How MASS Embeds Functional Safety
Guided by the Requirements of ISO 26262

Licinio Sousa
Member of MIPI Camera and Display Working Groups
Synopsys
Trends & New Applications

Transition from Distributed ECUs to centralized Domain Compute Modules

New applications for ADAS, Infotainment, Connected Car & V2X

Growing number & types of Sensors: Imaging, Lidar, Radar, Infra-Red

System & SoC level Functional Safety and Reliably

Requires High Performance FinFET Class Automotive SoCs
MIPI in Automotive

Cameras, displays, audio, sensors, storage, RFFE for 5G, Wi-Fi, Bluetooth, NFC

Reuse & extend well-proven protocols == reduced NRE/cost
Intra-box usage has been limited due to lack of native long-reach PHY

SPECIFICATIONS IN AUTOMOTIVE TODAY

Most MIPI interfaces are implemented as "short reach" (~15 to ~30cm+)

CSI-2
Camera Serial Interface protocol
Protocol for cameras, lidar, radar sensors

DSI-2
Display Serial Interface protocol
Protocol for smartphone, IoT and automotive displays

C-PHY SerDes
3-phase physical layer for CSI-2 & DSI-2
Short-reach physical layer for cameras and displays

D-PHY SerDes
Differential physical layer for CSI-2 & DSI-2
Short-reach physical layer for cameras and displays

I3C
Control and data bus protocol and interface
Sensor and general-purpose data and control interface within a module

RFEE
RF control protocol
Front-end control within a wireless module

UniPro for JEDEC UFS
Data transport protocol for UFS over M-PHY
Transport protocol for UFS storage

M-PHY SerDes for JEDEC UFS
Differential physical layer for UFS storage
Short-reach physical transport for UFS storage

A-PHY SerDes
Long-reach (up to 15m) asymmetrical physical layer (released Sep 2020)
MIPI Automotive SerDes Solutions (MASS) in the Car

**Electronic Control Unit (ECU)**
- Advanced driver assistance system (ADAS) based on sensor feeds
- Produces display feeds

**Sensors Examples**
- Camera
- Lidar

**Display Examples**
- Dashboard
- Console
- Side view mirrors
- Entertainment

**A-PHY (Bridges)**
- Translates between short-range MIPI C-PHY / D-PHY & long-range MIPI A-PHY
Annex D – Communication bus safety mechanisms:

- One-bit hardware redundancy
- Multi-bit hardware redundancy
- Read back of sent message
- Complete hardware redundancy
- Inspection using test patterns
- Transmission redundancy
  - Information redundancy
  - Frame counter
  - Timeout monitoring
  - Combination of information redundancy, frame counter and timeout monitoring
Functional Safety – Service Extensions (CSE/DSE)

• Flexible End-to-End Functional Safety and Security framework with SEP
  – Packet based: per SEP
  – Frame based: per Video Frame
  – Regions of Interest: per ROI
  – With compression enabled/disabled

• Example of FuSa Elements used
  – CRCs with Hamming distance > 3 - detecting communication failure (bad payload)
    • SEP Header CRC + SEP Footer CRC
    • ROIs, Compression Slices / Columns etc.
  – Message Sequence Counter – detecting packet loss / duplication
  – Timeout Monitoring – detecting potential loss of communication
  – Test pattern generators (solid colors, color bar, tiles etc.)
  – Faults injection – checking error detection mechanisms
MIPI CSI-2 Protocol with CSE

Figure 1 Layer Definitions for CSE Over A-PHY

Figure 2 Layer Definitions for CSE Over C/D-PHY
Developing Systems & SoCs Meeting Automotive Requirements

Reduce Risk and Accelerate Qualification

- **Temperature**
- **Lifetime**
- **Failure rate**

- **Functional Safety**: Accelerate ISO 26262 functional safety assessments to help ensure designers reach target ASIL levels
- **Reliability**: Reduce risk & development time for AEC-Q100 qualification of SoCs
- **Quality**: Meet quality levels required for automotive applications
Development Flows for ISO 26262 Functional Safety

Activities & Work Products for Automotive SoCs & IP

- Core Architecture
- ISO 26262 Safety Plan
- HW Safety Requirements
- HW Safety Goals
- FIT Rate Analysis
- HW Safety Features
- Consumer Flow
- +Automotive

- Core Spec
- FPGA
- Safety Manual
- Validation
- ASIC
- Digital Spec
- FMEDA Report
- IP/SoC Level Verification
- RTL Design
- Fault Injection / Coverage Analysis
- Module Design Verification
- Design Implementation
Automotive IP with FuSa Functionality

Synopsys Adds Specific Safety Mechanisms Functionality to DesignWare Automotive IP

Protection
- User interface protection
- Buffer point protection
- Error detection codes
- Parity protection data
- Parity protection on configuration registers
- Memory protection
- Bad state protection/prevention

Redundancy
- Duplicate key modules
- Triplicate key modules

More…
- Register concatenation
- Validity checking in key modules
- Dedicated interrupts for error reporting
- Processor Dual Core Lockstep support
- Processor user programmable watchdog timer

Note: Specific IP implements different range of safety features

Automotive Safety Integrity Level (ASIL)

Evolving ASIL Requirements
Additional Safety Mechanisms to Meet ASIL B & Beyond

Example of an Automotive-Grade MIPI CSI-2 IP

- Parity Protection delivered & checked at user interface
- Parity Protection on internal data paths
- ECC for closely coupled SRAMs
- User Interface: ECC added at data path ports, Parity added for address ports
- Register Space Protection
- Module Redundancy Protection for critical logic

- CSI-2 best-in-class example
- Safety Mechanisms to achieve ASIL B Random HW Fault metrics
- Each Safety Mechanism has an associated Reaction Time: Fault Handling Time Interval and Error Flag

Example of an Automotive-Grade MIPI CSI-2 IP
Safety Manager for SoC-Level Integration

Monitoring and Managing Functional Safety Capabilities

- Safety Manager monitors and manages all system failures and real-time faults; safe boot and mission-mode testing
Need to Design for Reliability

Handling the Stringent Operating Conditions

- Environmental
- Temperature
- Noise
- Vibration
- Long term operation
- Field rate (targeting 0%)

### AEC-Q100 Qualification

**Accelerated Lifetime Simulation Tests**
- HTOL
- ELFR
- ESD HBM
- ESD CDM
- IC Latch Up

**Electrical Verification Tests**
- E D
- CHAR

### SoC/IP Testchip

**Design**
- AUTO DRC/PDK
- Design Rules
- Mission Profile

**Testing**
- HTOL
- ELFR
- ESD
- CDM
- IC
- Latch Up

**Report**

### Grade

<table>
<thead>
<tr>
<th>Grade</th>
<th>Ambient Operating Temperature Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>-40°C to +150°C</td>
</tr>
<tr>
<td>1</td>
<td>-40°C to +125°C</td>
</tr>
<tr>
<td>2</td>
<td>-40°C to +105°C</td>
</tr>
<tr>
<td>3</td>
<td>-40°C to +85°C</td>
</tr>
</tbody>
</table>

### Operation time [h]

- Early life
- Useful life
- Wear out

### AEC-Q100 Standard

- Sample size
- Type of Test
- Test time
- Conditions
Need for a Comprehensive Automotive-Grade MIPI IP

MIPI Automotive-Grade IP Package
22nm - 16nm - 7nm - 5nm

Safety
- SAFETY MANUAL
- FMEDA
- FuSa CERTIFICATE
- RANDOM
- SYSTEMATIC
- WORK PRODUCTS

Reliability
- MISSION PROFILE
- AUTO PDK/RULES
- GRADE 2/1
- AEC-Q100 REPORT

Quality
- ISO 9001 QUALITY MANAGEMENT SYSTEM
- QUALITY MANUAL

Automotive SoC
22nm - 16nm - 7nm - 5nm
MIPI Automotive Workshop

An in-depth look at the MIPI Automotive SerDes Solutions (MASS) framework

Q&A