

Report of December 2024

Cybersecurity in mobility

Recent developments

Curated and summarized - Industry and Patent news

Published by Denndemeyer India Private Limited

Parag Thakre (pthakre@denndemeyer.com)

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

- ❑ Automotive OEMs are relying more on suppliers to provide certified solutions that meet global cybersecurity standards to protect in-vehicle systems from hacking. For instance, Phison became the first NAND controller supplier to achieve ISO/SAE 21434 certification, ensuring its NAND flash controllers used to provide storage solutions, meet crucial automotive security standards.
- ❑ Recent patents focus on Intrusion Detection and Prevention Systems (IDPS) for vehicle convoys to enhance safety. These systems use on-board units to collect real-time data from vehicles, comparing it to policies and norms. When deviations are detected, the system mitigates the security threats.
- ❑ Additionally, many inventions describe online anomaly detection systems for automobile CAN networks, using cloud servers to train models based on regional traits, user profiles, and threats. These models are sent to vehicle terminals to detect abnormalities, with real-time data sent back to improve detection.
- ❑ Leading tech companies are forming strategic partnerships to boost vehicle cybersecurity. AVL Software and PlaxidityX are prioritizing safety-critical systems with real-time monitoring, while VicOne and Samsung Semiconductor are using threat detection and machine learning to secure software-defined vehicles. VVDN and SecureThings.ai are developing cybersecurity solutions for connected and infotainment systems.
- ❑ Trend Micro's Zero Day Initiative (ZDI) found vulnerabilities in Mazda's car infotainment systems, allowing attackers to execute root code via a malicious USB device due to improper user input sanitization in the Mazda Connect Connectivity Master Unit (CMU), leading to a total system compromise.

Cybersecurity Solutions

AVL Software and Functions and PlaxidityX Collaborate to Protect Safety-Critical Vehicle Systems from Cyber Threats

AVL Software and Functions has teamed up with PlaxidityX to enhance the cyber security of its Ajunic® software platform. This partnership integrates PlaxidityX's intrusion detection and prevention systems (IDPS) into AVL's high-performance ECU solutions, protecting vehicles from cyber-attacks. This is crucial as vehicles become more connected and software-driven. The collaboration helps manufacturers meet security regulations without needing extensive in-house expertise. The Ajunic® platform, used for autonomous driving and battery management, will now include real-time threat monitoring and compliance with new standards, addressing the growing cyber security needs in the automotive industry.

Source

<https://plaxidityx.com/>



Partnership

VicOne Effectively Expands Its Partner Ecosystem and Welcomes Leading Chip Manufacturer to Enhance SDV Cybersecurity

VicOne and Samsung Semiconductor have partnered to enhance cybersecurity in software-defined vehicles (SDVs). They will integrate VicOne's xCarbon™ intrusion detection and prevention system (IDPS) with Samsung's Exynos Auto V920 chip. This collaboration aims to protect SDVs from cyber threats, ensuring safety and compliance with regulations. The combined solution will use real-time threat detection and machine learning to adapt to new threats. VicOne will showcase this technology at the electronica trade fair in Munich and the CES in Las Vegas, highlighting its comprehensive cybersecurity software and services for the automotive industry.

Source

<https://vicone.com/>



Collaborations

VVDN and SecureThings.ai Collaborate to Enhance Cybersecurity for Industry Solutions

VVDN Technologies has signed an MoU with SecureThings.ai to enhance cybersecurity for automotive, IoT, and cloud solutions. This partnership will integrate SecureThings.ai's advanced cybersecurity into VVDN's products, including vehicle connectivity and in-vehicle infotainment. The collaboration aims to meet global cybersecurity standards like ISO 21434. Key initiatives include real-time intrusion detection, continuous threat monitoring, and setting up a security research lab. This partnership will help VVDN deliver secure automotive solutions and comply with evolving cybersecurity regulations, ensuring robust protection for connected vehicles and IoT ecosystems.

Source

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



Certification

Phison Becomes the World's First NAND Controller Independent Supplier to Achieve ISO/SAE 21434 Certification

Phison Electronics has achieved ISO/SAE 21434 certification for automotive cybersecurity, becoming the first independent NAND controller supplier to do so. This certification ensures that Phison's automotive-grade solutions meet global cybersecurity standards, protecting in-vehicle systems from hacking. The certification process took about a year and involved extensive internal and external audits. Phison's CEO, K.S. Pua, highlighted that this milestone enhances the security and reliability of their products, boosting customer trust and competitiveness. This certification is crucial for meeting regulatory requirements, especially in the European market, and positions Phison as a leader in automotive cybersecurity.

Source

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



Mazda's infotainment systems hack

Unpatched Vulnerabilities Allow Hacking of Mazda Cars: ZDI

Trend Micro's Zero Day Initiative (ZDI) has found vulnerabilities in the infotainment systems of several Mazda car models, which could allow attackers to execute code with root privileges. These issues stem from the Mazda Connect Connectivity Master Unit (CMU) not properly sanitizing user input, enabling attackers to send commands via a specially crafted USB device. These flaws could result in a total system compromise, as several security defects, including CVE-2024-8355, CVE-2024-8359, CVE-2024-8360, CVE-2024-8358, CVE-2024-8357, and CVE-2024-8356, permit various attacks like SQL injection and OS command injection. Mazda has not yet patched these vulnerabilities.

Source

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



PATENT

The editor's shortlist

Patents of the month

Patents of the month

Published in November 2024

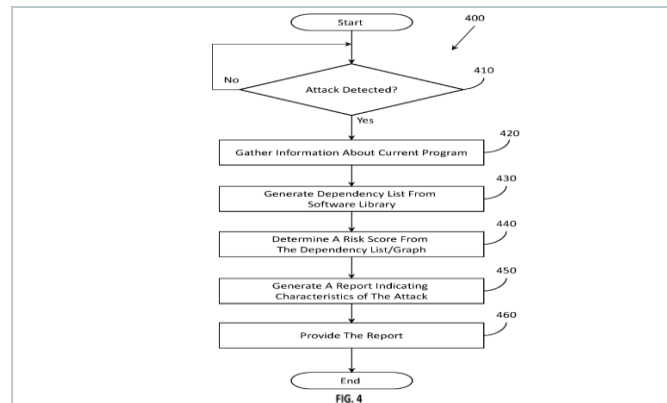
Shortlisted and summarized by our analyst

- [US12139169B2](#) - System and method for detecting exploitation of a component connected to an in-vehicle network
[Assignee: Argus Cyber Security](#)
- [US20240388915A1](#) - Enhanced vehicle to everything (V2X) cybersecurity capabilities
[Assignee: Qualcomm Inc](#)
- [US12143363B2](#) - CANBUS cybersecurity firewall
[Assignee: AT&T Inc](#)
- [US2024388441A1](#) - Secure controller area network in vehicles
[Assignee: Panasonic Holdings Corp](#)
- [US20240378137A1](#) - Computer-implemented method and system for learning-based anomaly detection in order to determine a software error in a networked vehicle
[Assignee: Bayerische Motoren Werke \(BMW\) AG](#)
- [WO2024243128A1](#) - System and method for adaptive method for automotive intrusion detection and prevention system for vehicles driving in convoy form or platooning
[Assignee: Robert Bosch](#)
- [EP4465606A1](#) - Abnormality detection device and abnormality detection method
[Assignee: Panasonic Intellectual Property Corp](#)
- [IN202417023749A](#) - Universal intrusion detection and prevention for vehicle networks
[Assignee: Sonatus Inc](#)
- [CN118906998A](#) - Abnormality detection method, device, equipment and medium for charging CAN interface
[Assignee: Guangzhou Xiaopeng Motors Technology Co Ltd](#)
- [CN111988342B](#) - Online automobile CAN network anomaly detection system
[Assignee: Dalian University Of Technology](#)



◀ US12139169B2

System and method for detecting exploitation of a component connected to an in-vehicle network



The patent addresses critical cybersecurity challenges faced by modern vehicles, especially autonomous fleets. It implements a robust detection mechanisms for unauthorized exploitation attempts while enhancing fleet management capabilities through centralized threat analysis. It involves monitoring the behavior of different vehicle components and identifying any unusual activity. This could include unauthorized software execution, unusual data transfers, or attempts to access sensitive systems. When such suspicious activity is detected, the system can take various actions like blocking the malicious activity, alerting the driver, or even remotely disabling certain vehicle functions to prevent further damage.

Company name Argus Cyber Security

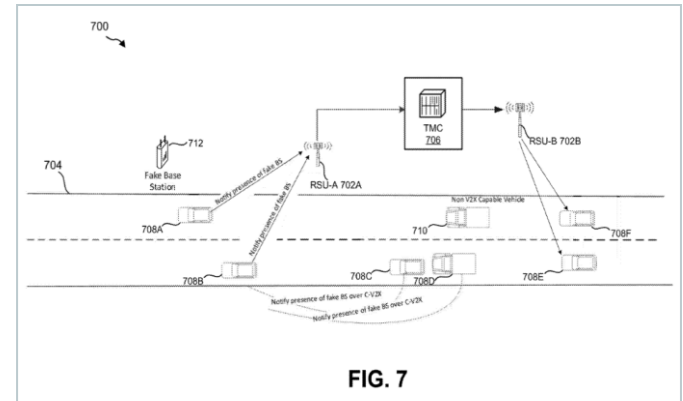
Inventors Galula Yaron,
Kruvi Nizzan

Priority date 10 Aug 2017

Publication date 12 Nov 2024

◀ US20240388915A1

Enhanced vehicle to everything (V2X) cybersecurity capabilities



This patent addresses the need for better cybersecurity in vehicle-to-everything (V2X) communications, as the increasing connectivity of vehicles makes them susceptible to wireless threats that can impact safety. The solution is a vehicular system equipped with a processor and memory that detects potential threats through wireless signals. When a threat is detected, the system creates a detailed report that includes information such as location, time, confidence levels, and threat scores, which is then sent to network nodes or other vehicles for further action.

Company name Qualcomm Inc

Inventors Shuman Mohammed Ataur Rahman,
Das Soumya,
De Subrata Kumar

Priority date 16 May 2023

Publication date 21 Nov 2024



◀ US12143363B2

CANBUS cybersecurity firewall

Company name AT&T Inc

Inventors Adams Steven, Langevin Maureen,
Murphy Christine, Avino Toby,
Liefert John, O'hern William,
Sheleheda Daniel, Ramachandran Jayaraman

Priority date 06 Dec 2021

Publication date 12 Nov 2024



Summarized by Deninemeyer

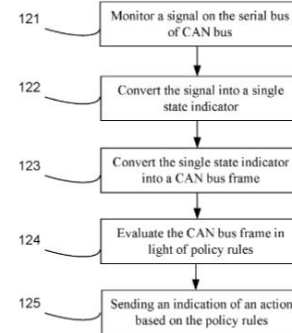


FIG. 2

This patent tackles the growing threat of cyber-attacks on vehicles using Controller Area Network (CAN) bus technology, which can endanger vehicle safety by allowing malicious traffic to move across interconnected systems, especially in automated and connected vehicles. The solution is a CAN bus cybersecurity firewall that monitors signals on a vehicle's CAN bus network. It includes a processor and memory that convert signals into CAN bus frames, compare them against predefined policy rules, and decide whether to take actions based on matches. If alert actions exceed a certain threshold without any allowed actions within a given timeframe, the system can drop the traffic.

◀ US2024388441A1

Secure controller area network in vehicles

Company name Panasonic Holdings Corp

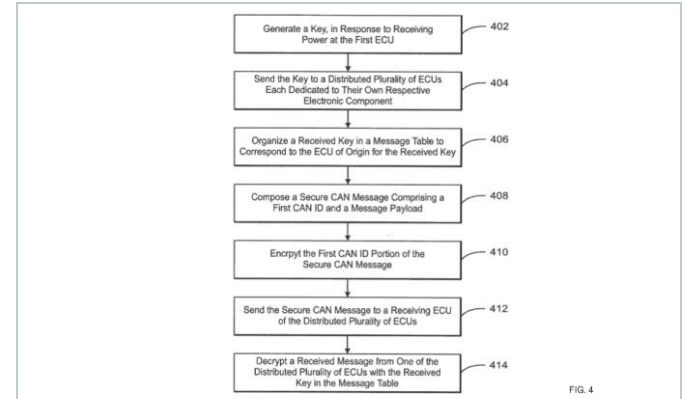
Inventors Kalaiselvam Kumaresh,
Muthiah Muthuganesan

Priority date 03 Oct 2018

Publication date 21 Nov 2024



Summarized by Denne Meyer



This patent addresses security vulnerabilities in vehicle controller area networks (CAN), where electronic controller units (ECUs) communicate without encryption, making data prone to interception and tampering. The solution is a system and method for creating a secure CAN by enabling encrypted communication between ECUs. Each ECU generates a unique key when powered up, these keys are exchanged securely among ECUs and stored in a message table. The CAN ID portion of messages is encrypted using the generated key before transmission, while the payload remains unencrypted due to its contextual nature. The encrypted CAN ID is then decrypted using the second key from the message table associated with the receiving ECU.

◀ US20240378137A1

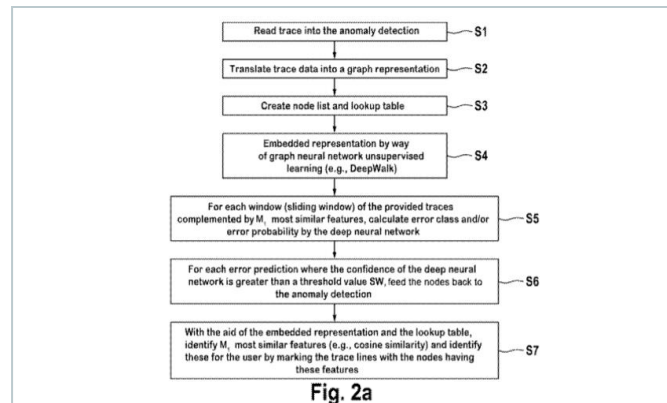
Computer-implemented method and system for learning-based anomaly detection in order to determine a software error in a networked vehicle

Company name Bayerische Motoren Werke AG

Inventors Frickenstein Alexander,
Kowol Maik

Priority date 22 July 2021

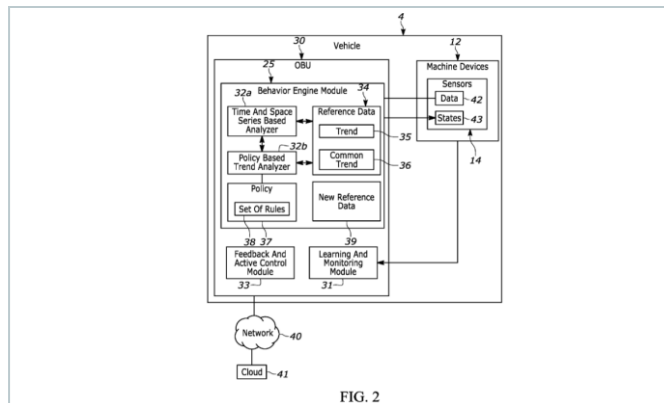
Publication date 14 Nov 2024



This patent addresses the challenge of detecting software errors in networked vehicles, where traditional testing methods struggle due to limited data collection during real-world use, making it difficult to efficiently identify and fix issues. The solution is a computer-implemented method using learning-based anomaly detection with graph neural networks (GNNs) and deep neural networks (DNNs). It works by translating diagnostic trace lines from a vehicle's controller into an undirected graph with nodes representing data segments. The GNN analyzes these nodes to identify features showing similarities and dependencies, and the features are fed into a DNN to output error probabilities or anomaly classes.

WO2024243128A1

System and method for adaptive method for automotive intrusion detection and prevention system for vehicles driving in convoy form or platooning



The patent addresses the need for better intrusion detection and prevention systems (IDS) in vehicles, especially those in convoy configurations, due to increased cyber-attack vulnerabilities. The solution involves an on-board unit that receives real-time data from multiple vehicles in a convoy, comparing it against predefined policies and normal operational trends. If deviations and policy violations are detected, the system mitigates potential threats. Improvements include real-time monitoring of vehicle behavior, using statistical methods and machine learning for robust analysis, and a leader vehicle model for centralized communication. This approach enhances security by effectively detecting and responding to anomalies in convoy driving scenarios.

Company name Robert Bosch

Inventors Merchan Jorge,
Gehrer Stefan,
Kolycheva Ekaterina,
Gehrmann Tobias

Priority date 19 May 2023

Publication date 28 Nov 2024

EP4465606A1

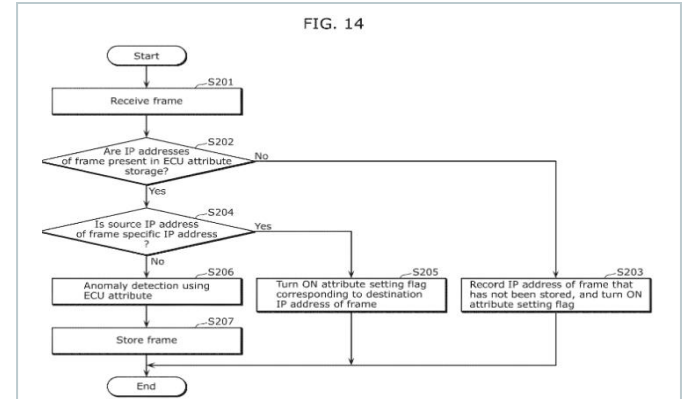
Abnormality detection device and abnormality detection method

Company name Panasonic Intellectual Property Corp

Inventors Adachi takahiro,
Ujiie yoshihiro,
Kishikawa takeshi

Priority date 14 Jan 2022

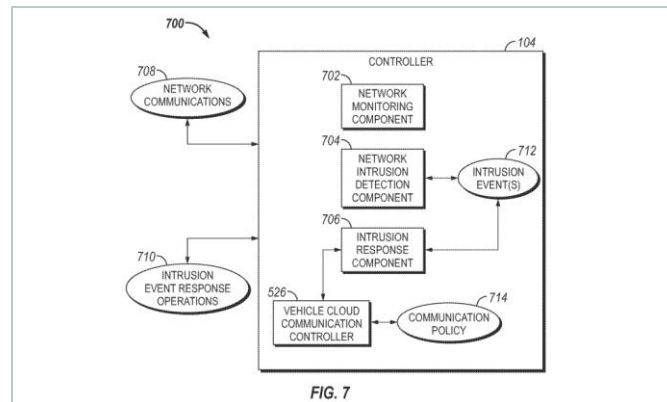
Publication date 20 Nov 2024



This patent addresses the difficulty of detecting unusual communication within vehicles that have multiple ECUs and networks, especially as system updates or new functions can change communication patterns and pose safety risks. The solution is an anomaly detection device that uses a storage system for ECU attributes, which define each ECU's function and data types it handles. It includes a communicator for message transmission and an anomaly detector that identifies abnormal communication based on the attributes of the source and destination ECUs. This method allows for real-time monitoring and updates of ECU attributes to adapt to evolving communication patterns.

◀ IN202417023749A

Universal intrusion detection and prevention for vehicle networks



This patent outlines a system designed to protect mobile applications like vehicles, which face growing cybersecurity threats due to their increased connectivity to external networks for services like entertainment and maintenance. The system aims to mitigate risks like malware, ransomware, and unauthorized access that can disrupt operations and compromise sensitive data. It includes a vehicle with multiple network zones, each having various endpoints, and a controller with components for network monitoring, intrusion detection, and response. The network monitoring component analyzes communication within the zones, the intrusion detection component identifies any potential security breaches, and the intrusion response component takes action to counteract detected threats.

Company name Sonatus Inc

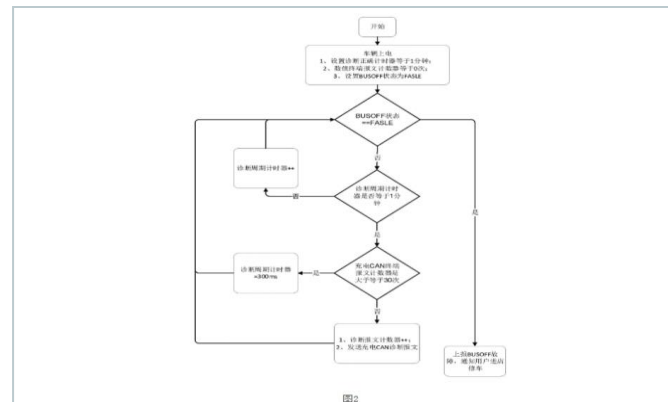
Inventors Fang yu,
Ling andrew,
Valenzuela felipe andres valdes,
Zong xuanran,
Dhankhar sudhir ramphal,
Chai fangming

Priority date 08 Oct 2021

Publication date 08 Nov 2024

◀ CN118906998A

Abnormality detection method, device, equipment and medium for charging CAN interface



This patent addresses the challenge of detecting abnormalities in the charging Controller Area Network (CAN) interface of electric vehicles, where current methods rely on user-initiated checks during charging failures, causing delays in fault identification and inefficient maintenance. The solution is a real-time anomaly detection method that starts immediately when the vehicle is powered on, checking if the charging CAN interface is in a normal state and sending diagnostic messages at regular intervals. The system then analyzes the feedback to identify any discrepancies that indicate abnormal conditions.

Company name Guangzhou Xiaopeng Motors Technology Co Ltd

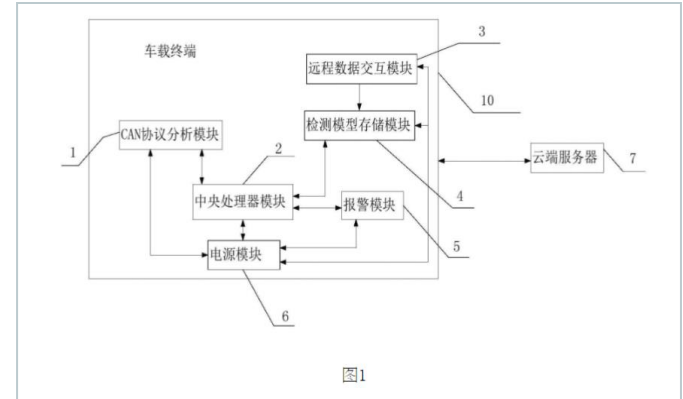
Inventors Zhang Ming

Priority date 27 Aug 2024

Publication date 08 Nov 2024

◀ CN111988342B

Online automobile CAN network anomaly detection system



This patent presents an online anomaly detection system for automobile CAN networks to enhance security as vehicles become more connected. Traditional safety methods like identity verification & encryption, are inadequate due to high computational demands and limited real-time adaptability. The proposed system uses a cloud server to train an anomaly detection model based on regional traits, user profiles, vehicle characteristics, and emerging threats. The cloud server transmits the trained model to different vehicle-mounted terminals to detect CAN network abnormality of the automobile, and meanwhile, the vehicle-mounted terminals transmit real-time data of the automobile to cloud server to update the CAN network abnormality detection model for improved threat detection.

Company name Dalian University Of Technology

Inventors Liu Pengbo,
Peng Haide,
Zhao Jian

Priority date 18 Sep 2020

Publication date 22 Nov 2024



We are now in India

Your global full-service IP partner

With **60 years of experience** and **23 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 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
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



Visit us

at www.dennemeyer.com to find out more about us.

 Denнемeyer India Private Limited
Bengaluru
info-india@denнемeyer.com

 North & East India
+91 79831 15166

South & West India
91 88266 88838

