



車用 SerDes 解決方案 (MASS) 的最新發展

主講者：James Goel 與 Rick Wietfeldt 博士

代表 MIPI 聯盟



James Goel: 大家好。我是 James Goel，MIPI 技術指導小組主席兼顯示器工作小組副主席。在我第一部分簡報結束後，Rick 會進行自我介紹。感謝大家參與 MIPI DevCon 2021 線上活動。

很高興今天與大家談談 MIPI 汽車用 SerDes 解決方案、簡稱 MASS 規範的最新發展。這組規範旨在為汽車系統提供低功耗高頻寬的顯示器及相機端到端解決方案的協同工作。這份簡報內容以

MASS 規範的策略發展方向為主，感興趣的讀者可以在本場次結束後，透過公開網站資訊了解更多技術細節。

Industry Trends Advancing Automotive Functional Safety and Security



Figure 1 Automotive industry trends defined as "CASE". (Source: MIPI Alliance)

James Goel: 許多汽車的應用都受到全新產業趨勢所驅動，亦即 CASE 四個字母各自代表的聯網 (connected)、自動化(automated)、共享(shared)和電氣化(electrified)。互聯汽車使用先進的 LTE 和 5G 網路來增加網路頻寬並驅動更高解析度的顯示器。先進的自動化，讓新的應用程式有更充分的時間運用更高解析、更豐富的聯網顯示器以及聯網感應器。共享是自動化的自然結果，讓應用程式藉由互連的 GPU 和 ECU，有更多機會採用端到端相機和顯示器。電氣化需要低功率的照明和高效率的顯示器。傳統的汽車應用程式，持續要求提高相機和幀率的解析度，同時降低功耗和電氣干擾容限。

MASS Functional Safety Application

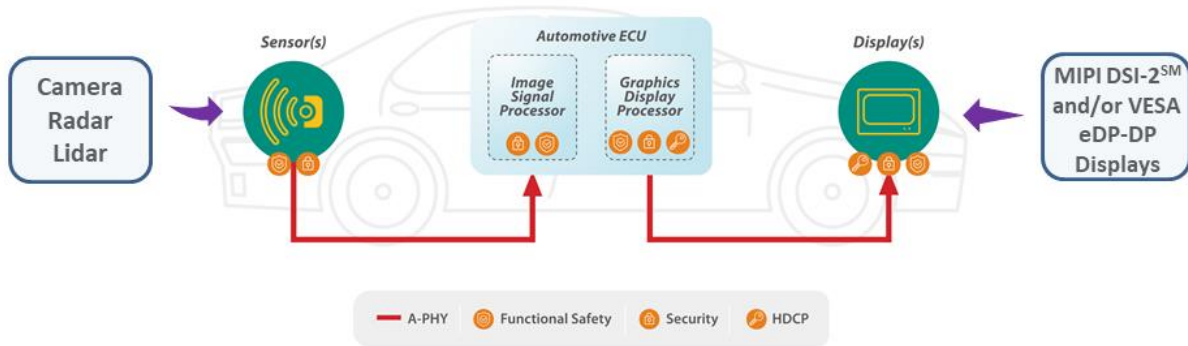
Digital Side Mirror Replacement



James Goel: 我們以汽車座艙的特定顯示器為例，說明 MASS 如何讓顯示器得以支援更嚴格的功能安全目標。圖中看到一個位置較低（low profile）、廣角的汽車相機感應器，搭配嵌入式顯示器，取代了傳統的乘客座側後視鏡。改用數位後視鏡之後，先進的光學系統減少了駕駛人的盲點，在夜間、低能見度、惡劣天氣條件下也依然能發揮作用。它還具有額外的感測器功能，能偵測駕駛人可能看不到的物體和汽車。如圖所示，汽車 ECU 分析了感測數據，並在螢幕上數位呈現了額外的安全標誌和警告符號。這項應用中的車用顯示器具有嚴格的安全目標，需要基於適當汽車危害分析的 ASIL D 認證。要能如此完整彙整，需要額外的像素訊息，確保能符合 ISO26262 確立的 ASIL D 定義。

MIPI Automotive SerDes Solutions (MASS)

Vision for Full SerDes Integration



Sensor and display endpoints with integrated long-reach connectivity (integrated A-PHYSM SerDes) connect to the ECU without intermediate bridges. Application-level functional safety and security data protection. HDCP for protecting premium content.

James Goel: MASS 系列規範專為端到端功能安全和未來的安全而設計。圖中左側的鏡頭雷達使用 MASS 規範來擷取資料，並透過功能安全和安全協議予以保護，標記來自感測器和 ECU 的完整圖標，再到顯示器。不同區塊分別透過 A-PHY SerDes 介面完成這一切。ECU 圖像訊號和圖形顯示處理器會協助顯示器產生新的像素輸出資料。透過 A-PHY SerDes，MASS 規範可以替顯示處理器輸出的像素提供安全保障，最終來到玻璃顯示器的部分。端到端 MASS 的作法有時稱為玻璃到玻璃，因為它從感測器捕捉到光的瞬間啟動，一直到光線離開顯示器為止。

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**

James Goel: ISO26262 系列為汽車功能安全標準。在許多其他參考設計和要求中，這些標準定義了屬於汽車領域中，以汽車安全完整性級別(automotive safety integrity level, ASILs)的風險基礎方法 (risk-based approach)，簡稱 ASIL。ASIL 用於檢索適用的 ISO26262 規範，用於避免在應用安全目標定義中的不合理剩餘風險 (unreasonable residual risk)。MASS 顯示器規範採用 ISO26262 Part 5 產品開發的硬體層級規範，作為顯示器繪圖管線的安全基礎。具體來說，附錄 D 豐富提供診斷覆蓋率的詳細指南訊息，能針對合規所需的單點故障和潛在故障指標進行診斷評估，同時也能評估隨機硬體故障所導致安全目標違規情況。

ISO26262-5 Annex D – Communications Bus



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

James Goel: 附件 D 提供了硬體故障模式分析，而顯示器安全工程師在嘗試符合顯示器安全目標時可以參考。表 D6 定義了適用於 MASS 規範下的顯示器介面的安全機制和關鍵性能測量建議。下面四行以及紅框文字概述的機制，可結合起來提供高級、典型、可實現的診斷覆蓋率。這些機制包括：使用 CRC-32 編碼的訊息冗餘、使用獨特 16 碼的分幀計數器以及使用倒數計時機制的超時監控。如表中最後一行所述，這三種機制的組合提供了可實現的高覆蓋率。

Adding Service Extensions Packets (SEPs)

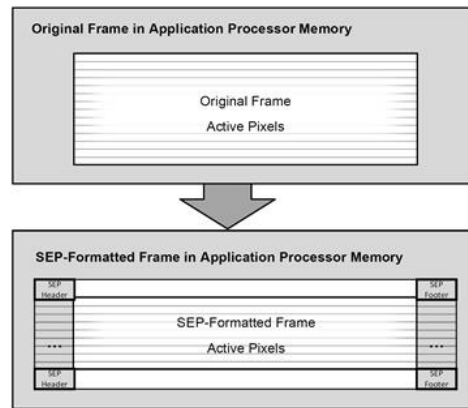


Figure 23 SEP Formatting in the Display Source

MIPI DSESM v1.0, MIPI PALSM/DSI-2SM v1.0

James Goel: MIPI 的顯示服務擴充功能(Display Services Extensions)、或說 DSE 規範定義了一種新的數據封包、如同附件 D 表 D0.6 中描述的安全機制類型。在 DSI-2 協議編碼器把像素轉換為位元的過程中，計算出來這些服務擴充封包（簡稱 SEP）。本圖說明了在 DSI-2 長數據封包(long packets)定義的影片中，SEP 數據封包如何被置放在每個結束與開始的行列的起始點。SEP 標頭和結尾數據封包，也保護 DSI-2 短數據封包的命令和控制介面。DSI-2 的 MIPI 協議適配層，定義了 SEP 數據封包的需求；當 DSI-2 長短數據封包轉換為 A-Packets、數據分幀並透過 A-PHY 發送時，也必須透過 DSI-2 的 MIPI 協議適配層。

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.

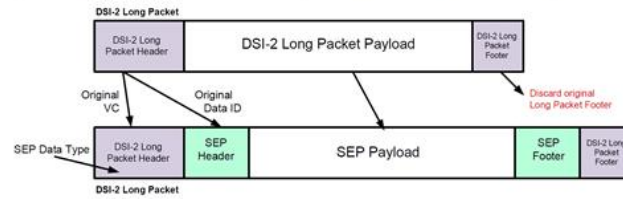


Figure 20 Converting DSI-2 Long Packet to SEP Within DSI-2 Long Packet

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

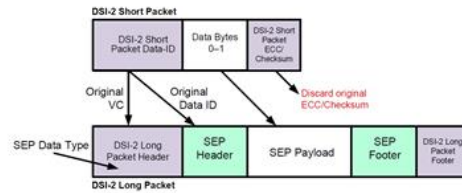


Figure 21 Converting DSI-2 Short Packet to SEP Within DSI-2 Long Packet

MIPI DSESM v1.0, MIPI PALSM/DSI-2SM v1.0

James Goel: 這張圖說明了 SEP 標頭和結尾數據封包，如何包覆 DSI-2 的短數據封包和長數據封包。DSI-2 長數據封包的有效載荷和 SEP 標頭，用於計算位於 SEP 結尾中的 CRC-32 值。這些數據封包組合起來，形成新的播放有效載荷，構成一組新的、可能會透過 A-PHY 傳輸的 DSI-2 長數據封包。DSI-2 短數據封包的轉換，也是透過一樣的過程。

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]	Reserved																															
ePH[4]	Reserved																															
ePH[5]	Reserved																HDCP streamCtr[31..0]															
ePH[6]	Reserved																HDCP InputCtr[31..0]															
ePH[7]	Reserved																HDCP InputCtr[64..32]															

Table 2 SEP Packet ePF Blocks: Overview

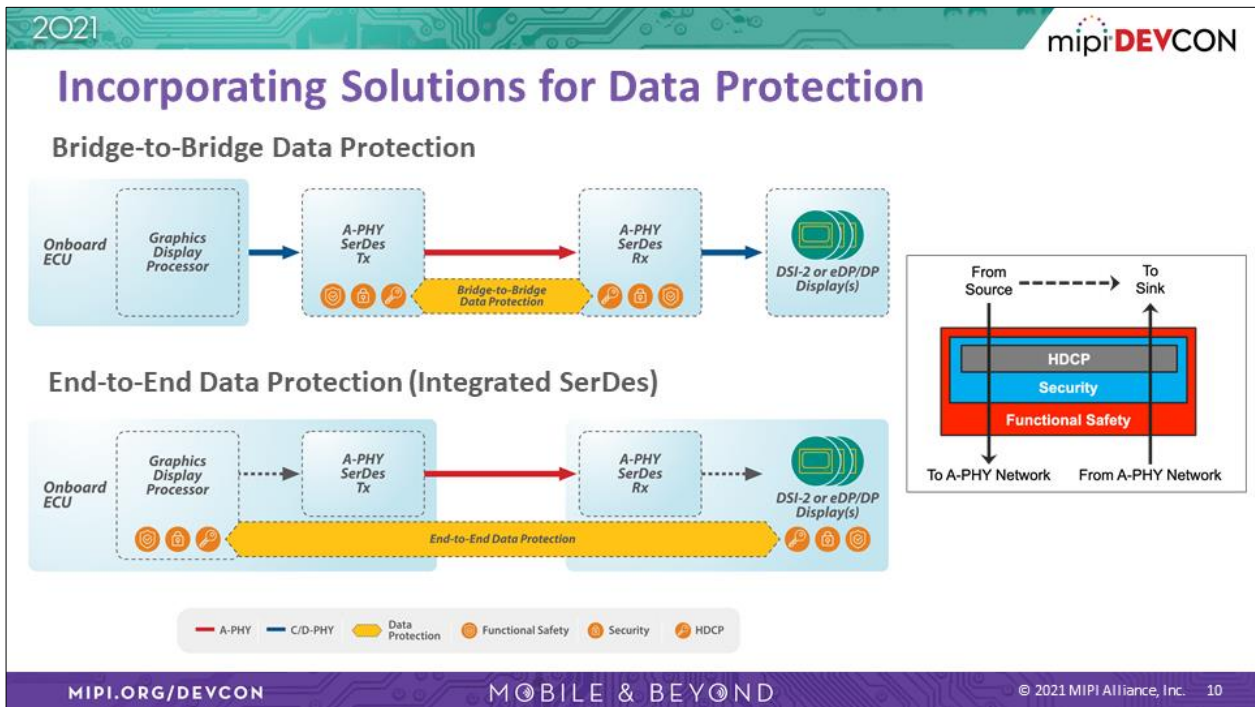
Bits	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
ePF[1]	Reserved																															
ePF[0]	Reserved																CRC-32															

MIPI DSESM v1.0

James Goel: 理解這些重要 SEP 數據封包的部分細節，深具啟發。SEP 數據封包標頭的前 32 個位元 (EPH zero)，包含了定義 SEP 有效載荷格式的 eDP (擴展資料類型)。DSE 規範目前支援 MIPI DSI-2 和 MIPI PAL，適用 VESA、eDP、DP、SEP 的有效載荷類型。EPH-2 內含 SEP 16 位元訊息計數器。這是 SEP 2.0 版本，是第一個透過配置功能安全顯示器、並以分幀會話傳送的數據封包，針對每個已傳輸的 SEP 數據封包，發送器也會逐步加一增強。顯示器應用程式，可能會選擇在每行活躍影片開始時、或在 SEP 數據封包傳輸過程中以其他應用程式指定的特定時間，重置訊息計數器。

訊息計數器的關鍵值，是要標記出唯一且具有單調遞增值的 SEP 數據封包。如果終端顯示接收端解碼了 SEP 訊息計數器，並跳過、重複或錯過了下一個序號值，就必須斷言 (assert) 錯誤條件，採取適當的系統層級行動，例如顯示器上閃爍錯誤警告。

要實現超時監控 (timeout monitoring)，也可以在既定數量的垂直接收訊號範圍內，透過顯示器追蹤解碼的 SEP 訊息計數器值的有效性。幀率為已知，因此垂直接收器之間的 SEP 訊息計數器值的數量會指示主機是否已在給定閾值內停止發送顯示數據。這對於特定的安全圖標至關重要。



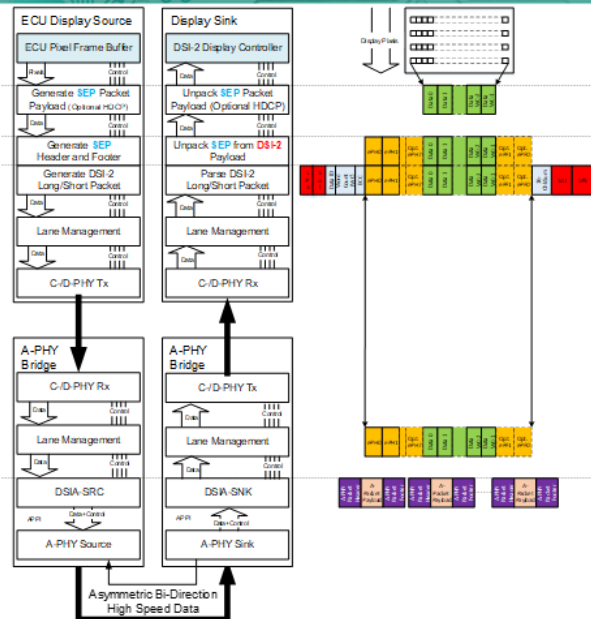
James Goel: 本圖解釋了 MASS 顯示器的功能安全性，以及未來在安全系統層級的作法。上圖顯示了最適合目前既有 ECU 和顯示器的橋接器間 MASS 解決方案。左側的 ECU 會生成源像素資料，使用標準 MIPI DSI-2 或 VESA eDP 原生介面，連接到 A-PHY 發射橋接器。以藍色箭頭表示。

A-PHY SerDes 發射器會透過 MIPI 協議適配層或 PAL 規範，把原生像素串流轉換為 A-Packet，並受功能安全、安全或 HDC 保護。A-PHY SerDes 會接收、驗證 A-Packets 的功能安全、安全性、HDCP 完整性，然後透過相同的 PAL 規格把 A-Packets 轉回原生 DSI-2 或 eDP 像素。

在這個例子中，FuSa 和安全性只建立在 MIPI A-PHY 橋接器之間。第二張圖勾勒出完全整合 A-PHY 的 MASS 顯示架構，在顯示器像素的生成過程中加入功能安全和系統安全，並透過 A-PHY 連結到最終端，直到顯示器解碼資料並發送到螢幕。這是 MASS 端到端顯示器解決方案的典型案例，因為完全整合的 A-PHY 案例不需要 A-PHY SerDes 橋接器。不過要等到市場完全採用這種解決方案，還需要時間。

接下來幾張投影片中會看到，不整合 A-PHY SerDes 橋接器也可以達到 MASS 端到端功能安全和安全性，只需把整合的 MIPI 顯示服務擴充功能規範，應用在下一代 DSI-2 ECU 內嵌協議生成器中。

Detailed Display Protocol Stack

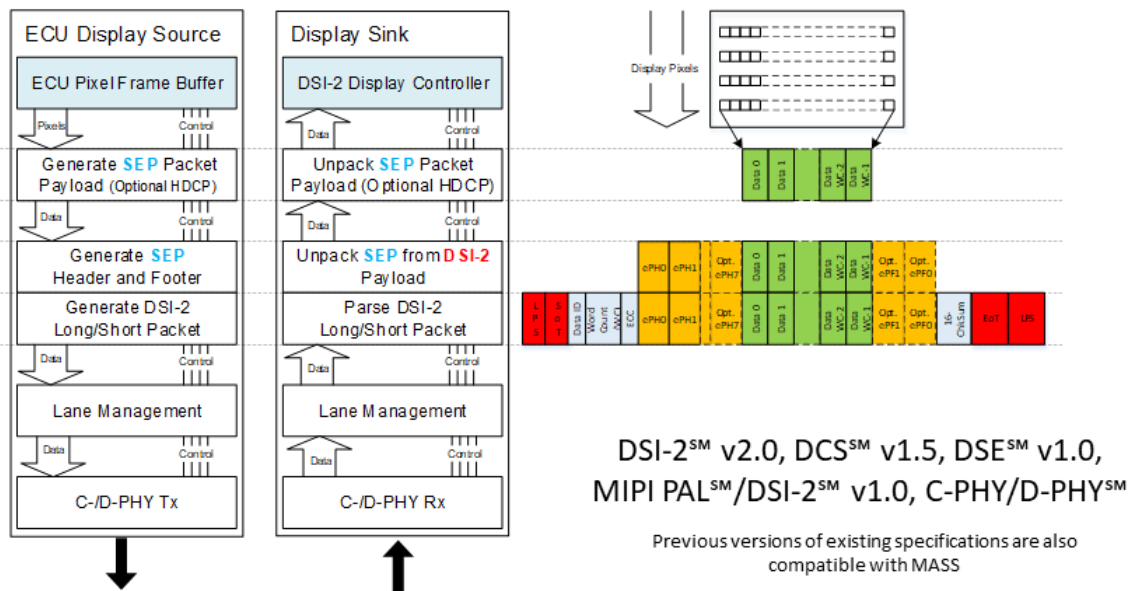


James Goel: 這張圖把垂直協議棧區格式展開來，針對服務擴充數據封包（SEP）如何從 ECU 顯示源到最終顯示玻璃端保護像素有效負載，提供低階訊息。

左側有四個主要模組，顯示源、A-PHY 接收橋接器、A-PHY 發送橋接器和最終顯示接收器。黑色粗箭頭表示主要實體連接：在 C- 和 D-PHY 連接之間、源和橋接器之間、以及 A-PHY 發送器和接收器之間。右側是堆疊區，右側棧區中每一層的詳細有效載荷細分。

以下兩張投影片會詳細介紹頂部和底部部分。

ECU Display Source and Sink



MIPI.ORG/DEVCON

MOBILE & BEYOND

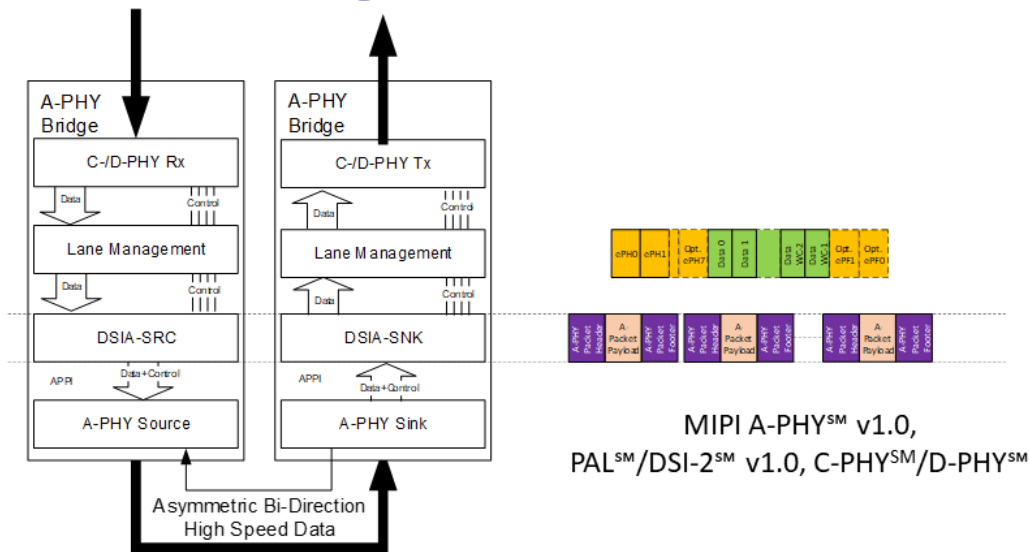
© 2021 MIPI Alliance, Inc. 12

James Goel: 這些圖是依據之前詳細的顯示器協定棧區頂部展開的，左側大塊是 ECU 顯示 DSI-2 源生成器，會生成顯示像素並透過 C-PHY 或 D-PHY 的原生 DSI-2，發送到外部 A-PHY 橋接器。

ECU 像素幀緩衝區中的第一個模塊，包含要送往顯示接收器的最終合成數據。在最右側，可以看到像素顯示緩衝區從上到下按光柵順序掃描，生成綠色的顯示數據字節，用於計算服務擴充封包中的顯示值。

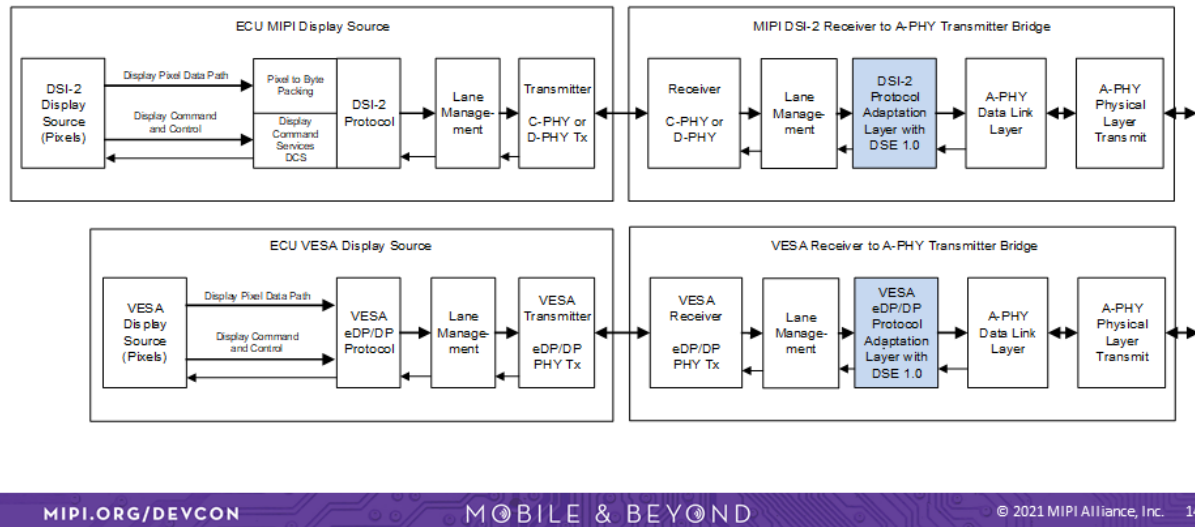
SEP 增強包頭 (EPH) 和增強包尾 (EPF) 含有基於綠色有效載荷的 CRC 和其他 SEP 字段資料。新的 SEP、加上數據字節訊息，形成了傳統 DSI-2 長數據封包的全新有效載荷。要注意的是，命令和控制訊息也受到 SEP 標頭和尾標的保護，形成與 DSI-2 短數據封包類似的有效載荷。這些 DSI-2 數據封包遵循傳統的報頭和頁腳結構，並通過相應 MIPI 規範中定義的 C-PHY 或 D-PHY 發送。在顯示接收器塊上，步驟相反過來，並會逐一驗證 DSI-2 和 SEP 頁眉和頁腳的正確性。如果顯示接收器檢測到錯誤，MASS 顯示系列不會指定 ECU 源或顯示接收器應如何反應，只會說明必須適當地處理並報告錯誤。

Detailed A-PHY Bridge PAL



James Goel: 圖中左側，是 DSI-2 接收器傳送到 A-PHY 發送器。在右側，是 A-PHY 接收器回到 DSI-2 發送器。左邊的橋接器收到 DSI-2 長封包和短封包，透過 DSI-2 或 PAL 規格的協議適配層，將之轉換為正確格式的 A-Packets，以供 A-PHY 傳輸。在右側方塊裡執行的步驟則相反，重新產生 C-PHY 或 D-PHY 發送的原始 DSI-2 長短數據封包。最右側的協議有效負載敘述，說明如何復原 DSI-2 數據封包並分幀為 A-Packets。A-PHY 規範也敘述了相關細節。

MASS Legacy ECUs with an External A-PHY Bridge

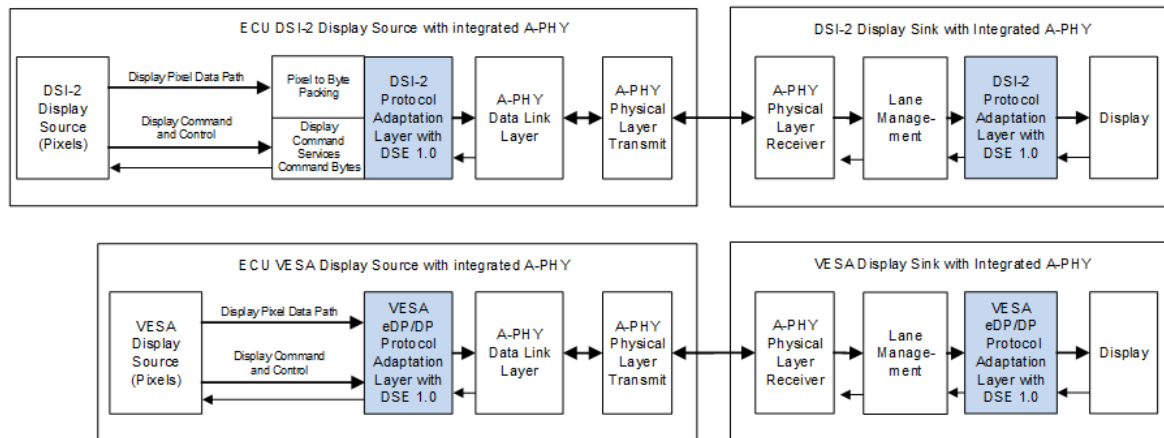


James Goel: 這兩個圖將之前的垂直汽車協定棧區向上轉換為詳細的水平數據管道。傳統汽車 ECU 顯示源僅產生原生的 DSI-2 或 VESA EDP，仍可以利用 MASS 顯示規範來提供功能安全及安全性，未來也能提供 A-PHY 橋接器間的安全性。

第一張圖說明了使用 DSI-2 和 C-PHY 或 D-PHY 發射器的 MIPI 傳統顯示源和接收器。該 ECU 連接到外部 DSI-2 到 A-PHY 橋接器。傳統 ECU 具有傳統的 DSI-2 介面，協議中並未加入 FuSa 或安全性。一旦 A-PHY 橋接器接收到資料，DSI-2 的協議適配層會在像素資料透過 A-PHY SerDes 介面傳輸之前，透過 DSE 規範增加功能安全性，並在未來增加安全性。

第二張圖顯示了傳統 VESA 發射器的類似配置。在 A-PHY 傳輸資料前，協議適配層或 VESA EDP 增加了功能安全性，未來也會加強安全性。

MASS New ECU with Integrated A-PHY

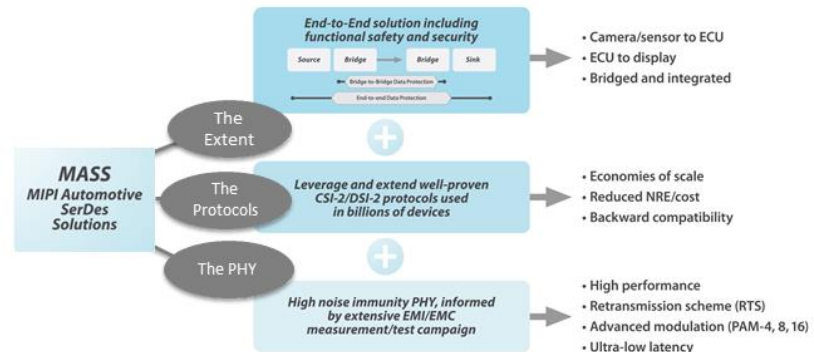


James Goel: 本圖說明 MASS 如何應用已經完整整合 A-PHY 的全新 ECU。這些搭載完整整合 MASS 顯示規範的新 ECU，可以利用到完整端到端功能安全性的優勢，未來也能享受協議適配層使用的顯示服務擴充的安全性。以上兩張圖中，協議適配層在像素協議和編碼管道啟動時，就完整整合到 ECU 裡，藉此確保 DSI-2 和 VESA 都能含括功能安全，未來在 DSI-2 和 VESA DP 原生串流中包含安全性。像素串流在 A-PHY 中全程受到保護，直到最終的像素協議解碼器，再到玻璃顯示部分。

James Goel: 這張投影片列出了以上討論的 MASS 延伸詳細訊息與連結。接下來交給 Rick 來談談安全性。

Security within the MASS Guiding Principles

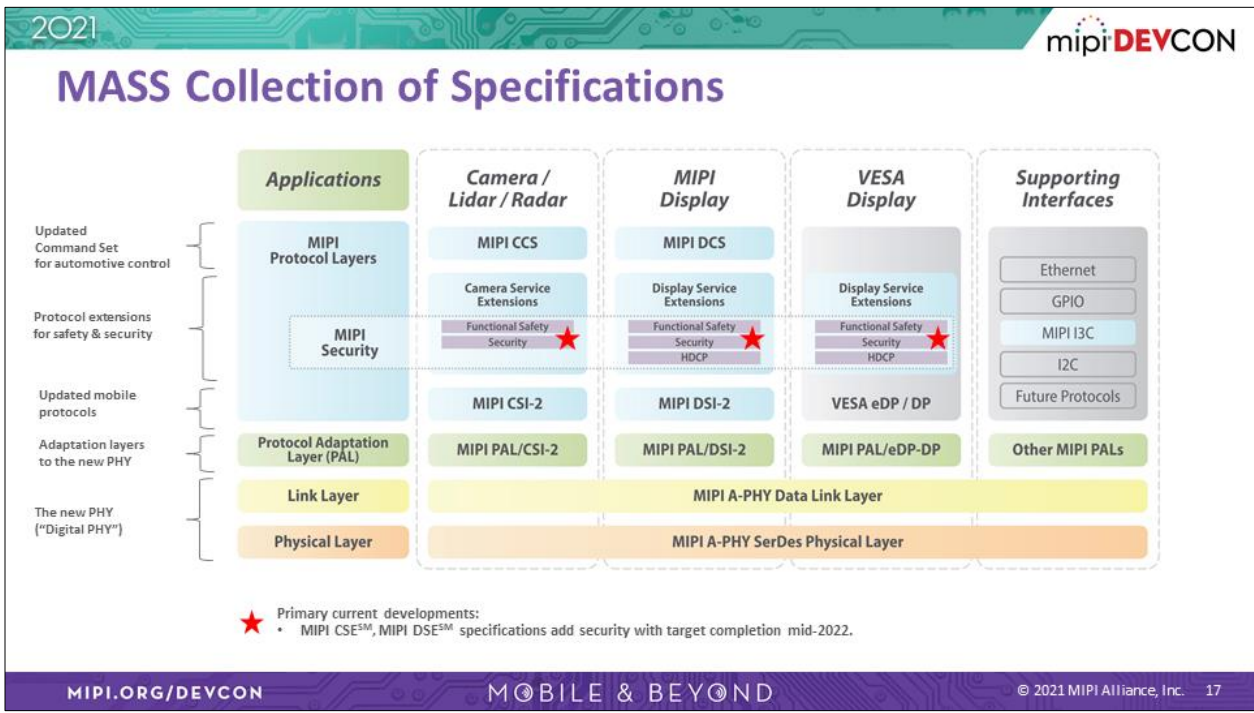
- MASS Guiding Principles
 - The Extent
 - The Protocols (CSI-2SM, DSI-2SM)
 - The PHY (A-PHYSM)
- MIPI Security is implemented as extensions to CSI-2 and DSI-2 protocols.
- This enables the Security to achieve an “end-to-end” **extent**, or **reach**.



Rick Wietfeldt: MASS 的安全及指導原則。

MIPI 安全性基於三個指導原則。第一：PHY，第二：協議，第三：範圍。這些是 MASS 協議的三個指導原則。

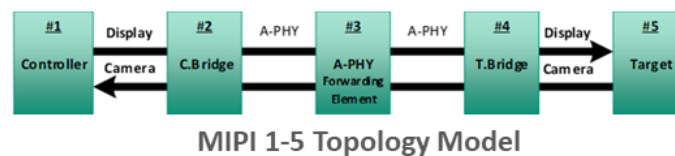
MIPI 的安全性，實踐 CSI-2 和 DSI-2 協議的擴充，讓它可以在許多生態系統中廣泛使用。藉由將安全性附加到協議中，實現端到端範圍的安全性。您可以在圖的上部看到橋到橋和端到端數據保護。



Rick Wietfeldt: 接下來我們討論 MASS 規範。您可以看到兩個主要應用程式—相機和顯示器。相機、光學雷達和雷達視為同一類。顯示器分兩種規格，MIPI DSI-2 和 VESA DisplayPort。您可以在棧區中看到 MIPI 安全（含有同一層內的功能安全 and 安全保護），直接附加在 CSI-2、DSI-2 和 DisplayPort 協議之上。最下面顯示了 A-PHY 數據連結層和物理層。安全性基本上是在協議層級實現，達成前述的端到端範圍。

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.



MIPI 1-5 Topology Model

Rick Wietfeldt: 這一頁說明高階系統和安全要求。

根本上來說，安全性包括三個關鍵要素：資料身份驗證，在元件之間建立信任級別；訊息完整性，確保訊息在傳輸過程中沒有被修改；機密性，藉由加密實現。依據下面顯示的 MIPI 1:5 模型來參考 MIPI 中的數據保護。下一頁會更清楚說明。

基本上，安全是由中央控制器以一對一的方式與其他組件進行管理，而非偏向點對點類型的安全模型。例如，資料安全可以在控制器#1 或其橋接器#2 中啟動，並在#4 或#5 中終止。相機安全可以反向啟動，從#5 或#4 開始，並在#1 控制器或其橋接器中終止。接下來我們將詳細討論 1:5 模型。

MASS System Model: The 1:5 Model

Security Model Components

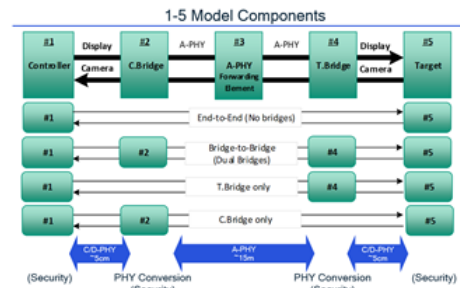
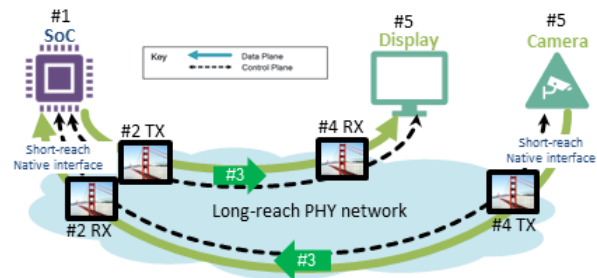
- #1: Controller (SoC)
- #2: Controller Bridge (C.Bridge)
- #3: Forwarding Element (aka Repeater)
- #4: Target Bridge (T.Bridge)
- #5: Target (Camera or Display)

Security Requirements

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

System Requirements (End-to-end)

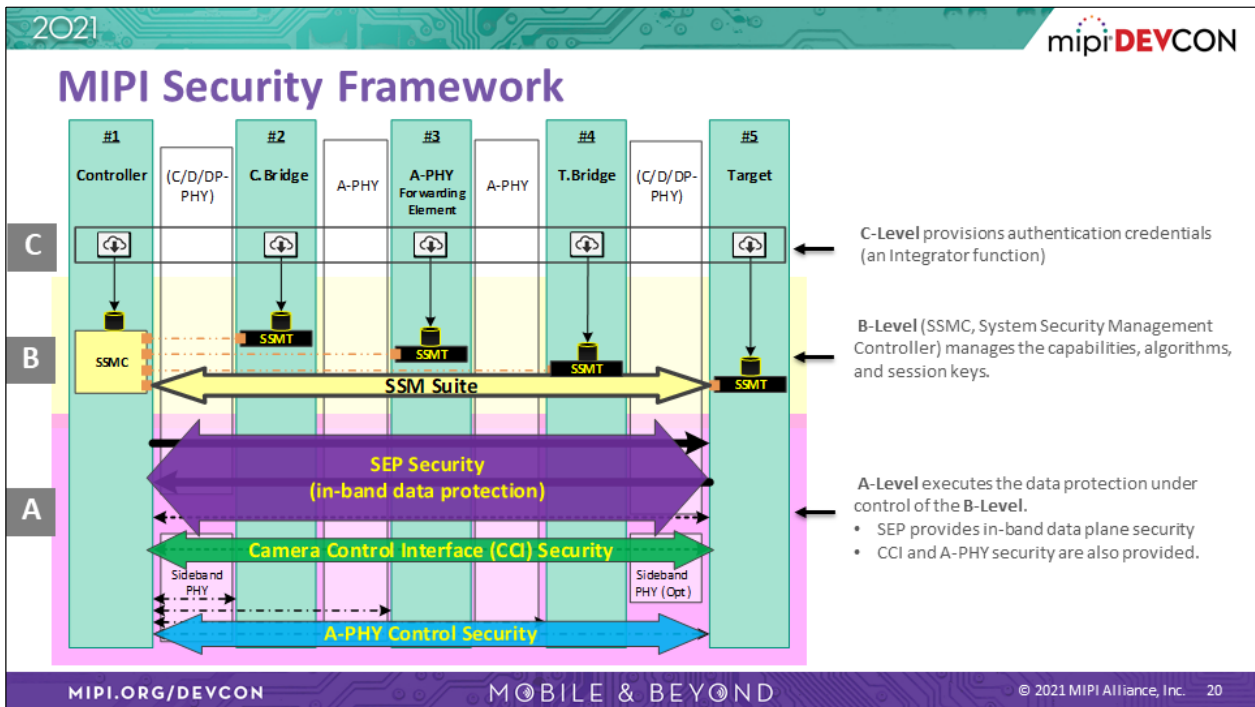
- Multiple system topologies (e.g., 15, 1245, 145, 125)
- End-to-end extent via protocol extensions
- Security for Data plane, and Control plane in-band/sideband
- Highly flexible operation, such as Heterogenous operation for displays, supporting DSI-2 and DP on a daisy chain.



Rick Wietfeldt: 這一頁更詳細地顯示了 1:5 模型。從圖形上看，您可以在相機中看到一個顯示器，標記為 #5，透過橋接器 #4 連接到 A-PHY 網路。A-PHY 網路另一端是其他橋接器，分別連接到 SOC，#2 和 #1。因此可以看到在特定時間內，特定系統中這些組件有會有許多不同變體。

右下角可以看到全部五個，一次兩個，以不同方式排列。系統要求如我們先前討論一下包括了身份驗證完整性和加密。

某些系統要求從在根本上是基於端到端的範圍，亦即協議層確保安全的能力。顯示器和相機的資料層和控制層自然都有相關安全需求。另外還可以進行一個很靈活的操作。例如，在菊花鏈拓樸 (daisy chain topology) 的顯示器情況下，其中多個顯示器以菊花鏈拓樸連接到控制器，一些顯示器可能是 DSI-2，另一些可能是 DisplayPort，並且安全性不會因為端對端的方式有所妥協。



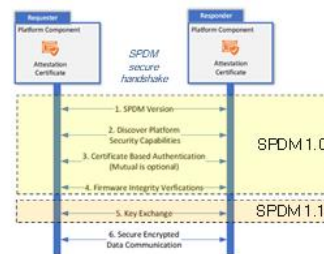
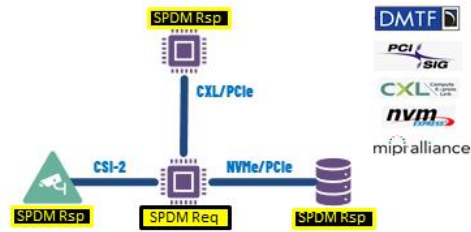
Rick Wietfeldt: 這裡我們說明 MIPI 安全框架，通常稱為 ABC 模型。這裡我們有 1:5 模型和 ABC 模型。在最上層，C 層提供身份驗證憑據。這是一個整合器功能——可以想像一枚 USB 快閃硬碟把金鑰推給每個元件。也可以根據整合商的需要，透過無線或乙太網絡連接進行自動化。

目前這不在 MIPI 規範中，MIPI 確實指定了 B 層級和 A 層級。您可以把 B 層級設想為稱為 SSMC（系統安全管理控制器）的軟體功能。底部的 A 層級則是在更高級別的 B 層級控制下執行資料保護。可以想像成這是進行加密的硬體，完整保護訊息，支援三種不同級別的安全性 - A-PHY、相機的 CCI，以及顯示器和相機資料層的 SEP 安全。

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.



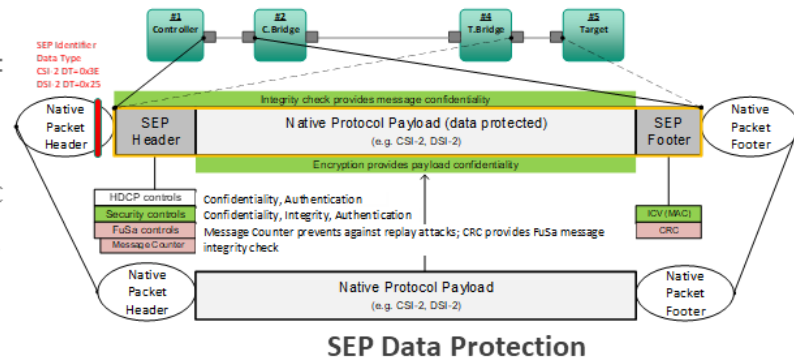
Rick Wietfeldt: MIPI 的安全規範採用簡稱為 SPDM 的 DMTF.org 規範，業界多個組織也採用 DMTF，包括 PCI-SIG、CXL、NVMe，以及新近的 MIPI。SPDM 參考 TLS 模式建立，TLS 正是全球網路使用的安全框架。

基本上有兩大步驟。會在通訊初始化（handshake）之後建立經驗證的會話金鑰，然後發送會話金鑰，保護資料層和控制層的資料。SPDM 訊息再次採通用定義，但在 MIPI 情況中，這些訊息透過 DSI、CSI-2 以及 CCI 或 I2C 傳送，以便單獨保護每個傳輸，如上一張投影片所示。

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.

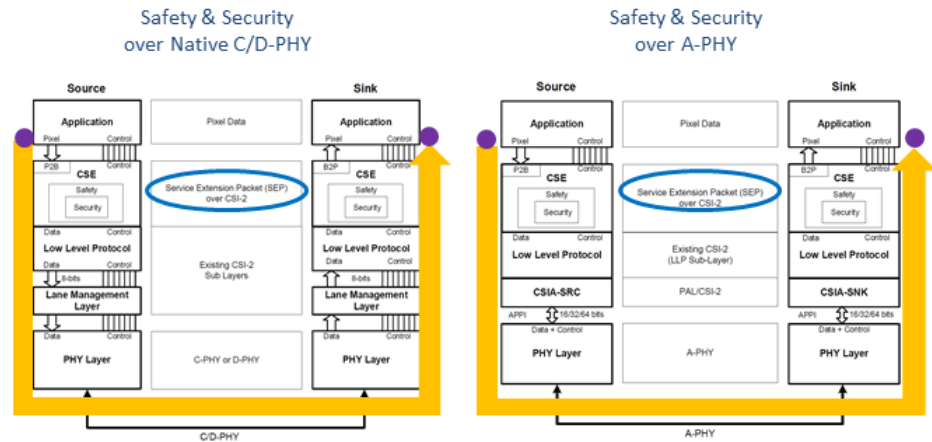


Rick Wietfeldt: 有關 MIPI SEP 格式部分，MIPI 安全的關鍵要素之一就是服務擴充封包。SEP 格式由一個 SEP 標頭和一個封裝有效載荷的尾標組成。有效載荷包括 CSI-2 和 DSI-2。右下角可以看到，本機協議有其本機數據包頭和本機數據包頁腳。這是市面上常見的 CSI-2 和 DSI-2 實踐。上面的 SEP 標頭，標記了所有安全控制，包括 HDCP 和功能安全。頁腳包含完整性校驗值或 MAC 以及 CRC 的關鍵元素。這裡的有效載荷，一般由 CSI-2 包或 DSI-2 包組成，受到保護時就能立即傳輸出去。

End-to-End Application-Level Safety & Security

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.



Rick Wietfeldt: 端到端應用程式級別。

這是 MIPI 安全的一項關鍵組成。我們要做的選擇，是參照 TLS 模式建立 MIPI 安全，並將 MIPI 服務擴展放置在應用層、源頭和接收器。基本上會盡量以端到端的方式，從像素源傳到像素接收器。圖中左側有兩個範例，說明藉由 C-PHY、D-PHY 從應用源到應用接收器的傳輸。右側也是一樣，但攜帶了遠程 A-PHY。紫色圓點說明了端到端的性質，就是在應用程式流程中，像素在何處被創建、在何處被消耗。

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.

Rick Wietfeldt: 簡言之，MASS 規範為當今初版的 CSE 和 DSE 的相機和顯示器，提供了功能安全解決方案。這些完整規範可供 MIPI 會員使用。CSE v1.0 和 DSE v1.0 規範正在更新，支援 CSI-2、DSI-2 以及 CCI (I2C) 邊帶的安全性。MIPI 安全性的關鍵要素之一，是協議本身的安全性置於何處，才能達成使用或不使用中間橋接器的端到端資料保護。如此也得以運用像是 TLS 這樣的[傳輸]層安全性，與 MACsec 等連結層安全性形成對比。

mipi[®]
DEVCON
MIPI ALLIANCE DEVELOPERS CONFERENCE

28-29
SEPTEMBER
2021

**THANK
YOU!**

[MIPI.ORG/DEVCON](https://mipi.org/devcon)

MOBILE & BEYOND

© 2021 MIPI Alliance, Inc. 25