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
- UCle starting to tackle software interfaces

![Diagram of Chiplet Ecosystem Solution Stack]

- Production Testing
- Scalable Design Verification/Platform Emulation
- SW Stack
  - Command Processor Firmware
  - Device driver
- Accelerator Interface
- D2D Protocol
- D2D Adapter
- D2D Control
- DMU (Die Management Unit)
- Chiplet FW authentication
- Secure Boot/Reset/Repair
- Runtime FW operation (Power, Thermal, Management/Telemetry)
- Manageability (SPDM/MCTP)
- Runtime RAS, Security

UCle™ (Universal Chiplet Interconnect Express) 2023
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) 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
Switch side view

- 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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI Express Extended Capability Header</td>
<td></td>
</tr>
<tr>
<td>Designated Vendor Specific Header 1</td>
<td></td>
</tr>
<tr>
<td>Reserved</td>
<td>Designated Vendor Specific Header 2</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Downstream Device SW view</th>
<th>Upstream Device SW view</th>
<th>Streaming Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCIe EP/Switch USP⁵</td>
<td>PCIe RP/Switch DSP¹</td>
<td>PCIe Root Port/Switch DSP as defined in PCIe Base Specification</td>
</tr>
<tr>
<td></td>
<td>CXL RP/Switch DSP²</td>
<td>Standard PCIe RP/Switch-DSP with additional CXL Flexbus Port DEVSEC capability</td>
</tr>
<tr>
<td></td>
<td>CXL Downstream Port RCRB³</td>
<td>CXL 1.1 compliant Host/Switch downstream Port</td>
</tr>
<tr>
<td></td>
<td>Streaming Device</td>
<td>CXL 1.1 compliant Device/schuster upstream port</td>
</tr>
<tr>
<td>PCIe RP/Switch DSP¹</td>
<td>Valid</td>
<td>Valid</td>
</tr>
<tr>
<td>CXL RP/Switch DSP²</td>
<td>Valid</td>
<td>Valid</td>
</tr>
<tr>
<td>CXL Downstream Port RCRB³</td>
<td>Illegal</td>
<td>Illegal</td>
</tr>
<tr>
<td>Streaming Protocol</td>
<td>CXL Upstream Port RCRB⁴</td>
<td>Illegal</td>
</tr>
<tr>
<td>PCIe EP/Switch USP⁵</td>
<td>Illegal</td>
<td>Illegal</td>
</tr>
<tr>
<td>CXL EP/Switch USP⁶</td>
<td>Valid</td>
<td>Valid</td>
</tr>
<tr>
<td>Streaming Protocol</td>
<td>Vendor defined</td>
<td>Vendor defined (PCIe SW model recommended)</td>
</tr>
</tbody>
</table>

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/schuster 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

RASM

Availability
A measure of system uptime. Unreliable components, inability to manage, and inability to service reduce availability.

Reliability
A measure of the reliability of systems and components. Better reliability increases availability and reduces replacement costs.

Serviceability
A measure of how easy it is to recover a system to full operation following a failure.

Manageability
A measure of how easy it is to inventory systems/components, configure, perform updates, and monitor and report failures.
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

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

### Initialization
- Minimal HW setup
- Links
- Runtime ATPG/BIST
- Fuses

### Enumeration
- Topology
- Identification
- Feature Discovery
- Uniquify

### FW Delivery
- Secure and Non-secure
- Validation

### Messaging
- Protocol
- Ordering
- Timeouts
- Failures
- Security
- Debug

### Events
- 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](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](http://www.UCIexpress.org)**
Thank You

www.UCIexpress.org