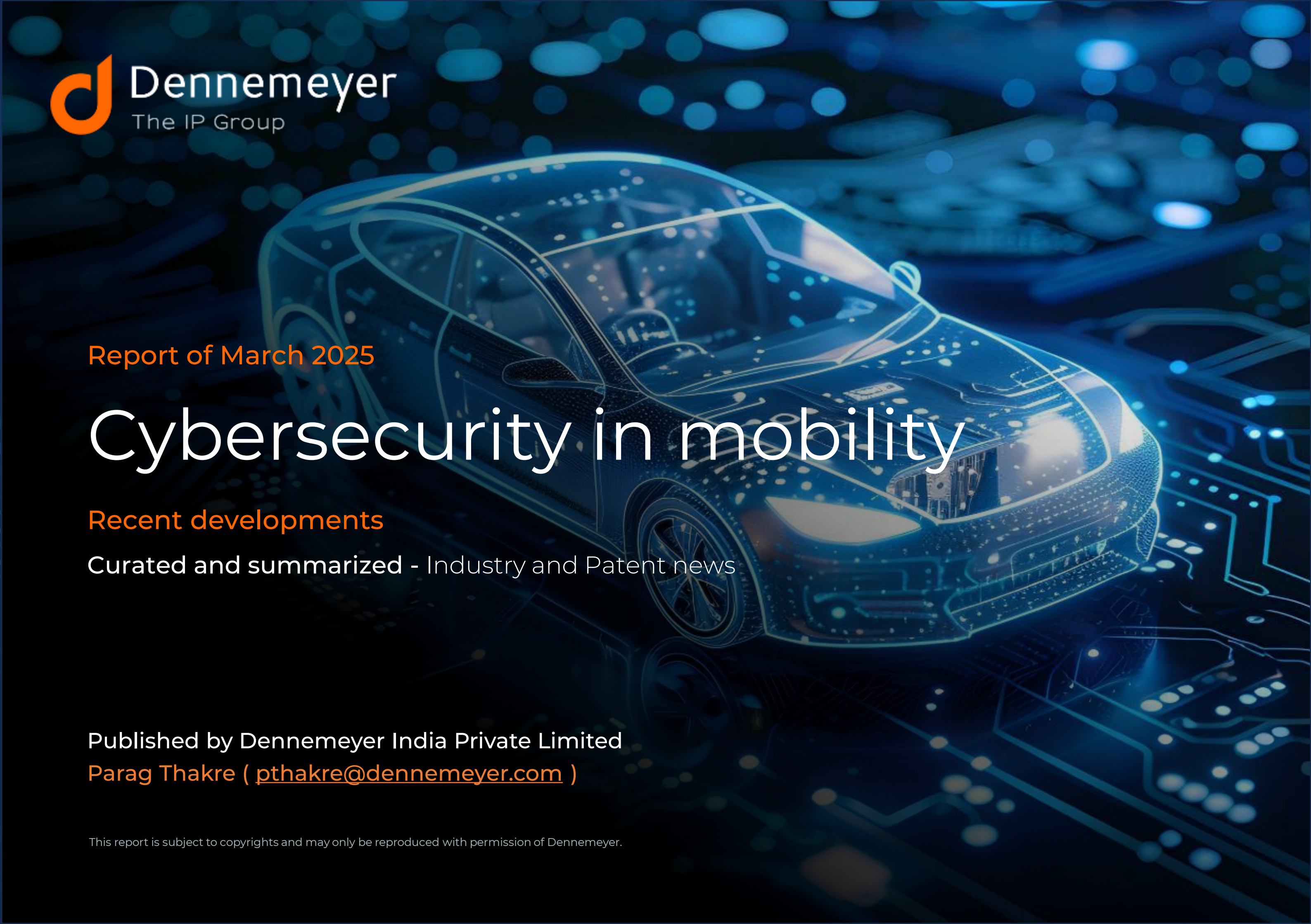


Dennemeyer
The IP Group

Report of March 2025

Cybersecurity in mobility

Recent developments

Curated and summarized - Industry and Patent news

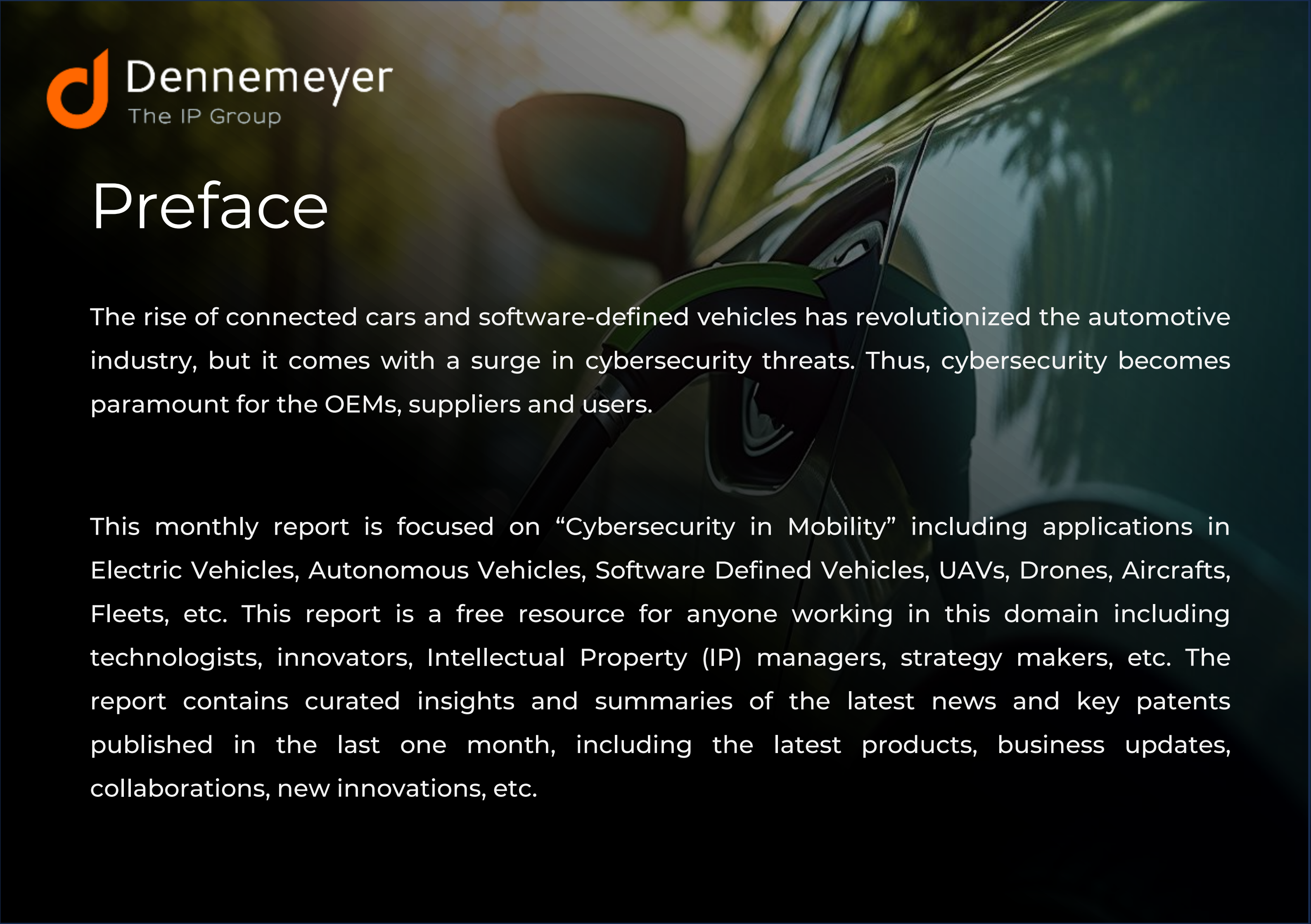
Published by Dennemeyer India Private Limited

Parag Thakre (pthakre@dennemeyer.com)

Dennemeyer
The IP Group

Subscribe now

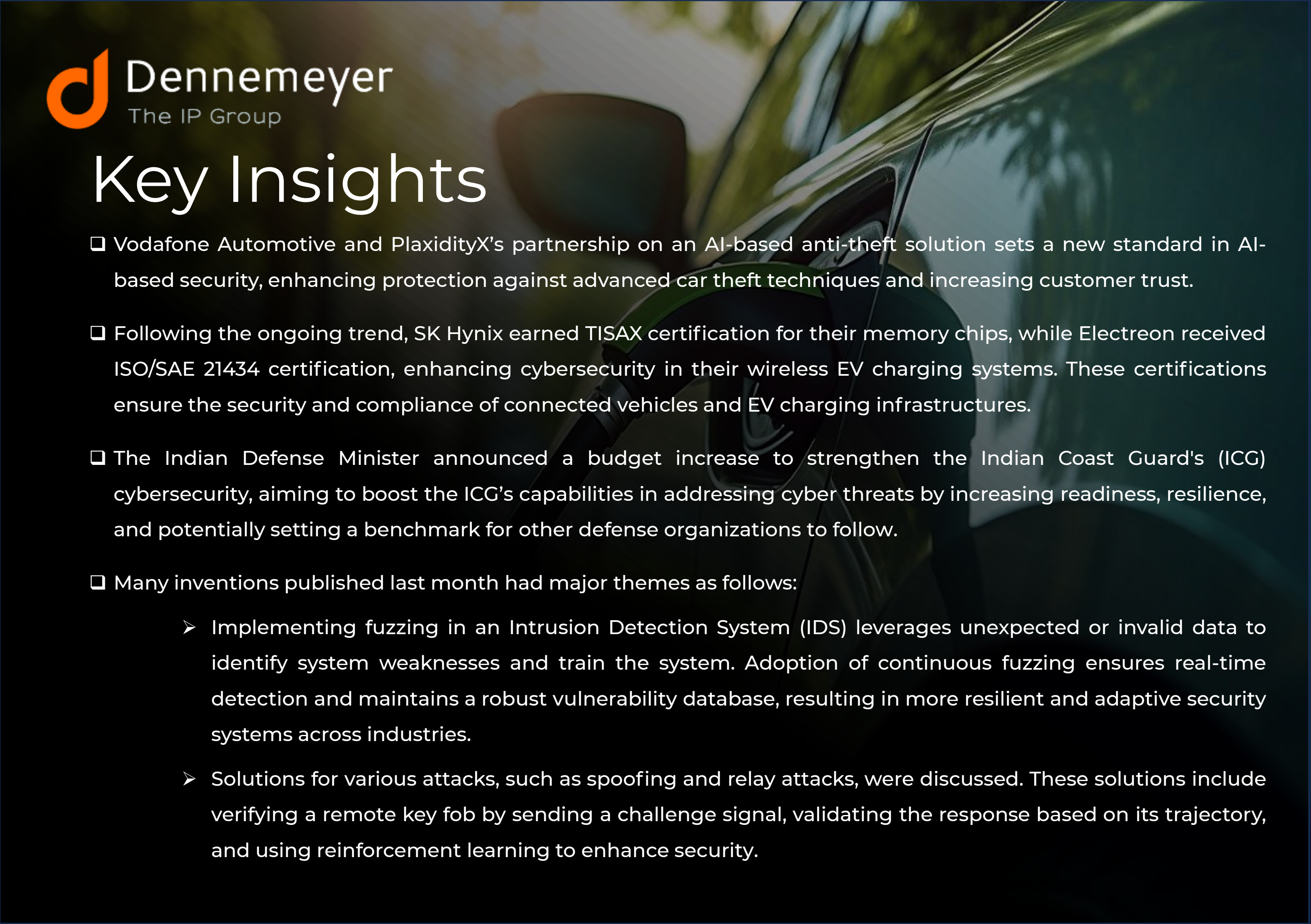
Scan the QR code to receive this monthly report via email in your inbox.



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

- ❑ Vodafone Automotive and PlaxidityX's partnership on an AI-based anti-theft solution sets a new standard in AI-based security, enhancing protection against advanced car theft techniques and increasing customer trust.

- ❑ Following the ongoing trend, SK Hynix earned TISAX certification for their memory chips, while Electreon received ISO/SAE 21434 certification, enhancing cybersecurity in their wireless EV charging systems. These certifications ensure the security and compliance of connected vehicles and EV charging infrastructures.

- ❑ The Indian Defense Minister announced a budget increase to strengthen the Indian Coast Guard's (ICG) cybersecurity, aiming to boost the ICG's capabilities in addressing cyber threats by increasing readiness, resilience, and potentially setting a benchmark for other defense organizations to follow.

- ❑ Many inventions published last month had major themes as follows:
  - ➢ Implementing fuzzing in an Intrusion Detection System (IDS) leverages unexpected or invalid data to identify system weaknesses and train the system. Adoption of continuous fuzzing ensures real-time detection and maintains a robust vulnerability database, resulting in more resilient and adaptive security systems across industries.
  - ➢ Solutions for various attacks, such as spoofing and relay attacks, were discussed. These solutions include verifying a remote key fob by sending a challenge signal, validating the response based on its trajectory, and using reinforcement learning to enhance security.

Partnership

Vodafone automotive and PlaxidityX join forces to protect vehicles from modern theft methods

Vodafone Automotive has partnered with PlaxidityX to integrate PlaxidityX's vDome anti-theft solution into Vodafone's car tracking products. This partnership tackles the growing issue of modern car theft, where criminals use electronic hacking devices to steal cars in seconds, costing billions of dollars annually. The vDome software uses AI to spot and stop theft attempts in real-time by identifying unauthorized activities on the vehicle network. This partnership aims to offer an additional layer of protection against advanced car theft techniques, ensuring the safety and security of vehicles.

Source
https://plaxidityx.com/

Cybersecurity Investments

Indian coast guard gets 26.5% budget hike—₹9,676.70 crore for cyber security & fleet upgrades.

At the 18th ICG Investiture Ceremony in New Delhi, the Indian Defense Minister awarded medals to the Indian Coast Guard (ICG) for their hard work in protecting India's coastal borders. He praised their efforts in keeping the coast secure and stopping illegal activities. He highlighted their achievements, such as seizing boats, arresting pirates, and conducting a major drug bust. The minister also warned about growing cyber threats and announced a 26.50% budget increase for the ICG for 2025-26 to modernize their equipment to fight against cyber attacks. He praised the ICG's focus on technology and assured them of continued government support.

Source
https://www.sudarshannews.in/

TISAX Certification

SK Hynix acquires 'TISAX' certification for the first time in the memory industry

SK Hynix, a leading memory chip manufacturer, has become the first in its industry to achieve TISAX certification, a global automobile industry information security certification. This certification, which is a key requirement for suppliers in the automotive industry, validates the company's robust security measures. As electric and connected cars become more common, the demand for reliable automotive semiconductors has increased. With this milestone, SK Hynix plans to accelerate the development of high-performance memory solutions needed for AI-driven future automobile technology. The company highlights its commitment to protecting against cyber threats and ensuring the performance of key automotive systems.

Source
https://news.skhynix.com/

Dennemeyer
The IP Group

Industry News

Data Security Audit

Driivz achieves SOC 2 type II attestation report for EV charging and energy management software

Driivz, a top global software supplier for EV charging operators, has completed the SOC 2 Type II audit for its EV Charging and Energy Management Platform. PwC conducted the audit, confirming that Driivz meets the highest standards for data security, privacy, and compliance. This certification shows that Driivz has put strong measures in place to protect customer data, ensuring the platform's security, availability, and confidentiality. With this certification, Driivz strengthens its reputation as a reliable partner for secure EV charging solutions, supporting the growing EV market.

Source
https://driivz.com/

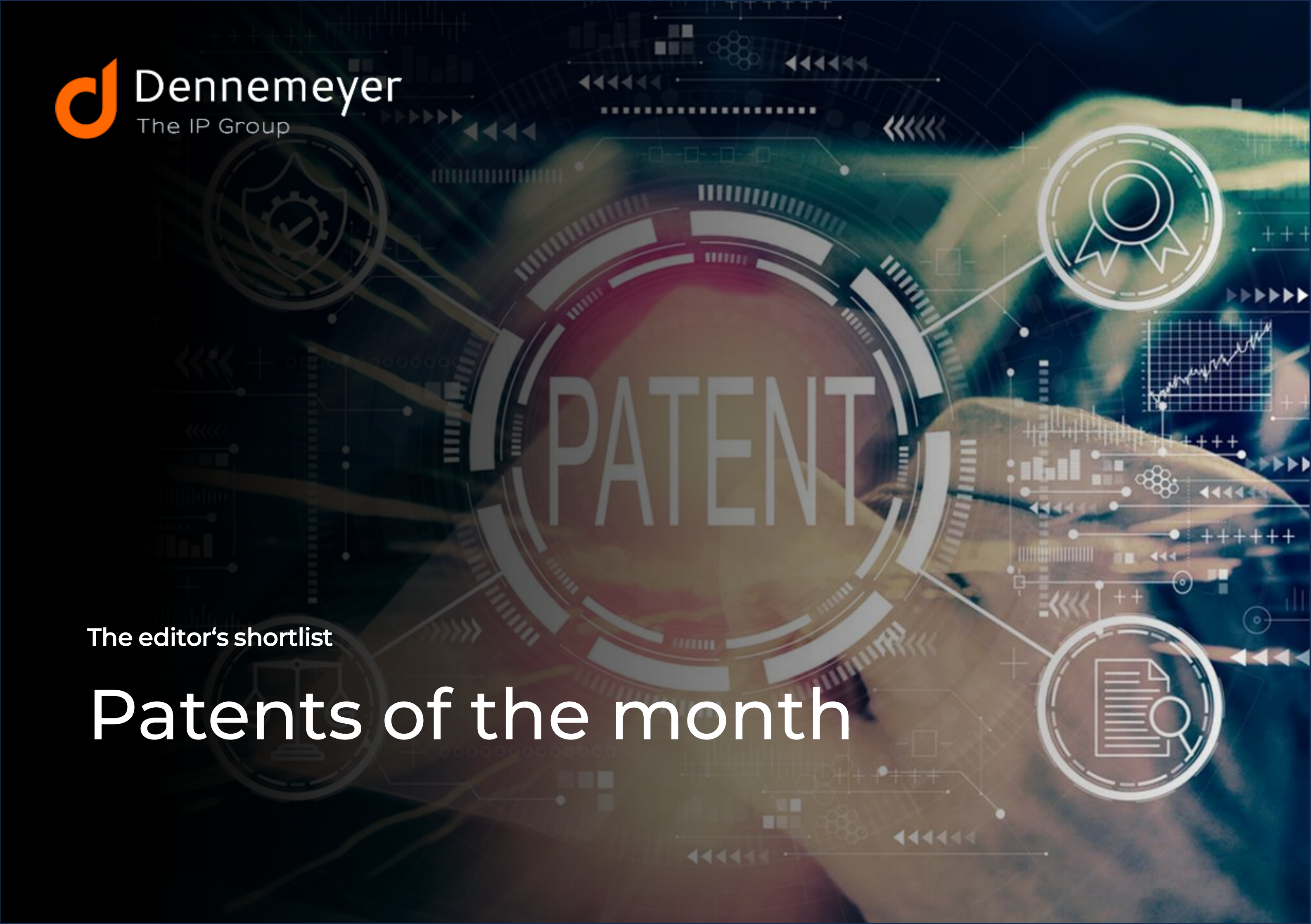
Secure Wireless Charging

Electreon earns ISO/SAE 21434 automotive cybersecurity standard certification, paving way for wider adoption of wireless charging by automakers

Electreon, a leader in wireless EV charging, has achieved ISO/SAE 21434 certification, ensuring strong cybersecurity measures are integrated into their charging systems throughout their lifecycle. This demonstrates Electreon’s commitment to secure EV charging and positions the company among a select few in the industry. The certification is expected to drive demand for Electreon’s solutions in large-scale transportation projects and strengthen partnerships with leading automakers. It also aligns with the United Nations' UNECE R155 regulation, which mandates cybersecurity for vehicles.

Source
https://ir.electreon.com/

Dennemeyer
The IP Group



The editor‘s shortlist

Patents of the month

Dennemeyer
The IP Group

Patents of the month

Published in February 2025

Shortlisted and summarized by our analyst

- US12221063B2 - In-vehicle electronic system, vehicle, control method, and computer readable storage medium
  Assignee: Honda Motor Co Ltd
- US20250045386A1 - Detection and mitigation of cyber attacks on aimed at vehicle's diagnostic sessions
  Assignee: Red Bend Ltd
- US2025071554A1 - Protection against relay attack for keyless entry systems in vehicles and systems
  Assignee: AT&T Intellectual Property LLP
- IN202517000832A - Secure uncrewed aerial vehicle direct communications
  Assignee: Lenovo Singapore Pte Ltd
- WO2025026864A1 - Computer-implemented method for identifying potential denial-of-service attack vulnerabilities in a network protocol program
  Assignee: Continental Automotive Technologies, Nanyang Technological University
- DE102024207181A1 - Systems and methods for improving and updating an IDS with fuzzing results
  Assignee: Robert Bosch Gmbh
- JP2025020641A - Attack analysis device, attack analysis method, and attack analysis program
  Assignee: Denso Corp
- KR102768410B1 - Method and system for providing security on in-vehicle network
  Assignee: Hyundai Motor, Kia Motors
- CN119547401A - Intrusion detection device and intrusion detection method
  Assignee: Hitachi Astemo Ltd
- CN119535499A - Automatic driving vehicle GNSS spoofing attack detection device and method based on reinforcement learning
  Assignee: State Grid Information &Telecommunication Group Co Ltd

US12221063B2

In-vehicle electronic system, vehicle, control method, and computer readable storage medium

Company name	Honda Motor Co Ltd
Inventors	Kato Hisahiro, Kono Satoshi, Saito Kanako, Takahashi Yusuke
Priority date	30 Mar 2021
Publication date	11 Feb 2025

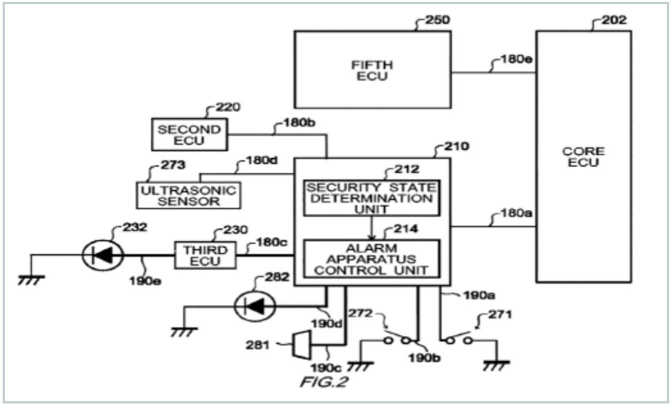


FIG.2

This invention introduces a smart in-vehicle electronic system capable of monitoring security issues and autonomously responding, even when the vehicle's ignition is off. It includes sensors to detect the vehicle's security status, an alarm that triggers upon detecting abnormal conditions, and a main Electronic Control Units (ECU) that connects directly to these sensors and the alarm. This ECU operates independently while communicating with other ECUs, enabling real-time security monitoring. The benefits of this invention include faster alarm responses, reduced power consumption when the car is off, and a simpler design with fewer ECUs, which could lower certification costs.

US20250045386A1

Detection and mitigation of cyber attacks on aimed at vehicle's diagnostic sessions

Company name	Red Bend Ltd
Inventors	Ben Zvi Arie
Priority date	02 Dec 2021
Publication date	06 Feb 2025

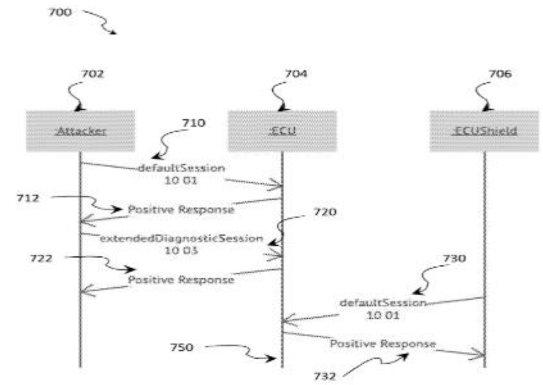


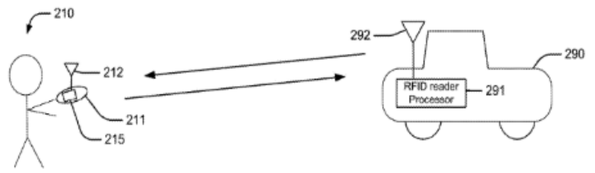
FIG.7

This patent addresses the risk of cyber attacks on vehicle diagnostics, where hackers can exploit weaknesses in ECUs to access and manipulate vehicle systems. The solution is a device that detects and stops such attacks on vehicles using a communication bus, specifically using Controller Area Network (CAN) protocols. It enforces a diagnostic policy by mapping requests to valid vehicle states. If a request doesn't match the current state, an interfering request is sent to stop the operation. This approach improves security by preventing invalid operations and ensuring no critical updates occur while the vehicle is in motion or in an inappropriate state.

US2025071554A1

Protection against relay attack for keyless entry systems in vehicles and systems

Company name	AT&T Intellectual Property LLP
Inventors	Joseph Soryal
Priority date	16 Aug 2019
Publication date	27 Feb 2025



201
FIG. 2A

This invention tackles the problem of cyber attacks on keyless entry systems, where hackers break into cars using relay devices by intercepting signals from key fobs used to unlock the vehicle. The solution is a device that wirelessly receives a request to unlock the car, sends challenge signals at random times, and uses different software methods for these signals. The device then receives response signals, figures out the remote system's trajectory based on these signals, and unlocks the car if the trajectory is verified. This improves security by preventing unauthorized access to vehicles.

IN202517000832A

Secure uncrewed aerial vehicle direct communications

Company name	Lenovo Singapore Pte Ltd
Inventors	Baskaran Sheeba Backia Mary, Kunz Andreas
Priority date	01 Aug 2022
Publication date	21 Feb 2025

Summarized by Dennemeyer

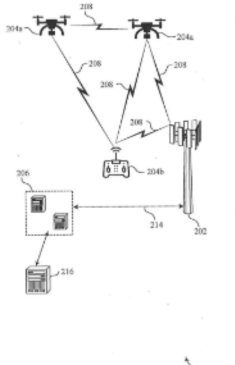


FIG. 2

This patent addresses the challenges of secure communication in wireless systems, especially for uncrewed aerial vehicles (UAVs) in 5G networks. Even though current systems are advanced, they have limited security measures and can be vulnerable to potential threats. This invention is designed to receive and verify an aircraft-to-everything (A2X) security policy. The user can request direct communication with a UAV controller for services, sending the A2X security policy for verification. The response from the UAV controller determines if the communication request is accepted or rejected, enhancing the security of UAV communications in 5G networks.

WO2025026864A1

Computer-implemented method for identifying potential denial-of-service attack vulnerabilities in a network protocol program

Company name	Continental Automotive Technologies, Nanyang Technological University
Inventors	Du Zhengjie, Li Yuekang, Zheng Yaowen, Liu Yang, Mahbub Sheikh Habib, Palige René, Kakkolangara Praveen, Sapin Etienne Alcide, Menon Suraj Jayakumar
Priority date	03 Aug 2023
Publication date	06 Feb 2025

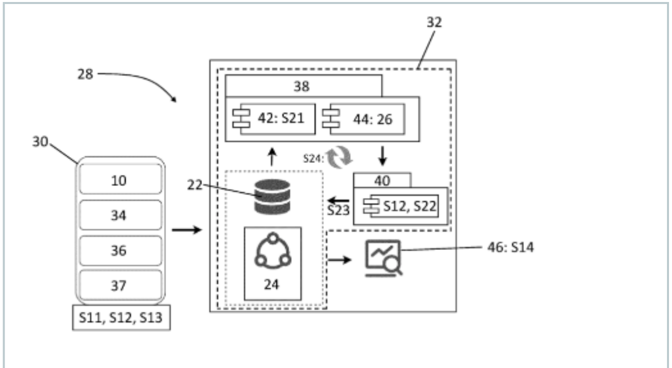


Fig. 3

This invention deals with the rise in denial-of-service (DoS) attacks that exploit weaknesses in network programs, causing services to crash or resources to be drained. Traditional methods mostly focus on finding bugs that cause crashes but don't address issues where the program's resources get exhausted. The solution involves creating test inputs, running them to see how the network behaves, and tracking how resources are used during these tests. This data is then used to build a model that helps identify potential DoS attack weaknesses based on resource usage. This solution improves vulnerability detection by focusing on resource depletion, using automated testing techniques to find new issues, and continuously updating the model to improve over time.

DE102024207181A1

Systems and methods for improving and updating an IDS with fuzzing results

Company name	Robert Bosch Gmbh
Inventors	Finn Gunter, Guajardo Merchan Jorge, Amarnath Rakshith, Ring Martin
Priority date	31 Jul 2023
Publication date	06 Feb 2025

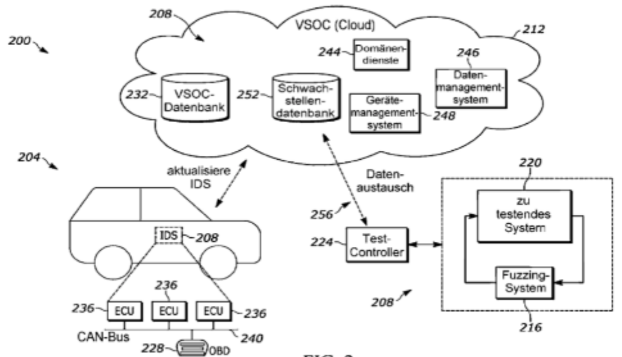


FIG. 2

This patent describes vulnerabilities in software programs within IDS that monitor and secure vehicle networks, which are increasingly susceptible to cyberattacks. The invention uses a process called fuzzing, where specially crafted inputs are sent to the software to find vulnerabilities. These detected vulnerabilities are then recorded, and updates are made to the IDS or software based on the findings. This invention provides improvements such as continuous fuzzing for real-time detection of new vulnerabilities, a comprehensive database to track issues across different hardware and software versions, and the ability to perform corrective actions automatically or with user instructions, improving response times to potential threats.

Dennemeyer
The IP Group

Latest patents

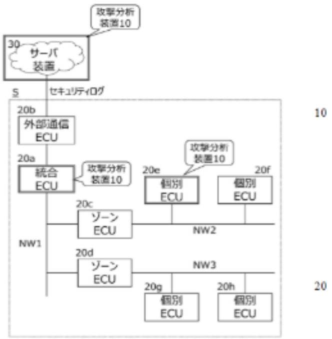
JP2025020641A

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

Company name	Denso Corp
Inventors	Nagara Keigo, Abe Taiji, Ikuse Tomonori, Hayakawa Keita, Egawa Masumi
Priority date	31 Jul 2023
Publication date	13 Feb 2025

Summarized by Dennemeyer

【図 2】



This invention deals with the growing risk of cyberattacks on electronic control systems in vehicles, especially due to their connectivity features. Traditional methods often struggle to identify the type or severity of these attacks accurately. The solution is an attack analysis device that gathers security logs showing detected issues and their locations. It stores information about predicted attacks and anomalies. Using this data, the device estimates received attacks. It then checks the accuracy of these estimations with context data from the logs. Finally, an output unit provides details about the estimated attack and its accuracy.

KR102768410B1

Method and system for providing security on in-vehicle network

Company name	Hyundai Motor, Kia Motors
Inventors	Kim Il, Kang Seong Yong, Cho A Ram
Priority date	21 Feb 2019
Publication date	13 Feb 2025

Summarized by Dennemeyer

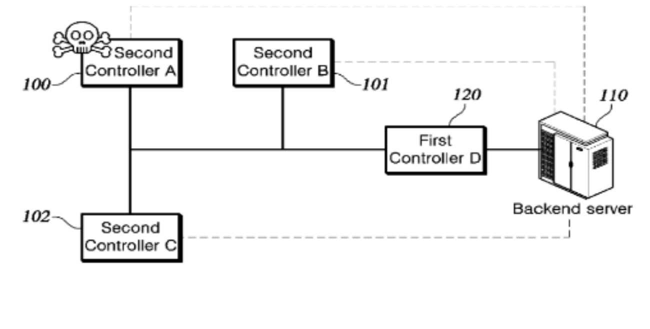


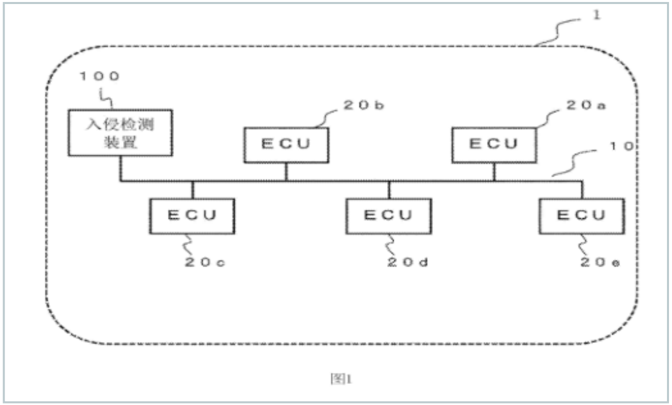
FIG. 1

This patent addresses security issues in in-vehicle networks, especially for ECUs and multimedia devices that interact with other external devices. These systems can be attacked, leading to unauthorized access and data theft. The invention secures the in-vehicle network by having a main controller verify the integrity of other controllers. It does this by sending requests for information from suspicious controllers, receiving encrypted responses, decrypting them, and comparing the data with stored anomalies to spot any unusual activity. If there are discrepancies or no response, the controller is flagged as suspicious.

CN119547401A

Intrusion detection device and intrusion detection method

Company name	Hitachi Astemo Ltd
Inventors	Nomura Teruaki , Morita Nobuhiro , Shuhei Kaneko , Fujii Yasumasa , Katakashi Kazuo
Priority date	20 Jul 2022
Publication date	28 Feb 2025



This invention deals with the rising threat of denial-of-service (DoS) attacks on vehicle control systems (ECUs). Hackers can exploit these systems through illegal communications. Traditional methods struggle to detect these attacks accurately, especially when hackers transmit illegal data within controlled limits. The fix involves an intrusion detection device that includes a communication unit for sending and receiving data, an attribute acquisition unit to obtain data attributes, a state acquisition section for communication control information, and an abnormality detection unit to identify anomalies based on the attributes and control information, thus improving the accuracy of detecting illegal communications.

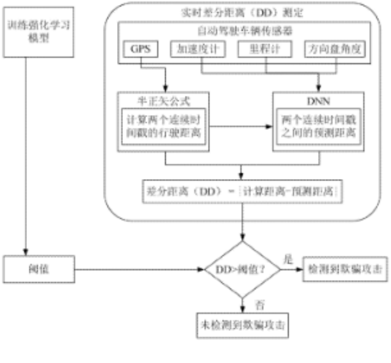


图1

CN119535499A

Automatic driving vehicle GNSS spoofing attack detection device and method based on reinforcement learning

Company name	State Grid Information &Telecommunication Group Co Ltd
Inventors	Chen Xiangdong, Yang Bojie, Chen Mengqi, Fu Haixuan
Priority date	07 Nov 2024
Publication date	28 Feb 2025

Summarized by Dennemeyer

This invention focuses on the need for reliable navigation in self-driving cars, which rely on Global Navigation Satellite Systems (GNSS) like GPS. These systems can be vulnerable to signal interference, especially in urban areas or tunnels, and can be targeted by hackers using jamming or spoofing attacks. The solution is to use reinforcement learning to spot spoofing attacks by analyzing GPS data and other vehicle metrics. A dataset is formed from normal and spoofed data, predicts vehicle movement using a neural network, and compares real-time data against expected values to detect anomalies, ensuring the safety and reliability of autonomous vehicle navigation.

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

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

DISCLAIMER: This report, including external links, is generated using databases and information sources believed to be reliable. While effort has been made to employ optimal resources for research and analysis, Dennemeyer expressly disclaims all warranties regarding the accuracy, completeness, or adequacy of the information provided. We do not control or endorse the content of external sites and are not responsible for their accuracy or legality. The information provided in this report should not be construed as legal advice, and users are strongly advised to consult with qualified legal professionals for specific legal guidance.