Why encrypt logged CAN data?

A common method for collecting raw CAN data is to log it on an SD card or to upload it to a server. In many cases, the collected CAN data is unencrypted. This article highlights three reasons why the lack of encryption may lead to problems.

Privacy regulations like GDPR and CCPA are key reasons for encrypting recorded CAN data at rest on SD cards (Source: CSS Electronics)

The complete article is published in the September issue of the CAN Newsletter magazine 2020. This is just an excerpt.

Privacy regulations

Recent years have shown a drastic increase in privacy regulations, including GDPR (general data protection regulation) in EU and CCPA (California consumer privacy act) in California. If a breach occurs, companies may face substantial fines. However, if the data is encrypted “at rest” (e.g. on an SD card) and “in transit” (e.g. during upload), fines may be waived or reduced.

CAN data is often linked to e.g. a driver of a vehicle and may contain information on VIN (vehicle identification number), speed, fuel consumption, DTCs (diagnostic trouble codes), and GPS (global positioning system) data. It is generally considered in scope of the privacy regulations. In short, not encrypted CAN data can have large financial consequences in case of data breaches.

Remote cyber-attacks of connected assets

Vehicles and machinery are increasingly connected, which exposes these assets to cyber-attacks. For example, a compromised CAN dongle can be used to remotely control asset functionality (e.g. turning a steering wheel) or to deny service of low-priority CAN messages by broadcast- ing high-priority CAN messages at high frequency.

Remote cyber-attacks via Classical CAN is an increasingly critical security risk (Source: CSS Electronics)

CAN FD may solve this problem via such solutions as Secure Onboard Communication (SecOC), effectively encrypting the CAN data and making it difficult to spoof the system. However, CAN FD is still in the early stages of roll- out and Classical CAN assets remain exposed.

If a dongle uploads unencrypted CAN data, an attacker may use this to reverse engineer the CAN frames required to control specific asset behavior. Such attacks can be harder to defend as the denial of service attacks. In short, not encrypting CAN data used in e.g. telematics may expose assets to critical cyber-attacks.

Business-critical data

CAN data is increasingly used by OEMs (original equipment manufacturers) e.g. in prototype fleet testing or as part of ‘black box’ systems used for legal compliance, insurance or warranty dispute handling. This type of CAN data is often sensitive in its nature. The validity of such data can be critical.

If you would like to read the full article you can download it free-of-charge or you download the entire magazine.

cw