Time Sensitive Network enabling next generation of automotive E/E architecture

Nobukatsu KITAJIMA
Renesas Electronics Corporation

Dnyaneshwar Kulkarni
Renesas Electronics Europe Ltd.

October 27th, 2015

ACT-AA-15-0051
Contents

1. In-Vehicle Network: Background to introduce Ethernet, New Challenge
2. Evolving E/E architecture
3. Ethernet AVB/TSN & Automotive perspective
4. Automotive Ethernet: Security
5. Automotive Ethernet: Functional Safety
1. In-Vehicle Network: Background to introduce Ethernet, New Challenge
In-Vehicle Network: Trend for Future

In-Vehicle Network 2020 - 2030

- To realize highly advanced functions like ADAS or Autonomous Driving, the ECUs in vehicle network functions will be more complicated. Also, the cooperative controls between ECUs are increased. Furthermore, the number of sensors will be increased, and the resolution for each sensor will be increased.
  - Data traffic will be increased.
- The connectivity to Out-of-Vehicle through wireless networks will be also increased to get real time traffic information and updated map.
  - To keep cars safely, appropriate security function should be prepared.
- Also, appropriate functional safety functions should be prepared for the advanced In-Vehicle Network.

For highly advance functions like autonomous driving…

Increasing connectivity to Out-of-Vehicle Network

Number of sensors will be increased, Sensor resolution will be increased

Number of ECUs/ECU functions will be increased

Cooperative controls between ECUs will be increased
Solution for increasing data traffic: Ethernet

- Both in and between application domains, data traffic tends to be increased.
- For autonomous driving, increasing number of sensors and sensor resolution will affect to further increase of data traffic.

→ CAN’s limitation. Started to introduce Ethernet in Vehicle.

<table>
<thead>
<tr>
<th>Application</th>
<th>2015 Rate (bps)</th>
<th>2015 Protocol</th>
<th>After 2020 Rate (bps)</th>
<th>After 2020 Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Powertrain/Body/Chassis</td>
<td>500K – 10M</td>
<td>CAN</td>
<td>1M – 100M</td>
<td>CAN FD Ethernet AVB/TSN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FlexRay</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ADAS (Sensor)</td>
<td>500K – 1M</td>
<td>CAN</td>
<td>1M – 100M – 1G or more</td>
<td>CAN FD Ethernet AVB/TSN</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diagnosis/Flashling</td>
<td>500K – 1M</td>
<td>CAN</td>
<td>1M – 100M – 1G or more</td>
<td>CAN FD Ethernet (AVB/TSN)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Camera/Infotainment</td>
<td>30M – 3G</td>
<td>Analog</td>
<td>100M – 1G or more</td>
<td>Ethernet AVB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LVDS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backbone</td>
<td>500K – 10M</td>
<td>CAN</td>
<td>1G or more</td>
<td>Ethernet AVB/TSN</td>
</tr>
</tbody>
</table>
Security: Solution for connecting Out-of-Vehicle Network is required

- Traditional Threat
  - Threat occurred from IT and Control meager

- Malware injection by record media or PDA devices

- Transmit malware/illegal data from spoofing servers

- Illegal V2X data reception

- Illegal CAN data mixing

- Reprogramming

- Software data readout

- Tuning by serial writer

- Sensor data alteration

- ECU replacement
Functional Safety: Solution for Networking In-Vehicle System is required

- **Power Train**: Engine Control, HEV/EV Motor, AT Control, Transmission
- **Optical coupler, IGBT, Power MOS, AFE**
- **Chassis**: Steering/EPS, Brake/ABS, Suspensions, Chassis Control
- **Power MOS Driver**
- **ADAS**: Collision Warning, Parking Assistant, Back monitor, Night vision
- **Safety**: Airbag, TPMS, Safety Cont.
- **Body & Security**: Instrument, Power Door, Power Window, Air Conditioning, Mirror, Wiper, Lighting
- **Body & Security**: IPD, Power MOS, LED Driver
- **Networking**: CAN, LIN, FlexRay, Ethernet, Ethernet AVB/TSN, Bluetooth
- **Infotainment**: Car Audio, Connectivity Audio, Car Navigation, Entertainment, ITS/GPS
- **R-Car for Navigation**: Renesas

© 2015 Renesas Electronics Corporation. All rights reserved.
2. Evolving E/E architecture
Pre-Crash Safety example

After getting and recognizing sensor data, ECU sends an emergency message to other domains for control operation.

- **Power Train**: Engine management is activated accordingly.
- **Chassis**: A stability control is performed accordingly.
- **ADAS**: After getting and recognizing sensor data, ECU sends an emergency message to other domains for control operation.
- **Body**: A seat belt is fastened.
- **Out of Car Network**: A warning message is sent to inform cars around.
- **Infotainment**: Emergency is indicated in instrument panel.
Evolving Network Architecture

2010: Local connections between ECUs

2015~20: Domains + Central Gateway

Beyond 2020: Domain Master Gateways
3. Ethernet AVB/TSN and Automotive Perspective
Ethernet Advantage

- Global widely proven network technology:
  - A lot of technical asset.
  - High speed: 100Mbps, 1Gbps, ... >> CAN: 1Mbps
  - Low cost: a lot of parts and tools are already in market. UTP.
  - A lot of developers in the world.

Issue for Ethernet: Best effort network

- Ethernet latency highly depends on traffic.
- There are not time synchronization mechanism between different Ethernet LAN nodes.

Reliable audio/video stream transfer on Ethernet LAN is difficult.

Solution

AVB (Audio Video Bridging) Task Group of IEEE802.1 proposed protocols which can solve above issues: (based on Residential Ethernet of 802.3 study group activities)

After above, the extension for kind of transfer data to include control data then, Task Group name was changed from “AVB” to “TSN” (Time-Sensitive Networking).
Ethernet AVB/TSN Standards

**AVB**

- Standardized completion in 2011.
- Guarantees stream data transfer latency by the combination of following standards.

  (+1) : End Station and MAC Bridge (Switch)

<table>
<thead>
<tr>
<th>Standard</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE802.1 BA</td>
<td>Audio Video Bridging system: Abstract for AVB system features.</td>
</tr>
<tr>
<td>IEEE802.1 AS</td>
<td>Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks: Time synchronizing protocol and process for nodes (*1) in AVB-net.</td>
</tr>
<tr>
<td>IEEE802.1 Qav</td>
<td>Forwarding and Queueing Enhancements for Time-Sensitive Streams. (Now IEEE802.1Q-2011): Bridge (Switch) transfer functions definition.</td>
</tr>
<tr>
<td>IEEE1722</td>
<td>Layer 2 Transport Protocol for Time-Sensitive Applications in Bridged Local Area Networks: Transfer protocol, data format, and time synchronization specific in AVB-net.</td>
</tr>
</tbody>
</table>

**AVB and TSN comparison**

<table>
<thead>
<tr>
<th>Standard</th>
<th>Contents</th>
<th>TSN</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE802.1 BA</td>
<td>Audio Video Bridging system</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>IEEE802.1 AS</td>
<td>Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks:</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>IEEE802.1 Qat</td>
<td>Stream Reservation Protocol (Now IEEE802.1Q-2011)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>IEEE802.1 Qav</td>
<td>Forwarding and Queueing Enhancements for Time-Sensitive Streams (Now IEEE802.1Q-2011)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>IEEE802.1 Qbu</td>
<td>draft</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>IEEE802.1 CB</td>
<td>draft</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>IEEE802.1 Qch</td>
<td>draft</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>IEEE802.1 Qci</td>
<td>draft</td>
</tr>
</tbody>
</table>

**Transport protocol for AVB/TSN**

<table>
<thead>
<tr>
<th>Standard</th>
<th>Renesas supported or not</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE1722</td>
<td>Support</td>
<td>Amending (IEEE1722a)</td>
</tr>
<tr>
<td>IEEE1722.1</td>
<td>t.b.c.</td>
<td>Amending</td>
</tr>
</tbody>
</table>

- IEEE802.1 AS-Revision (IEEE802.1ASbt) Timing and Synchronization: Enhancements and Performance Improvements: draft
- IEEE802.1Qcc Stream Reservation Protocol (SRP) Enhancements and Performance Improvements: draft
- IEEE802.1Qbv Enhancements for Scheduled Traffic: draft
- IEEE802.1Qbu Frame Preemption: draft
- IEEE802.1CB Frame Replication and Elimination for Reliability: draft
- IEEE802.1Ch Cyclic Queuing and Forwarding: No draft
- IEEE802.1Qci Per-Stream Filtering and Policing: No draft
- IEEE1722 Layer 2 Transport Protocol for Time-Sensitive Applications in Bridged Local Area Networks: Amending (IEEE1722a)

*: on August 24th, 2015

© 2015 Renesas Electronics Corporation. All rights reserved.
## Automotive Perspective on AVB/TSN standards

### AVB (Automotive profile) vs TSN

<table>
<thead>
<tr>
<th>AVB (Automotive profile)</th>
<th>TSN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intention</strong></td>
<td></td>
</tr>
<tr>
<td>• Audio video synchronisation</td>
<td>• Control application</td>
</tr>
<tr>
<td><strong>Attractive Feature</strong></td>
<td></td>
</tr>
<tr>
<td>• Clock synchronisation</td>
<td>• Clock synchronisation</td>
</tr>
<tr>
<td>• Static Stream reservation</td>
<td>• Stream reservation</td>
</tr>
<tr>
<td>• Traffic shaping</td>
<td>• Traffic shaping</td>
</tr>
<tr>
<td><strong>Automotive area</strong></td>
<td></td>
</tr>
<tr>
<td>• Infotainment</td>
<td>• ADAS</td>
</tr>
<tr>
<td>• ADAS</td>
<td>• Control application</td>
</tr>
<tr>
<td><strong>Specification Stability</strong></td>
<td></td>
</tr>
<tr>
<td>• Yes, automotive profile</td>
<td>• All Specifications in Draft</td>
</tr>
<tr>
<td></td>
<td>• No automotive profile</td>
</tr>
</tbody>
</table>

### Difficulties Automotive semiconductor face

- Standardisation of Requirement from OEM/Tier 1
  - Many a times implementation is ahead of Protocol standardisation
- Maintaining software compatibility with Legacy architecture
- Safety and Security requirements
- Conformance and Interoperability tests
  - Test houses
- Appropriate Tools
Automotive Ethernet: Alliances/Standardization Parties

- Promoting to introduce Ethernet in automotive system globally.
- OABR 100Mbps, 1-pair twisted pair.
- Reduced Twisted Pair Giga-bit Ethernet (RTPGE) for Automotive.

- Promoting AVB/TSN standardization in IEEE.
- Conformance & Interoperability.
- Automotive Profile.
- Software API.

- Promoting to introduce Automotive Ethernet for Japanese automotive industry.
- Scope is from PHY/Wire harness deployment to applications.

AUTOSAR and ISO are also preparing to handle with Ethernet.
Renesas AVB/TSN Hardware support

To support to realize accurate and stable AVB-net by following functions:

- IEEE802.1AS Time Synchronization function:
  - Real time counter for time synchronization.
  - Timestamping function for gPTP messages at transmission/reception.

- IEEE802.1Qav Transfer control function:
  - Max 4 kinds of transmission traffic class simultaneously.
    - SR Class A/B, Network traffic, Best effort traffic.
  - Traffic shaping with hardware credit counter.

- Data transfer function with time synchronization for IEEE1722:
  - Media clock recovery: Time synchronization with gPTP timer.

- Reception filter for A/V traffic, Network traffic (gPTP), and best effort traffic.

Enhancing functions mainly following TSN standard draft:

- Frame Preemption
- Frame Replication and Elimination for Reliability
4. Automotive Ethernet: Security
Security: Traditional and Anticipated Threat

- **Malware injection by record media or PDA devices**
- **Transmit malware/illegal data from spoofing servers**
- **Illegal V2X data reception**
- **Tuning by serial writer**
- **Software data readout**
- **Illegal CAN data mixing**
- **Reprogramming**
- **Traditional Threat**
- **Threat occurred from IT and Control meager**
- **Illegal V2X data reception**
- **Sensor data alteration**
- **ECU replacement**
- **Malware injection by record media or PDA devices**
In-Vehicle security standardization

European major security standard (Evita) defines each ECU’s security level in 3 stages (Full, Medium, Light). In-Vehicle security interpretation is widely taken.
Secure on-board communication in AUTOSAR

“SecOC” objective is to ensure in-vehicle message authenticity (MAC: Message Authentication Code)

source: “Specification of Module Secure Onboard Communication AUTOSAR Release 4.2.1” (AUTOSAR_SWS_SecureOnboardCommunication.pdf)
Automotive Ethernet Security

- Addition to CAN based system security solution so far, following Ethernet based system security standards are discussing in alliances, etc.
  - IEEE802.1X:
    - Port based network access control standard.
  - IEEE 802.1AE-2006:
    - MACsec.
    - IEEE802.1 frame encryption, and packet authentication standards.
  - IEEE 802.1X-REV:
    - Added MACsec key exchange etc to IEEE 802.1X-2004.

- Renesas plans to implement above functions with hardware and software.
5. Automotive Ethernet: Functional Safety
What's SIL/ASIL for communication protocol?

[ANSWER]

→ None.

[REASON]

→ Communication protocol depends on the application
  - Network topology
  - Time constraint
  - Communication System
  - etc.
Detectable failure mode by each communication protocol

- Ethernet (IEEE802.1Qch, CB, etc) can detect the following failure mode. (under confirmation)

<table>
<thead>
<tr>
<th></th>
<th>ET (Event Trigger) CAN</th>
<th>TT (Time Trigger) CAN</th>
<th>LIN</th>
<th>FlexRay</th>
<th>Ethernet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repetition</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Loss</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Insertion</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Wrong sequence</td>
<td>No</td>
<td>No</td>
<td>Insufficient</td>
<td>Insufficient</td>
<td>Yes</td>
</tr>
<tr>
<td>Data corruption</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Delay</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Masquerade</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>TBC.</td>
</tr>
</tbody>
</table>
Automotive Ethernet Functional Safety

- Redundancy with rings or meshes:
  - Ring or mesh configuration in physical, and realizes Ethernet logical:
    - When faults occur, Spanning tree protocol realizes new logical network (IEEE802.1D).
  - Link aggregation:
    - Physical multi connections.
  - Frame Replication and Elimination for Reliability (IEEE802.1CB)
    - Fault tolerance enhancement with integral redundant management.

- AUTOSAR E2E Communication Protection

- Renesas already has functional safety support program.
- Furthermore, Renesas plans to hardware support for TSN, and AUTOSAR E2E Protection support.
- Renesas will support the functional safety for Ethernet based E/E architectures.
Conclusion

- Ethernet is an important technical factor for future E/E architecture.
- New hardware and software support is necessary for Ethernet TSN, Security and Safety to realize future E/E architecture.
- Renesas plans to enhance its AVB solution to TSN with Security and Safety integration.
References (except Ethernet related standards)

- Requirements on E2E Communication Protection, AUTOSAR Release 4.2.1.
- Michael D. Johas Teener: Ethernet 101 for Automotive
Security Standardization


Japan
- IPA
- JSAE
- JasPar

Car2Car Communication Consortium
- HIS SHE
- PRESERVE
- Evita
- AUTOSAR CG607

Europe

US
- SAE TEVEES18
- TCG Automotive

© 2015 Renesas Electronics Corporation. All rights reserved.
Safety Requirement for Network

ASIL depends on ASIL transmitter, ASIL medium and ASIL receiver.

\[ \text{ASIL} = \min(\text{ASIL}_t, \text{ASIL}_m, \text{ASIL}_r) \]

Fault effect listed below can be considered for network

- Unwanted **repetition** of same message
- **Loss** of messages
- Unwanted **insertion** of messages
- **Wrong sequence** between messages
- **Data corruption**
- Message received/transmitted **later than expected**
- **Masquerade** (e.g. wrong address)

Refer: IEC61508, IEC62280
Responsibility of driving task will change from human driver to system as rising autonomous driving level.

Fail operational is a key technology for autonomous driving.

NHTSA: Preliminary Statement of Policy Concerning Automated Vehicles

- **Level 1**: Function-specific Automation
- **Level 2**: Combined Function Automation
- **Level 3**: Limited Self-Driving Automation
- **Level 4**: Full Self-Driving Automation

**Autonomous driving**

- System cover system failure (Fail operational)

**Roadmap for autonomous driving**

- **2015 (Now)**
- **After 2020**

**Driving task**

- **Human**
- **System**

**Driver Monitoring**

- Always
- Only emergency situation
- No need

**Highway Driving**

- Auto. Parking
- Auto. Driving
Different Approach for fail operational

Functional safety for cooperation with other ECUs will become important in addition to fail operational technology.

System architecture consideration for autonomous driving

Functional safety for the cooperation with other ECUs and fail operational

Cooperation with other ECUs

Partial fail operational

Now For Autonomous driving
Safety and Security approach for Renesas MCU

Renesas MCU for automotive support functional safety and security.
Dependent failure

- Dependent failure analysis is key activity for ISO26262 compliance.
- **Dependent failure**
  - **Common Cause failure**
    - Failure of two or more elements of an item resulting from a single specific event or root cause
  - **Cascading failure**
    - Failure of an element of an item causing another element or elements of the same item to fail

**Common cause failure**
- e.g. Failure of power or clock against dual core lock step

**Cascading failure**
- e.g. Unintended register update by lower ASIL task
Key technology for safety mechanism

- **Detection**
  - Normal safety mechanism by H/W and S/W

- **Isolation technology**
  - Avoidance of the fault to affect other mission logic
    - Hi-Z control
    - Double access to the peripherals
  - Protection
    - MPU, Guard (Memory, Peripheral)

- **Identification technology**
  - Identification of the fault
    - Error address buffer

- **Repair technology**
  - Diagnosis w/limited time, switchable mechanism
    - Dual MCU, TMR
    - Partial BIST, Partial Reset
    - Resource Switch function
  - Check pointing
Functional safety technology for next generation

To improve the operational margin by memory cell or circuit technology.