© Cymotive

**Cristian Ion**
Head of Secure Engineering
at Cymotive

# Commercial Vehicles in the Crosshairs of Hackers

Commercial vehicles are a popular target for malicious hackers. This is not a surprising development, as these vehicles often transport highly valuable cargo, making them a much more attractive target than passenger vehicles. The total value of goods transported worldwide is in the triple-digit billions.

If cybercriminals are allowed to operate undisturbed in this field, logistics companies are not the only ones to take harm. International supply chains are also at serious risk from large-scale cyberattacks on cargo fleets. The criminal motives behind potential attacks are not just financial in nature: Politically motivated criminals may also have an interest in disrupting the delivery of critical goods – such as military equipment.

Due to these high risks, commercial transport must be protected against cyberthreats particularly well. However, commercial vehicles are much more susceptible to attacks than passenger vehicles, making effective protection a far more difficult task; for several reasons: For example, commercial vehicles are usually modular in design, which is particularly evident in the case of agricultural vehicles: Tractors are often combined with equipment such as plows or harvesting equipment. If one component is infected with malware, it quickly spreads to the rest as well.

In addition, the lifecycle of commercial vehicles usually has a very long usage and high mileage. This offers cybercriminals more opportunities to launch compromising attacks. Many trucks are, for example, after their initial acquisition also retrofitted with new electronic devices such as telematics modules or other add-ons. Often, these additions do not have the same security standards as the truck's own components, which creates additional vulnerabilities.

So how does a reliable cybersecurity approach for commercial vehicles look like? For once, manufacturers should remember to sensibly extend the SAE J1939 network protocol currently used as a standard. The new J11939-91 standard, for example, is to be used in the future to facilitate additional network security features such as Secure Boot, Secure Flash as well as authentication and authorization. New basic security features are also available and can be integrated via a J1939-13 connector. In addition, new guidelines are currently being defined for secure communication within the vehicle as well as secure radio connections to external components (Over-the-Air/OTA), which includes the new UN 156 and ISO 24089 regulations.

Ensuring the effective protection of commercial vehicles against cyberthreats requires manufacturers to explore the possibilities of these expanded future security standards. They should be an integral part of every holistic security-by-design approach that focuses on the entire lifecycle of a commercial vehicle as well as its specific security requirements.