Dennemeyer
The IP Group

Report of November 2024

Cybersecurity in mobility

Recent developments

Curated and summarized - Industry and Patent news

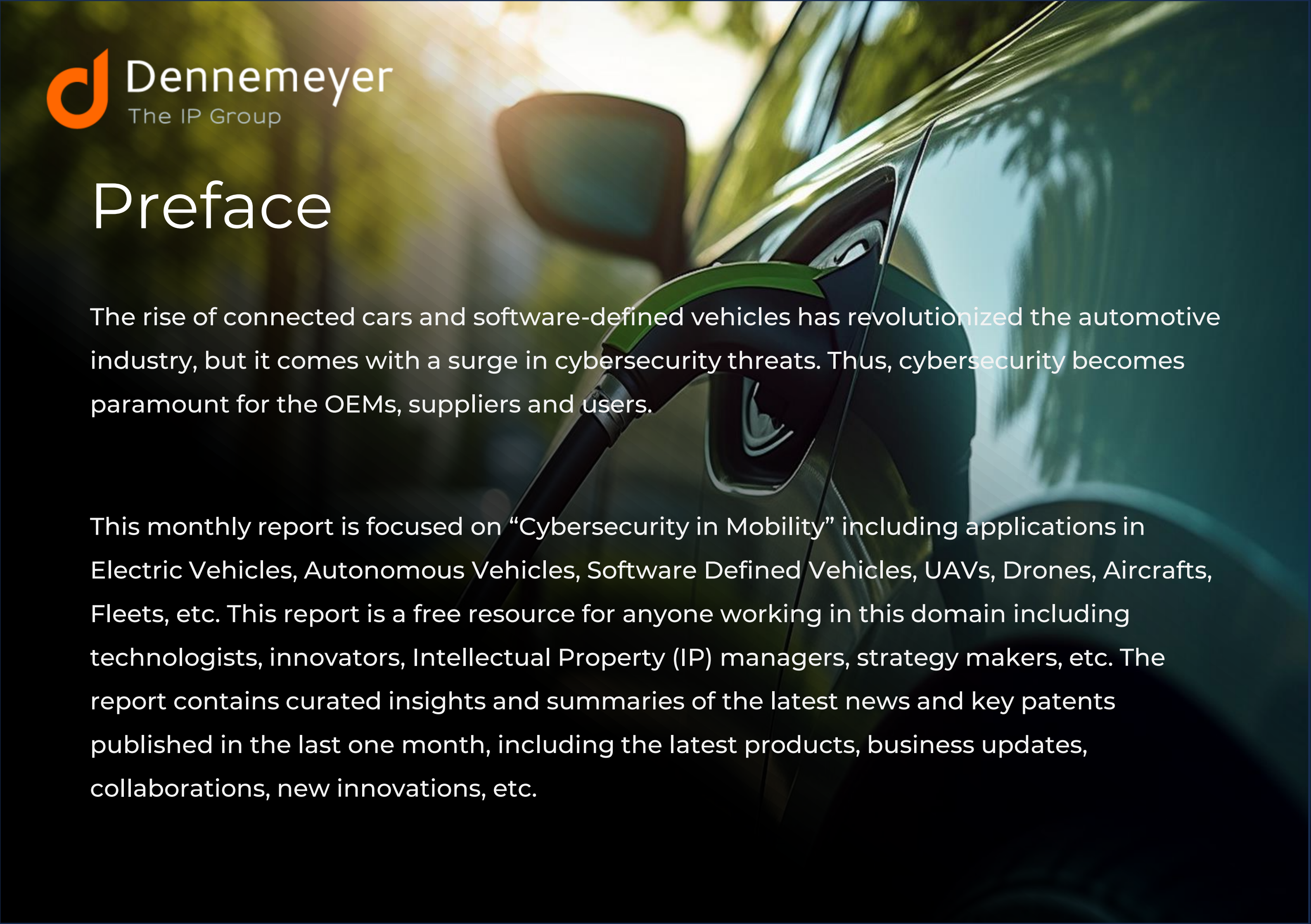
Published by Dennemeyer India Private Limited

Parag Thakre (pthakre@dennemeyer.com)

Dennemeyer
The IP Group

Subscribe now

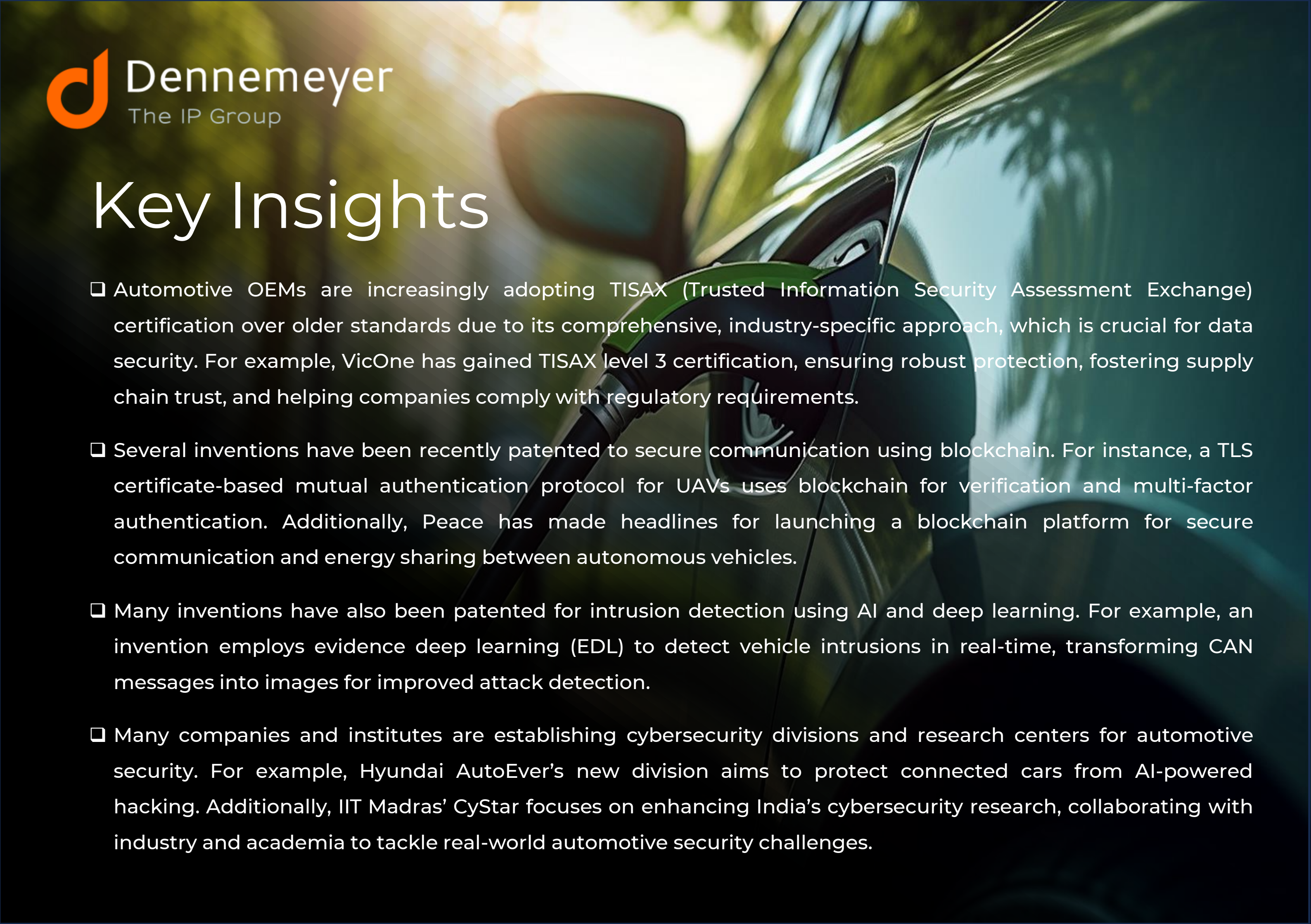
Scan the QR code to receive this monthly report via email in your inbox.



Preface

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

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



Key Insights

❑ Automotive OEMs are increasingly adopting TISAX (Trusted Information Security Assessment Exchange) certification over older standards due to its comprehensive, industry-specific approach, which is crucial for data security. For example, VicOne has gained TISAX level 3 certification, ensuring robust protection, fostering supply chain trust, and helping companies comply with regulatory requirements.

❑ Several inventions have been recently patented to secure communication using blockchain. For instance, a TLS certificate-based mutual authentication protocol for UAVs uses blockchain for verification and multi-factor authentication. Additionally, Peace has made headlines for launching a blockchain platform for secure communication and energy sharing between autonomous vehicles.

❑ Many inventions have also been patented for intrusion detection using AI and deep learning. For example, an invention employs evidence deep learning (EDL) to detect vehicle intrusions in real-time, transforming CAN messages into images for improved attack detection.

❑ Many companies and institutes are establishing cybersecurity divisions and research centers for automotive security. For example, Hyundai AutoEver’s new division aims to protect connected cars from AI-powered hacking. Additionally, IIT Madras’ CyStar focuses on enhancing India’s cybersecurity research, collaborating with industry and academia to tackle real-world automotive security challenges.

Cybersecurity Solutions

Hyundai Motor Group's software unit launches cybersecurity division

Hyundai AutoEver has launched a new cybersecurity division to protect connected cars from increasing cyber threats, particularly AI-powered hacking attacks. With connected cars making up 25% of vehicles in South Korea, Hyundai's Executive Chairman emphasized that security is crucial for survival. Recent incidents, such as the Tesla Model 3 hack in under two minutes, have demonstrated the vulnerability of modern vehicles. To combat these risks, Hyundai AutoEver plans to develop measures to prevent security breaches in connected cars, including the illegal duplication of digital keys and cyberattacks on running vehicles and infotainment systems.

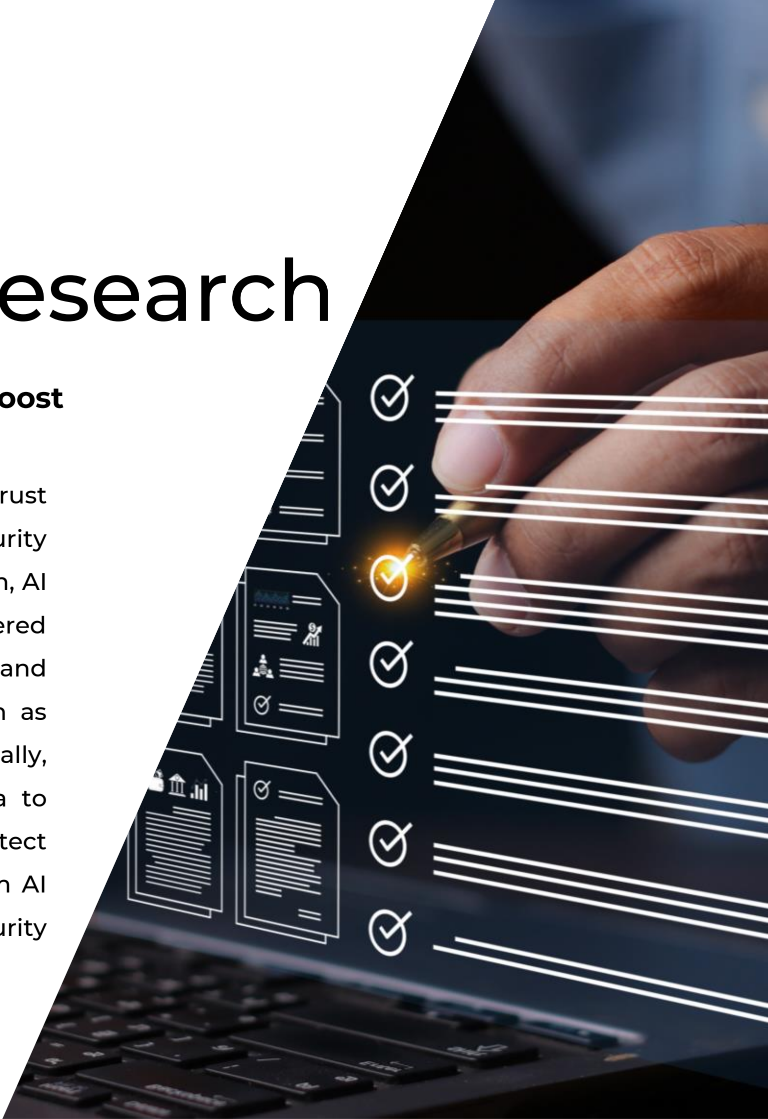
Source
https://www.kedglobal.com/

Strengthening Research

IIT Madras launches Cybersecurity Centre to boost Fundamental & Applied Research in India

IIT Madras has launched the Centre for Cybersecurity, Trust and Reliability (CyStar) to strengthen India's cybersecurity research and innovation. The center focuses on blockchain, AI security, cryptography, and IoT security. CyStar has partnered with companies like Vitesco Technologies, LG India, and Kaspersky to develop solutions for various sectors such as finance, healthcare, and automotive industries. Additionally, IIT Madras will collaborate with industry and academia to address real-world security challenges, aiming to protect critical infrastructure and address emerging threats from AI and quantum computing while training future cybersecurity professionals.

Source
https://www.iitm.ac.in/



Standard Certification

VicOne Achieves TISAX Assessment Level 3 Assuring Customers of Highest Level of Data Protection and Security Excellence

VicOne, a leader in automotive cybersecurity, has earned TISAX (Trusted Information Security Assessment Exchange) Level 3 certification, the highest security standard in the automotive industry. This certification, based on international security standards, guarantees top-level data protection for car manufacturers and their suppliers against cyber threats and is increasingly requested by automotive manufacturers (OEMs) worldwide. In addition to TISAX, VicOne also holds ASPICE CL2 and ISO/SAE 21434 certifications, further showcasing its advanced cybersecurity capabilities. VicOne's achievement enhances cybersecurity, boosts global vehicle data protection.

Source
https://vicone.com/

Blockchain

Peace Launches Blockchain Platform for Secure Autonomous Vehicle Communication and Energy Sharing

Peace, a leading innovator in autonomous vehicle technology, has launched a blockchain-based platform for secure communication and energy sharing between autonomous vehicles. Powered by Rapid Chain, the platform revolutionizes vehicle communication and energy sharing, creating a sustainable ecosystem for autonomous transportation. It prioritizes privacy and security through its decentralized nature. Using blockchain technology, Peace guarantees encrypted, secure, and transparent transactions. Smart contracts automate energy exchanges, while integrated IoT sensors enable real-time data sharing across the connected vehicle network, establishing a reliable transportation infrastructure.

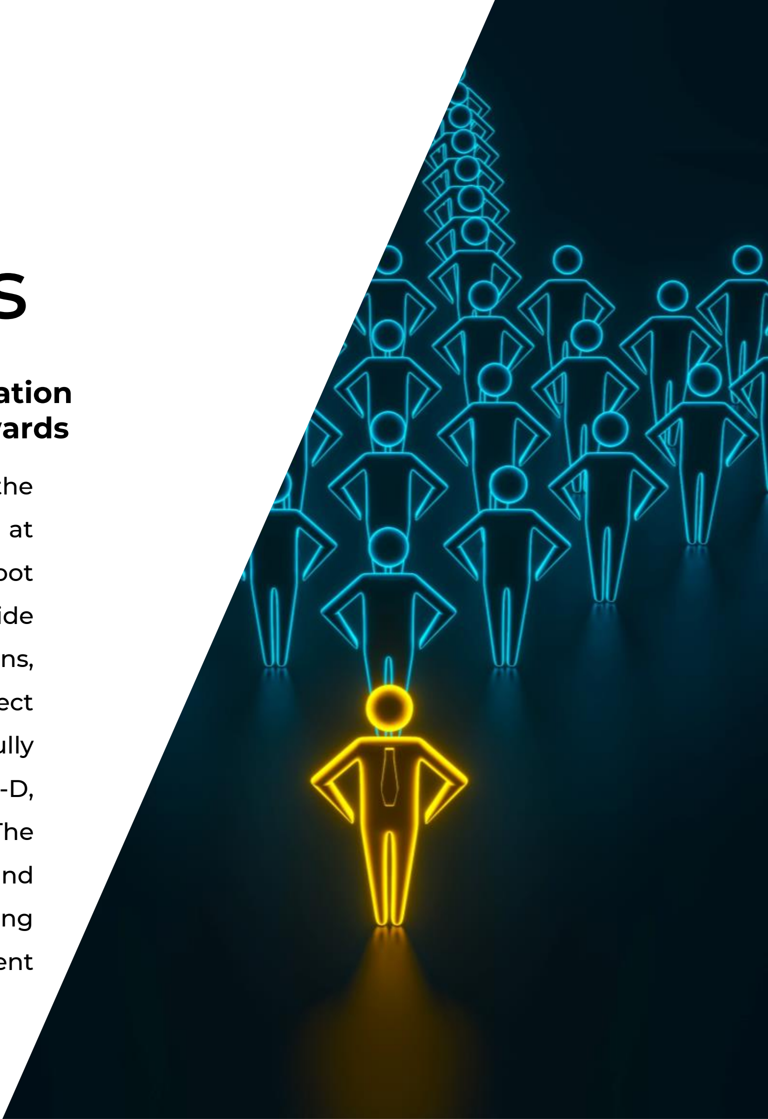
Source
https://www.msn.com/

AutoTech Awards

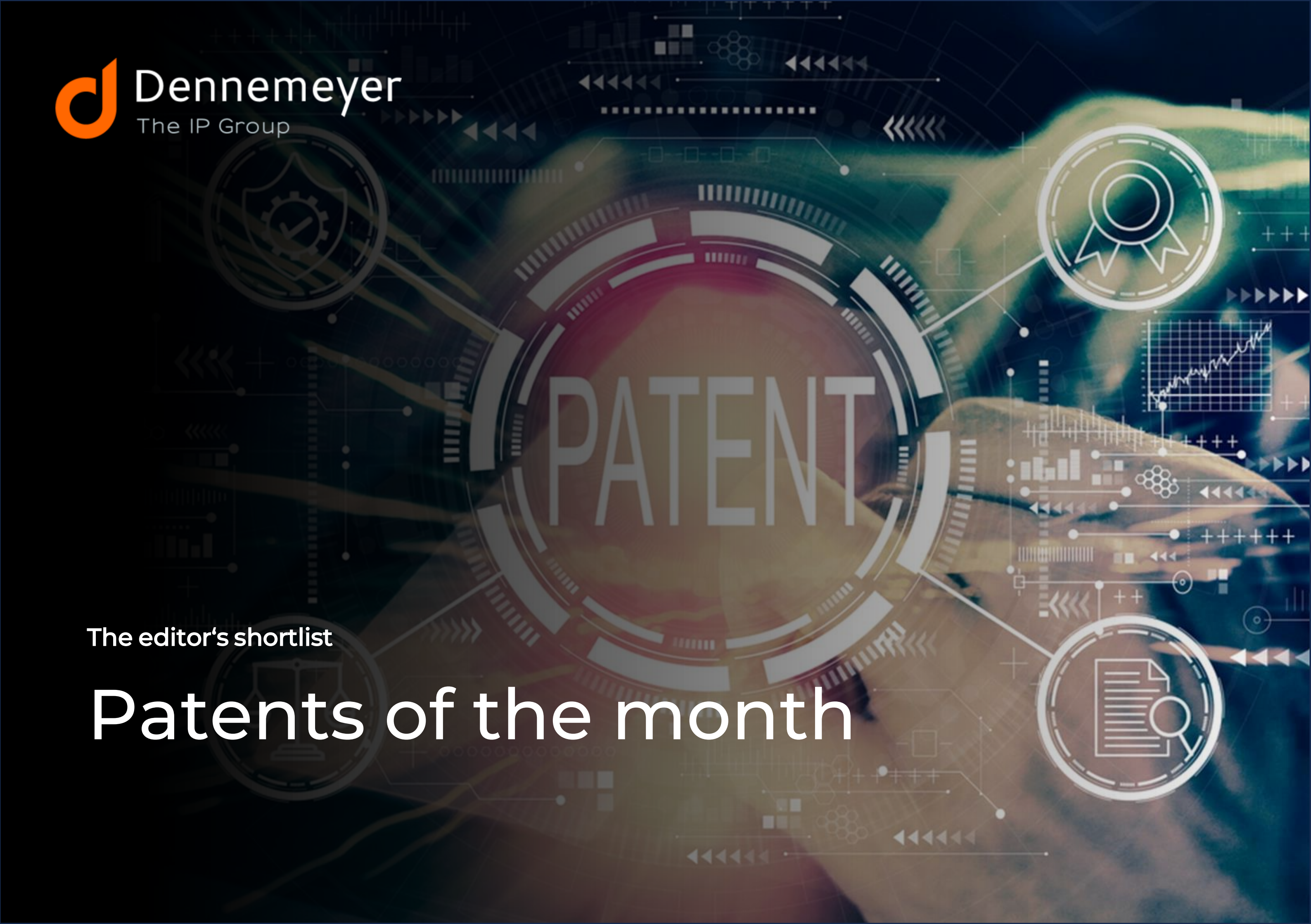
Rambus Wins Automotive Cybersecurity Innovation of the Year at 2024 AutoTech Breakthrough Awards

Rambus, a leading chip and silicon IP company, won the “Automotive Cybersecurity Innovation Of The Year” award at the 2024 AutoTech Breakthrough Awards for its RT-64x Root of Trust hardware security IP cores. These cores provide embedded HSM functionality for automotive applications, featuring a multi-layered security architecture to protect against various hardware and software attacks. Fully programmable and compliant with ISO 26262 ASIL-B, ASIL-D, and ISO 21434 standards, they ensure “security by design.” The cores protect automotive systems from faults, tampering, and cyber threats, ensuring a secure supply chain and supporting multi-tenant deployments with unique keys and independent access permissions.

Source
https://www.rambus.com/



Dennemeyer
The IP Group



The editor‘s shortlist

Patents of the month

Patents of the month

Published in October 2024

Shortlisted and summarized by our analyst

- US2024348635A1 - System and method for providing fleet cyber-security
  Assignee: Argus Cyber Security
- US12107876B2 - Intrusion path analysis device and intrusion path analysis method
  Assignee: Panasonic Intellectual Property Of America
- US12118083B2 - System and method for detection and prevention of cyber attacks at in-vehicle networks
  Assignee: High Sec Labs
- US12111921B2 - Incident response according to risk score
  Assignee: Denso Corp
- US20240354398A1 - Intrusion detection system
  Assignee: Mitsubishi Electric Corp
- EP4289114A4 - Secure communications with autonomous vehicles
  Assignee: Argo AI LLC
- IN552665A1 - ZT_BUSM: a robust blockchain based secure UAV-UAV communication using zero trust security model
  Assignee: Jaypee Institute Of Information Technology (JIIT)
- JP2024150116A - In-vehicle system, security management method, and security management program
  Assignee: Sumitomo Wiring Systems
- CN118865199A - Vehicle intrusion detection method based on DEEPSTREAM frames
  Assignee: Shangfei Intelligent Technology
- CN118869317A - Vehicle-mounted intrusion detection system and method based on evidence deep learning
  Assignee: Hefei University Of Technology

US2024348635A1

System and method for providing fleet cyber-security

Company name	Argus Cyber Security
Inventors	Galula Yaron, Ben-noon Ofer
Priority date	30 May 2017
Publication date	17 Oct 2024

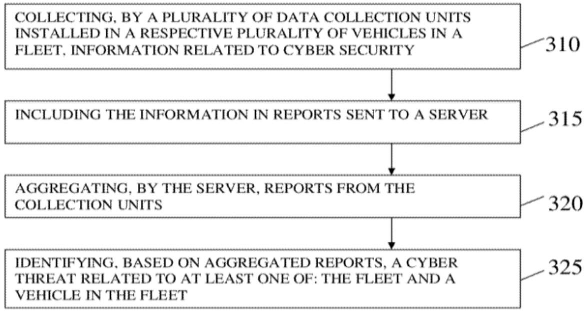

COLLECTING, BY A PLURALITY OF DATA COLLECTION UNITS INSTALLED IN A RESPECTIVE PLURALITY OF VEHICLES IN A FLEET, INFORMATION RELATED TO CYBER SECURITY
310
INCLUDING THE INFORMATION IN REPORTS SENT TO A SERVER
315
AGGREGATING, BY THE SERVER, REPORTS FROM THE COLLECTION UNITS
320
IDENTIFYING, BASED ON AGGREGATED REPORTS, A CYBER THREAT RELATED TO AT LEAST ONE OF: THE FLEET AND A VEHICLE IN THE FLEET
325

Fig. 3

The patent tackles the cybersecurity risks in modern cars that use electronic controls, which can be hacked to take over vehicle functions or entire fleets. It suggests installing data collection units (DCUs) in vehicles to gather cybersecurity data and send it to a central server in a security operations center (SOC). This server aggregates and analyzes data from multiple DCUs to find possible cyber-attack sources related to the fleet or a vehicle in the fleet. This method aims to boost vehicle network safety by identifying and monitoring threats early.

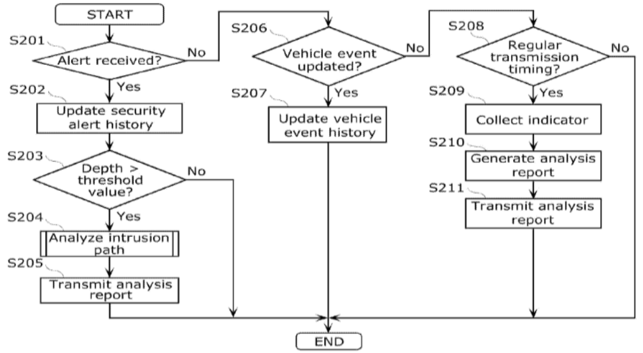
US12107876B2

Intrusion path analysis device and intrusion path analysis method

Company name	Panasonic Intellectual Property Of America
Inventors	Kishikawa Takeshi, Hirano Ryo, Haga Tomoyuki, Ujiie Yoshihiro
Priority date	14 Jan 2020
Publication date	01 Oct 2024

Summarized by Dennemeyer

FIG. 14



The patent addresses the challenge of identifying intrusion paths in vehicle control networks, where current methods can detect attacks but fail to trace the specific paths taken by attackers. It proposes an intrusion path analysis device that connects to the network, collects security alerts from sensors, and retrieves event histories. By analyzing these inputs along with an “intrusion depth” metric that indicates the level of intrusion when a security alert occurs, it determines the likely path of an attack, detailing entry points and intrusion depths, and issuing countermeasures based on the intrusion level. This approach enhances cybersecurity by systematically evaluating security alerts and historical data to improve detection and response to cyber threats.

US12118083B2

System and method for detection and prevention of cyber attacks at in-vehicle networks

Company name	High Sec Labs
Inventors	Soffer Aviv
Priority date	21 May 2020
Publication date	15 Oct 2024

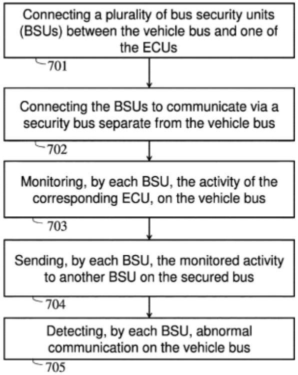

Connecting a plurality of bus security units (BSUs) between the vehicle bus and one of the ECUs
701
Connecting the BSUs to communicate via a security bus separate from the vehicle bus
702
Monitoring, by each BSU, the activity of the corresponding ECU, on the vehicle bus
703
Sending, by each BSU, the monitored activity to another BSU on the secured bus
704
Detecting, by each BSU, abnormal communication on the vehicle bus
705

FIG. 7

The patent deals with the increasing risk of cyber-attacks on vehicle networks as cars become more connected to wireless networks. Current systems like the CAN bus are vulnerable to hacking. The solution is a cybersecurity system with multiple bus security units (BSUs) that monitor and protect the ECUs in the vehicle. Each BSU connects between an ECU and the vehicle bus and communicates through a separate security bus. The BSUs detect unusual communications, share data with other BSUs, block or disconnect compromised ECUs, add a firewall between the vehicle bus and the ECU, and can bypass the vehicle bus using the security bus.

US12111921B2

Incident response according to risk score

Company name	Denso Corp
Inventors	Mora-Golding Carlos, Kashani Ameer, Iyer Gopalakrishnan, Yamashita Hirofumi
Priority date	10 Mar 2022
Publication date	08 Oct 2024

Summarized by Dennemeyer

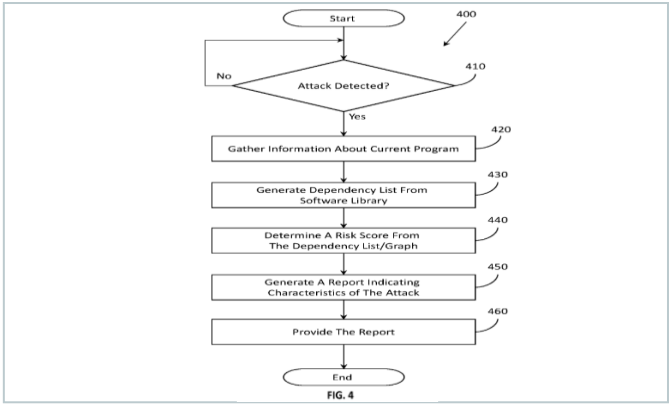

Start
400
410
No
Attack Detected?
Yes
420
Gather Information About Current Program
430
Generate Dependency List From Software Library
440
Determine A Risk Score From The Dependency List/Graph
450
Generate A Report Indicating Characteristics of The Attack
460
Provide The Report
End

FIG. 4

The patent tackles the problem of detecting and responding to attacks on vehicle electronic systems, which traditional methods struggle with due to modern vehicle complexity. It proposes a security system that detects attacks on vehicle components and gathers information about these components. The system also creates a dependency list specifying related components to the threatened component. It calculates a risk score based on factors like the attack's risk level, threatened component's risk type, and the combined risks of compromising related components. The system then generates a report with this information and can automatically respond to mitigate risks along with a risk score.

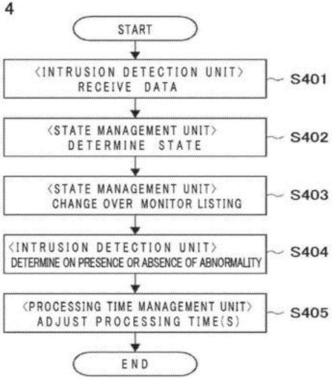
US20240354398A1

Intrusion detection system

Company name	Mitsubishi Electric Corp
Inventors	Okuyama Hiroshi, Matsui Toshinori
Priority date	25 Oct 2021
Publication date	24 Oct 2024

Summarized by Dennemeyer

FIG. 4


START
〈INTRUSION DETECTION UNIT〉
RECEIVE DATA
S401
〈STATE MANAGEMENT UNIT〉
DETERMINE STATE
S402
〈STATE MANAGEMENT UNIT〉
CHANGE OVER MONITOR LISTING
S403
〈INTRUSION DETECTION UNIT〉
DETERMINE ON PRESENCE OR ABSENCE OF ABNORMALITY
S404
〈PROCESSING TIME MANAGEMENT UNIT〉
ADJUST PROCESSING TIME(S)
S405
END

The patent tackles the problem of unauthorized data entering a vehicle’s control system through communication lines, causing abnormal behavior or data leaks. Existing systems struggle to detect such intrusions, especially when malicious data appears normal. The solution is an intrusion detection system (IDS) for vehicles that identifies unauthorized data entering via communication lines. It includes a monitor listing that sets rules to determine if data is normal or abnormal, IDS circuitry that compares incoming data with these rules to detect abnormalities, and state management circuitry that adjusts the monitoring rules based on vehicle’s state. Thus, vehicle security is improved by identifying and responding to unauthorized intrusions.

EP4289114A4

Secure communications with autonomous vehicles

Company name	Argo AI LLC
Inventors	Koniaris Kleanthes G
Priority date	05 Feb 2021
Publication date	09 Oct 2024

Summarized by Dennemeyer

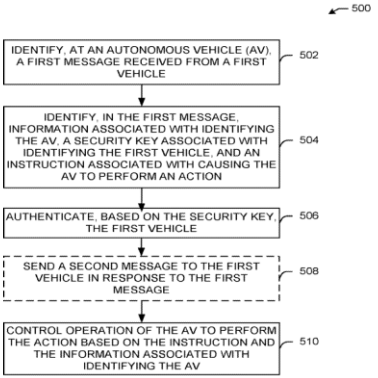

500
IDENTIFY, AT AN AUTONOMOUS VEHICLE (AV), A FIRST MESSAGE RECEIVED FROM A FIRST VEHICLE
502
IDENTIFY, IN THE FIRST MESSAGE, INFORMATION ASSOCIATED WITH IDENTIFYING THE AV, A SECURITY KEY ASSOCIATED WITH IDENTIFYING THE FIRST VEHICLE, AND AN INSTRUCTION ASSOCIATED WITH CAUSING THE AV TO PERFORM AN ACTION
504
AUTHENTICATE, BASED ON THE SECURITY KEY, THE FIRST VEHICLE
506
SEND A SECOND MESSAGE TO THE FIRST VEHICLE IN RESPONSE TO THE FIRST MESSAGE
508
CONTROL OPERATION OF THE AV TO PERFORM THE ACTION BASED ON THE INSTRUCTION AND THE INFORMATION ASSOCIATED WITH IDENTIFYING THE AV
510

FIG. 5

The patent addresses the problem of insecure communication between autonomous vehicles (AVs) and emergency vehicles (EVs), which can lead to spoofing or unauthorized commands that endanger public safety. The solution is a secure communication method where AVs receive messages from EVs with identifying information, security keys, and instructions. AVs authenticate the sender using these keys before acting on the instructions. This system allows AVs to perform actions like pulling over or changing speed, ensuring only verified emergency services can issue commands. This method uses cryptography for mutual authentication, supports both cloud-based and peer-to-peer communications, and helps prevent replay attacks with timestamps.

IN552665A1

ZT_BUSM: a robust blockchain based secure UAV-UAV communication using zero trust security model

Company name	Jaypee Institute Of Information Technology (JIIT)
Inventors	Dr. Juhi Gupta, Arushi Srivastava
Priority date	04 Jan 2023
Publication date	19 Oct 2024

Summarized by Dennemeyer

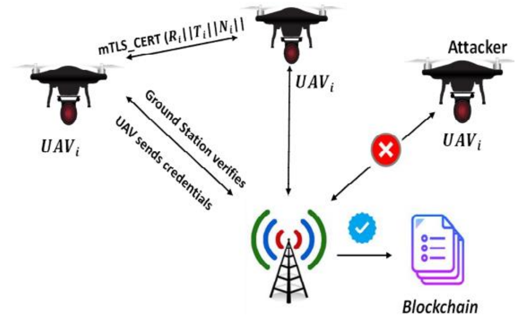


Figure 2

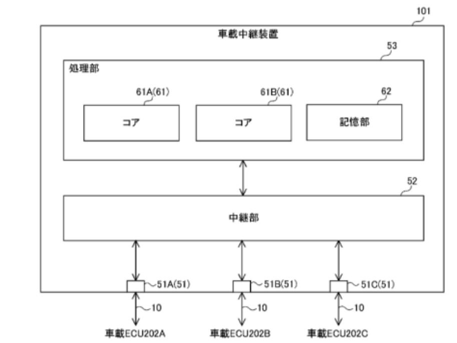
The invention addresses the security vulnerabilities of UAVs, which are prone to physical tampering and attacks from malicious eavesdroppers. It proposes a secure, TLS certificate-based mutual authentication protocol for UAVs through a Ground Station (GS). This creates a robust system by not trusting any interacting UAVs. The model provides real-time evidence of a zero-trust security model for high-confidentiality data. Unlike prior models, which lack real-life attack testing, secure data encryption, and have high communication costs, this invention uses blockchain to verify UAV attributes and TLS certificates. It stores challenge-response pairs on the blockchain and employs multi-factor authentication with mutual-TLS certificates to ensure secure UAV-UAV communication.

JP2024150116A

In-vehicle system, security management method, and security management program

Company name	Sumitomo Wiring Systems
Inventors	Kazuyuki Inoue, Makoto Matsumoto, Keigo Kikuchi, Yusuke Takeuchi
Priority date	10 Apr 2023
Publication date	23 Oct 2024

【図３】



The patent addresses the challenge of securing vehicle systems when a security risk is detected in one part. Traditional methods can lead to service interruptions or vulnerabilities if an attack targets a single point of failure. The solution is a vehicle system with multiple functional units, each with different security setups. When a risk is detected in one unit, the system stops access to that unit and reroutes communications through another secure unit, allowing continued operation without exposing the system to threats.

CN118865199A

Vehicle intrusion detection method based on DEEPSTREAM frames

Company name	Shangfei Intelligent Technology
Inventors	Lu Fengling, Xu Wang, Chen Lei, Wang Ning, Zhang Yaofang, Sun Guoxin, Qian Jiayi, Xiong Zhao
Priority date	28 June 2024
Publication date	29 Oct 2024

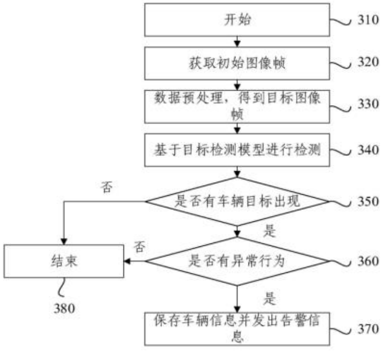


图3

The patent addresses the problem of poor real-time performance and high false alarm rates in vehicle intrusion detection due to inadequate hardware and model adaptability. It proposes a method using DEEPSTREAM frames to improve detection. This involves getting real-time video stream data from cameras, using a deep learning model trained on vehicle images to detect each frame, and identifying potential intrusions in specific areas based on the target detection model under the condition that the vehicle target appears in each target image. This approach makes detection faster, more accurate in identifying unusual vehicle behaviors, and better at handling different environments by enhancing the video quality.

CN118869317A

Vehicle-mounted intrusion detection system and method based on evidence deep learning

Company name	Hefei University Of Technology
Inventors	Shi Qin, Liu Junyu, Cheng Teng, Du Yufeng
Priority date	02 Aug 2024
Publication date	29 Oct 2024

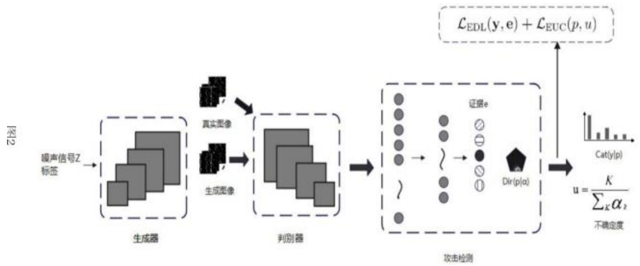


图2
噪声信号Z
标签
生成器
真实图像
生成图像
判别器
证据e
Dir(p|α)
攻击检测
$\mathcal{L}_{\mathrm{EDL}}(\mathbf{y},\mathbf{e})+\mathcal{L}_{\mathrm{EUC}}(p,u)$
Cat(y|p)
$u=\frac{K}{\sum_{K}\alpha_{i}}$
不确定度

The patent deals with increasing security threats in vehicle networks, especially the CAN bus, due to their complexity and connectivity. Traditional methods can't detect unknown attacks well because they need labeled data. The solution is an intrusion detection system in vehicles that uses evidence deep learning (EDL) to spot both known and unknown attacks in real-time. It collects CAN messages, turns them into images, extracts features with an improved GAN model, and uses EDL for classification and uncertainty estimation. This system improves the accuracy and reliability of detecting vehicle intrusions by better recognizing unknown attacks.

By the numbers

Founded in **1962**

180 jurisdictions covered worldwide

~2 Million patents maintained

~1 Million trademarks managed

60 years of experience in IP

>20 global offices

>900 employees and associates

Global presence

- Abu Dhabi, UAE
- Beijing, CN
- Bengaluru, IN
- Brasov, RO
- Chicago, USA
- Dubai, UAE
- Howald, LU
- Johannesburg, ZA
- Manila, PH
- Melbourne, AU
- Munich, DE
- Paris, FR
- Rio de Janeiro, BR
- Rome, IT
- Singapore, SG
- Stockport, UK
- Taipei,TW
- Tokyo, JP
- Turin, IT
- Vargarda, SE
- Warsaw, PL
- Woking, UK
- Zagreb, HR

Talk to us now

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

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

Dennemeyer
The IP Group

Visit us

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

Dennemeyer India Private Limited
Bengaluru
info-india@dennemeyer.com

North & East India
+91 79831 15166

South & West India
91 88266 88838