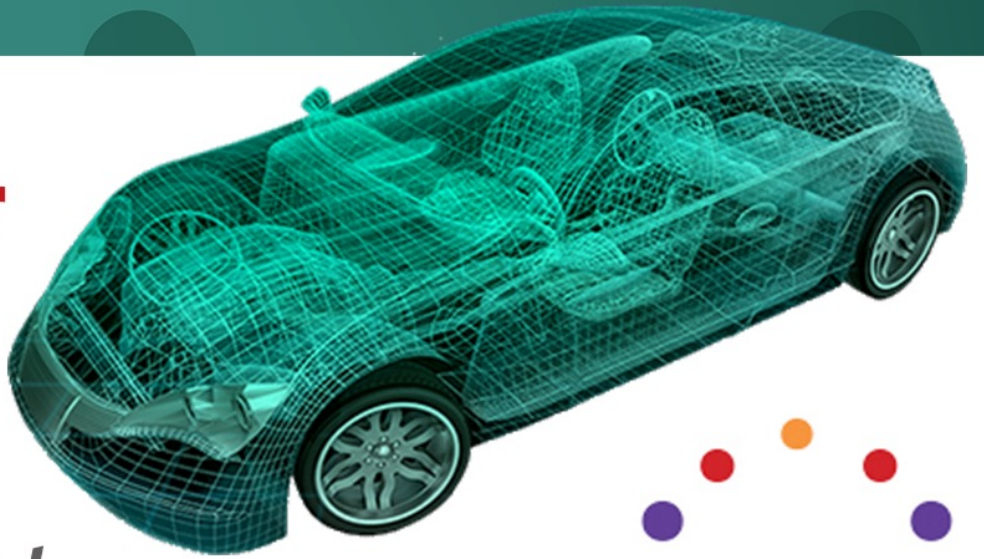
MIPI Automotive Workshop

15 November 2022



Live Virtual Event

mipi alliance

mipi alliance

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

MIPI CSI-2® Security Framework: A New Approach for End-to-End Protection of Camera Data Streams

Rick Wietfeldt & Phil Hawkes, Qualcomm Inc.
MIPI Security Working Group Co-Chairs

15 November 2022

Overview

- MIPI Alliance is developing an industry security framework to protect MIPI CSI-2-based sensor data for ADAS/AD applications.
- We refer to the Security framework as *Source-selective Partial-integrity and Encryption (SSPIE)* to capture its key attributes of operating at the application layer (source-selective), offering flexible security levels (including partial integrity) and optional encryption.
- Specifications are targeting 1Q 2023 for MIPI member review.

Agenda

- MIPI Security Introduction
- Security Extent: End-to-end, Application-based
- Service Layering (Security, FuSa)
- Security Flexibility
- Summary

MIPI Security Introduction

MIPI Automotive Security Goals

Considerable (1-10s Gbps) sensor data volume from multiple (10-30) sensors over long distances (1-10-15m)

Multiple sensor technologies (camera, lidar, radar) including for ADAS/AD

Authentication (required)

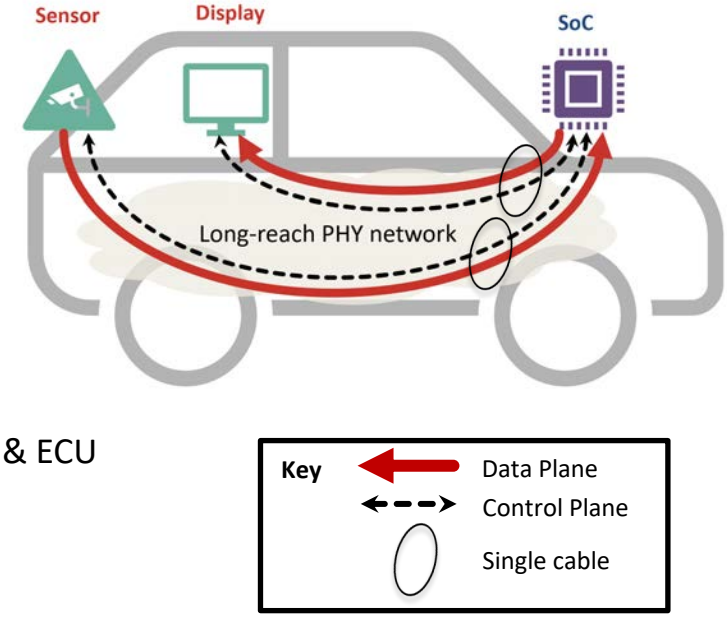
- Establishes trust between Sensor & ECU **1-way** ("ECU validates the Sensor") or **2-way/Mutual** authentication (both)
  - *Security consideration*: Legitimate components are installed to verify authenticity and performance

Integrity (required)

- Ensures sensor data/control is unaltered between Sensor & ECU
  - *Security consideration*: Manipulating sensor ADAS data
- Provided by Message Authentication Code (MAC)

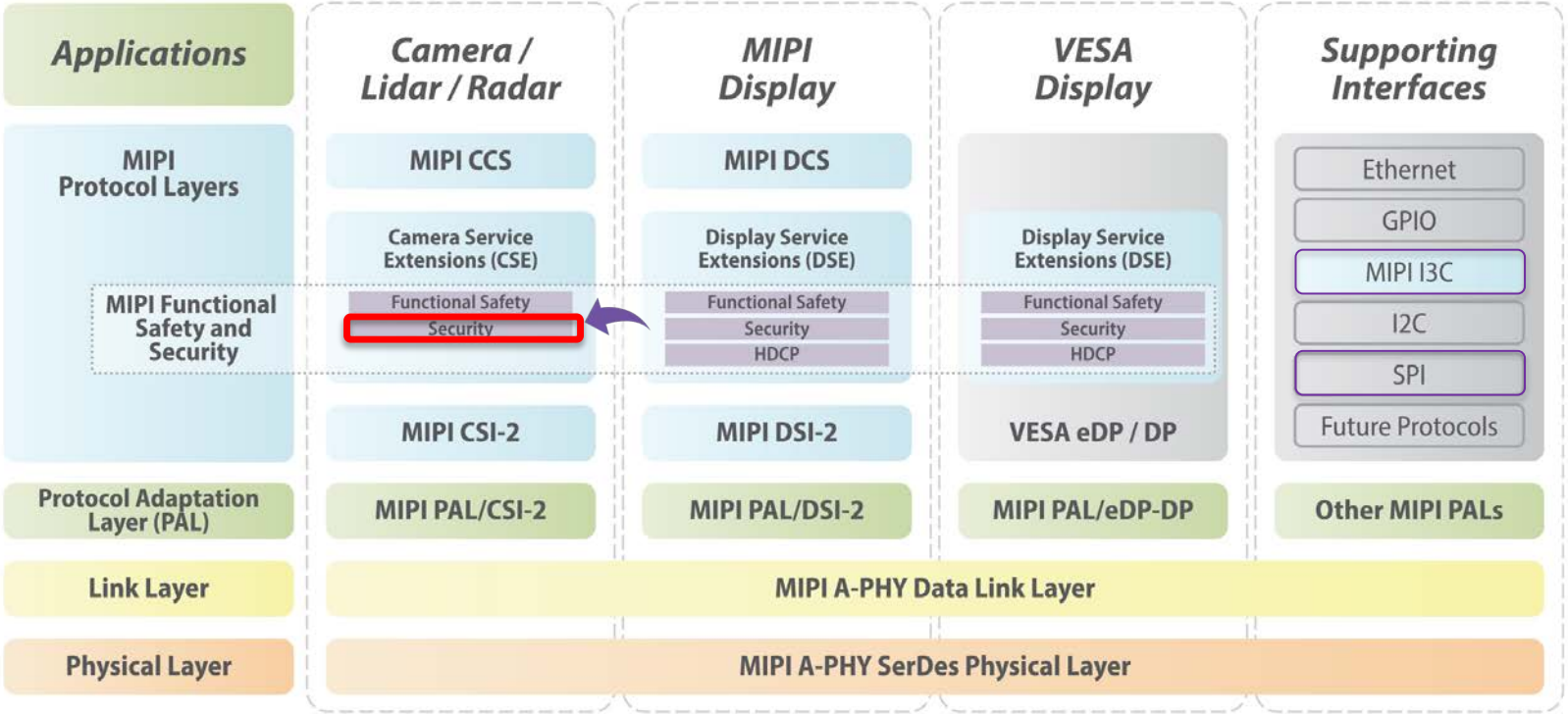
Confidentiality (optional)

- Protects sensor data against unauthorized access between Sensor & ECU
  - *Security consideration*: Privacy: location-revealing images
- Provided by Message encryption



MASS Stack, MIPI Security for Camera Sensor

MASS[SM]: MIPI Automotive SerDes Solutions



Under development, due 1Q 2023:
MIPI **CSE**[SM] **v2.0**, MIPI **Security v1.0**, MIPI **CCISE**[SM] **v1.0** (Command & Control Interface Service Extensions)

MIPI Security Extent:

End-to-End, Application-Based

 |

MIPI Security Extent: “End-to-End” “App-Based”

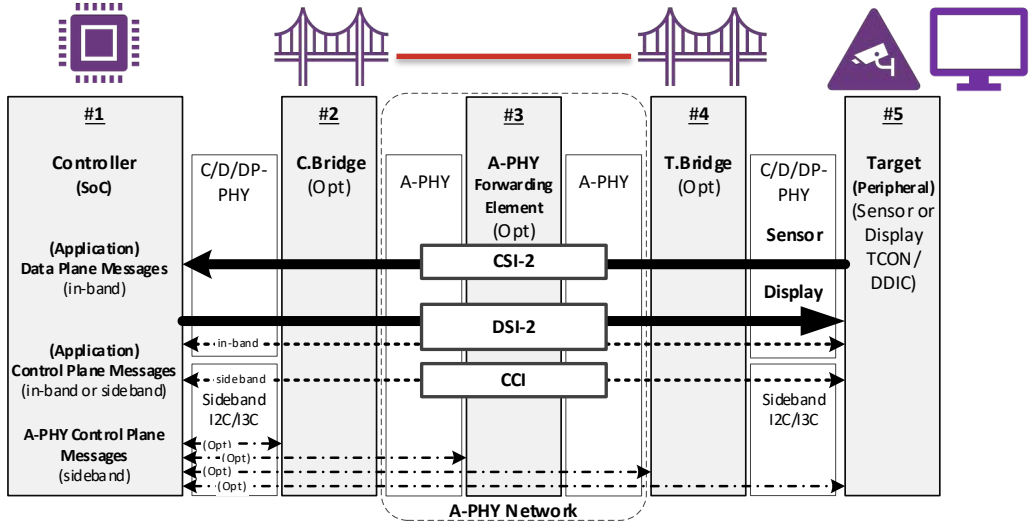
MIPI Security (and FuSa) *extent* may be described in two ways:

- End-to-End
  - From the “ultimate data source” (sensor) to the “ultimate data sink” (SoC), i.e., not involving intermediate bridges/aggregators
  - In MIPI’s “1-5 Model” this means extent “1-5” (not involving entities 2, 3, 4)
- Application-Based
  - From the source Application layer to the sink’s application layer
  - In CSI-2, by “Application layer” is meant “Pixels” (i.e., where Pixels are formed (post-ADC) to where Pixels are received for processing)

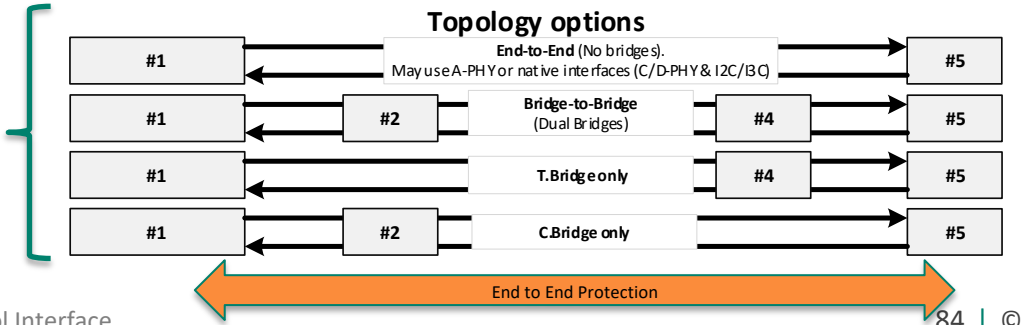
1-5 Model: Reference Topology

End-to-End Security and FuSa Protection

- Up to 5 functional **Components** in a system
- **Controller** (#1) connects to **Bridges** (Aggregators) (#2, #4), **Forwarding Elements** (#3) & **Targets** (#5)



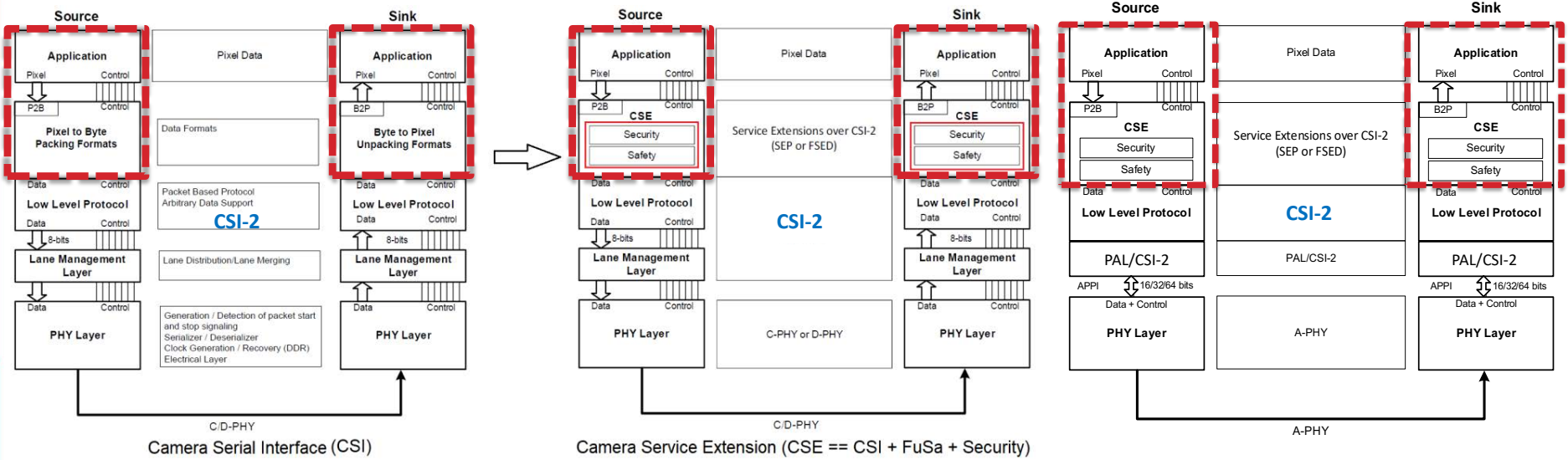
- Security is nominally implemented only in #1 and #5 but may be implemented in bridges/aggregators #2 and #4 (not in #3).



CCI: Camera Control Interface

MIPI CSE Layering, Application Layer

CSE is “above” the CSI-2 protocol, at the **Application Layer** that operates on **Pixels** (Security & FuSa).
Application-aware security allows app-specific security measures, e.g., protect only certain DTs [partial integrity].



CSI-2 (No data protection)
(C-/D-PHY[SM])

CSI-2 + Data protection
(C/D-PHY[SM])

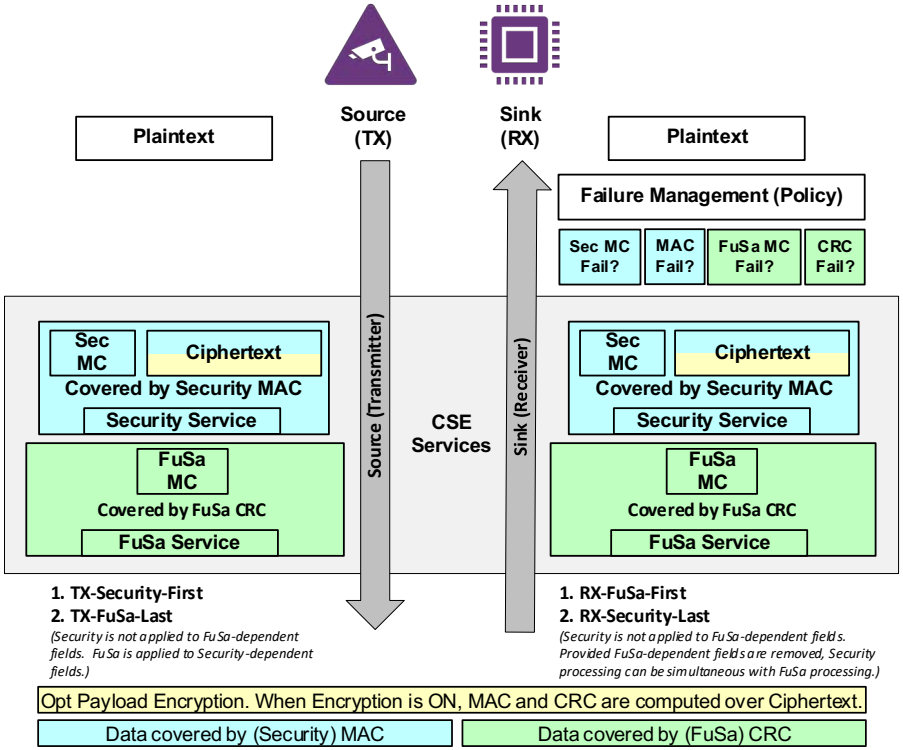
CSI-2 + Data protection
(A-PHY®)

MIPI Service Layering:

TX-Security-first, TX-FuSa-last

 |

CSE Services Layering (Security, FuSa)



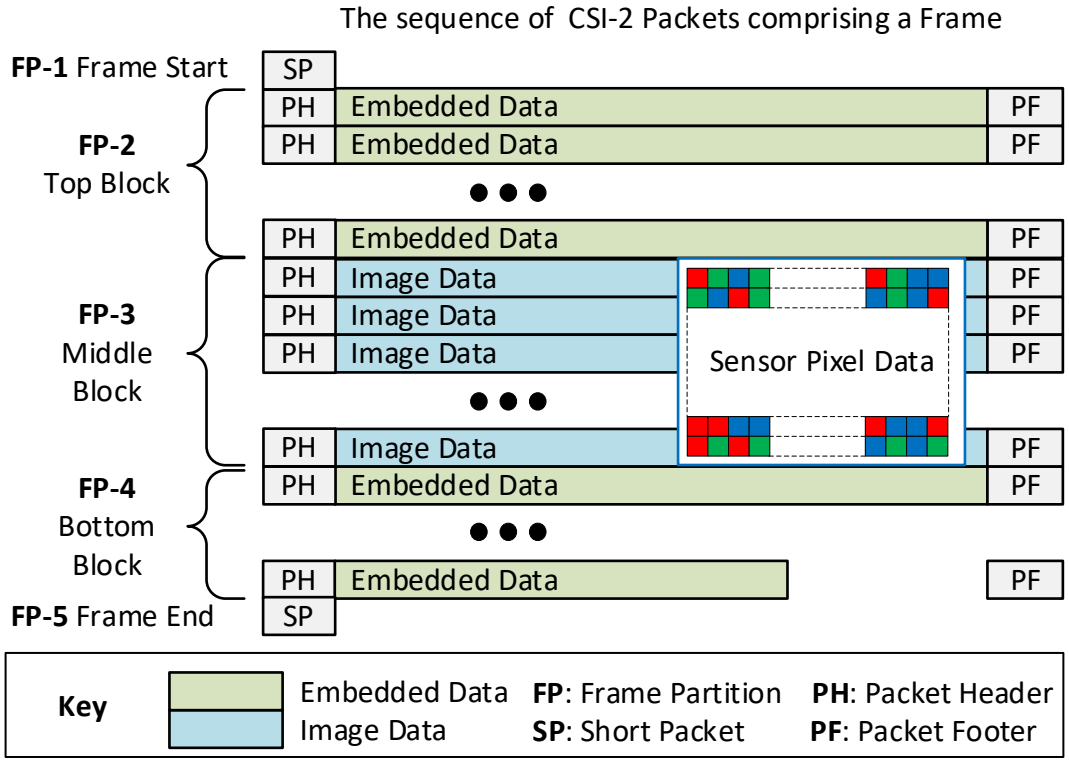
- TX processing:
  - TX Security-first
  - TX FuSa-last
- RX processing:
  - RX FuSa-first
  - RX Security-last
- Failure management policy is out-of-scope and implementation-dependent

MAC: Message Authentication Code
CRC: Cyclical Redundancy Check
MC: Message Counter
FuSa: Functional Safety

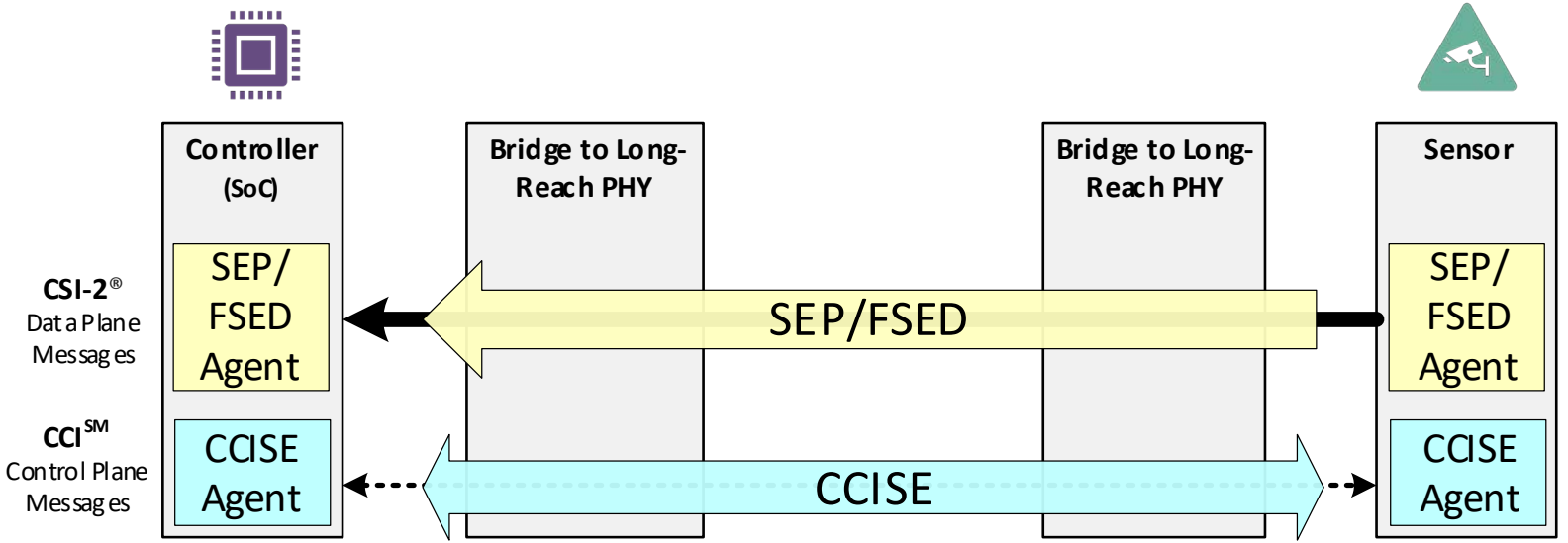
Security Flexibility

MIPI CSI-2 Frame Anatomy (Frame Partitions)

- A sensor can transmit data in multiple Virtual Channels (VCs)
- Each VC consists of a sequence of Frames
- Each Frame is a sequence of MIPI CSI-2 packets
- Frame can be partitioned into 5 Frame Partitions (FP)
- MIPI CSI-2 packets from multiple VCs can be interleaved



Security Provided by *SEP*, *FSED*, *CCISE* Protocols

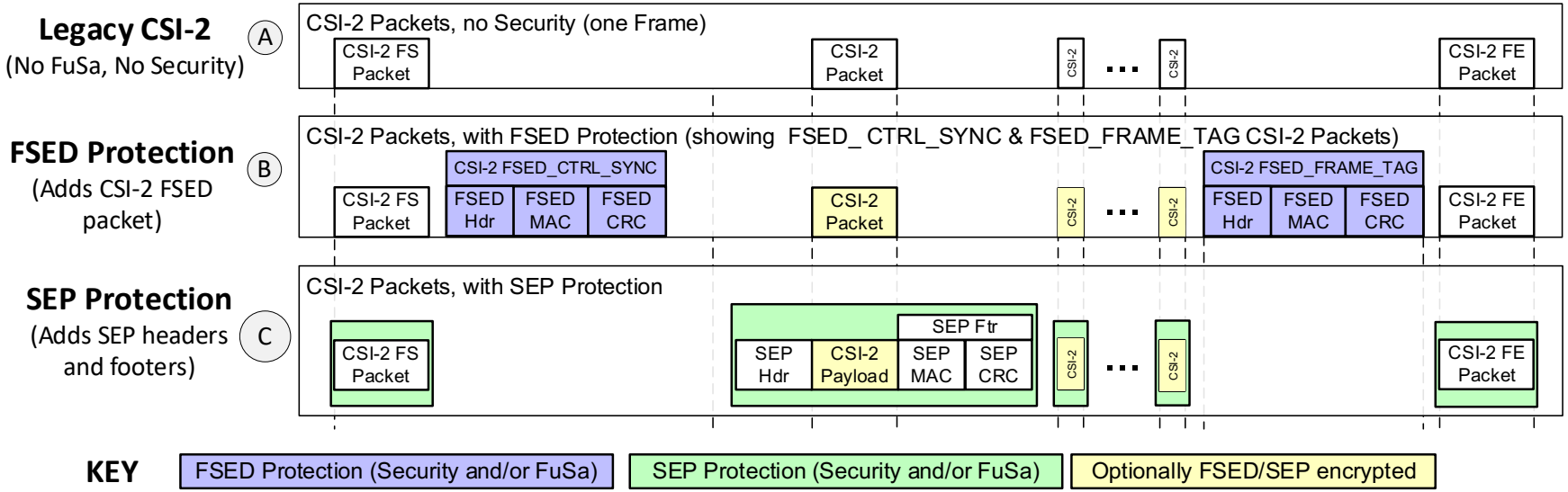


SEP:
Service Extensions Packet
Granularity: Message-Based
Sensor/Bridge-to-Controller/Bridge

FSED:
Frame-Based Service Extensions Data
Granularity: Frame-Based
Sensor-to-Controller

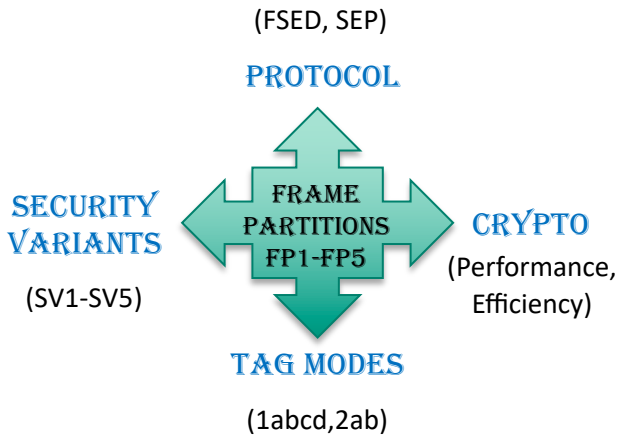
CCISE:
Command and Control Interface Service Extensions
Granularity: I²C Transaction (Start→Stop)
Sensor-to-Controller

FSED/SEP: Protocol Comparison



Flexible Security

- Flexibility vectors, either fixed or flexible for each Frame Partition (FP) within a Frame
  - Protocol: fixed in a system for all frames
    - FSED, SEP
  - Crypto algorithms: f(FP)
    - Performance, efficiency selections
  - Tag Modes: f(FP)
    - How often to compute the MAC
  - Security Variants: f(FP)
    - Security levels including Partial Integrity



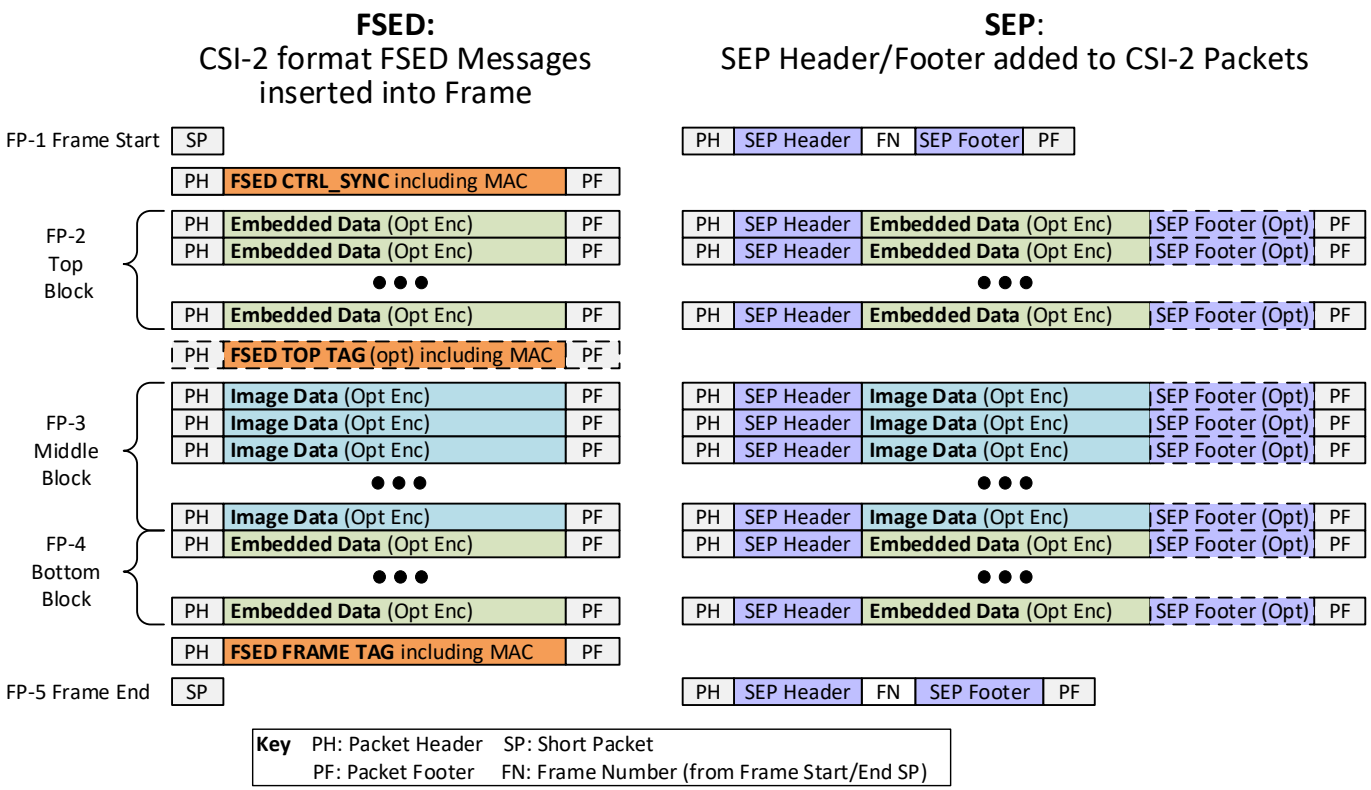
Note: f(FP) means the parameter is flexible for each Frame Partition.

Flexibility: Protocol FSED, SEP

FSED = Frame-based protocol, suitable for legacy and new systems

SEP = Packet and Frame-based, suitable for new systems

A system may implement FSED, SEP or both. Only one is active in a given system (not dynamically changed).



Flexibility: Crypto Algorithms

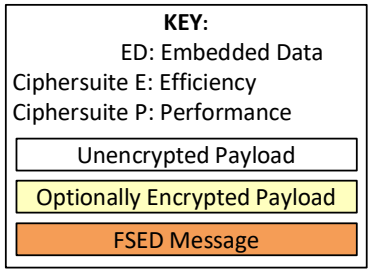
- "Efficiency" sensors: lower Gbps, *can't* afford additional HW
- "Performance" sensors: Higher Gbps, *can* afford additional HW
- **Efficiency "E" Algorithms**: AES-CMAC Integrity. No Encryption
  - AES HW for integrity only. Sensor *can't* afford encryption.
  - Not parallelizable – limited throughput, but enough for "Efficiency" sensors
- **Performance "P" Algorithms: AES-GMAC Integrity w/opt AES-CTR Encryption**
  - AES-GMAC *needs* Galois Field Multiplier HW
  - (Opt) AES HW for encryption
  - AES-GMAC and AES-CTR parallelizable – easily scale for high performance MIPI CSI-2
- Both **algorithm** types ("E" & "P") support use of AES with 128 or 256-bit keys
- ECU controls which Ciphersuite is applied

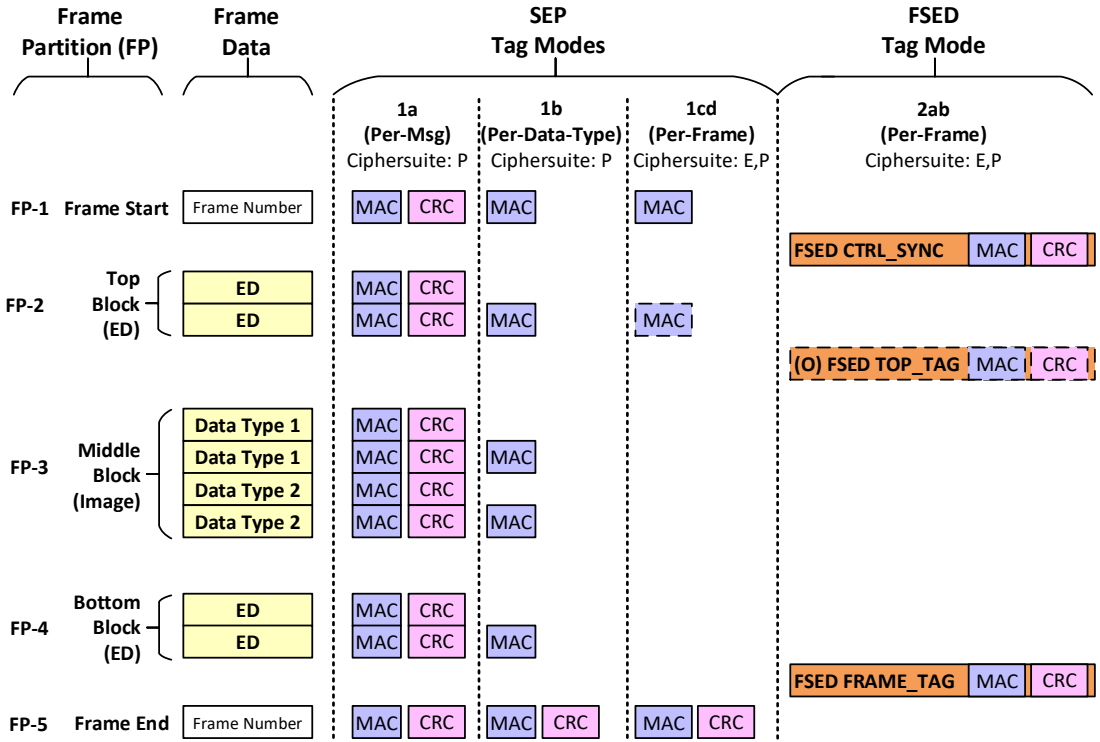
Flexibility: Tag Modes

Tag = Security MAC &/or FuSa CRC

Tag Mode identifies when Tag is sent within a given Frame, & which packets are covered by Tag. Different for SEP/FSED.

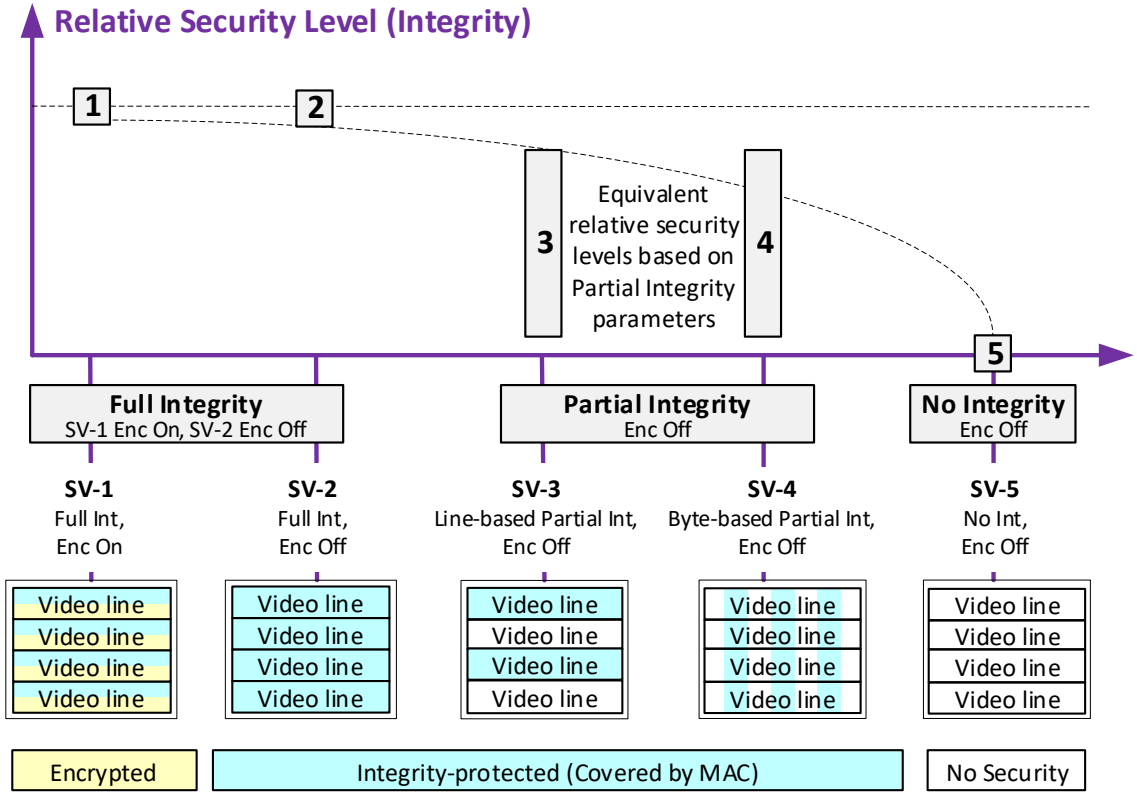
ECU controls which Tag Mode is applied.





Flexibility: Security Variants

- **Security Variants (SV)** enable applying Integrity/Encryption for only specified portions of video frame
  - Enables tradeoffs between security level, computation and power consumption
- **Partial integrity (SV-3, SV-4)**: some data are integrity protected; other data are skipped



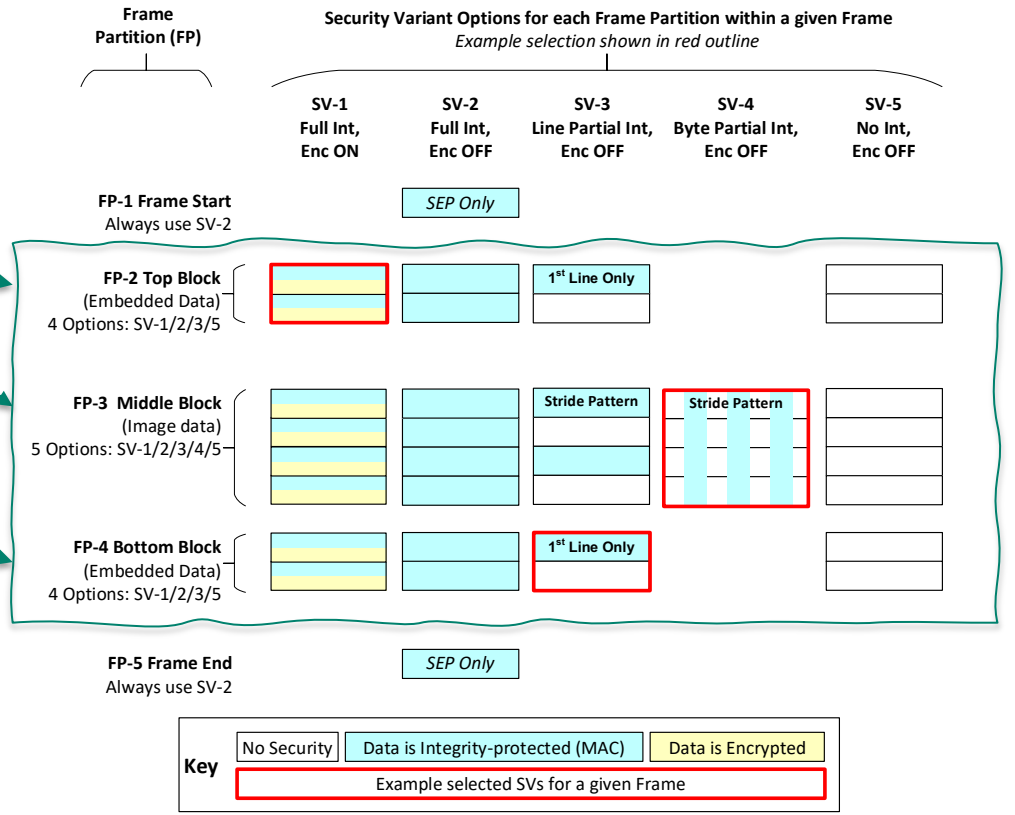
Flexibility: Security Variant vs. Frame Partition

Security Variant can be programmed separately for **FP-2**, **FP-3**, **FP-4** within a given frame

- **FP-2** has 4 SV options (SV-1/2/3/5)
- **FP-3** has 5 SV options (SV-1/2/3/4/5)
  - For SV-3 & SV-4 in Middle Block, **Stride Pattern** selects which data is integrity protected (blue) and which data is not protected (white)
- **FP-4** has 4 SV options (SV-1/2/3/5)

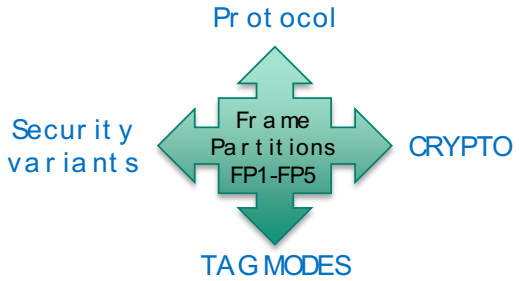
ECU controls:

- Which Security Variants are applied in FP-2/Top, FP-3/Middle and FP-4/Bottom Block
- The Stride Pattern for FP-3/Middle Block SV-3 & SV-4
- Selections on a per-frame basis if needed



Flexible Security

- Of the four flexibility options (Protocol, Crypto, Tag Mode, Security Variant), most options may be fixed for an extended period of time, e.g., minutes to hours.
- ECU controls the security operations based on system needs
  - Each virtual channel is controlled independently
  - Changes can be applied on frame boundaries
- Partial integrity allows the most dramatic dynamic control of integrity computation, thus power and heat dissipation, mainly in the sensors where image quality may degrade with power/heat.

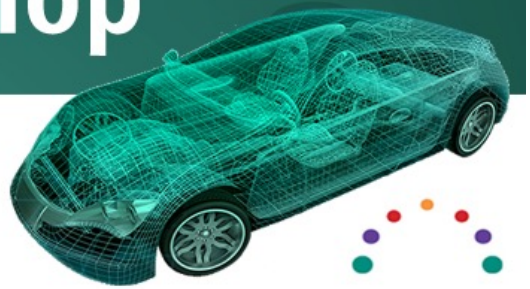


Summary

Summary

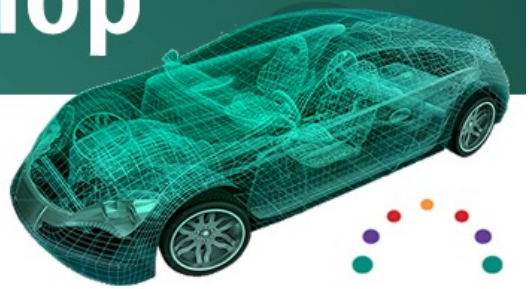
- MIPI CSE CSI-2-based security for ADAS/ADS offers OEMs a flexible security framework operating end-to-end and on an application basis. Distinguished from link-based security.
- MIPI Security flexibility enables system tradeoffs, such as using partial integrity to tradeoff security level for power/thermal reduction.
- The MIPI Security (v1.0), CSE (v2.0) and CCISE (v1.0) specs are targeted for **1Q 2023**
- MIPI CSE may be used on any SerDes/PHY where CSI-2 use is permitted by MIPI policy.
- Further information may be obtained via admin@mipi.org

MIPI Automotive Workshop



Q&A

MIPI Automotive Workshop



THANK YOU

Check back at http://www.mipi.org/2022-automotive-workshop
to view recordings of any sessions you missed