Securing CAN networks in commercial vehicles

(Source: Adobe Stock/NXP)

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.

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 CO_2 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. [1]

Remote scalable cyberattacks have high adverse impacts

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[2] 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[3]. Even conservative estimates predict a bug every 1000 lines of code[4]. 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.

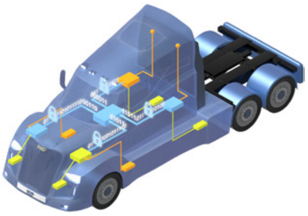


Figure 1: Securing CAN networks in commercial vehicles with NXP Secure CAN transceivers (Source: NXP)

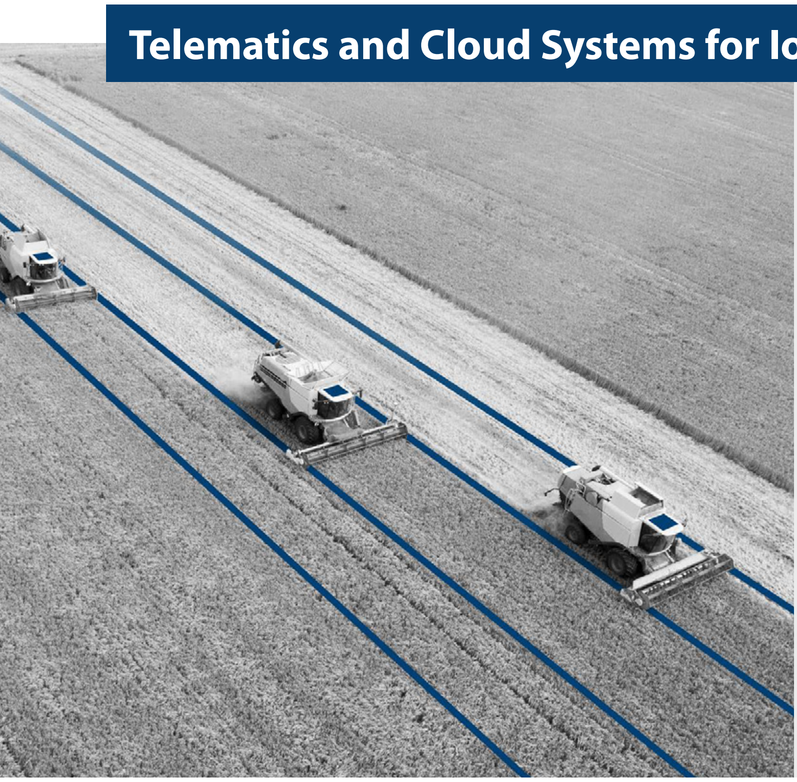
UNECE R155 – Mandatory cybersecurity compliance

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 will be on the road in one of the 54 countries[5] 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 ▷

Sontheim

High-end Connectivity and Data Management

Telematics and Cloud Systems for IoT and Service 4.0



Continuous digitization for smart vehicles

Modular on-board units – from cost-saving entry telematics up to high-end modules. Including updates-over-the-air, embedded diagnostic functionality and up to 4× CAN channels (CAN FD ready).

Sontheim IoT Device Manager and IoT Analytics Manager – for a highly secure, comfortable and individual visualization as well as management of your data and fleet.

COMhawk® xt – Telematic ECU Series

CAN
Up to 4× CAN acc. to ISO 11898

LTE, WLAN, Bluetooth, LAN

Multi-protocol support (J1939, J2534, UDS, KWP, …)

Positioning (GNSS)

Embedded diagnostic functionality

Integrated update-over-the-air functionality

www.s-i-e.de

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.

Figure 2: Long life platforms, integration of several sub-assemblies, software complexity 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)

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[6]. 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.

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. ▷

External CAN interfaces

Because CAN is an unsecured data link layer protocol, communication with external devices needs to be protected. In commercial road vehicles, there are several external CAN interfaces. First of all, there is a CAN interface for diagnostic purposes, which is also used for updating software to the in-vehicle ECUs (electronic control unit). Additionally, several trucks provide a CAN-based interface to trailers and semi-trailers. In Europe, this interface is based on the ISO 11992-2 (mandated by EU regulation) and ISO 11992-3 (optional) standards. These are two independent point-to-point CAN-based links. They do not provide cybersecurity measures. In Europe, it is demanded that any trailer or semi-trailer should be connectable to any truck. The related ISO 11992 gateway ECUs need to provide firewalls to protect the in-vehicle networks against attackers. There is also in some commercial vehicles a CAN-based gateway for builder builders (e.g. CiA 422 series, DIN 4630 and DIN 14704). These also need firewalls. Currently, they do not have. Both external interfaces, for trailer connection and body applications, are in commercial vehicles unsecure. CiA intends to specify a common solution and invites truck and trailer suppliers as well as body builders to develop jointly-standardized security measures for these external CAN-based interfaces.

Comment by Holger Zeltwanger, CiA Managing Director

Secure CAN transceivers

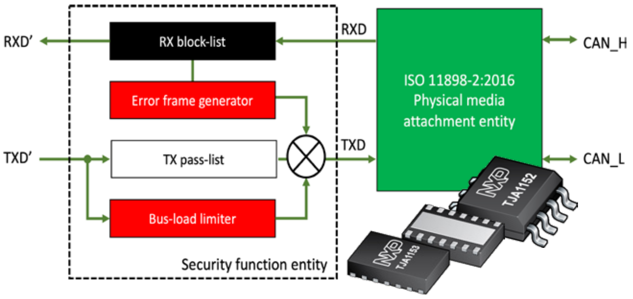


Figure 3: The TJA1152 Secure CAN transceiver features stand-by mode and the TJA1153 supports sleep mode; both are compliant with ISO 11898-2:2016. The block diagram shows a secure CAN transceiver. (Source: CiA/NXP)

Local network authentication

The NXP Secure CAN transceivers can serve to ensure authentication of communication on a local network, i.e., for CAN data frames not transmitted over a gateway. It does so using a configurable transmission pass-list, or list of user pre-configured CAN-IDs, built into the transceiver itself. This ensures that the local host is only allowed to send these legitimate CAN data frames. A CAN-ID block-list ensures that no other node uses the CAN-IDs that are legitimately owned by the aforementioned local host. The J1939 protocols specifies unique source addresses (SA) for ECUs (to be assigned by the network designer), which can be masked using the

secure CAN transceivers to enable securing the communication based on a pass-list and block-list for CAN-IDs as determined by the OEM in order to fulfill the network's security requirements.

Tamper protection

To circumvent the secure CAN spoofing protection, a hacker could attempt to carry out a man-in-the-middle attack to manipulate a legitimately initiated CAN frame by taking control at the data field to insert rogue data along with an appropriately altered CRC value. In Error Active state, the CAN controller detects and invalidates the manipulated frame. However, in Error Passive state, the modifications are not signaled by an error frame. The secure CAN transceiver has tamper protection on transmit and receive paths to protect from a man-in-the-middle attack by generating the requisite error frame when the CAN controller of the legitimate sender is in the Error Passive state.

Flooding denial-of-service protection

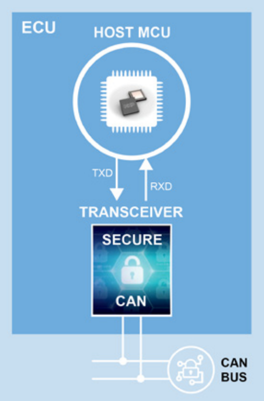


Figure 4: The Secure CAN transceivers have configurable pass and block lists for CAN-IDs, rate limiting, and an integrated CAN controller for generating error frames and switching to secure mode (bus off for TX) (Source: NXP)

One of the significant benefits of the NXP TJA1152 and TJA1153 transceivers is the provision for adding user configurable flooding protection thresholds, to prevent a compromised local host from flooding the network with high-priority CAN-IDs that are part of the transceiver's transmission pass-list. In a shared communication channel such as a CAN network, a timing failure can have serious consequences, especially for control and safety functions. With the exception of braking, most systems in commercial vehicles do not have a back-up CAN channel, which raises the importance of keeping the network available at all times. The flooding protection can also help avoid impact to the CAN network on critical pathways where a babbling-idiot failure triggered from the local host's software could cause bus overload with an excessive transmission of the permitted CAN-IDs.

Software and MCU independent security

As the provided security functions are without cryptography or dependence on any other micro-controller features, they are compatible with all MCUs including legacy ones. Moreover, the security functions being built into the transceiver, there is no software impact, as is usually the case with a key-based security approach. By implementing the transceiver with security measures into commercial vehicles, the need for updating network architectures and software to include sophisticated cryptographic solutions and the associated expensive hardware is avoided.

How secure is secure CAN?

The transceivers have an option to be fully locked after the initial configuration making the CAN-IDs effectively hard-coded for complete security. However, to provide flexibility to the OEMs, there is provided the possibility to locally or remotely reconfigure the transceiver using a secure boot microcontroller. This should be done only in the first few seconds after the microcontroller goes through a secure boot to prevent a runtime compromised ECU from updating the Secure CAN transceiver's configured CAN-IDs or flooding thresholds maliciously. The Secure CAN transceivers have a configurable parameter that can be set to ensure this limited time window for configurability.

Drop-in security

The TJA1152 and TJA1153 Secure CAN transceivers are key enablers for addressing challenges for commercial vehicle cybersecurity. The transceivers are available as drop-in replacements to legacy CAN HS (high-speed) and CAN FD transceivers, enabling a simple populating of the solution in an application. The transceivers serve as a one-size-fits-all security enabler for Tier-1s that are implementing security across a wide variety of commercial vehicle OEMs. An initial configuration of the transceivers is sufficient to secure vehicles equipped with a different mix of legacy and new ECUs, and varying levels of software flexibility, while reducing cost for network security.

Improving time to root cause on cyber-incidents

Imagine a remote fleet spoofing attack on a business's commercial vehicles for theft of valuable cargo. OEMs implement IDS (Intrusion Detection System) systems to quickly understand the details of such an attack, in order to carry out forensics on the compromised ECU, and issue a fix to avoid a repeat of the incident. But what if one could prevent the attack from bringing harm in the first place? The secure transceivers prevent a successful attack on the victim ECU by invalidating the malicious CAN data frame with a CAN error frame, and switching to secure mode preventing any communication by the compromised ECU temporarily. This provides a ready signal to a network monitoring IDS on which node in the local network was hacked due to the

Reference

[1] Road transport study: Digitalization is progressing rapidly, but cybersecurity awareness still in its infancy (press release by Continental, 2020)
[2] Charlie Miller and Chris Valasek, Remote Exploitation of an Unaltered Passenger Vehicle, 2015
[3] Addressing the cybersecurity risks
[4] The danger of complexity: More code, more bugs
[6] “Transceiver with cyber security functions”, Bernd Elend, Tony Adamson (both NXP Semiconductors)
[7] „Autosar SecOC for CAN FD“, Dr. Tobias Islinger, Yasuhiro Mori, Jennifer Neumüller, Martin Prisching, Dr. Robert Schmidt (all Denso Automotive Deutschland)
[8] Gloria D'Anna, Cybersecurity for commercial vehicles (hardcover), SAE, Detroit 2018

absent ECU heartbeat. This latter feature will help the OEM immensely to reduce the time to root cause on the incident and implement a security fix quickly, having to search through only the identified compromised sender, and not the entire subnetwork.

The commercial vehicle industry is in as much of an inflection as the passenger vehicle industry. Their security experts are working hard on meeting the cybersecurity compliance requirements, given the unique challenges they face. NXP's TJA1152 and TJA1153 Secure CAN transceivers help bring the industry one step closer to securing their in-vehicle CAN network communication. ◀

REF	MITIGATION ACCORDING TO UNECE R155 (ANNEX 5)	
M1-M5	(not relevant for embedded software)	
M6	Systems shall implement security by design to minimize risks	NXP ISO/SAE 21434 certified
M7	Access control techniques and designs shall be applied to protect system data/code	
M8	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data	
M9	Measures to prevent and detect access shall be employed	
M10	The vehicle shall verify the authenticity and integrity of messages it receives	TJA115x configurable CAN ID passlist and blocklist
M11	Security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules)	
M12	Confidential data transmitted to or from the vehicle shall be protected	
M13	Measures to detect and recover from a denial of service attack shall be employed	TJA115x configurable flooding protection
M14	Measures to protect systems against embedded viruses/malware should be considered	
M15	Measures to detect malicious internal messages or activity should be considered	TJA115x rule set
M16	Secure software update procedures shall be employed	
M17	(M17 is not defined in the standard)	
M18	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege	
M19	Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions	TJA115x enables IDS identify compromised sender node

Figure 5: The NXP CAN transceivers TJA1152 and TJA1153 enable meeting some of the UNECE R155 security mitigation requirements for CAN networks (Source: NXP)

Acknowledgements: The author would like to thank Cindy Weissmueller and Holger Zeltwanger from CiA, Tony Adamson, Thierry Walrant, Sebastian Kleis, Georg Olma, Verena Windischbacher, Damaris Ochoa, and Garance Aubert-Mazenq from NXP as well as Florian Rehm from ZF for their valuable discussions and inputs.

Author

Karthik Sivaramakrishnan
NXP Semiconductors
karthik.sivaramakrishnan@nxp.com
www.nxp.com