IF IT'S NOT MIPI, IT'S NOT MOBILE

2021 MIPI Automotive Workshop:

How the MIPI Security Framework Protects Automotive SerDes Applications from Security Risks

Rick Wietfeldt, Philip Hawkes
Security WG Co-Chairs

Overview

- Introduction to MIPI Security
- Key System and Security Requirements
- Solution Details
- Summary

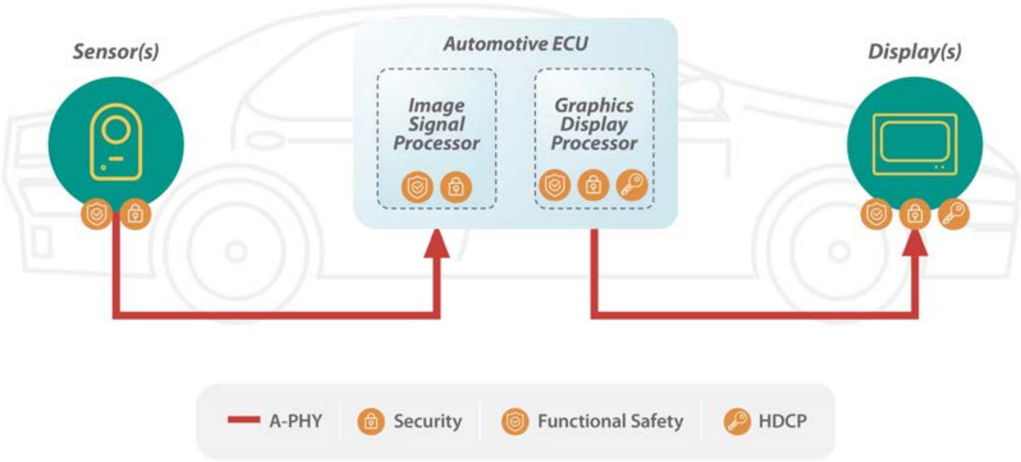
Introduction to MIPI Security

MIPI Security in Automotive

Goal: To “secure” from end to end the application connections between components:

- SoCs (ECUs)
- Sensors, Displays
- Optional Bridges (convert C-/D-PHY to A-PHY)

MIPI CSI-2
Camera
Radar
Lidar



MIPI DSI/DSI-2
VESA eDP/DP

Let's Define Security

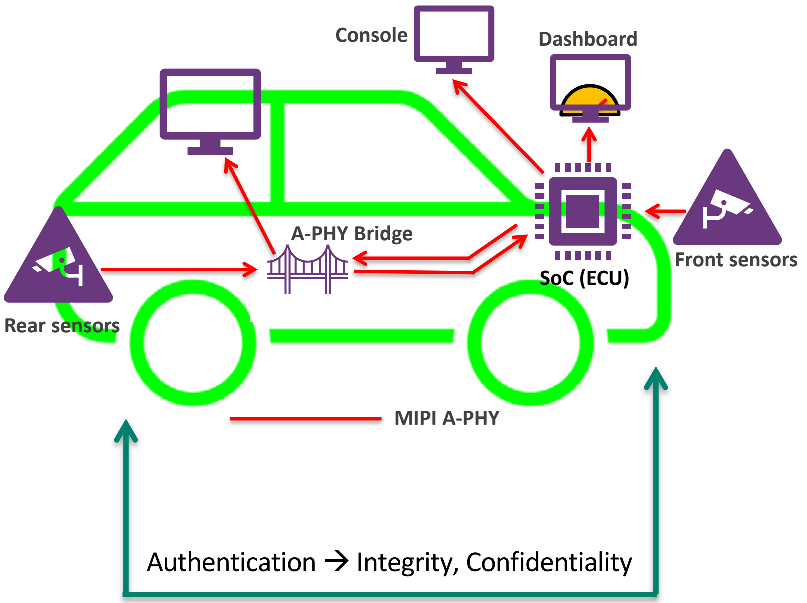
Two steps (well-known in security):

1 **Authentication** to establish trust between components
- Mutual authentication is often desired

2 Once trust is established, then address the following for both data plane and control planes…

Integrity (required)
- Ensures data is unaltered to/from the ECU
- Provided by Message Authentication Code (MAC)

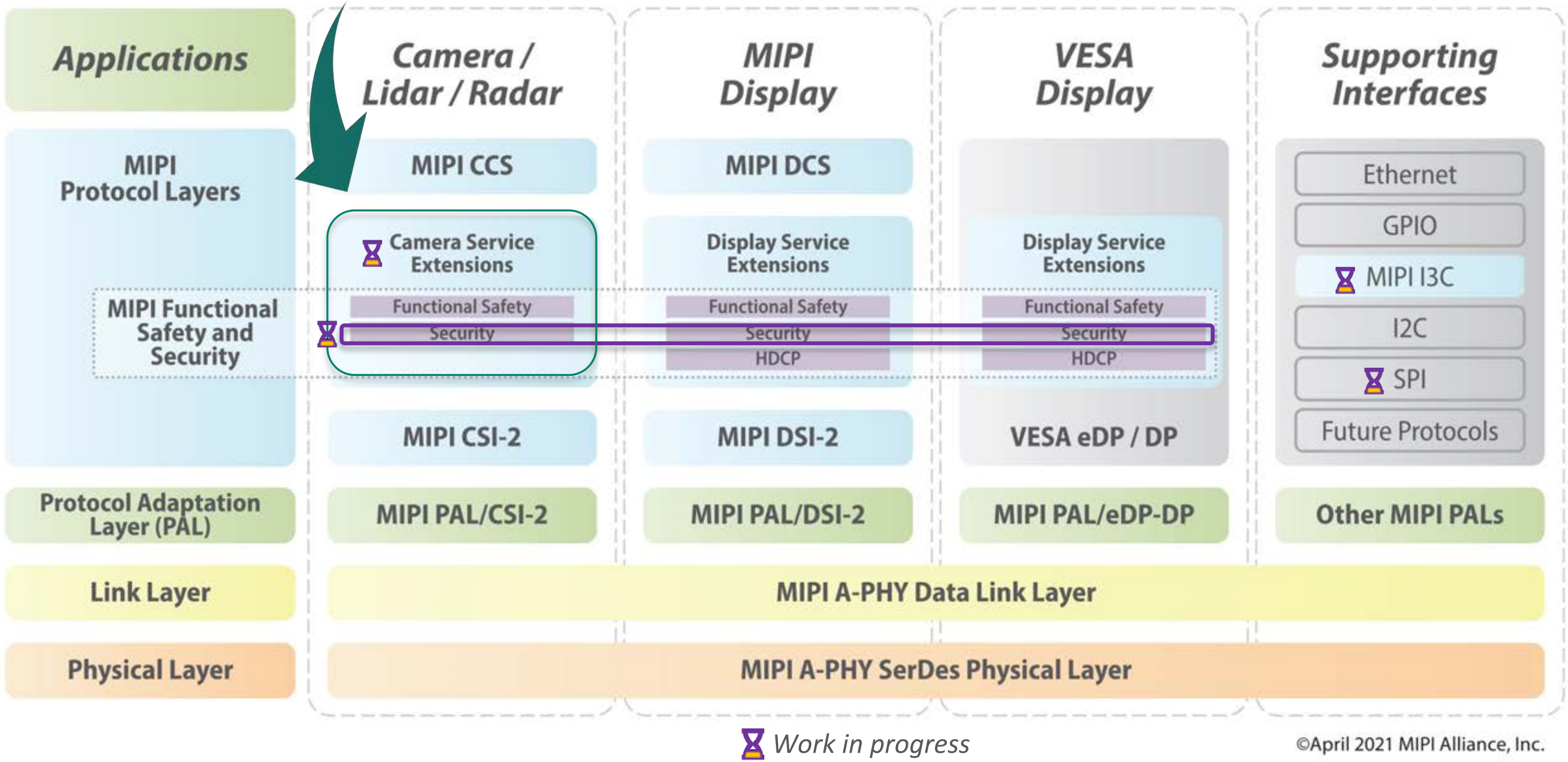
Confidentiality (optional)
- Protects sensor data against unauthorized access
- Provided by message encryption



MIPI is addressing security from the application layer and not just the link layer

Security in the MASS Framework

Service extensions add functional safety and security to the application protocols. FuSa is complete, and **security will start with CSI-2 via updated Camera Service Extensions + MIPI Security Specification**.



Key System and Security Requirements (Sensor Focus)

 |

Key System Security Requirements

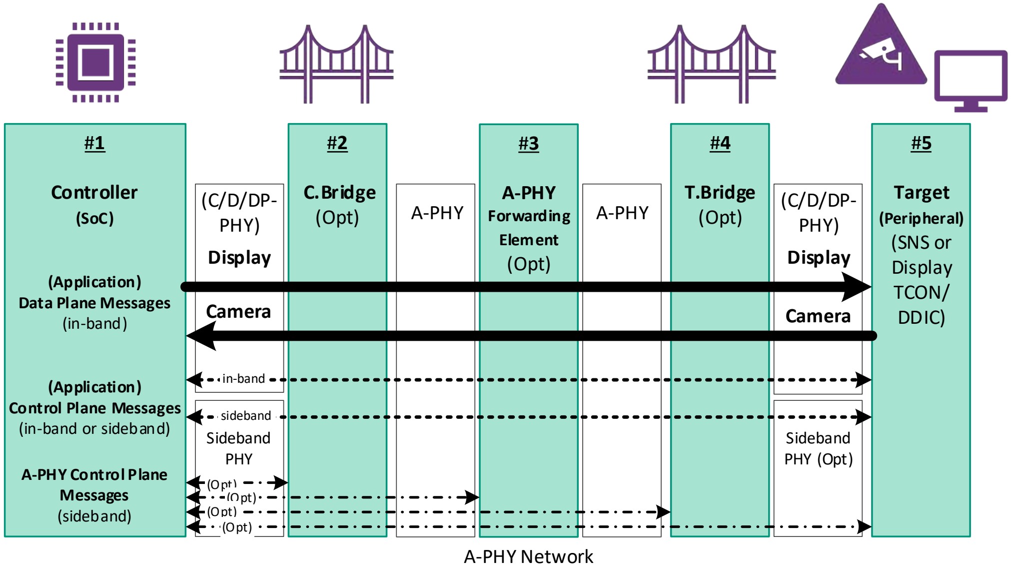
End-to-end considerations from sensor to SoC:

- **Flexible topologies:**
  - Unicast, multicast, multi-sensor, multi-SoC, aggregation/disaggregation
  - With and without bridge chips
- **Flexible endpoint interfaces/features** in the ecosystem:
  - C-/D-PHY flexibility
    (e.g., sensor interface to its bridge may be 1-trio C-PHY, whereas the SoC bridge interface to the SoC may be 2-lane D-PHY)
  - I2C and/or I3C flexibility; even SPI, Ethernet

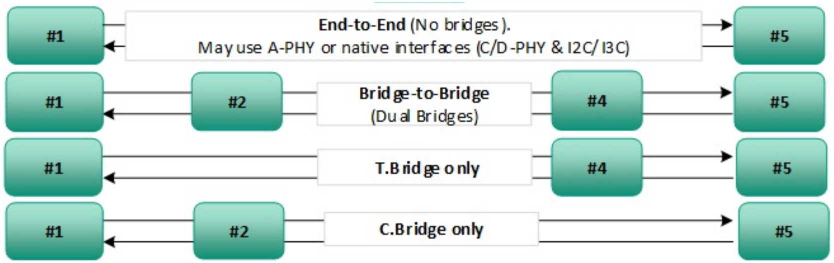
Security must be "application-based:"

- **"Highly granular" sensor security options** to support system performance/cost tradeoffs
  - Per eVC (virtual channel) security controls:
    - Per-pixel, per-message, per-frame, full and partial integrity
  - Algorithm options suitable for higher/lower tier sensors
- End-to-end security from **pixel source to pixel sink at the CSI-2 layer or above**

MASS 1-5 Model



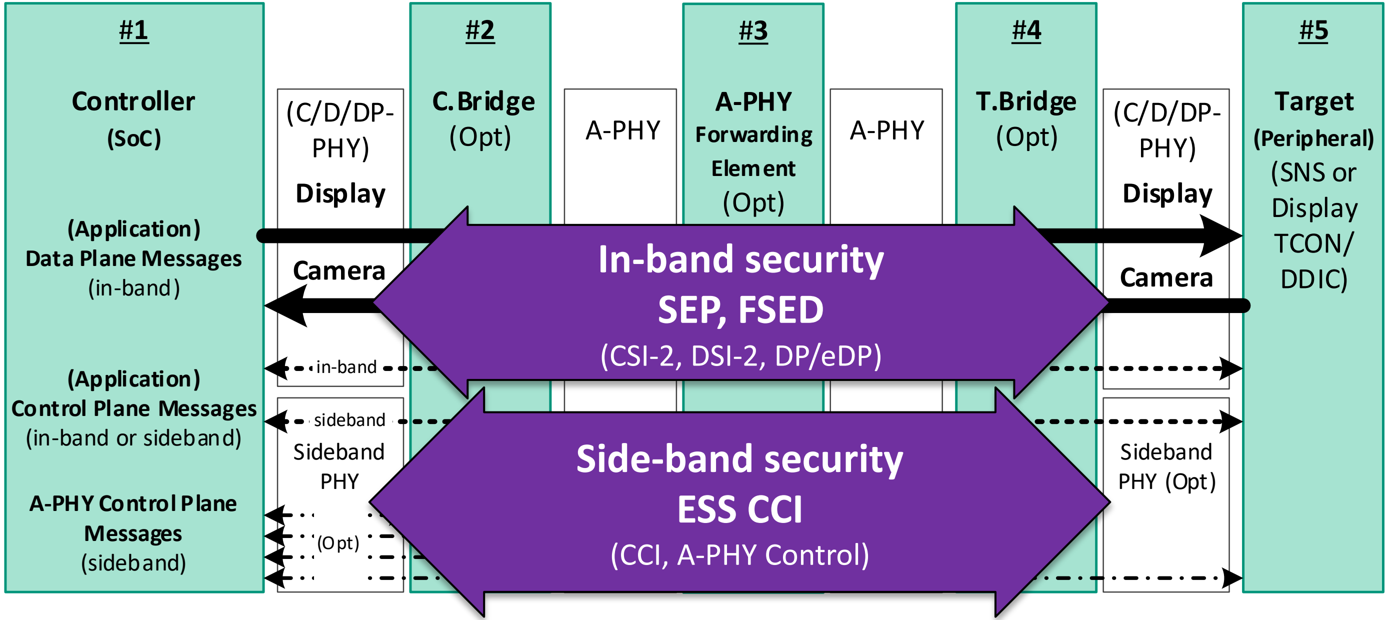
Support any combination of solutions with and without bridges.



mipi alliance

System & Security Details

Data Security Services: SEP, FSED, ESS CCI

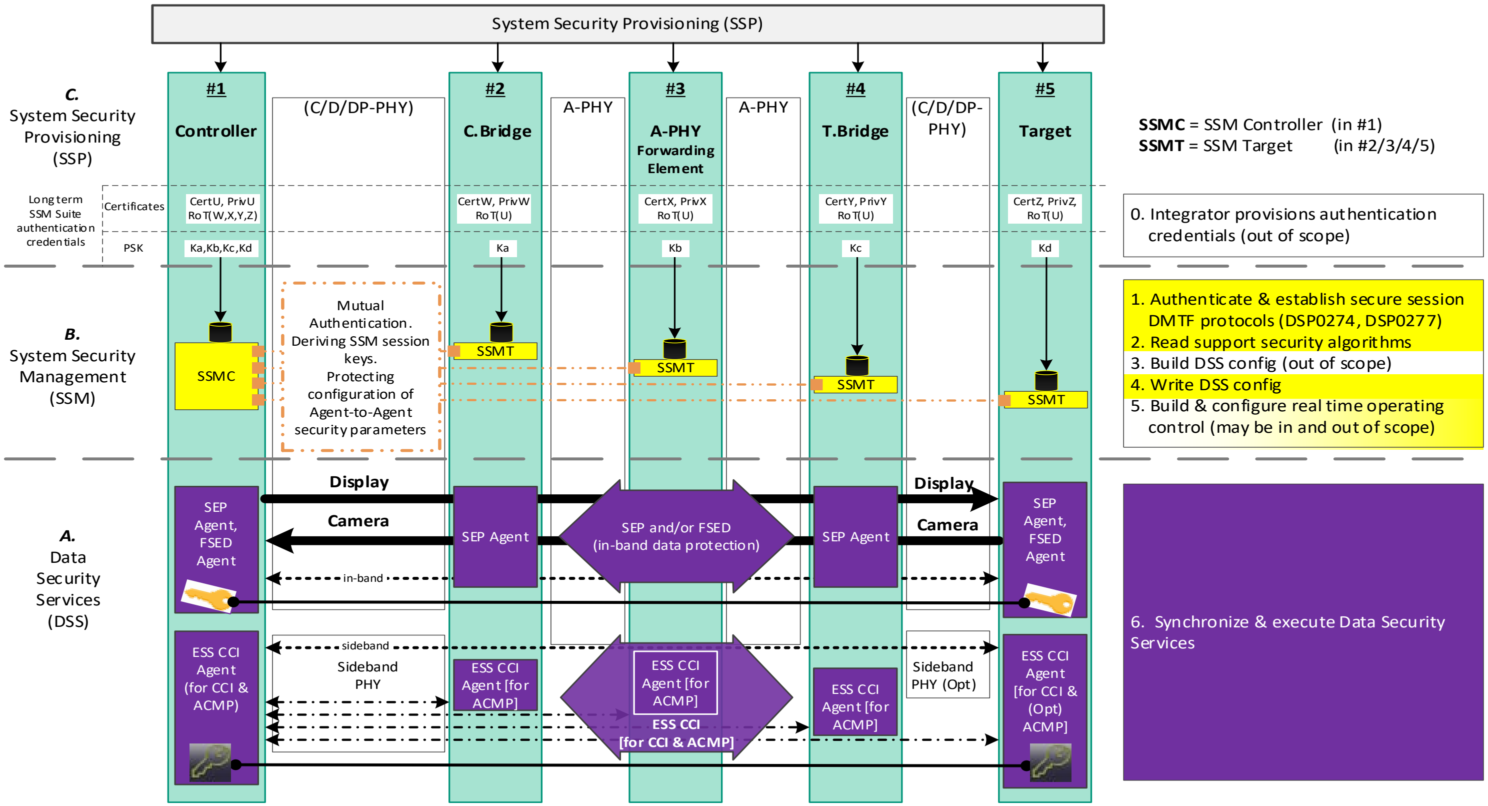


SEP: Service Extensions Packet
Message-based (i.e., protects *messages*)
End-to-end (1-5) or link-based

FSED: Frame-Based Service Extensions Data
Pixels-based (i.e., protects *individual pixels*)
End-to-end (1-5)

ESS CCI: Enhanced Safety & Security CCI
Transaction-based (i.e., protects *I2C transactions*)
End-to-end (1-5)

MIPI Security Framework: 1-5/ABC/0-6

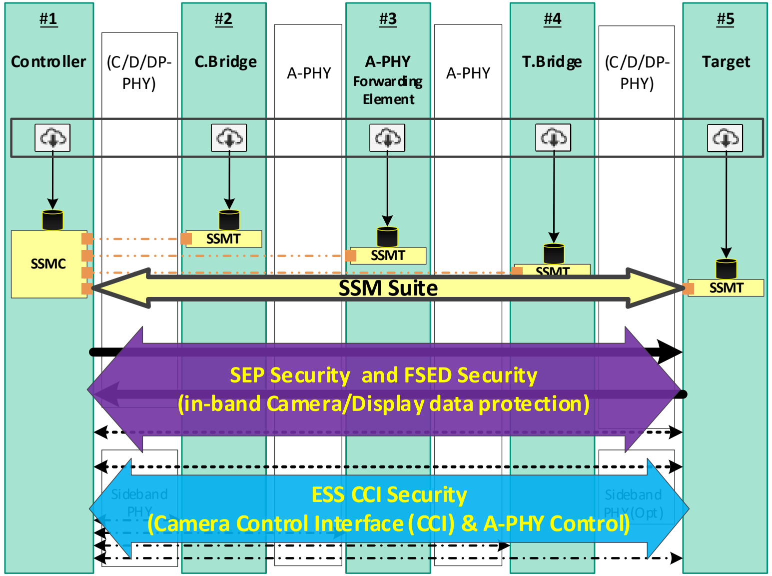


Note the end-to-end security extent from Controller (#1) to Sensor (#5)

System Security Management (SSM) Suite

Set of protocols that establish secure connections between components

- Controller-driven communications to each component (reminiscent of a mobile architecture)
- **DMTF SPDM** performs symmetric/asymmetric mutual authentication to establish the "secure session" with each component ("VPN")
- **DMTF Secured Messages** protects the MIPI SACP protocol (integrity, encryption)
- **MIPI SACP:**
  - Reads security capability registers for data security services
  - Writes security SA registers for data Security Services ("the keys" – "the security service association")
- **SSM Suite** defined in MIPI Security Specification

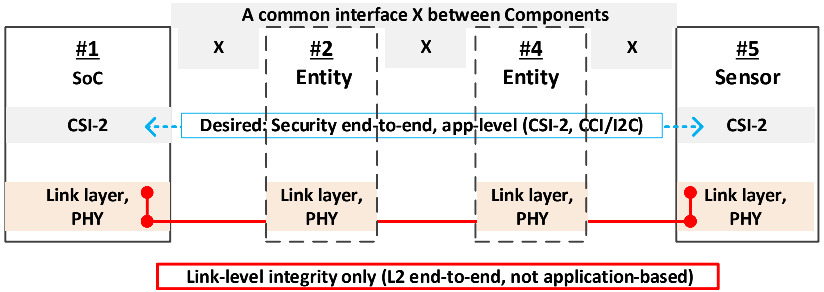


KEY:
DMTF: Distributed Management Task Force
SPDM: Security Protocol and Data Model (DMTF protocol)
SACP: Service Association Configuration Protocol (MIPI security protocol)

mipi alliance

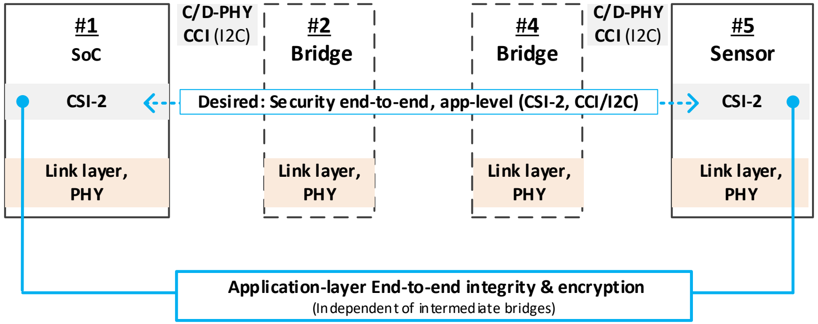
Security Coverage: Link vs. Application-Based

Link-Based (L2) End to End



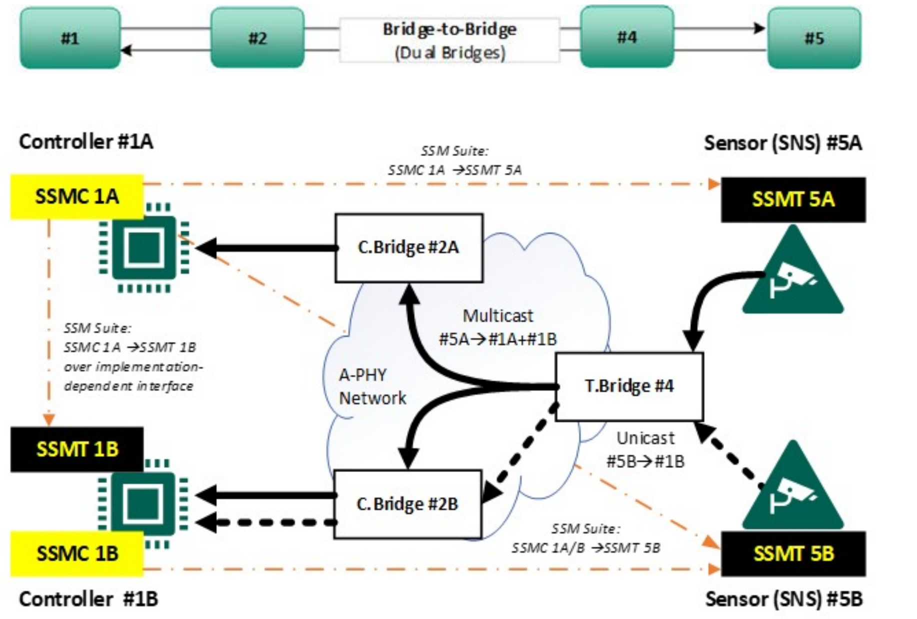
- Per link or end-to-end-based security (integrity & encryption) but at link level only
- Needs a separate security function at a higher layer (e.g., TLS over IPsec/MACsec) if application security is desired

Application (L7) End to End



- End-to-end-based security (integrity & encryption) at application layer (also provides "link protection")

Topologies: Multi-cast, Multi-controller



Two controllers: #1A, #1B.

Two sensors: #5A, #5B.

Controller #1B is an SSMT configured by the SSMC on Controller #1A.

Sensor #5A data is multicast to Controller #1A and Controller #1B.

The Security Service for this multicast is managed by SSMC 1A in Controller #1A, which configures the Data Security in Sensor #5A via SSMT 5A and configures the Data Security in Controller #1B via SSMT 1B.

KEY:

SSMC: System Security Management *Controller* (SPDM Requester)
SSMT: System Security Management *Target* (SPDM Responder)
- - - - - SSM Suite (DMTF and MIPI protocols)

mipi alliance

 |

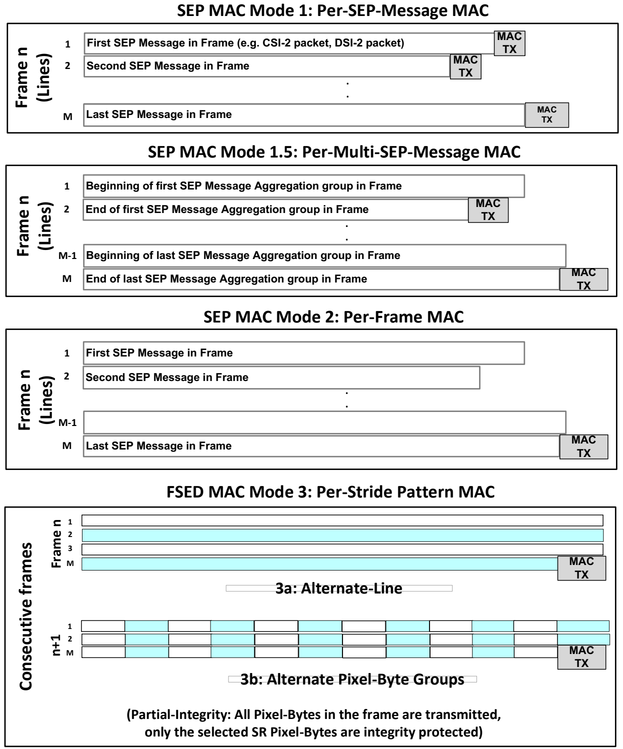
Complexity & Cost Scalability (Sensor MAC Modes)

A key part of scalability is to reduce MAC computations for lower tier sensors/controllers

Higher performance use case (e.g., AES-GCM)

Lower complexity/cost sensors

Lower performance use case (e.g., AES-CMAC, AES-CTR)



A single MAC is computed in the Sensor for each SEP Message (shown as 1 Message per Line).
MAC transmitted after each SEP Message.

Repeat for all SEP Messages in Frame.

A single MAC is accumulated in the Sensor over multiple SEP Messages.
Each MAC may be transmitted after each Multi-Message group.

Repeat for all SEP Message groups in Frame.

A single MAC is accumulated in the Sensor over an entire frame of SEP Messages.

MAC may be transmitted at end of Frame.

A single MAC is accumulated in the Sensor over the Stride Pattern Pixel-Bytes within a Frame (shown shaded).

One Stride Pattern per Frame.
Stride Pattern may change each Frame.

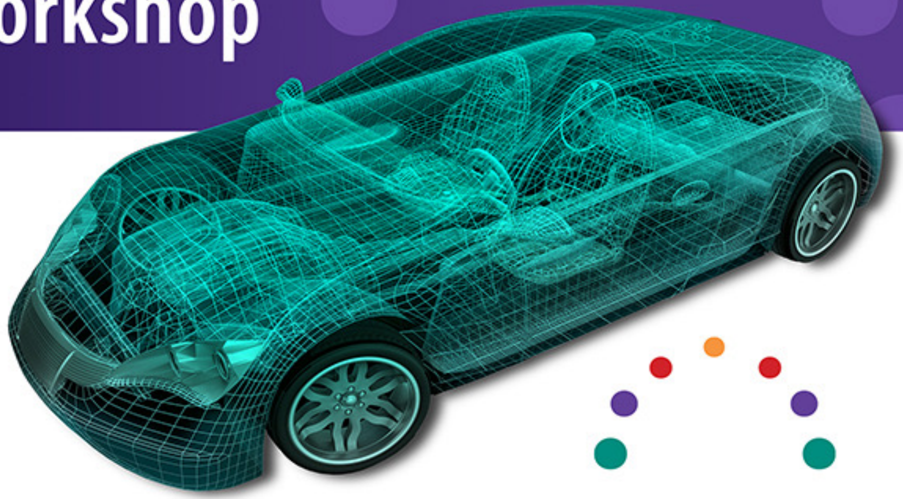
The Stride Pattern MAC per Frame is transmitted at end of each Frame (in CSI-2 format packet).

Summary

- MIPI is developing **an industry standard to protect automotive sensor/CSI-2 and display/DSI-2 data streams**. MIPI is also liaising with VESA to develop comparable MASS security for DisplayPort.
- MIPI CSI-2 security for ADAS provides a system-level solution – it provides application-based and end-to-end security.
  - MACsec (link-based) is well-understood, but application-level security is desired. To do this, an additional security protocol "beyond the link" (MIPI Security) is required.
  - MIPI defines highly granular sensor security controls at the application/system level.
  - All sensor/SoC communications are protected at this higher layer… across all intermediate components.
- MIPI Security is initially targeted for automotive, but it is **applicable for any CSI-2 application**.
- The **MIPI Security** (v1.0) and **CSE** (v2.0) specifications are targeted for **3Q 2022**.
- **Feedback from automotive Tier 1s and OEMs on the security specification is welcomed**. Contact admin@mipi.org for more information.
- Stay tuned for a **MIPI Security Workshop** to be held in early 2022.

MIPI Automotive Workshop

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



Q&A