Controller Area Network Security Data Diode

Extended Abstract

Introduction

A controller area network (CAN) security data diode converts a stub of the linear CAN bus from being able to read and write to read-only. This effectively isolates a network node by preventing it from writing data to the network. The CAN data diode is a hardware-based solution that gives system integrators and vehicle owners the ability to take active steps in preventing any detrimental CAN traffic from affecting the normal operation of a vehicle. The original concept for the CAN security data diode was to isolate electronic logging devices (ELDs) on heavy vehicles, but the hardware device can be used to isolate any read-only node on a CAN bus (e.g. a radio).

Problem Statement

Even though the controller area network protocol has reliable delivery mechanisms built in with the acknowledgment field, CAN lacks message authentication mechanisms at the protocol level. This means unintended or malicious network traffic can be introduced to the system without recourse. Devices connected to the vehicle CAN networks are capable of both receiving and sending information with equal access to the direct-link vehicle network. A cybersecurity breach in any of the connected controller applications affecting the CAN communications can lead to serious consequences.

In new vertically integrated vehicle systems a designer can specify some application layer authentication mechanisms like checksums, or cryptographic message authentication code (CMAC). However, in legacy systems, aftermarket device installations, or horizontally integrated industries, like heavy vehicles, the ability to implement application layer protections is challenging. Furthermore, federal regulations, like the ELD mandate for heavy vehicles, may require the installation of wirelessly connected devices to a vehicle. The introduction of these ELD devices to the SAE J1939 network is required on all trucks that are so equipped, which reaches back as far as model year 2000 vehicles. Legacy fleets are now required to have wirelessly enabled electronic devices connected to the same controller area network that is used by the brakes, engine, instrument cluster. Vehicle manufacturers have little influence on the quality and security of the ELD devices connected on their vehicles.

Implementation

The CAN security data diode works by using two CAN transceivers in a configuration such that the transceiver connected to the main CAN bus (let's call this the J1939 transceiver) has its receive data line (RXD) connected to the transmit data line (TXD) of a transceiver connected to the isolated node (let's call this the ELD transceiver). This would act as a CAN relay where the J1939 transceiver would convert the differential CAN signal into a logic signal which is sent to the ELD transceiver to be converted back to the differential CAN signal. There is no inspection of or filtering of the data, so latency is minimized. However, the reverse connection is not made, so any data received from the ELD transceiver that would be sent out on the TXD logic pin is not received by the J1939 transceiver. Removing the connection from RXD of the ELD transceiver to the TXD of the J1939 transceiver eliminates the ability for messages generated from the isolated node to be seen on the main CAN bus.

Since the physical implementation of the diode functionality is based solely on hardware transceivers, there is no way for a software vulnerability to exist in the diode. To attack or circumvent the CAN data diode itself, someone could physically remove it from the wiring harness.

Dealing with messages on isolated nodes

While the intended use of the CAN security data diode is to enforce a read-only policy, there may be times when the isolated node would legitimately respond. For example, an isolated device may respond to a request for component information defined in SAE J1939. Another example is address claiming according to the SAE J1939 specification. If the back-to-back transceiver solution is deployed on its own, then the network on the isolated ELD side would be incomplete. Since the CAN controller is responsible for sending acknowledgment bits for received messages, the transceiver only implementation would not be able to satisfy this functionality. Without the ability for the isolated device to have its messages acknowledged, the messages will retry and accumulate errors. This may affect the functionality of the isolated device as it would be in an error state.

To alleviate the issue for a lack of acknowledgement, another CAN node needs to be present on the isolated bus. This node needs to contain both a controller and a transceiver with settings to match the bitrate of the original communications system. This new node on the isolated side of the network is build into the CAN data diode and is called the Acknowledger node.

Another challenge for an isolated ELD node when sending messages is arbitration. For the non-destructive media access control solution used by CAN to work, the nodes on the network need to be able to monitor the bus. When isolating a node, then the rest of the nodes cannot detect when the isolated node tries to transmit data. This means the main CAN bus will detect a quiet bus, even if the isolated node tries to transmit. Since the bus is quiet, the nodes on the J1939 side may begin transmitting, even if the isolated node is in the middle of transmitting a message. If this happens, bits may be flipped, or the CAN structure may be violated, and the isolated node will detect that it did not receive what it sent. This will initiate the error handling process on the isolated node. This process will likely try to send the message again during the next bus quiet phase, but the same issue may come up again. During times with heavy busloads, the process may repeat enough times for the isolated node on the ELD network to accumulate enough transmit error counts to enter an error passive or bus off state.

To prevent the effect of a so-called "chatty" main CAN bus sending the isolated node into an error state, the Acknowledger node built into the data diode will track error counts and be able to silence the ELD transceiver that is forwarding the busy traffic from the main CAN bus. This temporary respite for the isolated node enables a successful transmission from the isolated node on the ELD side of the network, which keeps the isolated node from going into an error passive or bus-off state.

ELD Request Proxy

In the case of an ELD that is governed by regulation, there are certain data elements that need to be requested according to the SAE J1939 standard. These elements include engine hours and vehicle identification number. Since these elements are required, it is likely that an ELD would request them using the SAE J1939 parameter group number for requesting data. However, if the ELD is isolated and cannot request this information, another device on the network must provide it. In some cases, these messages are requested by and among the modules already on the network. However, if they are not readily available during normal operation, then a so-called requester node will need to act as a requesting proxy for the ELD. This purpose-built device can be integrated into the CAN data diode or installed as a separate device. The requester should only request data elements if they are not already present. Both ISO 14229 messages and SAE J1939 message should be examined to look for the required data elements.

Hardware Circuit Description

A reference design, as shown in the Appendix, was built using STMicroelectronics' STM32F042G4 ARM Cortex-M0 microprocessors with built-in CAN controllers. These were coupled with Texas Instruments' CAN transceivers from the TCAN33X family. In quantities of 100, the price per unit (including the enclosure) was $53.96 with US-based manufacturing for the prototype units.

There are four CAN transceivers; two of the transceivers are dedicated to the data diode functionality. The data diode transceivers are the TI-TCAN330 devices with silent mode and shutdown mode. The silent mode is controlled on pin 8 of the transceiver and is connected to the Acknowledger microprocessor. If the Acknowledger detects receive errors, which are likely from interference between the isolated node and the main CAN bus, then it will put the ELD transceiver into silent mode to prevent the transmission of data from the main bus to the isolated bus. The J1939 transceiver is always in silent mode. Pin 5 of the data diode transceivers are used to toggle the shutdown modes for the system to reduce power when the CAN bus is silent.

The remaining two CAN transceivers are connected to the STM32F0 processors. These are the TI TCAN334 that have a shutdown mode and a low power standby mode with wake. The standby mode enables the transceiver to wake with network traffic and to inform the requester microcontroller to activate the remaining transceivers. After a timeout period of low or reduced traffic, the microprocessors will enable the transceivers' low power modes.

When a CAN security data diode is installed, it will automatically determine the best bit timing to match the bitrate of the vehicle network. The two most popular choices are 250,000 bps and 500,000 bps. The process of automatically determining the bitrate, or autobaud feature, leverages the receive error counter (REC) functionality of

the CAN controller. The initial guess for the bit timing is loaded from a register in EEPROM. If REC increases when new messages arrive, a new value is tried until messages arrive. The new value is stored in the EEPROM, which will keep the unit from iterating over the valid bit timing combinations if the device is installed on the same vehicle (or a CAN bus with the same rate).

The CAN terminating resistors are also isolated with the CAN Data diode. Therefore, the ELD and Acknowledger transceivers are connected to a differential pair that has 60 ohms of resistance across the pair. Examination of the wave forms as observed with an oscilloscope on the differential signaling pair on either side of the CAN Data diode shows there is no recognizable lag in the signals from one side to another. In other words, any delay in the signal is influenced only by electronic wave propagation in the semiconductors since there is no filtering mechanism in place.

The physical connectors to the CAN data diode reference use a DSUB 15 connector with two rows. The industry standard pinout has battery power on pin 8, ignition signal on pin 1, ground on pin 6, J1939H on pin 13, and J1939L on Pin 12. All other pins pass through. The raw battery and ignition connections are reverse polarity protected with a Schottky diode. Conductive noise suppression is handled by a hybrid varistor. Noise and Electrostatic Discharge protections are built into the CAN transceivers. All components selected for the reference build are AEC rated for an automotive environment.

If an ignition signal line is not present at the location of installation, then a resistor connects the conductive path for the ignition signal to the raw battery line, which pulls the ignition signal high. The Infineon linear Low Dropout (LDO) regulator supplies 3.3V to the board with a maximum current draw of 100mA when the enable pin is pulled high. The ignition line is connected to the enable pin for a hardware-based power regulation system. If the ignition line is not independent of the battery voltage, then the programming in the microprocessors will need to manage current draw when the vehicle is off. The reference design draws about 30 mA when on. The software for the Acknowledger and the Requester are programs that implement their necessary functions of initializing the hardware systems, setting the bit rates, and scheduling the processes for performing the requests and power monitoring. A CAN based updating systems was purposely not implemented as changes to the CAN data diode will need to be done with physical access. For the reference hardware, programming is done using a SWD enabled JTAG device. The board has the Cortex -M headers with ten pins (fine pitched). These programs are needed to isolate the ELD for heavy trucks and manage power saving features. The programming and debugging headers on the printed circuit board are to the outside of the rest of the functional circuits. This feature enables production without debug headers by simply changing the board outline.

Test Results

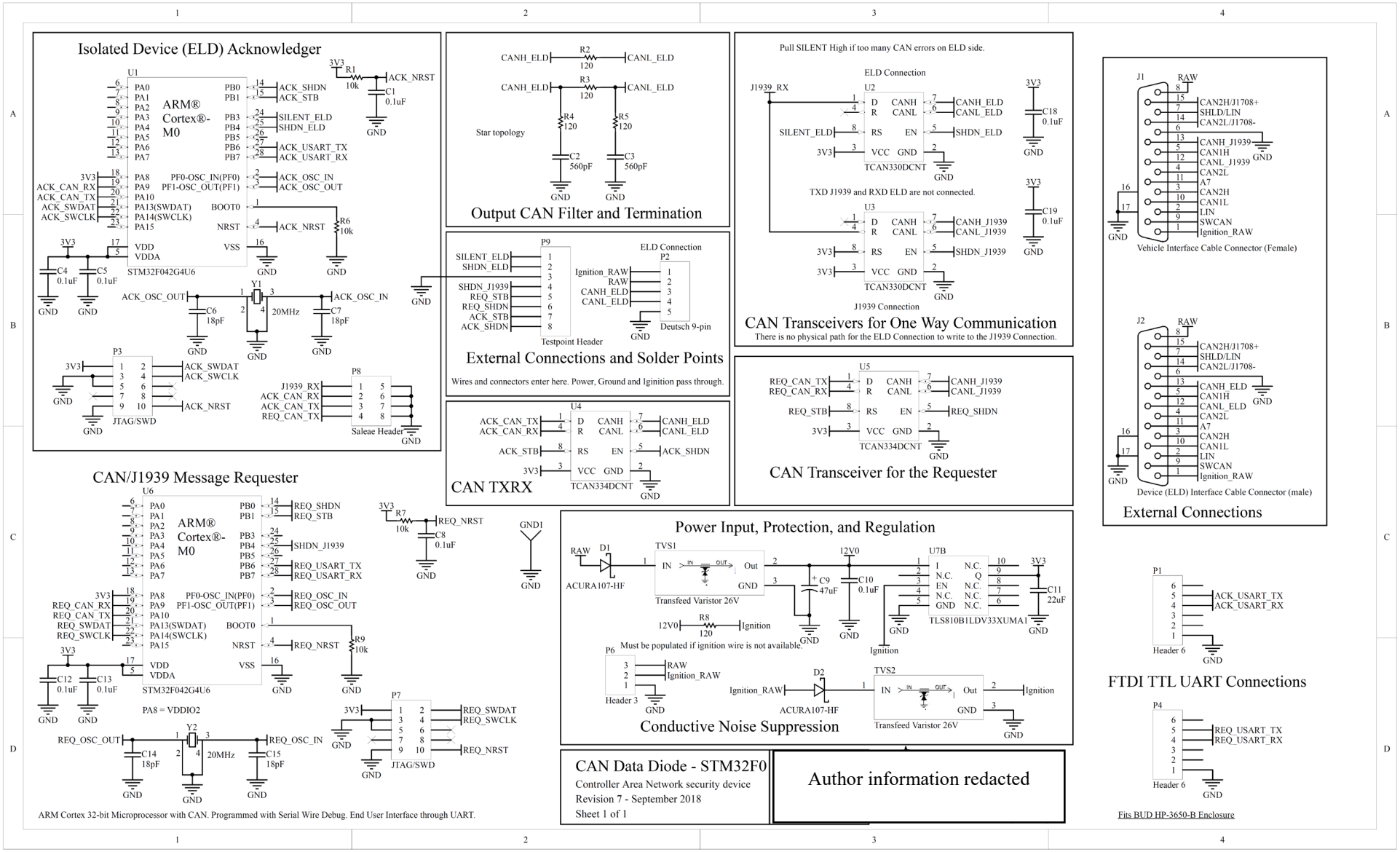
Test results up to 1 Mbps shows all CAN traffic flows from the J1939 side to the ELD side error free when the isolated ELD node is quiet. The acknowledger functions as desired can be observed through the CAN TX line sending out acknowledgment bits for every CAN message passing through the data diode. If the ELD side is “compromised” and tries a denial of service attack by flooding the bus, the CAN Data Diode isolates that attack and no disruption of the main CAN bus is noticed when observing with both an oscilloscope and a CAN data logger.

Discussion and Conclusion

The CAN security data diode is well suited to isolate read-only nodes that may not have well understood security properties. Some of the earliest academic research by Koscher, et al[i] demonstrated a radio unit could be exploited to affect the CAN bus. If the radio does not need to write to the CAN bus, then the CAN data diode can guarantee read-only behavior and offers a robust security solution to protect against unknown security vulnerabilities in radio head units. Printed circuit board adaptations to accommodate J1962 OBD-II connectors are possible, which could enhance security for the diagnostic ports to accommodate installation of after-market devices to the diagnostics port.

The CAN data diode is applicable wherever a read-only or monitoring device is installed, regardless of the vehicle or industry. Rail, busses, and maritime applications may have more opportunities for passengers to tamper with wiring or accessing the CAN bus in an unauthorized way. The CAN data diode can mitigate the effect of a threat actor accessing the CAN through a monitoring device. Asset tracking and data logging features are also good candidates to be isolated behind a CAN Data Diode. The CAN security data diode is a hardware-based solution to mitigate the effect of an exploited node on a CAN bus.

Appendix: Reference Design Schematic



References:

[i] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage. 2010. Experimental Security Analysis of a Modern Automobile. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy* (SP '10). IEEE Computer Society, Washington, DC, USA, 447-462. DOI=http://dx.doi.org/10.1109/SP.2010.34