Ethernet based Layer 2 Data Safety

Ethernet Layer 2 End-to-End Data Safety
Aboubacar Diarra – Robert Bosch GmbH

Automotive Electronics
Ethernet based Layer 2 Data Safety

Outline

→ Motivation
→ Existing Automotive Layer 2 Data Safety Paradigms
→ Automotive Use-Cases
→ Current Ethernet based Data Safety Mechanisms
→ Data Safety Evaluation Criteria & Next Steps
Ethernet based Layer 2 Data Safety

Motivation

Why a Data Safety Mechanism?
- Several influences such as high temperatures, electromagnetic interferences etc. in in-vehicle networks
- Errors occurrence like data corruption, packet loss & link failure.
- That is why, existing in-vehicle communication systems like CAN provide dedicated error detection & correction mechanisms on Layer 2.
- Need of Data Safety Mechanisms for Ethernet in in-vehicle networks.

Why on Layer 2?
- Common automotive protocols like CAN, FlexRay & LIN run on Layer 1, 2
- CAN implements Error Handling on Layer 2.
- Layer 2 chosen mainly for performance and cost reasons

What about Ethernet?
- Need of Layer 2 Data Safety for reliable and cost-efficient communication for in-vehicle networks (and Industrial automation)
Existing Automotive Layer 2 Data Safety Paradigms
(Example of CAN Error Handling)

CAN Frame Overview

<table>
<thead>
<tr>
<th>SOF</th>
<th>Identifier</th>
<th>RTR</th>
<th>IDE</th>
<th>r0</th>
<th>DLC</th>
<th>DATA</th>
<th>CRC</th>
<th>ACK</th>
<th>EOF</th>
<th>IFS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Bit</td>
<td>11 or 19 Bits</td>
<td>1 Bit</td>
<td>1 Bit</td>
<td>1 Bit</td>
<td>4 Bits</td>
<td>64 Bits</td>
<td>16 Bits</td>
<td>2 Bits</td>
<td>1 Bit</td>
<td>3 Bits</td>
</tr>
</tbody>
</table>

Different types of error on a CAN Bus
- **CRC Error**: when the computed CRC value on reception is different to the transmitted one
- **Bit Error**: when a node reads 0 (or 1) on the bus after sending 1 (or 0)
- **Bit Stuffing Error**: when more than 5 bits of the same weight are sent on the bus
- **ACK Delimiter Error**: when the field is dominant
- **CRC Delimiter Error**: same case for the ACK Delimiter Error
- **ACK Slot Error**: When a dominant bit is sent by a node during the ACK Slot

Error Signaling
- When a node detects an error, it sends an Error Frame after the ACK Delimiter
Existing Automotive Layer 2 Data Safety Paradigms (Example of CAN Error Handling)

**Active Error Frame**
- Active Error Flag (6 Dominant Bits)
- Active Error Delimiter (8 Recessive Bits)

**Passive Error Frame**
- Passive Error Flag (6 Recessive Bits)
- Passive Error Delimiter (8 Recessive Bits)

Error Counters to isolate faulty nodes from the network!

Such mechanisms might also be needed in automotive Ethernet based sub-networks!

Different Error States on a CAN Node

- **Error Active**
  - REC > 127
  - TEC > 127

- **Error Passive**
  - REC < 128
  - TEC < 128

- **Bus off**
  - TEC > 255

**REC**: Receive Error Count
**TEC**: Transmit Error Count

Restart request & 128 occurrences of 11 consecutive recessive bits
Ethernet based Layer 2 Data Safety

Typical potential Layer 2 Data Safety Use-Cases

Unicast Peer to Peer Radar Sensor Data Fusion

Multicast Radar Sensor Data Fusion

CAN Layer 2 End to End (E2E) Data Safety
Automotive Control Data Encapsulation in Ethernet Frames via 1722a
Current Ethernet based Data Safety Mechanisms

- **AVB / TSN Mechanisms**
  - **IEEE 802.1 Qat** Stream Reservation Protocol to guarantee necessary bandwidth resources to handle a stream from the sender to the receiver.
  - **IEEE 802.1 Qav** Queuing & Forwarding traffic shaper to prevent bursts during data transmission.
  - **IEEE 802.1 CB** Seamless Redundancy for fault-tolerance without failover.

- **Other Mechanism**
  - TCP/IP that runs Layer 3/4 based Acknowledgment and Retransmission Mechanisms for Data Integrity
  - Pragmatic General Multicast (PGM): a Layer 4 IETF experimental Mechanism for Data Transmission reliability via Negative Acknowledgment and Retransmission Mechanisms
  - Any other mechanism?

- **Scope**
  - Focus on the PGM & improve it on layer 2 for in-vehicle communication
Focus on PGM Error Detection & Correction (1)

Error Signaling

The PGM Sender can now resend the lost or corrupted packet.

No need to send any NCF and forward any NAK because they have already been sent for the same lost packet.

NAK: Negative Acknowledgment
NCF: NAK Confirmation
Focus on PGM Error Detection & Correction (2)

Error Correction

Scope:
Adapt & Improve this mechanism on layer 2

RD ATA: Repair Data
Data Safety Evaluation Criteria & Next Steps

>Data Safety Evaluation Criteria
- Fault occurrence probability in a network supporting current AVB/TSN Mechanisms
- Fault recovery time
- Packet reception guaranty time
- Bandwidth needed to correct a fault
- Faulty receiver nodes isolation conditions
- Data Consistency in the System

>Next Steps
- Evaluate Data Safety Criteria
- Identify different failure scenarios in an Ethernet based network
- Analyze the necessity of a layer 2 error detection & correction process based on:
  - ACK & Negative ACK Mechanisms
  - Retransmission Mechanisms
  - Error Counter Implementation
Ethernet based Layer 2 Data Safety

Thank You for your Attention
Any Questions?