Dennemeyer
The IP Group

Report of April 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

Key Insights

- Risk Management and Automation Platform gaining traction as OEMs seek to comply with cybersecurity regulations and standards.
- Introduction of new Automotive Threat Matrix (ATM) to accelerate automotive cybersecurity governance.
- An invention to encrypt the communication between the vehicles.
- Inventions on detecting intrusion/attack/threats within the vehicle.
- An invention to secure Electric Vehicle (EV) charging system.
- An invention to protect vehicles from unauthorized access to data bus of a vehicle.

Dennemeyer
The IP Group

Industry news

Security Platform

EVSec Risk Management and Automation Platform Gains Traction as Companies Seek to Efficiently Meet Regulatory Requirements

EVSec, a risk-driven product security platform from C2A Security, is gaining popularity as more automotive companies work to comply with cybersecurity regulations and standards, like UN Regulation No. 155 (taking effect in 2024), ISO/SAE 21434, Chinese GB Standards, and others. EVSec lets developers manage software and operations at scale while focusing on creative features. As part of agile software development, EVSec uses continuous feedback from product operations and vulnerabilities to improve development and design.

Source
c2a-sec.com

Dennemeyer
The IP Group

Industry news

Threat Matrix

Auto-ISAC launches automotive threat matrix for cybersecurity

The Automotive Information Sharing and Analysis Center (Auto-ISAC) introduced the Automotive Threat Matrix (ATM) which provides a common threat taxonomy intended to accelerate all aspects of automotive cybersecurity governance. With this innovation, the automotive industry can better assess threats and risks, classify and share cyber threat intelligence. This tool helps automakers, manufacturers, and other automotive stakeholders improve their cybersecurity posture. It aims to protect their vehicles from cyberattacks.

Source
automotiveisac.com

Dennemeyer
The IP Group

Industry news

Test Framework

ETAS initiates open-source-based automotive test framework

ETAS is developing an open-source-based test automation framework for automotive systems together with partners such as VW/CARIAD, Mercedes Benz Tech Innovation, and AVL. The project is being realized under the name “Eclipse openDuT” (Device under Test). With its modular structure, this framework will support a wide range of test applications and provide the essential infrastructure for testing automotive systems like security testing, safety testing, functional tests, and homologation tests (e.g., for type approval in accordance with UN-R155) for individual automotive components as well as for a network of cars.

Source
www.etas.com

Dennemeyer
The IP Group

Industry news

EV Charger

SK builds cybersecurity enhancement system for EV chargers

In collaboration with Fescaro Co., a company specializing in automotive software and security systems, South Korean charger maker SK signet Inc. built an EV charging cybersecurity system. Fescaro and SK Signet examined EV charger cybersecurity together, identifying threats, evaluating them, and developing countermeasures based on their priorities. Additionally, SK Signet plans to create a charger integrated support system (CISS), with features like real-time charging monitoring and control and wireless software updates (OTA), to improve customers' convenience and security.

Source
www.mk.co.kr

Dennemeyer
The IP Group

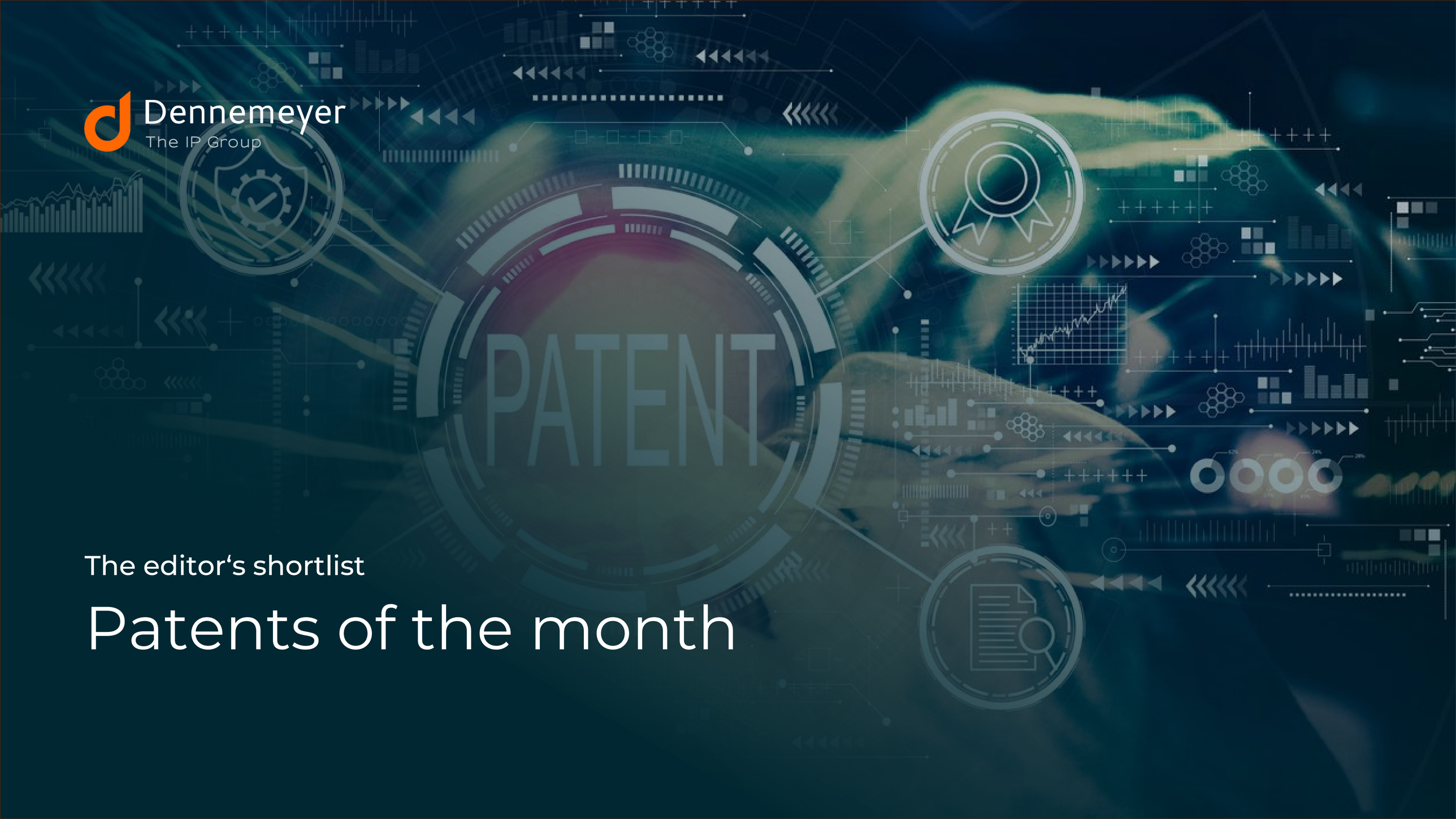
Industry news

Partnership

THALES ANNOUNCES PARTNERSHIP WITH SAPORO IN BELGIUM TO EMPOWER ORGANIZATIONS WITH ENHANCED CYBERSECURITY RESILIENCE

The partnership combines Thales' extensive experience in securing critical infrastructure and digital assets with Saporo's innovative attack path management platform. Using this combined offering, organizations can continuously identify weaknesses in the access structure, simulate attacker behaviors, and take decisive action to mitigate risks before they're exploited.

Source
www.thalesgroup.com



The editor‘s shortlist

Patents of the month

Dennemeyer
The IP Group

Patents of the month

Published in March 2024

Shortlisted and summarized by our analyst

- US2024104199A1 - Systems and methods for robust scan and upload cyber security patch to edge node
  Assignee: Honeywell international
- US20240078309A1 - Systems and methods for monitoring a plurality of vehicles
  Assignee: Vehiqilla Inc.
- US20240095378A1 - Method for encrypting security-relevant data in a vehicle
  Assignee: Continental Automotive Technologies GmbH
- US11937082B1 - Secure electric vehicle charger and system incorporating thereof
  Assignee: Eve Energy Ventures Inc
- US20240089281A1 - Attack analysis device, attack analysis method, and storage medium
  Assignee: Denso Corp
- WO2024056489A1 - Detection of external interventions in a computer system with zone separation for a device, in particular for a vehicle
  Assignee: Robert Bosch
- EP4335079A1 - Method and device for protecting against an intrusion on a data bus of a vehicle
  Assignee: Stellantis Auto SAS
- IN202321075948A - System and method for secured Vehicle-to-Everything (V2X) communication
  Assignee: Minda Corp , Reva Univ
- CN117793670A - Internet of vehicles secure communication method under block chain architecture
  Assignee: Xidian Univ

Dennemeyer
The IP Group

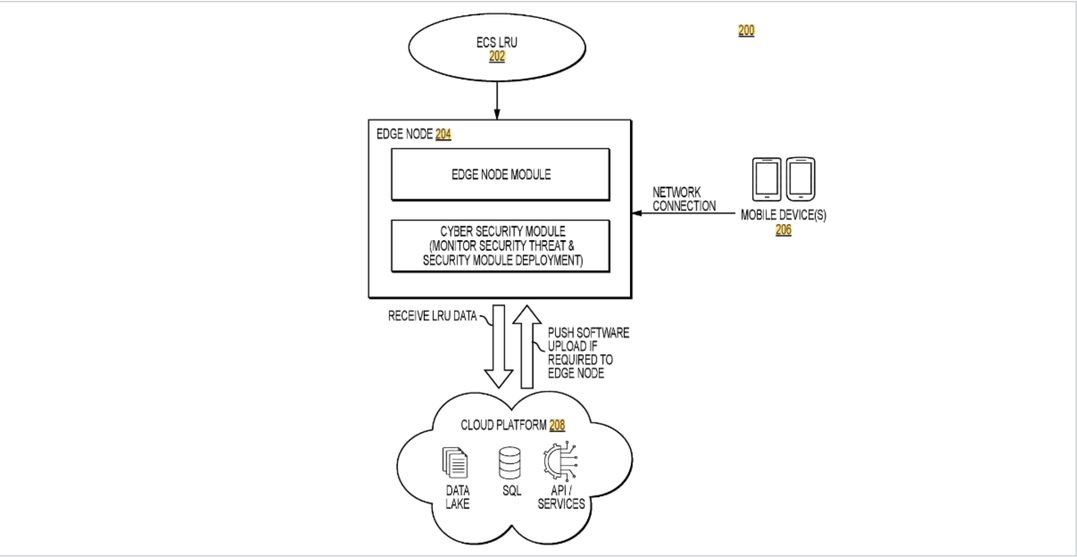
Latest patents

US2024104199A1

Systems and methods for robust scan and upload cyber security patch to edge node

Company name	Honeywell international
Inventors	Sridhar Kommisetty Rathnaiahsetty, Avinash Nittur Venkatesh, Gagandeep Singh
Priority date	21 Dec 2022
Publication date	28 March 2024

Summarized by Dennemeyer



The patent talks about a system that helps keep airplanes safe from cyber attacks. It divides the edge node of an aircraft into two parts - one for regular functions and another to watch out for security threats. The system collects data from the airplane and determines whether the airplane is at the ground. If it is grounded and engines are off, the system connects the edge node’s wireless interface to a centralized service hosted on a cloud, which then checks for any potential security issues. If there are any problems, it updates the security software on the plane automatically to protect against those threats. This process ensures that the airplane stays secure.

Dennemeyer
The IP Group

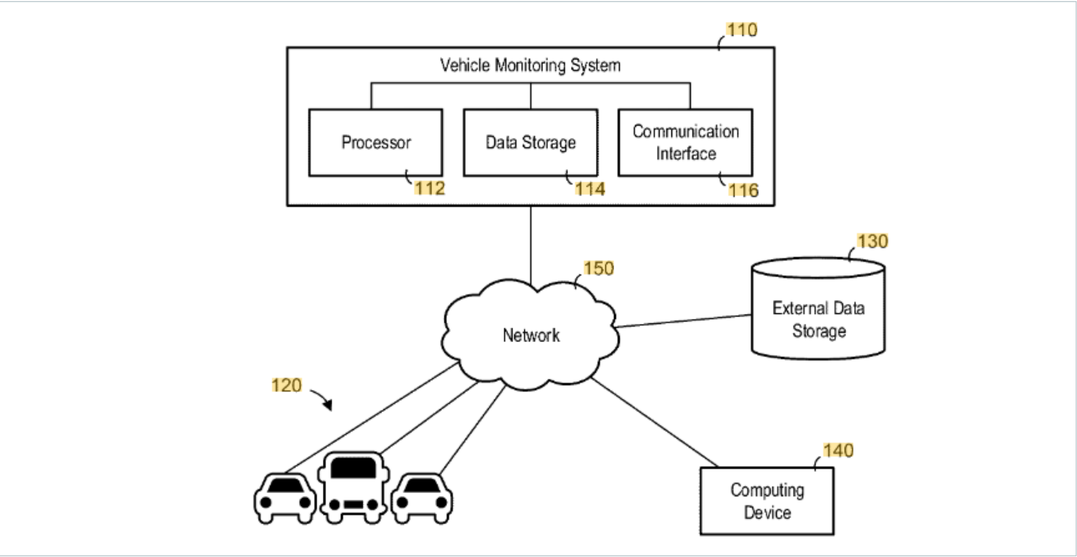
Latest patents

US20240078309A1

Systems and methods for monitoring a plurality of vehicles

Company name	Vehiqilla Inc
Inventors	Ali Jamshed Khan
Priority date	12 Oct 2023
Publication date	07 Mar 2024

Summarized by Dennemeyer



The patent describes a system and method for monitoring multiple vehicles to detect cybersecurity threats. The system uses processors to analyze cyber risk data for different electronic control unit (ECU) models in the vehicles. It receives security logs from each vehicle, maps them with ECU models and cyber risk scores, and detects threats based on events in the logs and corresponding risk scores. If any suspicious activity is found in the car's records along with high-risk levels, an alert is sent out to the vehicle to warn about possible dangers.

Dennemeyer
The IP Group

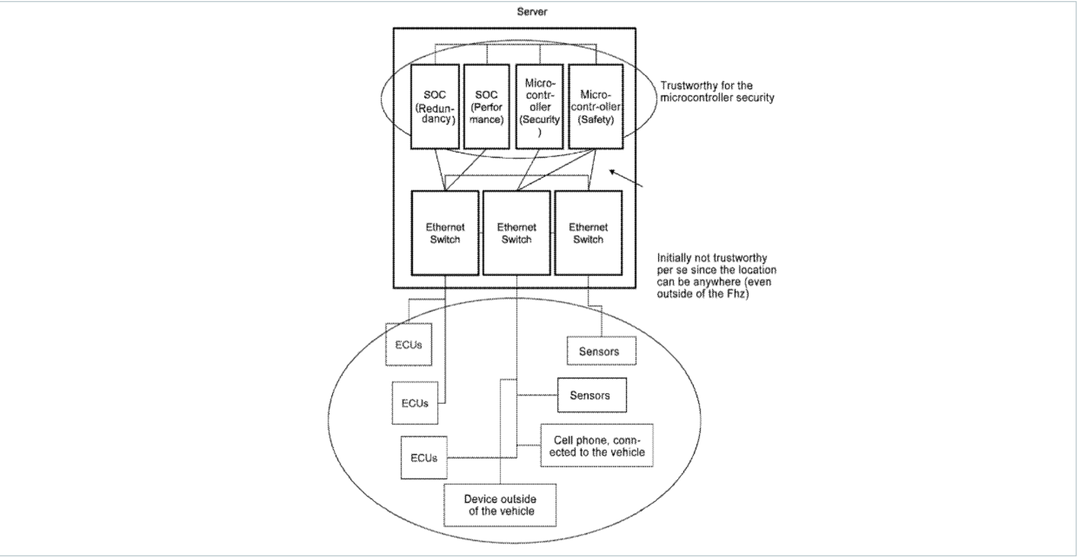
Latest patents

US20240095378A1

Method for encrypting security-relevant data in a vehicle

Company name	Continental Automotive Technologies GmbH
Inventors	Helge Zinner
Priority date	21 Jan 2021
Publication date	21 Mar 2024

Summarized by Dennemeyer



This invention talks about making sure that only trusted connections can happen within the car's systems. The technology focuses on understanding where each communication partner (e.g. controllers or sensors) is located in the vehicle and deciding if it's safe to share information with them based on their distance. This method helps protect against attacks and makes sure data stays secure inside the vehicle. Overall, the invention improves security in vehicles by checking who is talking inside the car network and making sure everything stays safe from potential threats.

Dennemeyer
The IP Group

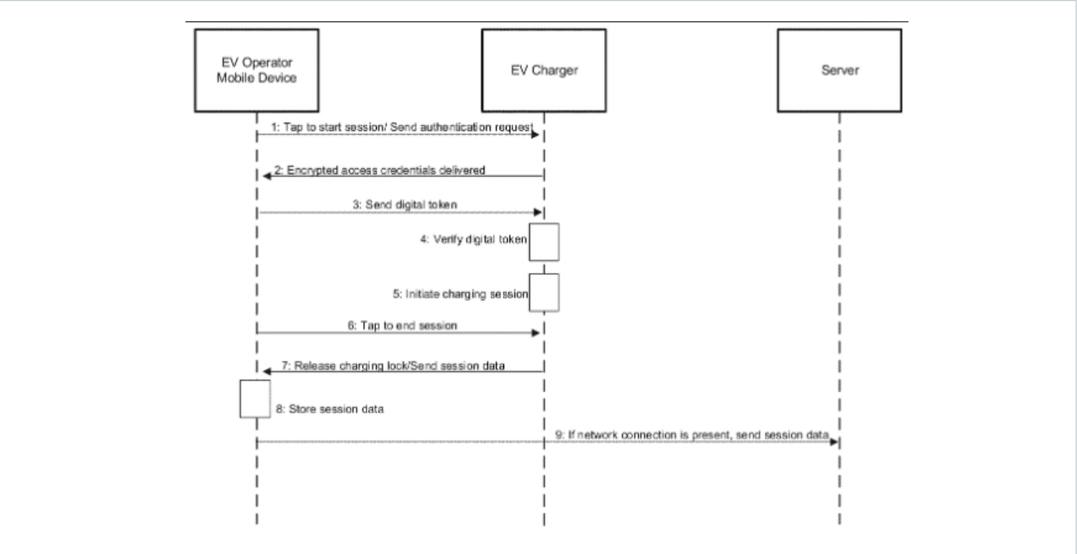
Latest patents

US11937082B1

Secure electric vehicle charger and system incorporating thereof

Company name	Eve Energy Ventures Inc
Inventors	Nikhil Srinath Bharadwaj
Priority date	02 Dec 2020
Publication date	19 Mar 2024

Summarized by Dennemeyer



The invention relates to secure electric vehicle (EV) charging system. The system includes an EV charger that communicates with mobile devices using a short-range communication system like NFC. The mobile device sends a digital certificate/token with cryptographic information to authenticate the session. The EV charger verifies the digital token by using cryptographic information contained within the digital certificate, allowing it to start a charging session even without an internet connection. After the session, data is stored on the mobile device and can be sent back to a server when there is an internet connection available.

Dennemeyer
The IP Group

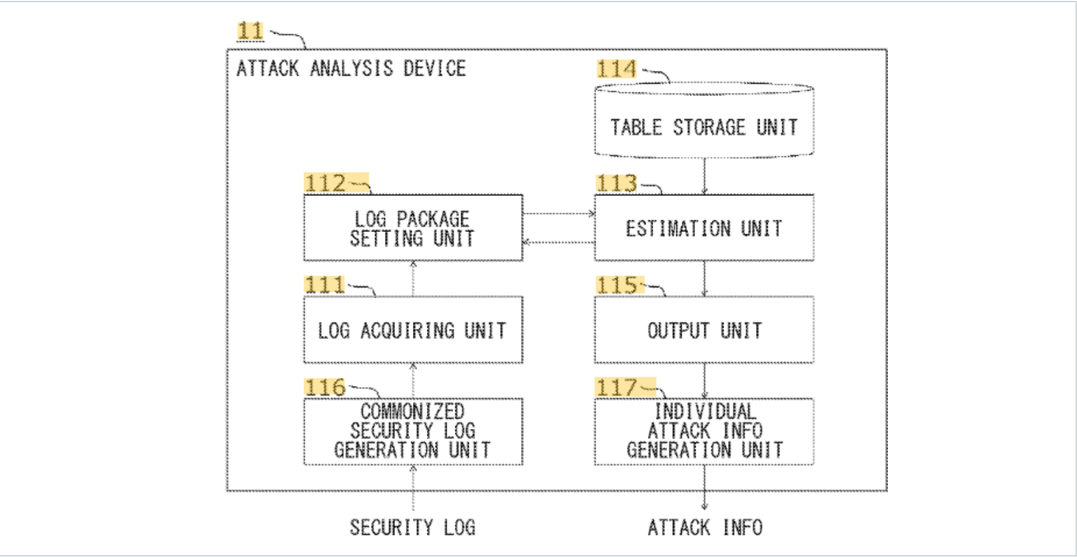
Latest patents

US20240089281A1

Attack analysis device, attack analysis method, and storage medium

Company name	Denso Corp
Inventors	Nagara Keigo
Priority date	14 Sep 2022
Publication date	14 Mar 2024

Summarized by Dennemeyer



The invention talks about a device for analyzing an attack received by an electronic control system mounted to a moving object, such as a vehicle. It works by collecting security logs from different parts of the system, grouping them together based on certain rules, and then figuring out if there was an attack based on these grouped logs. It analyzes patterns in how abnormalities occur across different parts of the electronic system over time and identifies potential cyberattacks more accurately. It uses information such as ECU types (different parts), sensor types (which sensors detected issues), timestamps (when issues occurred), or other data included in security logs to group them effectively for analysis.

Dennemeyer
The IP Group

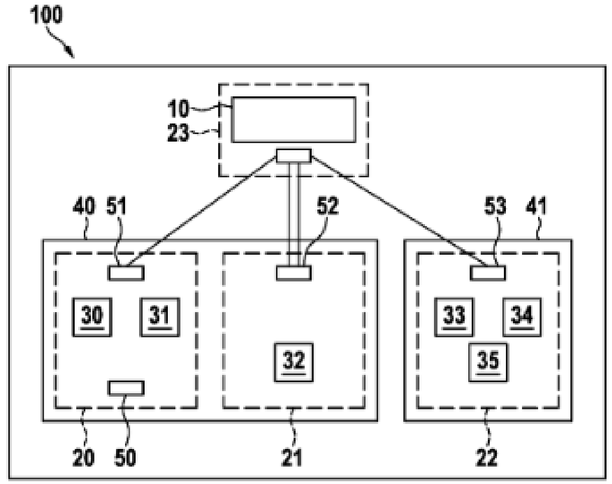
Latest patents

WO2024056489A1

Detection of external interventions in a computer system with zone separation for a device, in particular for a vehicle

Company name	Robert Bosch
Inventors	Jauss Manuel, Hallaczek Lara, Kneib Marcel
Priority date	16 Sep 2022
Publication date	21 Mar 2024

Summarized by Dennemeyer



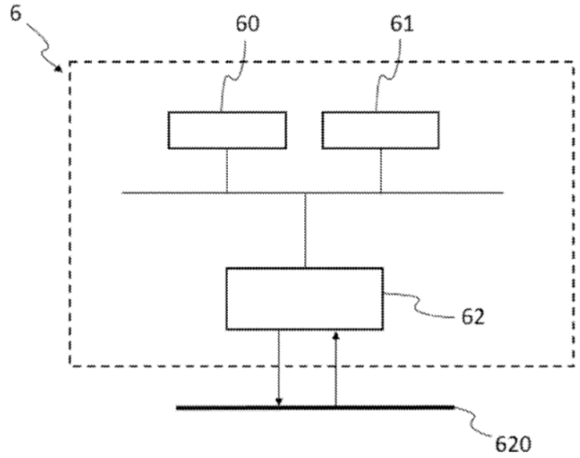
The patent talks about a system that helps keep a vehicle safe from outside attacks. It uses the concept of separating trust zones within an electronic control unit (ECU). Each zone gets assigned specific parts of the system modules and resources. If there's any unauthorized access or manipulation in one zone, it won't easily affect the other zones. The system also has a security module that checks for any rule violations in how resources are assigned to these zones. If there's an issue, it can take action to protect the system. The present techniques offer the possibility of detecting (and, for example, accumulating and responding to) such regulatory violations in vehicle in a centralized manner.

Dennemeyer
The IP Group

Latest patents

EP4335079A1

Method and device for protecting against an intrusion on a data bus of a vehicle



Company name	Stellantis Auto SAS
Inventors	Scheerle Marc, Biswojyothi Monith, Bhagat Preet
Priority date	31 Mar 2022
Publication date	13 Mar 2024

Summarized by Dennemeyer

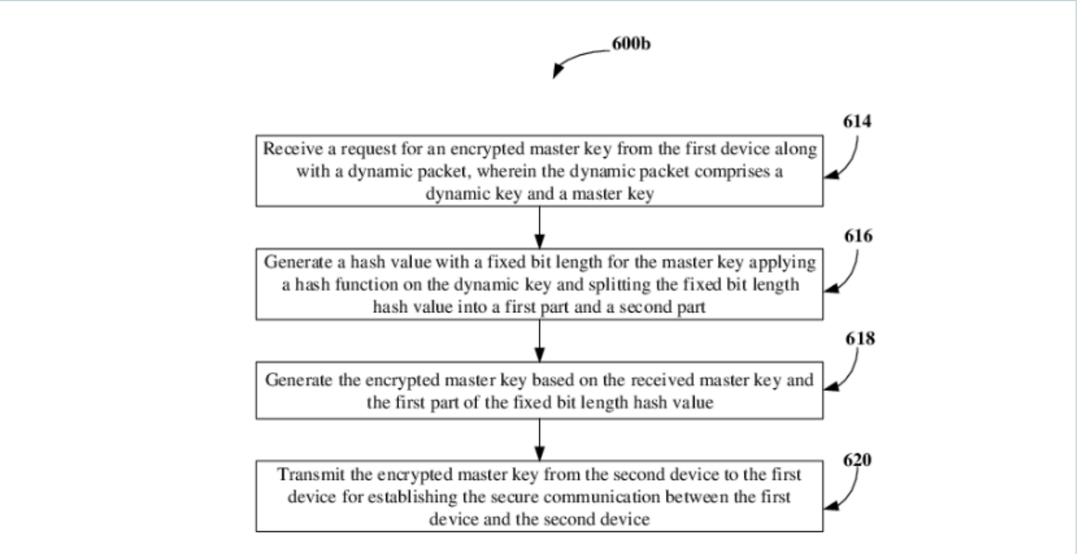
The invention describes a way to protect vehicles from unauthorized access to data bus of a vehicle. To detect the intrusion a device is connected to the data bus, which inspects the value of a counter associated with each message. When an intrusion is detected, a filtering request is sent to the vehicle controllers to filter out the suspicious message. This request includes information about the message that needs filtering and is sent periodically. This way, the invention improves the security of data exchanges between controllers connected by a data bus of a vehicle.

Dennemeyer
The IP Group

Latest patents

IN202321075948A

System and method for secured Vehicle-to-Everything (V2X) communication



Company name	Minda Corp , Reva Univ
Inventors	Suresh D, Parag Parandkar, Prashanth Joshi, Sudharshan K M
Priority date	07 Nov 2023
Publication date	22 Mar 2024

Summarized by Dennemeyer

The invention relates to performing a key encryption and cyber security for vehicular communications. The idea is to enhance the security in the cellular based Vehicle-to-Everything (V2X) communication to overcome security issues during communication between two Electronic Control Units ECUs. The ECUs use a master key and a dynamic key for establishing a secure communication in V2X environment. The dynamic key is used to encrypt/decrypt the master key to initiate a secure communication.

Dennemeyer
The IP Group

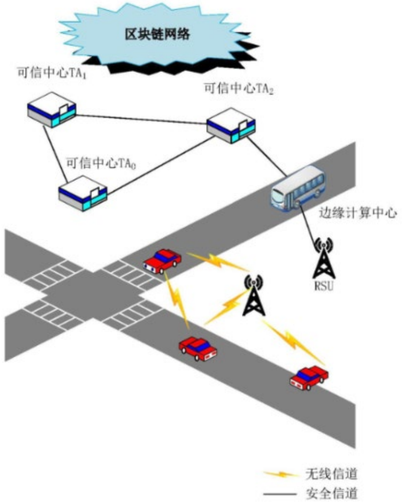
Latest patents

CN117793670A

Internet of vehicles secure communication method under block chain architecture

Company name	Xidian Univ
Inventors	Cao Xuefei , Li Qiaobin , Li Hui , Song Qipeng , Jing Peidong , You Wei , Dang Lanjun
Priority date	27 Dec 2023
Publication date	29 Mar 2024

Summarized by Dennemeyer



The invention establishes an Internet of Vehicles (IoV) system using blockchain architecture. When a driver starts their vehicle, it requests access to a roadside unit. The roadside units authenticate the vehicle bidirectionally using edge computing and blockchain. It also generates a group key for a group of vehicles, which will be used to encrypt the communication between the vehicles. Which in turn enhances vehicle anonymity, improves reliability, and increases authentication efficiency. It ensures user privacy and secure communication within the IoV system.

Dennemeyer
The IP Group

Thank you.

You want to know more? Visit us on www.dennemeyer.com

Contact us at

Dennemeyer India Private Limited

North & East India
+91 79831 15166

South & West India
91 88266 88838