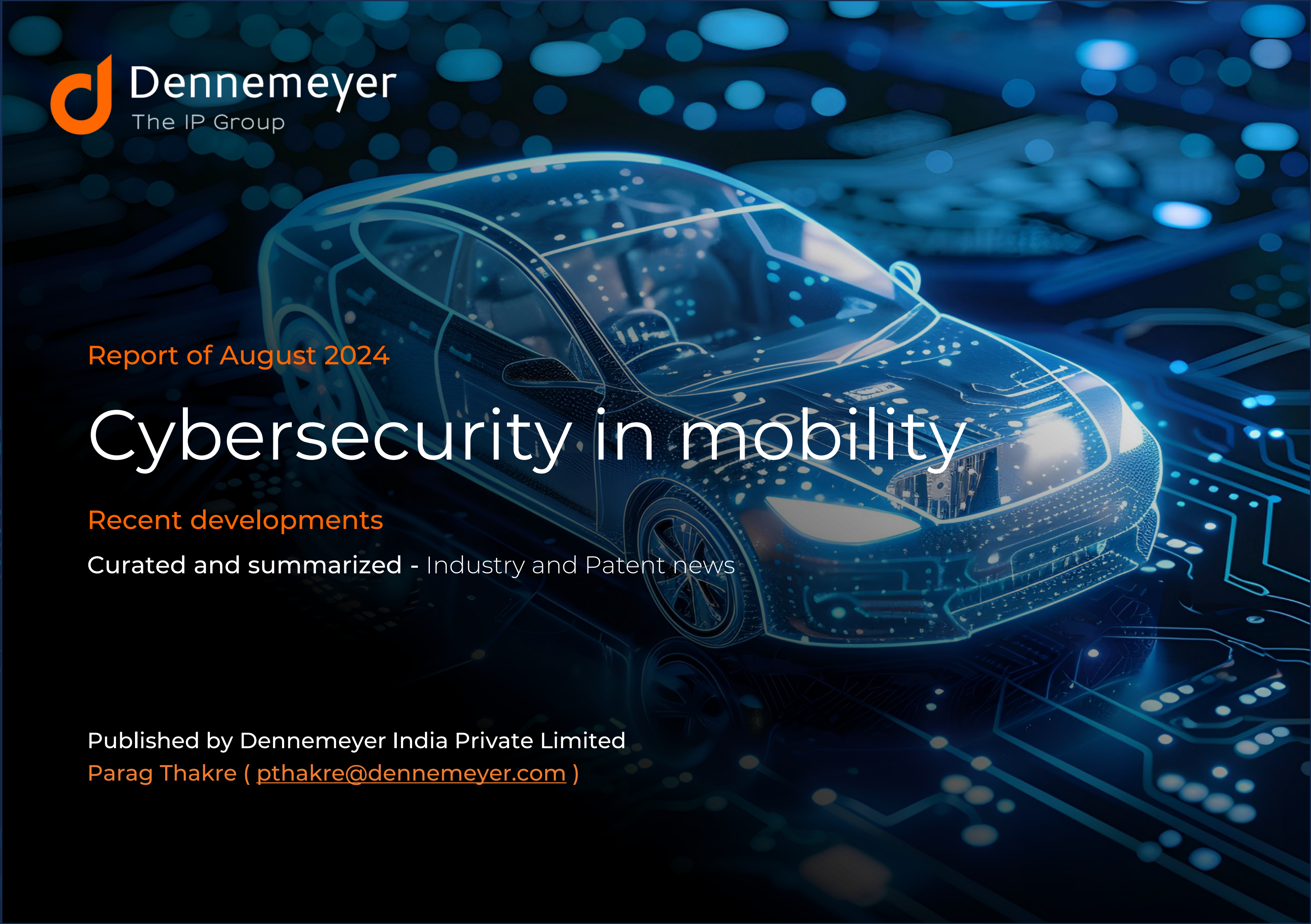
Dennemeyer
The IP Group



Report of August 2024

Cybersecurity in mobility

Recent developments

Curated and summarized - Industry and Patent news

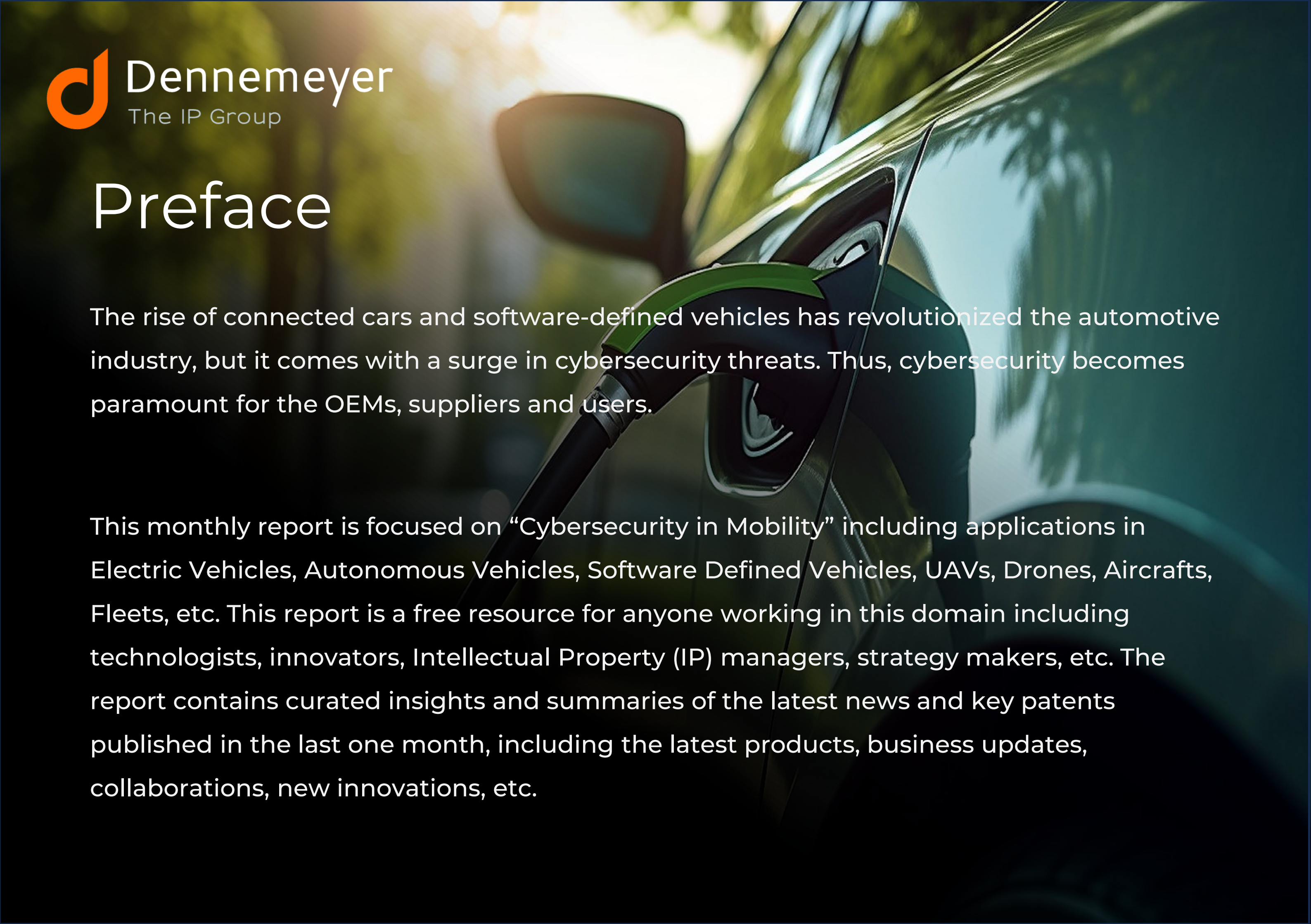
Published by Dennemeyer India Private Limited

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.

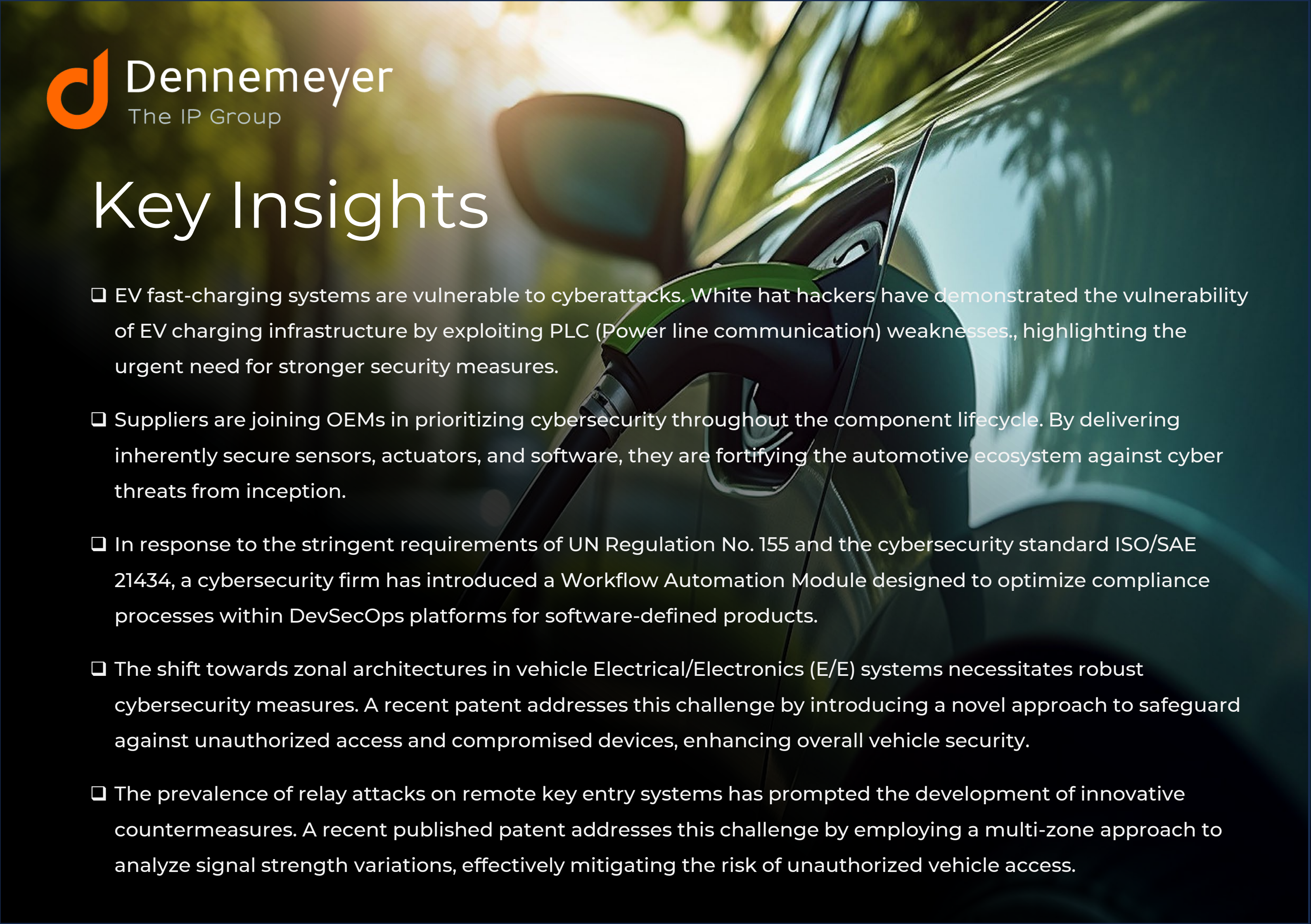


Preface

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.

Dennemeyer
The IP Group



Key Insights

❑ EV fast-charging systems are vulnerable to cyberattacks. White hat hackers have demonstrated the vulnerability of EV charging infrastructure by exploiting PLC (Power line communication) weaknesses., highlighting the urgent need for stronger security measures.

❑ Suppliers are joining OEMs in prioritizing cybersecurity throughout the component lifecycle. By delivering inherently secure sensors, actuators, and software, they are fortifying the automotive ecosystem against cyber threats from inception.

❑ In response to the stringent requirements of UN Regulation No. 155 and the cybersecurity standard ISO/SAE 21434, a cybersecurity firm has introduced a Workflow Automation Module designed to optimize compliance processes within DevSecOps platforms for software-defined products.

❑ The shift towards zonal architectures in vehicle Electrical/Electronics (E/E) systems necessitates robust cybersecurity measures. A recent patent addresses this challenge by introducing a novel approach to safeguard against unauthorized access and compromised devices, enhancing overall vehicle security.

❑ The prevalence of relay attacks on remote key entry systems has prompted the development of innovative countermeasures. A recent published patent addresses this challenge by employing a multi-zone approach to analyze signal strength variations, effectively mitigating the risk of unauthorized vehicle access.

Partnership

FPT Software and VinCSS Join Hands to Accelerate Cybersecurity in Automotive Industry

FPT Software and VinCSS have partnered to enhance cybersecurity in the automotive sector. By combining their expertise and resources, they aim to provide comprehensive solutions to OEMs and Tier 1 suppliers, meeting stringent global standards. FPT Software will integrate VinCSS's cybersecurity solutions into its offerings, expanding its market reach to the US and Europe. In return, VinCSS gains access to FPT Software's global client network. Both companies will collaborate on developing new solutions, training initiatives, and business opportunities to boost safety and improve customer experience in connected mobility.

Source
https://fptsoftware.com/

EV-charger security

SwRI evaluates cybersecurity risks associated with EV fast-charging equipment

Researchers at Southwest Research Institute have uncovered significant cybersecurity vulnerabilities in electric vehicles using rapid DC fast-charging systems. By exploiting weaknesses in the power line communication layer (PLC), they gained unauthorized access to both the charging equipment and the vehicle itself. These findings highlight the urgent need for stronger encryption and security measures in EV charging infrastructure to protect against potential cyberattacks, data breaches, and disruptions to the charging process, as well as the broader electric grid.

Source
https://www.swri.org/

Securing Smart car

From Vietnam to the World: VinCSS Introduces Initiative to Protect Smart Vehicles

A Vietnamese cybersecurity company, VinCSS, has introduced a new solution to protect smart car software and data from cyberattacks. Their system leverages the FIDO Device Onboarding Protocol to create a secure environment for communication between devices and vehicles. This prevents unauthorized access and malicious software installation, safeguarding the car's navigation, safety, and user privacy. This innovation comes at a critical time, as the number of smart cars is projected to explode, creating a massive potential target for hackers.

Source
https://blog.vincss.net/

Dennemeyer
The IP Group

Industry News

Standard Certification

MCNEX. Achieves International Standard Certification for Automotive Cybersecurity

MCNEX, a Korean automotive technology company specializing in cameras, sensors, and software, has achieved ISO/SAE 21434 cybersecurity certification from DNV. This certification, mandatory for all mass-produced vehicles in major global markets starting July 2024, validates MCNEX's commitment to robust cybersecurity practices across its entire product lifecycle. The company's expertise is now recognized as meeting the highest international standards for vehicle security.

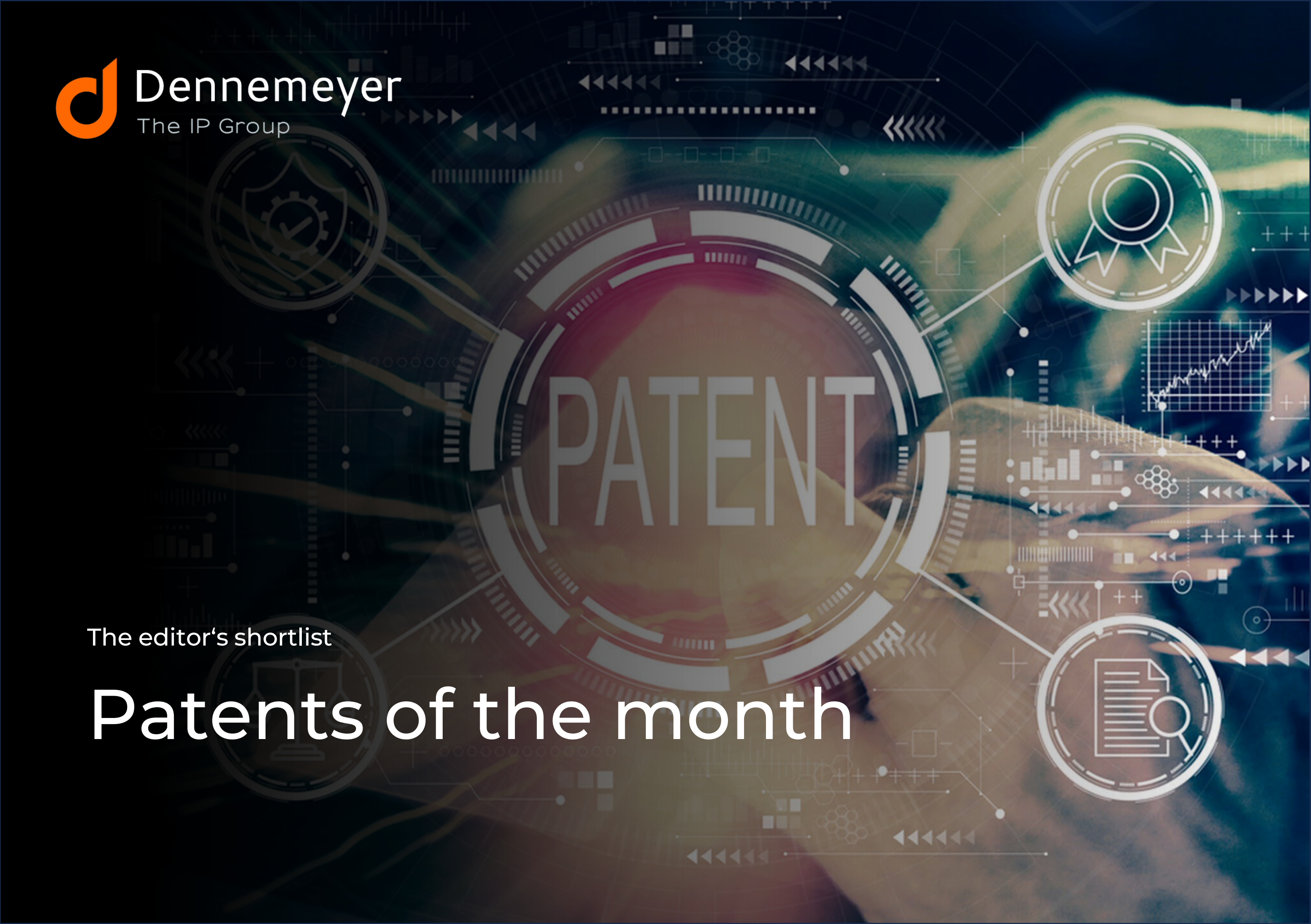
Source
https://mcnex.com/

Regulatory Compliance

C2A Security Adds a Workflow Automation Module to its Product DevSecOps Platform to Address the Increased Demand for Efficient Regulatory Compliance for Software-Defined Products

C2A Security has launched a new Workflow Automation Module for its EVSec DevSecOps platform to streamline compliance processes and enhance operational efficiency for software-defined products. The module automates tasks, integrates with various tools, and offers customizable workflows to help companies like Daimler Truck AG navigate complex regulations like UN Regulation No. 155, ISO/SAE 21434, and NIST 8473, reducing compliance burdens and operational risks while improving product security.

Source
https://c2a-sec.com/



The editor‘s shortlist

Patents of the month

Patents of the month

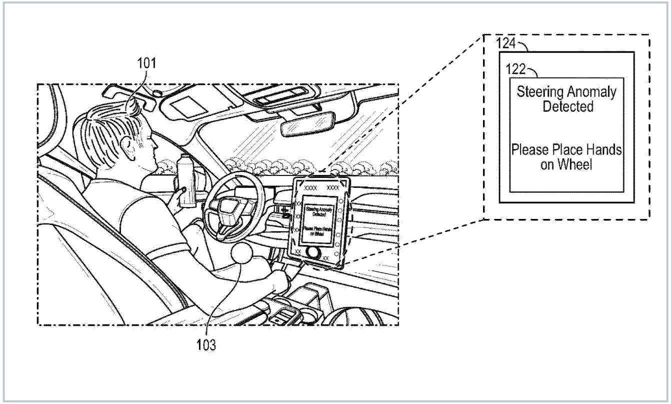
Published in July 2024

Shortlisted and summarized by our analyst

- US2024227869A1 - Systems and methods for mitigating spoofing of vehicle features
  Assignee: Ford Global Technologies
- US12047352B2 - Security configurations for zonal computing architecture
  Assignee: Micron Technology
- US2024236131A1 - Vehicle security analysis device, method, and program thereof
  Assignee: NTT Communications , NTT Security Japan
- US2024223581A1 - Detection rule output method, security system, and detection rule output device
  Assignee: Panasonic Automotive Systems Co Ltd
- US12052275B2 - Method for protection from cyber attacks to a vehicle, and corresponding device
  Assignee: Marelli Europe SPA
- US12036947B2 - Method and system for relay attack prevention using subzones
  Assignee: Robert Bosch GMBH
- EP4405836A1 - Techniques for misbehavior detection in wireless communications systems
  Assignee: Qualcomm INC
- EP4363888A4 - Method for detecting anomalies of lidar point cloud data and related device
  Assignee: Huawei Investment & Holding Co Ltd
- IN202411049438A - A system and a method for vehicle security and threat scanner
  Assignee: Individual Inventor
- CN118339553A - Detection and mitigation of cyber attacks on aimed at vehicle's diagnostic sessions
  Assignee: Red Bend Ltd (Samsung Group)

US2024227869A1

Systems and methods for mitigating spoofing of vehicle features



Company name	Ford Global Technologies
Inventors	Herman David Michael, Amodeo Catherine Marie, Jain Yashanshu, Colarusso Christopher
Priority date	01-Apr-2022
Publication date	11-Jul-2024

The patent addresses the vulnerability of ADAS systems to spoofing attacks that mimic human input, potentially compromising safety. It introduces a novel approach to detect spoofing by analyzing steering torque sensor data in conjunction with road disturbance models and machine learning algorithms. This system can accurately differentiate between genuine and spoofed inputs, enabling automated responses like vehicle slowdown or deactivation of autonomous modes, significantly enhancing vehicle safety against spoofing threats.

US12047352B2

Security configurations for zonal computing architecture

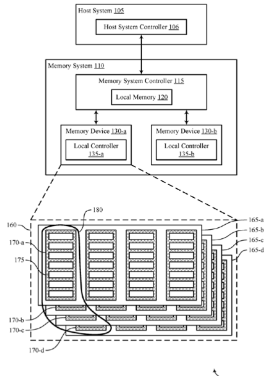


FIG. 1

Company name	Micron Technology
Inventors	Kale Poorna, Bielby Robert Noel
Priority date	29-Dec-2021
Publication date	23-Jul-2024

The patent addresses the growing security concerns in vehicle zonal computing systems by introducing a novel approach to device authentication. It proposes a system where each device must authenticate itself through a memory-based verification process before being allowed to communicate with central processors. This method, coupled with periodic re-authentication and update verification, significantly enhances the security posture of the vehicle by preventing unauthorized access and mitigating risks associated with compromised devices, thereby safeguarding the overall integrity of the zonal computing architecture.

Dennemeyer
The IP Group

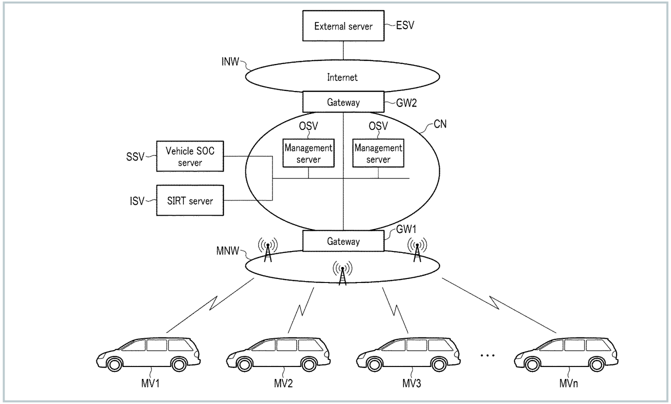
Latest patents

US2024236131A1

Vehicle security analysis device, method, and program thereof

Company name	NTT Communications , NTT Security Japan
Inventors	Ueno Satoshi, Wakasugi Atsushi, Nakata Kensuke, Chiba Yasunobu
Priority date	24-Sep-2021
Publication date	11-Jul-2024

Summarized by Dennemeyer



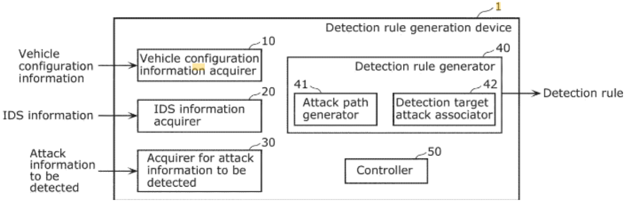
The patent introduces a novel approach to analyzing cyberattacks on connected vehicles by correlating multiple individual attacks over time to uncover broader attack scenarios. By processing sensor log data and comparing it against predefined attack patterns, the system can identify complex attack patterns that would be missed by traditional methods focused on isolated attacks. This comprehensive analysis enables a deeper understanding of cyber threats, leading to more effective prevention and response strategies for safeguarding connected vehicles.

US2024223581A1

Detection rule output method, security system, and detection rule output device

Company name	Panasonic Automotive Systems Co Ltd
Inventors	Takeuchi Akihito, Kawaguchi Nobutaka, Torisaki Yuishi
Priority date	19-Aug-2021
Publication date	04-Jul-2024

FIG. 1


1
Detection rule generation device
Vehicle configuration information
10
Vehicle configuration information acquirer
40
Detection rule generator
IDS information
20
IDS information acquirer
41
Attack path generator
42
Detection target attack associator
Detection rule
Attack information to be detected
30
Acquirer for attack information to be detected
50
Controller

The patent proposes an automated method to generate tailored detection rules for vehicle security systems. By leveraging vehicle configuration details, intrusion detection system data, and specific attack information, the system can output comprehensive detection rules identifying potential abnormality locations within the vehicle's network. This approach simplifies rule creation, enhances accuracy, and allows for prioritization of detection efforts, ultimately improving the vehicle's cybersecurity posture.

Dennemeyer
The IP Group

Latest patents

US12052275B2

Method for protection from cyber attacks to a vehicle, and corresponding device

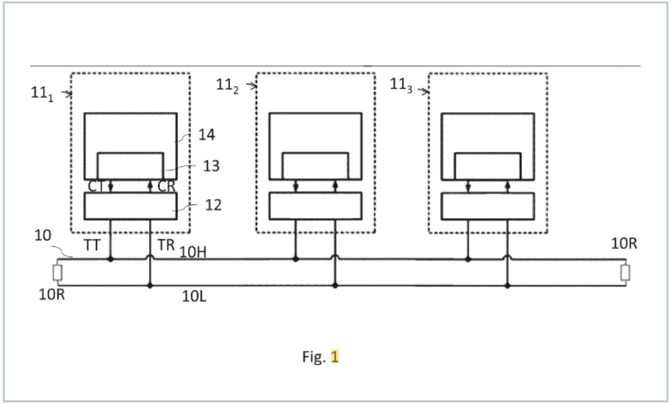


Fig. 1

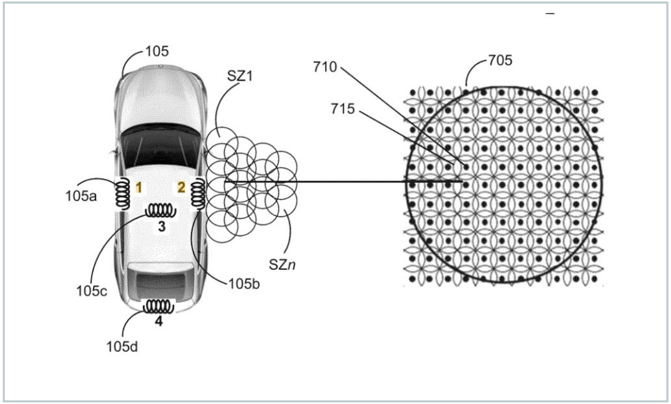
Company name	Marelli Europe SPA
Inventors	Rosadini Christian, Cornelio Anastasia, Nesci Walter, Saponara Sergio, Gagliardi Alessio, De Cesare Paola
Priority date	26-May-2021
Publication date	30-Jul-2024

Summarized by Dennemeyer

The patent introduces a novel approach to enhance vehicle cybersecurity by accurately identifying the source and type of cyberattacks on the CAN bus. It employs statistical analysis and machine learning to analyze voltage levels of CAN messages, classifying them based on their originating node and distinguishing between internal and external attacks. This advanced monitoring system not only detects intrusions but also provides crucial information about the attack source, enabling timely and targeted countermeasures to protect the vehicle.

US12036947B2

Method and system for relay attack prevention using subzones



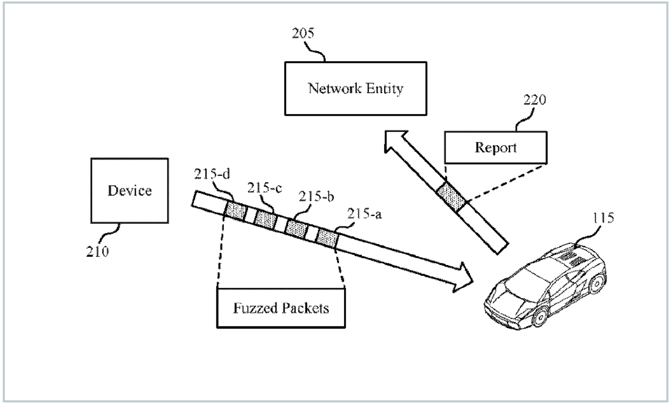
Company name	Robert Bosch GMBH
Inventors	Kelly Matthew
Priority date	10-Dec-2018
Publication date	16-July-2024

Summarized by Dennemeyer

The patent addresses the vulnerability of Passive Entry Passive Start (PEPS) systems to relay attacks by introducing a novel method for detecting the presence of a relay device. By dividing the vehicle's inclusion zone into multiple subzones and analyzing signal strength variations, the system can accurately differentiate between legitimate key fobs and relay-based attempts. Continuous monitoring and adaptive subzone management enhance the system's effectiveness in preventing unauthorized vehicle access.

EP4405836A1

Techniques for misbehavior detection in wireless communications systems



Company name	Qualcomm INC
Inventors	Petit Jonathan, Monteuuis Jean-philippe, Ansari Mohammad Raashid, Chen Cong
Priority date	24-Sep-2021
Publication date	31-Jul-2024

The patent proposes a novel method to detect fuzzing attacks in V2X communications by analyzing packet information elements (IEs) over time. It identifies potential attacks by comparing IE values against their defaults and generates aggregated reports of detected fuzzing patterns. This approach improves detection accuracy by considering multiple messages rather than isolated incidents and utilizes machine learning for enhanced pattern recognition. By streamlining the reporting process, the system reduces computational overhead while providing valuable insights for security enhancement.

EP4363888A4

Method for detecting anomalies of lidar point cloud data and related device

Company name	Huawei Investment & Holding Co Ltd
Inventors	Revadigar Girish Shivalingappa, Wei Zhuo, Kang Suk, Seo Kang, Lee Hwejae, Kwak Byung, Kim Huy Kang, Jeong Seonghoon
Priority date	24-Aug-2021
Publication date	31-Jul-2024

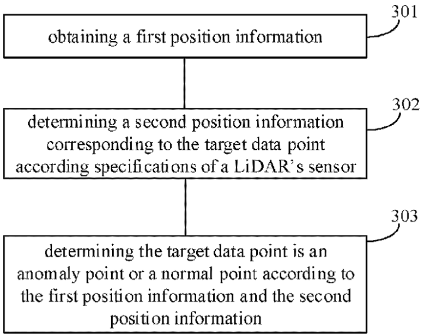

301
obtaining a first position information
302
determining a second position information corresponding to the target data point according specifications of a LiDAR's sensor
303
determining the target data point is an anomaly point or a normal point according to the first position information and the second position information

FIG. 3

The patent introduces a novel method to enhance the reliability and security of LiDAR systems by detecting anomalies in point cloud data. It calculates an anomaly score based on the deviation of target data points from expected positions, allowing for efficient identification of potential attacks or malfunctions. The real-time nature of the calculations and its compatibility with existing systems make it a practical solution for improving the safety of vehicles equipped with LiDAR technology.

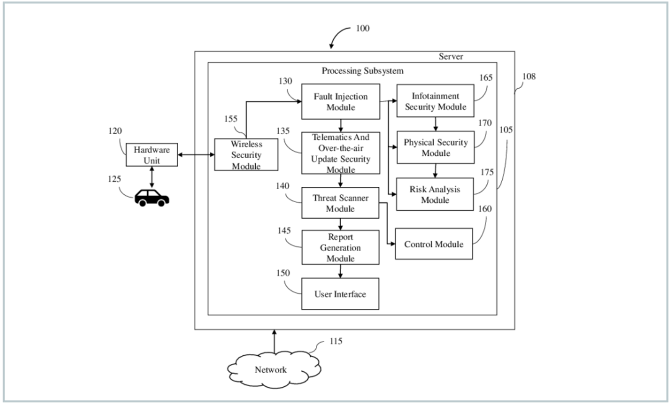
Summarized by Dennemeyer

IN202411049438A

A system and a method for vehicle security and threat scanner

Company name	Individual Inventor
Inventors	Pooja Upadhyay
Priority date	27-Jun-2024
Publication date	12-Jul-2024

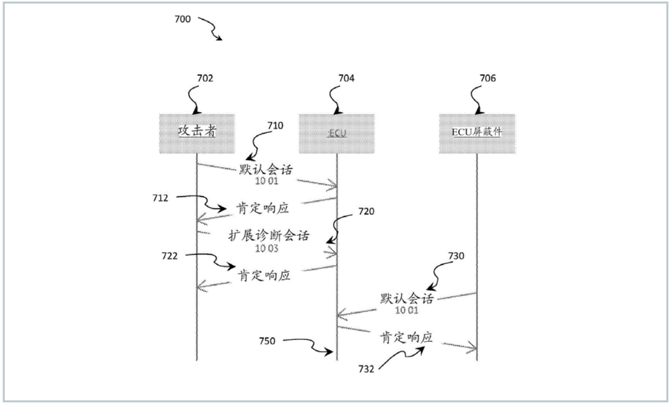
Summarized by Dennemeyer



The invention addresses the growing security concerns in increasingly digitized and interconnected vehicles. It aims to enhance vehicle security by developing a comprehensive threat scanner capable of identifying vulnerabilities in various vehicle components and systems. This includes injecting faults, assessing infotainment systems, evaluating telematics and OTA updates, examining physical security, analyzing data handling, testing communication protocols, and assessing anti-tamper mechanisms. The ultimate goal is to generate detailed reports for users to improve vehicle security.

CN118339553A

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	12-July-2024

The patent addresses the vulnerability of vehicles and machinery to diagnostic cyberattacks on the CAN bus. It introduces a novel approach to detect and mitigate these attacks by enforcing a diagnostic policy based on vehicle state. By mapping valid diagnostic requests to specific vehicle states and automatically interfering with invalid requests, the system enhances security and prevents unauthorized access and manipulation of ECUs. This solution is applicable to various machine types beyond vehicles.

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 79831 15166

South & West India
91 88266 88838