

Report of September 2024

# Cybersecurity in mobility

Recent developments

Curated and summarized - Industry and Patent news

Published by Denne Meyer India Private Limited

Parag Thakre ( [pthakre@denne Meyer.com](mailto:pthakre@denne Meyer.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

- ❑ Railways, as critical infrastructure, depend heavily on secure signaling systems for safe operations. Neglecting cybersecurity in these systems poses significant risks. The collaboration between RailTel and Cylus aims to use advanced technologies to strengthen railway signaling system security, ensuring continued reliability and resilience against cyber threats.
- ❑ Tech giants like Amazon are actively supporting automakers in meeting UNECE Regulations UN155 by offering specialized technology solutions such as device connectivity, management and security monitoring for connected vehicle security.
- ❑ The Federal Aviation Administration (FAA) is proposing new cybersecurity standards for aircraft. This reflects the growing recognition that cybersecurity is a critical aspect of aviation safety and should be integrated into all stages of aircraft development and operation, like automobiles.
- ❑ Several patent applications have been published to prevent cyberattacks in vehicles and protect against cyberattacks. These patent applications include test cases for automotive cybersecurity detection, generating more relevant attack scenarios, secure communication between vehicle components, and secure messaging schemes for vehicle networks. It is evident that companies are increasingly interested in building security during the early stages of development. .

# Cyberalliance

## **RailTel and Cylus Join Forces to Strengthen Cybersecurity in Indian Railways**

Cylus and RailTel have partnered to strengthen the cybersecurity of Indian railway infrastructure. Cylus will provide its rail-specific cybersecurity solution, CylusOne™, to RailTel. This collaboration will focus on enhancing the security of railway signaling systems, both trackside, onboard, and SCADA systems. Key aspects of the partnership include market expansion, professional services integration, and competence development. Both companies are committed to ensuring the safety and reliability of vital railway technologies in India.

Source

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



# Partnership

## **Sasken partners with Trustonic to bring advanced security options to Automotive OEMs**

Sasken and Trustonic have partnered to offer advanced cybersecurity solutions to automotive OEMs. Sasken, a specialist in product engineering, will leverage Trustonic's world-leading TEE technology, "Kinibi," to provide secure platforms for connected vehicles. With their combined expertise, they aim to deliver cutting-edge, safe, and innovative solutions to the automotive industry. Trustonic's platform, already deployed in billions of devices and millions of vehicles, ensures a robust and secure foundation for OEMs to build upon.

Source

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



# Connected vehicle

## **Securing the future of mobility: UNECE WP.29 and AWS IoT for connected vehicle cybersecurity**

The growing reliance on technology in the automotive industry has made cybersecurity a critical concern. To address this, the United Nations Economic Commission for Europe (UNECE) has introduced new regulations (UNR 155 and 156) to protect these vehicles. These regulations mandate that manufacturers implement cybersecurity throughout the vehicle lifecycle. AWS IoT offers a comprehensive suite of services, including device connectivity, management, security monitoring, and data analytics, to help automotive companies meet these regulations and ensure the security of their connected vehicles.

Source

<https://aws.amazon.com/>



# Cybersecurity Solution

## **Kondukto and ETAS Developing Joint Cybersecurity Solution for the Automotive Industry**

ETAS, has partnered with Kondukto to expand its cybersecurity portfolio with Kondukto's Application Security Posture Management (ASPM) and vulnerability management platform. This collaboration will empower ETAS' automotive OEM partners to gain enhanced visibility into their software supply chain, enabling them to better assess risks and enhance their security posture. Additionally, ETAS customers will benefit from industry-leading security automation capabilities and contextual decision-making support, resulting in faster remediation times and improved overall code quality within the ecosystem.

Source

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





# Regulations

## FAA Proposed New Cybersecurity Rules for Airplanes

The Federal Aviation Administration (FAA) has proposed new cybersecurity regulations for transport category airplanes, engines, and propellers to address growing cyber threats. The proposed changes will be incorporated into Title 14 of the Code of Federal Regulations, specifically parts 25, 33, and 35. The proposed regulation focuses on enhancing the cybersecurity of aircraft systems by introducing new design standards, and require applicants to take design approvals to identify, assess, and mitigate cybersecurity threats in their aircraft systems. The regulations aim to align with international standards and protect against intentional unauthorized electronic interactions (IUEI).

Source

<https://cybersecuritynews.com/>



# Rebranding

## **Introducing PlaxidityX: Argus Cyber Security Ltd. Unveils New Company Name**

Argus Cyber Security has rebranded to PlaxidityX, emphasizing its focus on meeting the future security challenges of the mobility sector. Founded a decade ago, the company has been a pioneer in automotive cyber security, raising awareness and educating the market. The name PlaxidityX signifies the company's comprehensive end-to-end solution and broader market presence, positioning it for accelerated growth and expansion of market share. The company has rebranded to PlaxidityX to reflect its growth, partnerships with leading tech companies, and launches of innovative products like vDome and the DevSecOps platform.

Source

<https://plaxidityx.com/>





PATENT

The editor's shortlist

# Patents of the month

## Patents of the month

Published in August 2024



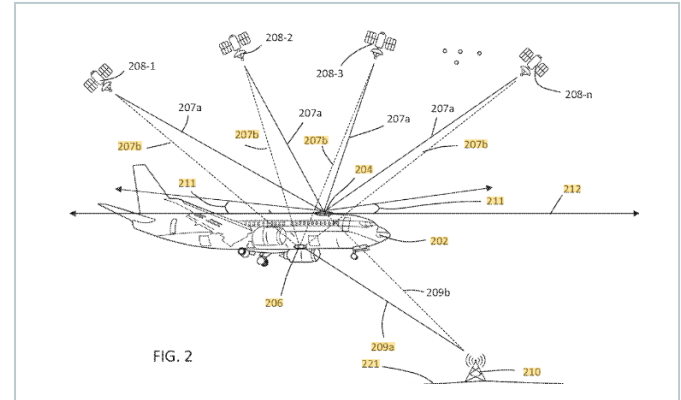
### Shortlisted and summarized by our analyst

- [US20240255650A1](#) - Satellite signal spoofing detection system  
Assignee: Honeywell International Inc
- [US2024264929A1](#) - Method, system and device for generating test case for automotive cybersecurity detection  
Assignee: Catarc Software Testing Tianjin Co Ltd
- [US2024291687A1](#) - Apparatus for secured communication between control devices in a vehicle, electronic processing unit and vehicle  
Assignee: ZF CV System Global GMBH
- [US2024275613A1](#) - Method and system for handling dynamic cybersecurity posture of a V2X entity  
Assignee: BlackBerry Ltd.
- [WO2024170019A1](#) - Method and vehicle for querying service-oriented authorisation in networks  
Assignee: BMW AG
- [WO2024172190A1](#) - Method for evaluating security of vehicle internal network  
Assignee: AHOPE Ltd.
- [EP4413698A1](#) - Sufficiently secure controller area network  
Assignee: University of Michigan
- [EP4105801B1](#) - Using staged machine learning to enhance vehicles cybersecurity  
Assignee: Red Bend (Samsung Group)
- [IN202441056189A](#) - Charge guard: early detection of DDoS attacks at EV charging stations using lightweight micro neural network  
Assignee: Individual Inventor
- [CN118473745A](#) - Vehicle-mounted network intrusion detection method and device, electronic equipment and storage medium  
Assignee: GAC AION NEW ENERGY AUTOMOBILE



« US20240255650A1

## Satellite signal spoofing detection system



The patent proposes a system to detect satellite signal spoofing by comparing signals received from dual antennas strategically placed on different sides of a vehicle. The system compares primary satellite signals received by the primary antenna with secondary satellite signals received by the secondary antenna to determine if a spoofing signal is present. The comparison includes analyzing parameters such as the number of satellites used in position computations, protection limits, and the number of visible satellites. This approach enhances detection capabilities, incorporates multiple data points for comparison, and provides real-time communication regarding detected spoofing threats.

Company name Honeywell International Inc

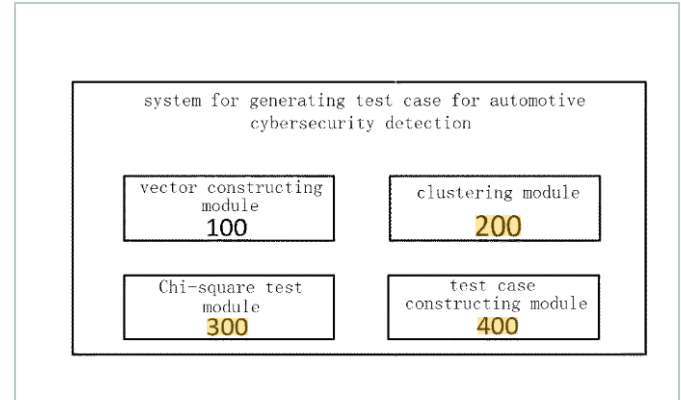
Inventors Kumar Perumal  
Lenka Sanjay

Priority date 01-Feb-2023

Publication date 01-Aug-2024

《 US2024264929A1

# Method, system and device for generating test case for automotive cybersecurity detection



The patent proposes a method to generate test cases for automotive cybersecurity detection by inputting risk assessment results from TARA reports and constructing attack vectors. These vectors undergo cluster analysis and Chi-square testing to identify key impact risks and create risk matching terms. The resulting attack modes are then developed into actionable test case sets. This approach enhances the effectiveness and efficiency of automotive cybersecurity testing by utilizing multi-dimensional information, employing advanced statistical techniques, and facilitating rapid testing while ensuring compliance with regulatory standards.

Company name    Catarc Software Testing Tianjin Co Ltd

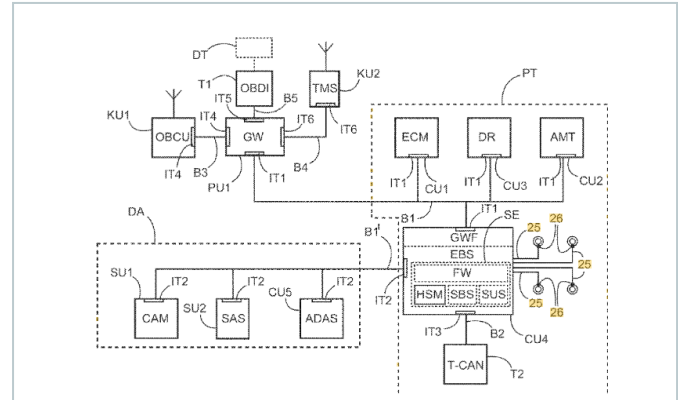
Inventors        He Kexun,  
                      Li Baotian,  
                      Shao Xuebin,  
                      Han Yanyan,  
                      Wang Baizheng,  
                      Shao Wen

Priority date     06-Feb-2023

Publication date 08-Aug-2024

《 US2024291687A1

# Apparatus for secured communication between control devices in a vehicle, electronic processing unit and vehicle



The invention presents a network architecture for securing communication between control units in a vehicle, particularly for use with legacy control units that lack secured CAN transceivers or SecOC (Secure Onboard Communication). The proposed solution allows legacy control units to remain usable while ensuring protection against cyberattacks. It achieves this by using a secured control unit with gateway and firewall functions, thereby avoiding the need for additional separate gateway devices and potentially reducing costs. This solution allows for a mix of secured and vulnerable control units in a vehicle communication bus system while complying with cybersecurity requirements.

Company name ZF CV System Global GMBH

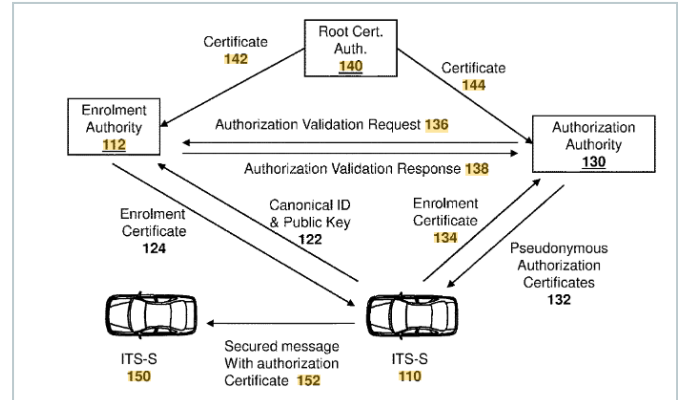
Inventors Rehm Florian,  
Urban Seelmann Christian

Priority date 07-Jul-2021

Publication date 29-Aug-2024

« US2024275613A1

# Method and system for handling dynamic cybersecurity posture of a V2X entity



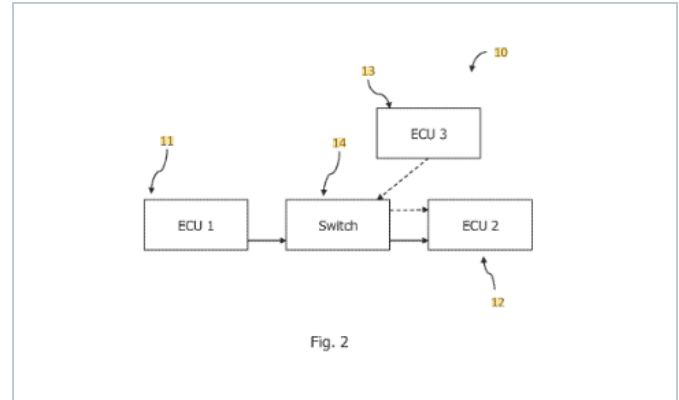
The invention addresses the challenge of ensuring the trustworthiness of messages in ITS (intelligent transportation systems) communications, particularly regarding the cybersecurity of the sending entity. A compromised sending entity could send illegitimate messages that could negatively impact the ITS system. The invention aims to provide a mechanism to assess the cybersecurity posture of sending entities, allowing receiving devices to make informed decisions about the trustworthiness of received messages. This helps to mitigate the risks associated with compromised entities and ensures the reliability and integrity of ITS communications.

Company name	BlackBerry Ltd.
Inventors	Russell Nicholas James, Barrett Stephen John, Vanderveen Michaela
Priority date	29-Apr-2020
Publication date	15-Aug-2024



« WO2024170019A1

## Method and vehicle for querying service-oriented authorisation in networks



The patent proposes a method for communicating access rights within a network of control units in modern motor vehicles. This method involves each unit having an assigned access authorization list that specifies authorized communication partners. By verifying authorizations before data exchanges, the method establishes clear communication boundaries, allows for dynamic updates of authorization relationships, and incorporates service discovery phases. Overall, this patent provides a structured approach to managing data exchange permissions among vehicle control units, significantly improving security against unauthorized access while ensuring operational efficiency.

Company name BMW AG

Inventors Philipp Obergfell  
Thilo Denzer

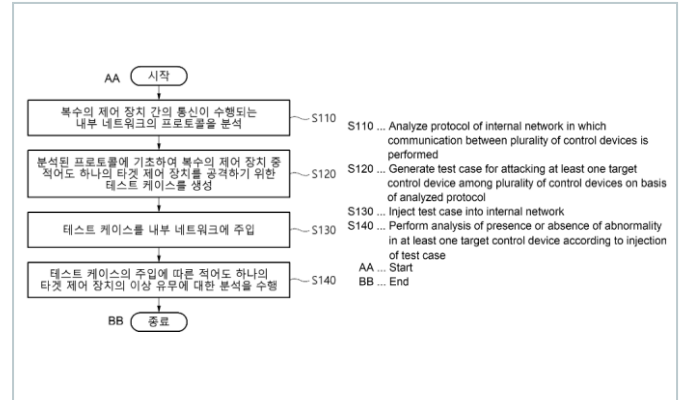
Priority date 17-Feb-2023

Publication date 22-Aug-2024



《 WO2024172190A1

## Method for evaluating security of vehicle internal network



The patent proposes a method for evaluating the security of an in-vehicle network using a computing device. The method involves analyzing communication protocols, generating test cases, injecting these test cases into the internal network, and assessing abnormal behavior in target control devices. The evaluation can be conducted in either HILS or SILS environments. This approach establishes both HILS and SILS testing environments, utilizes fuzzing algorithms to generate tailored attack scenarios, and provides comprehensive monitoring capabilities to identify vulnerabilities. Overall, this patent presents a systematic approach for enhancing vehicle cybersecurity through rigorous testing methodologies.

Company name AHOPE Ltd.

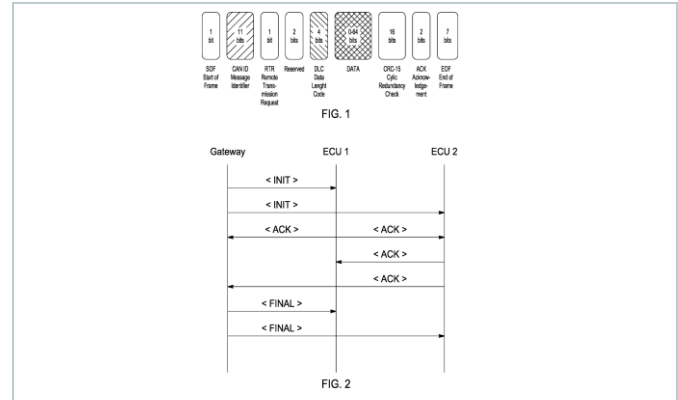
Inventors Jo Sangwon,  
Kim Yeonwoo,  
Lee Wonil

Priority date 13-Feb-2023

Publication date 22-Aug-2024

《 EP4413698A1

# Sufficiently secure controller area network



The invention presents a secure messaging scheme for vehicle networks that addresses the limitations of traditional cryptography-based solutions. The scheme uses bit rotation techniques for encoding and decoding data frames, ensuring security while maintaining performance requirements. It also includes mechanisms for establishing data sessions, authenticating messages, and verifying the authenticity of certificates. This provides a practical and secure solution for the automotive industry, balancing security and performance needs in resource-constrained environments.

Company name University of Michigan

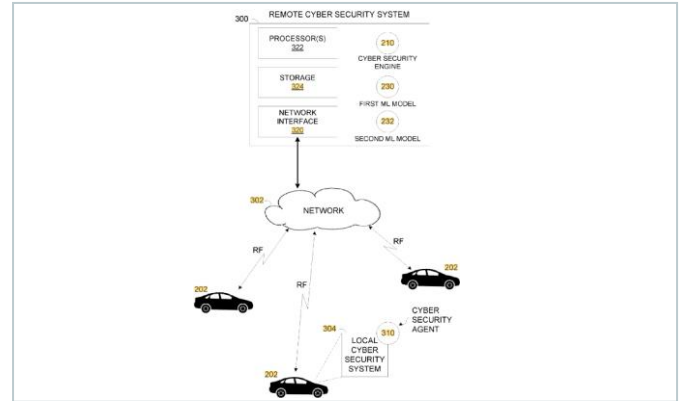
Inventors Pese Mert Dieter  
Shin Kang G.

Priority date 04-Oct-2021

Publication date 14-Aug-2024

《 EP4105801B1

# Using staged machine learning to enhance vehicles cybersecurity



The invention presents a method for detecting potential cyberattacks in vehicle environments using staged machine learning models. The method involves creating feature vectors from vehicle operational data, using unsupervised ML models to detect anomalies, and using supervised ML models to identify potential cyberattack events. The system utilizes a two-stage pipeline, configures the unsupervised model with high recall settings, and reduces the need for extensive labeled training datasets. This approach enhances anomaly detection capabilities and addresses limitations in traditional methods, improving vehicle cybersecurity.

Company name	Red Bend
Inventors	Mendelowitz Shachar, Morgulis Nir
Priority date	14-Jun-2021
Publication date	21-Aug-2024



《 IN202441056189A

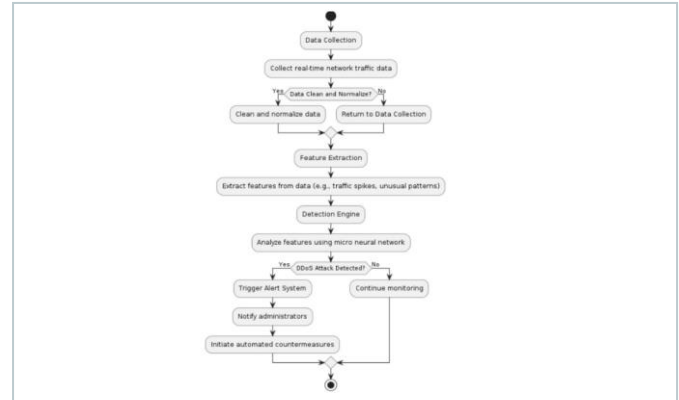
## Charge guard: early detection of DDoS attacks at EV charging stations using lightweight micro neural network

Company name Individual Inventor

Inventors DR RAJAN

Priority date 23-Jul-2024

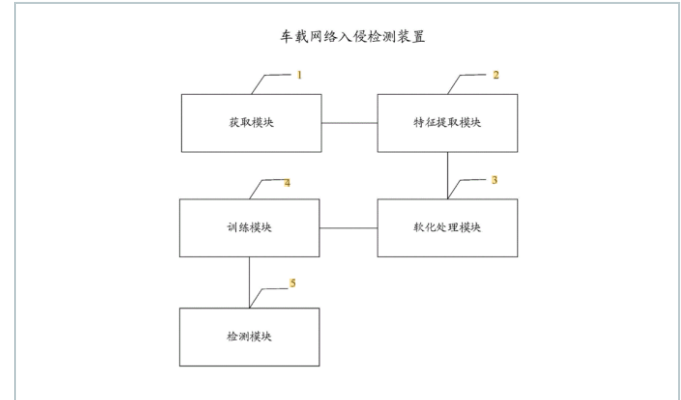
Publication date 02-Aug-2024



The invention presents a novel system for the early detection of DDoS attacks at EV charging stations using a lightweight micro neural network. This system is designed to operate within the constrained hardware environments typically found in EV charging stations, ensuring real-time detection capabilities without necessitating extensive hardware upgrades. The system collects real-time data, preprocesses it, analyzes it using the micro neural network, and triggers alerts upon identifying potential threats. This approach enhances the security and reliability of EV charging infrastructure by providing a robust solution to detect and mitigate potential cyber threats efficiently.

《 CN118473745A

# Vehicle-mounted network intrusion detection method and device, electronic equipment and storage medium



The patent proposes a method for detecting intrusions in vehicle-mounted networks using a two-model approach: a teacher model and a student model. The method involves acquiring preprocessed network data, extracting features using the teacher model to generate prediction probabilities, applying label softening on these probabilities to create softened labels, training the student model based on these softened labels, and finally inputting test data into the trained student model for intrusion detection. This approach enhances precision, improves generalization capability, and reduces false positives/negatives, thereby providing a more effective intrusion detection method for vehicle-mounted networks.

Company name GAC AION NEW ENERGY AUTOMOBILE

Inventors Wang Shumin,  
Yang Wushuang,  
Song Yu

Priority date 11-May-2024

Publication date 09-Aug-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 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





# Visit us

at [www.dennemeyer.com](http://www.dennemeyer.com) to find out more about us.

 Denнемeyer India Private Limited  
Bengaluru  
[info-india@dennemeyer.com](mailto:info-india@dennemeyer.com)

 North & East India  
**+91 79831 15166**

South & West India  
**91 88266 88838**

