Dennemeyer
The IP Group

Report of April 2026

Cybersecurity in mobility

Recent developments

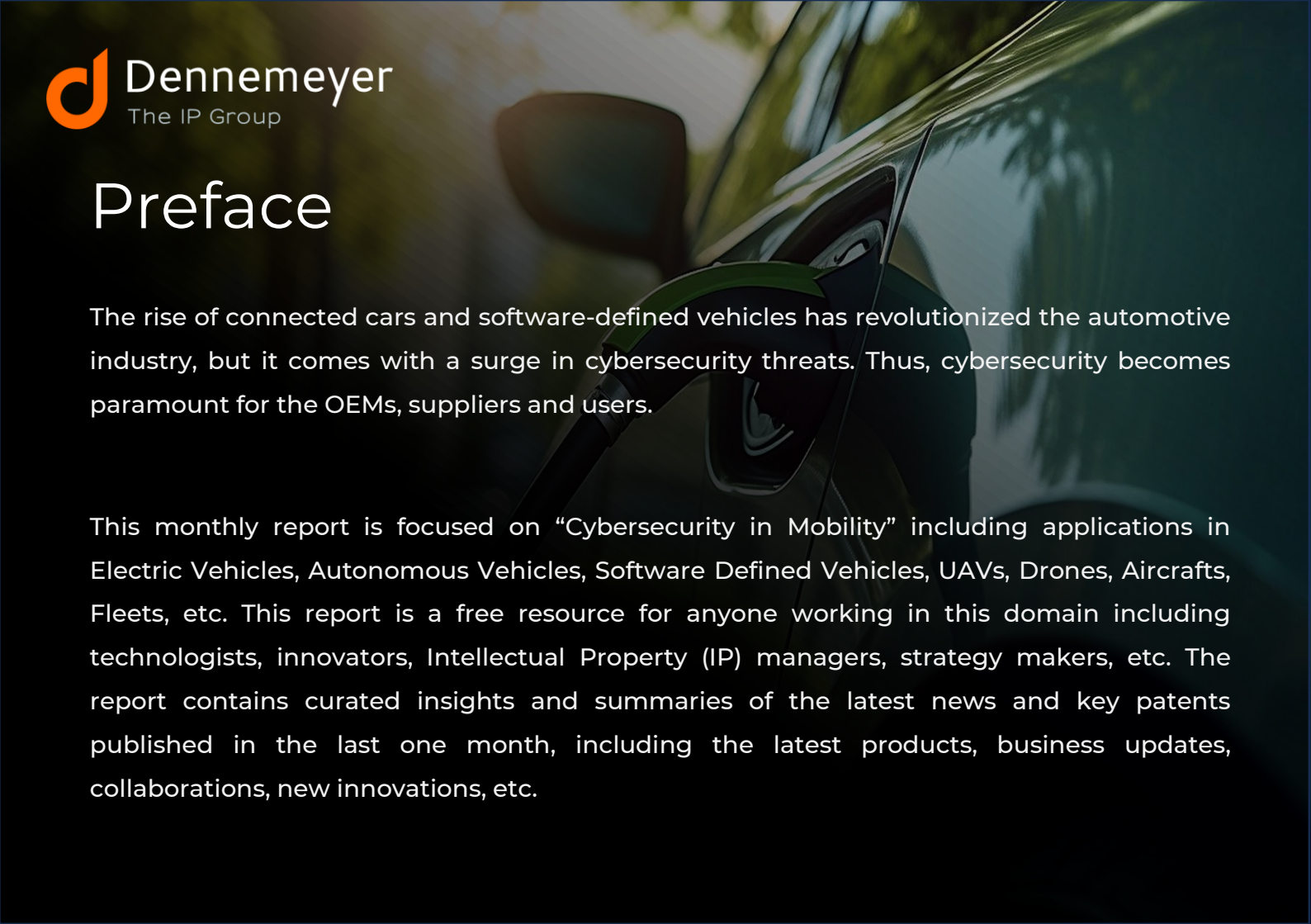
Curated and summarized - Industry and Patent news

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.



Dennemeyer
The IP Group

Preface

The rise of connected cars and software-defined vehicles has revolutionized the automotive industry, but it comes with a surge in cybersecurity threats. Thus, cybersecurity becomes paramount for the OEMs, suppliers and users.

This monthly report is focused on “Cybersecurity in Mobility” including applications in Electric Vehicles, Autonomous Vehicles, Software Defined Vehicles, UAVs, Drones, Aircrafts, Fleets, etc. This report is a free resource for anyone working in this domain including technologists, innovators, Intellectual Property (IP) managers, strategy makers, etc. The report contains curated insights and summaries of the latest news and key patents published in the last one month, including the latest products, business updates, collaborations, new innovations, etc.

Dennemeyer
The IP Group

Key Insights

- The cyberattack on the breathalyzer company, Intoxalock, shows that a security breach at a third-party ignition interlock provider can immediately prevent drivers from operating their vehicle. As connected aftermarket systems expand, insurers, regulators, and fleet operators are likely to focus more on uptime, recovery, and cybersecurity controls for ignition interlock services that affect vehicle access.

- The tire pressure sensor vulnerability identified by researchers shows that even basic vehicle components can be used to track vehicles and compromise driver privacy. This will likely increase focus on wireless sensor security and pressure OEMs to add encryption, authentication, and stronger cyber protection to low-cost vehicle electronics that were previously considered low risk.

- Deloitte's ConnectSafe facility signals a shift in India, towards hands-on cyber testing for connected systems, rather than relying solely on policy and software reviews. As threat complexity grows, more organizations are likely to turn to dedicated cyber labs to test real-world attacks, validate connected systems, and strengthen resilience across mobility and critical infrastructure.

- Microchip's new security chips and cloud services highlight the growing role of hardware-based trust in vehicle cybersecurity. This will likely help OEMs and suppliers meet stricter compliance demands faster, while boosting demand for built-in secure authentication, key management, and protected software updates.

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

  - Several inventions go beyond static Intrusion detection systems rules by using CAN timing analysis, transformer-based log monitoring, and multi-source data fusion across CAN, infotainment, networking, and sensors to detect anomalies more accurately while reducing false alarms.
  - Patents focusing on maintaining safety and continuity during an attack, rather than shutting systems down, by using relay-based rerouting for emergency communication, fallback sensing, and attack containment.

Dennemeyer
The IP Group

Industry News

Breathalyzer Cyberattack

Cyberattack on vehicle breathalyzer company leaves drivers stranded across the US

A cyberattack hit Intoxalock, a company that makes breathalyzer devices that must be used to start certain vehicles. The attack happened on March 14 and forced the company to shut down parts of its systems for safety. These devices need regular calibration and the outage stopped Intoxalock from performing those updates. Because of this, many drivers across the United States cannot start their cars when their device shows that a calibration is overdue. Many users reported being locked out of their vehicles with no way to drive. Reports show that drivers from New York to Minnesota are dealing with the same issue. Intoxalock has not said whether the attack involved ransomware or a data breach. The company serves about 150000 drivers across 46 states. Intoxalock has not given a timeline for when its systems will be fixed.

Source
https://techcrunch.com/

Dennemeyer
The IP Group

Industry News

Collaboration

Vivicta and Valmet automotive deepen their collaboration – modern IT solutions support Valmet automotive's expanding business

Vivicta and Valmet Automotive have renewed their partnership, with Vivicta providing modern cybersecurity solutions to help Valmet Automotive expand efficiently and securely into new industries, including defence. The new agreement includes productized IT services that use AI and automation to enhance cybersecurity, manage critical environments, and speed up response times. Vivicta's services cover capacity, end-user support, security, and integration, supporting Valmet Automotive's modernization and strategic business goals. Vivicta has worked with Valmet Automotive for over ten years, handling infrastructure, cybersecurity, and SAP system management. The partnership aims to ensure safe, agile, and flexible operations as Valmet Automotive grows.

Source
https://www.vivicta.com/

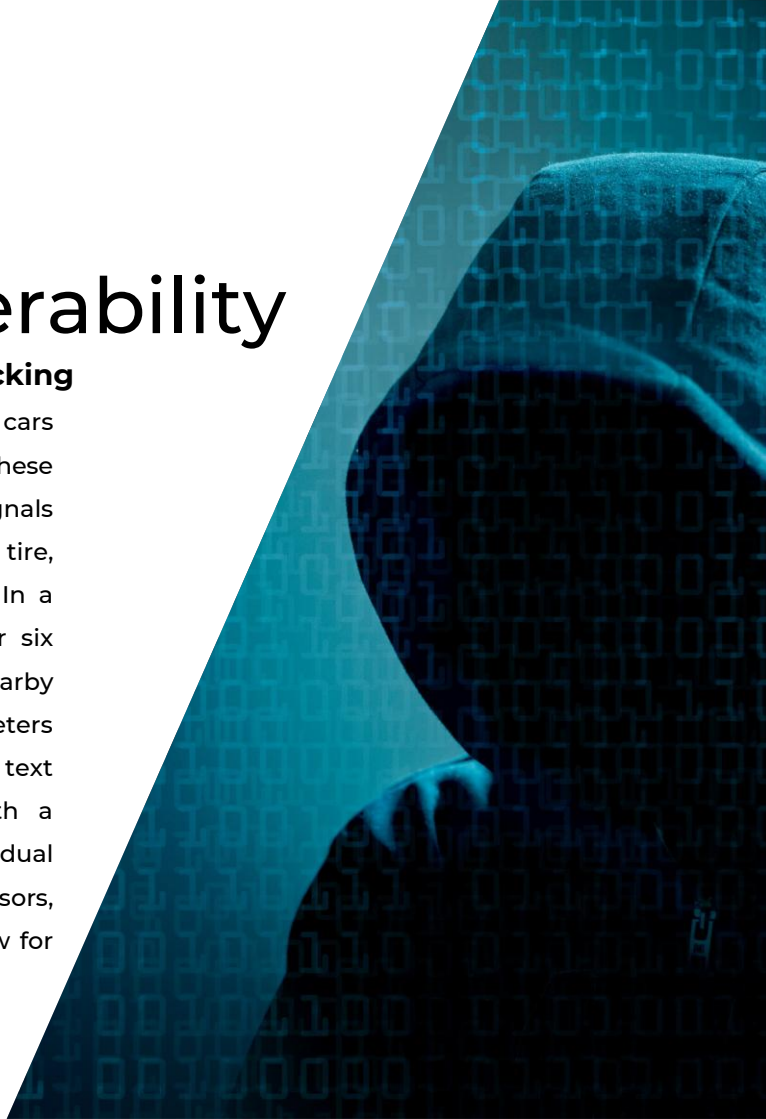
Dennemeyer
The IP Group

Industry News

Tire Sensor’s Vulnerability

Vehicle tire pressure sensors enable silent tracking

Researchers found that tire pressure sensors in modern cars can be used to secretly track vehicles and their owners. These sensors, required in the US since 2007, send wireless signals with tire data, but also include a unique ID for each tire, making it possible to identify and follow specific cars. In a study, researchers used cheap receivers to collect over six million signals from 20,000 cars, proving that anyone nearby could intercept these transmissions from up to 50 meters away, even inside buildings. The data is sent in clear text without encryption or authentication, so anyone with a receiver can pick up the signals and match them to individual vehicles. This vulnerability means that tire pressure sensors, meant for safety, can leak sensitive information and allow for low-cost vehicle tracking.



Source
https://www.darkreading.com/

Dennemeyer
The IP Group

Industry News

Microchip Strengthens Vehicle Security

Microchip expands security services in the trust platform to help manufacturers meet cybersecurity regulations

Microchip Technology has introduced new secure authentication chips and cloud services to help industrial and automotive manufacturers meet tough cybersecurity regulations. These chips are preconfigured to make hardware based authentication easier and faster to implement, while the cloud services offer management of cryptographic keys and secure firmware updates. These solutions support compliance with all major automotive cybersecurity standards. The chips transmit secure data, allow remote updates, and ensure that only authenticated software is used in vehicles. Both products help create a hardware rooted chain of trust from manufacturing to in field operation, reducing complexity and speeding up compliance ready product development.

Source
https://ir.microchip.com/

Dennemeyer
The IP Group

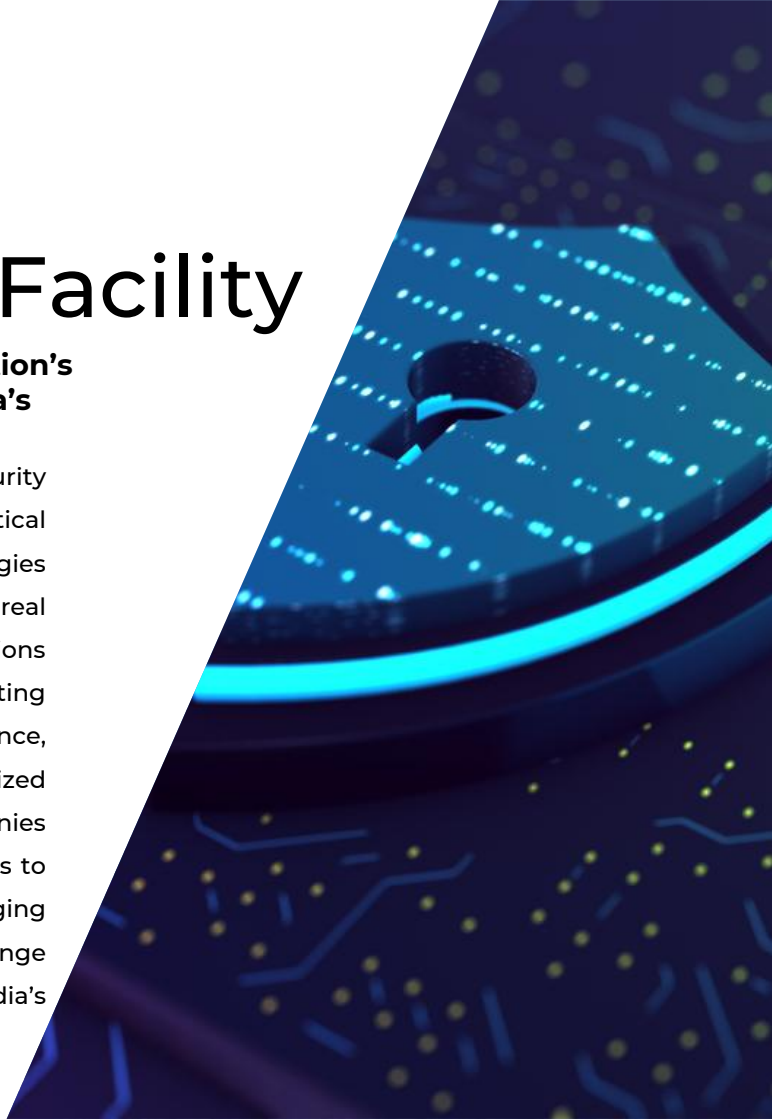
Industry News

Deloitte’s Cyber Facility

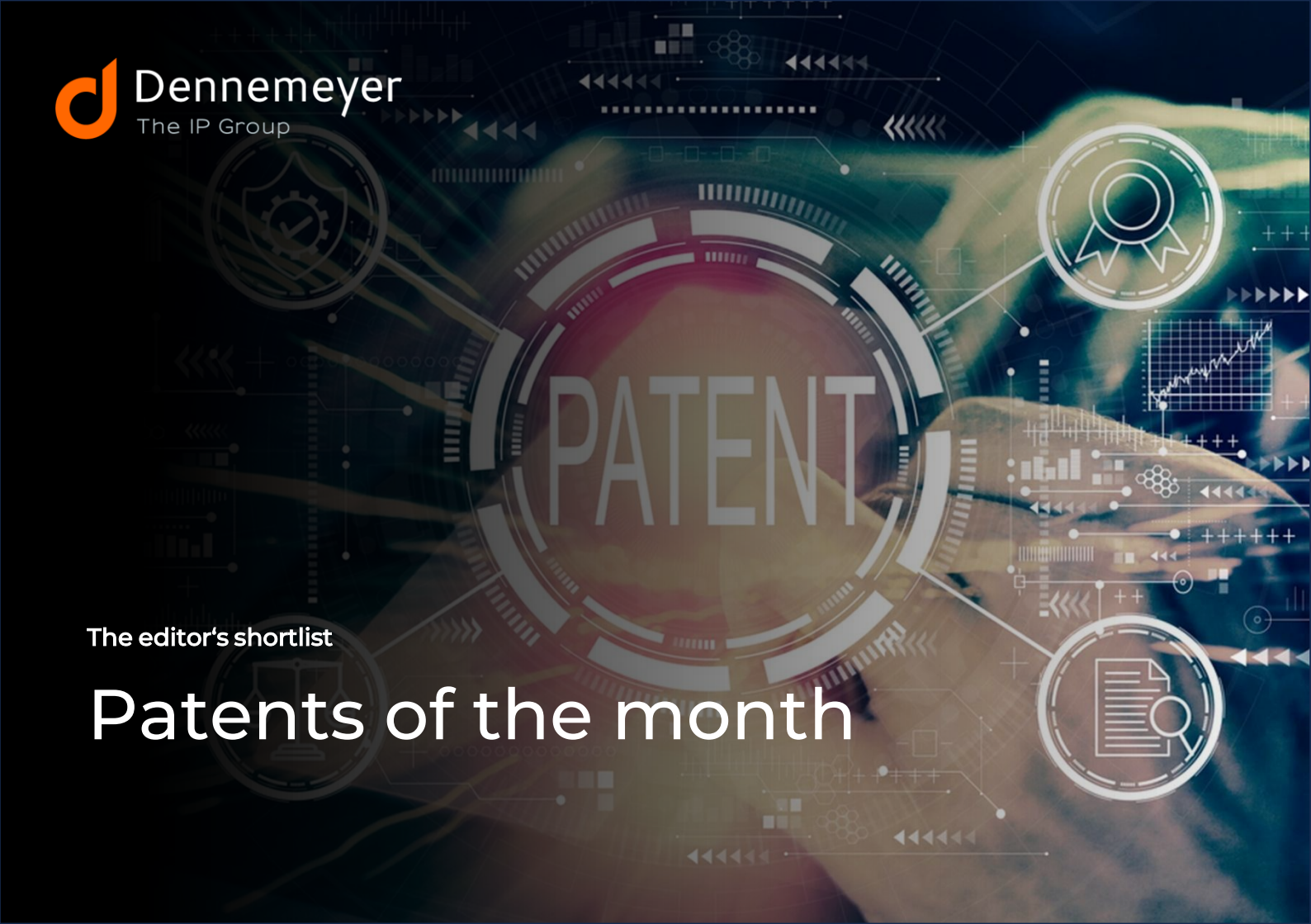
Deloitte India unveils ConnectSafe™ – The nation’s first of its kind cyber facility to safeguard India’s connected ecosystems

Deloitte India has launched ConnectSafe™, a cybersecurity facility focused on protecting people and critical infrastructure as India rapidly adopts connected technologies in mobility, healthcare, and energy. The facility simulates real world cyber threats across industries, allowing organizations to test and strengthen their security without disrupting operations. It provides advanced testing, threat intelligence, real time detection, system validation, and specialized protection for software defined vehicles, helping companies prepare for complex attacks on everything from hospitals to power grids. It also addresses the risks posed by aging operational technology, which has become a major challenge in digital transformation, and supports the growth of India’s digital public infrastructure.

Source
https://www.deloitte.com/



Dennemeyer
The IP Group



The editor's shortlist

Patents of the month

Dennemeyer
The IP Group

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

Patents of the month

Published in March 2026

Shortlisted and summarized by our analyst

- US2026067300A1 - Gateway including an intrusion detection system in a controller area network of a vehicle and a method of operating the same
  Assignee: Hyundai Motor Co; Kia Corp
- US12587558B2 - System and method of artificial intelligence assisted cyber threat identification via webserver logs
  Assignee: Robert Bosch GMBH
- US12572649B2 - Method for protection from cyber attacks to a vehicle based upon time analysis, and corresponding device
  Assignee: Marelli Europe SPA
- EP4715645A1 - A computer-implemented method for conducting cyber security analysis and detecting potential cyber threats
  Assignee: Argus Cyber Security Ltd
- EP4708094A1 - Computer-implemented method for assessing a level of cyber security risks of an electronic control unit
  Assignee: Argus Cyber Security Ltd
- JP7827150B2 - In-vehicle device, security management method, and computer program
  Assignee: Sumitomo Electric Ind Ltd; Sumitomo Wiring System Ltd; Auto Network Gijutsu Kenkyusho Kk
- KR202600333394A - Unmanned aerial vehicle capable of detecting and response to cyber attacks, and method thereof
  Assignee: Terten Co., Ltd.
- IN202641020812A - Multi layered LiDAR security architecture for detecting and mitigating cyber physical attacks in autonomous vehicles.
  Assignee: Individual Inventors
- CN121690677A - New energy automobile CAN bus UDS diagnosis attack test method, system and medium
  Assignee: China Automotive Engineering Research Institute Co Ltd; CAIC New Energy Technology Co Ltd
- CN121690826A - Automobile electronic intrusion determination method and equipment based on multisource fusion data
  Assignee: Zhixin Control System Co Ltd

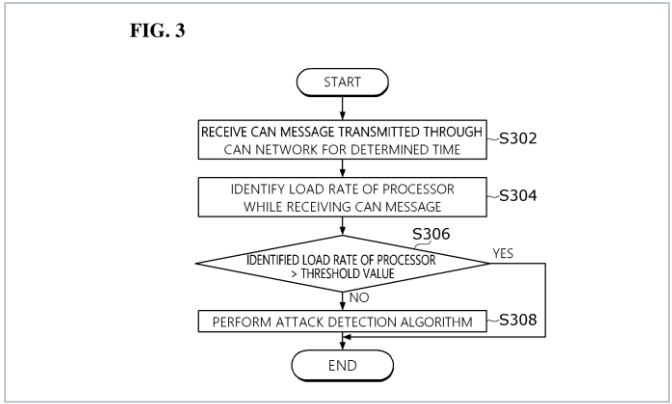
Dennemeyer
The IP Group

Latest patents

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

US2026067300A1

Gateway including an intrusion detection system in a controller area network of a vehicle and a method of operating the same



Company name	Hyundai Motor Co, Kia Corp
Inventors	Kang Dong Woo
Priority date	30 Aug 2024
Publication date	05 Mar 2026

The invention addresses the growing cyber risk in vehicles where many ECUs communicate over CAN networks, but some vehicles have limited processing power that cannot reliably run heavy intrusion detection algorithms. In this invention, the in-vehicle intrusion detection system (IDS) decides whether to run its attack detection algorithm based on how busy the processor is at that moment. The system listens to CAN messages for a set duration based on the fastest message cycle, measures the processor load during that period, and compares it with a predefined threshold. This threshold can vary depending on the vehicle's functions, specifications, driving conditions, and communication environment. If the processor load is below the threshold, the attack detection algorithm runs, and if it is above, the system waits to avoid overload and interruption of important vehicle functions.

Dennemeyer
The IP Group

Latest patents

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

US12587558B2

System and method of artificial intelligence assisted cyber threat identification via webserver logs

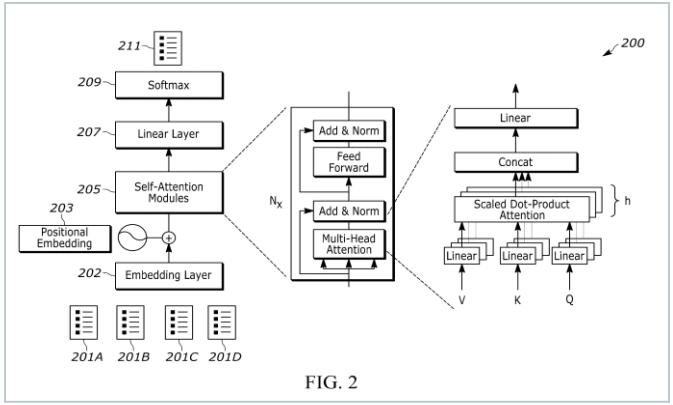


FIG. 2

Company name	Robert Bosch GMBH
Inventors	Qiu Chen, Lin Wan Yi, Cabrita Condessa Filipe J
Priority date	26 Apr 2024
Publication date	24 Mar 2026

The invention uses a trained transformer model to spot cyber threats by first learning what normal server activity looks like from past logs and then comparing this to new incoming logs. The model turns the historical logs into numerical vectors, adds timing information, processes them, and learns to predict what the next normal log should be. After training, the model receives real-time logs and calculates a user-score based on how different these logs are from the normal pattern it learned. It also calculates a server-score by comparing the new logs to clusters of normal behavior formed during training. If the combined score goes above a set limit, the system decides that the new logs may indicate a cyber threat. By using both prediction of the next log and comparison to normal clusters, the invention can more accurately detect unusual or suspicious behavior.

Summarized by Dennemeyer

Dennemeyer
The IP Group

Latest patents

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

US12572649B2

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

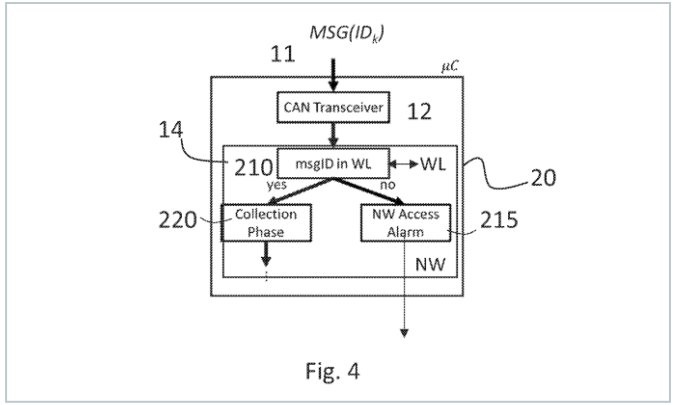


Fig. 4

Company name	Marelli Europe SPA
Inventors	Rosadini Christian, Chiarelli Simona, Cornelio Anastasia, Nesci Walter, Saponara Sergio, Dini Pierpaolo, Gagliardi Alessio
Priority date	02 Feb 2022
Publication date	10 Mar 2026

The invention protects a vehicle's CAN-bus network from cyber attacks by figuring out which ECU is sending malicious messages, something older systems cannot do because CAN messages do not include MAC addresses. It learns the normal timing pattern of each message ID by recording when messages usually arrive and calculating basic statistics like average timing and variation, creating confidence intervals that represent normal behavior for each node. During real-time use, it keeps checking the arrival times of new messages and compares them with these learned patterns, giving each message a "membership vote" that shows how closely it matches normal timing. If a message falls outside its expected timing range, the system marks it as suspicious and can identify which ECU is likely compromised.

Summarized by Dennemeyer

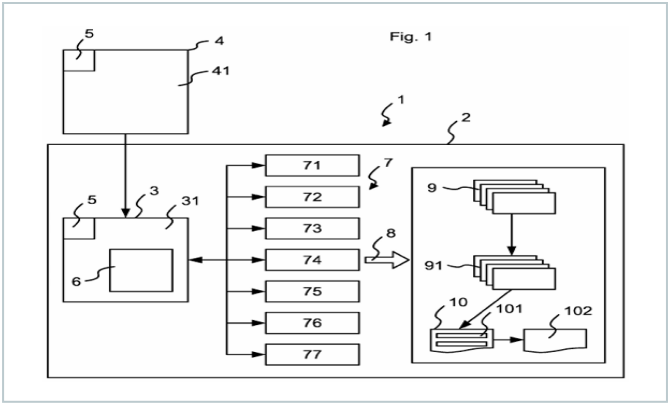
Dennemeyer
The IP Group

Latest patents

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

EP4715645A1

A computer-implemented method for conducting cyber security analysis and detecting potential cyber threats



Company name	Argus Cyber Security Ltd
Inventors	Bari Ephraim Yael, Lavi Oron, Ben Aharon Dolev
Priority date	18 Sep 2024
Publication date	25 Mar 2026

The invention describes a virtual inspection system that analyzes software used in devices like vehicle control units by running it inside a simulated environment, allowing earlier and safer detection of cyber threats. It uses different inspection modules that test the software in various ways, such as sending random inputs, checking known vulnerabilities, trying known exploits, reviewing permissions, and analyzing logs. Each module produces results that help the virtual environment identify possible threats, evaluate them, and generate a report that lists every detected threat along with a priority rating. The system can also propose fixes and even apply mitigation code automatically, including code generated by a large language model. By simulating hardware through virtual computing devices or virtual ECUs, it allows thorough testing without needing physical components, improving development efficiency and cybersecurity.

Dennemeyer
The IP Group

Latest patents

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

EP4708094A1

Computer-implemented method for assessing a level of cyber security risks of an electronic control unit

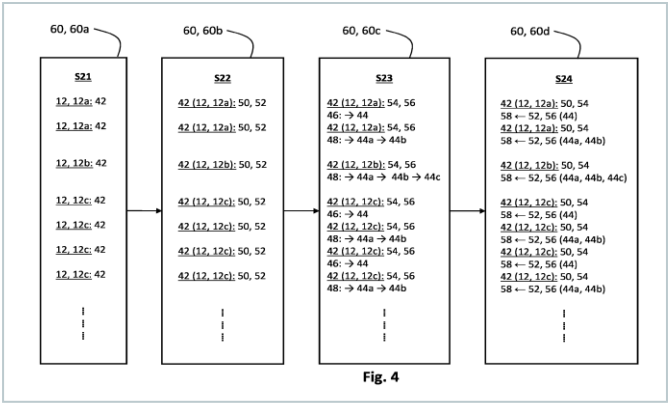


Fig. 4

Company name	Argus Cyber Security Ltd
Inventors	Bari Ephraim Yael, Lavi Oron
Priority date	10 Sep 2024
Publication date	11 Mar 2026

The invention makes the Threat Analysis and Risk Assessment process for ECUs much easier and faster by automatically finding which ECU parts are vulnerable, what threats they might face, and how attackers could reach them based on the ECU's design. It calculates how serious each threat is by combining the possible damage with how easy the attack path is, creating risk values that help judge the ECU's overall cybersecurity level. The system can automatically generate reports, compare the risks with standard threat lists, and recommend actions to reduce those risks. It can also update the assessment whenever the ECU's design changes, keeping the cybersecurity analysis current. By looking at both hardware and software parts, along with all the communication links between them, it provides a more complete understanding of the risks and suggest required fixes.

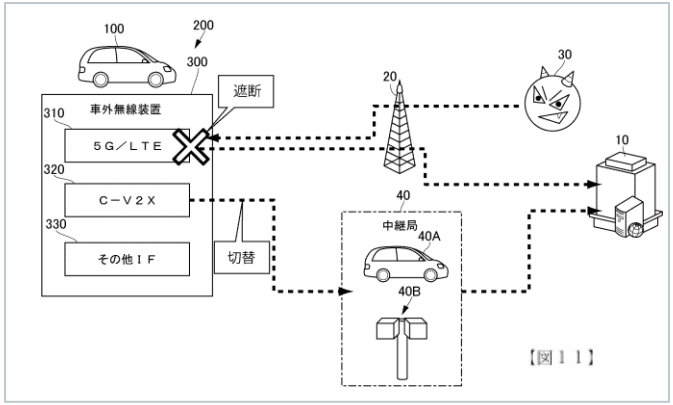
Dennemeyer
The IP Group

Latest patents

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

JP7827150B2

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



Company name	Sumitomo Electric Ind Ltd; Sumitomo Wiring System Ltd; Auto Network Gijutsu Kenkyusho Kk
Inventors	Akhihiro Ogawa, Kazuhiro Kakito, Satoshi Shimizu
Priority date	15 Jul 2022
Publication date	10 Mar 2026

The invention provides an in-vehicle security system that ensures a vehicle can continue performing essential communications, such as automatic emergency notifications, even when a cyberattack is detected. Traditional approaches cut all external communication during an attack, which risks blocking life-saving services; this system avoids that by managing multiple wireless interfaces and switching communication routes instead of shutting them down. When a cyberattack is detected, the wireless interface management unit reroutes communication through a different relay station chosen from a managed list. Each relay station is evaluated not only for connectivity but also for its security strength, and the relay station selection unit chooses the most secure available option. By switching to a safer communication path rather than stopping communication altogether, the system preserves critical external connectivity.

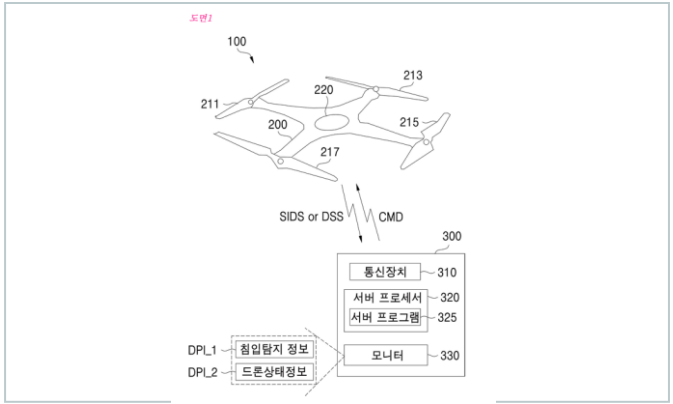
Dennemeyer
The IP Group

Latest patents

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

KR20260033394A

Unmanned aerial vehicle capable of detecting and response to cyber attacks, and method thereof



Company name	Terten Co., Ltd.
Inventors	Yoo Young-il, Daegeun Kim
Priority date	02 Sep 2024
Publication date	10 Mar 2026

The invention describes a drone that can detect and respond to cyber attacks targeting both its mission computer and its flight controller by integrating these components together with an IDS on a single printed circuit board. The drone uses sensors and a GPS receiver to gather signals for flight and mission control, while the IDS monitors for cyber attacks and generates alerts when threats are detected. When an intrusion occurs, the system sends a warning to a ground server through a wireless transceiver, and if a return command is configured, it instructs the flight controller to automatically return the drone to its starting point. Because the IDS can be turned on or off through remote commands, the ground server can manage security behavior as needed. By integrating the flight controller, mission computer, and IDS on one board, the design reduces wiring errors, improves signal integrity, and enhances response speed.

Dennemeyer
The IP Group

Latest patents

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

IN202641020812A

Multi layered LiDAR security architecture for detecting and mitigating cyber physical attacks in autonomous vehicles.

Company name	Individual Inventors
Inventors	Preetham Konda Nagaraja, Ramesh Kurbet
Priority date	23 Feb 2026
Publication date	06 Mar 2026

Summarized by Dennemeyer

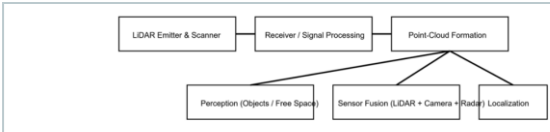


Fig. 1: LiDAR system and data path to perception.

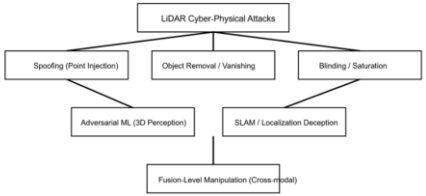


Fig. 2: Attack taxonomy (spoofing, removal, blinding, adversarial ML, SLAM, fusion).

The invention introduces a multi-layer LiDAR security system that protects autonomous vehicles from real-world LiDAR attacks, such as fake objects, hidden obstacles, sensor blinding, or tricks that confuse localization. It first checks the raw LiDAR signals to spot unusual timing, intensity, or saturation patterns that could mean someone is injecting or manipulating laser signals. Then it looks at the point cloud to see whether objects move unnaturally, appear or disappear suddenly, or have shapes that don't make sense. The system also compares LiDAR results with camera and radar data, and if they do not match, it reduces how much the vehicle relies on LiDAR to make decisions. To protect localization, it watches for abnormal scan-matching results, sudden pose changes, and map inconsistencies. When an attack is detected, it can remove fake objects, block suspicious data, or trigger a safe driving action.

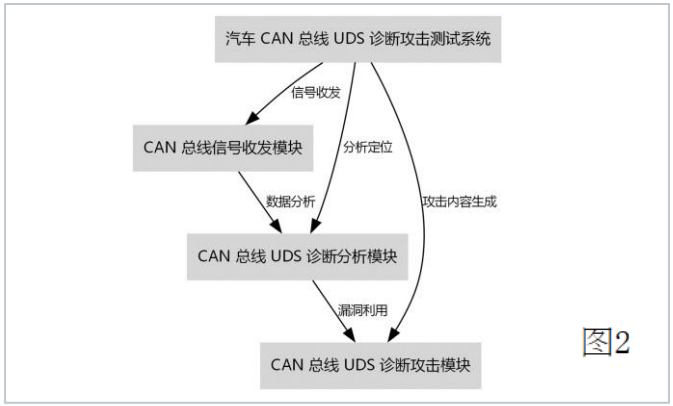
Dennemeyer
The IP Group

Latest patents

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

CN121690677A

New energy automobile CAN bus UDS diagnosis attack test method, system and medium



Company name	China Automotive Engineering Research Institute Co Ltd, CAIC New Energy Technology Co Ltd
Inventors	Wang Peng, Bai Qin, Wang Yi, Liu Junli, Zhao Zhichao, Liu Ming, Liu Ning, Fu Jiyao, Guo Dianxiang
Priority date	25 Nov 2025
Publication date	17 Mar 2026

The invention describes a method for testing security vulnerabilities in the CAN bus UDS (Unified Diagnostic Services) of new EVs by imitating real cyberattacks and simulating actual attack behaviors to uncover weaknesses that could allow malicious actors to disrupt vehicle functions or tamper with diagnostic data. It begins by collecting diagnostic IDs, then uses machine learning to predict likely IDs. Next, it launches attack tests on basic diagnostic services to determine if they can be accessed or misused without permission. After that, the method collects and analyzes diagnostic data identifiers (DIDs) stored in the vehicle. It tests both reading and writing of these DIDs to identify risks where data could be altered or manipulated. Reinforcement learning is used to adjust attack settings based on the system's responses, enhancing the effectiveness of the attack testing.

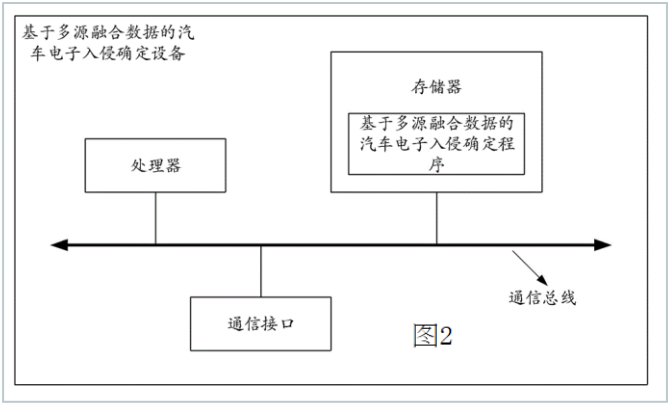
Dennemeyer
The IP Group

Latest patents

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

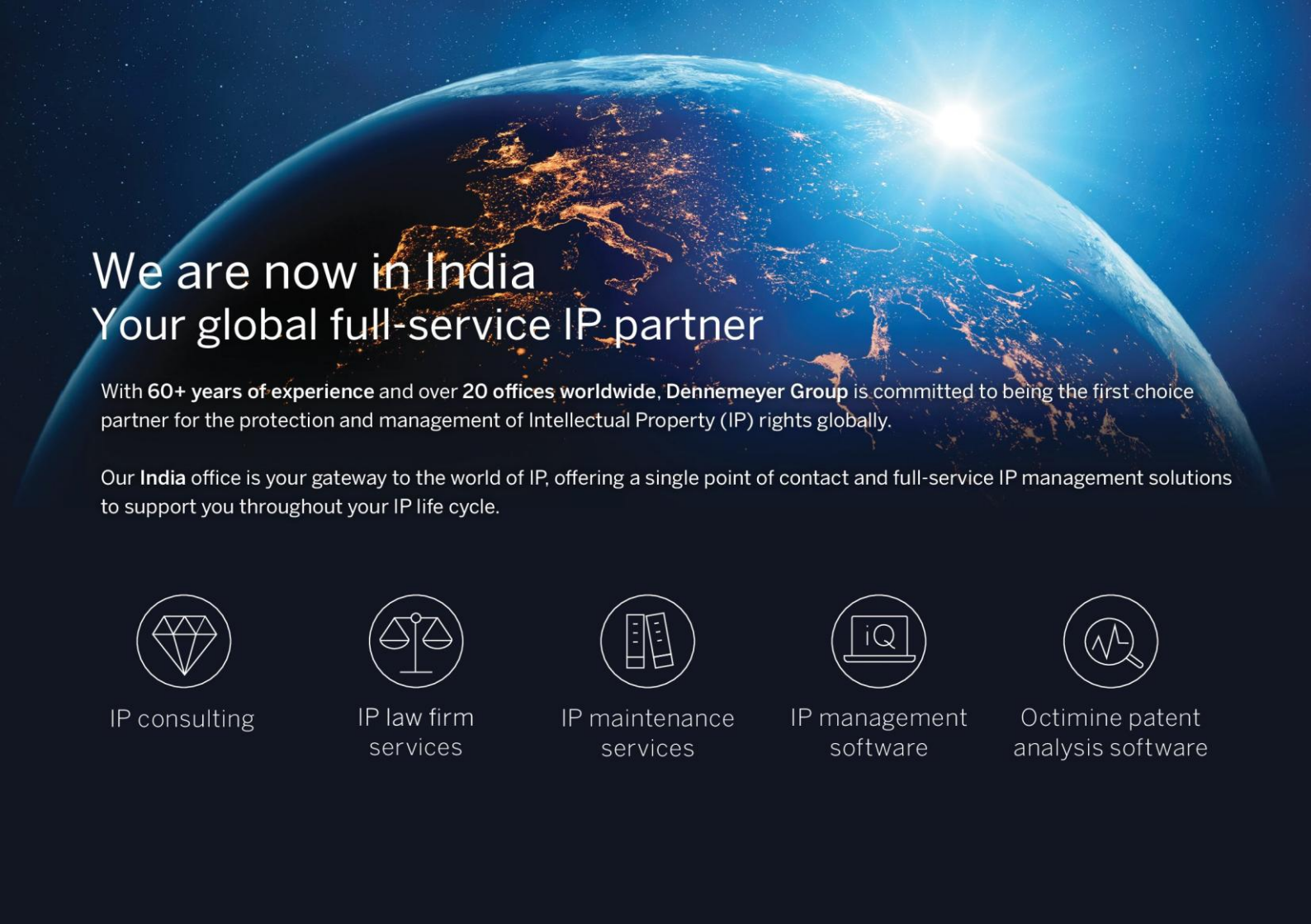
CN121690826A

Automobile electronic intrusion determination method and equipment based on multisource fusion data



Company name	Zhixin Control System Co Ltd
Inventors	Fu Jiwei, Zheng Chunyang, Liu Xiujin
Priority date	25 Dec 2025
Publication date	17 Mar 2026

The invention employs an automobile intrusion detection method that overcomes the limitations of traditional systems that rely solely on CAN bus data by combining data from the CAN bus, the infotainment system, vehicle networking modules, and vehicle state sensors. It then filters, synchronizes, and fuses these data to form rich multi-dimensional feature vectors. These fused data samples are labeled with early-warning levels to build a training dataset used to teach a preset neural network how different intrusion patterns appear across multiple channels. The trained model then analyzes real-time multi-source vehicle data to output an early-warning level that reflects the likelihood and severity of an electronic intrusion. By integrating diverse data types, the system improves detection accuracy, reduces false alarms, and better identifies complex attack behaviors.



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