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.

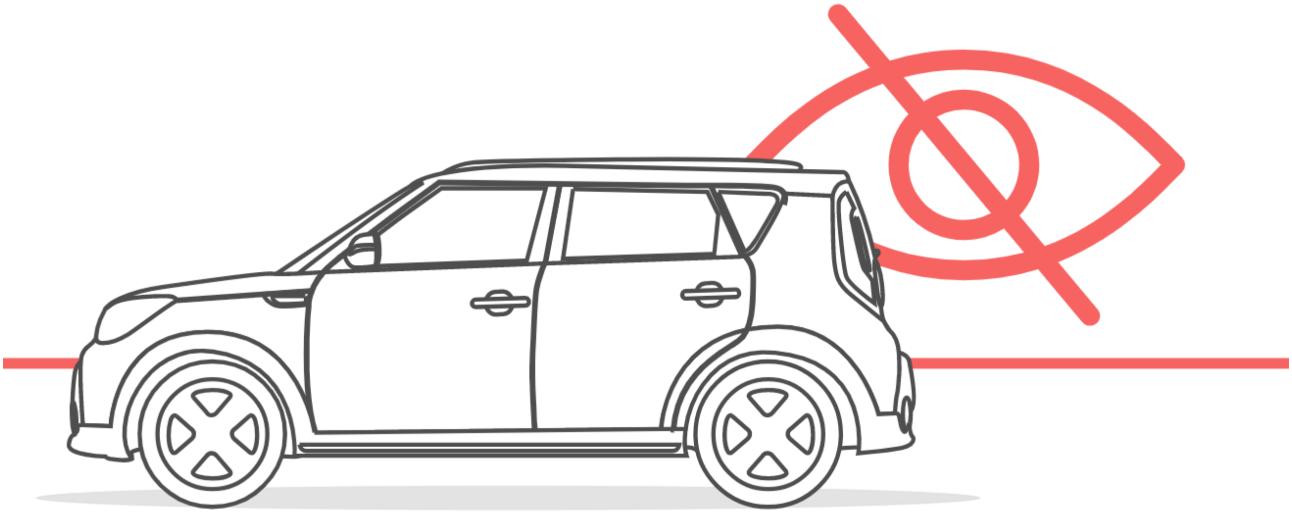

Figure 1: Privacy regulations like GDPR and CCPA are key reasons for encrypting recorded CAN data at rest on SD cards (Source: CSS Electronics)

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 broadcasting high-priority CAN messages at high frequency.

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.

For example, a dispute may arise if a CAN-based asset breaks down in the field. This could lead to large financial consequences. Here, an OEM might use CAN log files to prove that the asset failure was due to the incorrect usage. However, before the OEM can collect the unencrypted CAN data from the SD card, it is possible for the end user to modify the log files e.g. to remove the traces ▷

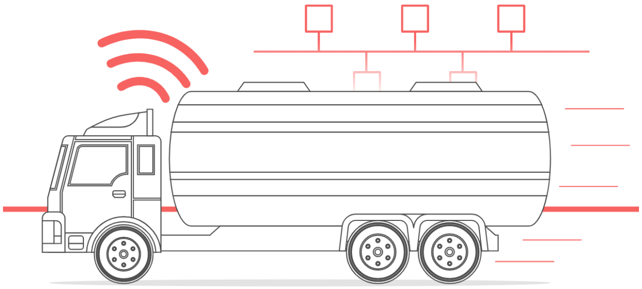

Figure 2: Remote cyber-attacks via Classical CAN is an increasingly critical security risk (Source: CSS Electronics)

Figure 3: Data integrity is essential for use cases where data is used as a legal proof (e.g. warranty dispute handling) (Source: CSS Electronics)

Figure 5: The CANedge2 is designed for end-to-end security (Source: CSS Electronics)

of the incorrect usage. Conversely, the end user may claim that the OEM has injected false data into the log files. In short, unencrypted CAN data logs may be stolen or falsified - with big consequences.

Is raw CAN data not already encrypted?

Someone may argue that "raw" CAN data is already encrypted as the data must be decoded to be interpretable (e.g. via DBC files). There are fallacies to this view. A large share of data logging use cases relates to J1939 data (heavy duty vehicles) or OBD2 data (cars). In both cases, data can be easily decoded via DBC files available for purchase or free online. Secondly, even if the data is 100 % proprietary with a carefully protected DBC file, the data can still be decrypted via reverse engineering. In the view from CSS Electronics, raw CAN data is equivalent to a plain text.

Things to consider when encrypting CAN data

To encrypt the CAN data, companies should consider various aspects of their data logging setup:

- If data is stored on an SD card, the data logger should be real-time encryptable. This means that the files should not be temporarily exposed e.g. while the batch-processing process.
- The data encryption must ensure data integrity to prove that the data contents were not changed. The risk of data falsification can be removed e.g. by deploying an AES-GCM (advanced encryption standard, Galois-counter mode) algorithm.
- If CAN data is uploaded via a WiFi connection or 3G/4G cellular networks, the device should support HTTPS (hypertext transfer protocol secure) for secure data transfer.
- All involved passwords must be encrypted if these are stored on a device or an SD card.

A key challenge considering the above requirements is that real-time data encryption is a computationally intensive task. As such, proper encryption requires dedicated hardware components, which are not available in most CAN data loggers deployed in the field today.

Data encryption implementation

At CSS Electronics, encryption was a key design criterion for the CANedge data logger. CSS faced increasing demand from customers for encryption, in particular after the roll-out of the CCPA. Many OEMs see this as make-or-break for their use cases. To meet the demand for encryption, the CANedge1 and CANedge2 data loggers support data encryption. ◀

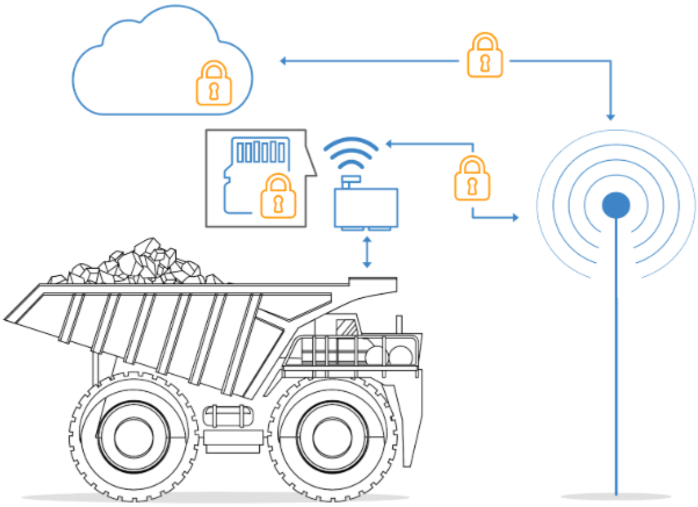

Figure 4: A modern telematics solution needs to address multiple security risks (Source: CSS Electronics)

Author

Martin Falch
CSS Electronics
contact@csselectronics.com
www.csselectronics.com