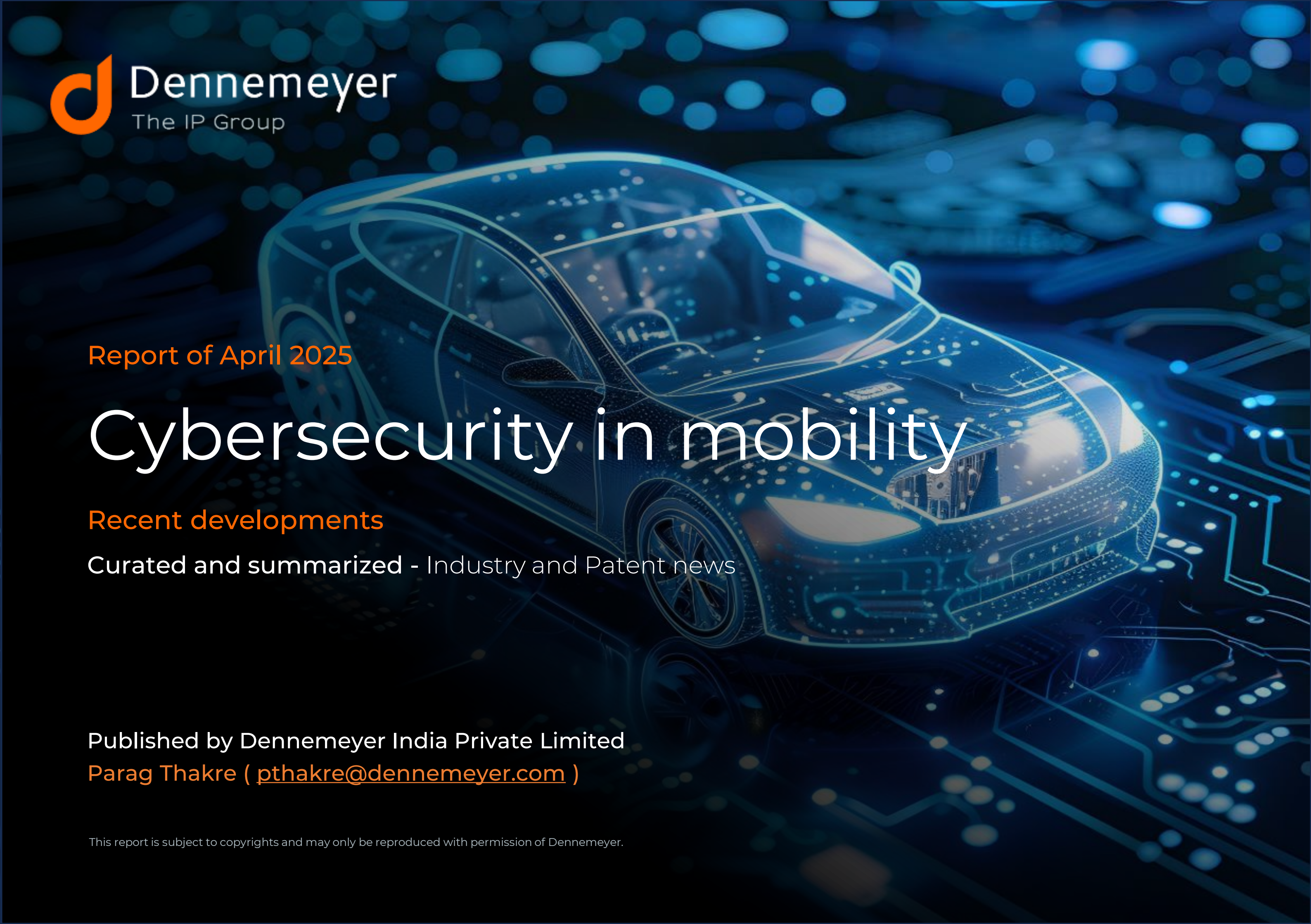


Dennemeyer
The IP Group

Report of April 2025

Cybersecurity in mobility

Recent developments

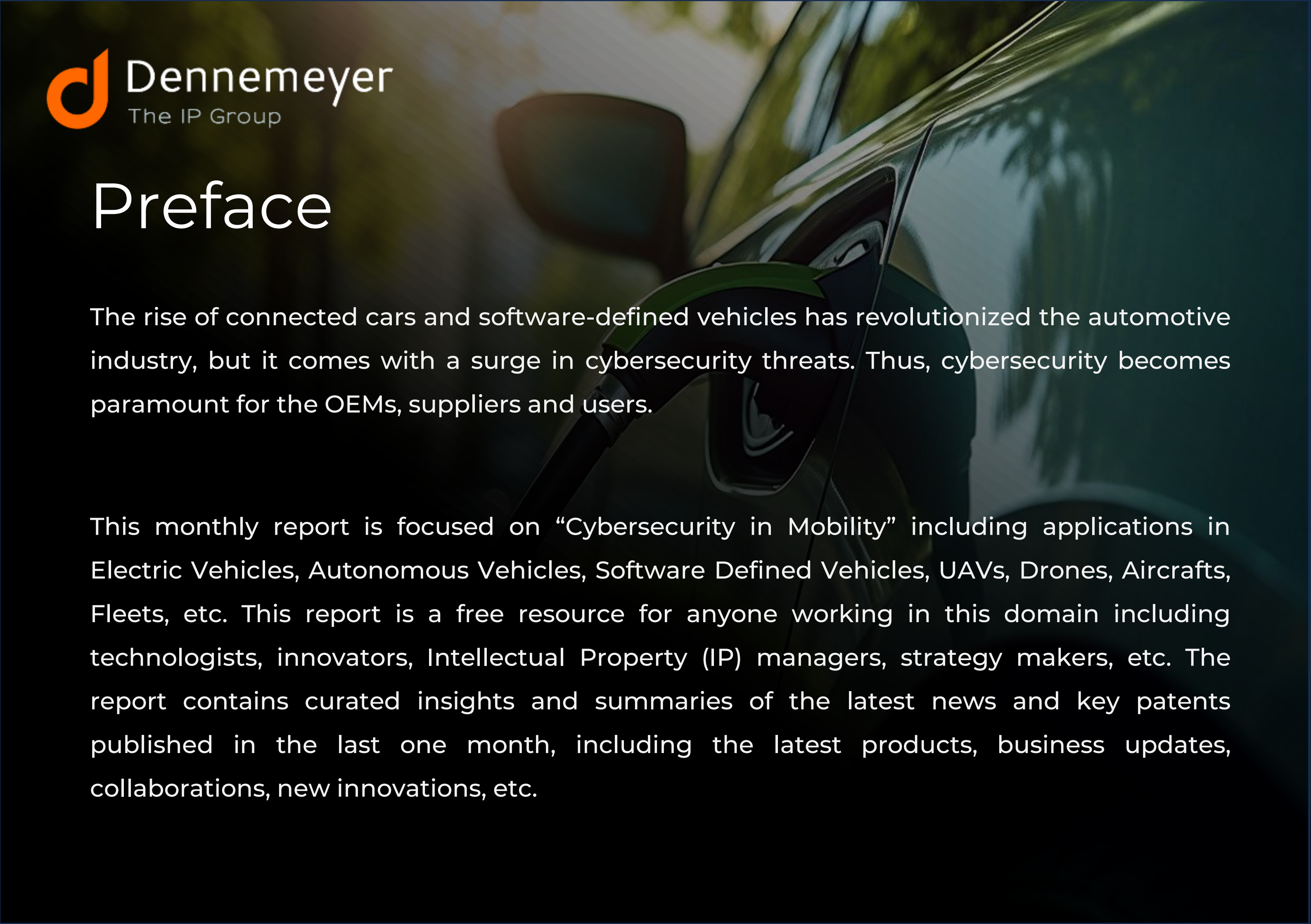
Curated and summarized - Industry and Patent news

Published by Dennemeyer India Private Limited
Parag Thakre (pthakre@dennemeyer.com)

Dennemeyer
The IP Group

Subscribe now

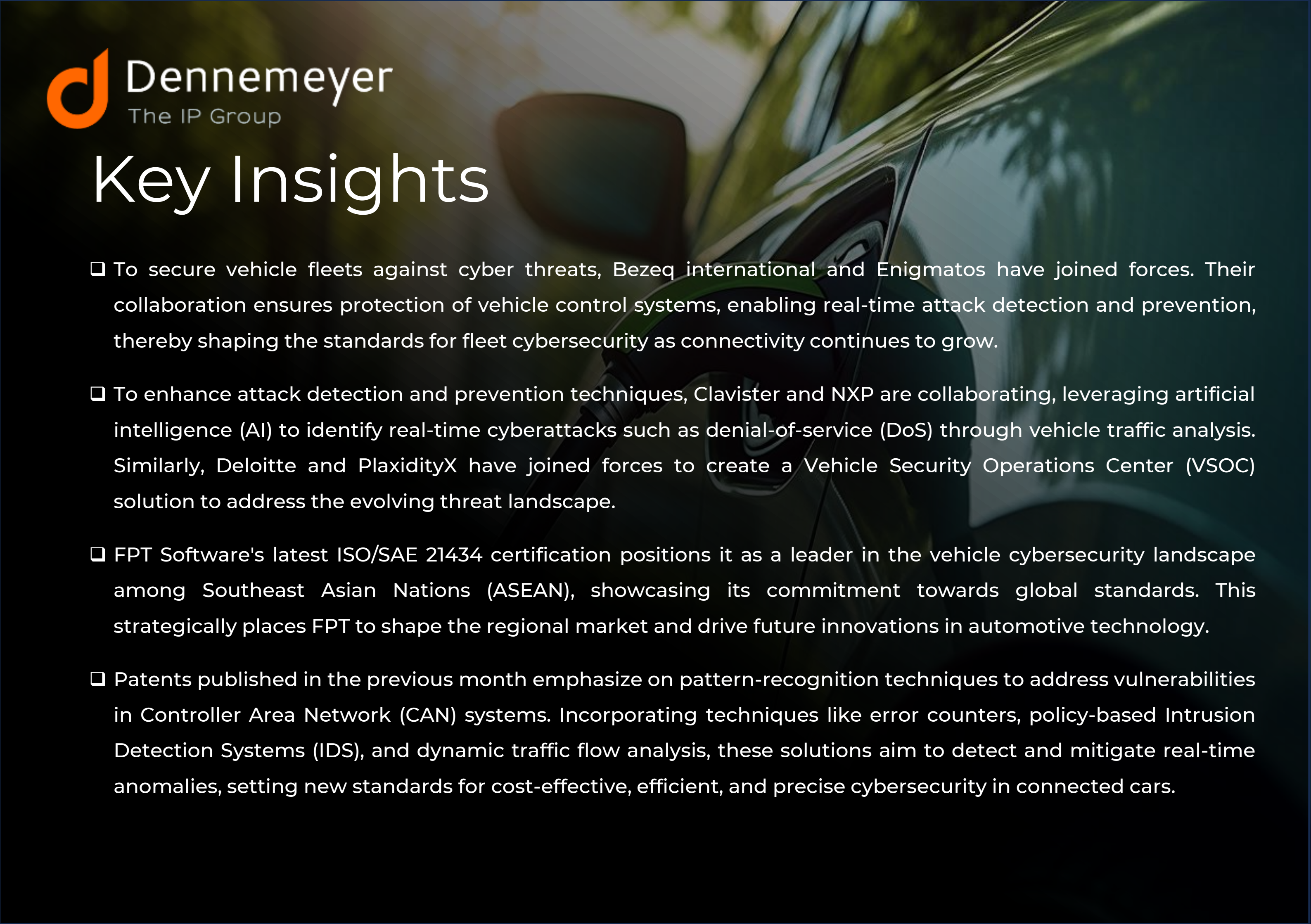
Scan the QR code to receive this monthly report via email in your inbox.



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

□ To secure vehicle fleets against cyber threats, Bezeq international and Enigmatos have joined forces. Their collaboration ensures protection of vehicle control systems, enabling real-time attack detection and prevention, thereby shaping the standards for fleet cybersecurity as connectivity continues to grow.

□ To enhance attack detection and prevention techniques, Clavister and NXP are collaborating, leveraging artificial intelligence (AI) to identify real-time cyberattacks such as denial-of-service (DoS) through vehicle traffic analysis. Similarly, Deloitte and PlaxidityX have joined forces to create a Vehicle Security Operations Center (VSOC) solution to address the evolving threat landscape.

□ FPT Software's latest ISO/SAE 21434 certification positions it as a leader in the vehicle cybersecurity landscape among Southeast Asian Nations (ASEAN), showcasing its commitment towards global standards. This strategically places FPT to shape the regional market and drive future innovations in automotive technology.

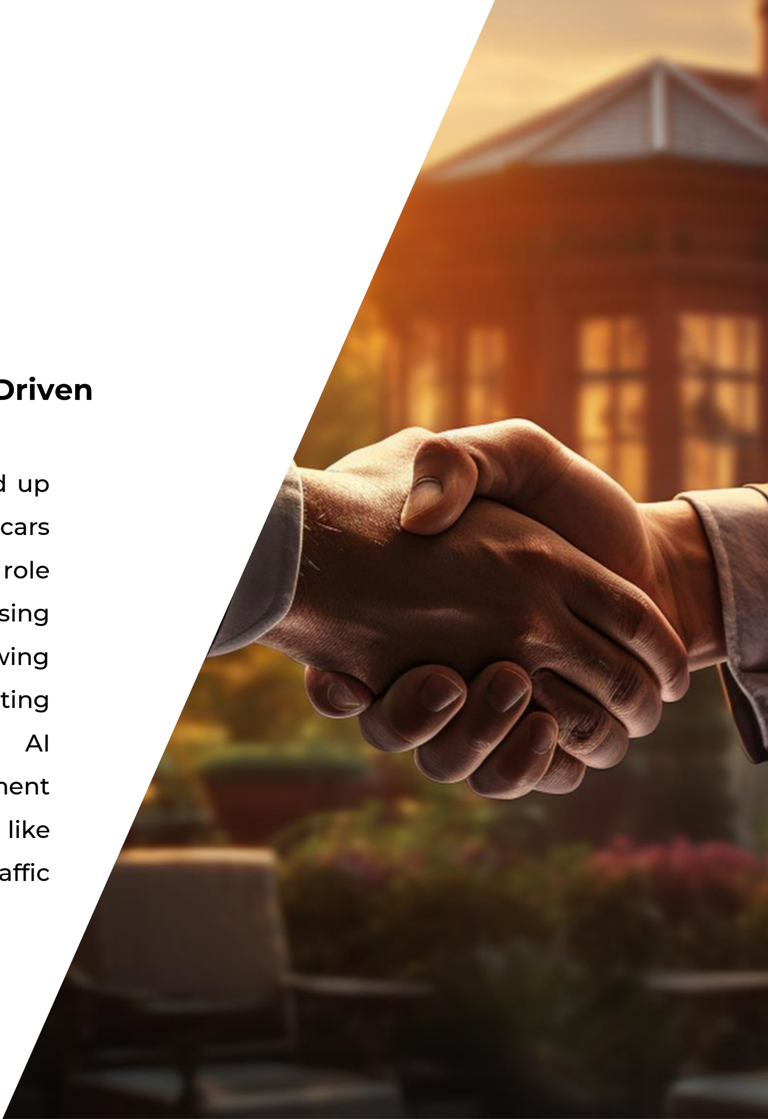
□ Patents published in the previous month emphasize on pattern-recognition techniques to address vulnerabilities in Controller Area Network (CAN) systems. Incorporating techniques like error counters, policy-based Intrusion Detection Systems (IDS), and dynamic traffic flow analysis, these solutions aim to detect and mitigate real-time anomalies, setting new standards for cost-effective, efficient, and precise cybersecurity in connected cars.

Collaboration

Clavister and NXP Collaborate to Advance AI-Driven Cybersecurity in the Automotive Industry

Clavister, a European cybersecurity provider, has teamed up with NXP Semiconductors to enhance cybersecurity for cars using artificial intelligence (AI). NXP, known for its leading role in automotive technology, aims to address the increasing cybersecurity challenges faced by modern vehicles following new UN regulations. The collaboration focuses on preventing cyber threats in connected cars, using Clavister's AI technology integrated with NXP's OrangeBox Development Platform. This system can detect real-time cyberattacks like denial-of-service (DOS) attacks through vehicle traffic analysis.

Source
https://www.clavister.com/

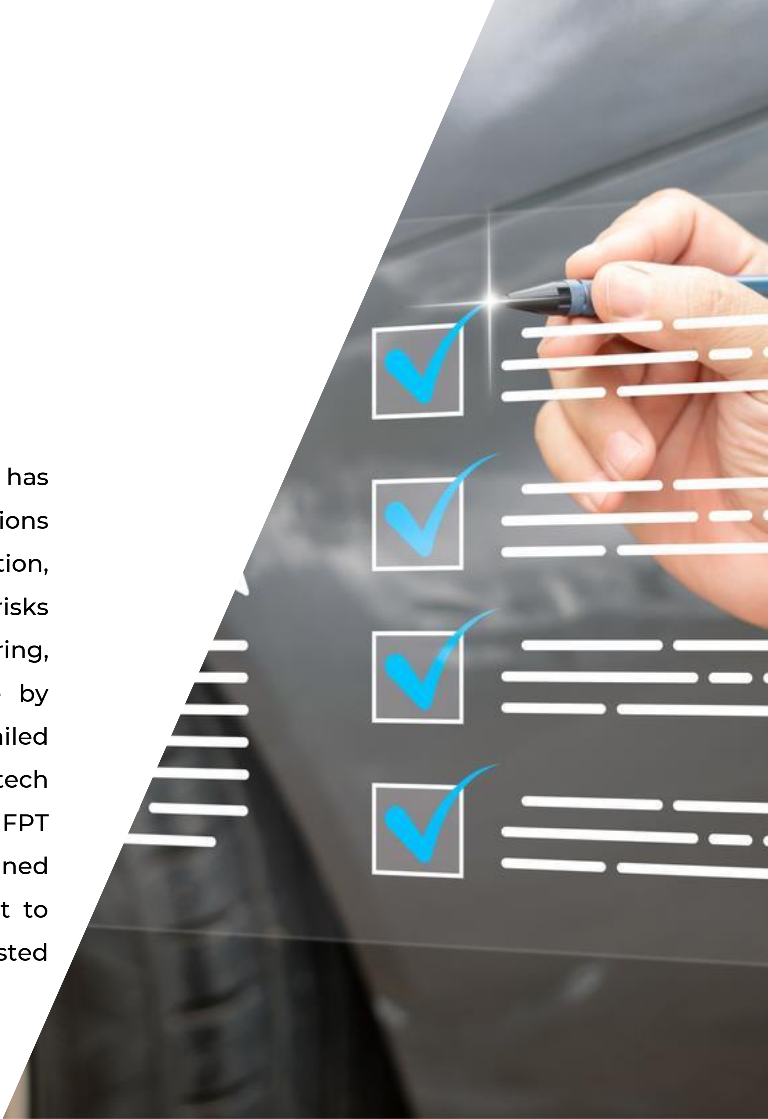


Certification

FPT Achieves ISO SAE 21434 Certification for Automotive Cybersecurity

FPT, a top automotive software company from Vietnam, has become the first Association of Southeast Asian Nations (ASEAN) business to earn the ISO/SAE 21434 certification, which ensures road vehicles are protected from cyber risks throughout their lifecycle, covering design, manufacturing, maintenance, and more. FPT achieved this milestone by training its engineers extensively and developing detailed compliance processes. With two decades of automotive tech experience, FPT also formed its dedicated subsidiary, FPT Automotive, to cater to the demand for software-defined vehicles. This certification showcases FPT's commitment to global standards and solidifies its position as a trusted technology partner for leading car manufacturers.

Source
https://fptsoftware.com/



Dennemeyer
The IP Group

Industry News

Vehicle fleet security

Bezeq International, Enigmatos join forces to secure commercial vehicle fleets

Bezeq International, a leader in communication and cybersecurity, has partnered with Enigmatos, an expert in vehicle cybersecurity technologies, to enhance protection for commercial vehicle fleets. They have integrated their services to enable real-time detection and prevention of cyberattacks. The focus is on securing the Controller Area Network (CAN), which vehicles use for internal communication. Enigmatos, known for safeguarding large fleets like Hungary's public transport, brings its expertise to enhance vehicle safety and protect sensitive data, while Bezeq's team swiftly monitors and addresses threats, tackling risks in the increasingly connected automotive industry.

Source
https://www.jpost.com/

Partnership

Deloitte Spain and PlaxidityX Join Forces to Deliver Transformative Automotive Cyber Security Solutions

PlaxidityX and Deloitte have joined forces to create a Vehicle Security Operations Center (VSOC) solution aimed at combating cyberattacks on connected vehicles. This solution combines PlaxidityX's advanced detection and response (XDR) platform with Deloitte's expertise in managed security services to provide real-time threat detection, analytics, and swift responses. Specifically designed for vehicle security, the VSOC ensures compliance with automotive cybersecurity regulations, standards like UN R155 and ISO/SAE 21434. With PlaxidityX already securing over 72 million vehicles globally, this partnership promises stronger cybersecurity for automakers and a safer automotive ecosystem.

Source
https://plaxidityx.com/

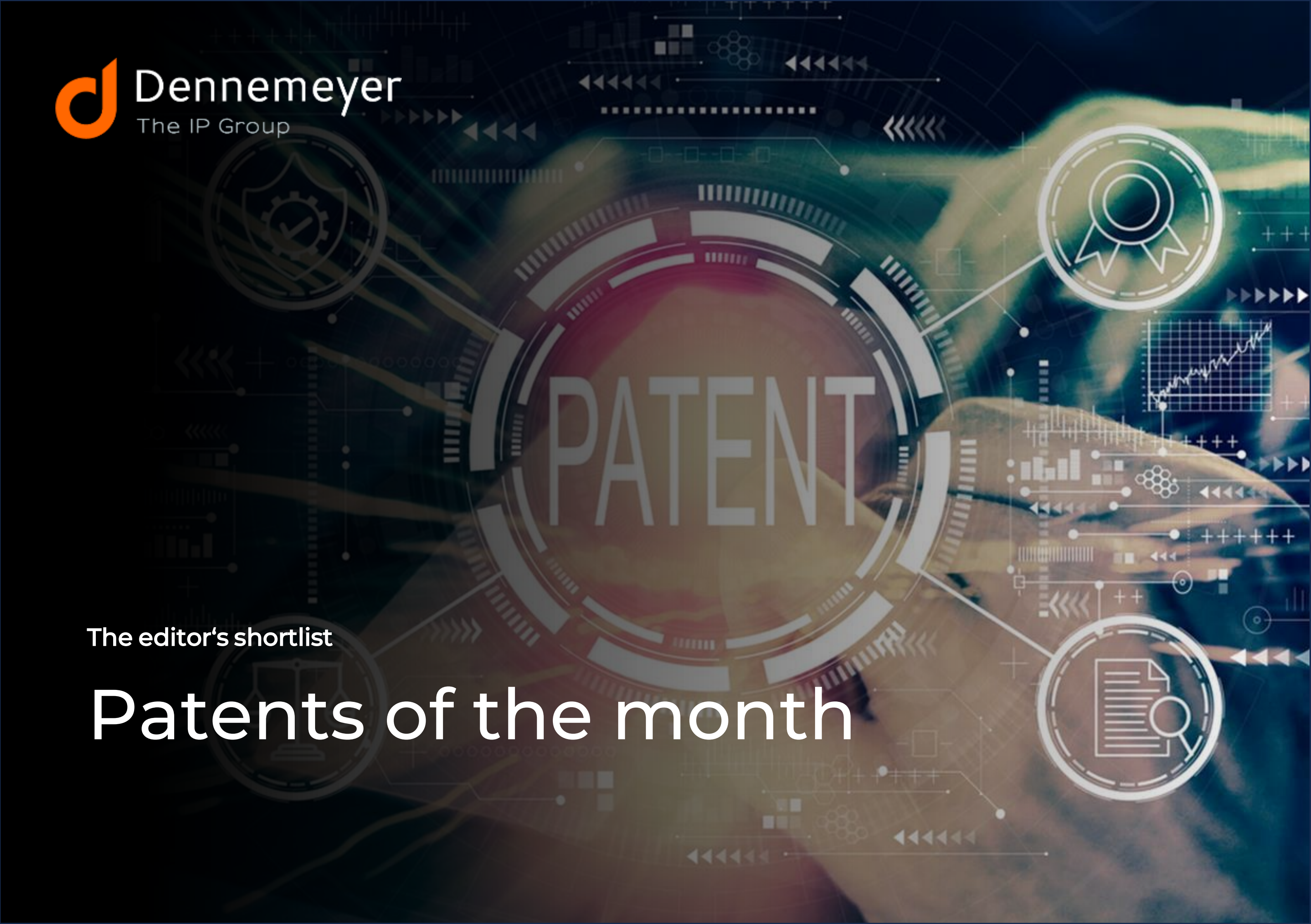
Decentralized automotive safety

Siemens Cre8Ventures & Minima: A Partnership to Set To Revolutionize Robotics, Automotive, Energy, and Healthcare Equipment

Siemens has joined forces with Minima, a decentralized blockchain provider, to enhance security in industries like automotive, energy, and healthcare. Their collaboration brings advanced AI, robust data integrity, and decentralized security solutions to Siemens' Digital Twin Marketplace. For automotive security enhancements this system ensures secure communication, tamper-proof data integrity, Decentralized Security Infrastructure, and Smart Contracts for Automotive Transactions, addressing key challenges in automotive cybersecurity and compliance. By combining efforts, they aim to drive secure innovation across critical sectors while enabling startups and industry leaders to adopt safer technologies.

Source
https://blogs.sw.siemens.com/

Dennemeyer
The IP Group



The editor‘s shortlist

Patents of the month

Dennemeyer
The IP Group

Patents of the month

Published in March 2025

Shortlisted and summarized by our analyst

- US12244615B2 - Method for protection from cyber attacks to a vehicle based upon time analysis, and corresponding device
  Assignee: Marelli Europe SPA
- US2025103705A1 - IDPS dynamic allocation device and method based on resource usage recognition
  Assignee: Hyundai Motor Co; Kia Corp
- US12248579B1 - AI-based vehicle cybersecurity with 5G/6G sub-network topology
  Assignee: Newman David E, Massengill R Kemp
- WO2025062231A1 - Systems and methods of securing vehicle services from denial-of-service attacks using dynamic signature
  Assignee: Nio Technology Anhui Co Ltd
- EP4522444A2 - Systems, methods, and apparatus for cyberattack mitigation and protection for extreme fast charging infrastructure
  Assignee: Battelle Energy Alliance LLC
- DE102016108923B4 - Spoofing detection
  Assignee: Ford Global Technologies
- DE102023208599A1 - Automated detection of known vulnerability
  Assignee: Robert Bosch GMBH
- IN202421020626A - System to detect an intrusion at a smart vehicle and/or components thereof
  Assignee: Matter Motor Works Pvt Ltd
- JP2025041520A - Apparatus and method for constructing an intrusion detection system utilizing intrusion detection rules applied to CAN communication
  Assignee: Autocrypto Company Limited
- KR20250032729A - Vehicle control system for detecting hacking on can communication network and operating in normal state and method for operation thereof
  Assignee: Korea Institute of Engineering and Technology Industry-Academic Cooperation Foundation

US12244615B2

Method for protection from cyber attacks to a vehicle based upon time analysis, and corresponding device

Company name	Marelli Europe SPA
Inventors	Rosadini Christian, Chiarelli Simona, Nesci Walter, Saponara Sergio, Gagliardi Alessio, Dini Pierpaolo
Priority date	06 Sep 2021
Publication date	04 Mar 2025

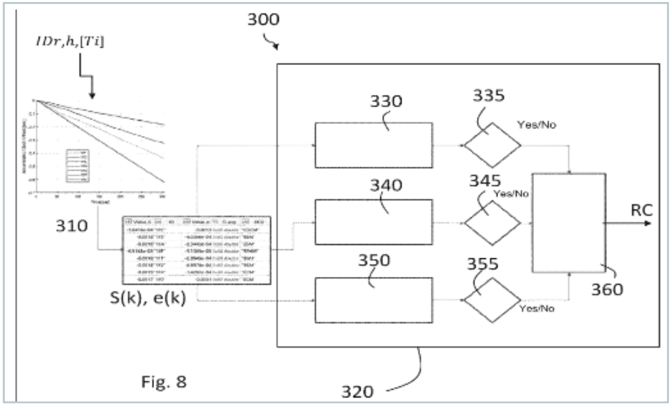


Fig. 8

This patent focuses on enhancing vehicular cybersecurity by addressing weaknesses in Controller Area Network (CAN) communications, where current systems can detect attacks but struggle to pinpoint their source. The proposed solution analyzes regular messages exchanged within the network to identify anomalies. It categorizes these messages based on their transmission frequency, evaluates arrival times, calculates offsets, and employs mathematics (regression analysis) to uncover suspicious activity. By examining patterns and relationships in the data, it distinguishes genuine messages from potentially compromised ones.

Summarized by Dennemeyer

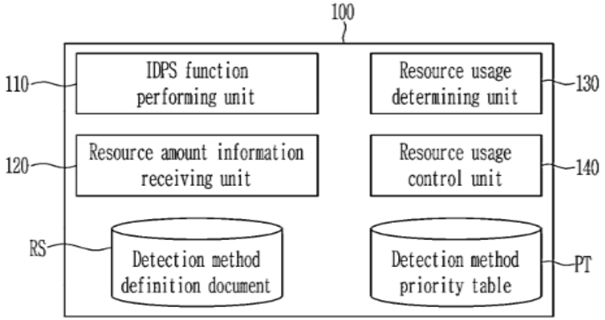
US2025103705A1

IDPS dynamic allocation device and method based on resource usage recognition

Company name	Hyundai Motor Co; Kia Corp
Inventors	Choi Hakhui
Priority date	27 Sep 2023
Publication date	27 Mar 2025

Summarized by Dennemeyer

FIG. 2


100
110
IDPS function performing unit
Resource usage determining unit
130
120
Resource amount information receiving unit
Resource usage control unit
140
RS
Detection method definition document
Detection method priority table
PT

This patent explains a method to ensure a vehicle's Intrusion Detection and Prevention System (IDPS) doesn’t overwhelm its main control unit (ECU) or disrupt critical vehicle functions. The suggested approach employs a dynamic allocation device that monitors resource usage in real time. If usage exceeds predefined limits, it deactivates lower-priority detection methods based on a set priority list. This approach keeps the IDPS operating efficiently without impacting the ECU’s performance, ensuring optimal resource management, effective threat detection, and secure vehicle operations while enhancing cybersecurity in connected cars.

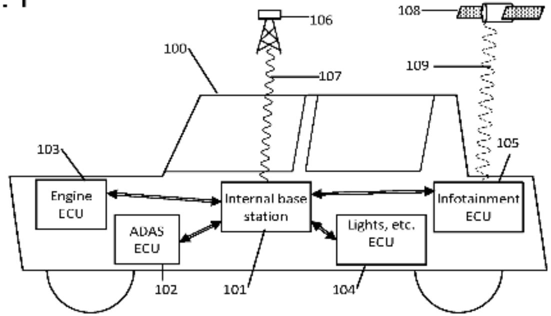
US12248579B1

AI-based vehicle cybersecurity with 5G/6G sub-network topology

Company name	Newman David E, Massengill R Kemp
Inventors	Newman David E, Massengill R Kemp
Priority date	24 Aug 2023
Publication date	11 Mar 2025

Summarized by Dennemeyer

FIG. 1



This patent introduces a new 5G/6G network design to address cybersecurity threats in modern vehicles, which rely heavily on interconnected electronic control units (ECUs) and sensors. Inside the vehicle, a wireless network is established where ECUs are registered as user devices and communicate wirelessly with an internal base station. Each ECU is connected to sensors or actuators equipped with processors and wireless transmitters to ensure secure communication. A special (Doppler-corrected) wireless link facilitates communication between the vehicle's internal network and an external base station. AI-powered detection mechanisms safeguard communications at both the ECU and device levels, ensuring that only authorized data exchanges occur.

WO2025062231A1

Systems and methods of securing vehicle services from denial-of-service attacks using dynamic signature

Company name	Nio Technology Anhui Co Ltd
Inventors	Cai Hao, Xie Haiyong, Wang Qingyuan, Zhao Minzheng
Priority date	19 Sep 2023
Publication date	27 Mar 2025

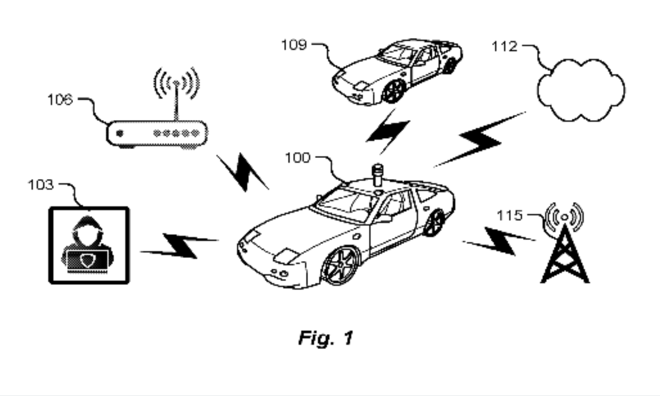


Fig. 1

This patent discusses vulnerabilities in vehicle systems to denial-of-service (DoS) attacks, which can disrupt performance as vehicles increasingly rely on data from sensors and networks. The presented idea analyzes dynamically changing traffic flow signatures to detect and prevent such attacks. It examines communication session data, assigns quality of service (QoS) priorities, and compares actual traffic to expected patterns. Valid sessions are prioritized, while suspicious ones are dropped, and expectations are adjusted in real time to prevent repeated attacks. The approach enhances security with dynamic updates, integrates system components, and ensures effective protection without impacting performance.

EP4522444A2

Systems, methods, and apparatus for cyberattack mitigation and protection for extreme fast charging infrastructure

Company name	Battelle Energy Alliance LLC
Inventors	Rohde Kenneth W, Carlson Richard W, Salinas Sean C, Crepeau Matthew J
Priority date	10 May 2022
Publication date	19 Mar 2025

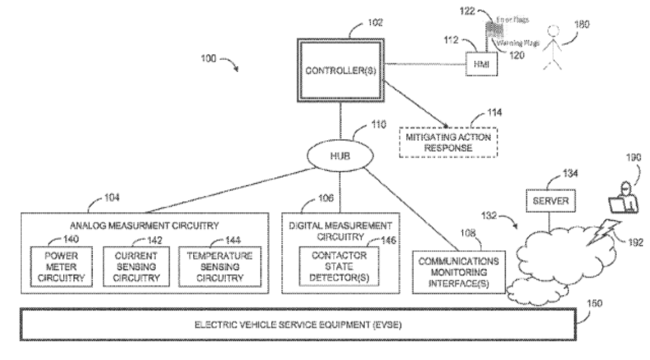

100
102
CONTROLLER(S)
112
HMI
122
Error Flags
Warning Flags
120
180
110
HUB
114
MITIGATING ACTION RESPONSE
190
134
SERVER
104
ANALOG MEASURMENT CIRCUITRY
140
POWER METER CIRCUITRY
142
CURRENT SENSING CIRCUITRY
144
TEMPERATURE SENSING CIRCUITRY
106
DIGITAL MEASUREMENT CIRCUITRY
146
CONTACTOR STATE DETECTOR(S)
108
COMMUNICATIONS MONITORING INTERFACE(S)
132
192
150
ELECTRIC VEHICLE SERVICE EQUIPMENT (EVSE)

FIG. 1

The patent addresses cybersecurity risks specifically in vehicular fast-charging infrastructure that threaten safety and operational reliability. It introduces a system designed to remove these risks using controllers that work with analog circuitry and a communications monitoring interface to identify anomalies in signals and monitored communications. Upon detecting such conditions, protective actions are initiated to ensure the secure operation of the electric vehicle supply equipment (EVSE). This innovation enhances cybersecurity for EVSE by offering precise detection and immediate mitigation of potential threats, thereby maintaining integrity and safety in high-power EV charging setups.

❮ DE102016108923B4

Spoofing detection

Company name	Ford Global Technologies
Inventors	James Martin Lawlis
Priority date	19 May 2015
Publication date	27 Mar 2025

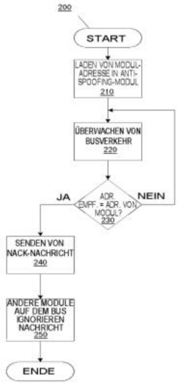

200
START
LADEN VON MODUL-ADRESSE IN ANTI-SPOOFING-MODUL
210
ÜBERWACHEN VON BUSVERKEHR
220
ADR. EMPF. = ADR. VON MODUL?
230
JA
NEIN
SENDEN VON NACK-NACHRICHT
240
ANDERE MODULE AUF DEM BUS IGNORIEREN NACHRICHT
250
ENDE

FIG. 3

This patent tackles the problem of spoofing in automotive networks, where fake devices pretend to be legitimate electronic control units (ECUs) and send false messages, potentially causing dangerous actions by vehicle systems. The suggested approach monitors network messages, storing the address of the real ECU and comparing it against incoming messages. If a message falsely claims to be from the legitimate ECU, a negative acknowledgment (NACK) is sent to warn other ECUs to ignore it. Repeated NACKs from the same sender lead to its removal from the communication system.

DE102023208599A1

Automated detection of known vulnerability

Company name	Robert Bosch GMBH
Inventors	Nicolae Irina, Ring Martin
Priority date	06 Sep 2023
Publication date	06 Mar 2025

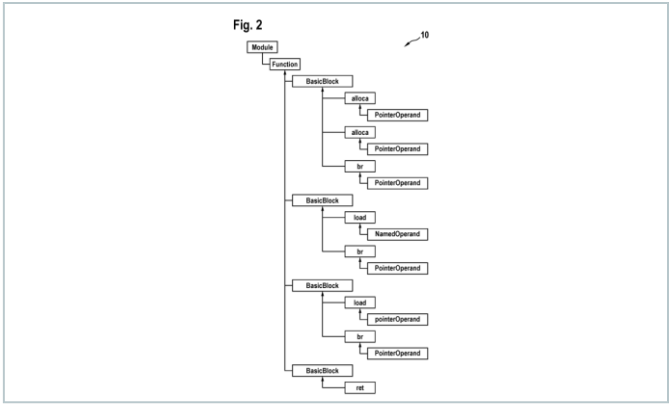


Fig. 2

This patent focuses on the issue of detecting software vulnerabilities in complex systems like vehicle computing units. Traditional methods often generate many false positives, making it hard for developers to pinpoint real security threats. It uses an automated process with static code analysis to extract necessary data from the software, identifies its key components, and matches them against known vulnerabilities using machine learning. This approach helps pinpoint the actual problems while minimizing false alarms. By combining automation and machine learning, it enhances accuracy, reduces manual effort, and ensures continuous monitoring of the software, improving security management throughout its lifecycle.

IN202421020626A

System to detect an intrusion at a smart vehicle and/or components thereof

Company name	Matter Motor Works Pvt Ltd
Inventors	Kumar Prasad Telikepalli, Satish Thimmalapura, Sunjeev Arora, Pankaj Kumar Bharti
Priority date	19 Mar 2024
Publication date	14 Mar 2025

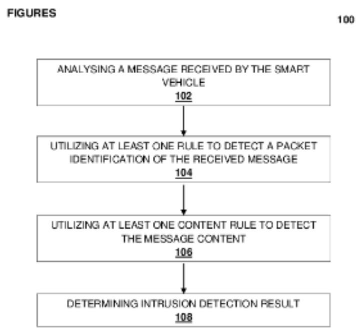

FIGURES
100
ANALYSING A MESSAGE RECEIVED BY THE SMART VEHICLE
102
UTILIZING AT LEAST ONE RULE TO DETECT A PACKET IDENTIFICATION OF THE RECEIVED MESSAGE
104
UTILIZING AT LEAST ONE CONTENT RULE TO DETECT THE MESSAGE CONTENT
106
DETERMINING INTRUSION DETECTION RESULT
108

FIG. 1

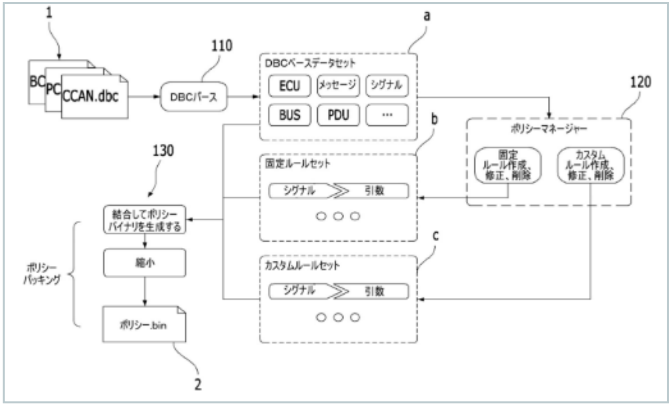
This patent talks about enhancing cybersecurity in smart vehicles by addressing vulnerabilities in their communication networks, such as the Controller Area Network (CAN) and others. The proposed system involves a computer that analyzes incoming messages to verify identifiers and content. It uses specific rules to identify irregularities in message details or identification, producing two separate results to assist in detecting issues. Based on these results, the system determines whether an intrusion has occurred.

JP2025041520A

Apparatus and method for constructing an intrusion detection system utilizing intrusion detection rules applied to CAN communication

Company name	Autocrypto Company Limited
Inventors	Kim duk so
Priority date	13 Sep 2023
Publication date	26 Mar 2025

Summarized by Dennemeyer

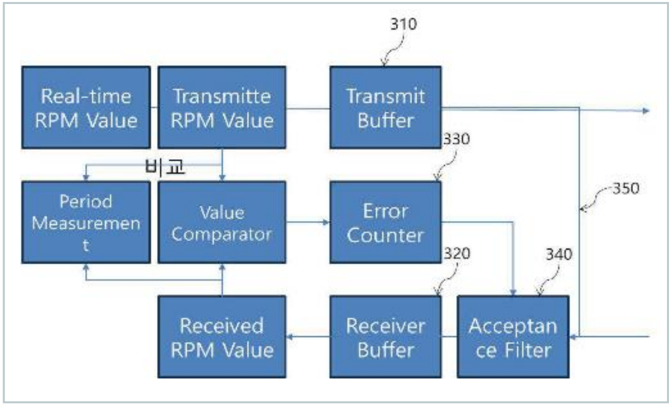


This patent discusses the development of an intrusion detection system (IDS) for Controller Area Network (CAN) communications used in vehicles, addressing the increasing need for vehicle cybersecurity due to technologies like self-driving and Vehicle-to-everything (V2X) communication. The system detects unusual or suspicious messages in the vehicle's network, particularly those that deviate from regular patterns, to prevent attacks more effectively. It accomplishes this by analyzing CAN data to extract key details, applying detection rules, and consolidating these rules into a policy file. This policy file serves as the foundation of the IDS, enabling accurate and reliable risk detection while ensuring robust security for modern automotive communication networks.

KR20250032729A

Vehicle control system for detecting hacking on can communication network and operating in normal state and method for operation thereof

Company name	Korea Institute of Engineering and Technology Industry-Academic Cooperation Foundation
Inventors	Seokhyun Seo
Priority date	30 Aug 2023
Publication date	07 Mar 2025



This patent tackles security issues in vehicle control systems that use Controller Area Network (CAN) communication, where unencrypted messages are vulnerable to hacking attempts that could disrupt vehicle functions. The solution uses controllers that regularly send messages with specific identifiers about vehicle parameters. If a message with the same identifier arrives too soon, an error counter increases. Once the counter reaches a set limit, the system sends a warning about a possible hack and blocks it. This approach enhances safety by detecting unexpected data patterns in real time without requiring extra encryption hardware, making the system both efficient and secure.

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.