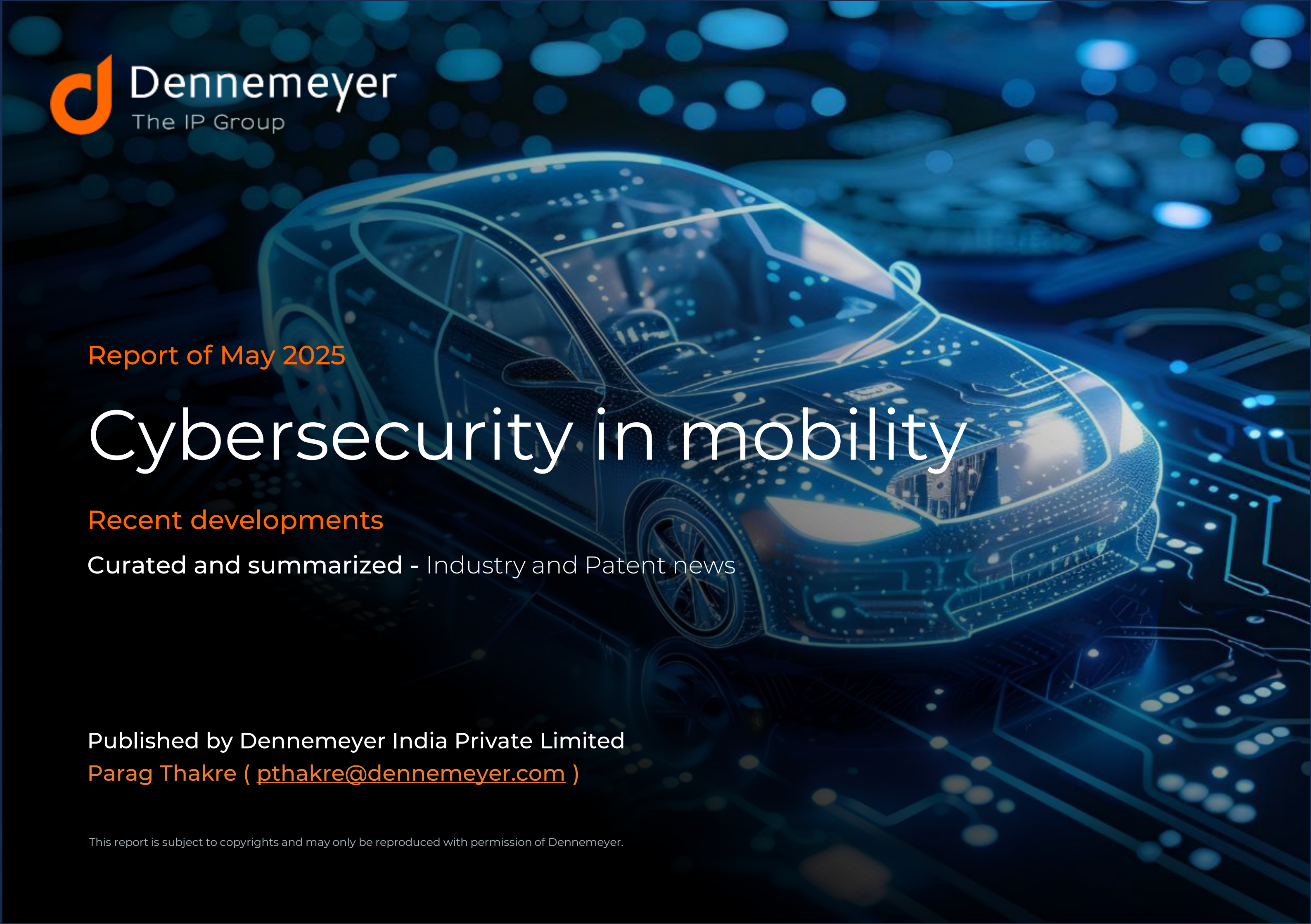


Dennemeyer
The IP Group

Report of May 2025

Cybersecurity in mobility

Recent developments

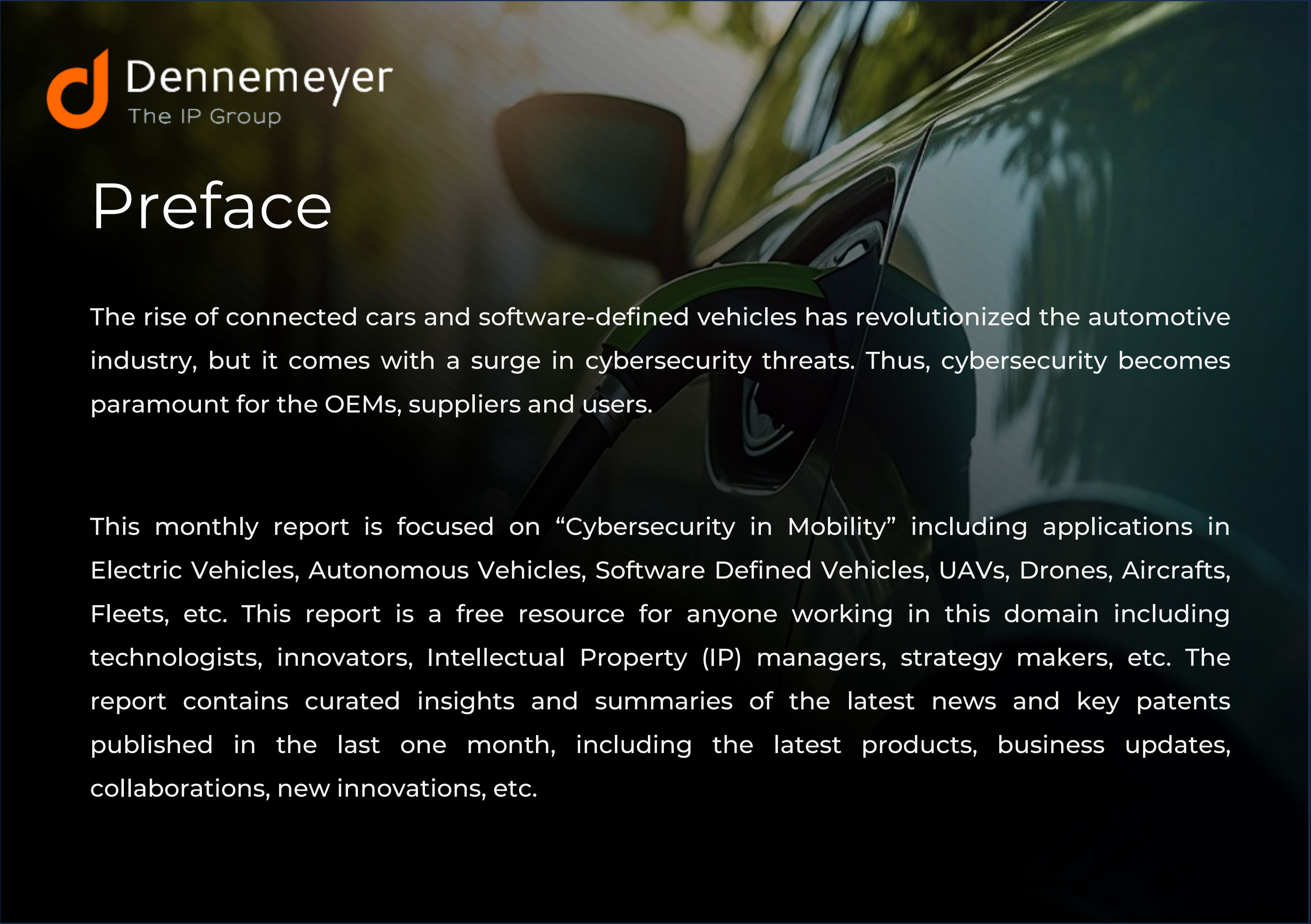
Curated and summarized - Industry and Patent news

Published by Dennemeyer India Private Limited
Parag Thakre (pthakre@dennemeyer.com)

Dennemeyer
The IP Group

Subscribe now

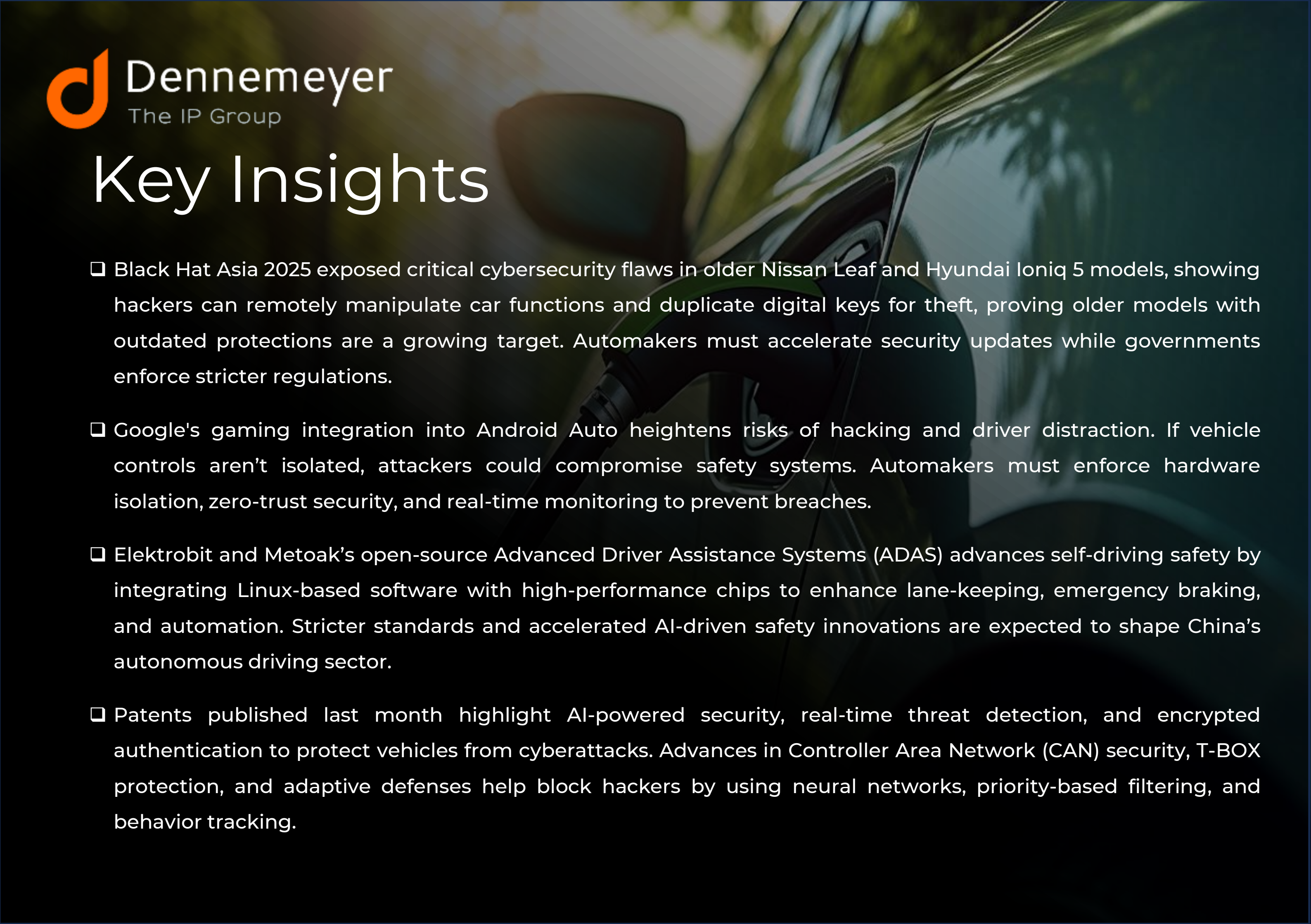
Scan the QR code to receive this monthly report via email in your inbox.



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

- ❑ Black Hat Asia 2025 exposed critical cybersecurity flaws in older Nissan Leaf and Hyundai Ioniq 5 models, showing hackers can remotely manipulate car functions and duplicate digital keys for theft, proving older models with outdated protections are a growing target. Automakers must accelerate security updates while governments enforce stricter regulations.

- ❑ Google's gaming integration into Android Auto heightens risks of hacking and driver distraction. If vehicle controls aren't isolated, attackers could compromise safety systems. Automakers must enforce hardware isolation, zero-trust security, and real-time monitoring to prevent breaches.

- ❑ Elektrobit and Metoak's open-source Advanced Driver Assistance Systems (ADAS) advances self-driving safety by integrating Linux-based software with high-performance chips to enhance lane-keeping, emergency braking, and automation. Stricter standards and accelerated AI-driven safety innovations are expected to shape China's autonomous driving sector.

- ❑ Patents published last month highlight AI-powered security, real-time threat detection, and encrypted authentication to protect vehicles from cyberattacks. Advances in Controller Area Network (CAN) security, T-BOX protection, and adaptive defenses help block hackers by using neural networks, priority-based filtering, and behavior tracking.

Remote Car Hacking

Nissan Leaf Vulnerability Exploited to Gain Control Over the Car Remotely

Researchers have discovered security flaws in second-generation Nissan Leaf EVs that allow hackers to take control of key functions remotely, such as unlocking doors, adjusting mirrors, and even interfering with the car's steering. The attack, demonstrated at Black Hat Asia 2025, starts with a weakness in the car's Bluetooth system. Hackers can take advantage of this by sending a harmful audio signal that tricks the system. Once they gain access to the car's network, they can disable security features, bypass protections, and take full control of various functions like opening windows, disabling locks, and interfering with the steering. Nissan was informed of the issue in 2023 but took time to develop fixes, promising dealership updates by late 2025.

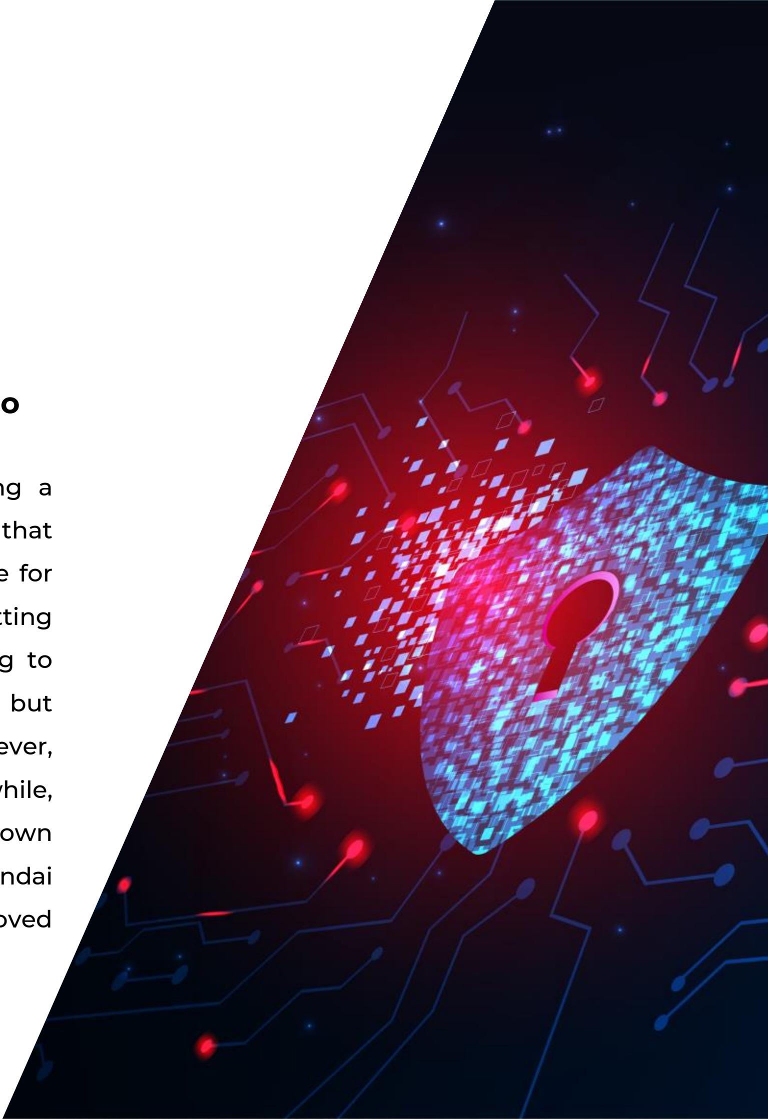
Source
https://cybersecuritynews.com/

Hacked under 20 seconds

Hyundai Car Stolen in Under 20 Seconds Due to Security Flaw

A security camera captured footage of a thief stealing a Hyundai Ioniq 5 in less than 20 seconds using a device that copies the car's digital key. This tool, which is sold online for $16,000, can save and duplicate the car's signal, letting criminals unlock and start keyless cars without needing to physically break in. Hyundai admits the problem exists but says it's something the whole auto industry faces. However, the company has not recalled affected vehicles. Meanwhile, the UK government is working on stricter laws to crack down on those selling or using devices that help steal cars. Hyundai assures that models from 2024 and beyond have improved security, but older cars remain vulnerable.

Source
https://www.watanserb.com/



Google’s In-Car Gaming

Playing Android games in cars? Your vehicle might get hacked

Google’s plan to bring gaming to cars through Android Auto has raised concerns about safety and security. Experts warn that these games could distract drivers and expose vehicles to hacking. If gaming systems aren’t fully isolated from critical functions like steering and braking, hackers could potentially take control. Additionally, they require internet connectivity, which further increases risks, making cars vulnerable to data theft, remote attacks, and expanding the attack surface. Researchers have previously hacked vehicles through onboard entertainment systems, highlighting security flaws in connected cars. Google states that gaming will only work when the car is parked. But critics argue that this doesn’t fully address cybersecurity concerns and stronger security measures are required.

Source
https://www.newsbytesapp.com/

Partnership

Elektrobit and Metoak forge strategic partnership to establish new benchmark for intelligent driving safety ecosystem

Elektrobit, a global leader in automotive software, has teamed up with Metoak, that specializes in manufacturing chips and providing solutions for self-driving cars, to create a new safety system for intelligent driving. Together, they have launched the first open-source operating system in China that meets safety standards for Advanced Driver Assistance Systems (ADAS). It works by combining Elektrobit's EB corbos Linux software with Metoak's powerful chips. The goal is to improve key driving features like keeping vehicles in their lanes, emergency braking, and other automated functions.

Source
https://www.elektrobit.com/

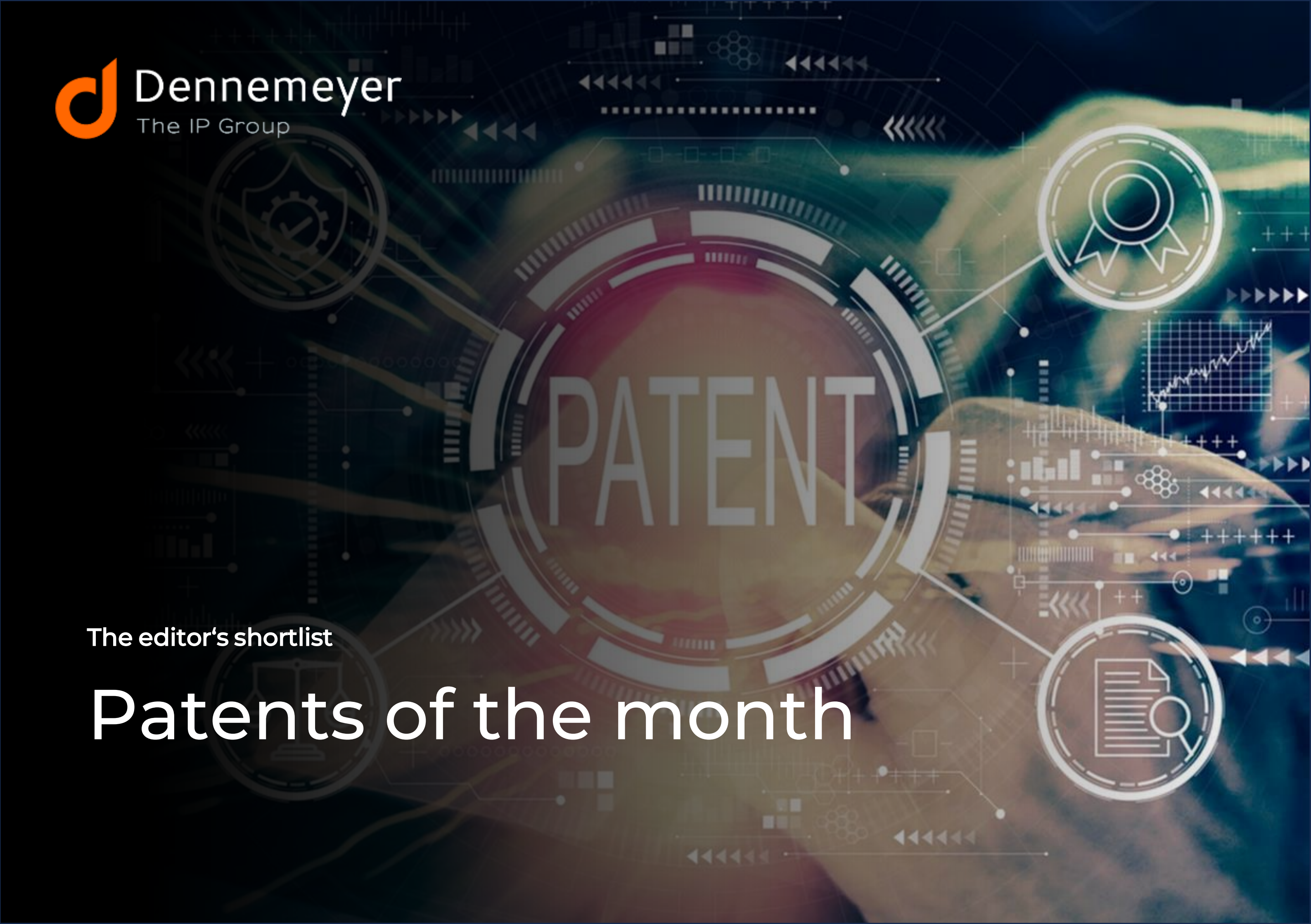
Automotive Testing Lab

DEKRA Celebrates Grand Opening of Michigan Automotive Advanced Testing Laboratory for Future Mobility

DEKRA, a global leader in safety and testing, is launching its new Michigan Automotive Test Center to support the evolving mobility industry. This facility offers critical testing and certification services for electric vehicles, automotive connectivity, cybersecurity, and AI. It is equipped to conduct high-voltage electromagnetic compatibility tests, environmental simulations, and cybersecurity assessments, ensuring vehicle safety and reliability. Additionally, it will function as an authorized testing lab for Apple CarPlay and CarKey certification. By setting global safety and security standards, DEKRA aims to help automakers improve vehicle reliability and digital system security, driving innovation in automotive technology.

Source
https://www.dekra.us/

Dennemeyer
The IP Group



The editor‘s shortlist

Patents of the month

Patents of the month

Published in April 2025

Shortlisted and summarized by our analyst

- US2025117490A1 - Software vulnerability analysis
  Assignee: Continental Automotive Technology GMBH
- US12273378B2 - Denial of service response to the detection of illicit signals on the in-vehicle communication network
  Assignee: Waymo LLC
- US12282548B2 - Universally applicable signal-based controller area network (CAN) intrusion detection system
  Assignee: Ut Battelle LLC
- IN202421026809A - System to enhance cybersecurity during charging of an electric vehicle
  Assignee: Matter Motor Works Pvt Ltd
- KR102791477B1 - Apparatus for node of prevention of the Denial of Service attack on CAN communication and method for shifting priority using the same
  Assignee: Hyundai Motor Co
- EP4533736A1 - Protection against cybersecurity attacks on transmission control units
  Assignee: ZF Friedrichshafen Ag
- EP3648082B1 - Systems and methods for detecting and alerting security threats in vehicles
  Assignee: Honeywell International Inc
- JP7665640B2 - System for detecting intrusions into in-vehicle networks and method of implementing same
  Assignee: KIA Corporation, Hyundai Motor Company
- DE112023002438T5 - Threat analysis procedures, threat analysis system and program
  Assignee: Panasonic Automotive Systems Co Ltd
- CN119892451A - Internet of vehicles intrusion detection system based on T-BOX
  Assignee: Shandong Branch Center National Computer Network & Information Security Management Center

US2025117490A1

Software vulnerability analysis

Company name	Continental Automotive Technology GMBH
Inventors	Xiong Siyang, Habib Sheikh Mahbub, Wang Yi Estelle, Dehm Mathias
Priority date	08 May 2021
Publication date	04 Apr 2025

Summarized by Dennemeyer

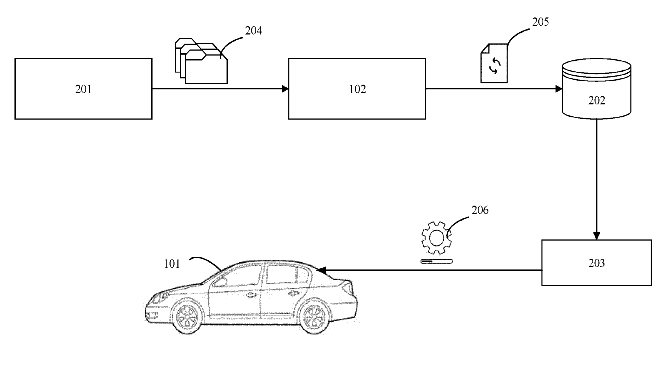


Figure 2

This patent improves cybersecurity in automotive systems by addressing software vulnerabilities that can lead to failures in critical vehicle functions. It works by carefully checking application files against stored rules, database information, and expert guidelines to find potential security risks. It updates vulnerability databases in real time, allowing for immediate threat detection and patch implementation. It uses two types of analysis: static, which examines code before it runs, and dynamic, which monitors behavior while running to effectively spot issues. Additionally, it connects to cybersecurity databases like the Common Vulnerabilities and Exposure (CVE) system, ensuring that new threats are recognized immediately and reducing the risk of cyberattacks.

Dennemeyer
The IP Group

Latest patents

US12273378B2

Denial of service response to the detection of illicit signals on the in-vehicle communication network

Company name	Waymo LLC
Inventors	Huang Tsengchan Stephan
Priority date	15 Jul 2021
Publication date	08 Apr 2025

Summarized by Dennemeyer

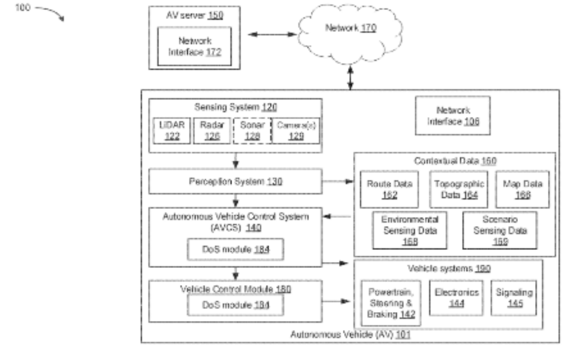


FIG. 1

This patent focuses on protecting a vehicle's communication system from harmful signals that could disrupt its functions. It continuously monitors for unauthorized signals, evaluates their risk, and responds if needed. When a signal exceeds a certain danger level, the system takes action to reduce potential threats. This real-time detection and response method improves vehicle security while ensuring backup systems keep the vehicle running safely, even if part of the network is affected. Since it relies on software rather than costly hardware, it offers an efficient and affordable way to boost cybersecurity and shield electronic control units from malicious interference.

US12282548B2

Universally applicable signal-based controller area network (CAN) intrusion detection system

Company name	Ut Battelle LLC
Inventors	Bridges Robert A, Verma Kiren E, Iannacone Michael, Hollifield Samuel C, Moriano Pablo, Sosnowski Jordan
Priority date	23 Apr 2021
Publication date	22 Apr 2025

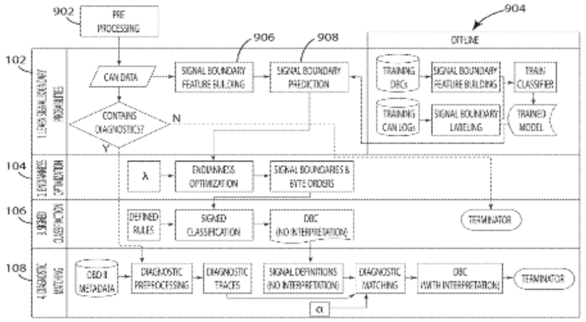


Fig. 9

This patent presents a security architecture for vehicles that detects cyberattacks on the Controller Area Network (CAN). Hackers try to send fake signals that seem real, potentially disrupting the car's functions. To prevent this, the system includes a CAN transceiver that receives data and works with a controller to spot suspicious activity. It analyzes signal patterns over time to identify possible threats. A standout feature is its ability to decode encrypted or proprietary messages without needing special manufacturer access. This strengthens vehicle cybersecurity, making operations safer and more secure against evolving risks.

Summarized by Dennemeyer

IN202421026809A

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	04 Apr 2025

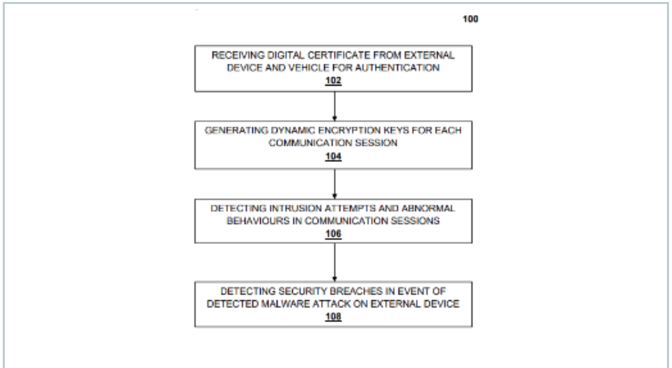

100
RECEIVING DIGITAL CERTIFICATE FROM EXTERNAL DEVICE AND VEHICLE FOR AUTHENTICATION
102
GENERATING DYNAMIC ENCRYPTION KEYS FOR EACH COMMUNICATION SESSION
104
DETECTING INTRUSION ATTEMPTS AND ABNORMAL BEHAVIOURS IN COMMUNICATION SESSIONS
106
DETECTING SECURITY BREACHES IN EVENT OF DETECTED MALWARE ATTACK ON EXTERNAL DEVICE
108

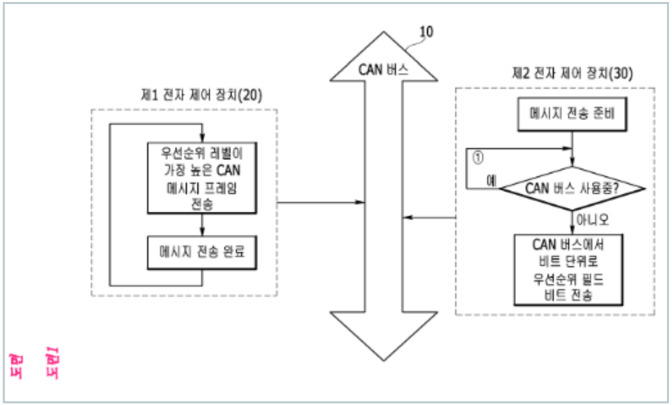
FIG. 1

This patent introduces a cybersecurity framework for EV charging stations to prevent threats like stolen credentials and harmful software injections during charging. It includes a security unit that constantly checks software integrity using encryption and comparison techniques to detect cyber risks. If a threat is found, an alert system notifies users and fleets, allowing a quick response. Before a charging session starts, the framework verifies certificates to confirm the station's security. Additionally, a digital map highlights risky stations with color codes for easy identification. By automating security checks and offering real-time monitoring, this system enhances EV charging safety and minimizes disruptions.

KR102791477B1

Apparatus for node of prevention of the Denial of Service attack on CAN communication and method for shifting priority using the same

Company name	Hyundai Motor Co
Inventors	Ashwin Kulkarni
Priority date	27 May 2019
Publication date	03 Apr 2025



This patent helps protect vehicles from cyberattacks, specifically Denial-of-Service (DoS) attacks in the Controller Area Network (CAN) system. Hackers can exploit the open nature of CAN messages to disrupt vehicle functions. Traditional encryption slows communication, and simply monitoring messages isn't enough to stop attacks. To solve this, the invention introduces a mechanism that ranks message importance, detects errors, and adjusts priority values dynamically when an attack is detected. It uses sensor data to update message priority, preventing long-lasting system failures and reducing disruptions. This makes hacking much more difficult while ensuring key vehicle functions continue to work smoothly, keeping the system secure and reliable.

EP4533736A1

Protection against cybersecurity attacks on transmission control units

Company name	ZF Friedrichshafen Ag
Inventors	Biel Steffen
Priority date	10 May 2022
Publication date	19 Mar 2025

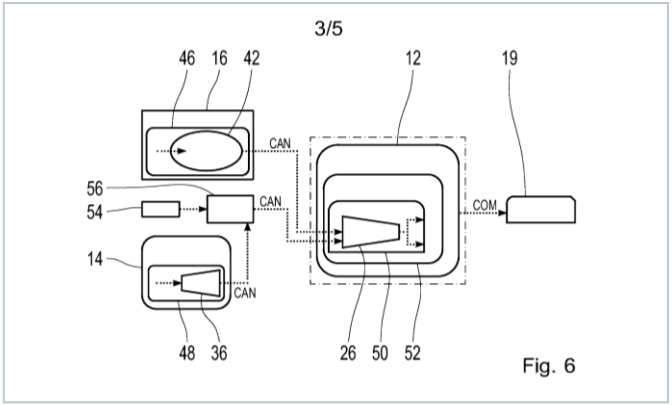


Fig. 6

This patent enhances vehicle security against cyber threats by addressing weaknesses in their control frameworks. Normally, security keys are sent over networks to safeguard critical functions, but hackers can steal them. Instead of relying on these keys, this invention utilizes artificial neural networks to generate and verify security signals instantly. It receives a signal to determine if access is permitted, then a specialized unit compares the signal and fine-tunes the mechanism to improve accuracy. A feedback process detects errors as the model learns, and finally, it decides whether the vehicle functions should be activated. Since no security keys are directly transmitted and each signal is unique, it becomes significantly harder for hackers to breach security. This innovation makes vehicles more resistant to cyberattacks.

EP3648082B1

Systems and methods for detecting and alerting security threats in vehicles

Company name	Honeywell International Inc
Inventors	Nicholls James Alexander, Stokely John, Clark Dereck, Ishihara Yasuo
Priority date	30 Oct 2018
Publication date	09 Apr 2025

Summarized by Dennemeyer

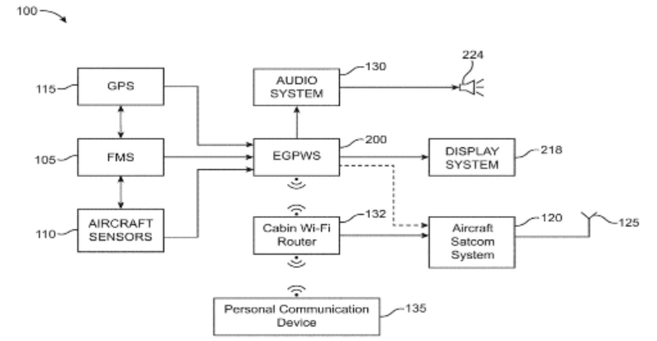


FIG. 1

This patent focuses on enhancing vehicle safety by detecting unusual vehicle route changes that may pose physical or cyber risks due to the connectivity and complexity of modern vehicles. The solution features an onboard monitoring system that retrieves and analyzes the planned route, identifies potential threats, and sends alerts when security risks are detected. It accounts for factors such as route deviations, interactions with the surrounding environment, and validation requests from ground services before confirming an anomaly. By integrating wireless communication and real-time alerts for crew members, this technology enables swift responses to threats while minimizing false alarms, ensuring smooth and secure vehicle operations.

Dennemeyer
The IP Group

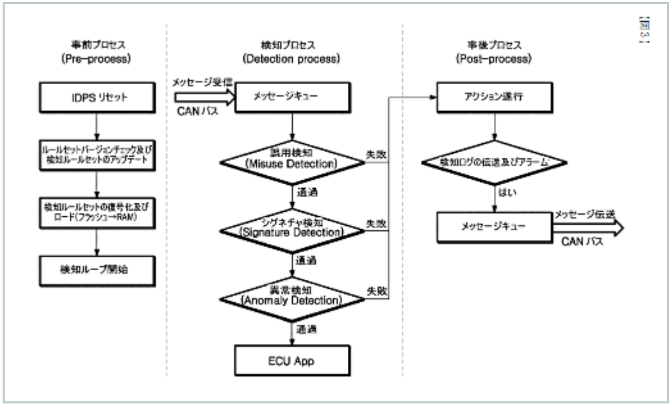
Latest patents

JP7665640B2

System for detecting intrusions into in-vehicle networks and method of implementing same

Company name	KIA Corporation, Hyundai Motor Company
Inventors	Kim Tae Guen, Cho A Ram, Park Seung Wook, Lim Wha Pyeong
Priority date	10 Feb 2020
Publication date	21 Apr 2025

Summarized by Dennemeyer



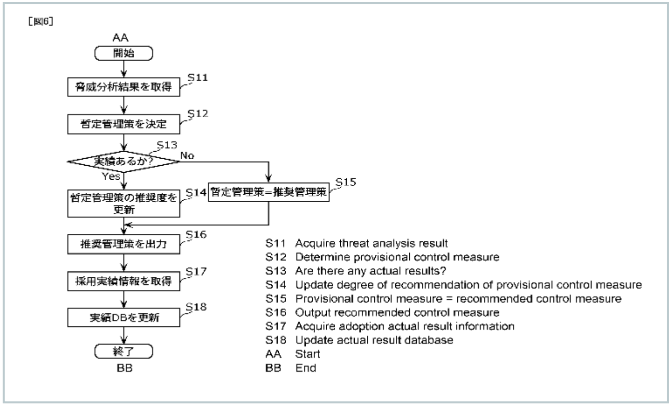
The patent presents a solution to the growing security threats in vehicle networks, where numerous ECUs are interconnected, making them vulnerable to cyberattacks. It introduces a security framework that records network messages, verifies them using encrypted rules, and analyzes threats to assess their severity and detection confidence. All security logs and rules are securely stored in an encrypted platform. An interface manager transmits reports to a central hub, prioritizing the most critical incidents. The setup operates efficiently with minimal resource consumption, making it ideal for vehicles. A dynamic scoring method enhances threat detection accuracy, enabling users to make informed decisions and improve overall vehicle safety.

DE112023002438T5

Threat analysis procedures, threat analysis system and program

Company name	Panasonic Automotive Systems Co Ltd
Inventors	Aoshima Hatsuho, Nemoto Yusuke, Wada Hiroyuki, Nagata Minehisa
Priority date	30 May 2022
Publication date	03 Apr 2025

Summarized by Dennemeyer


[図6]
AA
開始
脅威分析結果を取得
S11
暫定管理策を決定
S12
S13
実績あるか？
No
Yes
暫定管理策の推奨度を更新
S14
暫定管理策＝推奨管理策
S15
推奨管理策を出力
S16
採用実績情報を取得
S17
実績DBを更新
S18
終了
BB
S11 Acquire threat analysis result
S12 Determine provisional control measure
S13 Are there any actual results?
S14 Update degree of recommendation of provisional control measure
S15 Provisional control measure = recommended control measure
S16 Output recommended control measure
S17 Acquire adoption actual result information
S18 Update actual result database
AA Start
BB End

The patent introduces a process for analyzing and countering cyber threats targeting mobile entities like vehicles, addressing the limitations of traditional security assessments conducted during development. It works by studying cyberattacks, suggesting different countermeasures, and ranking them based on how often they've been successfully used before. By using past implementation data, it ensures the best solutions are chosen. It also adapts in real time, improving security based on user feedback. This means vehicles stay protected as new cyber threats emerge without relying on outdated security methods. Overall, this helps strengthens decision-making, making cybersecurity more flexible and responsive to evolving attack vectors.

CN119892451A

Internet of vehicles intrusion detection system based on T-BOX

Company name	Shandong Branch Center National Computer Network & Information Security Management Center
Inventors	Li Rui, Li Shengbao, Jiao Liang, Song Jiangjing, Xiang Yuanyuan, Zhang Tai, Liu Jing, Xue Junkai, Liu Yi, Zhu Xiushan
Priority date	09 Jan 2025
Publication date	25 Apr 2025

Summarized by Dennemeyer

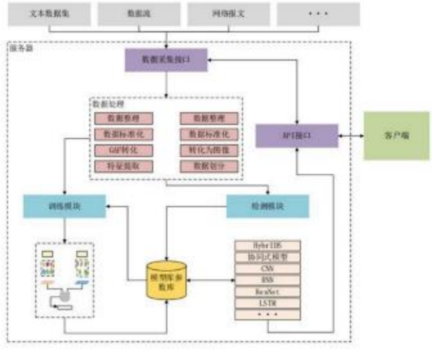


图1

This patent is about enhancing the security of smart vehicles by addressing vulnerabilities in the T-BOX system. The T-BOX helps the vehicle communicate with outside networks, but it can be hacked. To mitigate this risk, an advanced security system capable of detecting cyber-attacks is introduced. It works by constantly gathering key vehicle data, training smart security models to recognize risks, and scanning for unusual activity that could indicate a cyber-attack. It also includes a real-time supervision platform that keeps everything under constant watch. It uses advanced AI models to improve how well it detects unusual network activity. With continuous monitoring and adaptive security measures, this invention ensures that connected vehicles are better protected against cyber threats like unauthorized access and data breaches.

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
- Vargarda, SE
- Warsaw, PL
- Woking, UK
- Zagreb, HR

Talk to us now

Find out how we can support you
in these services and more.

- Patent Renewals
- Trademark Renewals
- Trademark Filing
- Recordals
- PCT Nationalization
- European Patent Validation
- DIAMS IP Management Software
- IP Analytics

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.