Latest Developments within MIPI Automotive SerDes Solutions (MASS)
Industry Trends Advancing Automotive Functional Safety and Security

Figure 1 Automotive industry trends defined as “CASE”. (Source: MIPI Alliance)
MASS Functional Safety Application

Digital Side Mirror Replacement
Sensor and display endpoints with integrated long-reach connectivity (integrated A-PHY℠ SerDes) connect to the ECU without intermediate bridges. Application-level functional safety and security data protection. HDCP for protecting premium content.
ISO26262 Part 5: Product development at the Hardware Level

• ISO26262 automotive functional safety standard
  – Reference for automotive safety lifecycle
  – Automotive-specific risk-based analysis for Automotive Safety Integrity Levels (ASILs)
  – Uses ASILs to specific applicable requirements

• Part 5: Hardware level
  – Specification of hardware safety requirements
  – Evaluation of safety goal violations due to random failures
  – Annex D: informative guidelines for appropriate safety mechanisms
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
Adding Service Extensions Packets (SEPs)

MIPI DSE℠ v1.0, MIPI PAL℠/DSI-2℠ v1.0

Figure 23 SEP Formatting in the Display Source
C.1 Converting DSI-2 Long and Short Packets to SEP

Figure 20 illustrates conversion from a DSI-2 Long Packet to SEP carried within DSI-2 Long Packet.

Figure 20 Converting DSI-2 Long Packet to SEP Within DSI-2 Long Packet

Figure 21 illustrates conversion from a DSI-2 Short Packet to SEP carried within DSI-2 Long Packet.

Figure 21 Converting DSI-2 Short Packet to SEP Within DSI-2 Long Packet

MIPI DSE℠ v1.0, MIPI PAL℠/DSI-2℠ v1.0
**MASS Display Services Extension (DSE 1.0)**

**Services Extensions Protocol (SEP) Header and Footer**

- **eDT** – extended Data Type
  - CSI, DSI
  - VESA eDP/DP
- **Message Counter**
- **CRC-32**
  - Hamming distance of 3 or more

---

### Table 1 SEP Packet ePH Blocks: Overview

| Bits  | 31 | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|-------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| ePH[0]| R  | eVC| eDT| R  | ePFEN| Reserved| ePHEN|       |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| ePH[1]|     |     | Reserved|     |     |     | SEP Payload Length|     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| ePH[2]|     | Service Descriptor| Reserved|     |     |     | Message Counter|     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| ePH[3]|     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| ePH[4]|     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| ePH[5]|     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| ePH[6]|     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| ePH[7]|     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |

### Table 2 SEP Packet ePF Blocks: Overview

| Bits  | 31 | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|-------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| ePF[1]|     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| ePF[0]|     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |

**CRC-32**

---

MIPI DSE℠ v1.0
Incorporating Solutions for Data Protection

Bridge-to-Bridge Data Protection

End-to-End Data Protection (Integrated SerDes)
Detailed Display Protocol Stack

ECU Display Source
- ECU Pixel Frame Buffer
  - Generate SEP Packet Payload (Optional HDCP)
    - Generate SEP Header and Footer
      - Generate DSI-2 Long/Short Packet
        - Lane Management
          - C/D-PHY Tx

Display Sink
- DSI-2 Display Controller
  - Unpack SEP Packet Payload (Optional HDCP)
    - Unpack SEP from DSI-2 Payload
      - Parse DSI-2 Long/Short Packet
        - Lane Management
          - C/D-PHY Rx

A-PHY Bridge
- C/D-PHY Rx
  - Lane Management
    - DSIA-SRC
      - A-PHY Source

A-PHY Bridge
- C/D-PHY Tx
  - Lane Management
    - DSIA-SNK
      - A-PHY Sink

Asymmetric Bi-Direction High Speed Data
ECU Display Source and Sink

**ECU Display Source**
- ECU Pixel Frame Buffer
  - Pixels
  - Control
  - Generate SEP Packet Payload (Optional HDCP)
    - Data
    - Control
    - Lane Management
    - C-/D-PHY Tx

**Displays Sink**
- DSI-2 Display Controller
  - Data
  - Control
  - Unpack SEP Packet Payload (Optional HDCP)
    - Data
    - Control
    - Lane Management
    - C-/D-PHY Rx
- DSI-2 Display Controller
  - Data
  - Control
  - Unpack SEP Packet from DSI-2 Payload
    - Data
    - Control
    - Lane Management
    - C-/D-PHY Rx

---

DSI-2℠ v2.0, DCS℠ v1.5, DSE℠ v1.0, MIPI PAL℠/DSI-2℠ v1.0, C-PHY/D-PHY℠

Previous versions of existing specifications are also compatible with MASS.
Detailed A-PHY Bridge PAL

MIPI A-PHY℠ v1.0, PAL℠/DSI-2℠ v1.0, C-PHY℠/D-PHY℠
MASS Legacy ECUs with an External A-PHY Bridge

ECU MIPI Display Source

- **DSI-2 Display Source (Pixels)**
  - Display Pixel Data Path
  - Display Command and Control
- **Pixel to Byte Packing**
- **DSI-2 Protocol**
- **Lane Management**
- **Transmitter C-PHY or D-PHY Tx**

MIPI DSI-2 Receiver to A-PHY Transmitter Bridge

- **Receiver C-PHY or D-PHY**
- **Lane Management**
- **DSI-2 Protocol Adaptation Layer with DSE 1.0**
- **A-PHY Data Link Layer**
- **A-PHY Physical Layer Transmit**

ECU VESA Display Source

- **VESA Display Source (Pixels)**
  - Display Pixel Data Path
  - Display Command and Control
- **VESA eDP/DP Protocol**
- **Lane Management**
- **VESA Transmitter eDP/DP PHY Tx**

VESA Receiver to A-PHY Transmitter Bridge

- **VESA Receiver eDP/DP PHY Tx**
- **Lane Management**
- **VESA eDP/DP Protocol Adaptation Layer with DSE 1.0**
- **A-PHY Data Link Layer**
- **A-PHY Physical Layer Transmit**

Display Command and Control

Display Pixel Data Path

Display Command Services DCS

DSI-2

VESA eDP/DP Protocol

Lane Management

Transmitter

C-PHY or D-PHY Tx

DSI-2 Protocol Adaptation Layer with DSE 1.0

A-PHY Data Link Layer

A-PHY Physical Layer Transmit

Display Pixel Data Path

Display Command and Control

Display Command Services DCS

DSI-2

VESA eDP/DP Protocol

Lane Management

Transmitter

eDP/DP PHY Tx

DSI-2 Protocol Adaptation Layer with DSE 1.0

A-PHY Data Link Layer

A-PHY Physical Layer Transmit
MASS New ECU with Integrated A-PHY

**ECU DSI-2 Display Source with integrated A-PHY**

- DSI-2 Display Source (Pixels)
- Display Command and Control
- Display Pixel Data Path

**DSI-2 Protocol Adaptation Layer with DSE 1.0**

- Pixel to Byte Packing
- Display Command Services Command Bytes

**A-PHY Data Link Layer**

**A-PHY Physical Layer Transmit**

**DSI-2 Display Sink with Integrated A-PHY**

- A-PHY Physical Layer Receiver
- Lane Management
- DSI-2 Protocol Adaptation Layer with DSE 1.0

**Display**

**ECU VESA Display Source with integrated A-PHY**

- VESA Display Source (Pixels)
- Display Command and Control
- Display Pixel Data Path

**VESA eDP/DP Protocol Adaptation Layer with DSE 1.0**

- A-PHY Data Link Layer
- A-PHY Physical Layer Transmit

**VESA Display Sink with Integrated A-PHY**

- A-PHY Physical Layer Receiver
- Lane Management
- VESA eDP/DP Protocol Adaptation Layer with DSE 1.0

**Display**
Security within the MASS Guiding Principles

• MASS Guiding Principles
  – The Extent
  – The Protocols (CSI-2\textsuperscript{SM}, DSI-2\textsuperscript{SM})
  – The PHY (A-PHY\textsuperscript{SM})

• MIPI Security is implemented as extensions to CSI-2 and DSI-2 protocols.

• This enables the Security to achieve an “end-to-end” extent, or reach.
MASS Collection of Specifications

Updated Command Set for automotive control
Protocol extensions for safety & security
Updated mobile protocols
Adaptation layers to the new PHY
The new PHY ("Digital PHY")

Primary current developments:
- MIPI CSE™, MIPI DSE™ specifications add security with target completion mid-2022.
High-Level System and Security Requirements

- Security includes:
  - Device authentication, message integrity, confidentiality (encryption).
- We refer to data protections according to the MIPI 1:5 Model shown below (more on next page).
- Security is managed by the Controller engaging with each Component 1:1, this is not a “peer-to-peer” model of security (n-to-m)
- For example:
  - Display security may be initiated from #1 or #2 and terminated in #4 or #5.
  - Camera security may be initiated from #5 or #4 and terminated in #2 or #1.
MASS System Model: The 1:5 Model

Security Model Components
- #1: Controller (SoC)
- #2: Controller Bridge (C.Bridge)
- #3: Forwarding Element (aka Repeater)
- #4: Target Bridge (T.Bridge)
- #5: Target (Camera or Display)

Security Requirements
- Device Mutual Authentication (SoC as Root-of-trust)
- Message Integrity (MAC)
- Confidentiality (encryption)

System Requirements (End-to-end)
- Multiple system topologies (e.g., 15, 1245, 145, 125)
- End-to-end extent via protocol extensions
- Security for Data plane, and Control plane in-band/sideband
- Highly flexible operation, such as Heterogenous operation for displays, supporting DSI-2 and DP on a daisy chain.
MIPI Security Framework

C-Level provisions authentication credentials (an Integrator function)

B-Level (SSMC, System Security Management Controller) manages the capabilities, algorithms, and session keys.

A-Level executes the data protection under control of the B-Level.
  - SEP provides in-band data plane security
  - CCI and A-PHY security are also provided.
MIPI Security leverages DMTF.org SPDM Spec

SPDM: Security Protocol & Data Model

- DMTF now used within multiple Org specs
  - PCI-SIG, CXL, NVMe, and MIPI

- SPDM – Modeled after TLS.
  - Fundamentally used to establish authenticated session keys
    - **KEY_EXCHANGE** flow: based on certificates and/or raw public keys
    - **PSK_EXCHANGE** flow: based on PSKs, no DHE, constrained devices
  - Session-key keys can then be used to secure data.

- SPDM messages are carried across DSI-2, CSI-2 and CCI (I2C) to protect each transport individually.
MIPI SEP Format (Service Extensions Packet)

SEP Format consists of a SEP Header and SEP Footer that encapsulate the payload, where:

- Header identifies all security controls
- Footer includes the MAC (and CRC for functional safety).
- The payload nominally consists of a single CSI-2/DSI-2 packet and may be transmitted immediately.

**SEP Data Protection**

- Encryption provides payload confidentiality
- Integrity check provides message confidentiality
- Confidentiality, Authentication
- Confidentiality, Integrity, Authentication
- Message Counter prevents against replay attacks; CRC provides FuSa message integrity check
MIPI leverages TLS security principals and places the MIPI Service extensions at the application layer source/sink.

- Essentially as “end-to-end” as possible, from the pixel-source to the pixel-sink.
Summary

• The MASS specifications provide functional safety solutions for automotive cameras and displays within the first versions of MIPI CSE and DSE.
  – These specifications are complete and available to MIPI members.
• The CSE v1.0 and DSE v1.0 specifications are being updated to support security (device authentication, message integrity and optional encryption) over MIPI CSI-2, DSI-2 and CCI (I2C) sideband.
• Placement of security in the CSI-2/DSI-2 protocols allows end-to-end data protection with or without intermediate bridges.
  – This allows application layer security like TLS, contrasted to link layer security like MACsec.
THANK YOU!