Ethernet Layer 2 Data Safety

Ethernet Layer 2 End-to-End Data Safety

IEEE 802.1 Plenary Meeting - Dallas - 2013.11.12

Abou Diarra – Robert Bosch GmbH

Automotive Electronics
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 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)
Motivation

- The topic has been highlighted by another automotive organization

3. JasPar Requirement (2) Ack and Retry

Continuously real time monitoring system for network condition is required for automotive.

- The method realized with upper layer protocol like TCP/IP does not meet automotive real time requirement.
- Also, every End station needs more processing load if we use such kind of upper layer protocol, in compare with CAN.

-> JasPar thinks that new solution has to be prepared at Layer2.
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>

- **Sequence Delimiter**: 15 Bits
- **Slot Delimiter**: 1 Bit
- **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
Ethernet Layer 2 Data Safety

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 maybe also be needed in automotive Ethernet based sub-networks!

![Different Error States on a CAN Node](image)

- **TEC > 255**
- **REC > 127**
- **TEC < 128**
- **REC < 128**

**Error Active**

**Error Passive**

**Bus off**

**REC**: Receive Error Count

**TEC**: Transmit Error Count

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

Automotive Use-Cases

- Automatic Doors Unlocking in crash situation

Automotive Control Data Encapsulation in Ethernet Frames via 1722a
Ethernet Layer 2 Data Safety

Automotive Use-Cases

- Road traffic signs recognition for Automated Driving

CAN Layer 2 End to End (E2E) Data Safety
Automotive Control Data Encapsulation in Ethernet Frames via 1722a
Automotive Use-Cases

Requirements on Data

- Event based control data transmission
- No strict and severe latency requirement
  - Latency in ms range tolerable
- Bandwidth/Resources available
- Frame Reception on target CAN mandatory
  - In case of packet corruption or loss on the link, a retransmission is needed
Ethernet Layer 2 Data Safety

Automotive Use-Cases

- Radar Sensors Data Fusion

MRR → Fusion ECU

LRR

Unicast Peer to Peer Radar Sensor Data Fusion

MRR → SW → Fusion ECU

LRR

Multicast Radar Sensor Data Fusion

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Nbr of Objects</th>
<th>Object 0</th>
<th>Object 1</th>
<th>...</th>
<th>Object n</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Application PDU

PDU Fragmentation

PDU: Protocol Data Unit
PI: Protocol Info
SDU: Segmented Data Unit
Ethernet Layer 2 Data Safety

Automotive Use-Cases

→ Radar Sensors Data Fusion

Requirements on Data

- **Bandwidth Resources needed**
  - From 540 kbps to 300 Mbps

- **Data Fragmentation & Reassembly may be needed**
  - When a PDU is too large to be encapsulated in only one Ethernet Frame
  - Sequence number needed in fragments frames for reassembly
  - Any lost or corrupted fragment needs to be retransmitted

- **Packets Reception on Fusion ECUs mandatory**
  - Radar ECUs need to know that PDUs they sent are correctly received by Fusion ECUs

- **No strict and severe recovery time**
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
- Find a solution based on PGM and/or other possible improvements and adapt them on layer 2 for in-vehicle communication
Department | 6/26/2013 | © Robert Bosch GmbH 2013. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Automotive Electronics

Ethernet Layer 2 Data Safety

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

Failure !

Failure !

PGM Receiver 1
PGM Receiver 2
PGM Receiver 3
PGM Receiver 4

PGM Bridge 1
PGM Bridge 2
PGM Bridge 3

PGM Sender
PGM Sender
PGM Sender
PGM Error Detection & Correction (2)

Error Correction

PGM Sender → PGM Bridge 1 → PGM Bridge 2 → PGM Bridge 3

PGM Sender → PGM Bridge 1 → PGM Bridge 2 → PGM Bridge 3

PGM Receiver 1 → PGM Bridge 3

PGM Receiver 2 → PGM Bridge 3

PGM Receiver 3 → PGM Bridge 3

PGM Receiver 4 → PGM Bridge 3

RDATA: Repair Data

Failure!

RDATA: Repair Data

RDATA: Repair Data

RDATA: 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
Thank You for your Attention
Any Questions?