Software Manageability & Security

Agenda

- High level goals
- Chiplets – Attach model, challenges and solution stack
- System Topology examples
- SW View of integrated device – Host & Switch
- DVSEC Register Overview
- D2D Adapter/PHY, Implementation Specific Registers
- Manageability Overview
- Security Overview
- Summary

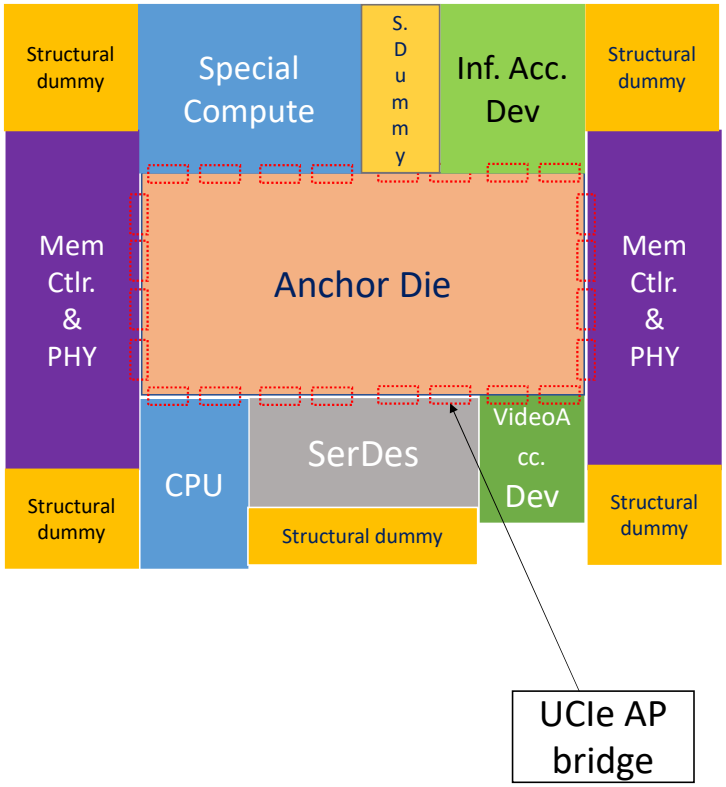
High level Goals

- Enable systems in package (SIP) solutions
  - Focus on flexibility and ease of deployment to accelerate ecosystem development
- Compatible with existing SW for fast adoption
  - Builds on PCIe/CXL SW constructs (DVSEC, Host register blocks, Etc.) and interfaces
  - Link can be managed by FW (for pre-UCIe OS) or natively by UCIe-aware OS
- CXL/PCIe protocols supported
  - Streaming protocol support is vendor-defined
- Reduce complexity wherever possible to allow efficient UCIe implementation
  - e.g., No RCiEP in UCIe IPs

Flexible architecture; backward compatible SW; Extensible/flexible for future usage models

Chiplet Attach/Usage Model

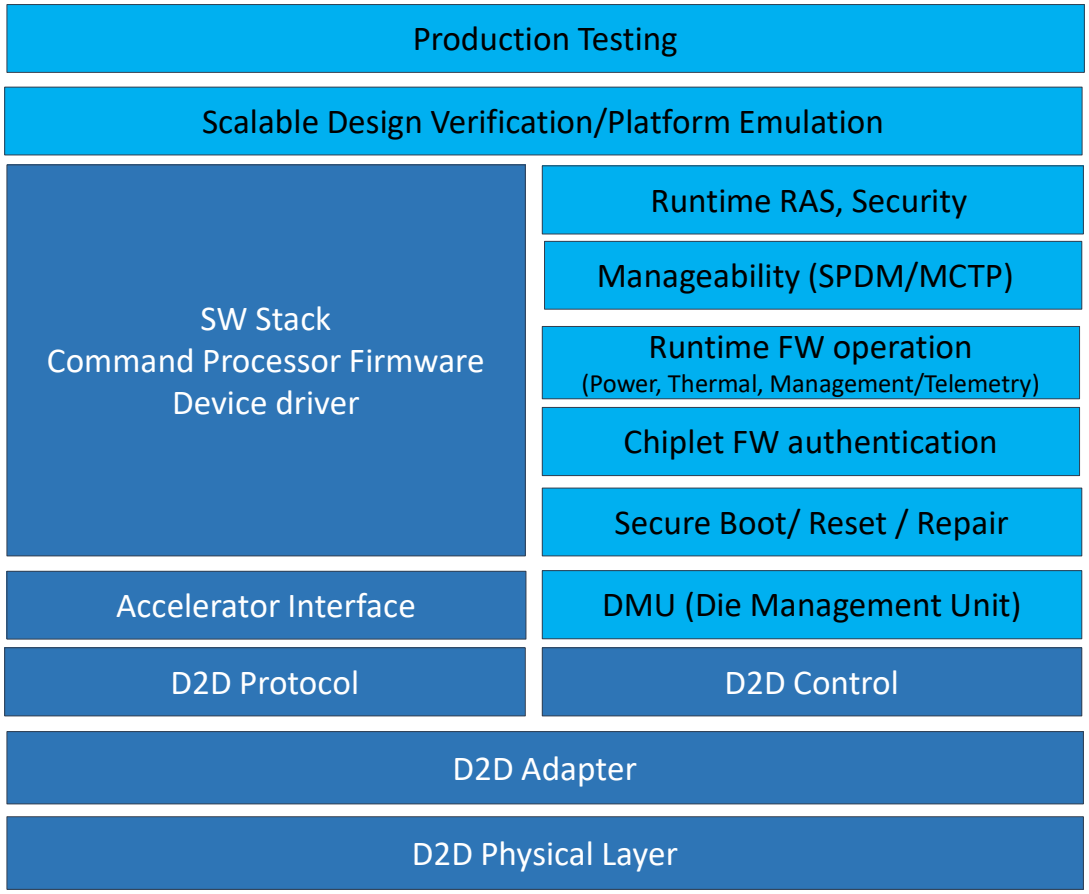
- Pcie/CXL device (well established)
  - Software/driver
  - Address translation
  - Error isolation and recovery
  - Use Cases: Inference, video, crypto, compression, networking functions, etc.
- SerDes I/O chiplets
  - Use case: Pcie 32G/64G/128G ; Ethernet 50G/100G/200G ; CPO
- Memory Controller+PHY chiplets
  - Simple protocol desired for standardization
  - Streaming protocol supported for proprietary use case
  - Use Case: Flexible memory technology (HBM / DDR / LPDDR / G6 /..)
- Generic compute attach
  - Standard coherency architecture like CXL (simplified) or CHI



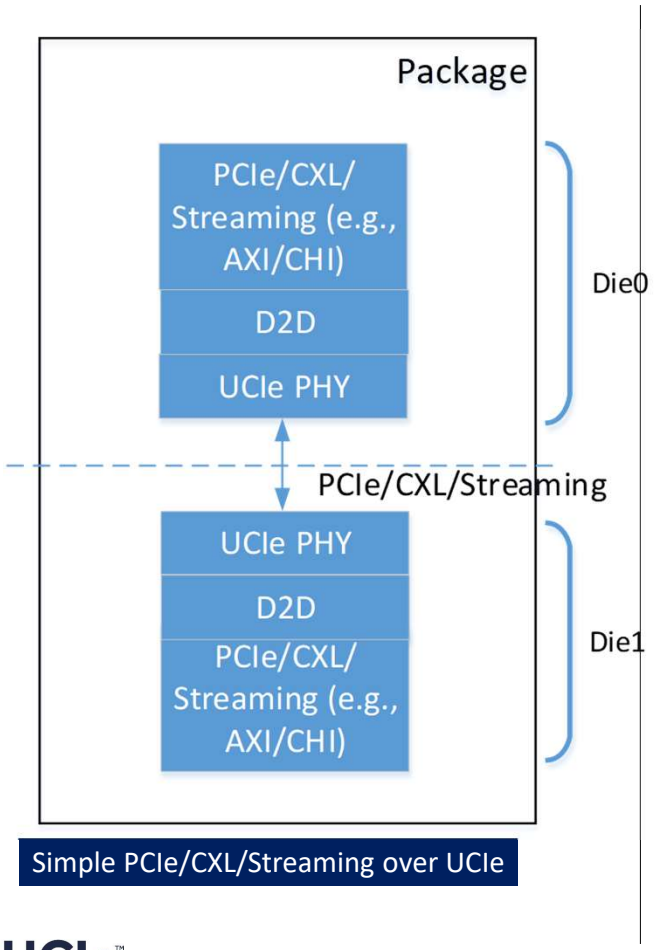
Chiplet Ecosystem Solution Stack

PCIE/CXL DEVICE INTEGRATION MODEL

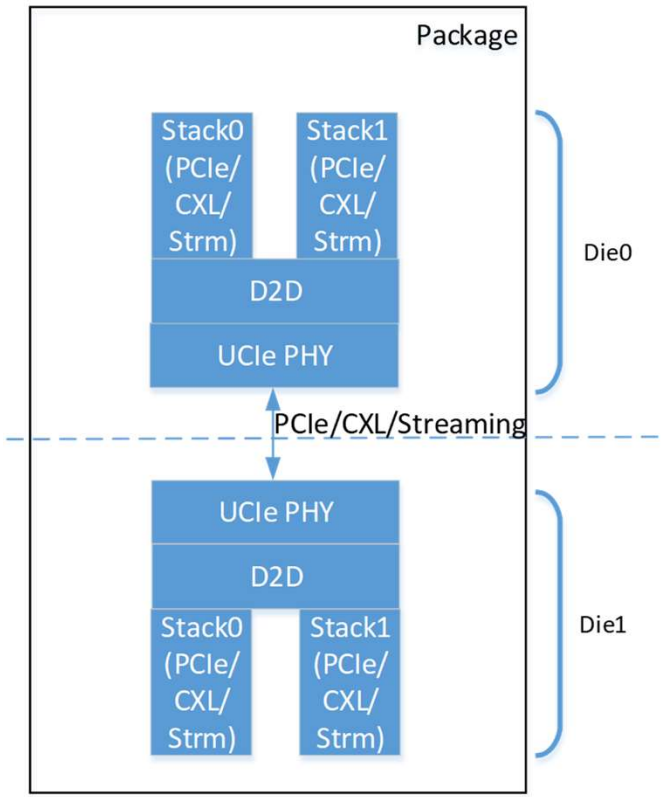
- Two independent hardware stack
  - Protocol and Control
- Die management unit (DMU)
  - Hardware + Firmware
- Standard control and management software interface
- Platform specific firmware
- UCIe starting to tackle software interfaces



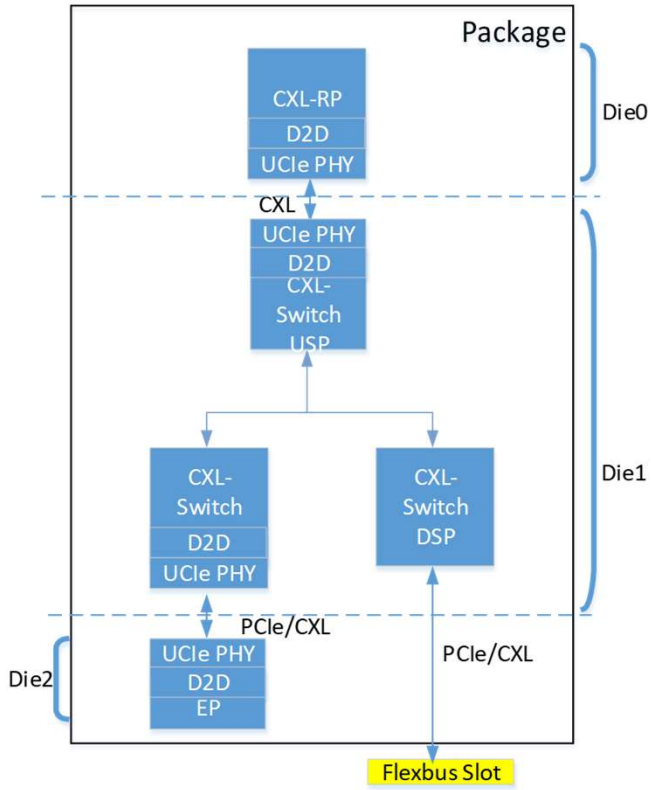
UCIe System Topology Examples



Simple PCIe/CXL/Streaming over UCIe

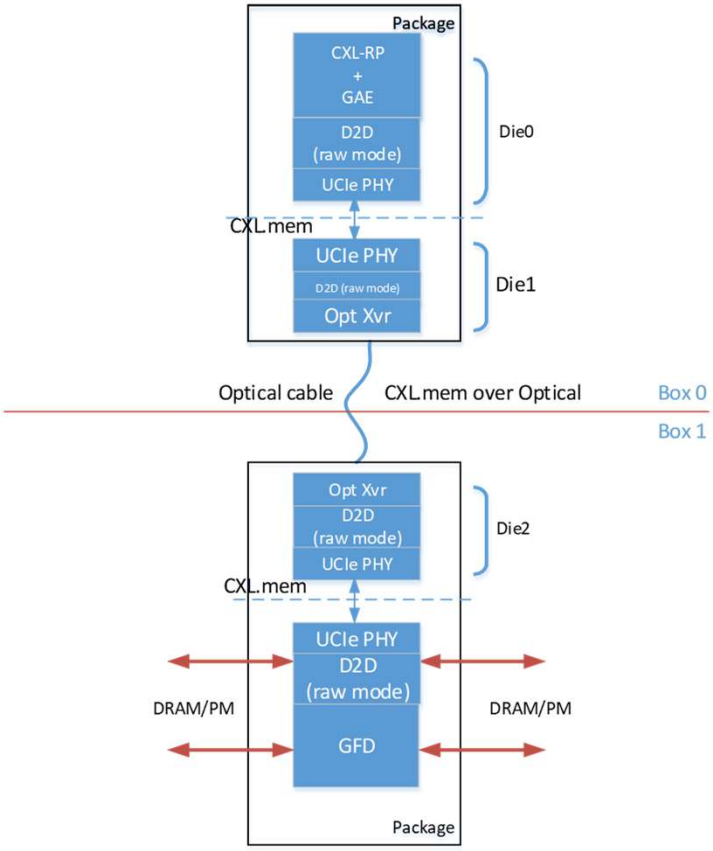


Multiple protocol stacks over UCIe

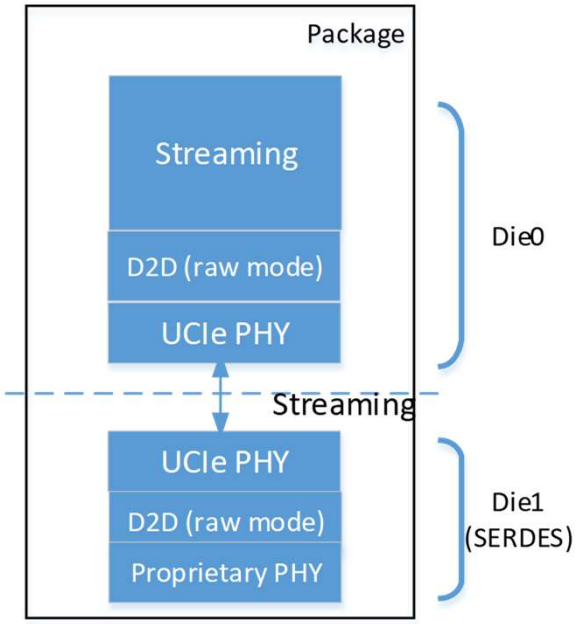


Switched PCIe/CXL over UCIe

UCIe System Topology Examples



Disaggregated Memory with UCIe Optical

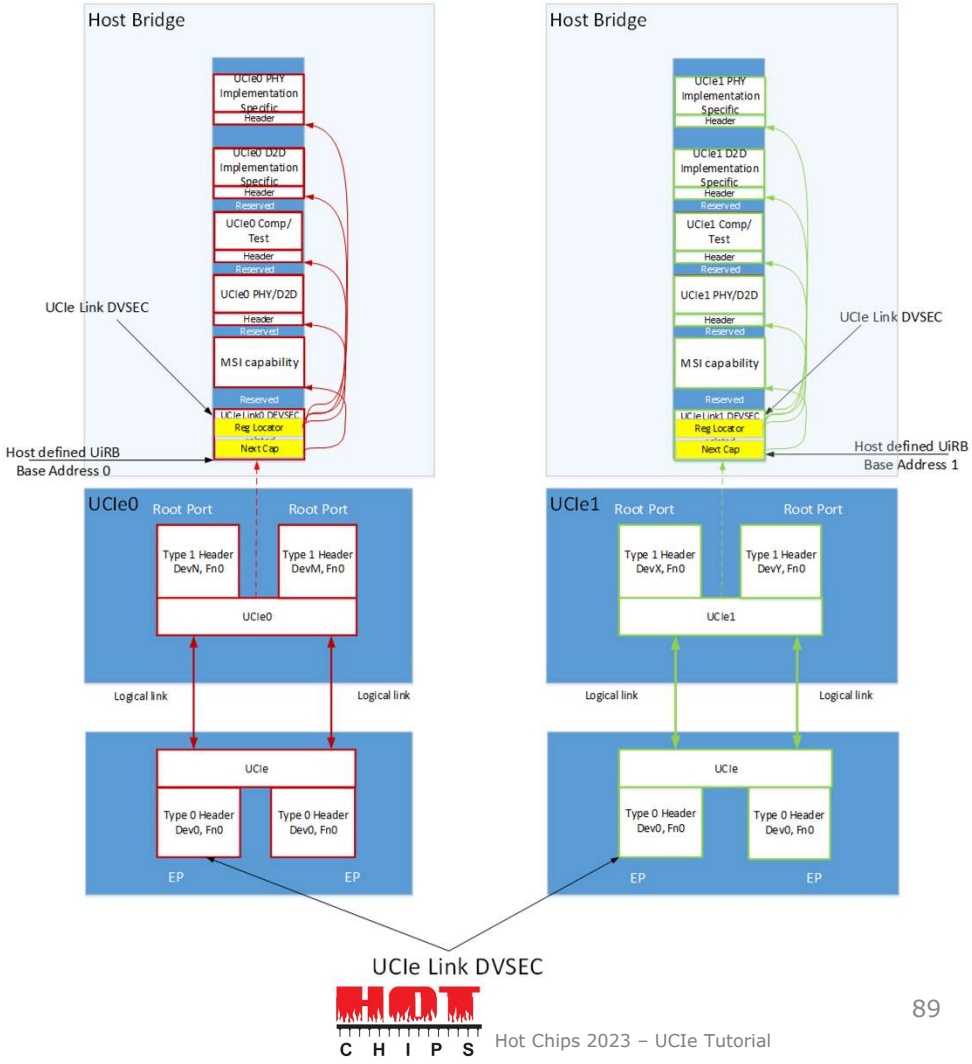


Proprietary SERDES solution with UCIe

SW View of integrated Device – Host side view

- Host
  - UCIe links discoverable by OS through UCIe Early Discovery Table (UEDT [1]) populated by FW
  - UCIe link details enumerated via new Link-DVSEC capability in Host-specific Register Block (UiRB)
- EP/Switch USP
  - UCIe enumerated via new DVSEC

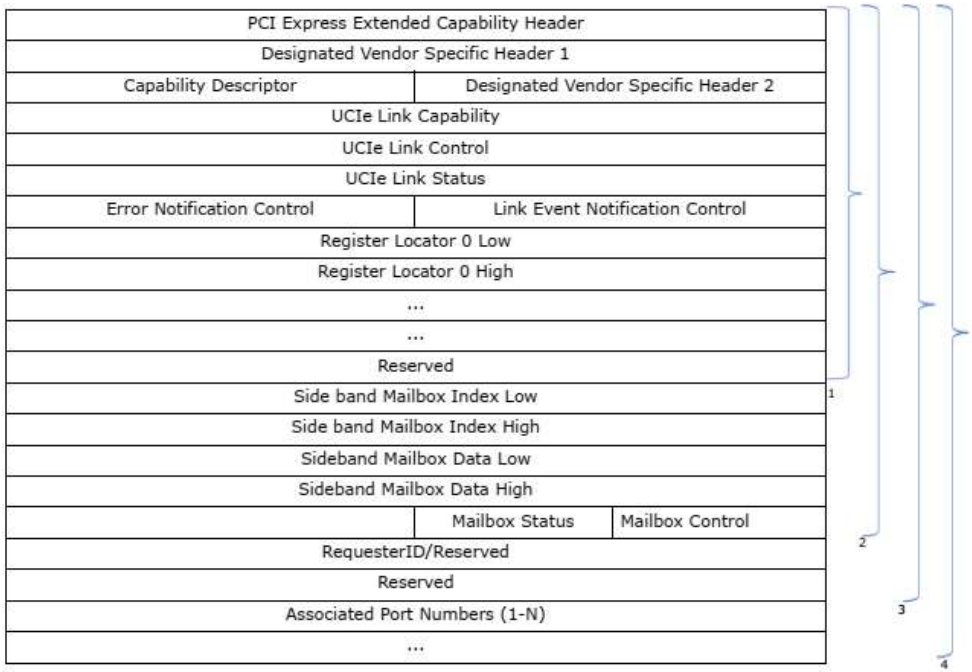
Industry standard PCIe/CXL SW model for UCIe enumeration and control



[1] **Detailed in 1.0 Errata document**

UCIe Link DVSEC – For basic Link Functionality

- New UCIe DVSEC with UCIe Consortium ID of 0xD2DE
- UCIe Link Capabilities, Control, Status
  - Link width/speed, Stack support, Packaging type, (re)train Etc.
- Error/Link Event Notification Control/Status
- Register Locators
  - For registers beyond the basic functionality in DVSEC – Test/Compliance, Implementation specific, D2D/PHY
- Mailbox
  - For sideband access of far-side chiplet's UCIe registers, for debug
- Associated DevFn
  - For enumerating interdependent RP/DSP links in a multi-stack UCIe scenario



1 applies to UCIe-EP, UCIe-USP, UCIe-Retimer

2 applies to UCIe-EP, UCIe-USP when paired with a retimer

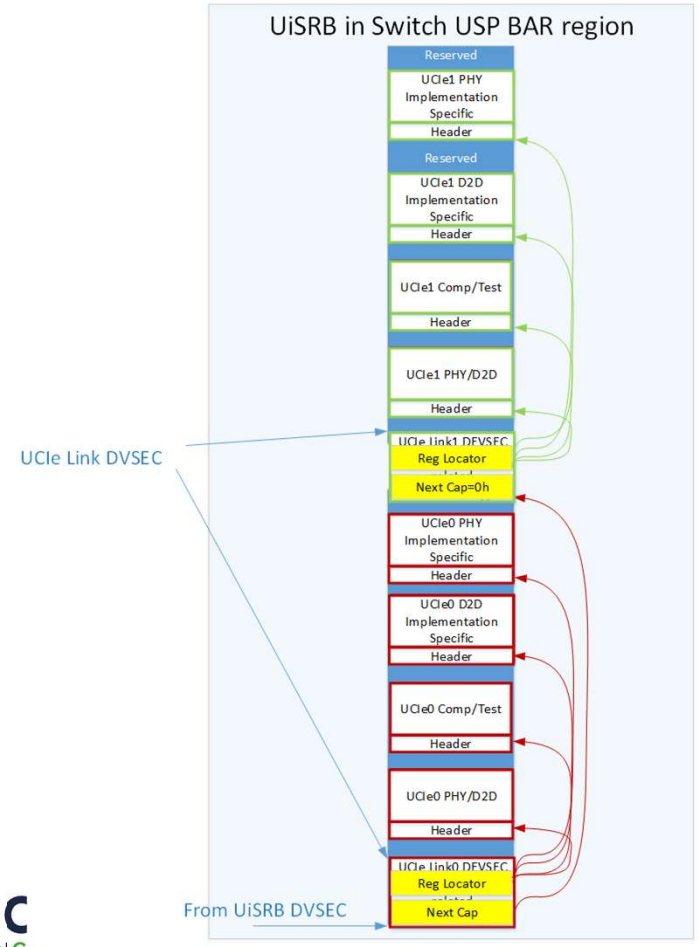
3 applies to UCIe-RP

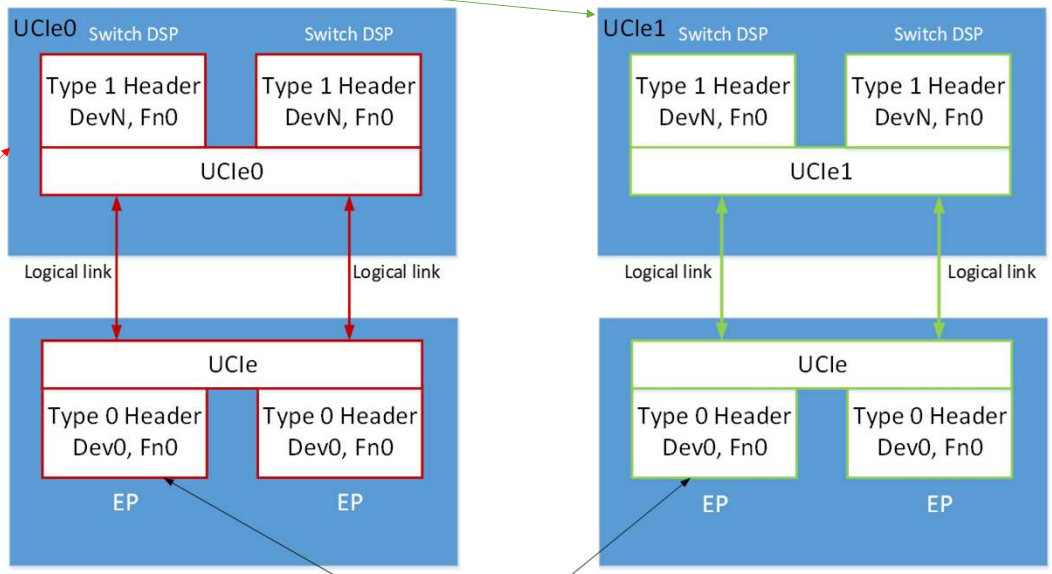
4 applies to UCIe-DSP

Switch side view

Industry standard PCIe Model for UCIe enumeration and control

- UCIe on PCIe/CXL Switch DSP
  - Enumerated via new UCIe Switch Register Block (UiSRB) DVSEC capability in Switch USP





UCIe Switch Register Block (UiSRB) DVSEC

For Switch DSP UCIe Discovery

- Provides the Base address for enumerating UCIe links below Switch DSPs
- Included in Switch USP config Space
- Base address part of one of the BARs of the Switch USP

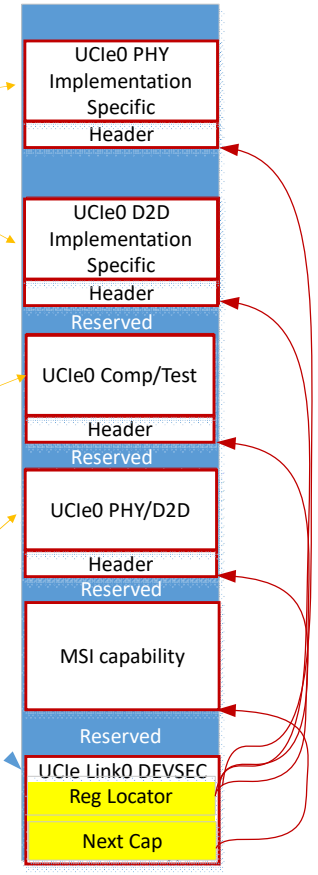
PCI Express Extended Capability Header	
Designated Vendor Specific Header 1	
Reserved	Designated Vendor Specific Header 2
UCIe Switch Register Block (UiSRB) Base address	

D2D Adapter/PHY, Implementation Specific Registers

Vendor-defined registers for PHY layer and D2D adapter separately[1] – VendorID part of Header

Being defined by Compliance/Test team

D2D/PHY error registers, Run time link testing, Repair control, Debug registers, Etc.



Upstream/Downstream Chiplet SW Compatibility

Downstream Device SW view	Upstream Device SW view			
	PCIe RP/Switch DSP[1]	CXL RP/Switch DSP[2]	CXL Downstream Port RCRB[3]	Streaming Device
PCIe EP/Switch USP[5]	Valid	Valid	illegal	Vendor defined (PCIe SW model recommended)
CXL Upstream Port RCRB[4]	Illegal	illegal	illegal	
CXL EP/Switch USP[6]	Valid	Valid	illegal	
Streaming Protocol	Vendor defined (PCIe SW model recommended)			

[1] PCIe RP/Switch DSP = PCIe Root Port/Switch DSP as defined in PCIe Base Specification

[2] CXL RP/Switch DSP = Standard PCIe RP/Switch-DSP with additional CXL Flexbus Port DEVSEC capability

[3] CXL Downstream Port RCRB = CXL 1.1 compliant Host/Switch downstream Port

[4] CXL Upstream Port RCRB = CXL 1.1 compliant Device/switch upstream port

[5] PCIe EP/Switch USP = PCIe Endpoint/Switch USP as defined in PCIe Base Specification

[6] CXL EP/Switch USP = CXL EP/Switch USP with additional CXL Flexbus Port DEVSEC capability

Summary

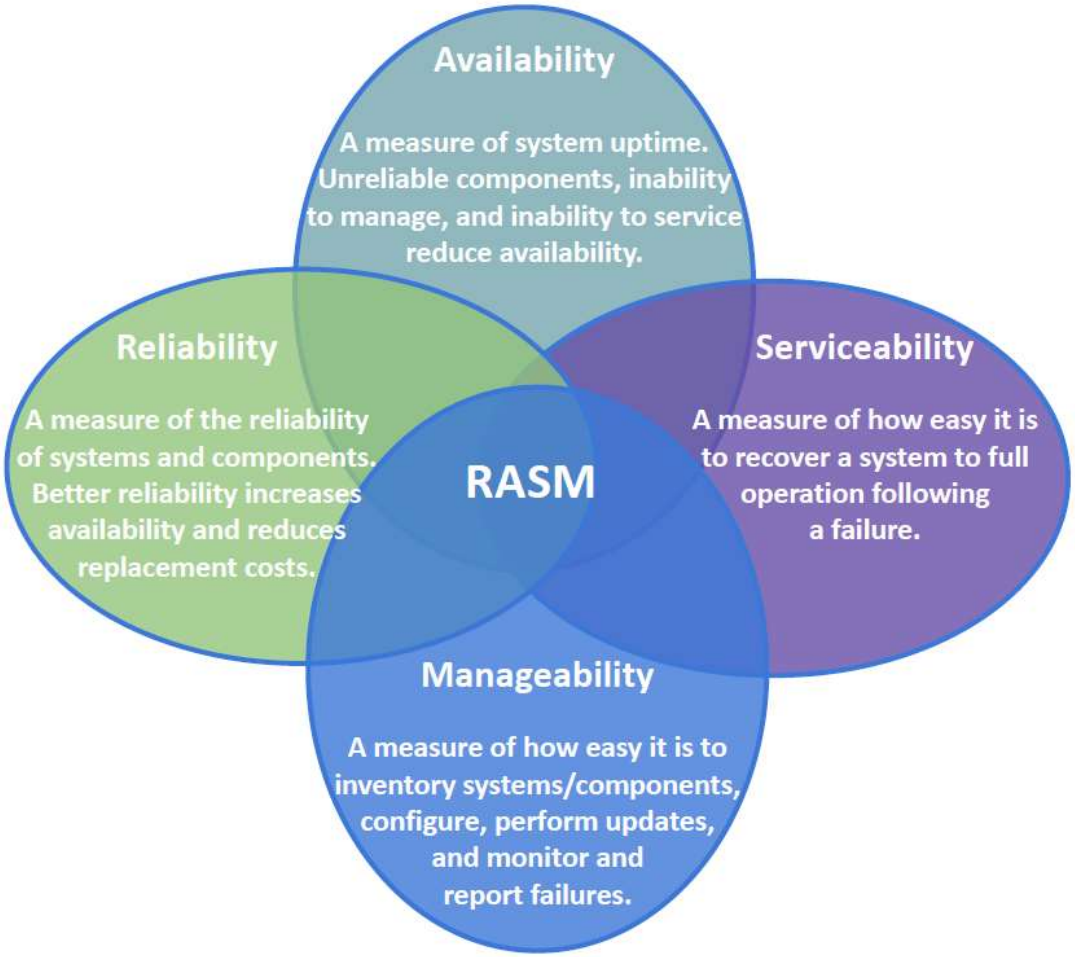
- Pcie/CXL device integration model is well established
- Helps to kick start an ecosystem
- Flexible system topologies
- SW model is leveraged from widely adopted PCIe
- Backward compatible and scalable for future use cases

Manageability

RASM

Pillars of Systems Management

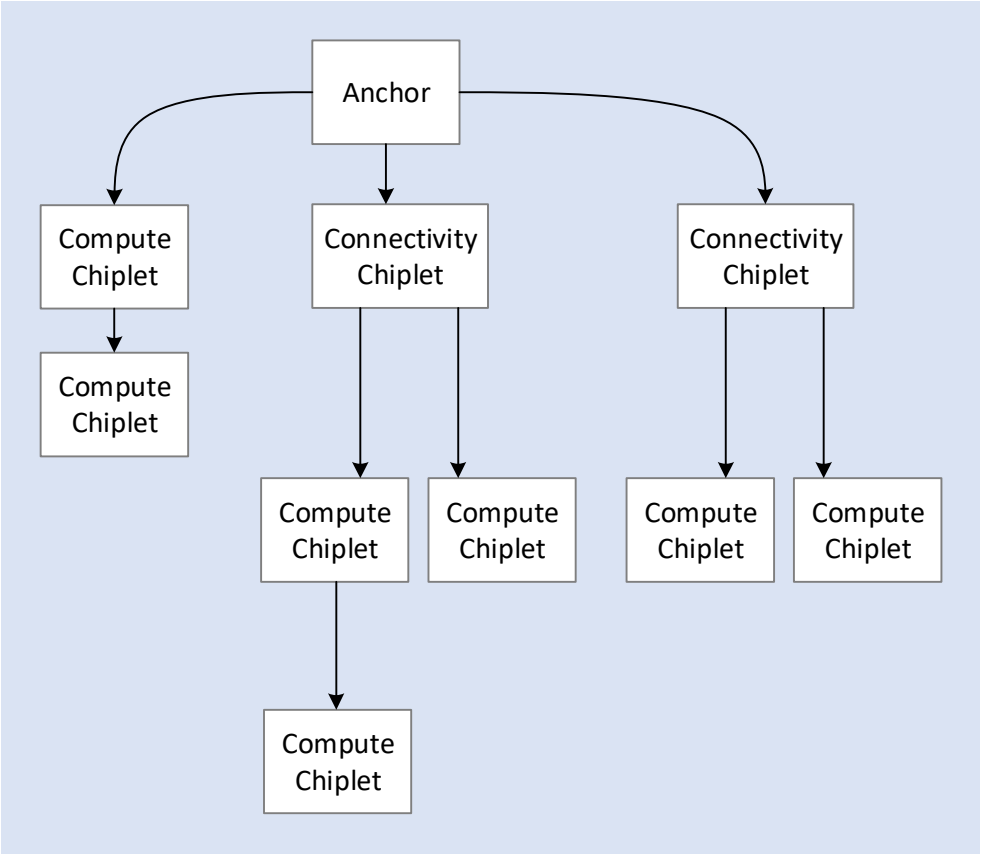
- Inventory
- Configuration & Control
- Monitoring, Logging, Alerting, and Debug



Manageability Guard Rails

- Focus on simple and efficient mechanisms that may be realized in hardware
- Manageability features should support an open chiplet ecosystem
- No complex protocols that require a processor in each chiplet
- Footprint: Must be Extremely Small
- Main band protocol independent
- Enable firmware loading

Manageability Hierarchy



- Anchor established on the SOC
  - Contains: Primary RoT, BMC communications
- Management hierarchy extends through every branch of the tree

Manageability Overview

Manageability Use Cases	Definition	Examples
Chiplet Initialization	Support initialization of chiplet hardware to get ready for firmware loading	Link initialization, clocks, resets, etc.
Chiplet Enumeration	Discovery of chiplet features and topology. Enumeration is focused on configuration and telemetry components; not a replacement for PCI enumeration (if present)	Discover topology, features, sensors and state settings (power, thermal, security, etc.).
FW Delivery	Delivery of firmware from anchor to chiplet. This can include secure delivery of the firmware.	Loading of DMU (Die Management Unit) and Device FW
Messaging	Standard communication for configuration, telemetry, etc. Secure messaging support	Power management, thermal management, RAS
Events	Asynchronous events	Thermal threshold notifications

Initialization	Enumeration	FW Delivery	Messaging	Events
• Minimal HW setup • Links • Runtime ATPG/BIST • Fuses	• Topology • Identification • Feature Discovery • Uniquify	• Secure and Non-secure • Validation	• Protocol • Ordering • Timeouts • Failures • Security • Debug	• Asynchronous notifications • Emergencies • Polling • Heartbeats

Security

Adversary Model & Threats

- Supply chain
- Hardware &
- Software

Threats

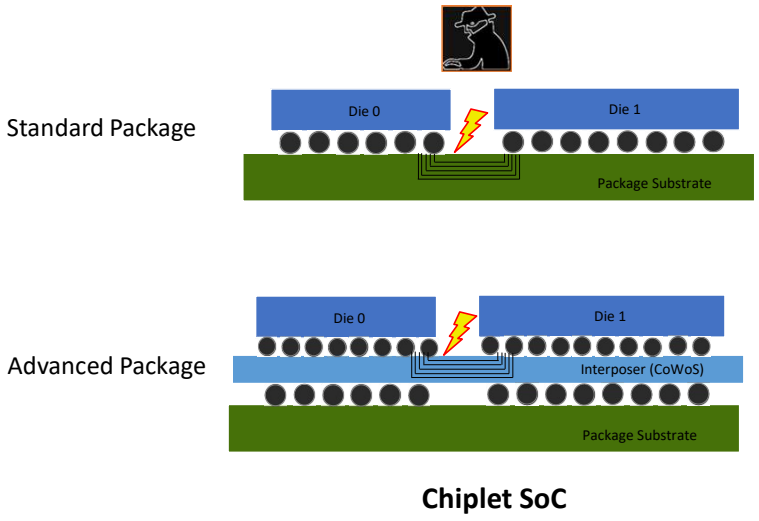
- Counterfeit / Compromised chiplets
- Boot modifications (configuration, firmware, etc.)
- Data leak (keys, memory, etc.)
- Probing on bus
- Access debug port

Physical Attack model

- Die not exposed however interconnect between individual dies are exposed on chip decapsulation.

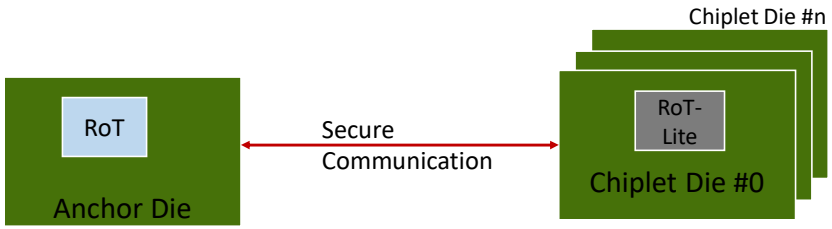
- Interconnect typically implemented in top metal layers.
(easier to do Man-in-Middle attacks)

- (Global/Local) EMFI on Interconnect much easier with interconnect position fully known. Non-invasive or semi-invasive attack possible.



SECURITY REQUIREMENTS

- Anchor die must include SoC RoT responsible for secure boot as well as **chiplet measurement and attestation**.
- No Secret key(s) should be passed in-clear between chiplet(s) to avoid man-in-middle attacks.
- Each Chiplet die must include **local Root of Trust** (represented as “RoT-Lite”) to provide any required basic security services like Chiplet fuse distribution, local key management , chiplet security policies etc.
- Anchor die RoT must load security policies (as part of chiplet FW) that are enforced by Chiplet local RoT.



Summary

- **UCIe is an open industry standard that establishes an open chiplet ecosystem and ubiquitous interconnect at the package level.**
  - Tremendous support across the industry with several companies announcing IP/VIP availability
  - Poised to be the interconnect of SoCs the same way PCIe and CXL are at the board level
  - UCIe 1.0 Specification is available to the public https://www.uciexpress.org/specification
  - UCIe 1.1 Specification expected to be released early August

- UCIe Consortium welcomes interested companies and institutions to join the organization at the **Contributor or Adopter level**.

- **Technical Working Groups** (Electrical, Protocol, Form Factor/Compliance, Manageability / Security, Systems and Software, Automotive) and **Marketing Working Group** driving the technology forward
  - Plenty of innovations happening in the consortium

- **Journey has started! Join us if you have not done so! Learn more by visiting** www.UCIexpress.org

Thank You

www.UCIexpress.org