PCI Express® Technology for Automotive Functional Safety (FuSa)

PCI-SIG® Automotive Webinar Series

June 16, 2021
Speakers

Ron DiGiuseppe
Automotive IP Segment Manager, Synopsys

Ron DiGiuseppe is the Automotive IP Segment Manager at Synopsys. He is responsible for automotive segment marketing for Synopsys DesignWare Intellectual Property (IP) solutions for ADAS, Connected Car, & Infotainment applications. Ron brings more than 22 years of semiconductor experience to Synopsys.

Prior to joining Synopsys, Ron held a range of management positions at Xilinx for automotive connectivity IP products as well as engineering development and management roles for companies including Oki Semiconductor, NEC, and Raytheon Corporation.

Stephanie Friederich
Systems Engineer, Intel Corporation

Stephanie Friederich is a Systems Engineer at Intel Corporation. She is responsible for system architecture for both automotive and industrial applications in the Autonomous Transportation and Infrastructure Division. Stephanie brings in experience in developing and debugging complex system designs including high speed data transmission.

Stephanie earned her MS and PhD in Electrical Engineering from the Karlsruhe Institute of Technology.

Thierry Beaumont
Functional Safety Engineer, Intel Corporation

Thierry Beaumont is a Functional Safety Engineer at Intel Corporation. He is responsible for analyses of SoC in the Autonomous Transportation and Infrastructure Division.

Prior to joining Intel Corporation, Thierry work for 10 years in the automotive industry, held team lead position and developer position for ECU up to ASIL D at Continental Powertrain.
Agenda

- Introduction of PCIe® technology in Automotive for Safety critical applications
- Functional Safety (FuSa) background
- PCIe Functionality for Functional Safety
- PCIe technology and additional safety mechanisms to meet ASIL B and beyond
- PCIe technology for Automotive FuSa Summary
Introduction

PCI EXPRESS® FOR AUTOMOTIVE FUNCTIONAL SAFETY (FUSA)
PCIe® Technology: Ideal for Automotive Applications (1/2)

**Technology Requirements**
- High Bandwidth
- Scalability
- Low Latency
- Hypervisor / Virtualized applications
- Better usage of power/thermal
- Security
- Functional safety

**Data Backbone**

**Technology Requirements**
- High Bandwidth
- Low Latency
- EMC/EMI Reliability of long reach cable link
- Security
- Functional safety
PCIe® Technology: Ideal for Automotive Applications (2/2)

Storage SSDs for Infotainment and AD

Technology Requirements
- High bandwidth and fast startup/boot
- Very Low latency
- Very High Endurance & Extended data retention
- Very High Density & Guaranteed write performance
- Stable performance over time/temperature
- SRIOV
- Functional Safety

Telematics Connectivity

Technology Requirements
- High Bandwidth/Throughput
- Data Reliability and Integrity
- EMC/EMI Reliability of long reach cable link
- Security
- Functional safety

Multi-modem:
- 5G
- V2X
- WiFi
- Bluetooth
- GNSS
<table>
<thead>
<tr>
<th>Use Case</th>
<th>Item</th>
<th>PCIe Use Model</th>
<th>Application</th>
</tr>
</thead>
</table>
| 1       | Scaling Compute Processing          | Chip-to-Chip            | ADAS & IVI Domain Controllers
Autonomous Vehicle (AV)
Zonal Architecture-Central
Processing                                           |
| 2       | Data Backbone                       | Long Reach              | Zonal Architecture-In Car Network                                           |
| 3       | PCIe Based Storage                  | Chip-to-Chip Module     | BlackBox
ADAS/AV Mapping
Infotainment                                               |
| 4       | Connectivity: Telematic Control Unit (TCU) | Chip-to-Chip Module Long Reach | Telematics: BT, WIFI, 4G & 5G V2X                                           |
PCI Express® technology is mission critical for automotive SoCs

- Interfaces: LPDDR5/4/4X, Ethernet TSN, MIPI, HDMI, CXL, eDP, CAN
- Processing: AI Accelerators, Embedded Vision, DSP, Security
- Security & SoC Safety Manager
- Sensor Fusion
- 16-/14-nm → 8-/7-nm → 5-nm
- Functional Safety
Functional Safety (FuSa) background

PCI EXPRESS® FOR AUTOMOTIVE FUNCTIONAL SAFETY

- Safety Standards and Automotive Safety Standard Overview
- Definition
- Example: Lane Departure Warning
Safety Standards

- **IEC 61508:2010**
  - Foundational standard
  - Electrical, electronic, and programmable electronic systems (typically in Industrial)
  - Stand-alone & basis for sector-specific standards

  - Programmable electronics installed in series production passenger vehicles
  - Addresses possible hazards caused by the malfunctioning behavior of safety related electrical and/or electronic (E/E) systems (i.e., **malfunctions in the presence of faults**)
  - 10 parts are Normative
  - 2 parts are Guideline
ISO 26262 Definition Fault and Safety Measure

• **fault** definition from ISO26262:2018 Part 1 Vocabulary
  abnormal condition that can cause an *element* or an *item* to fail

Note 1 to entry: *Permanent*, intermittent, and **transient faults** (especially soft -errors) are considered.
Note 2 to entry: When a subsystem is in an *error* state it could result in a fault for the *system*.
Note 3 to entry: An intermittent fault occurs from time to time and then disappears again. This type of fault can occur when a *component* is on the verge of breaking down or, for example, due to a glitch an internal malfunction in a switch. Some **systematic faults** (e.g. timing marginalities irregularities) could lead to intermittent faults.

• **safety measure** definition from ISO26262:2018 Part 1 Vocabulary
  activity or technical solution to **avoid or control systematic** failures and to **detect random hardware failures** or **control random hardware failures**, or **mitigate their harmful effects**

Note to entry: Safety measures include safety mechanisms.
Example : FMEA and software without the use of global variables, ECC, Parity
Example: ADAS Lane Departure Warning


- **Item**: Lane Departure Warning
- **Malfunction**: Lane departure warning is unavailable to notify driver of car drifting outside of lane
- **Hazard**: Car will stray from intended path

Malfunction / Hazard
Lane departure warning is unavailable to notify driver of car drifting outside of lane

Operational Domain
City Street (Exposure of E3)

Mitigation/failback
Driver maintains correct path (Controllability of C3)

Harm
Side collision with car (Severity of S2)

ISO 26262 Part 10 Clause 9 Safety Element out of Context

<table>
<thead>
<tr>
<th>Assumed Safety Goal</th>
<th>ASIL</th>
<th>Assumed Safe State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault on the inter processor communication shall be mitigated</td>
<td>B</td>
<td>Feature deactivated and driver warned</td>
</tr>
</tbody>
</table>
ISO 26262 Work Product Overview

- Item Definition
- Functional Safety Concept
- Safety Plan
- Technical Safety Concept
- Hardware Safety Requirement
- Software Safety Requirement

- Integration and Testing
- Failure Mode Effect Analyses (FMEA)
- Safety Manual
Systematic Faults

- Systematic faults can only be eliminated by a change of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.
- Examples of systematic faults include incorrect requirements,
  - **Work Product Related**
    - Item Definition
    - Safety Plan
    - Functional Safety Concept
    - Technical Safety Concept
    - Hardware Safety Requirement
    - Software Safety Requirement
    - Software Unit Testing
    - Verification of Software Requirements
    - Tool Classification and Qualification for Hardware and Software

What Types of Faults Does ISO Cover?

- Software Unit Testing
- Verification of Software Requirements
What Types of Faults Does ISO Cover?

Hardware Random Faults

• Related to faults of the hardware itself:
  • Permanent Fault examples: Stuck-at bit, over voltage condition
  • Transient Fault example: Soft error Rate due to radiation strike

• JESD89-2A TEST METHOD FOR ALPHA SOURCE ACCELERATED SOFT ERROR RATE
• JESD89-3A TEST METHOD FOR BEAM ACCELERATED SOFT ERROR RATE

<table>
<thead>
<tr>
<th></th>
<th>ASIL B</th>
<th>ASIL C</th>
<th>ASIL D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Point Fault metric (SPFM)</td>
<td>≥90%</td>
<td>≥97%</td>
<td>≥99%</td>
</tr>
<tr>
<td>Latent Fault Metric (LFM)</td>
<td>≥60%</td>
<td>≥80%</td>
<td>≥90%</td>
</tr>
<tr>
<td>Probabilistic metric for Random HW Failures (PMHF)</td>
<td>100 FIT</td>
<td>100 FIT</td>
<td>10 FIT</td>
</tr>
</tbody>
</table>
PCIe® Specification Safety Features

PCI EXPRESS® FOR AUTOMOTIVE FUNCTIONAL SAFETY (FUSA)

- PCIe technology use-cases and safety expectations
- Reliability, Availability, Serviceability (RAS) as FuSa enabler
### PCIe® Specification Safety Features

**PCIe use-cases and safety expectations**

**Application**
- Chip-to-Chip communication
- Compute scalability
- ADAS domain controllers

**Trend**
- Increase in compute processing
- High bandwidth
- Low latency requirement motivating native PCIe links

**Technology Requirements**
- Scalability
- High bandwidth & low latency
- Automotive functional safety

PCIe technology provides basic requirements inherently
Data Reliability already given by PCIe spec

End-to-End Data Integrity on Data Link Layer

- 32-bit CRC (LCRC) code to detect errors in TLPs on a Link-by-Link basis
- Applies a Link-by-Link retransmit mechanism for error recovery
- LCRC is regenerated by PCIe switches and increases the risk of data corruption

Enabling end-to-end data integrity detection by adding transaction Layer end-to-end 32-bit CRC (ECRC) can be placed in the TLP Digest field at the end of a TLP
PCIe® Specification Safety Features

**PCIe Advanced Error Reporting (AER) Capability**

- Optional feature that can be implemented by PCIe devices supporting advanced error control and reporting
- Error registers show the status of individual errors on a PCI Express device function and define the error severity, error logging, error mask ability and to identify the source of error
- AER provides the granularity and details of correctable and uncorrectable errors
- AER supports the safety goal to detect failures and then proceed to a safe state

*Advanced Error Reporting Extended Capability Header*

- Capability Version = 0x1 or 0x2
- PCI Express Extended Capability ID = 0x0001 for AER
Safety Goal
- Definition of safe state

Functional safety requirements derived from safety goal
- Avoid, detect, or control failure modes leading to incorrect data

PCIe® error logging and handling on a typical SoC

Avoid
- Data reliability trough ECRC and LCRC

Detect/control
- Advanced error reporting:
  - By completion status field: completer (EP or RC) reports errors to the requester (EP or RC)
  - By error message transactions: reporting errors to the host/RC.
PCIe® Technology and Additional Safety Mechanisms to meet ASIL B and Beyond

PCI EXPRESS® FOR AUTOMOTIVE FUNCTIONAL SAFETY (FUSA)

- Parity & ECC
- Flow Control
- Self-test
PCle® Technology and Additional Safety Mechanisms to Meet ASIL B and Beyond: Parity and ECC

- Safety Mechanisms to achieve ASIL B Random HW Fault metrics
  - Permanent and Transients faults
- Each Safety Mechanism has an associated Reaction Time: Fault Handling Time Interval and Error Flag

**User Interface**

- Parity Protection delivered & checked at user interface
- ECC for closely coupled SRAMs
- Parity Protection on internal data paths

**Parity Protection**
- Parity Protection on internal data paths
- Parity Protection for address ports

**Register Space Protection**
- User Interface: ECC added at data path ports

**Transaction**
- Parity added for address ports

**Data Link**

**Physical**

**RX TX**
PCIe® Technology and Additional Safety Mechanisms to Meet ASIL B and Beyond: Parity and ECC

Implement SoC Level Self-test e.g. LBIST

- Safety Manager monitors & manages all system failures & real-time faults; safe boot & mission-mode testing
- LBIST test all memory, logic & analog/mixed-signal circuitry
- Efficient management of critical security functions: secure boot, key management and cryptography
Managing SoC Level PCIe® FuSa

- PCIe application should monitor the safety interrupt outputs
  - Implement an application specific safe state transition scheme
- Respond to potential failure modes of the PCIe function
  - Based on each safety mechanism
  - Based on Safety Goal Violations
- Plan how the PCIe function responds to
  - Permanent HW faults e.g. perform reset
  - Transient faults: data correction or PCIe data replay
Summary

PCI Express® for Automotive Functional Safety (Fusa)

- PCIe Widely used in Safety Critical Automotive applications
- Compliance to ISO 26262 Functional Safety is required by automakers and Tier 1s
  - Development to identity/correct to Random HW Faults: Permanent & Transient
  - Development according to ISO 26262 ASIL Systematic
- PCIe Performance and scalability ideal for automotive SoCs & Systems
Q&A
Thank you for attending the second entry in the PCI-SIG® Automotive Webinar series.

Information about upcoming webinars will be available soon.

For more information, please visit www.pcisig.com