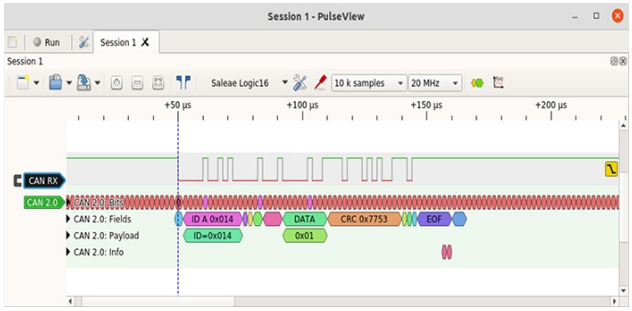
CAN Newsletter Online

CAN NEWSLETTER MAGAZINE

CAN decoder warns for malicious attacks

The open-source Sigrok project is a set of drivers and tools. It provides a desktop oscilloscope and logic analyzer UI (user interface) that can control different instruments (from Siglent, Rigol, and others).



Decoder screenshot of a CAN frame (Source: Canis Automotive Labs)

The complete article is published in the June issue of the CAN Newsletter magazine 2021. This is just an excerpt.

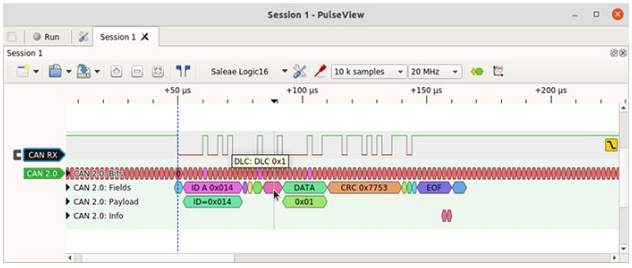
The UI runs on Mac OS, Windows and Linux and is called Pulseview. Integrated is also a command-line tool for batch decoding, useful in an automated test environment. Pulseview has an API (application programming interface) for protocol decoders. Recently, a decoder for CAN has been introduced. Figure 1 is a screenshot of the decoder showing a CAN frame. Here, the Pulseview interface runs on Ubuntu Linux. The logic analyzer hardware used here is a 16-channel Saleae Logic16. But the available USB logic analyzers that cost less than 10 US $ with eight channels and a sample rate of up to 20 MHz are also suitable for use with CAN. A falling-edge trigger condition is typically used with CAN (this is the sync point for the protocol). A pre-trigger buffer enables the decoder to see at least ten recessive bits to know that the next dominant bit is a new frame.

The decoder shows four lines of details about a CAN frame:

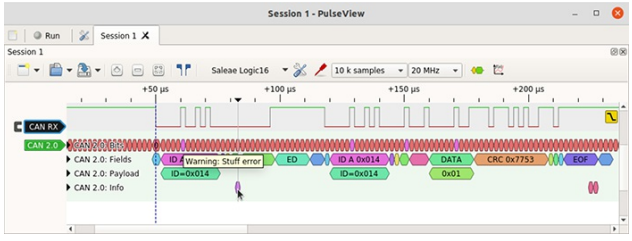
- The raw bitstream (including stuff bits)
- The decoded CAN fields
- The decoded CAN-ID and payload bytes
- An information line showing protocol events and warnings

View of details

Pulseview shows as much details as fits into an item for a given time scale, but a tooltip appears with the full data if the mouse pointer hovers over an item. For example, the value of the 4-bit DLC (data length code) field with a tooltip is shown in Figure 2. The decoder also checks the frame for valid fields and marks when an error is detected. For example, it will show in the warning line when the received CRC (cyclic redundancy check) does not match with the calculated CRC, when the ACK (acknowledge) field is not 0, when a stuff error has been detected, and so on. It also shows an active error frame including the superposition, the error delimiter, and the IFS (interframe space) field following an error frame.



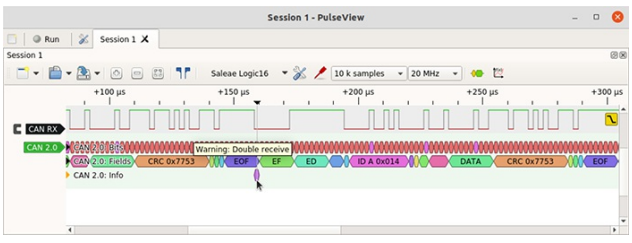
Value of the 4-bit DLC field shown with a tooltip (Source: Canis Automotive Labs)



Warning about a stuff error (Source: Canis Automotive Labs)

The warning as shown in Figure 3 is a stuff error – the result of an error being signaled by another CAN controller. The decoder shows the error flag (which includes the super-position of dominant bits from many controllers) and the error delimiter. The trace also shows the frame being re-transmitted successfully. The double-receive event is a particularly interesting property of CAN. Because a frame is received one bit-time before it is transmitted, it is possible that an error in the last bit of the EOF (end of frame) causes the transmitter to detect an error and retransmit the frame, leading to it being received twice. This is not a bug in the CAN protocol: it is an inevitable consequence of implementing an atomic broadcast protocol (something that most other communication protocols do not even attempt to provide, which is one reason why CAN is such a superbly reliable fieldbus protocol).

As seen in Figure 4, the decoder warns of this specific event (double receive). This event should happen rarely (a bit error must occur exactly at the last bit of EOF). But it can be engineered to occur by an attack on the bus: by deliberately injecting a dominant bit at the last bit of EOF, an attacker can force the frame to be retransmitted and received twice. If the frame being targeted contains an event data, then that event will be acted upon twice by receivers, which could cause all kinds of things to go wrong – the very purpose of a malicious attack. The decoder also shows when there is an overload frame – something that should never be seen since mod- ern CAN controllers never generate these frames.



Warning about a double receive (Source: Canis Automotive Labs)

If you would like to read the full article from Ken Tindell (Canis Automotive Labs), you can download it free of charge or you download the entire magazine.

cw