manipulation. If such vehicles are attacked, the impact could be even more severe.
- ❑ The integrity of ECU firmware is crucial, as it is updated over-the-air (OTA). And, to protect the firmware boot process, Karamba Security has introduced a secure boot solution for container images during runtime. Containers are packages of software that contain all the necessary elements to run in any environment.
- ❑ Many companies are coming forward with the products/solutions which are complying with the UN Regulations 155 and 156, to enhance the vehicle security. For example, LG is providing compliant V2X solutions to Volkswagen. Similarly, UD Trucks partnered with VicOne to comply with the regulations, also to identify and address potential threats.
- ❑ Several inventions are patented last month to secure in-vehicle network such as adding the functionality of creating secure tunneling frame to network controller, prioritizing the severity of the attack on the network and generating mitigation action based on the severity.
- ❑ Many inventions have been patented recently to secure the electronic control unit (ECU). For example, the ECU is monitoring parameters like power supply current, communication response time, and MAC address integrity of the communicating ECU, adding strong encryption technique to ensure secure communication between the two ECU.



Cybersecurity awareness month

# Cybersecurity awareness month



October marks cybersecurity awareness month with the theme "Secure Our World", a global initiative aimed at fostering a culture of online safety. Launched in 2004, this annual event encourages individuals, businesses, and organizations to take proactive measures to protect themselves from cyber threats. The U.S. Department of Homeland Security and the National Cyber Security Alliance originally spearheaded this initiative, which has since expanded into a worldwide movement. October 2024 marks the 21st anniversary of Cybersecurity Awareness Month.

## Why is it celebrated?

**Raise awareness:** Educate individuals and organizations about the importance of cybersecurity and the risks associated with online activities.

**Promote best practices:** Encourage people to adopt safe online habits and use strong security measures to protect their personal and sensitive information.

**Foster collaboration:** Encourage collaboration between individuals, businesses, and governments to address cybersecurity challenges collectively.

**Highlight the need for ongoing vigilance:** Remind people that cybersecurity is an ongoing concern that requires constant attention and adaptation to evolving threats.



# Recommended actions for cybersecurity awareness month

- ❑ **Educate Yourself and Others:** Enhance your cybersecurity knowledge by attending webinars or online training sessions and following reputable cybersecurity sources like newsletters and reports. Use social media, public service announcements, and community events to raise awareness about common cyber threats and prevention tips. Sharing real-world examples of cyberattacks can also illustrate the importance of security and motivate others to act.
- ❑ **Encourage a Culture of Security:** Leverage this month as an opportunity to evaluate your current cybersecurity practices and take corrective actions. Create a workplace culture that empowers employees to report suspicious activities and emphasizes the importance of cybersecurity.
- ❑ **Conduct Regular Security Assessments:** Perform vulnerability scans, penetration testing, and risk assessments to identify and address potential weaknesses.





# Lebanon pager attack – special coverage

# Lebanon pager attack

The pager explosions in Lebanon were a series of coordinated attacks that occurred in September 2024. The exact mechanism of the explosions remains under investigation, but several theories have been put forward:

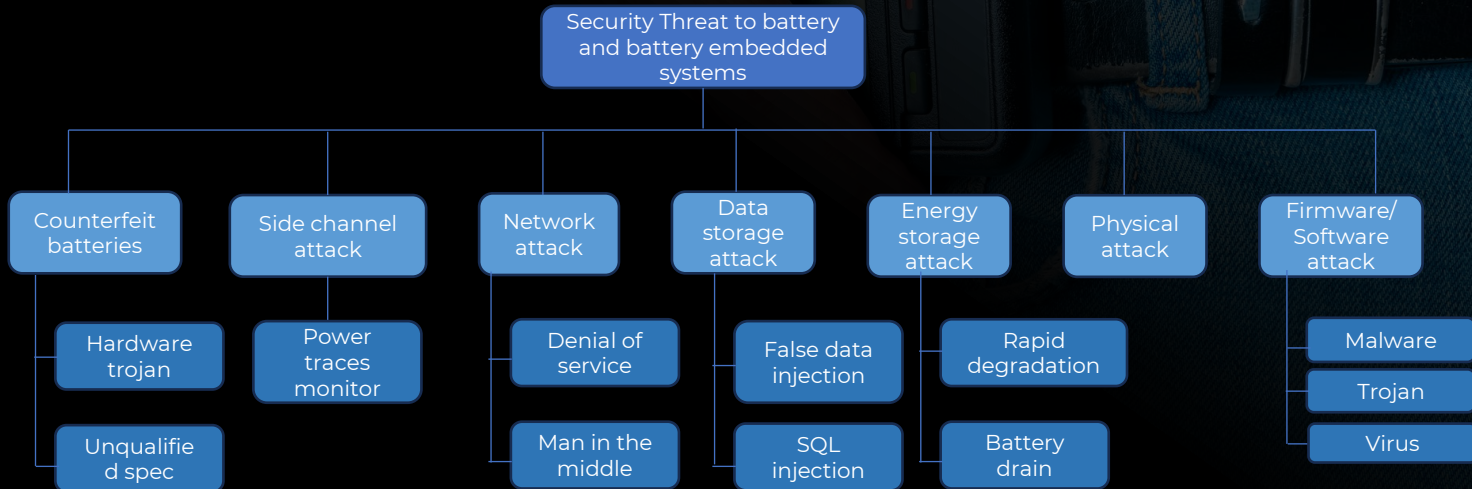
- ❑ **Remote Activation:** It's believed that small amounts of explosives were concealed within the pagers themselves. These explosives could have been triggered remotely, possibly using radio signals or cell phone networks.
- ❑ **Tampered Batteries:** Some experts speculate that the radio system that the pagers rely on was hacked, possibly through a doctored code. The batteries of the pagers could have been triggered to overheat, leading to a process called thermal runaway, which in turn caused the pager batteries to explode.
- ❑ **Software Vulnerabilities:** The pagers' software might have contained vulnerabilities that could be exploited by hackers to remotely control or trigger devices.
- ❑ **Malicious Code:** Hackers could have introduced malicious code into the pagers, either through updates or by compromising the supply chain, which could have been used to activate the explosives.

Here are the curated links to know more about the recent pager attack

[Source 1](#), [Source 2](#), [Source 3](#), [Source 4](#), [Source 5](#), [Source 6](#)

# Interesting literature on battery tampering

Batteries have become an integral part of various applications, from small embedded devices like pagers, walkie-talkie to electric vehicles. However, concerns have arisen regarding battery safety due to incidents like swelling, fire, and explosion, resulting in significant financial losses and tragic consequences. Several research papers published on the cyber threats of the batteries. The below taxonomy highlights the major attack vectors that would affect battery security.





# Interesting literature on hacking of closed network devices

- ❑ **Pager Bomb:** A pager-bomb is a type of improvised explosive device (IED) that is triggered by a pager signal. These devices have become less common with the rise of smart phones but were once widely used. The Red Scorpio system, originally designed as a car alarm pager, was often repurposed for use in pager-bombs. The transmitter in the car alarm would send a signal to the pager, which would then activate the explosive device. This highlights the potential dangers of repurposing commercial devices for malicious purposes.
- ❑ **A Real-time Inversion Attack on the GMR-2 Cipher Used in the Satellite Phones:** The GMR-2 cipher, used in Inmarsat satellite phones, has been found to be vulnerable to a new attack that can efficiently recover the encryption key using only a single-frame of known keystream. This attack exploits the cipher's weaknesses in its components and key schedule. By introducing the concept of a "valid key chain," the researchers were able to develop a real-time inversion attack that significantly reduces the search space for the encryption key.
- ❑ **Pagers can be hacked:** Hackers can easily intercept and decode data transmitted via pagers, exploiting the inherent lack of security in traditional pager systems. One of the primary tools used for this purpose is the Software Defined Radio (SDR), which can receive and decode various radio frequencies, including those used by pagers. The vulnerability lies in the fact that pager communications are typically not secured with encryption. This lack of encryption allows anyone with the right equipment and technical knowledge to intercept and decipher messages.





# Industry news

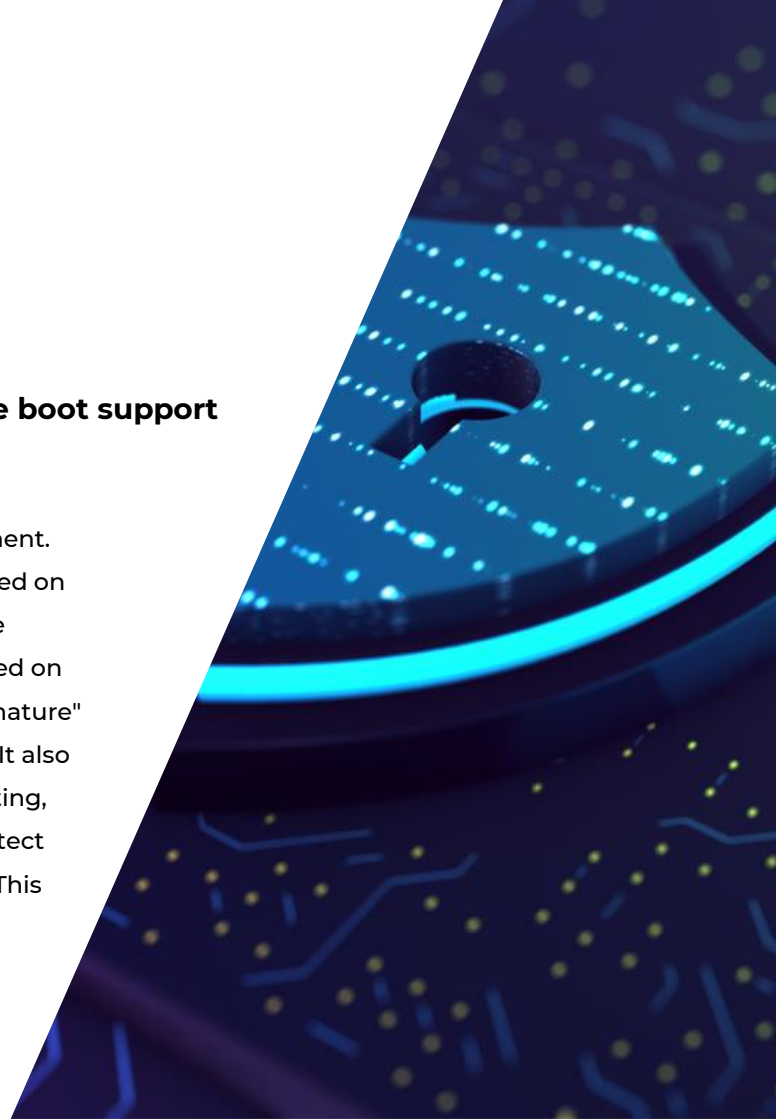
# Secure boot

## **Karamba security announces world-first secure boot support for containers**

Karamba Security's XGuard now supports Secure Boot for Containers, protecting them from tampering and replacement. This solution ensures the integrity of container images stored on IoT devices and ECU firmware. Traditional solutions validate cloud-based container images but don't protect those stored on devices. XGuard calculates the container's image hash "signature" and creates a policy to enforce allowed images at runtime. It also provides runtime security features like application whitelisting, file protection, and associated execution monitoring to protect running containers, without modifying the underlying OS. This security solution protects both the creation and running of containerized applications, making them more resistant to attacks.

Source

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



# Cybersecurity

## **UD Trucks selects uniquely flexible vicone solution to take advantage of contextualized security risk insights**

VicOne's xNexus platform is helping UD Trucks enhance its vehicle cybersecurity. The platform provides contextualized security risk insights, enabling UD Trucks to identify and address potential threats earlier. This is particularly important as the company focuses on developing electric and autonomous trucks. By leveraging VicOne's AI-powered solution, UD Trucks can improve its product security, meet regulatory requirements like UN R155, and maintain a competitive edge in the evolving automotive landscape.

Source

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



# Remote attack

## Millions of Kia vehicles were vulnerable to remote attacks with just a license plate number

Security researchers recently discovered vulnerabilities in the Kia dealer portal that allowed them to remotely take over any Kia vehicle built after 2013 using only a license plate number. Security researchers exploited a vulnerability in the Kia dealer website to gain unauthorized access to customer data and vehicle information. Using a third-party API, they converted license plate numbers to VIN (Vehicle Identification Number), allowing them to remotely control vehicles. This issue potentially affected millions of Kia vehicles worldwide. The researchers responsibly reported the vulnerabilities to Kia, who has since addressed them. Kia has confirmed that there is no evidence of malicious exploitation.

Source

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





# Investment

## **BMW i ventures announces investment in Runsafe security to bolster cybersecurity for critical infrastructure.**

BMW i Ventures has invested \$12 million in RunSafe Security, a cybersecurity firm specializing in software immunization. BMW i Ventures believes RunSafe's technology can protect embedded systems within connected devices from memory attacks. RunSafe's patented process protects software from cyberattacks without disrupting developer operations. With the expansion of its platform, RunSafe offers automated solutions for SBOM generation, vulnerability identification, and exploit prevention and remediation for embedded software deployed throughout critical infrastructure. RunSafe's solutions have been adopted by industry leaders in aerospace, defense, and energy.

Source

<https://www.press.bmwgroup.com/>



# V2X solution

## **LG first in world to receive new 'common criteria certification' in V2X device category**

LG Electronics' V2X solution for Volkswagen has received the first Common Criteria (CC) certification for security in the V2X device category. This highlights LG's advanced vehicle cybersecurity capabilities. The VW Transceiver Module designed for Volkswagen's MQB platform, successfully passed rigorous security evaluations and earned an EAL 2+ rating Spain's National Cryptologic Centre. LG is proactive in addressing V2X security threats and ensuring compliance with Europe's strict regulations UN 155 & 156. LG plans to achieve similar certification for its V2X solution for Volkswagen's MEB electric vehicle platform, reinforcing its commitment to vehicle security and its position in the global automotive market.

Source

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





PATENT

The editor's shortlist

# Patents of the month

## Patents of the month

Published in September 2024



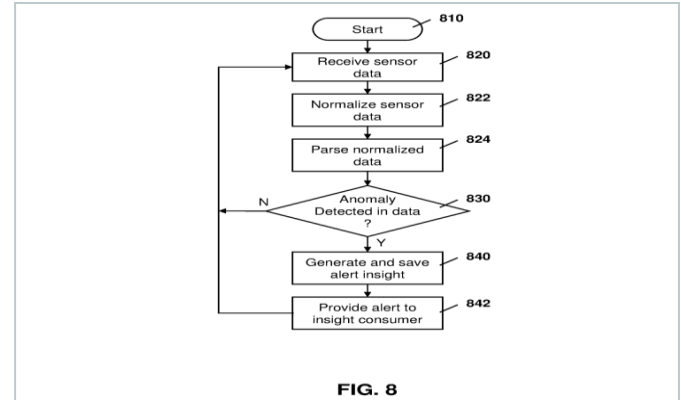
### Shortlisted and summarized by our analyst

- [US2024303324A1](#) - Method and system for intrusion detection for an in-vehicle infotainment system  
Assignee: BlackBerry Ltd
- [US12092733B2](#) - Radar anti-spoofing system for identifying ghost objects created by reciprocity-based sensor spoofing  
Assignee: GM Global Technology Operations LLC
- [US12095805B2](#) - Autonomous vehicle security measures in response to an attack on an in-vehicle communication network  
Assignee: Waymo LLC
- [US12089048B2](#) - In-vehicle system including abnormality detection unit configured to recognize lower lever control unit as unauthorized by monitoring plurality of elements of lower-level control unit  
Assignee: Yazaki Corp
- [US2024314139A1](#) - Secure vehicle communication networks and dynamic intervehicle compliance  
Assignee: International Business Machines Corp
- [EP4425827A1](#) - Secure tunnelling of a frame in an in-vehicle communication network  
Assignee: Infineon Technologies AG
- [EP4004782B1](#) - Intrusion anomaly monitoring in a vehicle environment  
Assignee: C2a Sec Ltd
- [IN549893A1](#) - Method and system for performing key encryption and cyber security in vehicles using SSM  
Assignee: Minda Corp
- [CN118677698A](#) - Analysis method for identifying network security risk and countermeasure of automobile ECU  
Assignee: Shanghai Yiyan Electronic Technology Co Ltd
- [CN118467008B](#) - Security management method, system, medium and electronic equipment for OTA upgrade  
Assignee: Chengdu Seres Technology Co Ltd



《 US2024303324A1

# Method and system for intrusion detection for an in-vehicle infotainment system



The patent deals with the risk of cyber attacks on modern vehicles, especially targeting in-vehicle infotainment (IVI) systems. As vehicles become more computerized and interconnected, they offer more opportunities for potential intrusions. The solution is a method for detecting these intrusions using a computing device within the IVI system. It involves collecting and normalizing security sensor data to spot anomalies and generate alerts when irregularities are found. Detection can be done through rules-based services or machine learning models. The system also includes synthetic sensors that provide real-time insights and communicate with security operations centers, helping to reduce cyber threats and maintain the vehicle's operational integrity.

Company name BlackBerry Ltd

Inventors Melgarejo Lermas Irene,  
Bells Matthew,  
Henkel Steven John,  
Shi Xiaobing,  
Sic Petar

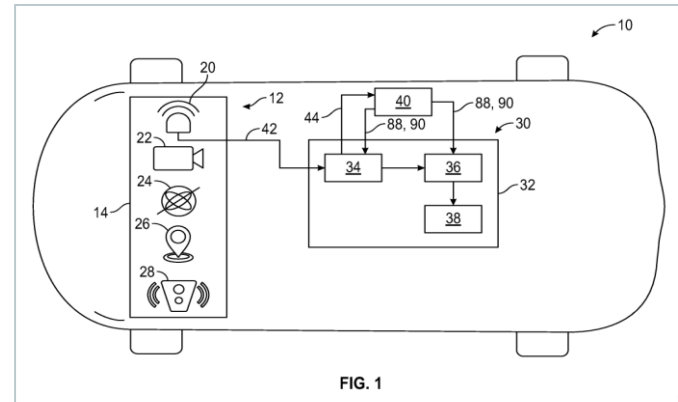
Priority date 10-Mar-2023

Publication date 12-Sep-2024



《 US12092733B2

# Radar anti-spoofing system for identifying ghost objects created by reciprocity-based sensor spoofing



The patent tackles the problem of identifying fake (ghost) objects in radar systems for self-driving cars caused by sensor spoofing in radar systems for autonomous vehicles. This spoofing happens when radar signals from real objects are mistaken for false ones due to timing errors such as mismatched time delays, which can be dangerous. The solution is a radar anti-spoofing system that uses multiple radar sensors and a controller to analyze these signals. The controller uses algorithms to cluster detected objects, calculate adjusted signal-to-noise ratio (SNR) and velocity-ratio measures, and determines if objects are real or fake based on set thresholds. This system enhances vehicle safety in areas prone to electronic interference.

Company name GM Global Technology Operations LLC

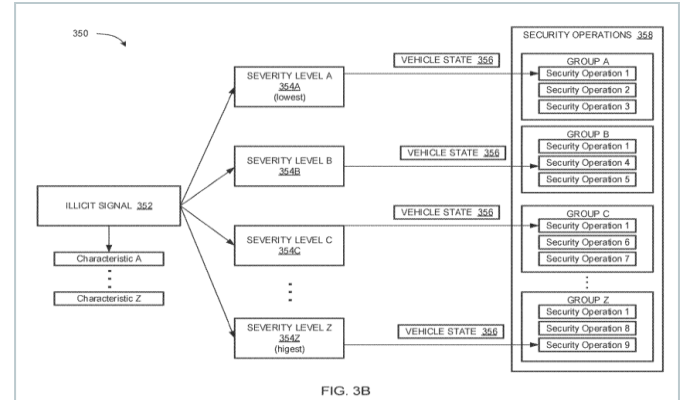
Inventors Yuri Owechko,  
Qin Jiang

Priority date 15-Dec-2021

Publication date 17-Sep-2024

《 US12095805B2

# Autonomous vehicle security measures in response to an attack on an in-vehicle communication network



The patent addresses the vulnerability of autonomous vehicles to attacks on their in-vehicle communication networks, which can lead to dangerous consequences such as compromised safety systems. Illicit signals (unauthorized or malicious signals) may be injected into these networks to manipulate critical vehicle functions, posing risks to passengers and property. The solution involves detecting these illicit signals, identifying their severity, selecting and performing appropriate security operations based on the severity and vehicle state to mitigate safety impacts., thereby enhancing overall vehicular safety while maintaining operational efficiency.

Company name Waymo LLC

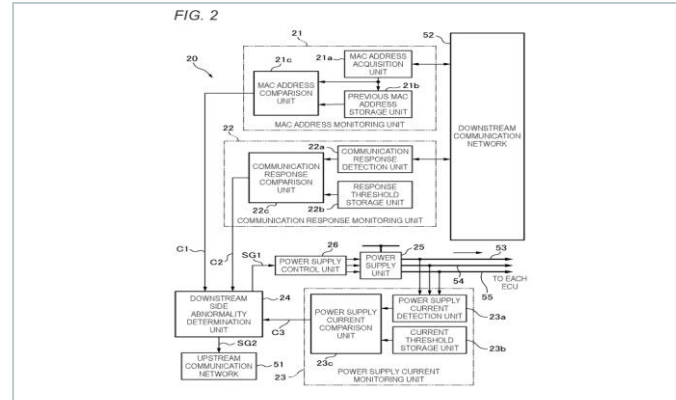
Inventors Tseng Chan Stephan Huang,  
Stacy Janes,  
Joshua Foust

Priority date 15-Jul-2021

Publication date 17-Sep-2024

《 US12089048B2

In-vehicle system including abnormality detection unit configured to recognize lower level control unit as unauthorized by monitoring plurality of elements of lower-level control unit



The patent addresses the risk of attacks on in-vehicle communication networks by unauthorized devices, which can compromise vehicle safety. Unauthorized devices may replace or connect to electronic control units (ECUs) within the vehicle, leading to potential attacks. The solution is an in-vehicle system with a central ECU that manages security, multiple zone control units, and lower-level ECUs. Zone control units monitor parameters like power supply current, communication response time, and MAC address integrity in the lower-level ECUs. If abnormalities are detected across two or more monitored elements in any lower-level ECU, it is flagged as unauthorized, leading to power cutoff and notification to the central ECU.

Company name Yazaki Corp

Inventors Jun Goto

Priority date 7-Apr-2021

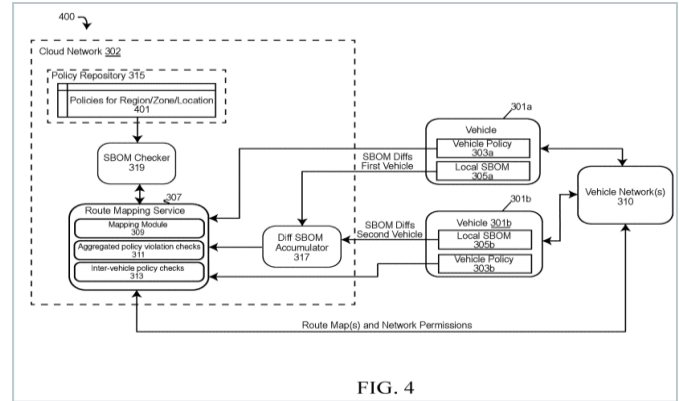
Publication date 10-Sep-2024





《 US2024314139A1

# Secure vehicle communication networks and dynamic intervehicle compliance



The patent focuses on the need for secure vehicle communication networks that follow different security policies as vehicles move through various locations. As vehicles rely more on software systems, there's a risk that if one vehicle's system doesn't meet standards, it could compromise the entire network. The solution uses computer-based methods and systems with Software Bills of Materials (SBOMs) to document and verify software components against location-specific policies set by governments or other institutions while the vehicle is on the move. Non-compliant vehicles can be muted from the network or rerouted entirely, thereby reducing the risks associated with software vulnerabilities in connected vehicles.

Company name International Business Machines Corp

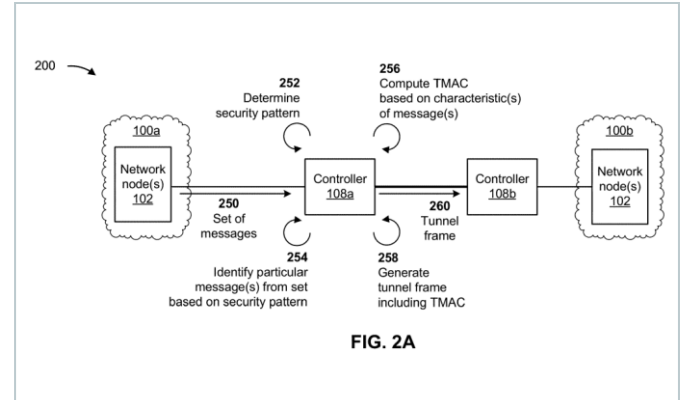
Inventors Sudheesh S. Kairali,  
Sarbjit K. Rakshit,  
Manish Anand Bhide,  
Murali Vasudev

Priority date 14-Mar-2023

Publication date 19-Sep-2024

《 EP4425827A1

# Secure tunnelling of a frame in an in-vehicle communication network



The patent focuses on making communication within vehicle networks secure to prevent unauthorized access and ensure messages authenticity. As vehicles become more interconnected, the risk of harmful commands increases. The solution is a network controller inside the vehicle that receives messages from different parts and creates a secure frame for them. It uses a security pattern to pick out important messages, calculates a code (TMAC) to verify these messages, and includes both the code and the messages in the secure frame (tunnel frame). It also checks how recent each message is to boost security. This method improves data security by identifying key message features, preventing old messages from being reused in attacks, and encrypting message headers to keep data safe.

Company name Infineon Technologies AG

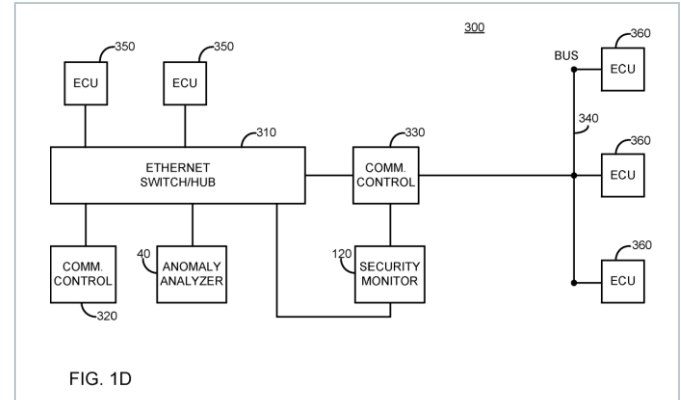
Inventors Anjana Ramamoorthy,  
Alexander Zeh

Priority date 13-Dec-2022

Publication date 4-Sep-2024

« **EP4004782B1**

# Intrusion anomaly monitoring in a vehicle environment



The patent addresses security issues in vehicles caused by the complexity and connection of electronic devices, which can be vulnerable to intrusion attacks. The solution is a system that watches for intrusion anomalies in vehicles using ECUs, a security monitor to find these activities, and an anomaly analyzer to compare detected anomalies against a list of known incidents. This system also looks at vehicle status signals to see if any known problems have happened and sends out signals based on this check. This patent aims to improve vehicle cybersecurity by actively watching for and finding possible attacks, protecting important vehicle functions from outside threats.

Company name C2a Sec Ltd

Inventors Yitzhack Davidovich,  
Aharon Naiman,  
Roie Kerstein

Priority date 24-Jul-2019

Publication date 4-Sep-2024

《 CN118677698A

# Analysis method for identifying network security risk and countermeasure of automobile ECU

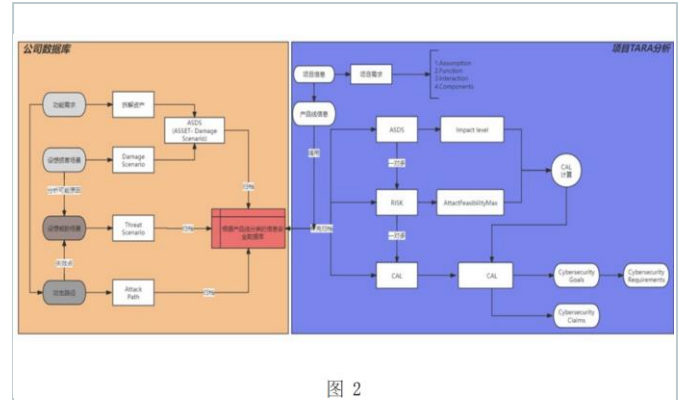


图 2

The patent addresses the need for a systematic method to identify network security risks and implement countermeasures for automobile ECUs. It recognizes that ECU communication safety is critical, especially with increasing connectivity and potential threats. The solution involves five steps: identifying threats, assessing vulnerabilities, analyzing risks by combining motivation, capability, and severity, prioritizing threats based on risk scores, and implementing precautionary measures. This method uses TARA methodology and ISO 21434 standards for a thorough evaluation which This enhances cybersecurity for automotive ECUs by systematically identifying threats and assessing vulnerabilities, improving security awareness, and ensuring regulatory compliance.

Company name Shanghai Yiyan Electronic Technology Co Ltd

Inventors Li Yannong

Priority date 13-Aug-2024

Publication date 20-Sep-2024



《 CN118467008B

# Security management method, system, medium and electronic equipment for OTA upgrade



The patent deals with security issues in Over-The-Air (OTA) vehicle upgrades, where data packets can be intercepted and tampered with during transmission over open networks, leading to risks like unauthorized access and system failures. The solution is a security management method that uses a whole vehicle controller and an intelligent cabin control domain. When an OTA upgrade is requested, the vehicle controller generates a timestamp-based dynamic key and its hash value, which are sent through different channels for secure verification. If verified, the dynamic key is stored securely for the OTA process. This method reduces the risk of key tampering, improves authenticity checks, and secures keys and hash values against interception, ensuring safe OTA upgrades.

Company name Chengdu Seres Technology Co Ltd

Inventors Wang Xingxing,  
Fan Li,  
Deng Lingtian,  
Han Bo,  
Chen Jianwei

Priority date 11-Jul-2024

Publication date 24-Sep-2024



« IN549893A1

# Method and system for performing key encryption and cyber security in vehicles using SSM

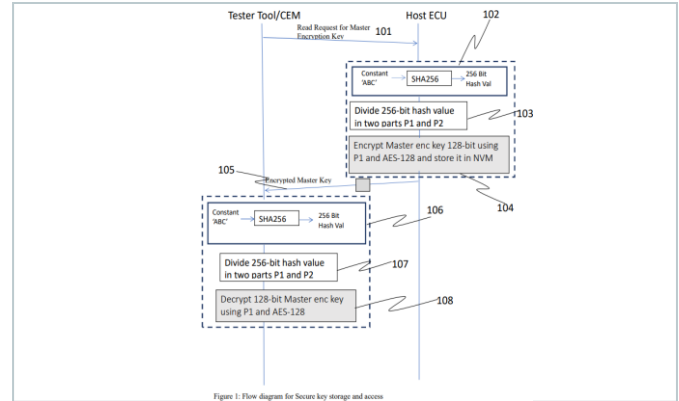


Figure 1: Flow diagram for Secure key storage and access

The patent addresses the need for cybersecurity in modern vehicles by protecting inter and intra-vehicle communications from cyber attacks. Traditional methods use Hardware Security Modules (HSM) that require dedicated memory chips for each ECU, which can be expensive and difficult to update. The solution involves securely exchanging a master key between two ECUs. The second ECU creates a hash value, splits it into two parts, and uses one part to encrypt the master key. This encrypted key is then sent back to the first ECU, ensuring secure communication between the two. This method enhances security by ensuring that only authorized ECUs can communicate, while also being more cost-effective and adaptable to new security algorithms.

Company name Minda Corp

Inventors C Naveen Andrew

Priority date 1-Jul-2021

Publication date 10-Sep-2024

# We are now in India

## Your global full-service IP partner

With 60+ years of experience and 23 offices worldwide, Denemeyer 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






# 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**

