Dennemeyer
The IP Group

Report of February 2026

Cybersecurity in mobility

Recent developments

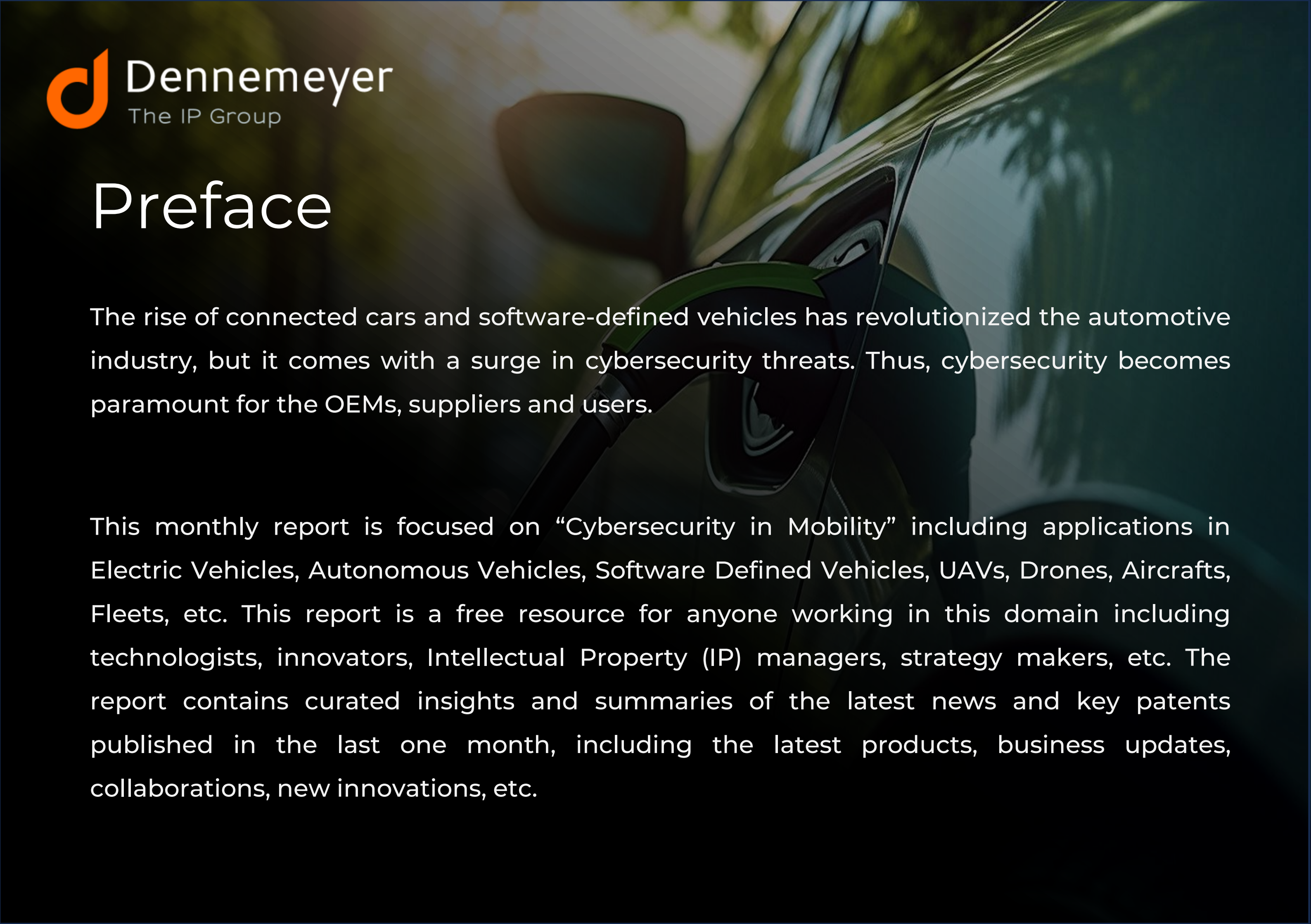
Curated and summarized - Industry and Patent news

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

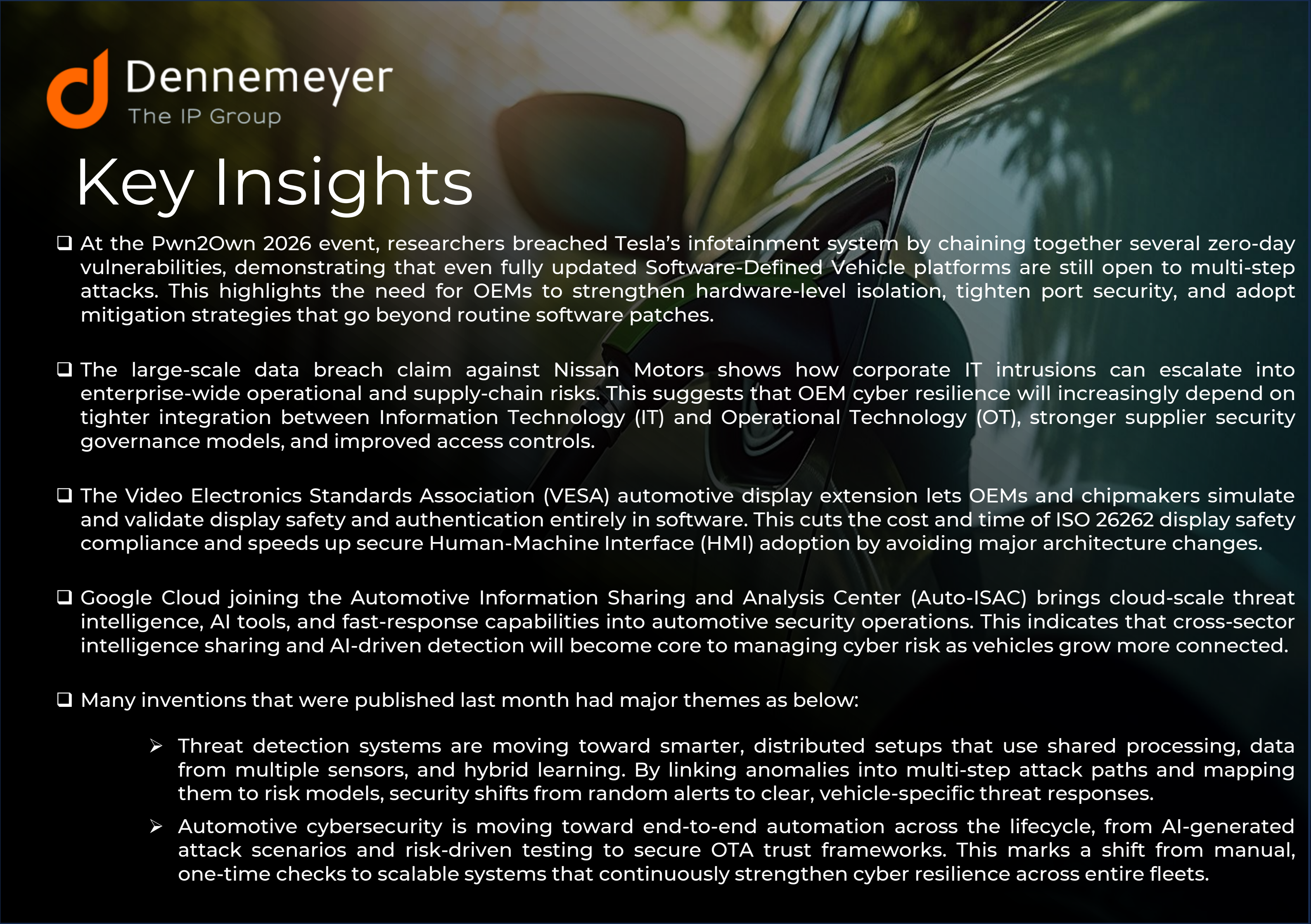
Scan the QR code to receive this monthly report via email in your inbox.



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

- At the Pwn2Own 2026 event, researchers breached Tesla’s infotainment system by chaining together several zero-day vulnerabilities, demonstrating that even fully updated Software-Defined Vehicle platforms are still open to multi-step attacks. This highlights the need for OEMs to strengthen hardware-level isolation, tighten port security, and adopt mitigation strategies that go beyond routine software patches.

- The large-scale data breach claim against Nissan Motors shows how corporate IT intrusions can escalate into enterprise-wide operational and supply-chain risks. This suggests that OEM cyber resilience will increasingly depend on tighter integration between Information Technology (IT) and Operational Technology (OT), stronger supplier security governance models, and improved access controls.

- The Video Electronics Standards Association (VESA) automotive display extension lets OEMs and chipmakers simulate and validate display safety and authentication entirely in software. This cuts the cost and time of ISO 26262 display safety compliance and speeds up secure Human-Machine Interface (HMI) adoption by avoiding major architecture changes.

- Google Cloud joining the Automotive Information Sharing and Analysis Center (Auto-ISAC) brings cloud-scale threat intelligence, AI tools, and fast-response capabilities into automotive security operations. This indicates that cross-sector intelligence sharing and AI-driven detection will become core to managing cyber risk as vehicles grow more connected.

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

    - Threat detection systems are moving toward smarter, distributed setups that use shared processing, data from multiple sensors, and hybrid learning. By linking anomalies into multi-step attack paths and mapping them to risk models, security shifts from random alerts to clear, vehicle-specific threat responses.

    - Automotive cybersecurity is moving toward end-to-end automation across the lifecycle, from AI-generated attack scenarios and risk-driven testing to secure OTA trust frameworks. This marks a shift from manual, one-time checks to scalable systems that continuously strengthen cyber resilience across entire fleets.

Tesla's Infotainment System Hacked

Tesla hacked, 37 zero-days demoed at Pwn2Own Automotive 2026 in Japan

Researchers at the Pwn2Own Automotive 2026 event in Tokyo earned more than 500,000 dollars on the first day by showing different car-hacking demos. One of the main highlights was the Synacktiv team, who managed to break into Tesla's infotainment system. They did this using a USB-based attack that combined two bugs, one that leaked information and another that let them write data on the system. This let them gain full control over the infotainment software, even though the car had the latest updates. The attack required plugging into a USB port, but it showed how chaining multiple flaws together can get around security protections and allow hackers to run high-level code.

Source
https://www.bleepingcomputer.com/

Strategic Partnership

Skoda partners with Upstream to strengthen cyber resilience across its connected vehicle ecosystem

Upstream, a provider of cloud-based automotive cybersecurity solutions, has partnered with Skoda to help the automaker manage cybersecurity risks across its connected vehicles, digital services, and supporting systems. As Skoda's digital footprint grows, the company needs a consistent and efficient way to detect threats, meet regulations, and protect operations. Upstream's platform brings all cyber threat intelligence, signals, and risk information into one shared environment for Skoda teams. This enables earlier identification of risks, smoother collaboration, and reduced manual work for compliance and reporting. Skoda says the partnership supports its activities under the UNECE R155 regulation and the ISO SAE 21434 standard and strengthens cybersecurity resilience across its ecosystem.

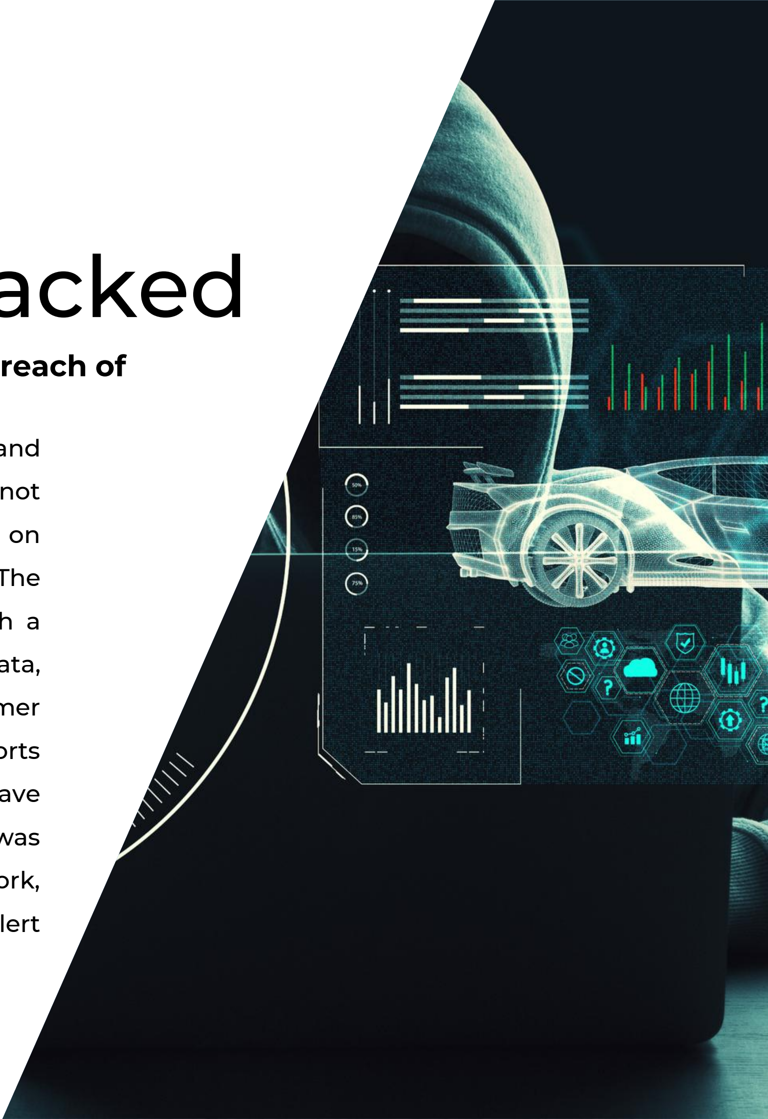
Source
https://upstream.auto/

Nissan Motors Hacked

Everest cybercrime group alleges successful breach of Nissan Motors

The Everest hacking group claims it has breached Nissan and stolen about 900 GB of sensitive data, although this has not yet been verified. The alleged breach was first observed on January 10, 2026, and the attackers shared sample proof. The full nature of the stolen data remains unclear, but such a large volume could include internal operations data, employee information, intellectual property, or customer records. Because Nissan operates globally and supports many downstream industries, a confirmed breach could have wide operational and supply-chain impact. The claim was flagged through Hackmanac's threat-intelligence network, which tracks cybercrime activities and has classified this alert as an active cyberattack.

Source
https://cyberpress.org/



Securing Automotive Displays

VESA formalizes automotive-grade DisplayPort

The Video Electronics Standards Association (VESA) has released DisplayPort Automotive Extension 1.1, adding stronger safety features for in-vehicle displays without changing the existing hardware. The update introduces a software emulator that allows automakers and chip makers to test safety, authentication, and tamper-detection behavior before hardware is built. This version supports multiple safety profiles under ISO 26262 standard and detects dropped, duplicated frames, and errors to ensure driver-critical information remains reliable. The extension is implemented as a thin layer on top of DisplayPort (hardware component), enabling adoption without major architectural changes. VESA is also preparing certification programs and aims to position DisplayPort as a trusted standard for safety-critical automotive displays.

Source
https://www.jonpeddie.com/

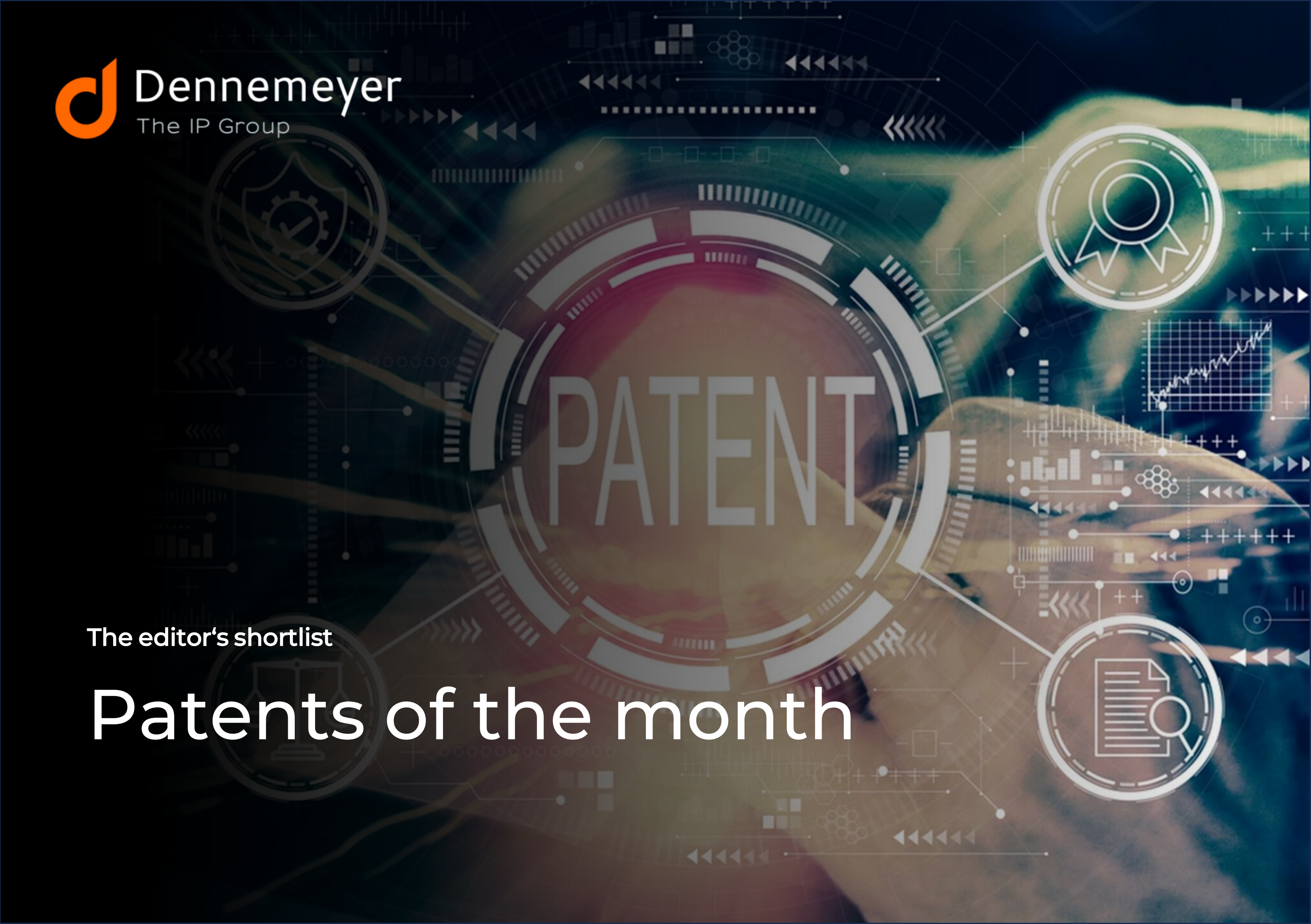
Collaborative Innovation

Auto-ISAC and Google partner to boost automotive sector cybersecurity

Google Cloud has joined the Automotive Information Sharing and Analysis Center (Auto-ISAC) as an Innovator Partner, strengthening its role in securing the global automotive sector. The partnership comes as modern vehicles increasingly depend on cloud systems, high-speed networks, and AI, expanding cyber risks across factories, supply chains, and connected cars. Google Cloud will contribute expertise in IT, OT, supply chain security, and software-defined vehicle security, supported by Mandiant intelligence. The collaboration aims to help members detect threats earlier, manage crises, and maintain operations. Google says this aligns with its five-year, 10-billion-dollar cybersecurity commitment and its existing partnerships with ISACs in the energy, healthcare, and finance sectors.

Source
https://cloud.google.com/

Dennemeyer
The IP Group



The editor‘s shortlist

Patents of the month

Patents of the month

Published in January 2026

Shortlisted and summarized by our analyst

- US2026012793A1 - In-vehicle device, roadside device, vehicle-external device, security management method, and computer program
  Assignee: AutoNetworks Technology Ltd, Sumitomo Electric Ind Ltd, Sumitomo Wiring System Ltd
- US2026012467A1 - Signal processing system of vehicle and vehicle including the same
  Assignee: LG Electronic Inc
- US20260030351A1 - Threat analysis system and threat analysis method
  Assignee: Panasonic Automotive Systems Co Ltd
- US12517811B2 - Method, system and device for generating test case for automotive cybersecurity detection
  Assignee: Catarc Software Testing Tianjin Co Ltd
- US2026012478A1 - Systems and methods for detecting and mitigating cyber attacks on converter-based energy equipment and associated communication networks
  Assignee: DER Security Corp
- EP4679304A1 - System and method for protecting a system
  Assignee: Argus Cyber Security Ltd
- JP2026004228A - Techniques for verifying accuracy and/or generating judgments regarding the risk of cyber attacks on a system
  Assignee: Robert Bosch Gmbh
- KR20260004809A - Device for providing an interface in which the automobile CAN communication simulation function is implemented
  Assignee: Konyang Univ Ind Cooperation Group
- CN121283750A - Rail vehicle network security risk detection method, device, equipment and medium
  Assignee: National High Speed Train Qingdao Technology Innovation Center
- CN121283680A - Method, system, medium and product for improving vehicle end intrusion detection function
  Assignee: SAIC General Motors Corp Ltd, Pan Asia Technical Automotive Center Co Ltd

US2026012793A1

In-vehicle device, roadside device, vehicle-external device, security management method, and computer program

Company name	AutoNetworks Technology Ltd, Sumitomo Electric Ind Ltd, Sumitomo Wiring System Ltd
Inventors	Ogawa Akihiro, Kakito Kazuhiro
Priority date	15 Jul 2022
Publication date	08 Jan 2026

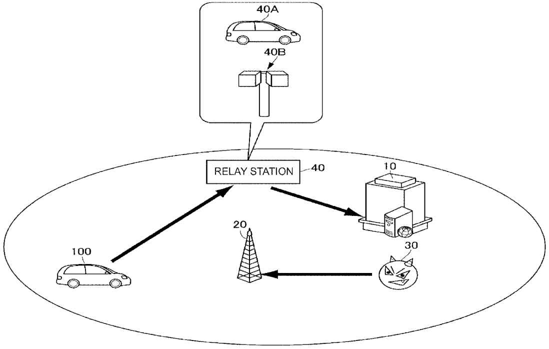


FIG. 2

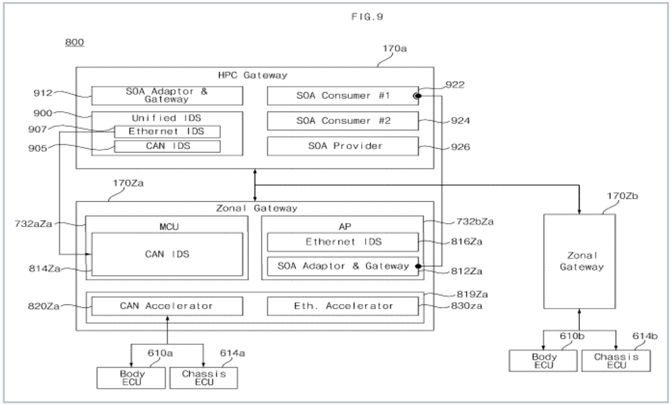
The patent describes an approach that prevents cyberattacks from blocking vital vehicle functions while keeping essential communication, such as emergency messages, active. The solution is an in-vehicle device that detects a cyberattack and immediately switches the vehicle's communication path from the attacked relay station (RS) to a different RS using another wireless interface, so the attack path is cut off while essential communication continues. The system can work with many wireless technologies such as cellular networks and vehicle-to-vehicle links, and it selects the safest RS by checking factors like security strength, risk scores, communication quality, and the vehicle's location. It constantly updates these choices as the car moves and can be managed either by the vehicle itself or by roadside units that instruct the vehicle which RS to use.

US20260124467A1

Signal processing system of vehicle and vehicle including the same

Company name	LG Electronic Inc
Inventors	Park Junsang, Cho Chaeguk
Priority date	25 Nov 2022
Publication date	08 Jan 2026

Summarized by Dennemeyer



This patent tackles problems in vehicle communication systems where current intrusion detection struggles with high processor load and false alarms, especially when Controller Area Network (CAN) messages travel over Ethernet. It uses two devices: one performs semantic checks that adapt to CAN or Ethernet inputs, while the other focuses on syntax checks on CAN messages. By splitting the work, the system lightens the load on each processor and improves detection accuracy. The primary device can also look at several sensor signals together and can inspect Ethernet frames that carry CAN data to prevent mistakes. When unusual but legitimate messages come in, the devices communicate to avoid false alarms. The system uses shared memory and fast communication between processors to keep data moving quickly, making intrusion detection in vehicles more reliable.

Dennemeyer
The IP Group

Latest patents

US20260030351A1

Threat analysis system and threat analysis method

Company name	Panasonic Automotive Systems Co Ltd
Inventors	Takumaru Nagai, Takashi Tokizaki, Takahiro Yoneda
Priority date	24 Jul 2024
Publication date	29 Jan 2026

Summarized by Dennemeyer

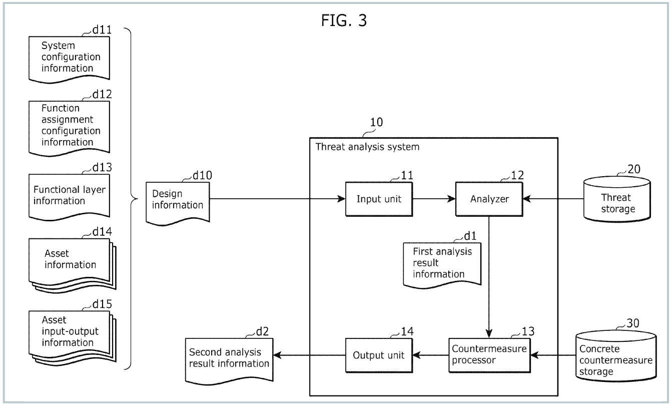


FIG. 3

d11
System configuration information
d12
Function assignment configuration information
d13
Functional layer information
d14
Asset information
d15
Asset input-output information
d10
Design information
10
Threat analysis system
11
Input unit
12
Analyzer
20
Threat storage
d1
First analysis result information
d2
Second analysis result information
14
Output unit
13
Countermeasure processor
30
Concrete countermeasure storage

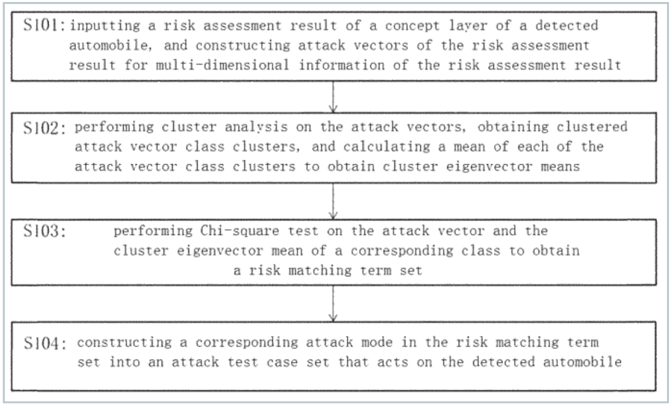
The patent describes a threat-analysis system that takes detailed information on vehicle electronic systems and identifies security threats more clearly by linking high-level management countermeasures with specific actions for each part of the vehicle's software stack. It looks at how components and data flows are arranged, identifies which parts could be attacked, and then produces an output that lists the threats along with practical countermeasures for layers like hardware, operating system, middleware, and applications. A built-in database helps translate general security advice into concrete steps for each layer, so developers know what to implement. The system also avoids repeating the same countermeasures and keeps track of which parts they protect, making cybersecurity planning simpler.

US12517811B2

Method, system and device for generating test case for automotive cybersecurity detection

Company name	Catarc Software Testing Tianjin Co Ltd
Inventors	He Kexun, Li Baotian, Shao Xuebin, Han Yanyan, Qin Yihong, Wang Baizheng, Shao Wen
Priority date	06 Feb 2023
Publication date	06 Jan 2026

Summarized by Dennemeyer



S101: inputting a risk assessment result of a concept layer of a detected automobile, and constructing attack vectors of the risk assessment result for multi-dimensional information of the risk assessment result

S102: performing cluster analysis on the attack vectors, obtaining clustered attack vector class clusters, and calculating a mean of each of the attack vector class clusters to obtain cluster eigenvector means

S103: performing Chi-square test on the attack vector and the cluster eigenvector mean of a corresponding class to obtain a risk matching term set

S104: constructing a corresponding attack mode in the risk matching term set into an attack test case set that acts on the detected automobile

The invention solves the problem that current automotive cybersecurity testing lacks scientific and objective test cases, even though connected cars face rising cyber risks and regulations like UNECE R155 require strong security testing. It does this by automatically creating cybersecurity test cases using risk data from Threat Analysis and Risk Assessment (TARA) reports. It converts hazard impact, attack feasibility, and risk values into attack vectors. These vectors are then grouped, placing similar risks together based on their related vehicle interface. A comparison check is performed to measure how closely each attack matches the typical pattern of its group. This reveals the most similar risks and groups them into a risk-matching set. Each matched attack is then turned into attack paths, producing usable cybersecurity test cases.

Dennemeyer
The IP Group

Latest patents

US2026012478A1

Systems and methods for detecting and mitigating cyber attacks on converter-based energy equipment and associated communication networks

Company name	DER Security Corp
Inventors	Johnson Jay, Kaur Kudrat J, Pineda Alvarado Jorge D
Priority date	01 Jul 2025
Publication date	08 Jan 2026

Summarized by Dennemeyer

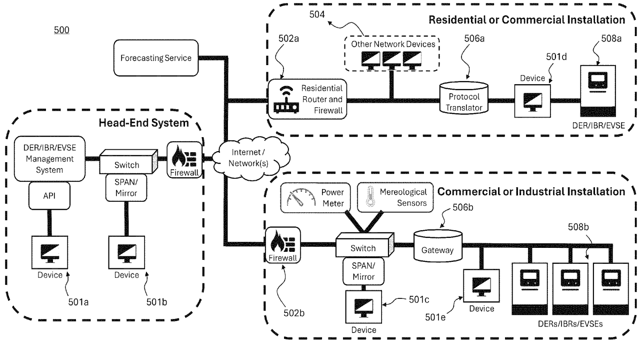


FIG. 5

The patent describes a way to protect electric vehicle charging equipment (EVSE) from cyberattacks by watching both the data being sent and the physical behavior of the charging devices. It checks how the EVSE should behave electrically, compares real activity with a digital-twin model, looks for protocol violations in network traffic, and even uses weather data when needed to judge whether incoming measurements are reasonable. If it finds abnormal patterns that look like an attack, it can undo harmful changes, block suspicious messages at routers or gateways, warn human operators, or change access rights to keep the EVSE running safely within the power grid. By combining protocol checks, physical-operation monitoring, and modeling, it can detect false-data injections or malicious commands.

EP4679304A1

System and method for protecting a system

Company name	Argus Cyber Security Ltd
Inventors	Bari Ephraim Yael, Lavi Oron
Priority date	12 Jul 2024
Publication date	14 Jan 2026

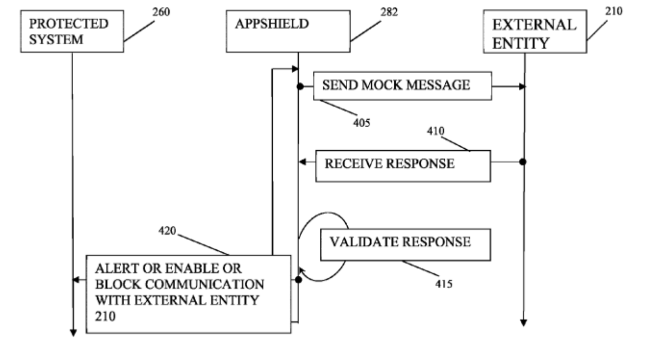


Fig. 4A

The invention addresses the problem that connected vehicles and IoT devices are vulnerable to malware that can intercept or alter messages, while current solutions lack an automatic way to detect such interference. The patent proposes sending mock messages to internal or external components, analyzing the responses, and comparing them with expected results to identify whether communications are being tampered with. It adapts to the device's state, component conditions, and message parameters, and can also use external agents to verify response authenticity. A unit then monitors internal bus traffic and external network messages using stored rules. If it detects unusual changes, it can block communication and alert the user, enabling real-time detection of man-in-the-middle attacks through active verification.

Dennemeyer
The IP Group

Latest patents

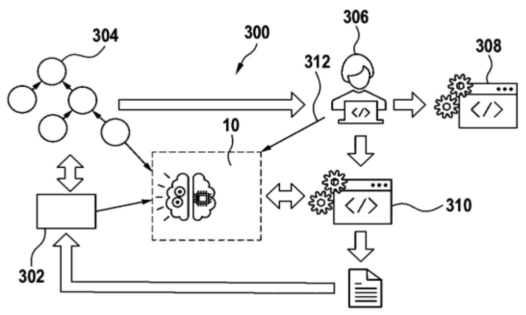
JP2026004228A

Techniques for verifying accuracy and/or generating judgments regarding the risk of cyber attacks on a system

Company name	Robert Bosch Gmbh
Inventors	Christopher Foote, Dominik Germanek, Martin Ring, Max Camilo Eizer, Niklas Iruk
Priority date	07 Jun 2024
Publication date	14 Jan 2026

Summarized by Dennemeyer

Fig. 3



The invention explains that checking cyber-attack risks during development takes a long time and depends on engineers testing things by hand, which can lead to mistakes and less reliable results. To fix this, it uses a machine-learning agent that can automatically create, run, and evaluate cyber-attacks after receiving a request. The agent uses a trained generative model to generate one or more attacks, execute them, and then review the results to confirm or update the system's cyber-risk assessment. It can repeat these tests on prototypes or in simulated setups like software-in-the-loop or hardware-in-the-loop. The system also includes training and setting up the agent so it can fit into normal development workflows, helping reduce costs and improving how well vulnerabilities are detected.

Dennemeyer
The IP Group

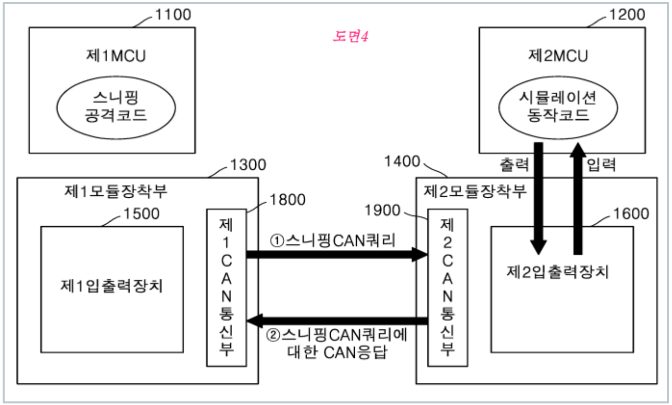
Latest patents

KR20260004809A

Device for providing an interface in which the automobile CAN communication simulation function is implemented

Company name	Konyang Univ Ind Cooperation Group
Inventors	Kim Dong-won
Priority date	02 Jul 2024
Publication date	09 Jan 2026

Summarized by Dennemeyer



This patent describes a hacker-board training device that lets users practice hacking attacks on car communication systems, like the CAN bus, without needing a real vehicle. The device uses two microcontroller units: one acts as the attacker running user-designed hacking code, while the other simulates how car parts would respond. Both units have input and output devices to make the simulation interactive and provide instant feedback. The microcontrollers communicate with each other and can connect to a computer for uploading custom attack or simulation code. The system supports both CAN sniffing and CAN injection and can also simulate other communication attacks using optional modules. This setup allows for hands-on learning, immediate physical feedback, and flexible training scenarios.

CN121283750A

Rail vehicle network security risk detection method, device, equipment and medium

Company name	National High Speed Train Qingdao Technology Innovation Center
Inventors	Jia Dongxiao, Liang Jianying, Liu Shaoqing, Du Jiewei, Tao Dongdong, Liu Weilong
Priority date	23 Oct 2025
Publication date	06 Jan 2026

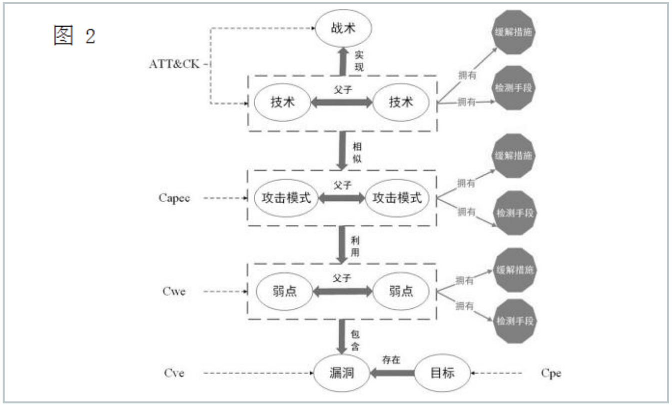


图 2

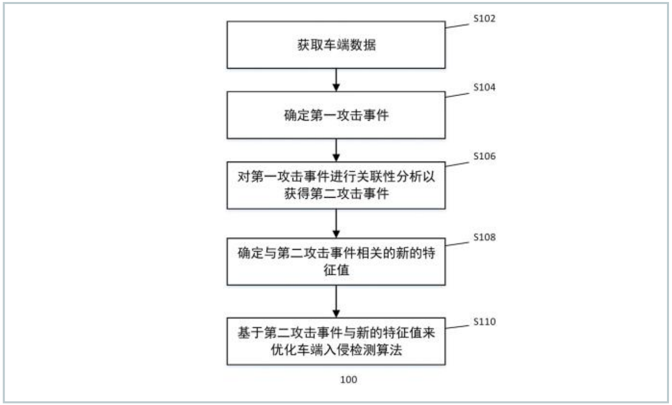
This patent talks about automatically finding and evaluating security risks in railway network systems. It does this by building a detailed knowledge graph that combines information about threats, the network layout, and user behavior. Using this graph, it examines each network device, creates attack graphs that show possible ways a hacker could move through the network, and calculates risk scores. It also connects real attack events to these paths to support deeper analysis and suggests fixes based on the scores. It uses data modeling and AI to pull useful information from logs and databases. Attack graphs are created by checking vulnerabilities and using algorithms to find the most dangerous paths. It also groups alarms to show how an attack progresses over time, allowing the system to automatically build attack paths and give a clearer picture of how attacks happen.

CN121283680A

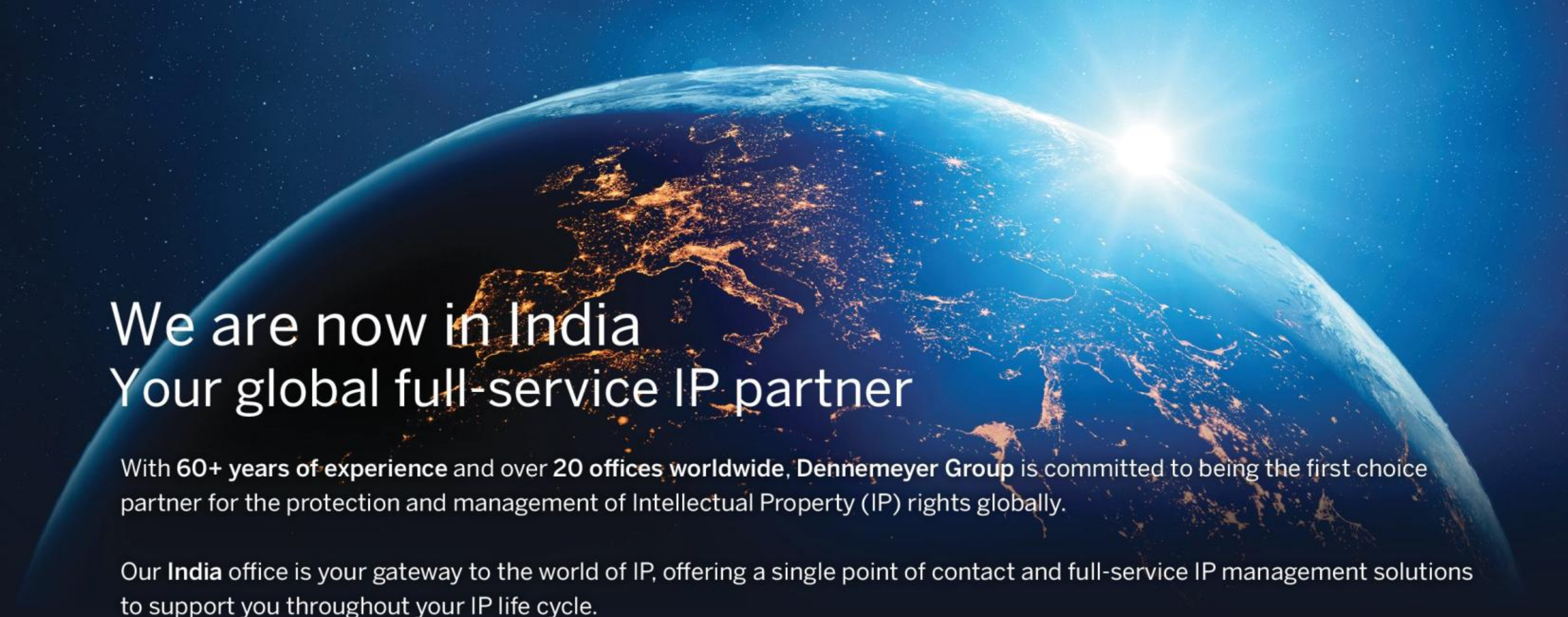
Method, system, medium and product for improving vehicle end intrusion detection function

Company name	SAIC General Motors Corp Ltd, Pan Asia Technical Automotive Center Co Ltd
Inventors	Zhang Jiaqi, Zhou Jingtian, Bi Xiaodong, Feng Haitao, Wei Shangqing
Priority date	17 Sep 2025
Publication date	06 Jan 2026

Summarized by Dennemeyer


获取车端数据
S102
确定第一攻击事件
S104
对第一攻击事件进行关联性分析以获得第二攻击事件
S106
确定与第二攻击事件相关的新的特征值
S108
基于第二攻击事件与新的特征值来优化车端入侵检测算法
S110
100

The invention solves the problem that connected vehicles face growing cyberattacks as pre-installed intrusion detection systems cannot keep up with new threats during real-world use. It continuously improves detection by learning from abnormal data collected from vehicles, identifying known attacks using stored indicators, and performing correlation analysis to uncover related but previously unknown attacks along the same attack path. It extracts new features from these findings, updates the database, and uses this data to refine the detection algorithm, which is then sent back to vehicles as an update. It combines unsupervised learning to separate normal and suspicious data with supervised learning to classify anomalies, uses attack patterns tailored to each vehicle setup, and builds multi-step attack paths to reveal hidden intermediate attacks that traditional systems miss.



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

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.