

Report of September 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)

This report is subject to copyrights and may only be reproduced with permission of Dennemeyer.

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

- ❑ LG's CSMS Level 3 certification at its Hai Phong facility positions it as a trusted Tier 1 supplier and strong cybersecurity differentiator, especially as compliance with regulations like UNECE R155 becomes essential. By embedding robust cybersecurity at the manufacturing level, LG reduces supply chain risk and gains strategic advantage as OEMs prioritize secure, compliant partners.
- ❑ Auto-ISAC's partnership with Manifest and FESCARO accelerates industry-wide collaboration, making cybersecurity a joint responsibility. AI-driven SBOM automation and SDV lifecycle protection mark a shift toward faster compliance, integrated security, and innovation, enabling OEMs and suppliers to secure market access and long-term resilience.
- ❑ The ransomware attack on Maryland Transit Administration's Mobility service highlights the growing threat to critical public infrastructure, particularly services supporting vulnerable populations. These disruptions highlight the need for stronger cybersecurity investment, faster incident response, and potential regulatory action to ensure resilience.
- ❑ Hyundai Mobis earned ISO 26262 ASIL-D certification for its semiconductors, ensuring over 99% reliability across its entire R&D process. This milestone strengthens its position in automotive safety, likely boosting OEM partnerships, shaping industry standards, and driving innovation in high-reliability chips for EVs and autonomous vehicles.
- ❑ Many inventions that were published last month had major themes as below:
 - Connected vehicles are adopting multi-layered ECU and network defenses that integrate electrical and message-layer signals with internal monitoring and log analysis to detect spoofing, replay, and denial-of-service attacks while safeguarding sensitive security data.
 - Automotive and charging ecosystems are implementing AI-driven, adaptive threat responses and quantum-resistant encryption, enabling real-time attack mitigation, autonomous system recovery, and protection against both current and emerging cyber threats.

Certification

LG secures top cybersecurity certification at largest vehicle component production base

LG Electronics announced that its Hai Phong manufacturing facility in Vietnam, the company's largest vehicle component production hub, has earned Cyber Security Management System (CSMS) Level 3 certification from TÜV Rheinland. This makes Hai Phong the first facility globally to receive both CSMS Level 2 and Level 3 certifications simultaneously. The certification validates LG's robust cybersecurity practices across the vehicle component lifecycle, reinforcing its leadership amid growing global regulations like UNECE R155. With rising cybersecurity risks in Software Defined Vehicles (SDVs), LG's achievement highlights its commitment to securing automotive production and meeting international standards.

Source

<https://www.lg.com/>



Cyber Alliance

Auto-ISAC partners with Manifest & FESCARO

The Automotive Information Sharing and Analysis Center (Auto-ISAC) has partnered with Manifest and FESCARO to strengthen vehicle cybersecurity across the automotive sector. Manifest specializes in AI and software supply chain security, helping automakers comply with global standards like UNECE R155, ISO/SAE 21434 and the European Cybersecurity Resilience Act (CRA), while automating Software Bill of Materials (SBOM) workflows and managing software vulnerabilities. FESCARO provides end-to-end cybersecurity for software-defined vehicles (SDVs), enabling OEMs to build resilient, lifecycle-wide protection. As Innovator Partners, both will collaborate with Auto-ISAC's members representing over 99% of North America's light-duty vehicles, to address evolving cyber threats.

Source

<https://automotiveisac.com/>



Security Breach

Security flaws in a carmaker's web portal let one hacker remotely unlock cars from anywhere

Security researcher Eaton Zveare uncovered critical flaws in a major automaker's online dealership portal that allowed him to create an admin account with unrestricted access to sensitive customer and vehicle data. The vulnerability bypassed authentication, enabling access to over 1,000 U.S. dealerships' records, personal and financial information, real-time vehicle locations, and even remote-control features like unlocking cars. Zveare demonstrated how easily someone could misuse the system using just a name or VIN. The flaws were quickly patched, but the incident highlights serious authentication and access control weaknesses in automotive dealer systems.

Source

<https://techcrunch.com/>



Ransomware Attack

Ransomware attack disrupts Maryland's public transit service for disabled travelers — MTA says it is investigating cybersecurity incident but core services operating normally

A ransomware attack has hit the Maryland Transit Administration (MTA), disrupting its Mobility service for disabled travelers. The system cannot accept new ride requests or changes, though previously scheduled trips are still being honored. MTA is investigating the breach with the Maryland Department of Information Technology after hackers gained unauthorized access to certain systems. The agency confirmed that other services, including buses, Metro Subway, Light Rail, MARC trains, and commuter buses, continue to operate normally. The incident reflects a broader trend, as ransomware gangs have increasingly targeted public transit, with cities in Missouri and Virginia experiencing similar disruptions in the past.

Source

<https://www.mta.maryland.gov/>



ISO26262 Certification

Hyundai Mobis acquires semiconductor development process certification for ISO 26262 ASIL-D

Hyundai Mobis has earned ISO 26262 ASIL-D certification, the highest safety grade for automotive semiconductors, covering its entire R&D process. Certified by Germany's Exida, it guarantees future chips meet strict global safety standards with over 99% reliability. Backed by its 2021 Autron acquisition, the company is producing 16 semiconductor types this year with output topping 20 million units and is developing 11 new chips for battery management, lighting, communication, and network SoCs within three years. Hyundai Mobis said the certification enhances its competitiveness as automakers demand proven safety standards and will share expertise to grow the semiconductor ecosystem through projects like smart lighting chips with Global Technologies and drive semiconductors with Dongwoon Anatech.

Source

<https://www.mobis.com/>



PATENT

The editor's shortlist

Patents of the month

Patents of the month

Published in August 2025

Shortlisted and summarized by our analyst

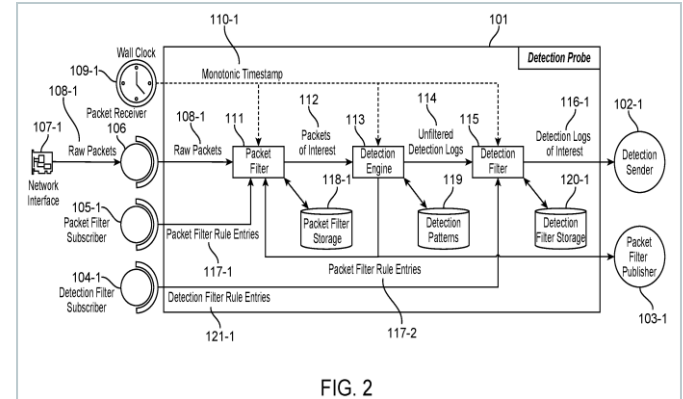
- [US12388857B1](#) - Adaptive network threat detection in distributed automotive execution environments of connected vehicles
[Assignee: VicOne Corp](#)
- [US12389231B2](#) - Method for securing communication between a communication system of a vehicle and a vehicle-external server
[Assignee: Mercedes Benz Group Ag](#)
- [US12401670B2](#) - Cyber security restoration engine
[Assignee: Darktrace Holding Ltd](#)
- [EP4597344A1](#) - Attack analysis device, attack analysis method, and attack analysis program
[Assignee: Nippon Denso Co](#)
- [EP3697056B1](#) - System and method for securing an in-vehicle network
[Assignee: Argus Cyber Security Ltd](#)
- [JP7722563B2](#) - Attack source identification system, attack source identification method and program
[Assignee: NTT Corp](#)
- [KR20250124468A](#) - Security network system mounted inside vehicle and communication method of the same
[Assignee: Samsung Electronic Co Ltd](#)
- [KR20250124785A](#) - Device and method for cancellation of signal injection attacks in PLC-based electric vehicle charging systems
[Assignee: Korea University Industrial & Academic Collaboration Foundation](#)
- [CN120433950A](#) - Network attack detection method applied to vehicle, vehicle and storage medium
[Assignee: BYD Co Ltd](#)
- [CN120567528A](#) - Real-time identification and dynamic defense method and device for train-mounted network attack
[Assignee: National High Speed Train Qingdao Technology Innovation Center](#)



US12388857B1

Adaptive network threat detection in distributed automotive execution environments of connected vehicles

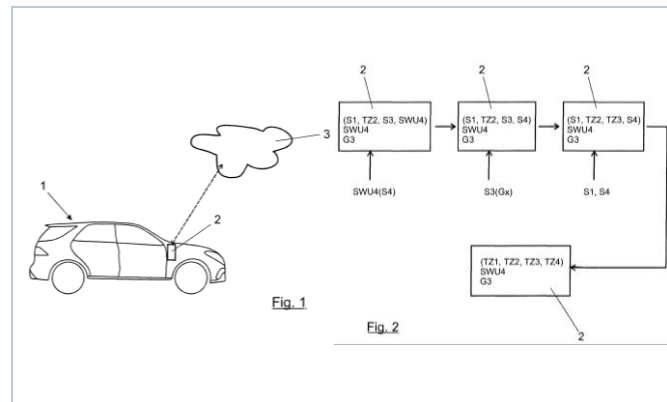
Company name	VicOne Corp
Inventors	Cheng Yi Li, Lu Chih Kang, Chen Zhi Wei, Chen Yi Ting
Priority date	06 Jul 2023
Publication date	12 Aug 2025



This paper describes a cybersecurity system for connected vehicles that detects and prevents network threats. It works by placing small detection units called probes inside different electronic control units (ECUs) of the vehicle, which monitor the vehicle's internal communication networks. These probes first collect raw network data, then filter out irrelevant packets to focus only on suspicious ones. They scan these filtered packets for signs of cyber threats and create logs of any suspicious activity. These logs are further filtered to keep only the most relevant threat data. The filtered logs from multiple ECUs are then combined by a central hub inside the vehicle. Finally, this combined data is sent to a cloud-based backend system, which analyzes it to identify and respond to potential cyberattacks across the vehicle's networks.

◀ US12389231B2

Method for securing communication between a communication system of a vehicle and a vehicle-external server



This patent focuses on securing communication between a vehicle and an external server, especially against future threats from quantum computers that could break today's encryption. It introduces a dual-layer security method: one that uses current encryption techniques and another that is resistant to quantum attacks. The system can switch to the stronger, quantum-resistant method when needed, either through a separate interface or a software update. It ensures that the necessary cryptographic keys are safely stored in the vehicle and allows for a one-way upgrade, meaning once the system switches to quantum-safe encryption, it cannot revert to the older, less secure method. This future-proofs vehicle communications against evolving cyber threats.

Company name Mercedes Benz Group Ag

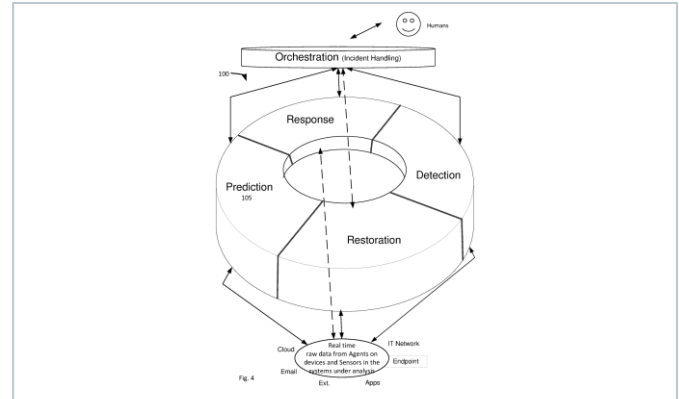
Inventors Friesen Viktor,
Pavlovic Viktor

Priority date 02 Feb 2021

Publication date 12 Aug 2025

◀ US12401670B2

Cyber security restoration engine



This patent introduces an AI-powered cybersecurity restoration engine that improves how systems recover from cyberattacks. Traditional incident responses follow a fixed step-by-step process, which limits adaptability during an ongoing threat. This invention solves that by enabling autonomous remediation, where the engine can independently restore compromised parts of a system and return them to a safe state. It also includes a communication module that works with other AI engines responsible for detecting and mitigating threats, allowing coordinated action during an attack. The system adapts in real time, meaning recovery can begin even while the attack is still happening, ensuring faster and more resilient protection.

Company name Darktrace Holding Ltd

Inventors Simon David Lincoln,
Stockdale Jack,
Dunn Matthew

Priority date 20 Feb 2018

Publication date 26 Aug 2025

EP4597344A1

Attack analysis device, attack analysis method, and attack analysis program

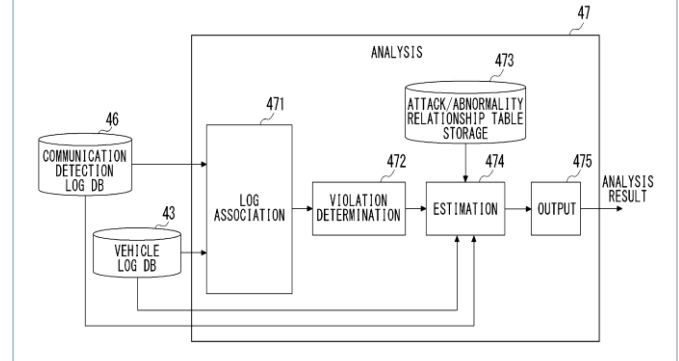
Company name Nippon Denso Co

Inventors Ikuse Tomonori,
Egawa Masumi,
Abe Taiji,
Utsunomiya Hiroyuki,
Nagara Keigo

Priority date 30 Sep 2022

Publication date 06 Aug 2025

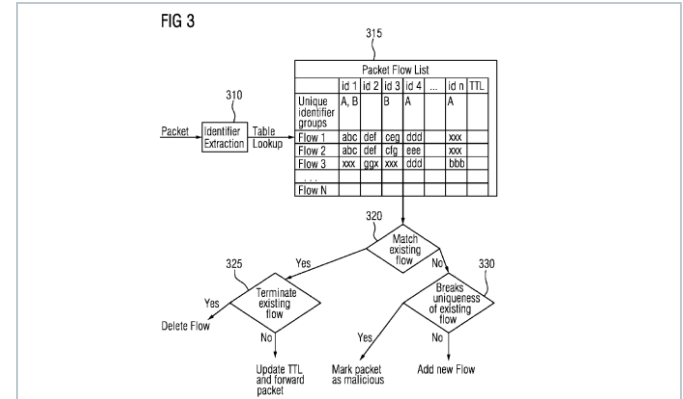
FIG. 6



This patent tackles the growing threat of cyber-attacks on modern vehicles that use advanced electronic control systems and external communication technologies like Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I). It introduces an attack analysis device that monitors both internal system logs and external communication logs to detect suspicious activity. The device checks if these logs match known types of cyber-attacks and determines whether any part of the vehicle's control system has been compromised. By linking internal and external data, it improves the accuracy of threat detection and helps identify violations more reliably. The system also uses multiple layers of defense within the vehicle to strengthen protection against cyber threats.

EP3697056B1

System and method for securing an in-vehicle network



This patent solves a major security flaw in network communications where attackers can sneak in harmful data packets by exploiting lower layers of the network that aren't usually checked. The invention solves that by strengthening security and verifying both the network-level and application-level identifiers of incoming packets. When a packet arrives, the system checks if its identifiers match those of known, legitimate sessions. If something doesn't add up, the packet can be flagged, logged, or blocked. This approach allows each message fragment to be authenticated individually, improves detection of spoofed or unauthorized packets, and keeps session data updated in real time based on actual traffic patterns.

Company name Argus Cyber Security Ltd

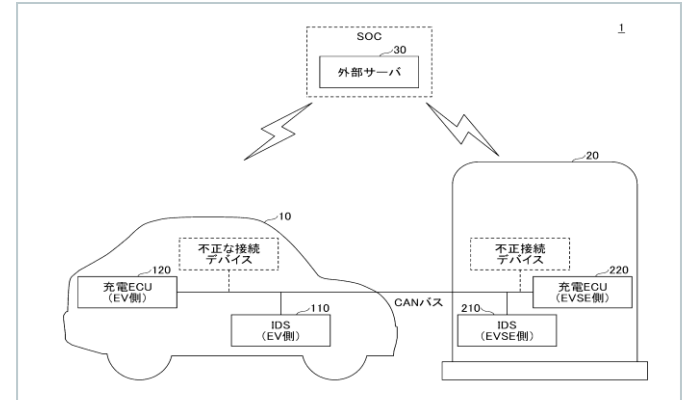
Inventors Geynis Amit,
Atad Matan,
Ben Noon Ofer

Priority date 18 Feb 2019

Publication date 20 Aug 2025

◀ JP7722563B2

Attack source identification system, attack source identification method and program



This patent introduces an approach for identifying the source of cyber-attacks targeting electric transport devices like EVs and their chargers. The approach uses intrusion detection systems (IDS) installed in both the vehicle and the charger, each equipped with a pre-trained learning model to determine if a known charging control device is responsible for the attack. These IDS units exchange their identification results and compare them to pinpoint the actual source of the attack. This collaborative approach improves the accuracy of identifying malicious devices, enhances threat detection based on learned communication patterns, and strengthens security not just for EVs but also for other electric transport modes like motorcycles and boats.

Company name NTT Corp

Inventors Nagayama Hiroki,
Nagafuchi Yukio,
Miyajima Asami

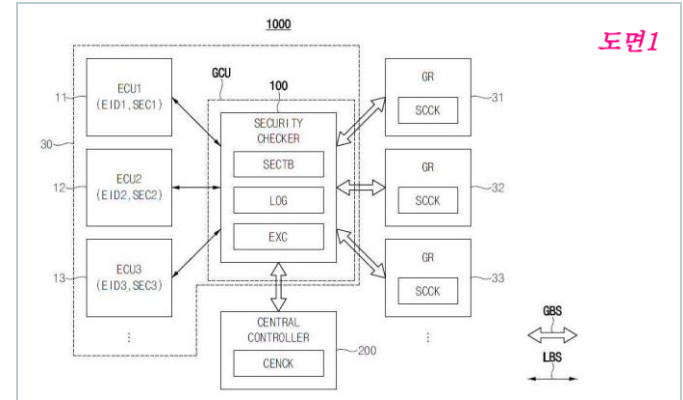
Priority date 31 Mar 2022

Publication date 13 Aug 2025



◀ KR20250124468A

Security network system mounted inside vehicle and communication method of the same



This patent introduces a security network for vehicles that enhances internal communication safety among electronic control units (ECUs). The approach includes a central controller and multiple Group Control Units (GCUs) connected via a global bus, with each ECU linked to a GCU through a local bus. When an ECU sends data, it includes its ID, the recipient's ID, and an authentication code. The GCU checks this information to confirm the sender and validate the message. This way, ECUs don't need to share security details directly, which reduces risks and strengthens overall vehicle cybersecurity.

Company name Samsung Electronic Co Ltd

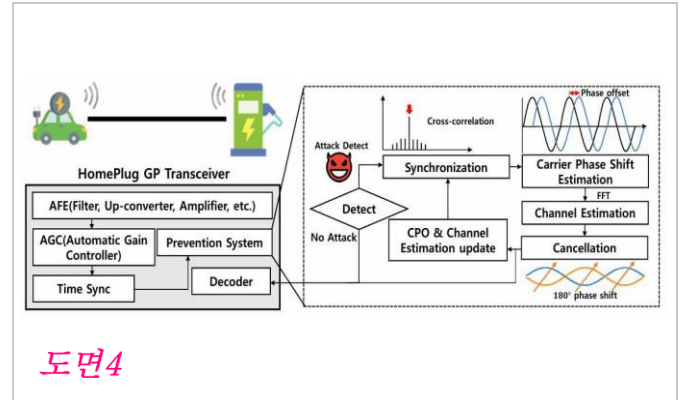
Inventors Jung Yong-taek

Priority date 13 Feb 2024

Publication date 20 Aug 2025

◀ KR20250124785A

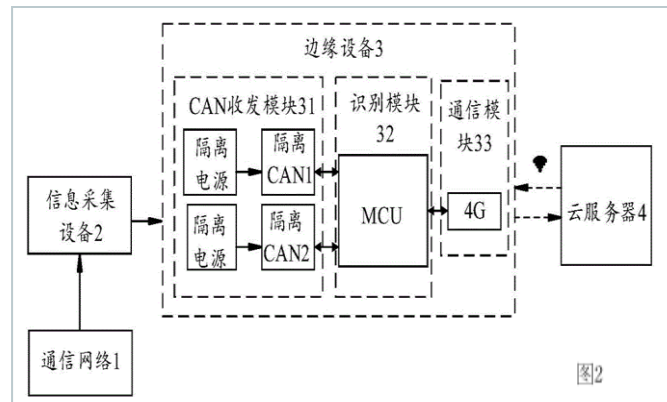
Device and method for cancellation of signal injection attacks in PLC-based electric vehicle charging systems



This invention introduces an approach for protecting electric vehicle charging systems from signal injection attacks during power line communication (PLC), which are cyberattacks where fake signals are inserted into the communication line to mislead the system. When a signal is received, the system identifies a suspicious pattern that may indicate an attack and then estimates its key transmission characteristics. Using this data, it creates a cancellation signal and adds it to the original signal to neutralize any follow-up attacks. This approach is more effective than existing methods, which struggle to detect malicious packets that appear standard, and it helps secure EV charging systems against sophisticated wireless injection threats.

◀ CN120433950A

Network attack detection method applied to vehicle, vehicle and storage medium



This patent talks about detecting cyber-attacks on a vehicle's communication network by analyzing both electrical signals and message content. When a message is received, the system checks the voltage at the physical layer, which is hard to fake, to spot camouflage attacks. It also examines message details from higher layers like the data link and application layers to detect threats such as replay and denial-of-service attacks. By combining these two types of information, physical signals and message verification data, it can accurately identify various attack types. This dual-layer approach improves the reliability and precision of detecting network attacks targeting vehicles.

Company name BYD Co Ltd

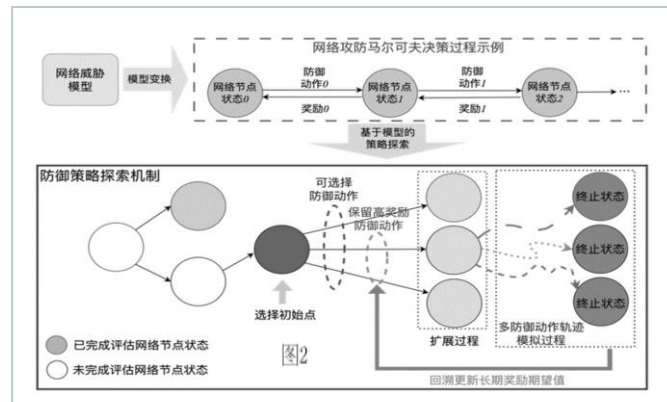
Inventors Yin Xijun,
Wang Ning,
Ma Sijia,
Zhang Hexin,
Sun Baoze

Priority date 25 Nov 2024

Publication date 05 Aug 2025

◀ CN120567528A

Real-time identification and dynamic defense method and device for train-mounted network attack



This patent presents a real-time method for detecting and defending against cyber-attacks on a train's onboard network. It starts by collecting live data from the train's network terminals, including traffic patterns, system logs, and behavior indicators. If an attack is detected, the system identifies its source and type, then uses a pre-trained model to generate several defense strategies such as isolating devices, blocking communication, limiting speed control, switching network links, or enabling encryption. These strategies are evaluated, and the one with the highest score is chosen to respond to the threat. This dynamic approach improves both detection accuracy and defense effectiveness, helping ensure the train's operational safety.

Company name	National High Speed Train Qingdao Technology Innovation Center
Inventors	Du Jiewei, Tao Dongdong Liang Jianying, Liu Weilong Liu Shaoqing, Du Qinghua, Jia Dongxiao,
Priority date	23 Jun 2025
Publication date	29 Aug 2025

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
- Records
- DIAMS IP Management Software
- Patent Search & Analysis

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