



车载 SerDes 解决方案 (MASS) 的最新发展

主讲者：James Goel 与 Rick Wietfeldt 博士

代表 MIPI 联盟



James Goel: 大家好。我是 James Goel，MIPI 技术指导小组主席兼显示器工作小组副主席。在我第一部分简报结束后，Rick 会进行自我介绍。感谢大家参与 MIPI DevCon 2021 在线活动。

很高兴今天与大家谈谈 MIPI 汽车用 SerDes 解决方案、简称 MASS 规范的最新发展。这组规范致力于为汽车系统提供低功耗高带宽的显示器及相机端到端解决方案的协同工作。这份简报内容以

MASS 规范的策略发展方向为主，感兴趣的读者可以在本场次结束后，通过公开网站信息了解更多技术细节。

Industry Trends Advancing Automotive Functional Safety and Security



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

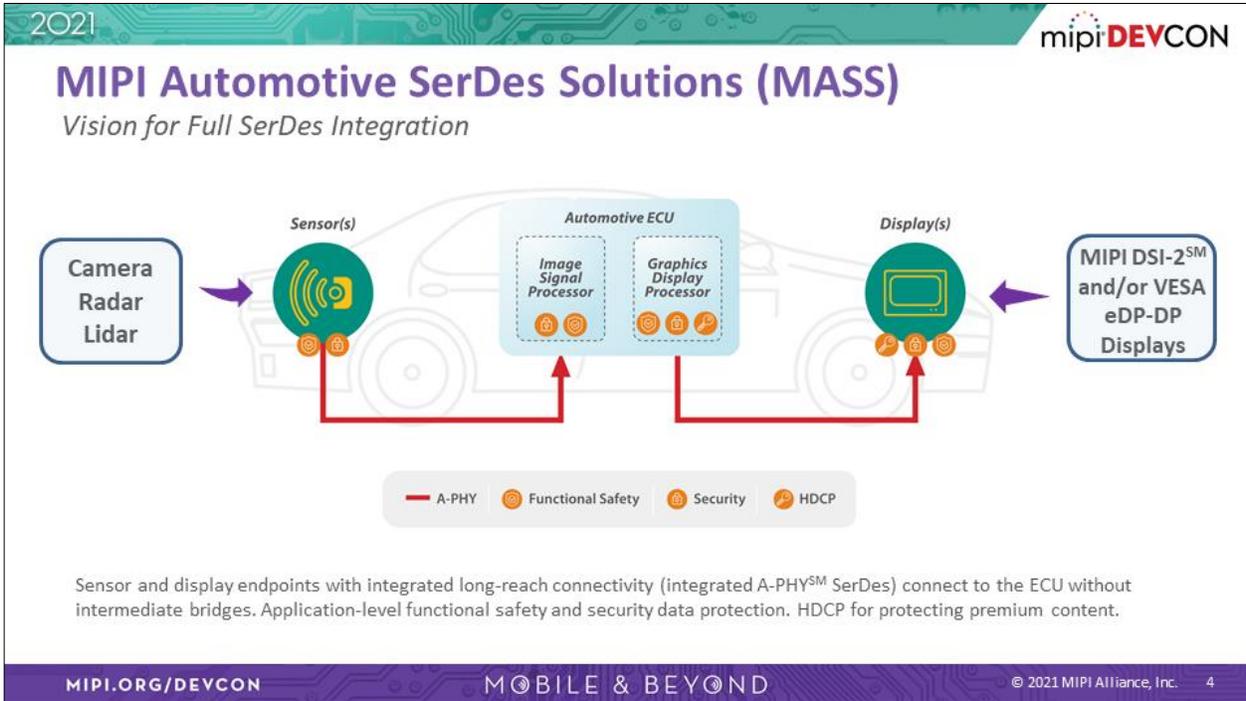
James Goel: 许多汽车的应用都受到全新产业趋势所驱动，亦即 CASE 四个字母各自代表的联网 (connected)、自动化(automated)、共享(shared)和电气化(electrified)。互联汽车使用先进的 LTE 和 5G 网络来增加网络带宽并驱动更高分辨率的显示器。先进的自动化，让新的应用程序有更充分的时间运用更高解析、更丰富的联网显示器以及联网传感器。共享是自动化的自然结果，让应用程序藉由互连的 GPU 和 ECU，有更多机会采用端到端相机和显示器。电气化需要低功率的照明和高效率的显示器。传统的汽车应用程序，持续要求提高相机和帧率的分辨率，同时降低功耗和电气干扰容限。

MASS Functional Safety Application

Digital Side Mirror Replacement



James Goel: 我们以汽车座舱的特定显示器为例，说明 MASS 如何让显示器得以支持更严格的功能安全目标。图中看到一个位置较低（low profile）、广角的汽车相机传感器，搭配嵌入式显示器，取代了传统的乘客座侧后视镜。改用数字后视镜之后，先进的光学系统减少了驾驶人的盲点，在夜间、低能见度、恶劣天气条件下也依然能发挥作用。它还具有额外的传感器功能，能侦测驾驶人可能看不到的物体和汽车。如图所示，汽车 ECU 分析了感测数据，并在屏幕上数字呈现了额外的安全标志和警告符号。这项应用中的车载显示器具有严格的安全目标，需要基于适当汽车危害分析的 ASIL D 认证。要能如此完整汇整，需要额外的像素信息，确保能符合 ISO26262 确立的 ASIL D 定义。



James Goel: MASS 系列规范专为端到端功能安全和未来的安全而设计。图中左侧的镜头雷达使用 MASS 规范来撷取数据，并通过功能安全和安全协议予以保护，标记来自传感器和 ECU 的完整图标，再到显示器。不同区块分别通过 A-PHY SerDes 接口完成这一切。ECU 图像讯号和图形显示处理器会协助显示器产生新的像素输出数据。通过 A-PHY SerDes，MASS 规范可以替显示处理器输出的像素提供安全保障，最终来到玻璃显示器的部分。端到端 MASS 的作法有时称为玻璃到玻璃，因为它从传感器捕捉到光的瞬间启动，一直到光线离开显示器为止。

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 系列为汽车功能安全标准。在许多其他参考设计和要求中，这些标准定义了属于汽车领域中，以汽车安全完整性级别(automotive safety integrity level, ASILs)的风险基础方法 (risk-based approach)，简称 ASIL。ASIL 用于检索适用的 ISO26262 规范，用于避免在应用安全目标定义中的不合理剩余风险 (unreasonable residual risk)。MASS 显示器规范采用 ISO26262 Part 5 产品开发的硬件层级规范，作为显示器绘图管线的安全基础。具体来说，附录 D 丰富提供诊断覆盖率详细指南信息，能针对合规所需的单点故障和潜在故障指标进行诊断评估，同时也能评估随机硬件故障所导致的安全目标违规情况。

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 提供了硬件故障模式分析，而显示器安全工程师在尝试符合显示器安全目标时可以参考。表 D6 定义了适用于 MASS 规范下的显示器接口的安全机制和关键性能测量建议。下面四行以及红框文字概述的机制，可结合起来提供高级、典型、可实现的诊断覆盖率。这些机制包括：使用 CRC-32 编码的信息冗余、使用独特 16 码的分帧计数器以及使用倒数计时机制的超时监控。如表中最后一行所述，这三种机制的组合提供了可实现的高覆盖率。

Adding Service Extensions Packets (SEPs)

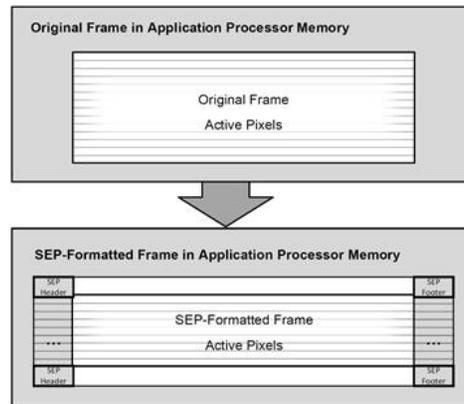


Figure 23 SEP Formatting in the Display Source

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

James Goel: MIPI 的显示服务扩充功能(Display Services Extensions)、或说 DSE 规范定义了一种新的数据封包、如同附件 D 表 D0.6 中描述的安全机制类型。在 DSI-2 协议编码器把像素转换为位的过程中, 计算出来这些服务扩充封包 (简称 SEP)。本图说明了在 DSI-2 长数据封包(long packets)定义的视频中, SEP 数据封包如何被置放在每个结束与开始的行列的起始点。SEP 标头和结尾数据封包, 也保护 DSI-2 短数据封包的命令和控制接口。DSI-2 的 MIPI 协议适配层, 定义了 SEP 数据封包的需求; 当 DSI-2 长短数据封包转换为 A-Packets、数据分帧并通过 A-PHY 发送时, 也必须通过 DSI-2 的 MIPI 协议适配层。

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.

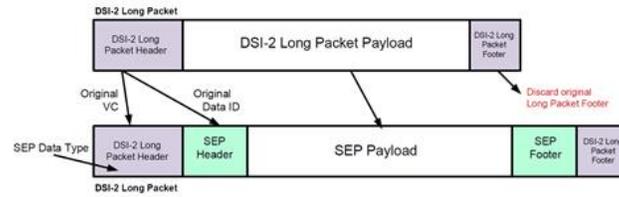


Figure 20 Converting DSI-2 Long Packet to SEP Within DSI-2 Long Packet

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

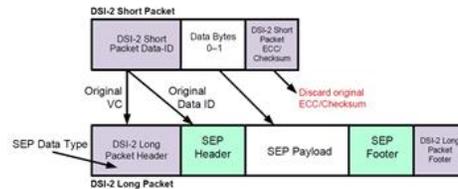


Figure 21 Converting DSI-2 Short Packet to SEP Within DSI-2 Long Packet

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

James Goel: 这张图说明了 SEP 标头和结尾数据封包，如何包覆 DSI-2 的短数据封包和长数据封包。DSI-2 长数据封包的有效载荷和 SEP 标头，用于计算位于 SEP 结尾中的 CRC-32 值。这些数据封包组合起来，形成新的播放有效载荷，构成一组新的、可能会通过 A-PHY 传输的 DSI-2 长数据封包。DSI-2 短数据封包的转换，也是通过一样的过程。

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]	HDCP streamCtr[31..0]																															
ePH[6]	HDCP InputCtr[31..0]																															
ePH[7]	HDCP InputCtr[64.32]																															

Table 2 SEP Packet ePF Blocks: Overview

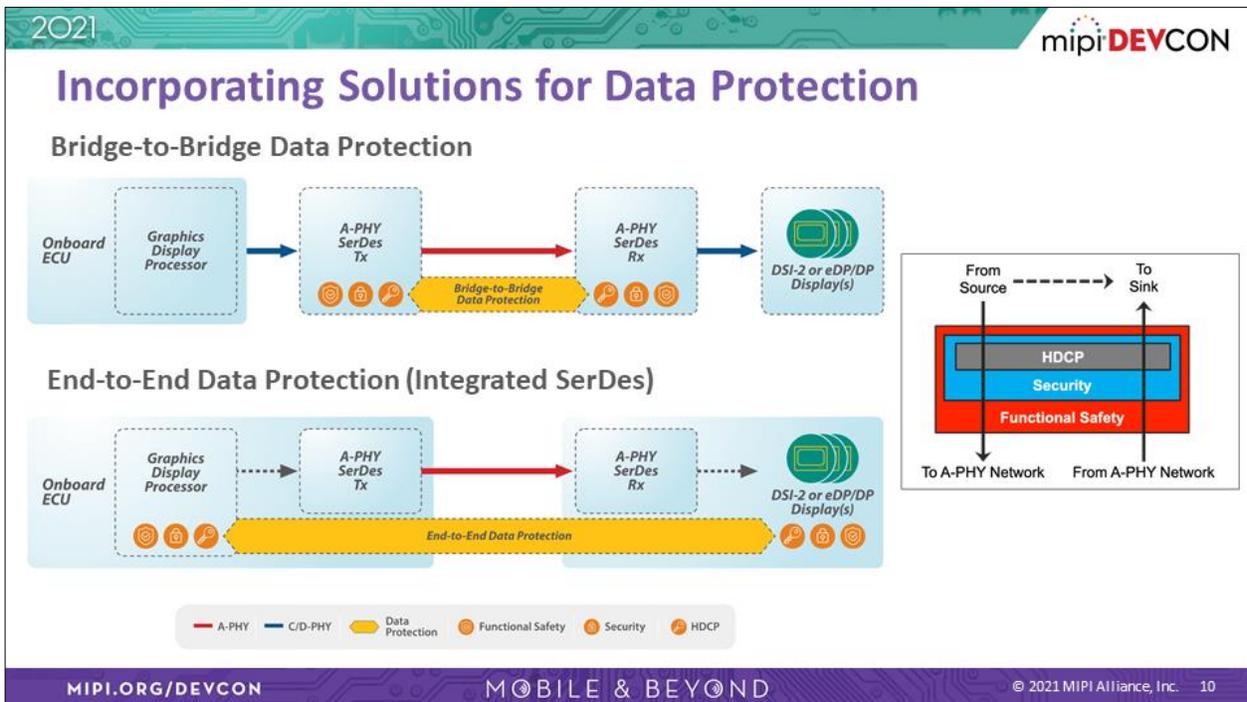
Bits	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
ePF[1]	Reserved																															
ePF[0]	CRC-32																															

MIPI DSESM v1.0

James Goel: 理解这些重要 SEP 数据封包的部分细节，深具启发。SEP 数据包头的前 32 个位（ePH zero），包含了定义 SEP 有效载荷格式的 eDP（扩展数据类型）。DSE 规范目前支持 MIPI DSI-2 和 MIPI PAL，适用 VESA、eDP、DP、SEP 的有效载荷类型。ePH-2 内含 SEP 16 位信息计数器。这是 SEP 2.0 版本，是第一个通过配置功能安全显示器、并以分帧会话传送的数据封包，针对每个已传输的 SEP 数据封包，发送器也会逐步加一增强。显示器应用程序，可能会选择在每行活跃影片开始时、或在 SEP 数据封包传输过程中以其他应用程序指定的特定时间，重置信息计数器。

信息计数器的关键值，是要标记出唯一且具有单调递增值的 SEP 数据封包。如果终端显示接收端译码了 SEP 信息计数器，并跳过、重复或错过了下一个序号值，就必须断言（assert）错误条件，采取适当的系统层级行动，例如显示器上闪烁错误警告。

要实现超时监控（timeout monitoring），也可以在既定数量的垂直接收讯号范围内，通过显示器追踪译码的 SEP 信息计数器值的有效性。帧率为已知，因此垂直接收器之间的 SEP 信息计数器值的数量会指示主机是否已在给定阈值内停止发送显示数据。这对于特定的安全图标至关重要。



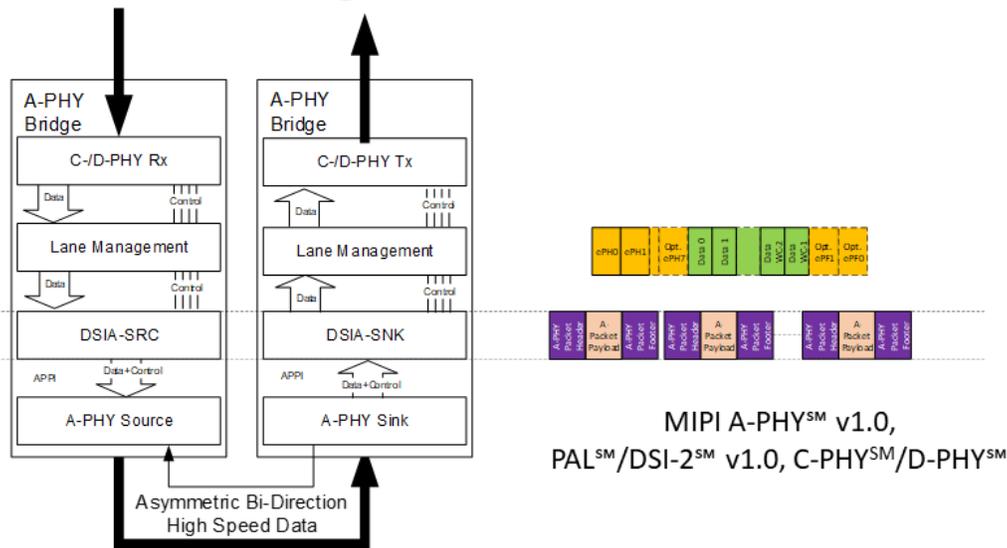
James Goel: 本图解释了 MASS 显示器的功能安全性，以及未来在安全系统层级的作法。上图显示了最适合目前既有 ECU 和显示器的网桥间 MASS 解决方案。左侧的 ECU 会生成源像素数据，使用标准 MIPI DSI-2 或 VESA eDP 原生接口，连接到 A-PHY 发射网桥。以蓝色箭头表示。

A-PHY SerDes 发射器会通过 MIPI 协议适配层或 PAL 规范，把原生像素串流转换为 A-Packet，并受功能安全、安全或 HDC 保护。A-PHY SerDes 会接收、验证 A-Packets 的功能安全、安全性、HDCP 完整性，然后通过相同的 PAL 规格把 A-Packets 转回原生 DSI-2 或 eDP 像素。

在这个例子中，FuSa 和安全性只建立在 MIPI A-PHY 网桥之间。第二张图勾勒出完全整合 A-PHY 的 MASS 显示架构，在显示器像素的生成过程中加入功能安全和系统安全，并通过 A-PHY 连接到最终端，直到显示器译码数据并发送到屏幕。这是 MASS 端到端显示器解决方案的典型案列，因为完全整合的 A-PHY 案列不需要 A-PHY SerDes 网桥。不过要等到市场完全采用这种解决方案，还需要时间。

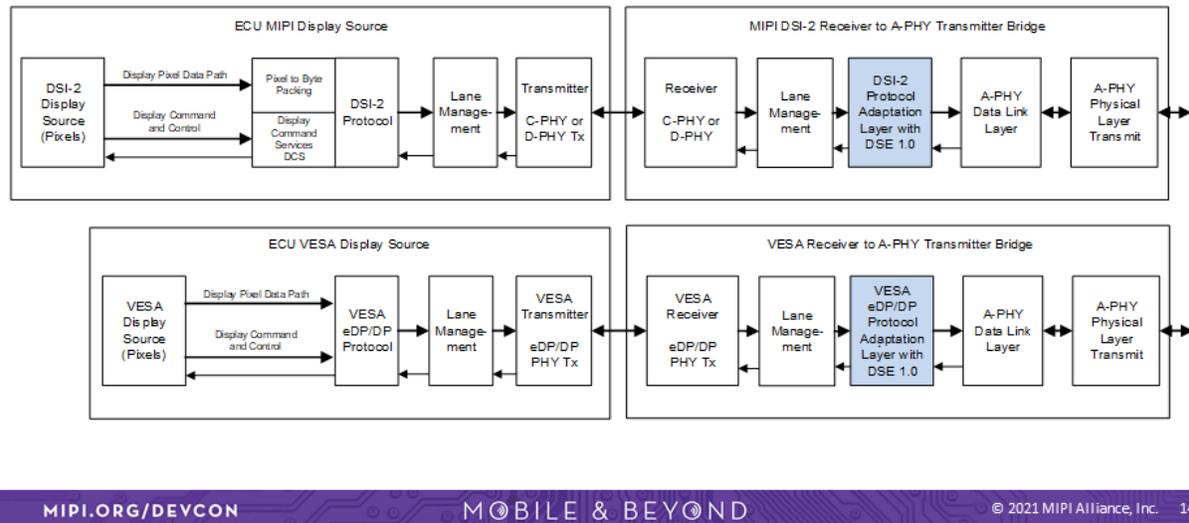
接下来几张投影片中会看到，不整合 A-PHY SerDes 网桥也可以达到 MASS 端到端功能安全和安全性，只需把整合的 MIPI 显示服务扩充功能规范，应用在下一代 DSI-2 ECU 内嵌协议生成器中。

Detailed A-PHY Bridge PAL



James Goel: 图中左侧，是 DSI-2 接收器传送到 A-PHY 发送器。在右侧，是 A-PHY 接收器回到 DSI-2 发送器。左边的网桥收到 DSI-2 长封包和短封包，通过 DSI-2 或 PAL 规格的协议适配层，将之转换为正确格式的 A-Packets，以供 A-PHY 传输。在右侧方块里执行的步骤则相反，重新产生 C-PHY 或 D-PHY 发送的原始 DSI-2 长短数据封包。最右侧的协议有效负载叙述，说明如何复原 DSI-2 数据封包并分帧为 A-Packets。A-PHY 规范也叙述了相关细节。

MASS Legacy ECUs with an External A-PHY Bridge

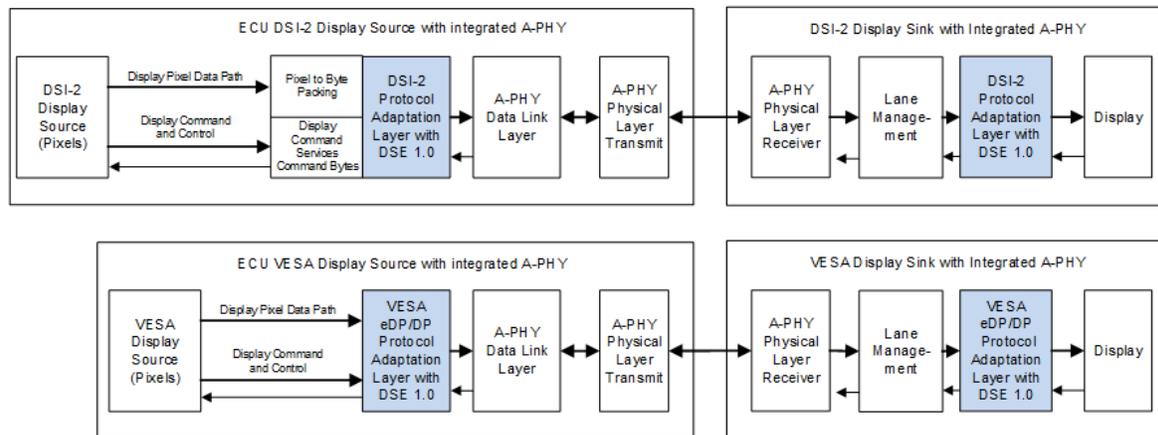


James Goel: 这两个图将之前的垂直汽车协议栈区向上转换为详细的水平数据管道。传统汽车 ECU 显示源仅产生原生的 DSI-2 或 VESA EDP，仍可以利用 MASS 显示规范来提供功能安全及安全性，未来也能提供 A-PHY 网桥间的安全性。

第一张图说明了使用 DSI-2 和 C-PHY 或 D-PHY 发射器的 MIPI 传统显示源和接收器。该 ECU 连接到外部 DSI-2 到 A-PHY 网桥。传统 ECU 具有传统的 DSI-2 接口，协议中并未加入 FuSa 或安全性。一旦 A-PHY 网桥接收到数据，DSI-2 的协议适配层会在像素数据通过 A-PHY SerDes 接口传输之前，通过 DSE 规范增加功能安全性，并在未来增加安全性。

第二张图显示了传统 VESA 发射器的类似配置。在 A-PHY 传输数据前，协议适配层或 VESA EDP 增加了功能安全性，未来也会加强安全性。

MASS New ECU with Integrated A-PHY

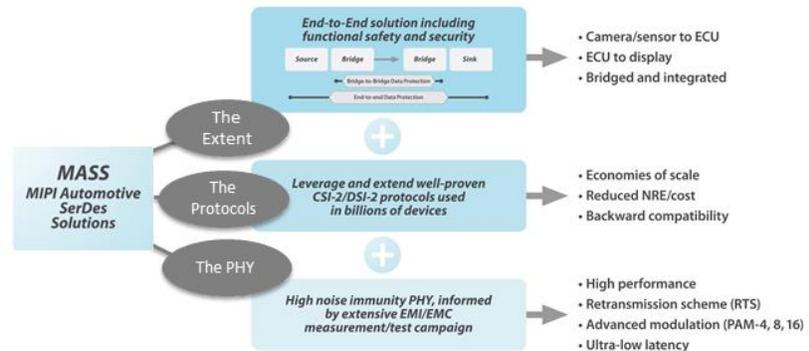


James Goel: 本图说明 MASS 如何应用已经完整整合 A-PHY 的全新 ECU。这些搭载完整整合 MASS 显示规范的新 ECU，可以利用到完整端到端功能安全性的优势，未来也能享受协议适配层使用的显示服务扩充的安全性。以上两张图中，协议适配层在像素协议和编码管道启动时，就完整整合到 ECU 里，藉此确保 DSI-2 和 VESA 都能含括功能安全，未来在 DSI-2 和 VESA DP 原生串流中包含安全性。像素串流在 A-PHY 中全程受到保护，直到最终的像素协议译码器，再到玻璃显示部分。

James Goel: 这张投影片列出了以上讨论的 MASS 延伸详细讯息与链接。接下来交给 Rick 来谈谈安全性。

Security within the MASS Guiding Principles

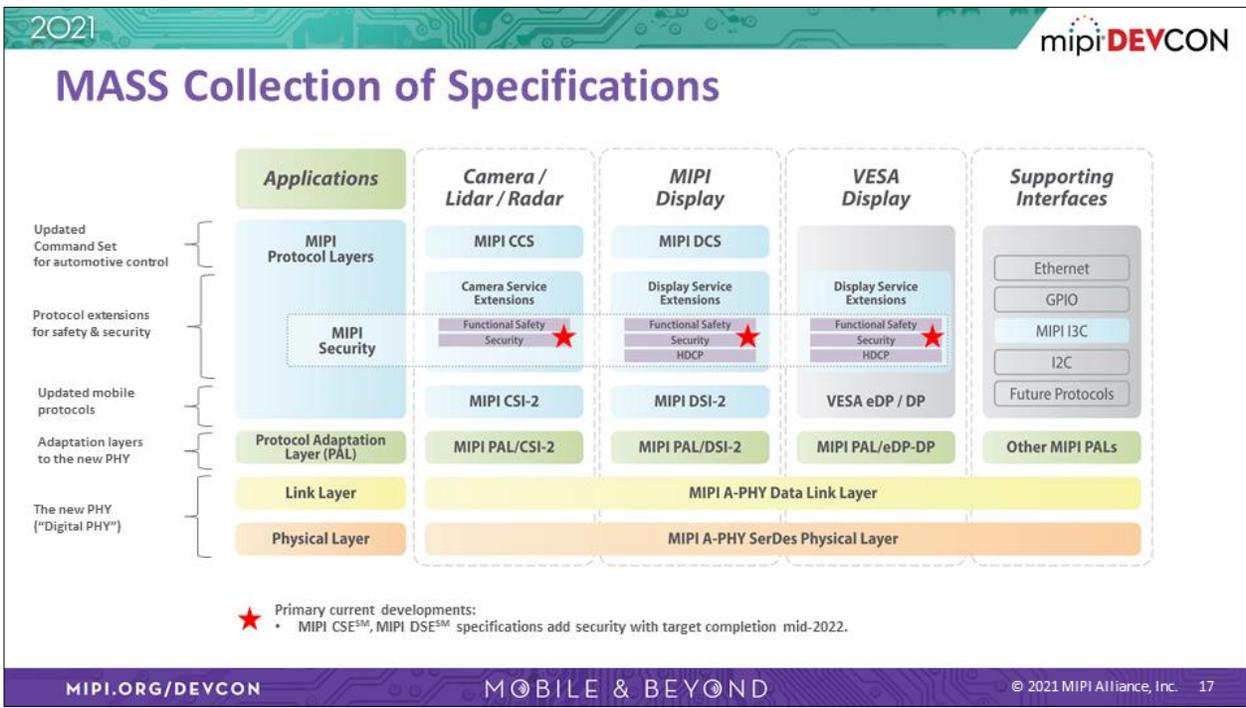
- MASS Guiding Principles
 - The Extent
 - The Protocols (CSI-2SM, DSI-2SM)
 - The PHY (A-PHYSM)
- MIPI Security is implemented as extensions to CSI-2 and DSI-2 protocols.
- This enables the Security to achieve an “end-to-end” **extent**, or **reach**.



Rick Wietfeldt: MASS 的安全及指导原则。

MIPI 安全性基于三个指导原则。第一：PHY，第二：协议，第三：范围。这些是 MASS 协议的三个指导原则。

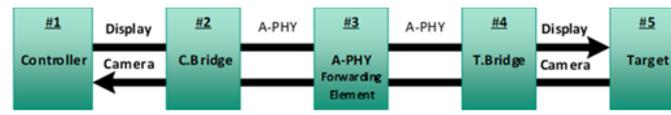
MIPI 的安全性，实践 CSI-2 和 DSI-2 协议的扩充，让它可以在许多生态系统中广泛使用。藉由将安全性附加到协议中，实现端到端范围的安全性。您可以在图的上部看到桥到桥和端到端数据保护。



Rick Wietfeldt: 接下来我们讨论 MASS 规范。您可以看到两个主要应用程序—相机和显示器。相机、光学雷达和雷达视为同一类。显示器分两种规格，MIPI DSI-2 和 VESA DisplayPort。您可以在栈区中看到 MIPI 安全（含有同一层内的功能安全和安全保护），直接附加在 CSI-2、DSI-2 和 DisplayPort 协议之上。最下面显示了 A-PHY 数据链接层和物理层。安全性基本上是在协议层级实现，达成前述的端到端范围。

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: 这一页说明高阶系统和安全要求。

根本上来说，安全性包括三个关键要素：数据身份验证，在组件之间建立信任级别；讯息完整性，确保讯息在传输过程中没有被修改；机密性，藉由加密实现。依据下面显示的 MIPI 1:5 模型来参考 MIPI 中的数据保护。下一页会更清楚说明。

基本上，安全是由中央控制器以一对一的方式与其他组件进行管理，而非偏向点对点类型的安全模型。例如，数据安全可以在控制器#1 或其网桥#2 中启动，并在#4 或#5 中终止。相机安全可以反向启动，从#5 或#4 开始，并在#1 控制器或其网桥中终止。接下来我们将详细讨论 1:5 模型。

MASS System Model: The 1:5 Model

Security Model Components

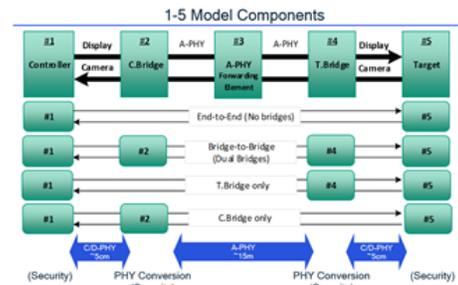
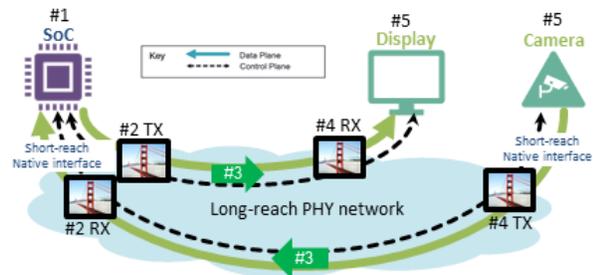
- #1: Controller (SoC)
- #2: Controller Bridge (C.Bridge)
- #3: Forwarding Element (aka Repeater)
- #4: Target Bridge (T.Bridge)
- #5: Target (Camera or Display)

Security Requirements

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

System Requirements (End-to-end)

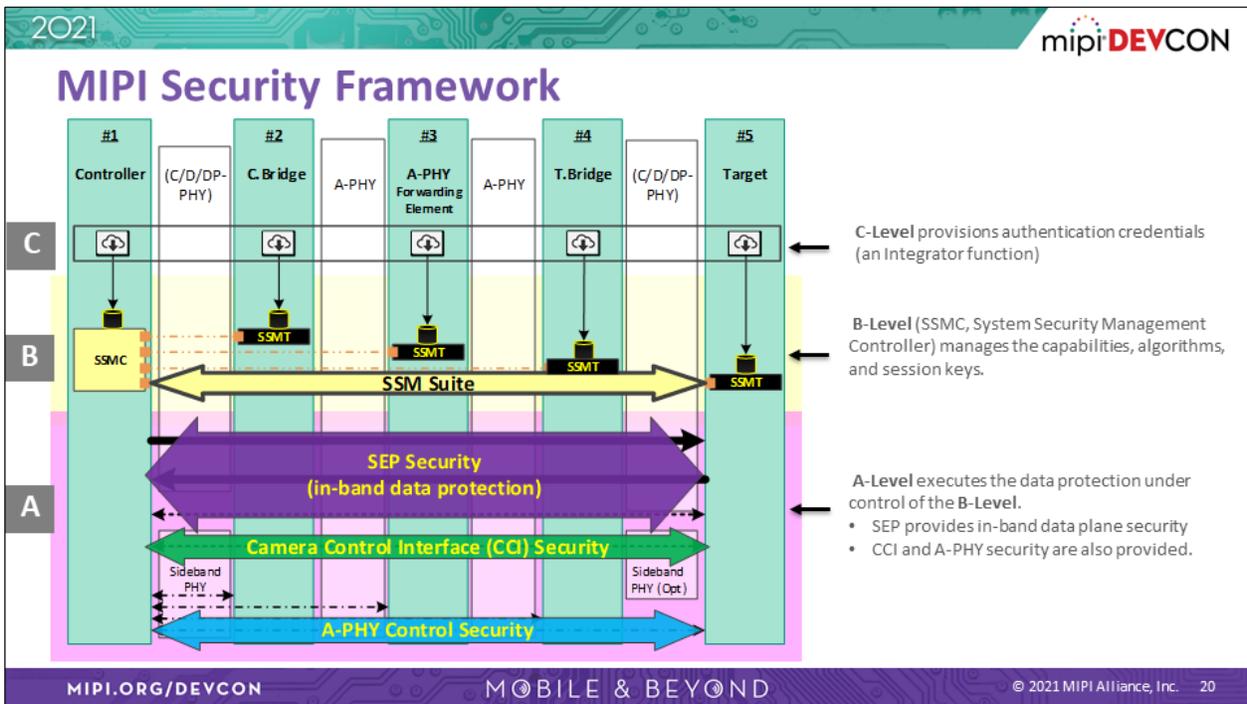
- Multiple system topologies (e.g., 15, 1245, 145, 125)
- End-to-end extent via protocol extensions
- Security for Data plane, and Control plane in-band/sideband
- Highly flexible operation, such as Heterogenous operation for displays, supporting DSI-2 and DP on a daisy chain.



Rick Wietfeldt: 这一页更详细地显示了 1:5 模型。从图形上看，您可以在相机中看到显示器，标记为 #5，通过网桥 #4 连接到 A-PHY 网络。A-PHY 网络另一端是其他网桥，分别连接到 SOC，#2 和 #1。因此可以看到在特定时间内，特定系统中这些组件会有许多不同变体。

右下角可以看到全部五个，一次两个，以不同方式排列。系统要求如我们先前讨论一下包括了身份验证完整性和加密。

某些系统要求从在根本上是基于端到端的范围，亦即协议层确保安全的能力。显示器和相机的数据层和控制层自然都有相关安全需求。另外还可以进行一个很灵活的操作。例如，在菊花链拓扑 (daisy chain topology) 的显示器情况下，其中多个显示器以菊花链拓扑连接到控制器，一些显示器可能是 DSI-2，另一些可能是 DisplayPort，并且安全性不会因为端对端的方式有所妥协。



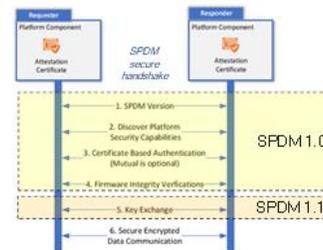
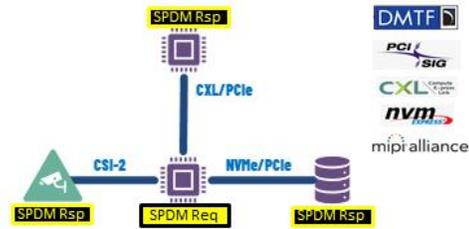
Rick Wietfeldt: 这里我们说明 MIPI 安全框架，通常称为 ABC 模型。这里我们有 1:5 模型和 ABC 模型。在最上层，C 层提供身份验证凭据。这是一个整合器功能——可以想象一枚 USB 快闪硬盘把密钥推给每个组件。也可以根据整合商的需要，通过无线或以太网络连接进行自动化。

目前这不在 MIPI 规范中，MIPI 确实指定了 B 层级和 A 层级。您可以把 B 层级设想为称为 SSMC（系统安全管理控制器）的软件功能。底部的 A 层级则是在更高级别的 B 层级控制下执行数据保护。可以想象成这是进行加密的硬件，完整保护讯息，支持三种不同级别的安全性 - A-PHY、相机的 CCI，以及显示器和相机数据层的 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 的安全规范采用简称为 SPDM 的 DMTF.org 规范，业界多个组织也采用 DMTF，包括 PCI-SIG、CXL、NVMe，以及新近的 MIPI。SPDM 参考 TLS 模式建立，TLS 正是全球网络使用的安全框架。

基本上有两大步骤。会在通讯初始化（handshake）之后建立经验证的会话密钥，然后发送会话密钥，保护数据层和控制层的数据。SPDM 讯息再次采用通用定义，但在 MIPI 情况中，这些讯息通过 DSI、CSI-2 以及 CCI 或 I2C 传送，以便单独保护每个传输，如上一张投影片所示。

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: 简言之，MASS 规范为当今初版的 CSE 和 DSE 的相机和显示器，提供了功能安全解决方案。这些完整规范可供 MIPI 会员使用。CSE v1.0 和 DSE v1.0 规范正在更新，支持 CSI-2、DSI-2 以及 CCI (I2C) 边带的安全性。MIPI 安全性的关键要素之一，是协议本身的安全性置于何处，才能达成使用或不使用中间网桥的端到端数据保护。如此也得以运用像是 TLS 这样的[传输]层安全性，与 MACsec 等连结层安全性形成对比。

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