mipi DEVCON
MIPI ALLIANCE DEVELOPERS CONFERENCE

20-21 SEPTEMBER 2022

Phil Hawkes, Rick Wietfeldt
Qualcomm Inc.
Security WG Co-Chairs

MIPI CSI-2® Security Framework

Agenda

- MIPI Alliance is developing an industry security specification to protect MIPI **CSI-2®-based sensor data** for ADAS/AD applications
- Two protocols **tailored** to MIPI CSI-2® frame structure:
  - **Service Extensions Protocol (SEP):** Adds headers/footers to packets
  - **Frame-based Service Extensions Data (FSED) :** Adds new packets
- **Flexibility** enables various tradeoffs
  - Security level vs computation/power consumption/thermal
- Enables **ECU control** based on **real-time** system needs
- MIPI specifications targeting December 2022

MIPI Automotive Security Goals

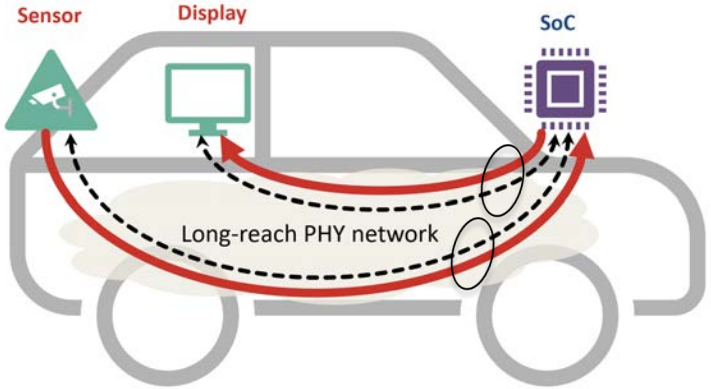
Considerable (10s Gbps) data volume in Distributing image data within the car over long distances 10-15m

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

Authentication establishes trust between Sensor & ECU

Integrity (required)

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

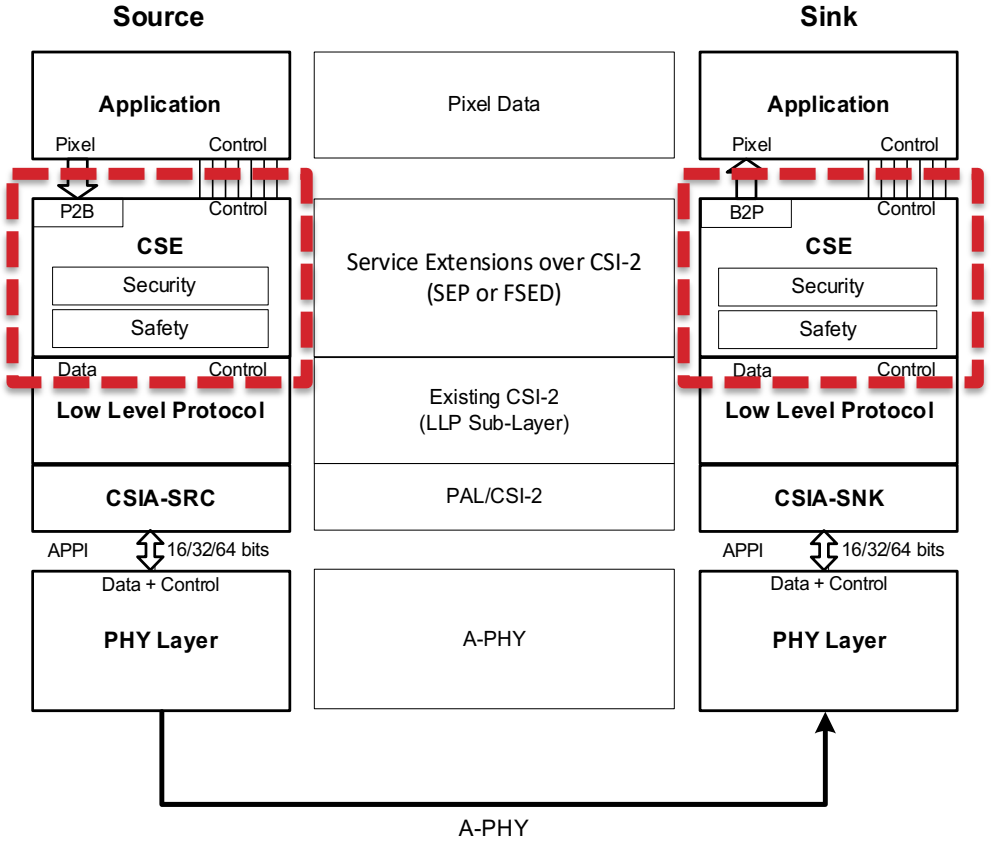


Confidentiality (optional)

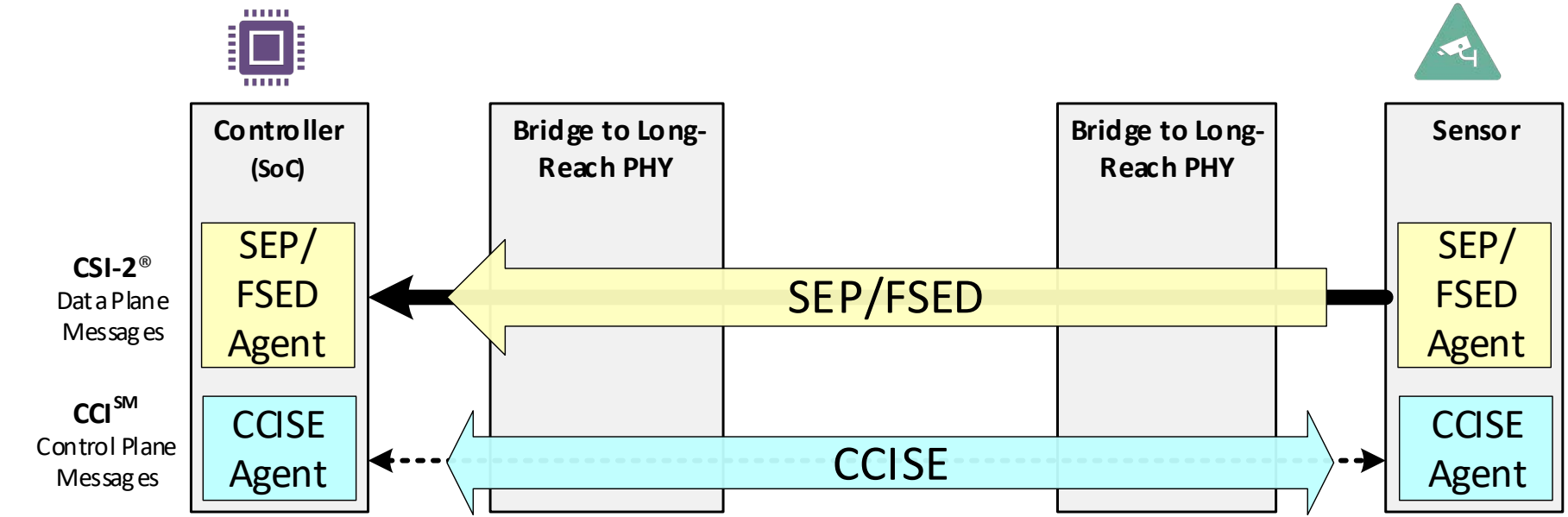
- Protects sensor data against unauthorized access between Sensor & ECU
  - *Security Consideration*: Privacy: location-revealing images
- Provided by Message encryption

Camera Services Extensions (CSE^{SM}) Layer

- Provides Services for MIPI CSI-2® Traffic, including Functional Safety & Security
- Sits above MIPI CSI-2® LLP (Low Level Protocol)
  - Data-Type aware
- CSE^{SM} Specification



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



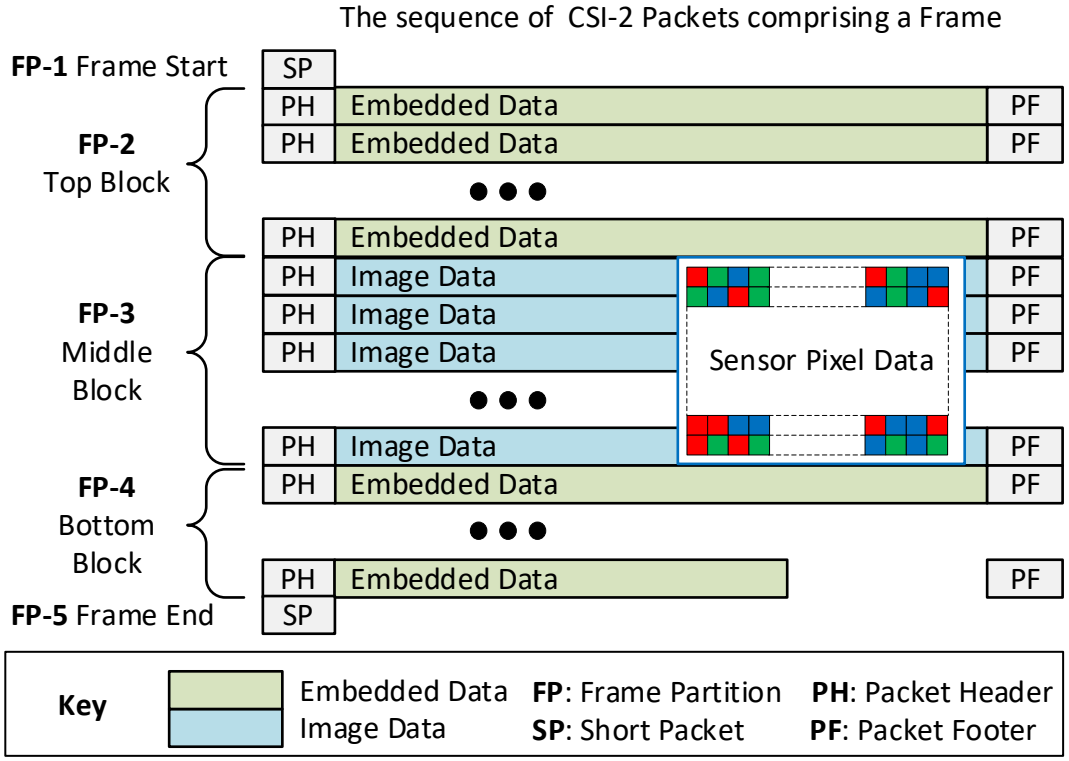
SEP:
Service Extensions Packet
Granularity: Message-based
Sensor/Bridge -to-Controller/Bridge

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

CCISE:
Command and Control Interface Service Extensions
Granularity: I^2C Transaction (Start→Stop)
Sensor-to-Controller

MIPI CSI-2 Frame Partitions

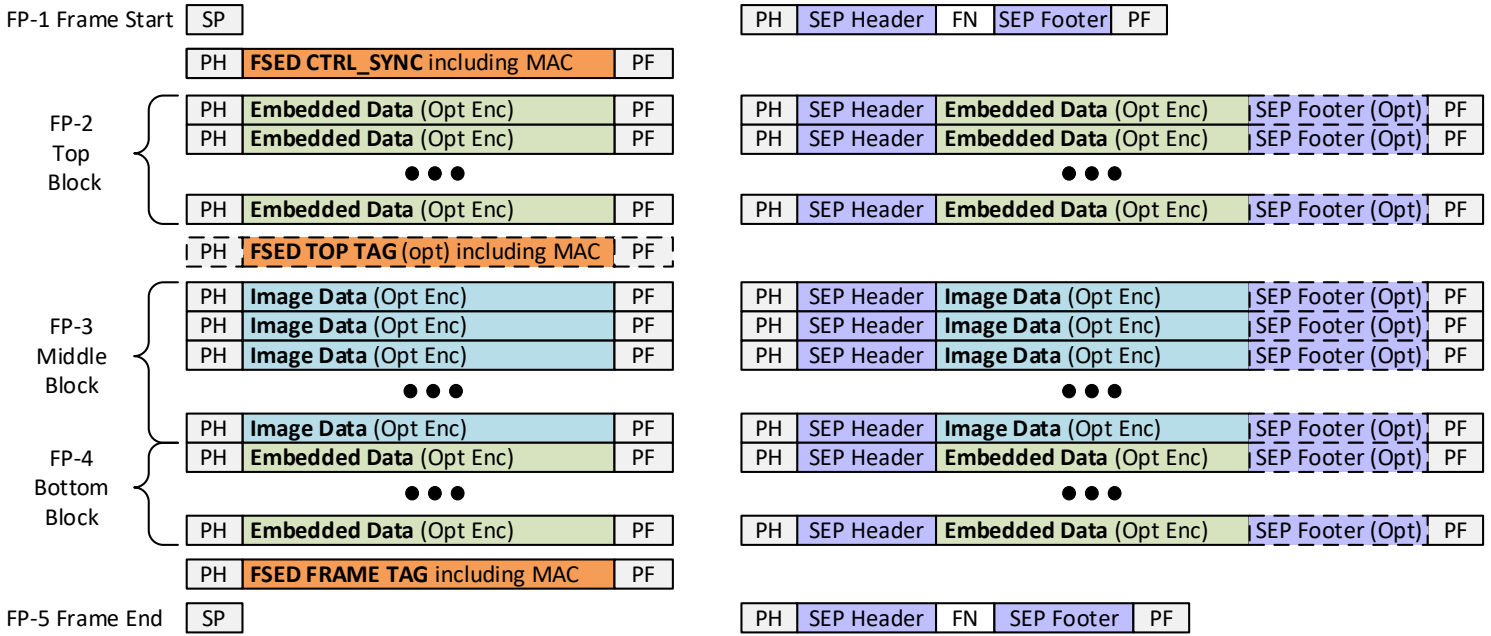
- A Sensor can transmit data in multiple Virtual Channels
- Each Virtual Channel is a sequence of Frames
- Frame is a sequence of MIPI CSI-2 packets
- Frame can be partitioned into 5 Frame Partitions
- MIPI CSI-2 packets from multiple virtual channels can be interleaved



FSED Frame Structure vs SEP Frame Structure

FSED:
CSI-2 format FSED Messages inserted into Frame

SEP:
SEP Header/Footer added to CSI-2 Packets



Key PH: Packet Header SP: Short Packet
PF: Packet Footer FN: Frame Number (from Frame Start/End SP)

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-bit key and 256-bit key
- ECU controls which Ciphersuite is applied

Flexibility: Tag Modes

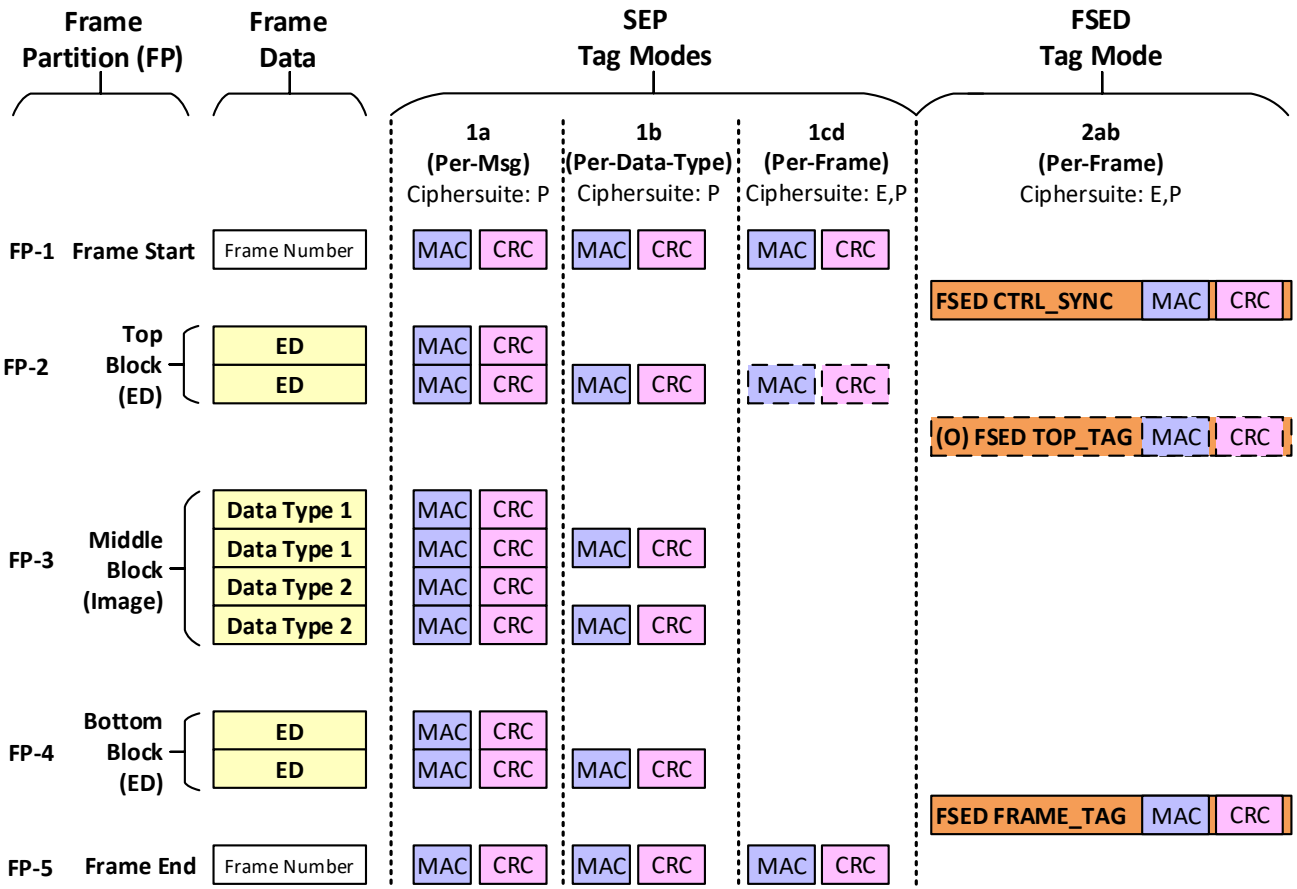
Tag = Security MAC &/or FuSa CRC

Tag Mode identifies when Tag is sent within a given Frame, & which packets are covered by Tag

ECU controls which Tag Mode is applied

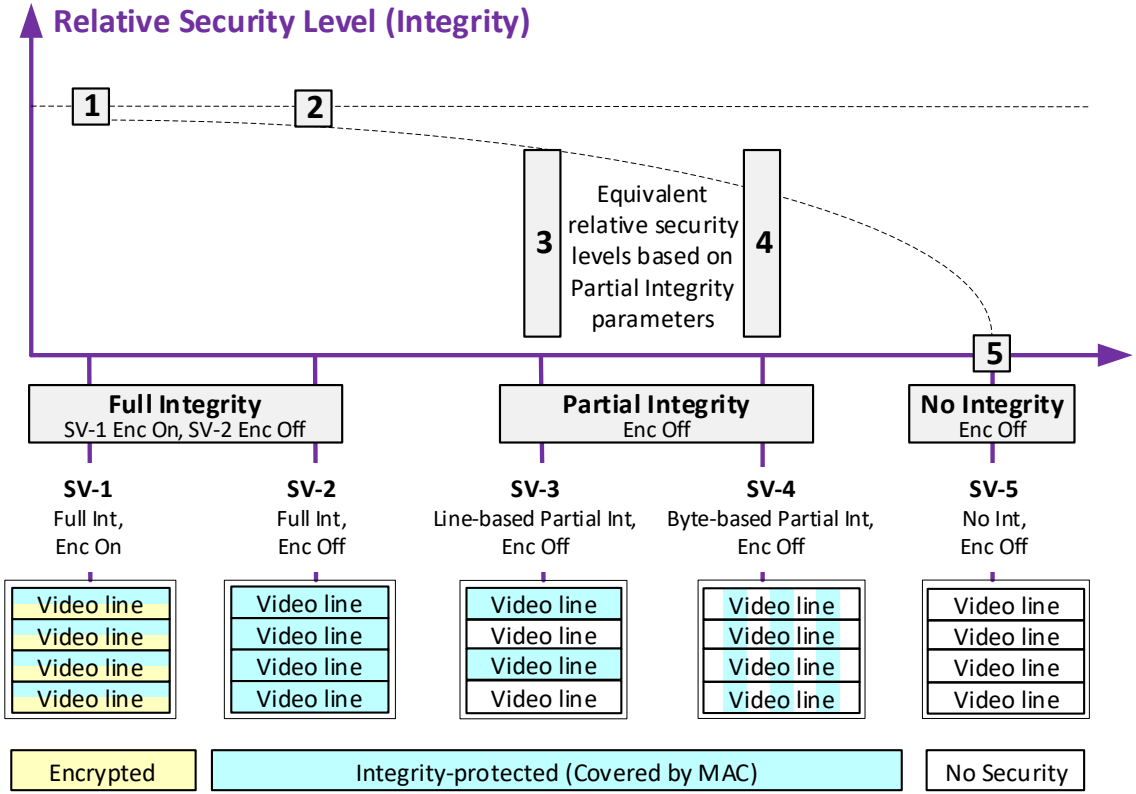
KEY:
ED: Embedded Data
Ciphersuite E: Efficiency
Ciphersuite P: Performance

- Unencrypted Payload
- Optionally Encrypted Payload
- FSED Message



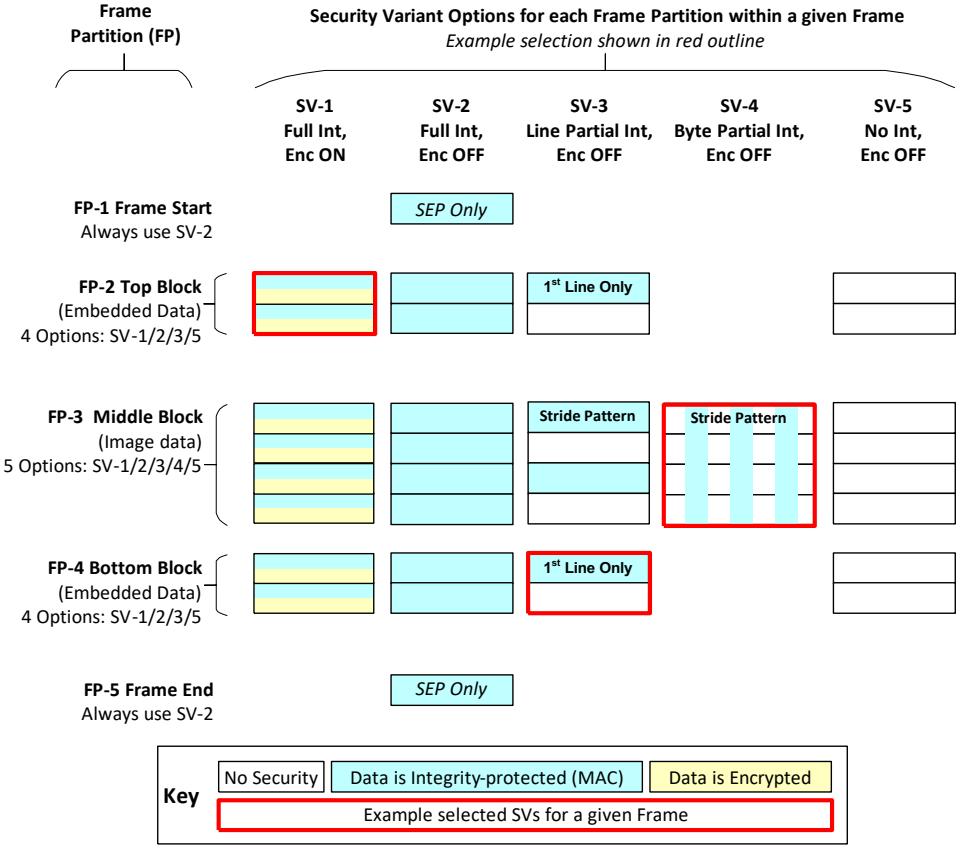
Flexibility: Security Variants

- Integrity protection may not be required on all data in frame
  - E.g., video frame spatial redundancy
  - **Partial integrity**: some data integrity protected; other data skipped
- Encryption may not be required for all data in frame
  - E.g., Encrypt Embedded Data, but not image data
- **Security Variants (SV)** enable applying Integrity/Encryption for only specified portions of Video frame
  - Enables tradeoffs between security, computation and power consumption



Flexibility: Security Variants & Frame Partitions

- Security Variant selected separately for FP-2, FP-3, FP-4 within a given Frame
  - FP-2: 4 options (SV-1/2/3/5)
  - FP-3: 5 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: 4 options (SV-1/2/3/5)
- ECU controls:
  - Which Security Variants are applied in Top, Middle and Bottom Block
  - Stride Pattern for Middle Block SV-3 & SV-4



Flexibility: ECU selects options

- MIPI CSI-2 security operations has four facets:
  - **Protocol:** SEP, FSED
  - **Ciphersuites**: Efficiency, Performance
  - **Tag Modes**: **SEP**: per-Message, per-Data-Type, per-Frame. **FSED**: per Frame
  - **Security Variants:** for each Frame Partition
- Vendors choose which options they implement
- ECU controls security operations based on system needs
  - Each Virtual Channel controlled independently
  - Changes can be applied on Frame boundaries
- *Commonalities of FSED & per-frame SEP enable dual-protocol implementations*

Conclusion

- MIPI Alliance is developing an industry security specification to protect MIPI **CSI-2-based sensor data** for ADAS/AD applications
- Two protocols **tailored** to MIPI CSI-2 Frame structure
  - **Service Extensions Protocol (SEP):** Adds headers/footers to packets
  - **Frame-based Service Extensions Data (FSED) :** Adds new packets
- **Flexibility** enables various tradeoffs
  - Security level vs computation/power consumption/thermal
- The MIPI Security (v1.0), CSE℠ (v2.0) and CCISE℠ (v1.0) specifications are targeted for **December 2022**
- Further information may be obtained via admin@mipi.org

ADDITIONAL RESOURCES

- Available now/soon
  - MIPI CSI-2 Security Technical Overview (ppt)
- Coming in December for MIPI Member Review
  - MIPI Security v1.0 Specification
  - MIPI CSE v2.0 Specification
  - MIPI CCISE v1.0 Specification
- MIPI Security Working Group
  - https://members.mipi.org/wg/Security/dashboard
- Security Update at MIPI Automotive Workshop, 15 Nov 2022, 07:00-10:30 PDT
  - https://www.mipi.org/knowledge-library/webinars/events/2022-automotive-workshop

mipi DEVCON

MIPI ALLIANCE DEVELOPERS CONFERENCE

20-21 SEPTEMBER 2022

THANK YOU!

mipi DEVCON

MIPI ALLIANCE DEVELOPERS CONFERENCE

20-21 SEPTEMBER 2022

Q&A