REVIEW ON ISO SAE 21434
Road vehicles – Cybersecurity engineering

A position paper of the Automotive Parts Remanufacturers Association Europe.

The purpose of this paper is to introduce the ISO SAE 21434 and review it from the remanufacturers' perspective.

Introduction

The ISO SAE 21434 standard aims at addressing the cybersecurity perspective in engineering of electrical and electronic (E/E) systems within road vehicles. By ensuring appropriate consideration of cybersecurity, this document aims to enable the engineering of E/E systems to keep up with changing technology and attack methods.
The standard specifies requirements for cybersecurity risk management regarding engineering for concept, product development, production, operation, maintenance, and decommissioning for road vehicle electrical and electronic (E/E) systems, including their components and interfaces.

While compliance with such standards is usually voluntary it can facilitate international business, be contractually required by customers or be considered as state of the art by a judge in case of an event. Like other standards it also creates a common language in the cybersecurity field which can make communication between stakeholders more efficient as well as increase overall quality of the products and business exchanges.

This standard therefore focuses on security or the protection of machines against maliciously acting humans, especially by describing methodologies enabling to create a cybersecurity culture during production testing and updates of automotive components and vehicles. Still, in the particular case of a passenger car, a malicious security breach could potentially lead to injury or death making it a critical topic.

Cybersecurity is and will be a very relevant topic for the years to come. Indeed, the volume of software used in modern passenger cars is quickly growing due to added features such as Advanced Driver Assistance Systems (ADAS), new comfort features, powertrain electrification and Information and Communication Technologies (ICT) adoption. Vehicles are now connected for safety reasons, an example being the European eCall emergency call functions installed on every model put in sale after 2018. ADAS, infotainment, remote diagnostics or remote service management services also require the vehicle to be connected, exposing it to new hacking techniques.

While this standard mostly concentrates on design phase applicable to Tier 1 or manufacturers, it also describes methodologies to define and document cybersecurity policies and processes in order to manage cybersecurity risks. It is important to note that this standard does not prescribe specific technologies or solutions as they might quickly become obsolete in this fast evolving field.

Analysis

This standard also improves the communication between independent remanufacturers and OEM customers. As an example: results from the Cybersecurity Assurance Level (CAL) assessment could lead to reasonable measures to be taken and documented in order to show due diligence that can limit the remanufacturer's liability in case of an event. The CAL can be seen as the counterpart of the Automotive Safety Integrity Level (ASIL) from ISO 26262.

In practice this could include cybersecurity measures applied to networks used by the test benches or to monitor access to the parts by the employee in order to avoid any external or internal interference such as command injection, data corruption or data leakage during the remanufacturing process.

One challenge especially for independent remanufacturers is created by the lack of access to software revisions, known vulnerabilities in documentation and updates. The impact will of course depend on the system vehicle update strategy but could ultimately lead to non-updated and potentially vulnerable parts being mounted on vehicles.

While some EU commission regulations including No 461/2010 and 330/2010 grant access to independent service providers, such as independent repair garages, to OEM software required to update vehicles and components by paying « reasonable and proportionate fees » in a way that « is not discouraging access », remanufacturers seem to stand in a grey zone.

An issue could also arise if the cybersecurity support of the car manufacturer ends. In this case all relevant information should be published as open source so that the independent aftermarket can take over the security support of the vehicle.

Recommendations

It is therefore obvious that the lack of access to software and relevant information could negatively impact the development of a futureproof circular economy within the automotive industry. This in turn could negatively impact emissions, raw material consumption as well as job creation related to automotive spare parts production within the European Union. It is therefore obvious that fair competition in the market depends upon EU regulations but also standards such as ISO SAE 21434 being adapted to the remanufacturing business.

It is obvious that adherence to such standard could enable remanufacturers to create a cybersecurity culture within their company as well as facilitate business, especially with OEM customers. It is therefore a necessity to create reman-specific standards and regulations in order to define the industry state of the art and give remanufacturers the means to achieve it.

Contact

APRA Europe AISBL
Silversquare Central
coworking community
Kantersteen 47
1000 Brussels
BELGIUM

info@apraeurope.org