The CANopen FD multi-level security demonstrator consists of a simple CANopen FD system with two generic I/O devices from Peak-System (buttons, signal lights) and a controller device with touch screen and text display (LED matrix). All of these are based on LPC54618 or LPC54S018 micro-controllers from NXP. An optional CANopen FD Bluetooth gateway can be used to provide a tablet remote access to the controller.

The different security levels implemented in the demonstrator protect from multiple attack levels:

- **Hardware level attack:** extract keys and/or codes from micro-controllers when unlimited physical access is available (through debug access or code extraction services).
- **Security solution:** Use micro-controllers with special protected non-volatile storage like the NXP LPC54Sxxx micro-controllers with PUF (physical unclonable functions) protection to protect code and keys.
- **CAN (FD) frame injection attack:** use a CAN sniffer connected to the system or a hijacked connected CAN (FD) device, listen to all CAN (FD) frames and inject frames to trigger control functions.
- **Security solution:** Use NXP TJA115x Secure CAN Transceiver (HW) or CANcrypt message monitoring (SW) to react to detected injections.
- **Advanced CAN (FD) frame injection attack:** perform CAN (FD) frame injections after the device monitoring these CAN IDs has been taken offline or from a hijacked, authorized device.
- **Security solution:** Use CANcrypt (FD) secure grouping with secure heartbeats and message authentication to prohibit injected, unauthorized messages from being accepted.

Many CAN-based networks open multiple attack vectors for hackers, especially after they have gained access to the system either remotely through a gateway or even physically.
CANcrypt-secured messages have a security record embedded and can be encrypted if needed. Authentication is provided based on an encrypted CRC16 value. The security algorithms used are configurable. Default methods are XTEA64 or AES128.

CANopen FD multi-level security demonstrator

Figure 3 shows the functional elements of the demonstrator. All CANopen FD devices are protected with CANcrypt message monitoring and secure grouping.

A CANgineBT-FD module by ESSolutions provides an Android tablet wireless access to the CANopen FD network. DTLS end-to-end security is established between the tablet and the controller and visualizer module which accepts remote control commands and displays text strings received by the tablet.

The demonstrator is shown at the Embedded World 2019 in Nuremberg, hall 4A, booth 220. A video about the demonstrator will be released after the Embedded World.

Author
Olaf Pfeiffer
EmSA (Embedded Systems Academy)
info@esacademy.com
www.esacademy.de