Dennemeyer
The IP Group

Report of January 2026

Cybersecurity in mobility

Recent developments

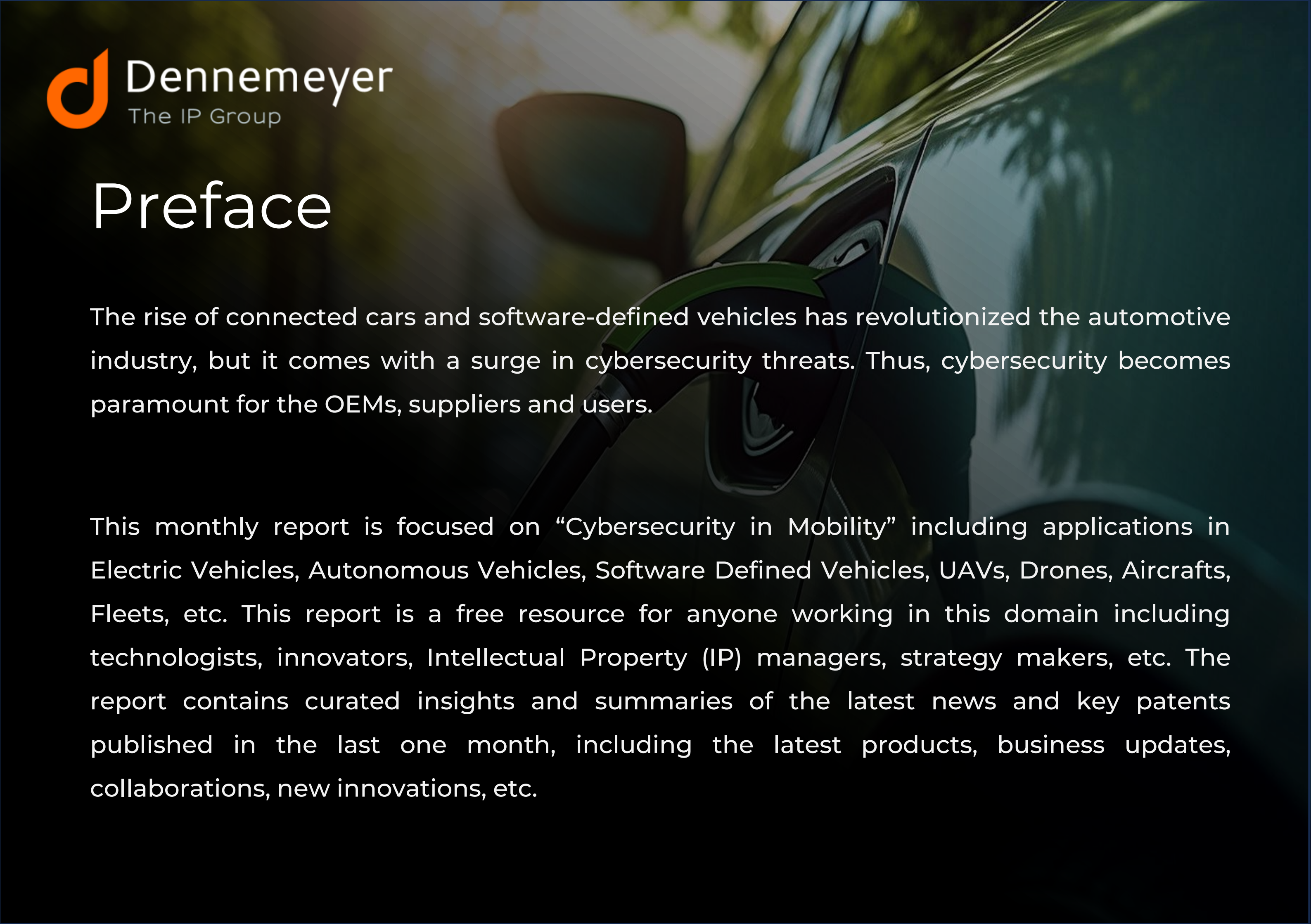
Curated and summarized - Industry and Patent news

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

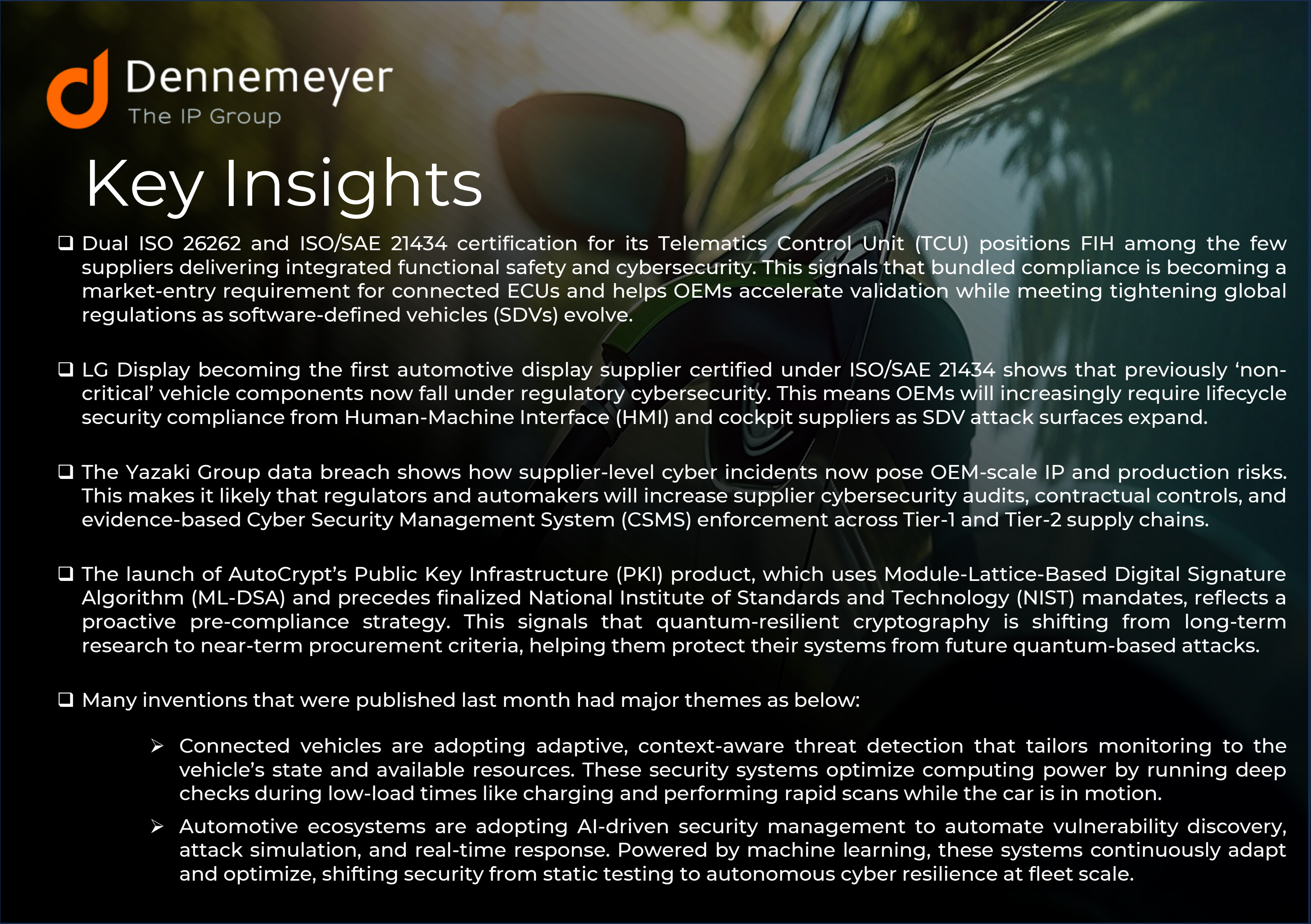
Scan the QR code to receive this monthly report via email in your inbox.



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.



Key Insights

- Dual ISO 26262 and ISO/SAE 21434 certification for its Telematics Control Unit (TCU) positions FIH among the few suppliers delivering integrated functional safety and cybersecurity. This signals that bundled compliance is becoming a market-entry requirement for connected ECUs and helps OEMs accelerate validation while meeting tightening global regulations as software-defined vehicles (SDVs) evolve.

- LG Display becoming the first automotive display supplier certified under ISO/SAE 21434 shows that previously 'non-critical' vehicle components now fall under regulatory cybersecurity. This means OEMs will increasingly require lifecycle security compliance from Human-Machine Interface (HMI) and cockpit suppliers as SDV attack surfaces expand.

- The Yazaki Group data breach shows how supplier-level cyber incidents now pose OEM-scale IP and production risks. This makes it likely that regulators and automakers will increase supplier cybersecurity audits, contractual controls, and evidence-based Cyber Security Management System (CSMS) enforcement across Tier-1 and Tier-2 supply chains.

- The launch of AutoCrypt's Public Key Infrastructure (PKI) product, which uses Module-Lattice-Based Digital Signature Algorithm (ML-DSA) and precedes finalized National Institute of Standards and Technology (NIST) mandates, reflects a proactive pre-compliance strategy. This signals that quantum-resilient cryptography is shifting from long-term research to near-term procurement criteria, helping them protect their systems from future quantum-based attacks.

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

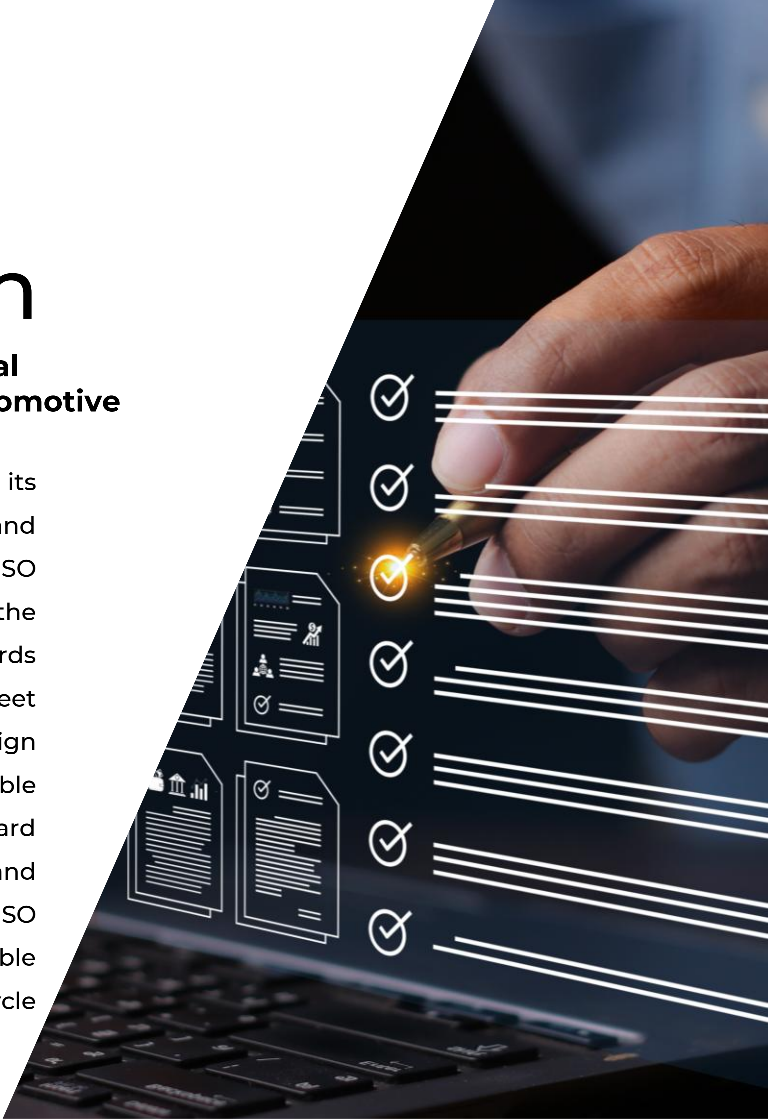
    - Connected vehicles are adopting adaptive, context-aware threat detection that tailors monitoring to the vehicle's state and available resources. These security systems optimize computing power by running deep checks during low-load times like charging and performing rapid scans while the car is in motion.
    - Automotive ecosystems are adopting AI-driven security management to automate vulnerability discovery, attack simulation, and real-time response. Powered by machine learning, these systems continuously adapt and optimize, shifting security from static testing to autonomous cyber resilience at fleet scale.

Dual Certification

FIH achieves ISO 26262 and ISO/SAE 21434 dual certifications from DEKRA, strengthening automotive safety and cybersecurity capabilities

FIH, a subsidiary of Foxconn, has announced that its Telematics Control Unit (TCU) has passed DEKRA testing and earned both ISO 26262 functional safety certification and ISO SAE 21434 cybersecurity certification, placing it among the few TCU makers to achieve both at once. These standards help customers reduce risks, speed up validation, and meet stricter global rules. FIH's strong ICT expertise and its design and manufacturing strengths support secure and reliable solutions for carmakers. As the auto industry moves toward electrification and software driven vehicles, safety and cybersecurity have become essential requirements. ISO 26262 ensures that vehicle electronics remain controllable during faults, while ISO SAE 21434 guides full lifecycle cybersecurity.

Source
https://www.fihmobile.com/



OLED Display Security

LG display becomes first in display industry to obtain automotive cybersecurity certification

LG announced that it has become the first automotive display manufacturer to receive the ISO SAE 21434 cybersecurity certificate for its latest Automotive OLED displays. These products will enter mass production next year. This achievement reinforces the company's leadership as cars continue to shift toward software driven designs. The global ISO SAE 21434 standard evaluates whether companies can manage cybersecurity risks throughout the entire lifecycle of a product. LG earned the certification by designing displays that can resist hacking from the development stage and by adding stronger circuit level security during production. These efforts are expected to strengthen the company's competitiveness in global bids, as securing automotive displays is crucial because they connect the vehicle's software systems with the driver.

Source
https://news.lgdisplay.com/

AutoCrypt's PKI Product

AutoCrypt announces product release of Post-Quantum PKI product, pioneering PQC-enabled solutions for automotive OEMs

AutoCrypt has launched AutoCrypt Public Key Infrastructure (PKI) Vehicles, a new security system that uses Module-Lattice-Based Digital Signature Algorithm (ML-DSA), which is a post quantum digital signature designed to stay secure even against future quantum computers. With this launch, the company becomes one of the first to offer ML-DSA based PKI for automotive systems and carmaker environments. The timing is important because industries around the world are preparing for new NIST rules on post quantum cryptography and growing cyber risks from quantum technology. ML-DSA was chosen by NIST in 2024 as part of the FIPS 204 digital signature standard, which is expected to become a global requirement. AutoCrypt says the new system will help automakers move to quantum safe security without needing to change their existing systems.

Source
https://autocrypt.io/

Automotive Testing

Geely opens world's largest vehicle testing centre

Geely Auto Group has opened the world's largest and most advanced automotive safety testing facility in Ningbo, China. Spanning over 45,000 square meters, it can test everything from high speed crashes and pedestrian protection to battery safety, cybersecurity, and health based safety checks for intelligent vehicles. The centre includes CNAS level cybersecurity testing that examines chips, firmware, data transfer, encryption, OTA updates, sensors, and controllers. It also evaluates harmful gases and odors through a special Golden Nose team to ensure vehicle interiors meet strict health standards. The facility has set five world records and combines global best practices with its own R and D strengths to exceed regulatory safety requirements. It also works with institutions like CATARC and Tsinghua University to advance safety research.

Source
https://global.geely.com/

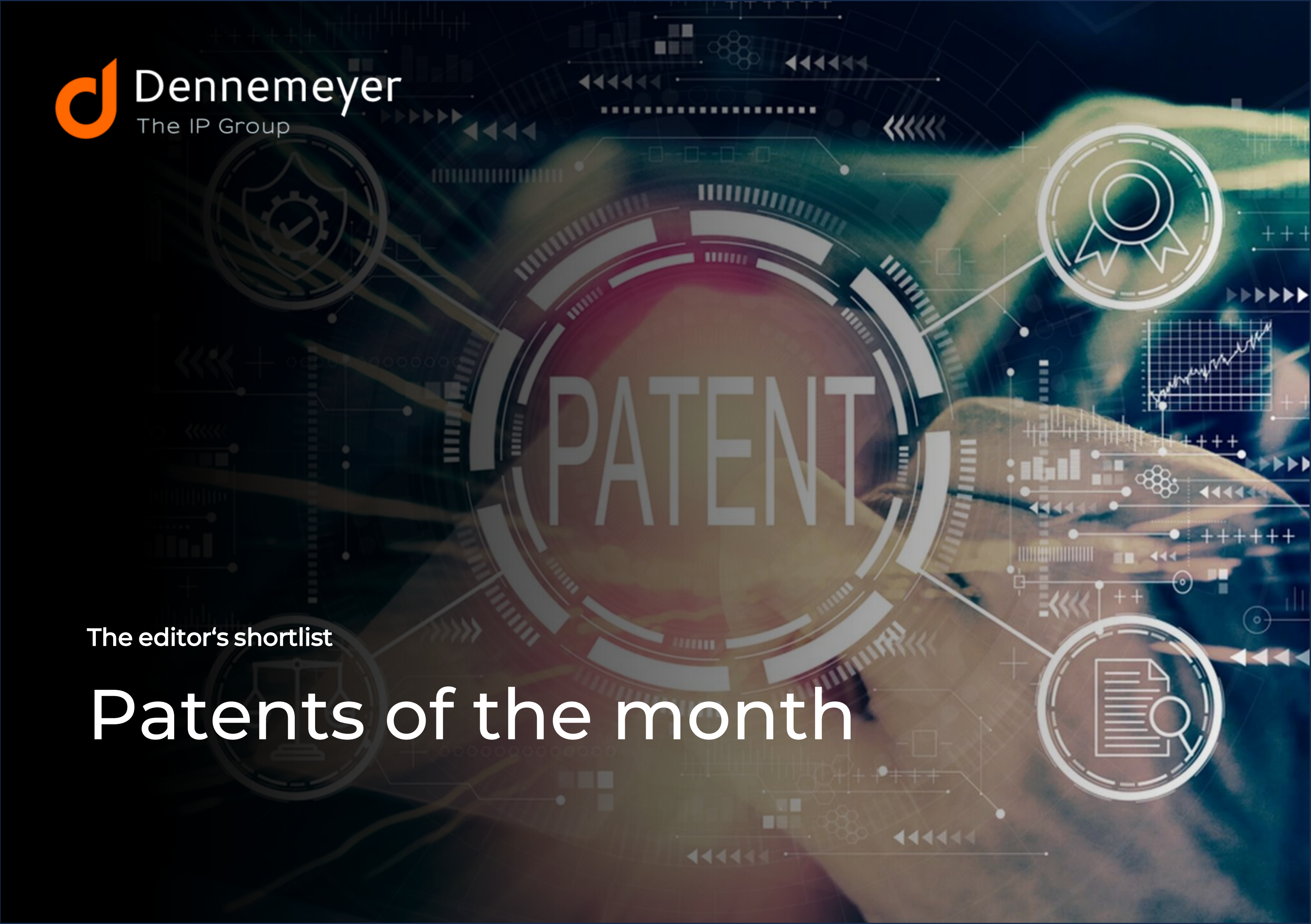
Data Breach

INC ransom claims attack on major automotive supplier Yazaki group, potentially impacting BMW, Nissan

The INC Ransom hacking group has claimed a cyberattack on Japan based automotive supplier Yazaki Group, saying they stole about 350 GB of confidential data. The attackers allege they took corporate documents, client information, NDAs, financial records, operational data, and even HR files containing employee medical details. They also claim to have obtained technical drawings, business agreements, and production documents linked to major automakers such as BMW, Nissan, and Scania. If true, this could expose sensitive intellectual property and disrupt supply chain security. The breach has not yet been verified but represents a serious risk to Yazaki and its global clients. This incident follows other recent automotive sector cyber events, including a Nissan Creative Box breach and a vulnerability that exposed remote car unlocking at 1,000 dealerships.

Source
https://www.technadu.com/

Dennemeyer
The IP Group



The editor's shortlist

Patents of the month

Dennemeyer
The IP Group

Patents of the month

Published in December 2025

Shortlisted and summarized by our analyst

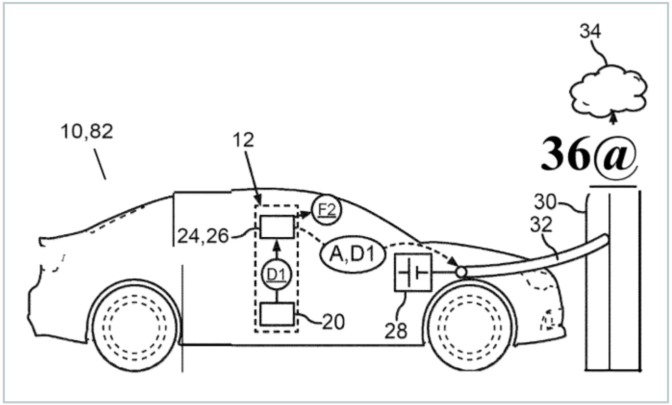
- US2025378160A1 - Method for monitoring data traffic of a motor vehicle and motor vehicle having an attack detection system
  Assignee: Audi AG
- US12513128B2 - In-vehicle network OTA security communication method and apparatus, vehicle-mounted system, and storage medium
  Assignee: Chengdu Kawa Technology Co Ltd
- US2025385933A1 - Cybersecurity for resource sharing among internet of things devices
  Assignee: GM Global Technology Operations LLC
- US12506766B2 - Method for evaluating security of in-vehicle network
  Assignee: Ahope Ltd
- US12505221B2 - Secure automotive system
  Assignee: Continental Automotive Technology GMBH
- EP4145765B1 - Method for protection from cyber attacks to a vehicle based upon time analysis, and corresponding device
  Assignee: Marelli Europe Spa
- EP4655962A1 - Method for detecting attack for vehicle and related device
  Assignee: Huawei Technology Co Ltd, Univ Hong Kong Science & Technology
- KR20250175287A - Techniques for determining correctness and/or generating an assessment of the risk of cyberattacks on a system
  Assignee: Robert Bosch GMBH
- IN575302A1 - System to enhance cybersecurity during charging of an electric vehicle
  Assignee: Matter Motor Works Pvt Ltd
- CN120354414B - Vulnerability testing method and device of vehicle-mounted system, electronic equipment and storage medium
  Assignee: Catarc Automotive Test Center Tianjin Co Ltd

US2025378160A1

Method for monitoring data traffic of a motor vehicle and motor vehicle having an attack detection system

Company name	Audi AG
Inventors	Corbett Christopher, Oelker Martin, Schmidt Karsten
Priority date	29 Jun 2022
Publication date	11 Dec 2025

Summarized by Dennemeyer



The patent describes a system that helps EVs detect cyberattacks effectively by analyzing network traffic when the vehicle is stationary. While driving, the vehicle lacks sufficient computing power to inspect all data, so it only records part of the traffic and performs basic intrusion checks on a smaller portion. Later, when the vehicle is stationary and charging, the stored data from the driving phase can be analyzed in detail without requiring additional onboard hardware. If the basic intrusion detection system spots something suspicious, or when the vehicle enters the charging state, data recording stops and a deeper investigation begins. If any abnormalities are found, relevant data can be securely uploaded through the internet connection available at the charging station.

US12513128B2

In-vehicle network OTA security communication method and apparatus, vehicle-mounted system, and storage medium

Company name	Chengdu Kawa Technology Co Ltd
Inventors	Chen Xi, Zheng Xuming, Wu Yongbo, Shuang Jianping
Priority date	18 Nov 2021
Publication date	30 Dec 2025

Summarized by Dennemeyer

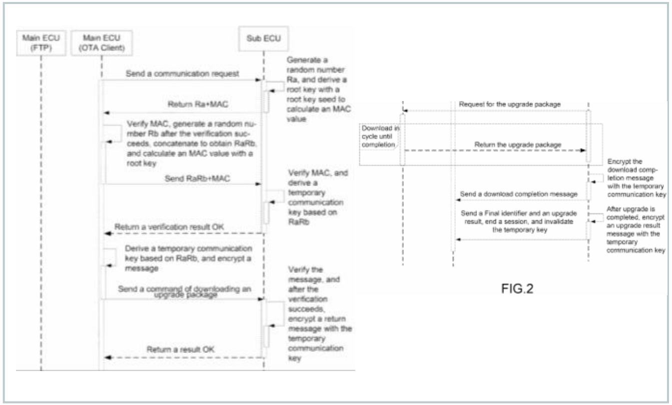

Main ECU (FTP)
Main ECU (OTA Client)
Sub ECU
Send a communication request
Generate a random number Ra, and derive a root key with a root key seed to calculate an MAC value
Return Ra+MAC
Verify MAC, generate a random number Rb after the verification succeeds, concatenate to obtain RaRb, and calculate an MAC value with a root key
Send RaRb+MAC
Verify MAC, and derive a temporary communication key based on RaRb
Return a verification result OK
Derive a temporary communication key based on RaRb, and encrypt a message
Send a command of downloading an upgrade package
Verify the message, and after the verification succeeds, encrypt a return message with the temporary communication key
Return a result OK
Request for the upgrade package
Download in cycle until completion
Return the upgrade package
Encrypt the download completion message with the temporary communication key
Send a download completion message
After upgrade is completed, encrypt an upgrade result message with the temporary communication key
Send a Final identifier and an upgrade result, end a session, and invalidate the temporary key

FIG.2

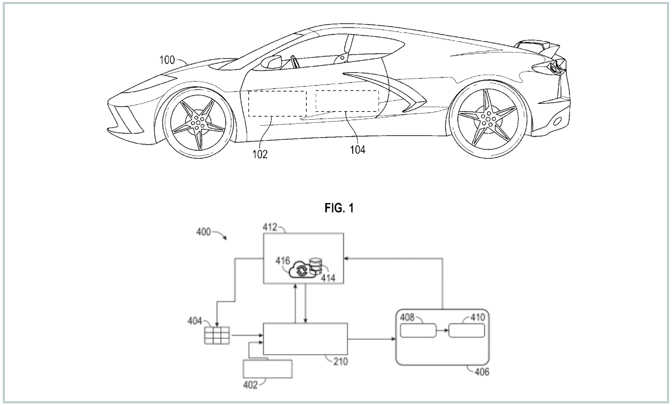
The patent introduces a way to perform over-the-air (OTA) updates in a vehicle's network to prevent cyberattacks during ECU software upgrades. Current OTA systems lack proper authentication, making it easy to tamper with update packages. The solution uses a main processor and sub-processors with preset root keys to create secure sessions. First, the sub-processor sends a random number and a check code (MAC values generated with secure algorithms) based on the root key. After verification, the main processor sends back another random number combined with the first one and a new check code. Once verified, a temporary key is created for encrypted data transfer. The update package is then sent securely using this key. After the update, the session ends and the temporary key is deleted. Each update uses a fresh key.

US2025385933A1

Cybersecurity for resource sharing among internet of things devices

Company name	GM Global Technology Operations LLC
Inventors	Adiththan Arun, Giusto Paolo, Vemuri Venkata Naga Siva Vikas, Layouni Mohamed A
Priority date	14 Jun 2024
Publication date	18 Dec 2025

Summarized by Dennemeyer

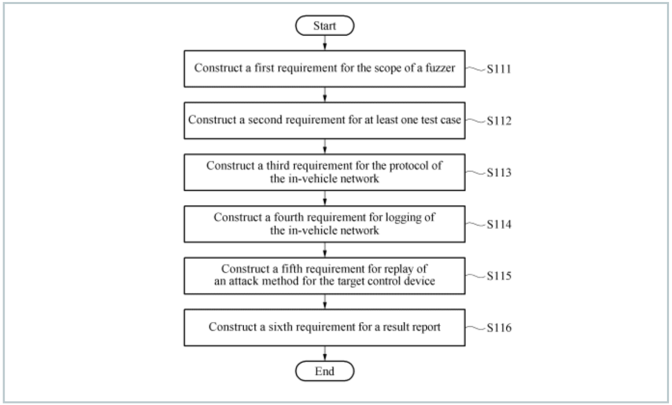


The patent improves cybersecurity for IoT devices in vehicles by addressing both known and emerging threats during resource sharing. Current methods rely on static threat matrices that fail to handle unknown risks or adapt dynamically. The solution analyzes data from IoT devices to detect potential threats and checks them against an existing security matrix. If a threat is new, the system uses large language models trained on global knowledge to find relevant information and mitigation strategies. This updated data is added to the security matrix in real time. For known threats, predefined actions are applied, while for new threats, suggested strategies are deployed. A smart optimizer ensures these actions do not overload system resources such as memory, bandwidth, or processing power. The approach supports continuous learning and adaptation for evolving risks.

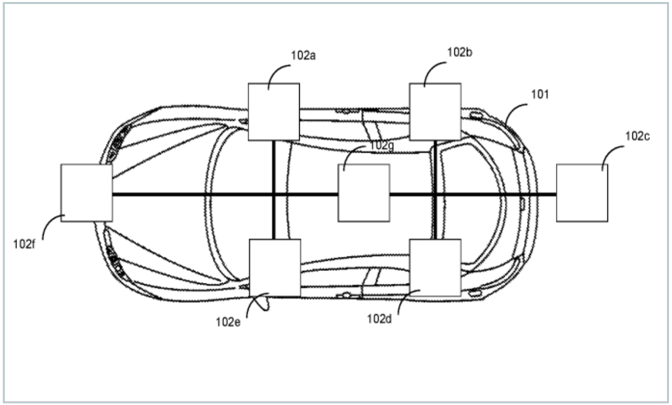
US12506766B2

Method for evaluating security of in-vehicle network

Company name	Ahope Ltd
Inventors	Jo Sangwon, Kim Yeonwoo
Priority date	14 Nov 2023
Publication date	23 Dec 2025


Start
Construct a first requirement for the scope of a fuzzer
S111
Construct a second requirement for at least one test case
S112
Construct a third requirement for the protocol of the in-vehicle network
S113
Construct a fourth requirement for logging of the in-vehicle network
S114
Construct a fifth requirement for replay of an attack method for the target control device
S115
Construct a sixth requirement for a result report
S116
End

The patent evaluates the security of in-vehicle networks such as CAN, CAN-FD, or Ethernet using a fuzzing-based testing framework. Modern vehicles rely on frequent ECU updates, which increases their vulnerability to cyberattacks. The solution builds a fuzzing framework that defines scope, protocol support, logging, replay attack capability, and reporting. It extracts message lists from CAN database files and generates test cases using various fuzzing algorithms. These test cases are injected into target control devices, and the system monitors responses for abnormalities. If issues are detected, further tests are triggered, and devices can be restarted or replayed for deeper analysis. This structured approach ensures comprehensive vulnerability detection while minimizing false positives.



❮ US12505221B2

Secure automotive system

Company name	Continental Automotive Technology GMBH
Inventors	Velivela Ramasubbarao
Priority date	23 Dec 2021
Publication date	23 Dec 2025

Summarized by Dennemeyer

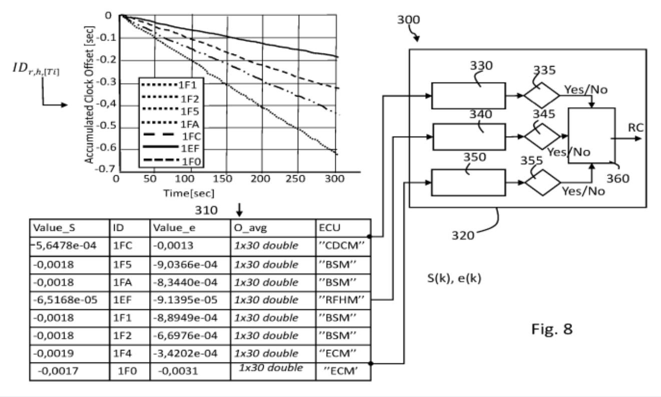
The patent talks about securing automotive ECUs against cyberattacks by verifying their integrity during each boot cycle. Modern vehicles rely on ECUs for critical functions, making them vulnerable to threats. The solution calculates cryptographic values called Message Authentication Codes (MACs) for one or more ECU modules. These values are compared with stored MACs created during manufacturing. If they match, the ECU operates normally; if not, the system responds based on the ECU's Cybersecurity Assurance Level (CAL). High-assurance ECUs shut down immediately, while lower levels allow limited operation before shutdown. Secure external access uses Public Key Infrastructure (PKI) with challenge response authentication involving device signatures. This layered approach ensures tamper detection and prevents unauthorized updates.

EP4145765B1

Method for protection from cyber attacks to a vehicle based upon time analysis, and corresponding device

Company name	Marelli Europe Spa
Inventors	Rosadini Christian, Chiarelli Simona, Nesci Walter, Saponara Sergio, Gagliardi Alessio, Dini Pierpaolo
Priority date	06 Sep 2021
Publication date	10 Dec 2025

Summarized by Dennemeyer



Value_S	ID	Value_e	O_avg	ECU
-5,6478e-04	1FC	-0,0013	*1x30 double*	''CDCM''
-0,0018	1F5	-9,0366e-04	*1x30 double*	''BSM''
-0,0018	1FA	-8,3440e-04	*1x30 double*	''BSM''
-6,5168e-05	1EF	-9.1395e-05	*1x30 double*	''RFHM''
-0,0018	1F1	-8,8949e-04	*1x30 double*	''BSM''
-0,0018	1F2	-6,6976e-04	*1x30 double*	''BSM''
-0,0019	1F4	-3,4202e-04	*1x30 double*	''ECM''
-0,0017	1F0	-0,0031	*1x30 double*	''ECM'

Fig. 8

The patent talks about a method for identifying which ECU sends messages on a vehicle's CAN bus, addressing the issue that CAN lacks MAC addresses for source tracing. Current systems can detect attacks but cannot pinpoint their origin, making it difficult to stop threats. The invention studies the timing of regular messages between nodes. It groups messages by how often they are sent, calculates average clock differences, and uses a formula to find patterns unique to each ECU. A check is then done to make sure messages from the same node match. The results classify messages and detect anomalies or attacks. This creates a "virtual MAC" by fingerprinting ECUs based on their clock drift. The system can be integrated into existing nodes or added separately to monitor subnetworks.

EP4655962A1

Method for detecting attack for vehicle and related device

Company name	Huawei Technology Co Ltd, Univ Hong Kong Science & Technology
Inventors	Revadigar Girish, Yang Tianci, Yang Nachuan, Yan Yamin, Shi Ling
Priority date	14 Feb 2023
Publication date	26 Aug 2025

Summarized by Dennemeyer

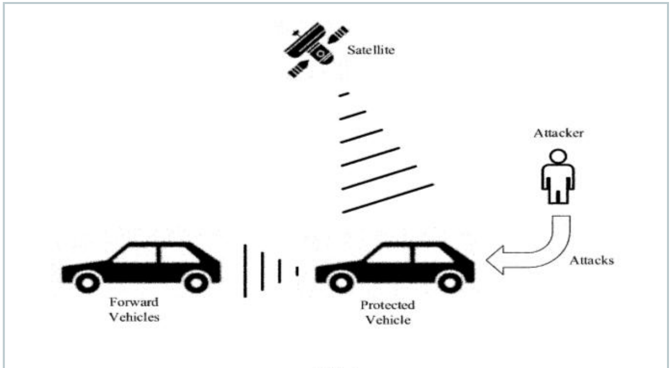


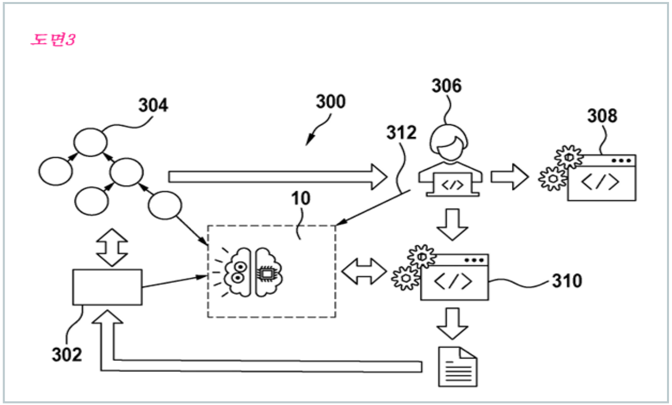
FIG. 1

The patent detects cyberattacks on vehicles using only the vehicle's own sensor and control data, without relying on external sources. Modern cars depend heavily on software and hardware for critical functions, making them vulnerable to malware or sensor manipulation that could cause accidents. The solution predicts sensor readings for the next moment using previously corrected data and control commands such as braking or acceleration by applying estimation techniques. It then compares these predictions with actual sensor observations and uses statistical tests to analyze differences over time to determine if an attack is occurring, reducing false alarms from short-term anomalies. The system operates autonomously inside the vehicle and supports multiple sensors, including speedometers, cameras, radar, and GNSS modules.

KR20250175287A

Techniques for determining correctness and/or generating an assessment of the risk of cyberattacks on a system

Company name	Robert Bosch GMBH
Inventors	Christopher Hoot, Dominic Germanic, Martin Ring Max Camillo Eisele, Niklas Ilke
Priority date	05 Jun 2025
Publication date	16 Dec 2025

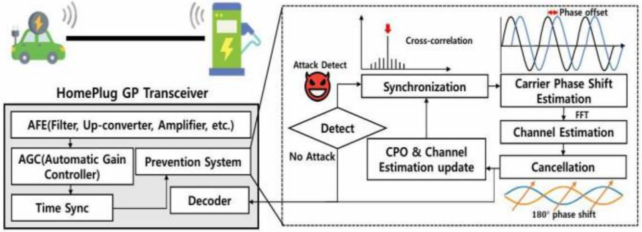


The patent verifies or generates an assessment of cyberattack risks on a specific system using machine learning (ML) automation. Traditional risk assessments are slow and often manual, requiring significant time and resources. The solution uses an ML agent connected to a generative ML model trained to create datasets and simulate attacks. When a query requests testing, the agent generates and executes one or more cyberattacks on the system. It then evaluates the results to determine if vulnerabilities exist and whether a prior risk assessment was accurate. If no prior assessment exists, the system generates a new risk score based on the attack outcomes. This process can run in a test or development environment and is fully automated, reducing execution time from hours or days to minutes.

IN575302A1

System to enhance cybersecurity during charging of an electric vehicle

Company name	Matter Motor Works Pvt Ltd
Inventors	Kumar Prasad Telikepalli, Ramachandran R, Pankaj Kumar Bharti
Priority date	31 Mar 2024
Publication date	05 Dec 2025



도면4

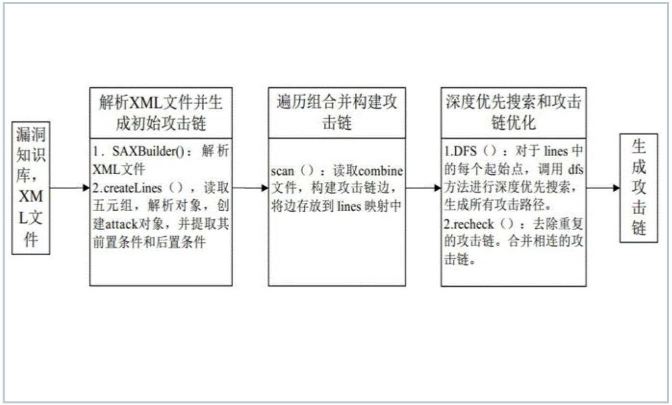
The patent improves cybersecurity during EV charging by verifying software integrity in real time. Modern EVs communicate with charging stations for power transfer and billing, but this creates risks such as malware injection and spoofing attacks. The solution uses a security unit in the vehicle to check software during charging. It generates a hash value for the software and compares it with a reference hash stored in a secure remote system. If the values differ, the system issues an alert and identifies the compromised charging station. The system also validates software certificates of charging stations and can revoke them if an attack is detected. Alerts are sent to fleet servers and may trigger geofencing to block access to risky stations. AI-based anomaly detection predicts threats before compromise, and alerts are secured using blockchain to prevent tampering.

CN120354414B

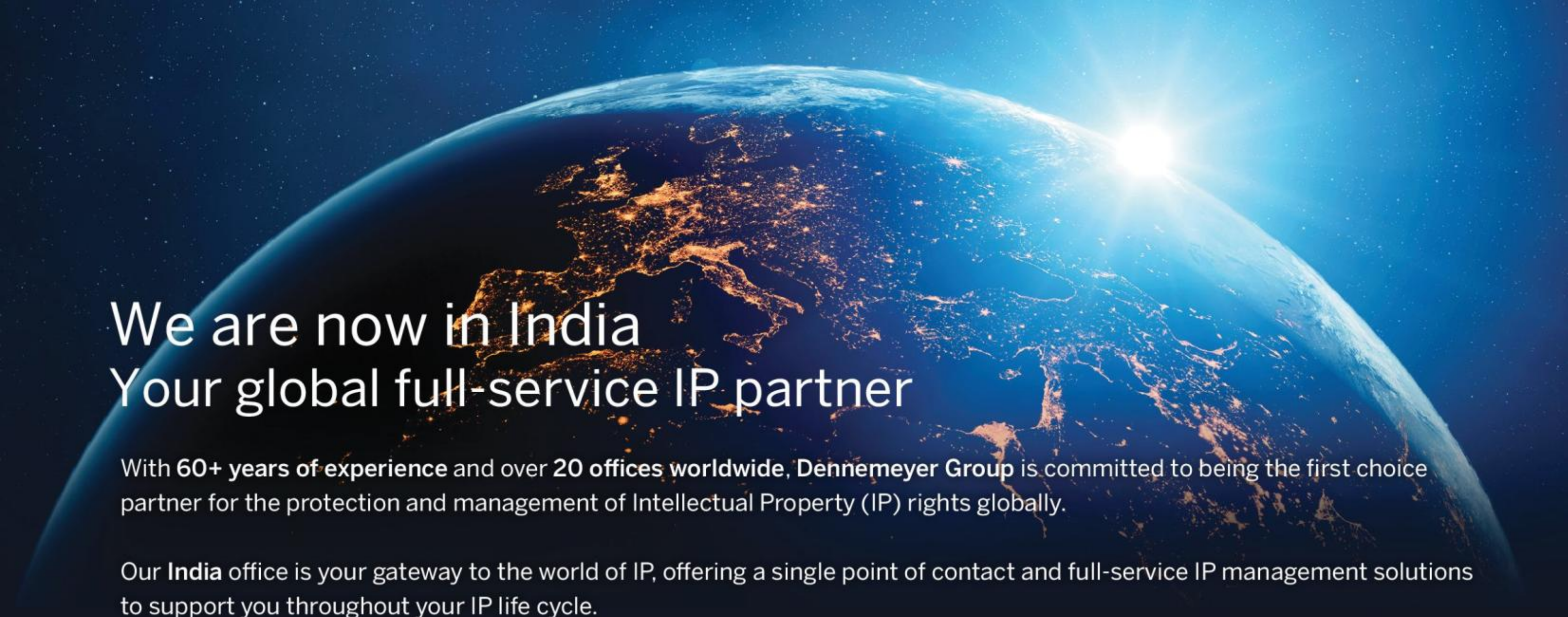
Vulnerability testing method and device of vehicle-mounted system, electronic equipment and storage medium

Company name	Catarc Automotive Test Center Tianjin Co Ltd
Inventors	Zhao Xiong, He Kexun, Qin Yihong, Zou Bowei, Fang Xiyu, Zhang Juan, Wang Ziyi, Zhang Jinchao
Priority date	09 Apr 2025
Publication date	09 Dec 2025

Summarized by Dennemeyer


漏洞知识库，XML文件
解析XML文件并生成初始攻击链
1．SAXBuilder()：解析XML文件
2.createLines（），读取五元组，解析对象，创建attack对象，并提取其前置条件和后置条件
遍历组合并构建攻击链
scan（）：读取combine文件，构建攻击链边，将边存放到lines映射中
深度优先搜索和攻击链优化
1.DFS（）：对于 lines 中的每个起始点，调用 dfs 方法进行深度优先搜索，生成所有攻击路径。
2.recheck（）：去除重复的攻击链。合并相连的攻击链。
生成攻击链

The patent discusses vulnerability testing in vehicle-mounted systems within Internet of Vehicles environments. Current methods combine all factors blindly, creating huge sample spaces and wasting time. The invention analyzes a vulnerability database to group vulnerabilities by category and count their occurrences. Using a preset coverage policy, it selects specific categories as target parameters instead of testing all combinations. Initial cross-category test cases are generated and expanded horizontally or vertically until coverage goals are met. Next, an attack chain graph is built using associations among vulnerabilities, and depth-first search is applied to generate possible attack paths. These paths are then deduplicated and logically merged to form an optimized set for testing, thereby reducing test cases and improving efficiency.



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.