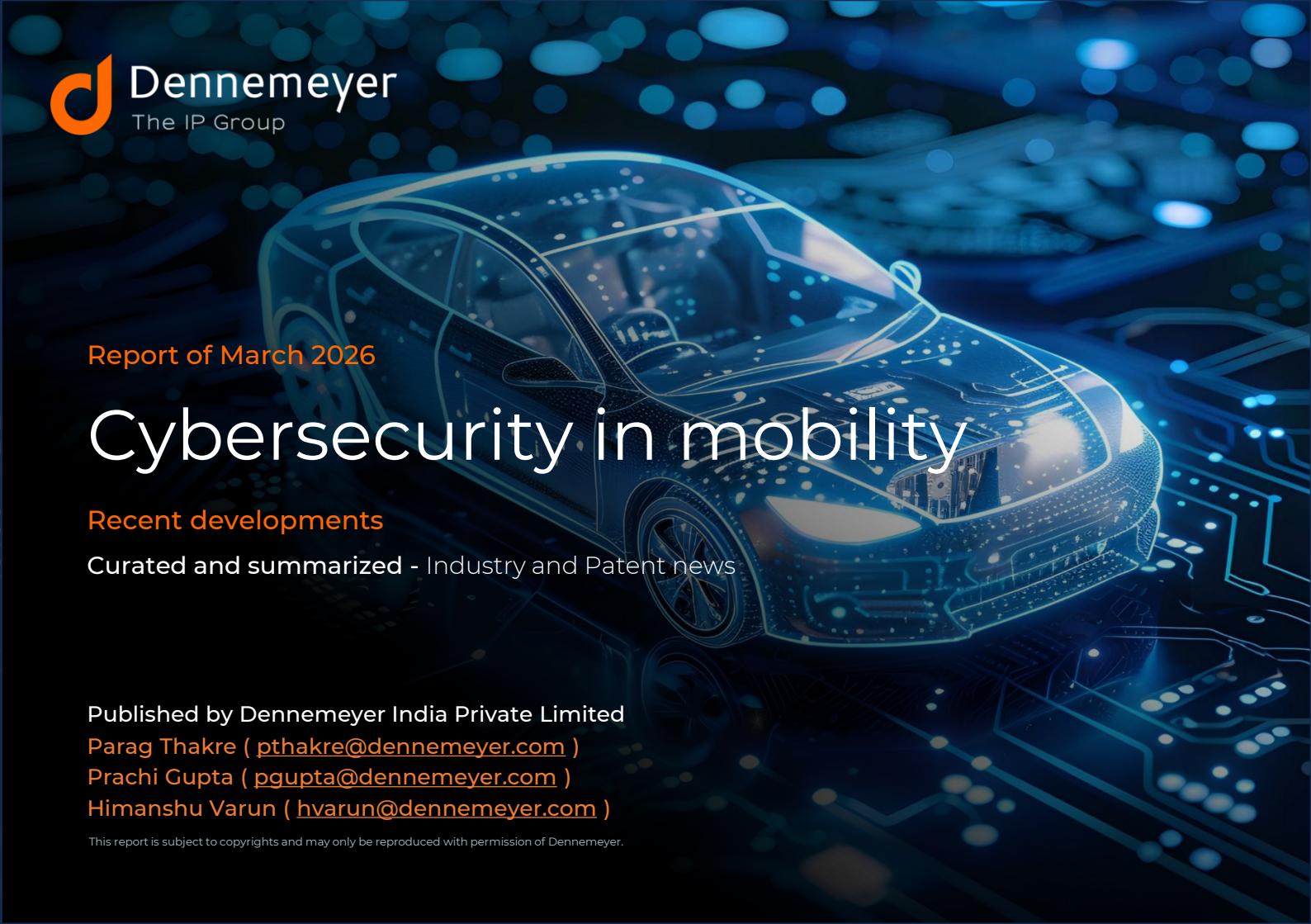
Dennemeyer
The IP Group



Report of March 2026

Cybersecurity in mobility

Recent developments

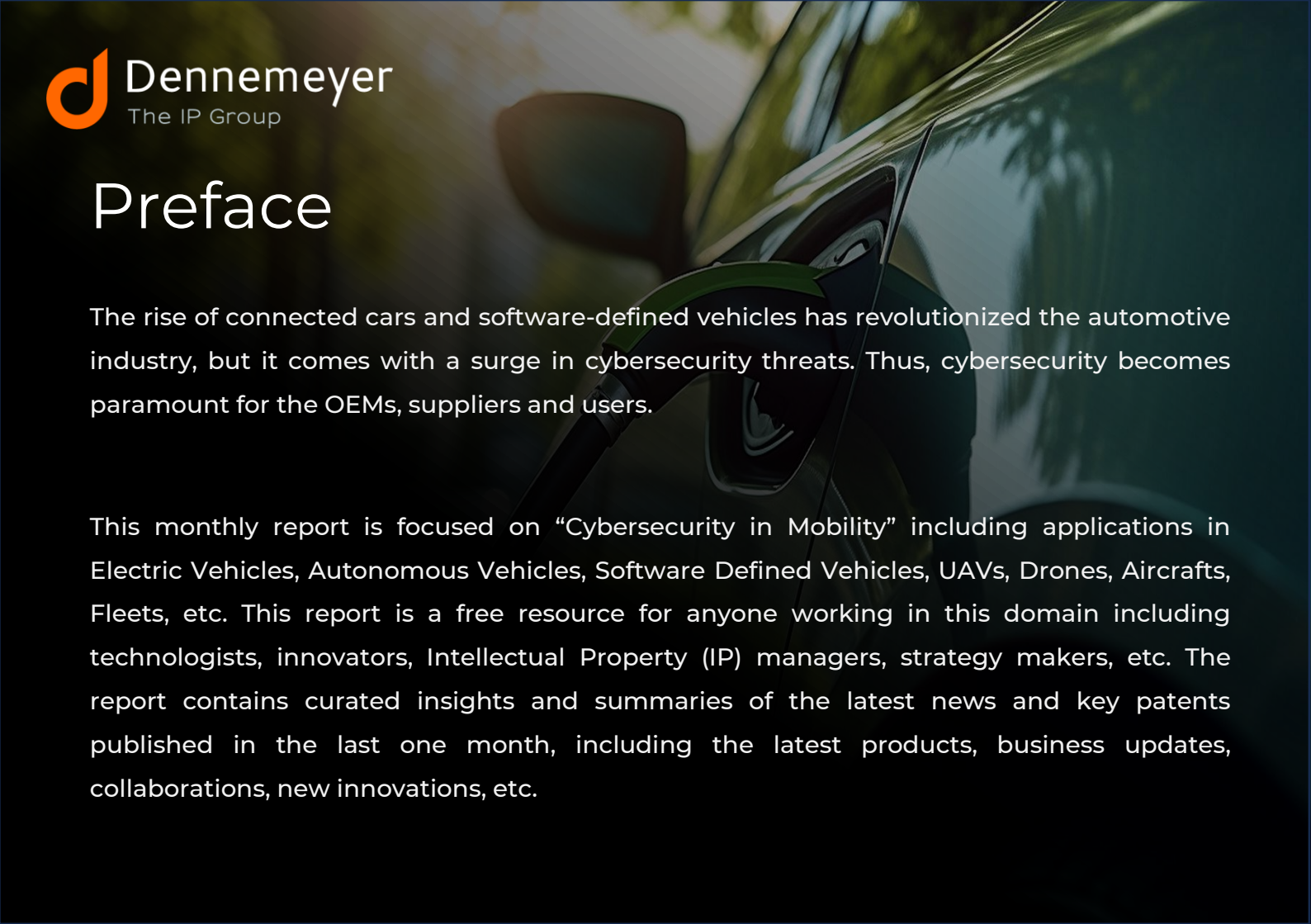
Curated and summarized - Industry and Patent news

Published by Dennemeyer India Private Limited
Parag Thakre (pthakre@dennemeyer.com)
Prachi Gupta (pgupta@dennemeyer.com)
Himanshu Varun (hvarun@dennemeyer.com)

Dennemeyer
The IP Group

Subscribe now

Scan the QR code to receive this monthly report via email in your inbox.
You can also subscribe to our other insights – Cellular Vehicle-to-Everything (C-V2X) and Path to Sustainability – via the same subscription center.



Dennemeyer
The IP Group

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.

Dennemeyer
The IP Group

Key Insights

- HSB's launch of cyber insurance for connected commercial vehicles turns cybersecurity from a cost center into an insurable risk. Insurers will likely require evidence of key cybersecurity controls and adherence to security practices to offer lower premiums. This will push fleets, OEMs, and telematics vendors to rapidly adopt a baseline Cybersecurity Management System (CSMS).

- The ransomware attack on DinnebierGruppe shows how attacks against mid-to-large automotive firms now threaten production continuity, and supplier networks. This suggests that automakers will increase supplier cybersecurity audits, strengthen contractual controls, and require evidence-based CSMS across supply chains.

- PlusAI's four ISO certifications ahead of its autonomous truck launch show that regulatory and safety compliance is becoming essential for scaling long-haul trucking operations. Vendors that can demonstrate strong safety, cybersecurity, and data-governance readiness will gain faster OEM validation and smoother global deployment.

- The Distributed Denial of Service (DDoS) attack that disrupted Deutsche Bahn's booking and information services shows how such incidents can significantly affect customer experience and operations even when no data is stolen. Transport authorities may prioritize DDoS mitigation and multi-region resilience and require demonstrable operational continuity plans to ensure service stability during such incidents.

- Many inventions that were published last month had major themes as below:

  - Connected vehicles now use layered attack detection that monitors network traffic. By combining replay checks with adaptive log management, these systems cut false alerts and make incident response more evidence driven.
  - Positioning integrity is becoming a major security issue, with new inventions countering Global Navigation Satellite System (GNSS) spoofing through sensor fusion, adaptive antennas, and roadside unit triangulation.

Dennemeyer
The IP Group

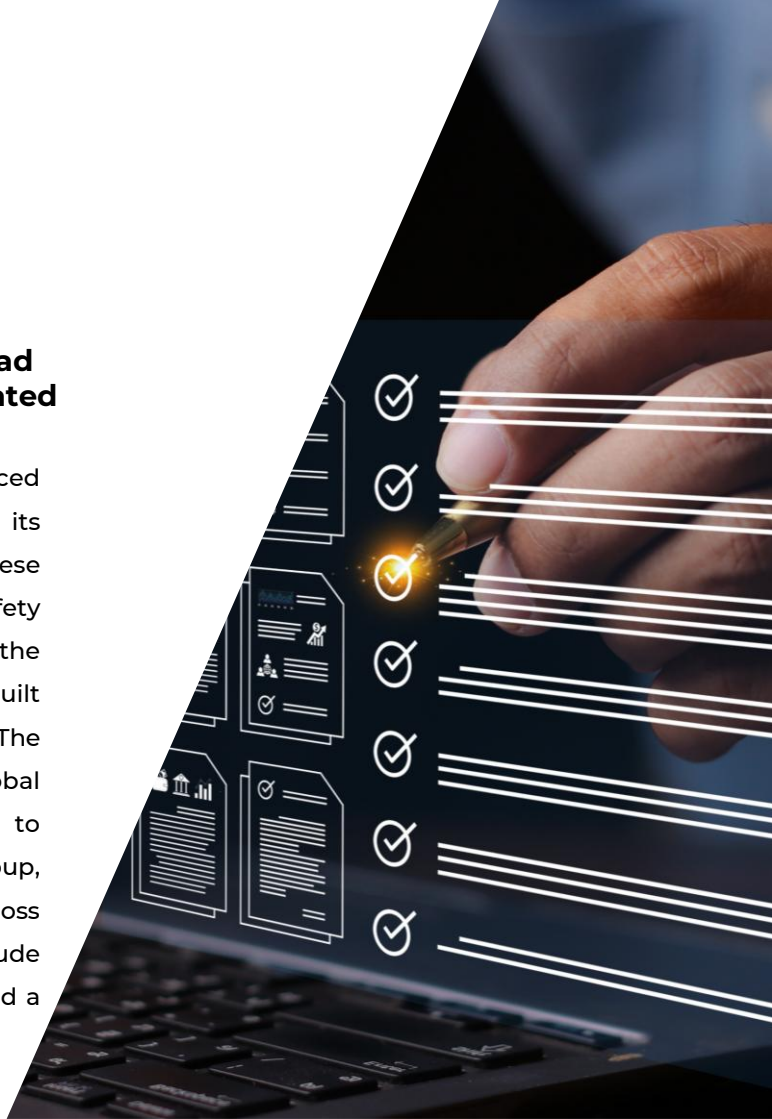
Industry News

Certification

PlusAI secures four key ISO certifications ahead of commercial launch of SuperDrive™-integrated factory-built autonomous trucks

PlusAI, a leader in autonomous truck software, announced that it has earned four major ISO certifications, proving its readiness for large scale commercial deployment. These certifications cover quality, cybersecurity, functional safety and data security. Together, these achievements clear the way for the company's planned 2027 launch of factory built autonomous trucks with global manufacturers. The company's SuperDrive platform is now validated for global scaling and factory level integration. PlusAI continues to strengthen partnerships with Traton Group, Iveco Group, Hyundai and others to expand autonomous trucking across the United States, Europe and Japan. New programs include the first Level 4 trucking corridor in southern Europe and a strategic entry into Japan with Mitsui and T2.

Source
https://plus.ai/



Dennemeyer
The IP Group

Industry News

Cyber Insurance

HSB launches cyber insurance for connected commercial vehicles

HSB, a premier specialty insurer, has introduced a new cyber insurance product that protects internet connected commercial vehicles from hackers and pays businesses for lost income after an attack. The coverage applies when a cyberattack damages a vehicle's systems, data, or onboard devices. It also includes protection against cyber extortion, identity theft, and operational disruption. HSB says cyberattacks on work vehicles are becoming a serious threat as more commercial cars and trucks rely on apps and connectivity. The insurance helps small and medium businesses recover by covering business income loss and extra expenses during interruptions. The policy includes cybersecurity services and pays to upgrade hardware and software to prevent future attacks.

Source
https://www.businesswire.com/

Dennemeyer
The IP Group

Industry News

Ransomware Attack

Cloak ransomware targets German auto giant Dinnebiergruppe.de

The ransomware group Cloak claimed it carried out a cyberattack on the German automobile company Dinnebiergruppe. The attackers posted an extortion message saying they would publish stolen data unless the company contacted them. Dinnebiergruppe is now dealing with a serious threat where sensitive information may be leaked. Ransomware attacks like this are becoming more common for both large and midsize companies. Security teams are advised to review how the attackers got in, check whether data was copied, and confirm that backups are safe and offline. Companies should also monitor the dark web for leaked credentials and use threat intelligence to detect danger early. Strengthening employee security by using multi factor authentication and phishing training is critical.

Source
https://www.dexpose.io/

Dennemeyer
The IP Group

Industry News

Denial of Service Attack

Deutsche Bahn says cyberattack hit ticket and info systems

Deutsche Bahn said it was hit by a major cyberattack that disrupted its website and Navigator app. The attack was a Distributed Denial of Service (DDoS) assault, where hackers overload systems with traffic until they slow down or stop working. The company said the attack targeted its IT systems in several waves and was large in scale. Travel information and ticket booking tools went down for many customers. After a period of partial recovery, most systems were stable again, but new problems soon re-emerged. Deutsche Bahn said its defensive measures helped limit the impact on passengers. The company refused to comment on who might be behind the attack and stressed its focus on protecting customer data.

Source
https://www.dw.com/

Dennemeyer
The IP Group

Industry News

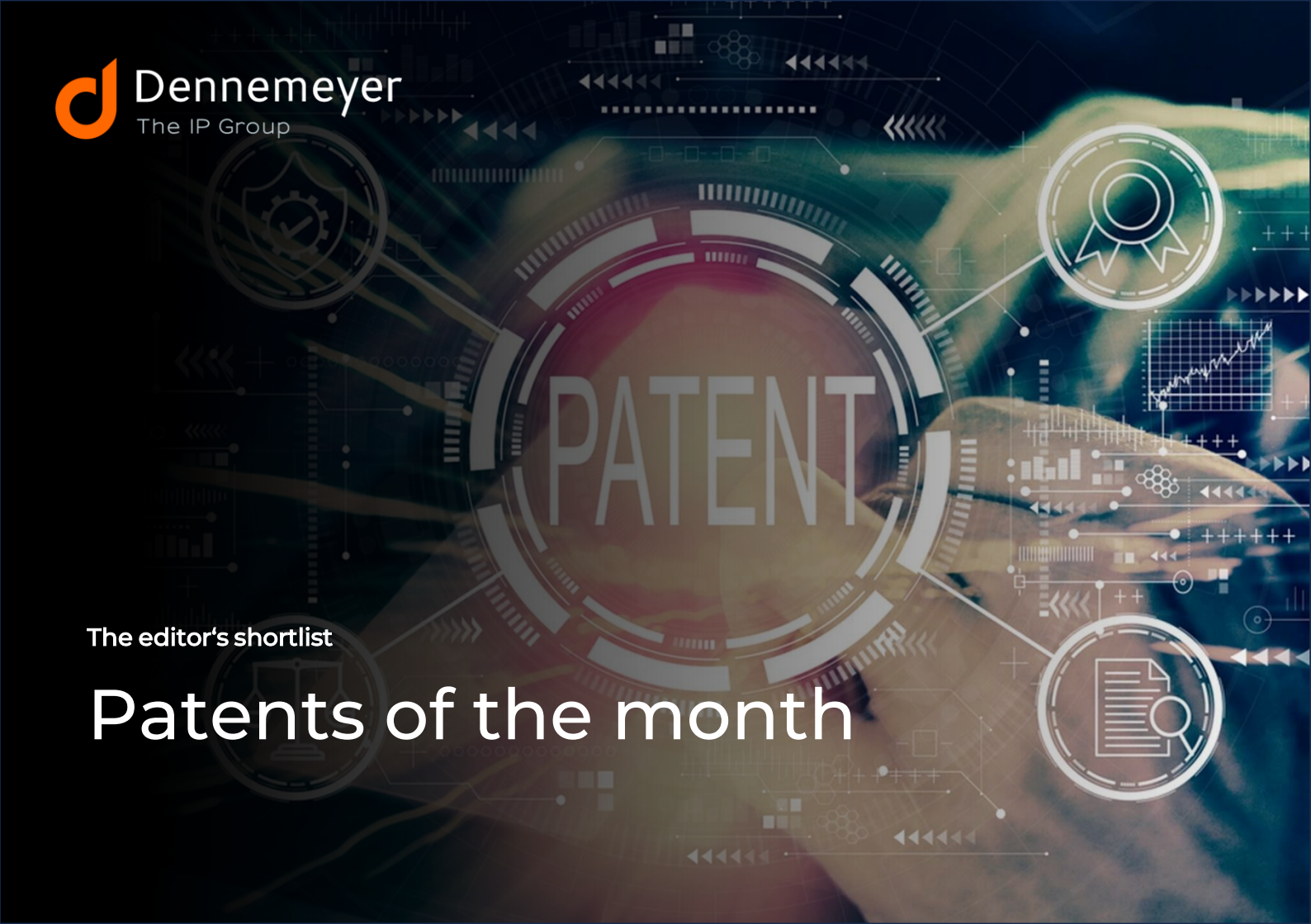
Data Breach

Hackers sell stolen Eurail traveler information on dark web

Eurail B.V. has confirmed that customer data stolen in a cyber breach earlier this year is now being sold on the dark web, with samples also appearing on Telegram. The Netherlands based company, which runs the Eurail Pass used for train travel across Europe, said hackers accessed customer information. Early findings show that order details, contact information, identity data, travel companion details and in some cases passport numbers may have been exposed. The company clarified that it does not store payment card details or passport copies. Eurail secured its systems after the breach and is still investigating with external cybersecurity and legal experts. Affected customers will be notified and are advised to change their Rail Planner app password, update related account passwords and monitor their bank and email accounts for unusual activity.

Source
https://securityaffairs.com/

Dennemeyer
The IP Group



The editor's shortlist

Patents of the month

Dennemeyer
The IP Group

Patents summarized with the help of Octi AI powered by Octimine Dennemeyer IP Group

Patents of the month

Published in February 2026

Shortlisted and summarized by our analyst

- US12542797B1 - Analysis and prioritization of vulnerabilities of connected vehicles
  Assignee: VicOne Corp
- US2026039669A1 - Electronic device and method for providing an alarm and storing a log according to detecting an attack on a vehicle network
  Assignee: Hyundai Motor Co, Kia Corp
- US2026043924A1 - Trusted PNT solution by CRPA assisted GNSS spoofing protection
  Assignee: Rockwell Collins Deutschland GMBH
- US12556572B2 - Cyber resilient trade-off evaluation systems for operational technology environments, including related methods and computer readable media
  Assignee: Battelle Energy Alliance LLC, Univ Idaho
- US2026057066A1 - Replay attack protection in automotive electronics
  Assignee: Qualcomm Inc
- US2026059304A1 - Secure communication for unmanned aerial vehicle in integrated ecosystem
  Assignee: Continental Automotive Technology GMBH
- EP4320464B1 - GNSS spoofing detection and recovery
  Assignee: Qualcomm Inc
- JP7809417B2 - Information providing method and information processing device
  Assignee: Panasonic Automotive System Co Ltd
- CN120956543B - Pure electric vehicle information safety anti-replay control method and system
  Assignee: Anhui Ankai Automobile Co Ltd
- CN119341786B - Network security hole implantation method and related device
  Assignee: China Merchants Testing Vehicle Technology Research Institute Co Ltd

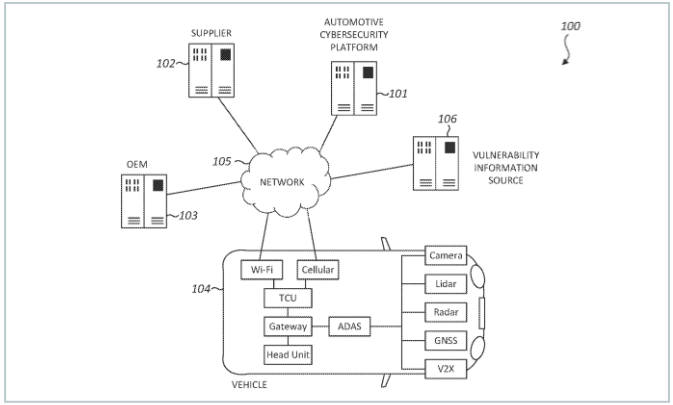
Dennemeyer
The IP Group

Latest patents

Patent summarized with the help of **Octi AI**

US12542797B1

Analysis and prioritization of vulnerabilities of connected vehicles



Company name	VicOne Corp
Inventors	Cheng Yi Li, Hsu Jui Chang
Priority date	09 Jan 2023
Publication date	03 Feb 2026

The patent describes a cybersecurity platform that helps car makers find software weaknesses in connected vehicles, which contain many ECUs running code from different suppliers and are therefore hard to assess manually. The platform gathers a list of software components used in all ECUs and matches them against vulnerability alerts coming from sources like vulnerability databases to identify which components are affected. It then examines metadata to check whether the vulnerable component would actually load and run inside the vehicle, meaning the flaw can truly be triggered. The system also studies how an attack would impact the vehicle by running simulated exploits across ECUs to understand real safety consequences. Using both external risk scores and these analyses, it calculates an overall risk value so OEMs can fix the most dangerous issues first.

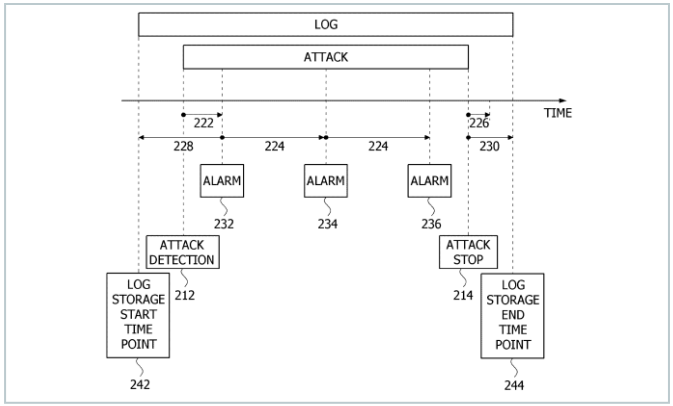
Dennemeyer
The IP Group

Latest patents

Patent summarized with the help of **Octi AI**

US2026039669A1

Electronic device and method for providing an alarm and storing a log according to detecting an attack on a vehicle network



Company name	Hyundai Motor Co, Kia Corp
Inventors	Jeong Seung Yeon
Priority date	02 Aug 2024
Publication date	05 Feb 2026

The patent talks about detecting cyberattacks in vehicular networks, since existing tools mainly focus on older systems. When suspicious activity is detected, it waits to see if the attack continues for a set amount of time before raising an alarm so that drivers and systems are not overwhelmed by false alerts. If the attack persists, it triggers an alarm and begins saving important logs from just before the attack and through the duration of the attack. Once the activity stops and no more attack behavior is seen for another defined period, it marks the attack as ended and continues saving logs for a while afterward to fully capture what happened. These time windows can be automatically adjusted depending on the attack type, such as bus flooding or replay attacks. The method also manages limited memory by keeping more important logs and erasing less important ones when needed.

Dennemeyer
The IP Group

Latest patents

Patent summarized with the help of **Octi AI**

US2026043924A1

Trusted PNT solution by CRPA assisted GNSS spoofing protection

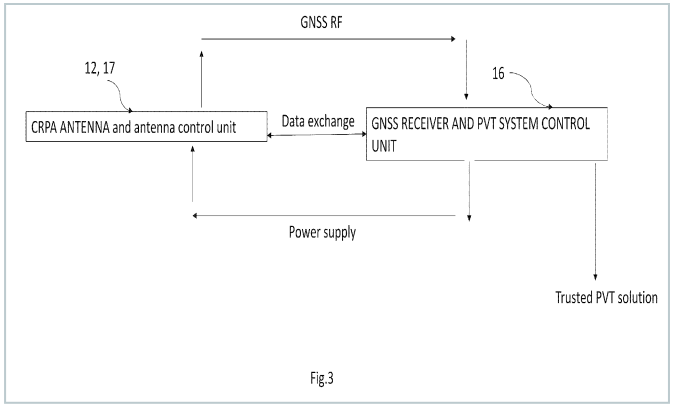


Fig.3

Company name	Rockwell Collins Deutschland GMBH
Inventors	Ehinger Markus
Priority date	22 Mar 2024
Publication date	12 Feb 2026

The patent detects Global Navigation Satellite System (GNSS) spoofing attacks, these attacks use fake satellite signals to fool a vehicle about its location or time. The invention uses a special antenna that can change how it listens to satellites. It first scans all visible satellites in one pattern and notes their signals, then scans them again in a different pattern. If the signal strength changes in a way that does not make sense, the system suspects spoofing. It also uses data from the vehicle's motion sensors and known satellite positions to point the antenna more accurately at real satellites. This helps confirm whether each satellite is where it should be. It also checks timing between scans to catch replay attacks that slightly shift time. If anything looks suspicious, the vehicle can ignore signals from that direction or restart its receiver to rebuild a correct location or time, making spoofing much harder.

Dennemeyer
The IP Group

Latest patents

Patent summarized with the help of **Octi AI**

US12556572B2

Cyber resilient trade-off evaluation systems for operational technology environments, including related methods and computer readable media

Company name	Battelle Energy Alliance LLC, Univ Idaho
Inventors	Rieger Craig G, Kolias Konstantinos, Ivans Robert Christopher
Priority date	12 Sep 2022
Publication date	17 Feb 2026

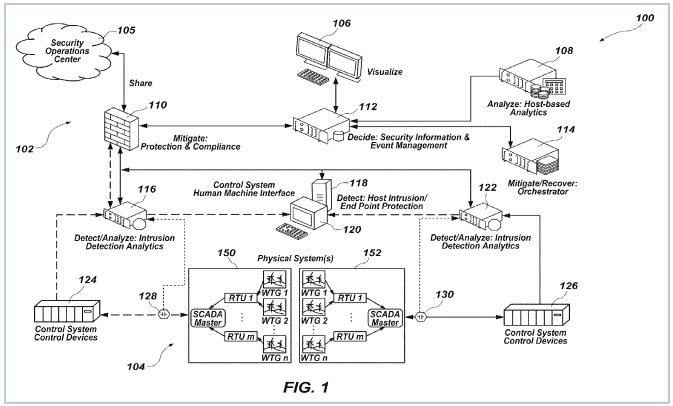


FIG. 1

The patent helps operators of critical infrastructures like power grids understand how different cyber attack countermeasures will affect both the digital and physical parts of their systems. It uses a digital twin that behaves like the real physical process, combined with cyber components, to simulate attacks and test how various mitigation strategies perform without risking the systems. For each candidate mitigation action, the system observes both the cyber response and the physical reaction, then calculates how resilient the overall system would be under that strategy. A special module automatically explores many combinations of mitigation settings and parameters to find the most effective options. Through repeated simulations, the system ranks these strategies based on their ability to maintain security while also keeping the physical process stable.

Dennemeyer
The IP Group

Latest patents

Patent summarized with the help of **Octi AI**

US2026057066A1

Replay attack protection in automotive electronics

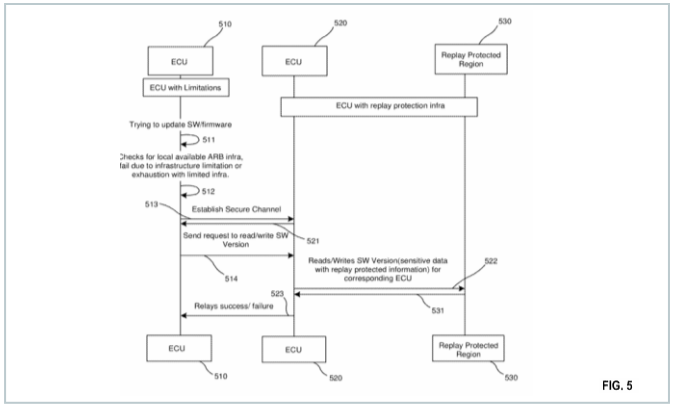


FIG. 5

Company name	Qualcomm Inc
Inventors	Raj Nishant, Rao Yashavantha, Tewari Piyush, Parasa Ananda Kishore, Maheshwari Shyam, Punoriyar Sourav Kumar
Priority date	22 Aug 2024
Publication date	26 Feb 2026

The patent explains a way to protect lightweight automotive ECUs from replay attacks during firmware updates by creating a secure connection with a more powerful central ECU. The secure channel exposes a replay-protected memory region located inside the central ECU for safely reading and writing sensitive update information. Through this channel, the lightweight ECU can request access to update data, read the first part of the sensitive software, write back updated data, and send results to the central ECU, while the central ECU manages the secure memory area. The secure channel uses layered protocol data units with headers for routing and control and payloads for the actual data. The system can confirm the secure channel, check whether the lightweight ECU has enough memory for the update, and send completion or failure messages once the update finishes.

Dennemeyer
The IP Group

Latest patents

Patent summarized with the help of **Octi AI**

US2026059304A1

Secure communication for unmanned aerial vehicle in integrated ecosystem

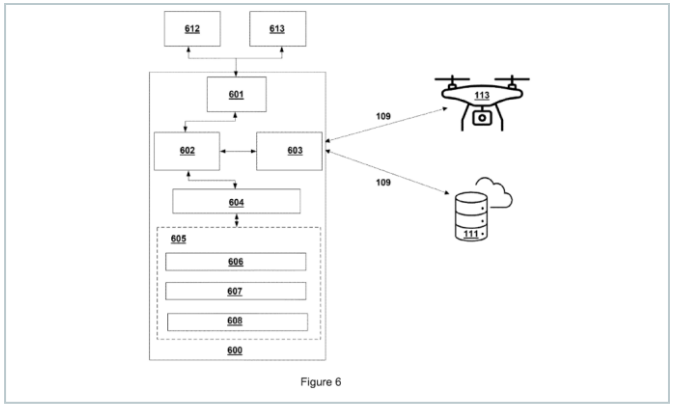


Figure 6

Company name	Continental Automotive Technology GMBH
Inventors	Pammu Ali Akbar
Priority date	25 Aug 2023
Publication date	26 Feb 2026

The patent describes a secure communication method for UAVs operating in a shared ecosystem, addressing risks like tampering, and spoofing attacks by ensuring every message between the user terminal, server, and UAV is authenticated. The process starts when the user terminal sends a delivery request to the server, receives a digitally signed delivery response, and verifies it using the server's public key. After verification, the user terminal asks the UAV for its battery level and forwards the delivery response only if it meets the minimum threshold defined in the response, ensuring the UAV can safely complete its route. The UAV then checks the signature in the forwarded response with its own public key and sends an acknowledgement. Once the acknowledgement is received, the user terminal generates a session key and sends it to the UAV so the UAV and server can communicate securely.

Dennemeyer
The IP Group

Latest patents

Patent summarized with the help of **Octi AI**

EP4320464B1

GNSS spoofing detection and recovery

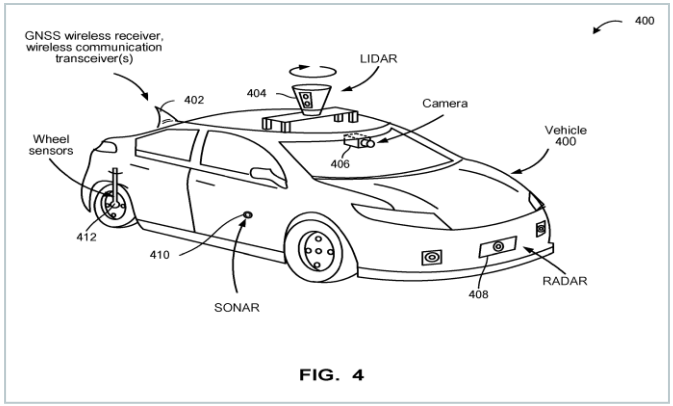


FIG. 4

Company name	Qualcomm Inc
Inventors	Sharma Arunandan, Slobodyanyuk Volodimir, Shuman Mohammed Ataur Rahman
Priority date	05 Apr 2021
Publication date	18 Feb 2026

The invention helps in spotting GNSS spoofing attacks by comparing a device's GNSS-based location with information from onboard sensors and nearby roadside units (RSUs). The mobile device first receives normal GNSS signals and then receives a message from an RSU that includes either the RSU's fixed location or a calculated estimate of the device's position. The device checks if its GNSS-derived position suddenly shifts in a way that disagrees with readings from sensors beyond a set threshold, which signals possible spoofing. It also checks if the GNSS-based position differs too much from the RSU's reference or calculated device position. If both types of discrepancies exceed their respective limits, the GNSS signal is flagged as spoofed. The device can then switch to safe backup positioning using non-GNSS sensors until authentic satellite signals return.

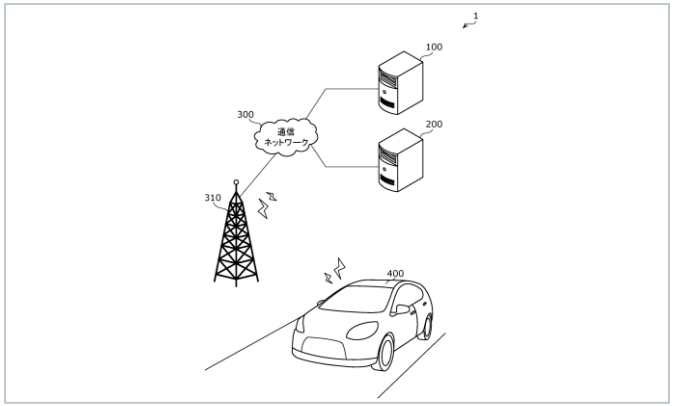
Dennemeyer
The IP Group

Latest patents

Patent summarized with the help of **Octi AI**

JP7809417B2

Information providing method and information processing device



Company name	Panasonic Automotive System Co Ltd
Inventors	Fukushima Hideyo, Hidaka Jun, Yoshida Junichi, Nakatsuji Shigeyoshi, Asanuma Masahito
Priority date	11 Nov 2022
Publication date	02 Feb 2026

The patent helps drivers understand what to do when their vehicle is under a cyberattack by clearly showing which parts of the vehicle are affected and whether it is still safe to keep driving. When the security system detects an attack on a specific function, it sends instructions to the vehicle so only the targeted non driving features like cameras, microphones, or GPS are forcibly stopped while keeping the actual driving functions working normally. The vehicle display then shows which feature has been disabled and gives the driver an option to turn it back on if they are willing to accept the risk. If the attack affects a critical driving function like braking or acceleration, the system instead stops that function for safety. Administrators managing fleets can also customize the rules so different types of services handle these situations in different ways.

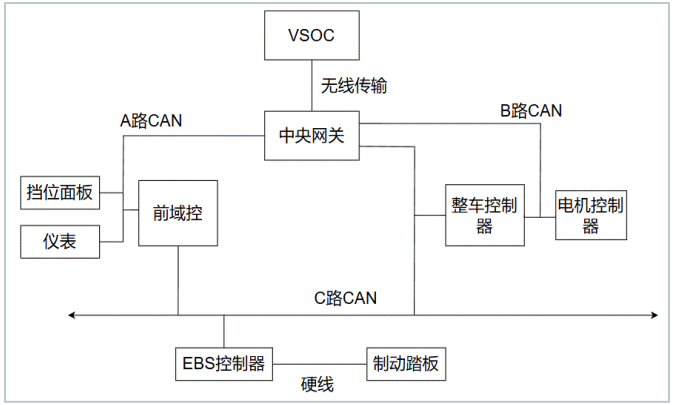
Dennemeyer
The IP Group

Latest patents

Patent summarized with the help of **Octi AI**

CN120956543B

Pure electric vehicle information safety anti-replay control method and system



Company name	Anhui Ankai Automobile Co Ltd
Inventors	Jiang Bo, Huang Liping, Wang Qilong, Chang Sheng, Hu Yang, Xie Feng, Zhang Zhen, Dong Jianying
Priority date	20 Oct 2025
Publication date	10 Feb 2026

The patent protects EVs from replay attacks on the CAN bus, where attackers record and resend important control messages, such as gear or brake commands. This can make the vehicle react in the wrong way and may even lead to loss of control. Because standard CAN protocols do not support adding extra verification fields, the invention uses software-based checks instead. For gear messages, the system checks whether the timing between messages looks normal and uses a changing password placed inside the existing data field to confirm that the message is real. For brake messages, where no custom data can be added, the system predicts when repeated illegal messages might appear and compares multiple frames to detect these attacks, even when they overlap or change timing. When an attack is found, the system alerts the driver, reduces vehicle power or even stopping the vehicle if the attack continues.

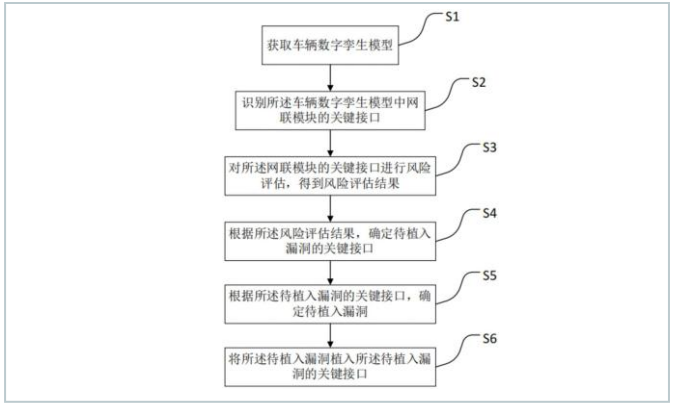
Dennemeyer
The IP Group

Latest patents

Patent summarized with the help of **Octi AI**

CN119341786B

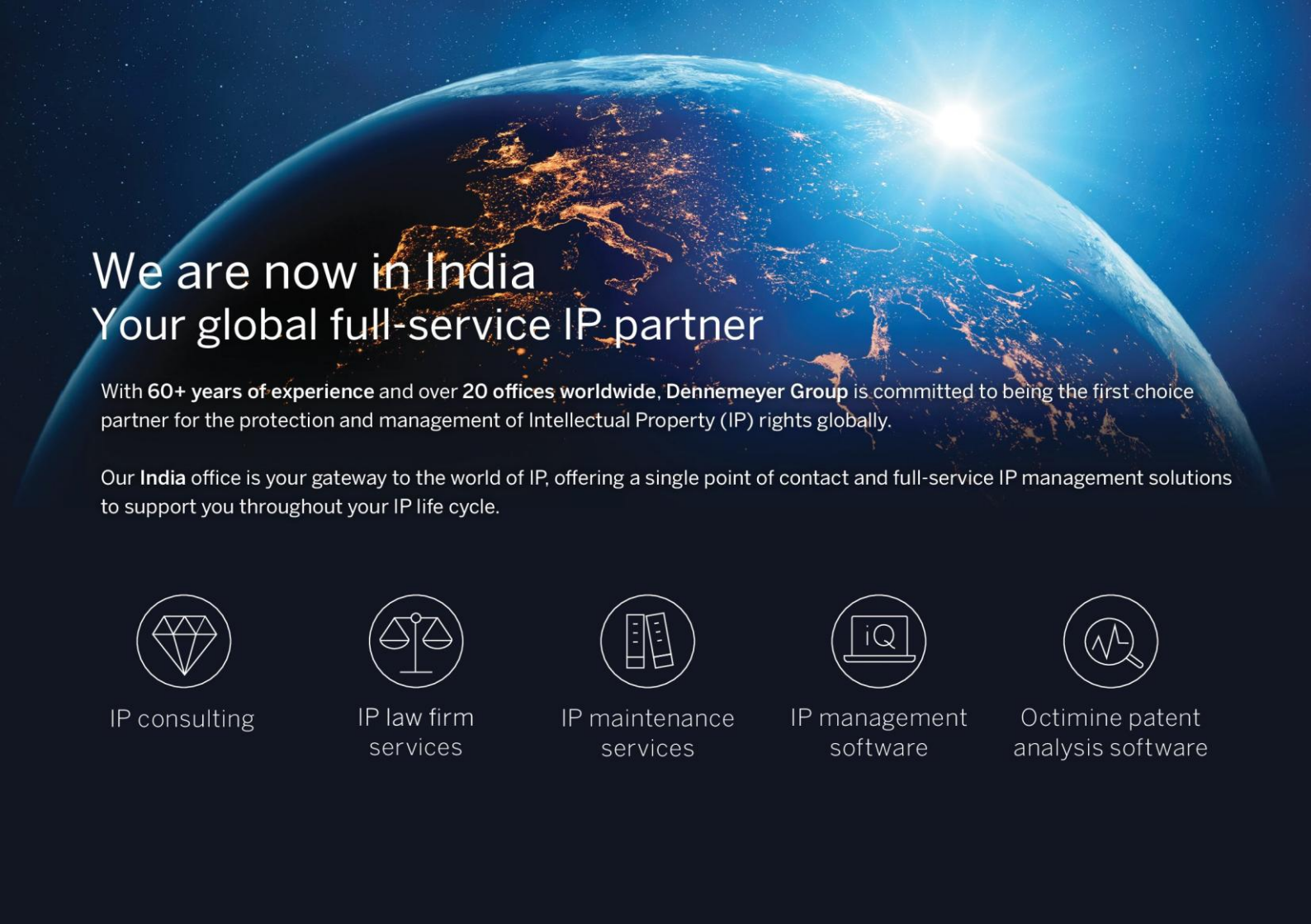
Network security hole implantation method and related device



Company name	China Merchants Testing Vehicle Technology Research Institute Co Ltd
Inventors	Zhou Peng, Wu Chao, Ke Xinqin, Zhang Zhiyong, Cao Fei, Zhang Xiong, Chen Zhenyan, Gong Chen, Yao Bo, Zhu Zixiao, Feng Chengjun, Zhang Xiang
Priority date	27 Sep 2024
Publication date	24 Feb 2026

Summarized by Dennemeyer

The patent improves virtual vehicle testing by adding realistic cybersecurity weaknesses into a vehicle's digital twin. First, it loads the digital twin and studies the vehicle's network to identify key interfaces. It then scores them using factors like how much data they handle, how frequently they are used, the importance of the data, its sensitivity, and timing requirements. Next, it runs simulated cyberattacks on these interfaces to see how many tries it takes to break them. From the results, it calculates defense scores that show how vulnerable each interface is. Using these risk levels, the system selects the most important interfaces and finds matching vulnerabilities from a security database. These vulnerabilities are then added to the interfaces to create a realistic cyber-risk environment. Finally, the system tests the added vulnerabilities, records the results, creates suitable mitigation strategies, and updates the overall security.



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

Dennemeyer
The IP Group

Visit us

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

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

North & East India
+91 9818599822

South & West India
+91 88266 88838