CAN Newsletter Online

CAN NEWSLETTER MAGAZINE

Securing CAN networks in commercial vehicles

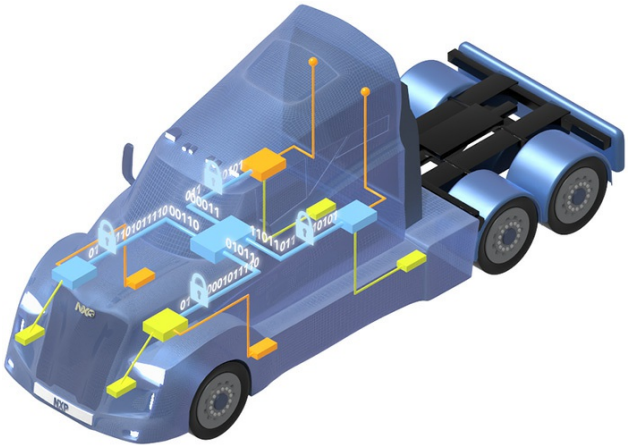
The UNECE (United Nations Economic Commission for Europe) demands cybersecurity for road vehicles. In order to protect the CAN network from compromised ECUs (electronic control units), a CAN transceiver with built-in security functions can be used. This avoids the complexity of end-to-end security solutions, which are especially hard to implement on commercial vehicles.

(Source: Adobe Stock/NXP)

The complete article is published in the September issue of the CAN Newsletter magazine 2022. This is just an excerpt.

Commercial road vehicles are the backbone of the modern consumer economy. Almost any business from construction, to energy, to online retail, at some point relies on the delivery of goods by commercial vehicles. These commercial vehicles are in turn becoming increasingly connected both to the external world and to each other via telematics. This enables commercial vehicle owners to optimize and manage their fleets via platooning for safety and efficiency improvements as well as cost and fuel consumption reduction to meet the increasingly stringent CO2 emissions requirements necessitated by climate change. However, the increased connectivity brings with it an increase in cyberattack surfaces and commercial vehicle fleets are prime targets for cybercrime due to the high value of the cargo they carry, and their importance to large businesses and the greater economy.

Remote scalable cyberattacks have high adverse impacts



Securing CAN networks in commercial vehicles with NXP Secure CAN transceivers (Source: NXP)

While commercial vehicle manufacturers are familiar with and prepared for the risk of physical attacks, typically carried out on one vehicle, such as odometer manipulation, or theft, they may risk being caught by surprise at the scale and impact of what is possible with remote cyberattacks. Remote security breaches have been demonstrated to impact the safety of the vehicle, resulting in the recall of millions of vehicles. Hackers can exploit a vehicle's wireless network or internet connection to gain entry into the vehicle's communication network and compromise security to access a vehicle's CAN (Controller Area Network) network and take over remote management of the vehicle while it is in motion. Modern ECUs in commercial vehicles run on millions of lines of code, which opens up vulnerabilities for compromising them. Even conservative estimates predict a bug every 1000 lines of code. A range of activities can then be carried out with malicious intent from fraudulent manipulation of data to complete control of safety critical functions such as steering, acceleration, and braking. Location tracking and theft are also among the potential motivations for hackers to inject malicious CAN data frames into the CAN network.

Long life platforms, integration of several sub-assemblies, software complexity

UNECE R155 – Mandatory cybersecurity compliance

The increase in connectivity brings with it an increased risk of malicious cyberattacks. These risks are relatively new to commercial vehicles and industry experts are looking at several approaches to mitigate these risks. However, there is already the expectation from regulatory bodies such as UNECE that it is no longer a question of if there is an attack but when there is an attack on a vehicle network. This has resulted in mandatory cybersecurity compliance regulation R155. It is applicable at first for new vehicle types but will then become applicable to all vehicles on the road, increasing the sense of urgency for the implementation of cybersecurity measures within vehicles that

for end-to-end security, the lack of a secure communication standard, cost pressures, and cyber regulation compliance are among the challenges faced by commercial vehicle manufacturers (Source: NXP)/figcaption>

will be on the road in one of the 54 countries that are party to the agreement. The R155 has explicit requirements such as "The vehicle shall verify the authenticity of the messages it receives" because in CAN data link layer communication, the sender is unknown and the intended receiver acts on a CAN data frame it receives, even if spoofed. Other requirements are important for safety, such as "Measures to detect and recover from a denial-of-service attack shall be employed", because a jammed CAN network could prevent the timely transmission of control and safety-critical messages. This makes it important not only to detect attacks, and implement fixes to avoid a repeat, but also to find ways to prevent them from causing harm in the first place.

Absence of a standard for secure communication

Several OEMs (original equipment manufacturer) who make passenger vehicles protect their CAN network via secure onboard communication implementation of Autosar SecOC. However, commercial vehicles employ the CAN-based SAE J1939 higher-layer protocol, which does not yet provide standardized cybersecurity measures. For example, there is no way to authenticate the origin of the message. There are ongoing efforts to arrive at a secure communication standard for J1939 but this is still several months from being finalized.

Long life platforms with legacy ECUs and architectures

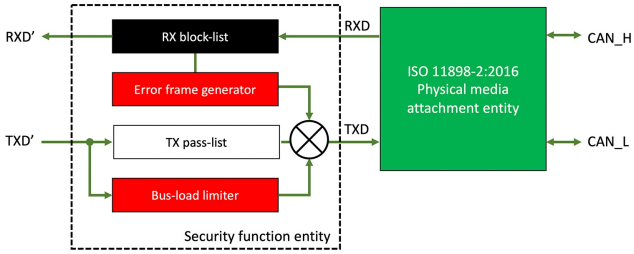
Eventually there will be a secure communication standard on J1939 called the J1939-91C. However, implementation would require micro-controllers supporting cryptographic functions. As most commercial vehicles have a long lifetime once commercially released, there is typically several micro-controllers without the required security features, not only the advanced ones for hardware acceleration of cryptographic key generation, but also more basic features of modern micro-controllers such as secure boot. Another vulnerability from the long life of commercial vehicle platforms is that these architectures were not designed with security as a focus. As a consequence, they do not have sufficient network separation between the individual CAN branches leaving a wider footprint of vulnerable devices in the event of an attack. To be able to implement such a secure communication standard effectively once released would still require a major in-vehicle network overhaul to implement. Moreover, there is a lot of know-how and infrastructure that will need to be put in place before the standards are widely adopted within the supply chain. This would still be out of reach for small truck and bus OEMs.

Custom security solutions are complex and prohibitive

As the owner of security in the vehicle, some passenger vehicle makers opt to secure their networks with custom security implementations in spite of the large one-time expense due to the security benefits they perceive. However, implementation of a custom end-to-end security solution is a challenge for commercial vehicle OEMs as they don't build the entire truck themselves but bring together different sub-assemblies which are integrated into the vehicle. Cryptographic security solutions that require complex software implementations can also be cumbersome for the commercial vehicle manufacturer's security teams to co-ordinate across their vast swath of suppliers. This would be an integration and testing nightmare. Besides, most small OEMs buy off-the-shelf solutions, thus providing little room for the Tier-I supplier to take on such one-off security projects.

Open architectures

Commercial vehicles are susceptible to malicious access to the vehicle network from the way they are constructed. As a single commercial vehicle chassis can be transformed into any of a number of different variants, this means that the CAN network might well come all the way to the exterior of the vehicle, for example to establish the connection between the vehicle chassis and a trailer. These could become easy entry points to malicious hackers. As the vehicle is put together from different sub-assemblies, the suppliers need to be able secure each sub-assembly's network locally, and independently, so that when they come together at the OEM, there aren't additional security vulnerabilities introduced.



The TJA1152 Secure CAN transceiver features stand-by mode and the TJA1153 supports sleep mode; both are compliant with ISO 11898-2:2016. The block diagram shows a secure CAN transceiver. (Source: CiA/NXP)

Affordable security is a must

Last but not the least is the commercial aspect of implementing security measures. While there is an increasing number of commercial vehicles hitting the road, driven by demand from industries such as construction, and e-commerce, the numbers are still vastly lower than those of passenger cars. This places significant pressure on the development costs of commercial vehicles. Commercial vehicle security solutions, therefore, need to not only be easy to implement but also affordable. The absence of a readily implementable secure communication standard, long lasting platforms with legacy components, deployment across a complex production hierarchy, open architectures for functional integration, and pressure on development costs require an affordable, easy to configure, integrate and validate solution.

But if you would like to read the full article, you can download it free of charge or you download the entire magazine.

cw