

2026
DESIGN AND VERIFICATION™
DVCON
CONFERENCE AND EXHIBITION

UNITED STATES

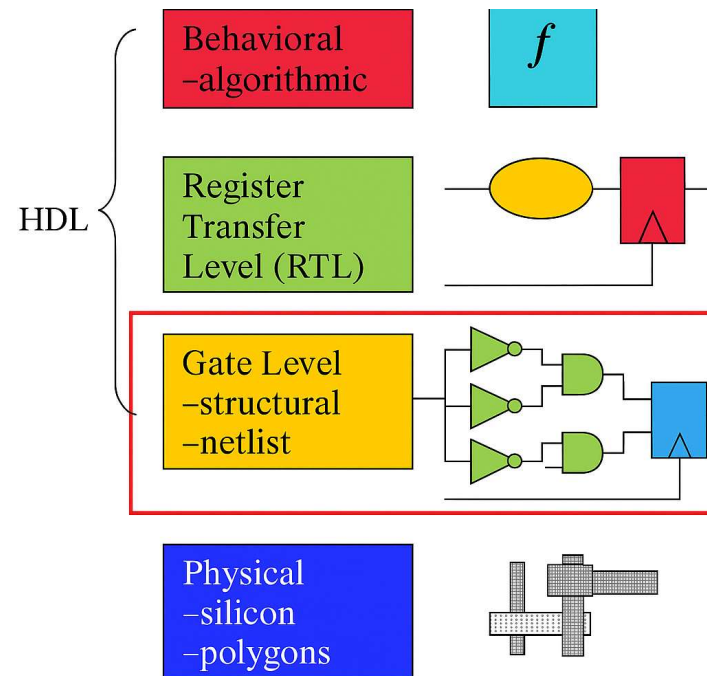
SANTA CLARA, CA, USA
MARCH 2 - 5, 2026

Liberating Verification from Boolean Shackles



REAL INTENT

Abstraction in Hardware Design



Hardware Has Changed – Verification Flows Haven't Kept Pace

- Today's designs include chiplets, AI accelerators, GPUs, multi-die interconnects, heterogeneous IP, and power/thermal/security concerns — all beyond what “classic” UVM/testbench flows were designed for.
- Yet most flows still look like they did a decade ago: regression dashboards, random seeds, code coverage reports, waveform debug.

Verification is Boolean Heavy

- Simulation
 - At its heart, simulation evaluates **Boolean signal activity over time**.
 - Coverage (toggle, branch, functional) is still Boolean: “hit/not hit.”
- Formal
 - Formal engines convert the design into a **Boolean satisfiability (SAT/SMT)** problem.
 - Properties (SVA/PSL) are essentially **Boolean expressions over time** (e.g., signal A must imply signal B within N cycles).

Early RTL design needs a different approach

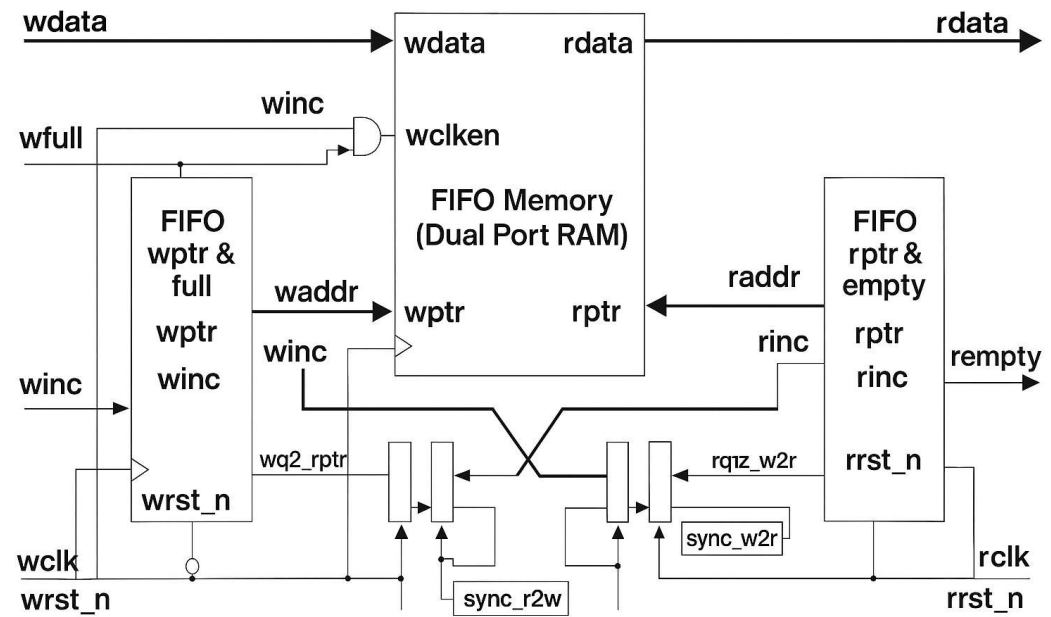
Static Sign-off: Minimally Boolean

Liberates from
Boolean shackles



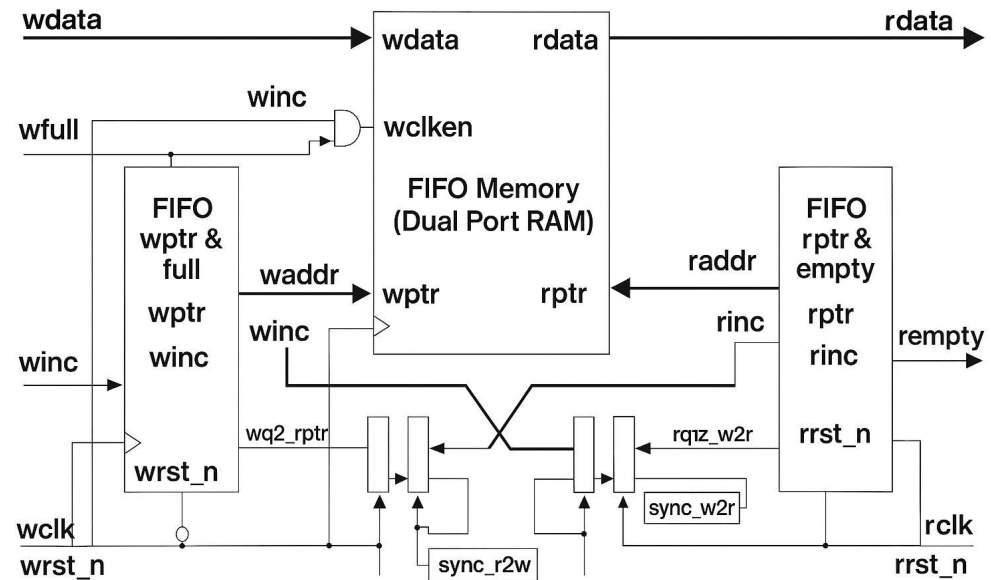
Asynchronous FIFO - Simulation

- Testbench drives input signals
- Outputs and internal signals are observed
- Coverage checks are Boolean



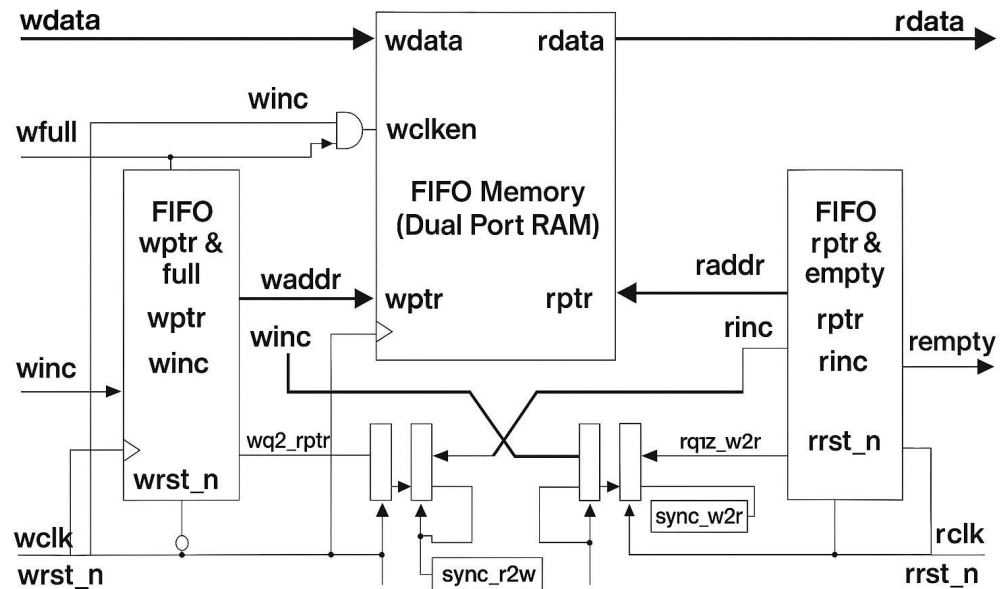
Asynchronous FIFO - Formal

- Assertions are created
- The tool turns these into Boolean constraints + SAT queries.
- Analysis is still mostly Boolean
- State space explosion happens on large size designs



Asynchronous FIFO – Static Analysis

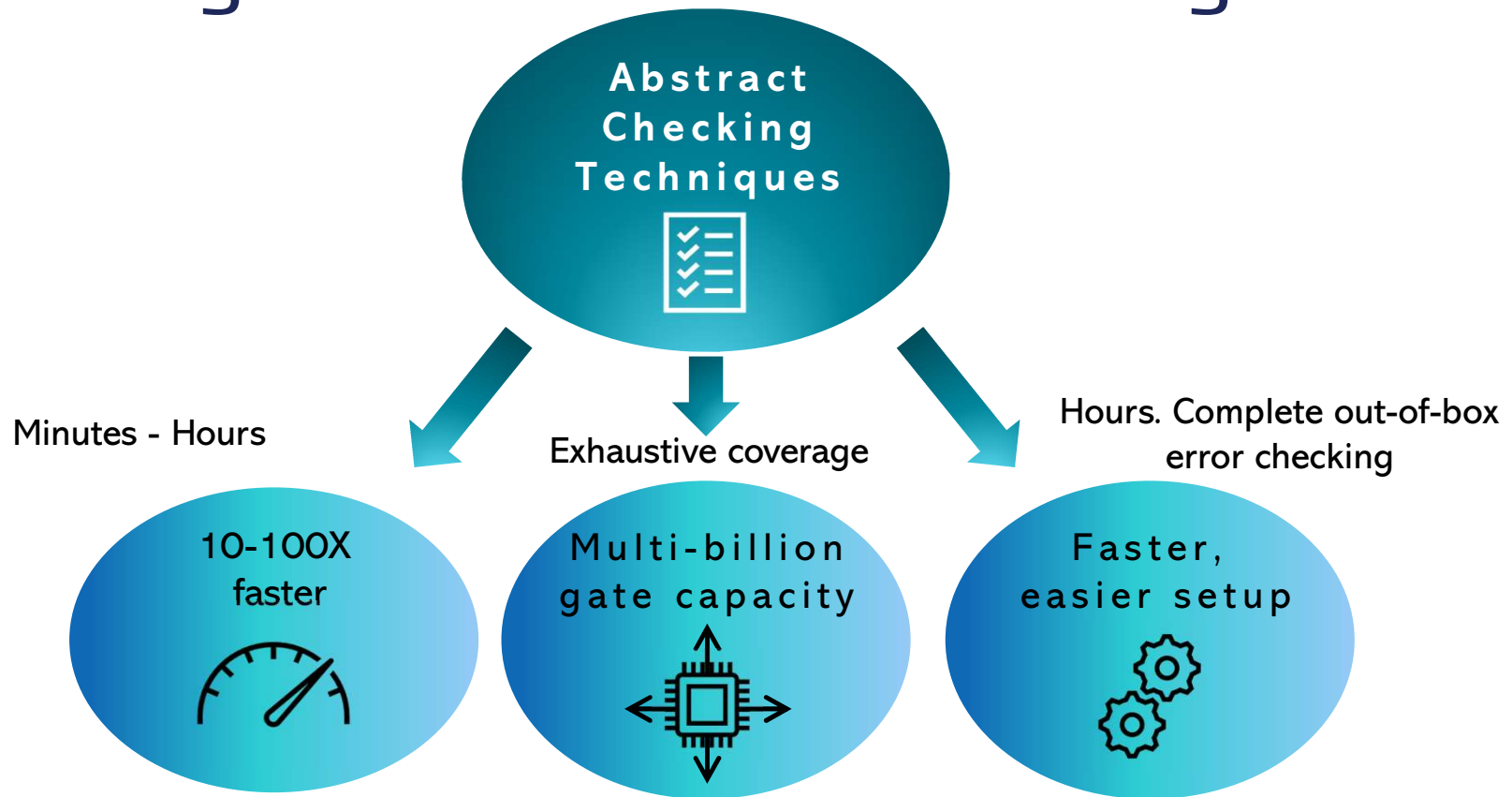
- Static analysis automatically abstract structures
 - RAM
 - Synchronizers
 - Pointer comparison
- Verifies correctness at abstract level
- **Minimally Boolean!**



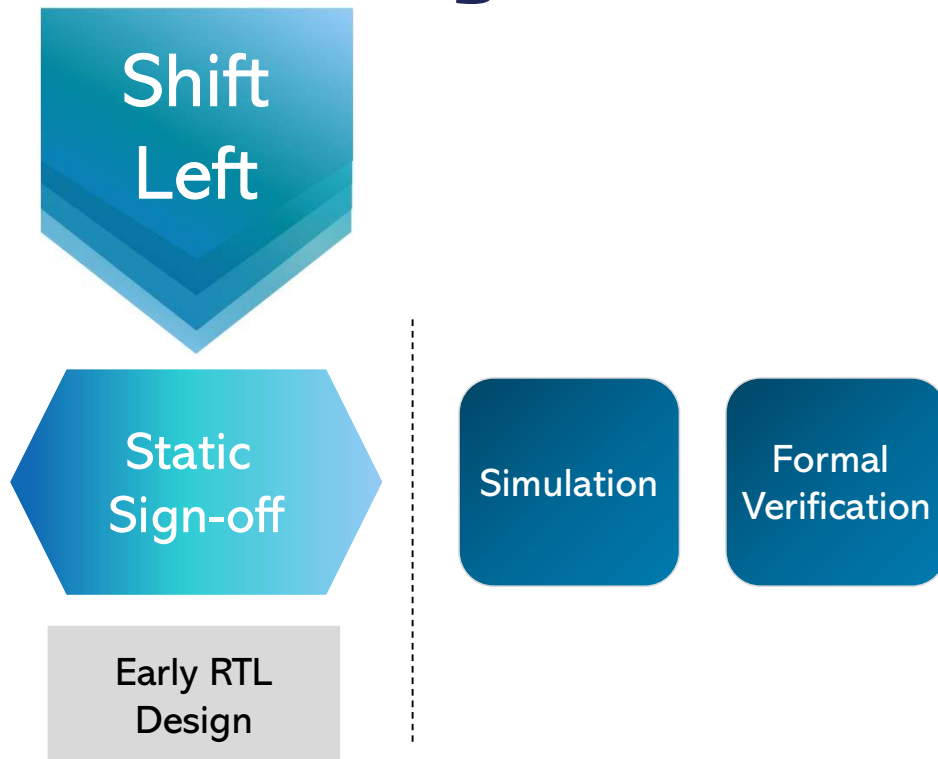
Static vs Simulation vs Formal Comparison

Simulation	Formal	Static
Testbench Needed	Assertions Needed	Automatic based on abstract structures
Will miss issues (not comprehensive)	Will miss issues (inconclusive)	Always catch
<i>Long time to setup (write appropriate large number of testbenches)</i>	Long time to setup (write appropriate assertions and then assumptions and wiggling to find real failures)	Fast setup
Long runtime	Long runtime	Fast runtime
No expert user needed	Expert User needed	No expert user needed
Large number of resources needed (compute and human)	Large number of resources needed (compute and expert human)	Low compute and human resources
Run on any size	Cannot run at top	Run on any size

Static sign-Off: Abstract checking



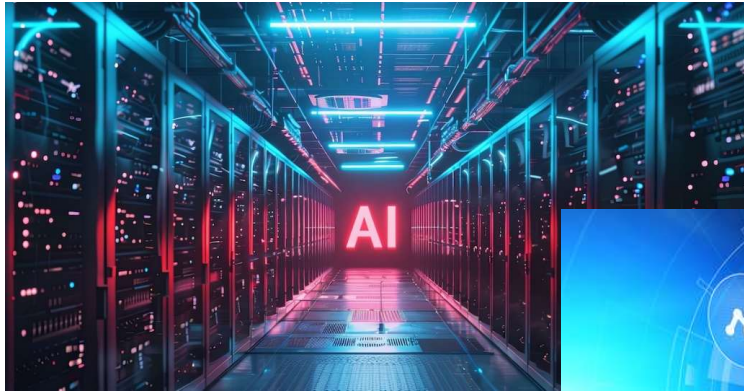
Static Sign-off: Starts Early



- Benefits

- Identify defects early: minimize costly rework, save time & resources
- Improve design quality: address design flaws, optimize architecture, higher quality designs
- Faster time-to-market: shorten design cycle
- Cost reduction: fixing issues late / missed failures; both very costly
- Risk reduction: catch failures, security vulnerabilities for robust design

Explosive Chip Market Growth with AI



AI Datacenters



Edge computing and AI Accelerators

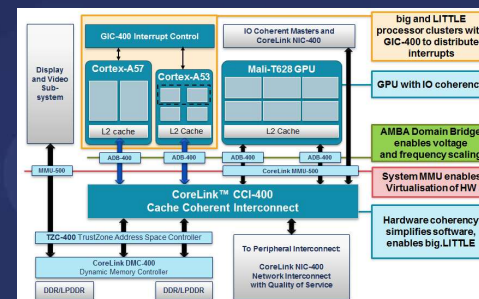
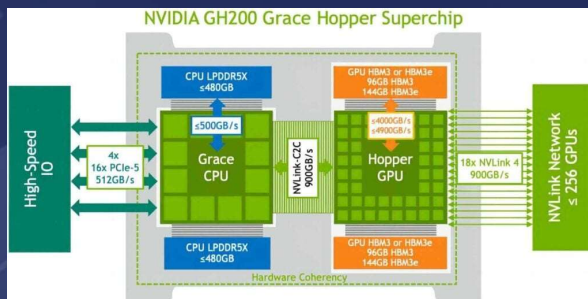


On-Device AI

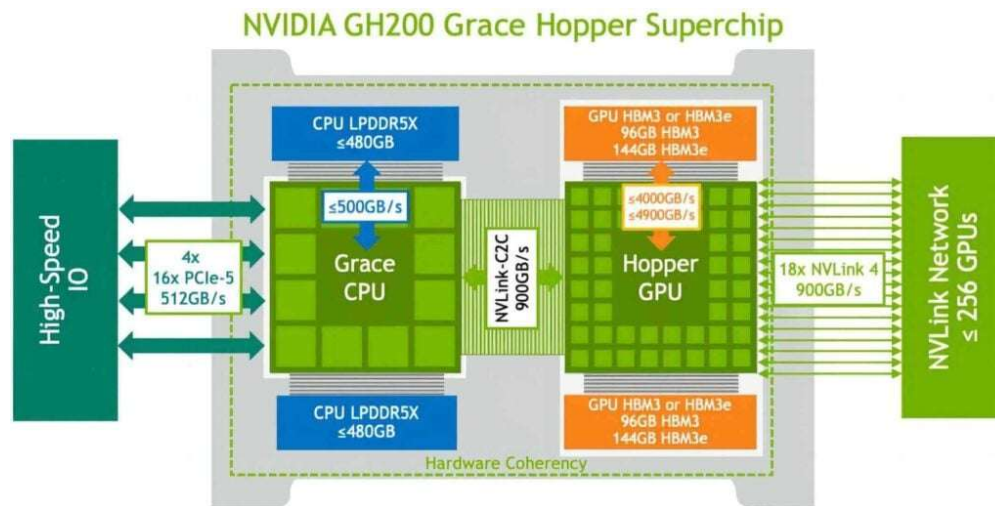
2026
DESIGN AND VERIFICATION™
DVCON
CONFERENCE AND EXHIBITION
UNITED STATES

SANTA CLARA, CA, USA
MARCH 2 - 5, 2026

Verification Challenges of these Chips

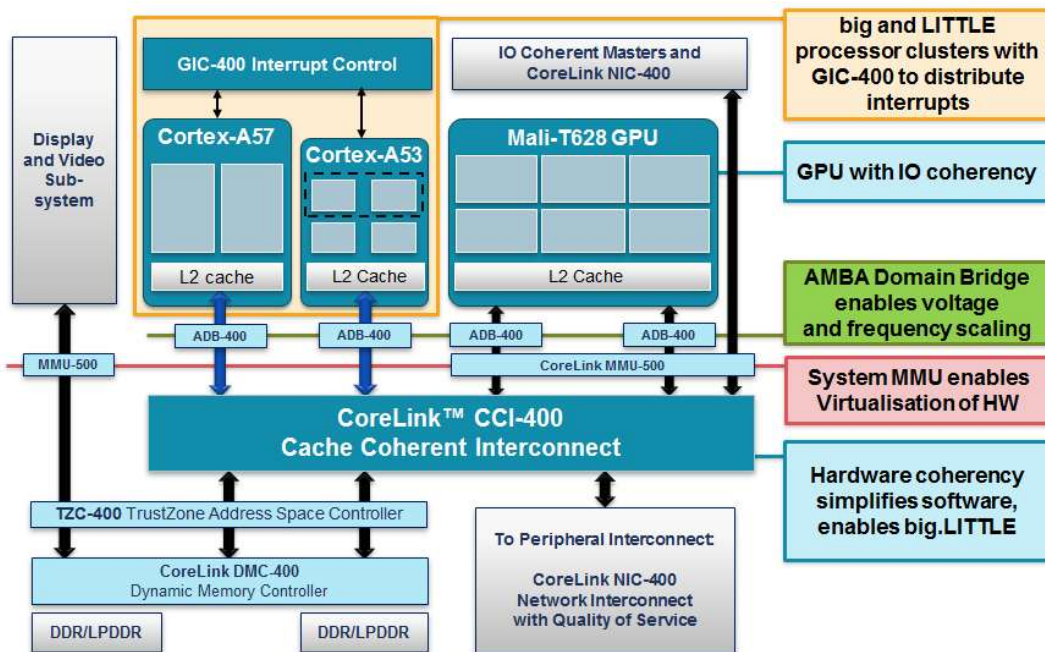


Verification Challenges AI Chips



- Massive Asynchronous paths and power domain verification – CPU-GPU-HBM
- CPU + GPU + High-Bandwidth Memories (HBM3/3e + LPDDR5X)
 - Protocol correctness
 - Cache coherency
 - Memory consistency
- NVLink-C2C
 - Interconnect verification
 - Topology correctness routing, congestion ...
- PCIe Gen5, HBM3(e) interfaces
 - I/O Verification
- Security and Reliability
 - Ensuring isolation between CPU/GPU address spaces
 - Preventing privilege escalation through NV Link or memory mapping
- System Level Verification

Verification Challenges Non-AI Chips

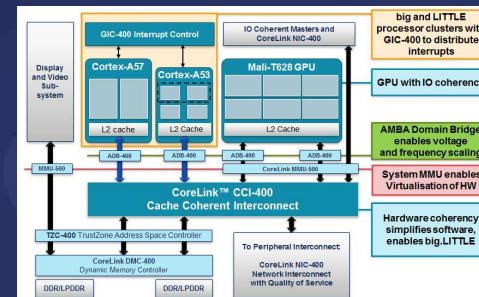
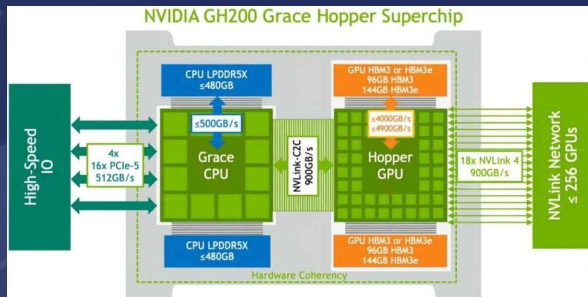


- Cortex-A57/A53 clusters
 - CPU Verification
- CoreLink CCI-400 cache coherent interconnect
 - Interconnect Verification
- GIC interrupt controller
 - Correct distribution between big and LITTLE clusters.
- Design Initialization
- Security (TrustZone, TZC-400)
 - World separation: Normal world vs Secure world must be strictly isolated.
 - Illegal access prevention: Verifying that GPU/DMA cannot access secure-only memory.
 - Corner case: Speculative loads/stores bypassing TZC checks.

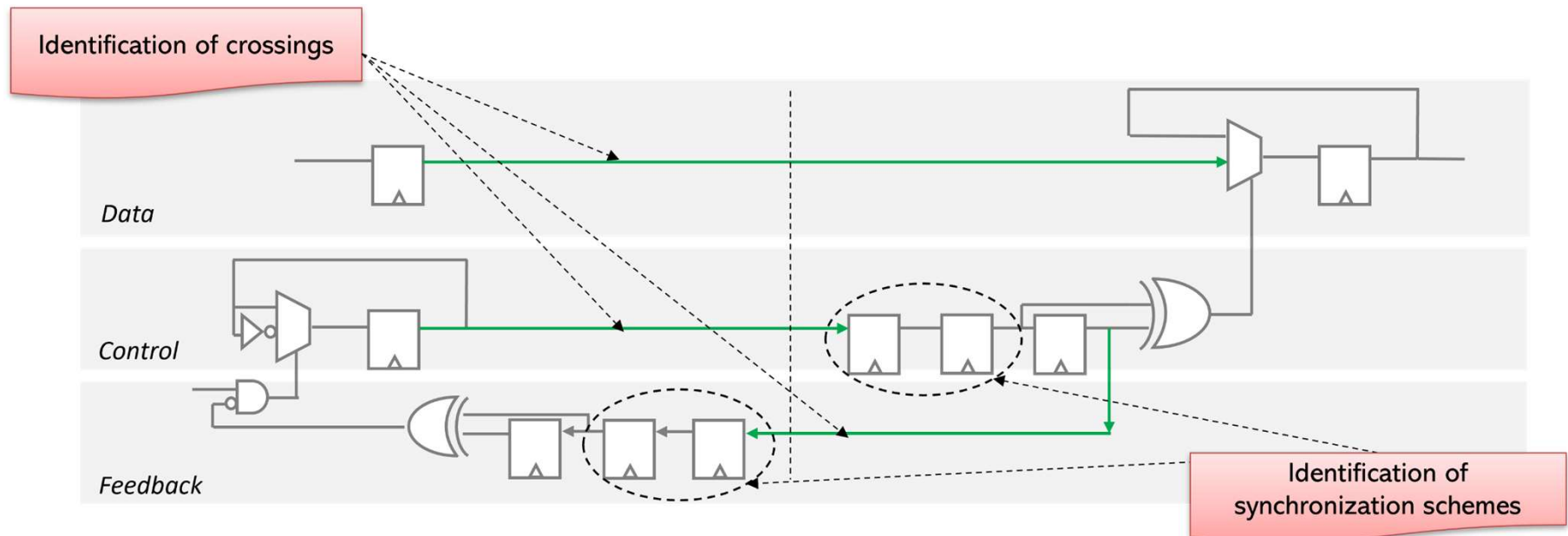
2026
DESIGN AND VERIFICATION™
DVCON
CONFERENCE AND EXHIBITION
UNITED STATES

SANTA CLARA, CA, USA
MARCH 2 - 5, 2026

Asynchronous Path Verification Challenges

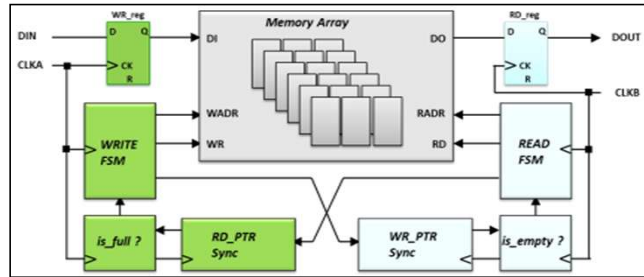


Handshake Functional Correctness

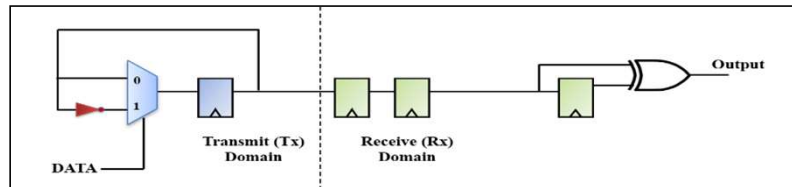


- Interpret underlying functional intent in multimode context
- Accurately identify CDC issues when crossings can be synchronous in some modes or asynchronous in some modes
- Automatically and in one run

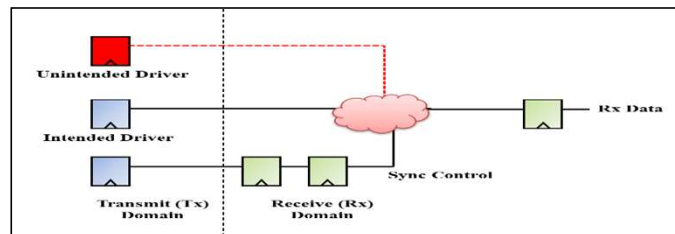
Handshake Functional Correctness



FIFO Handshake

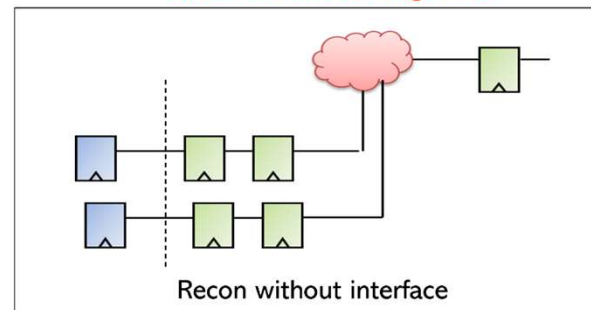


Auto-Identified Pulse Synchronizer

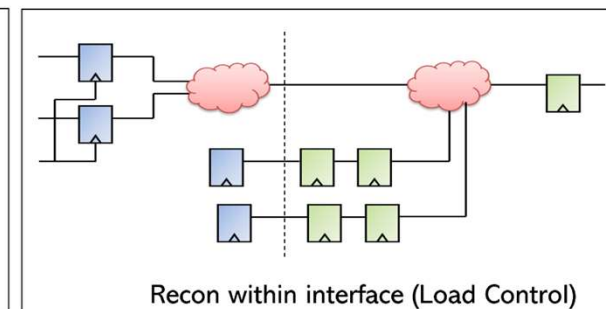
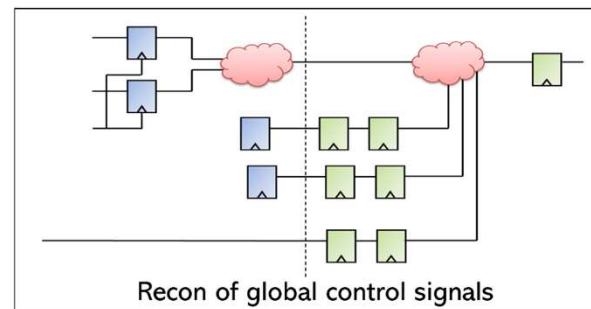
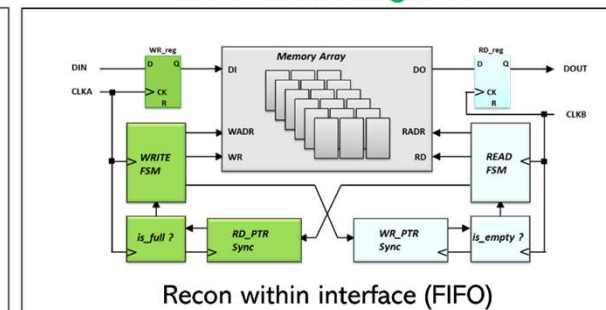


Unintended Driver - ERROR

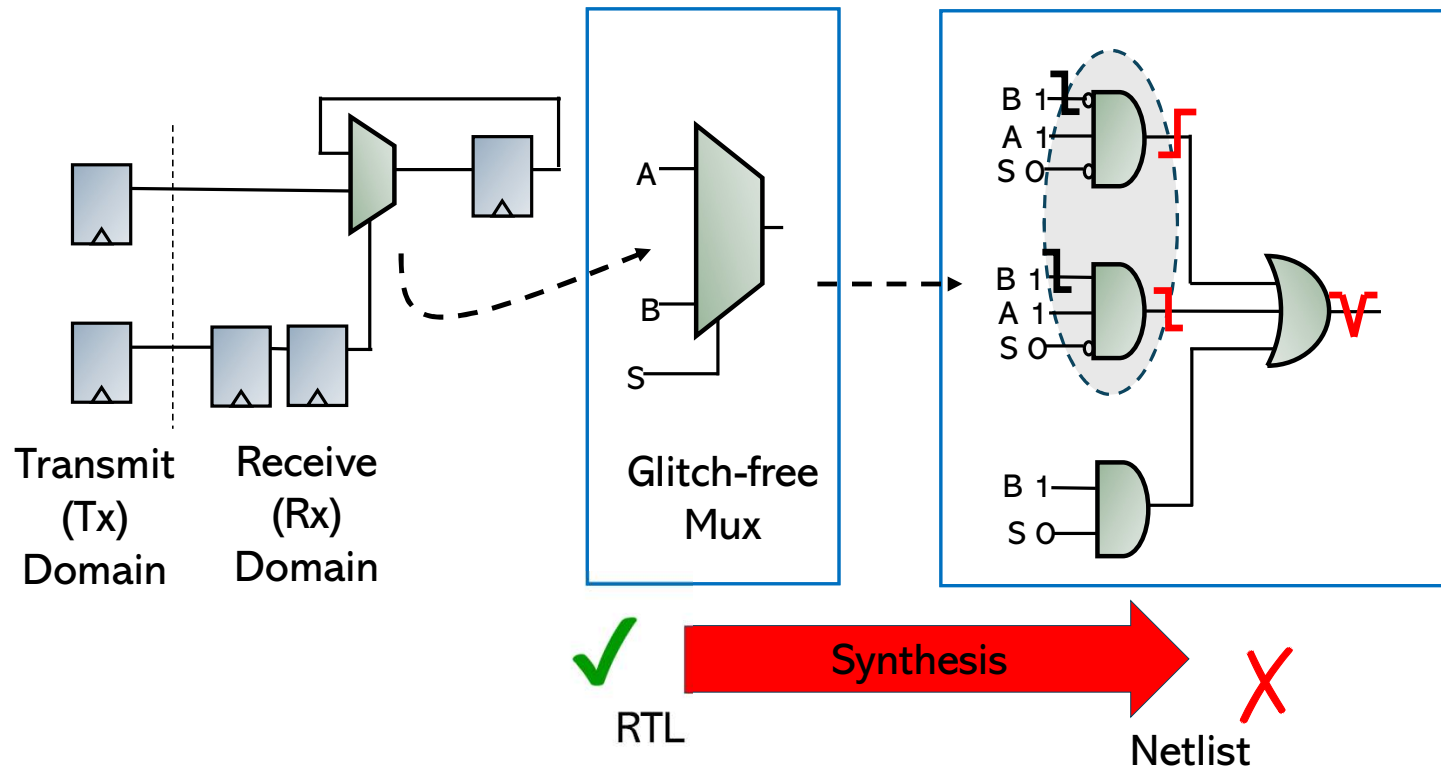
Unsafe Reconvergence



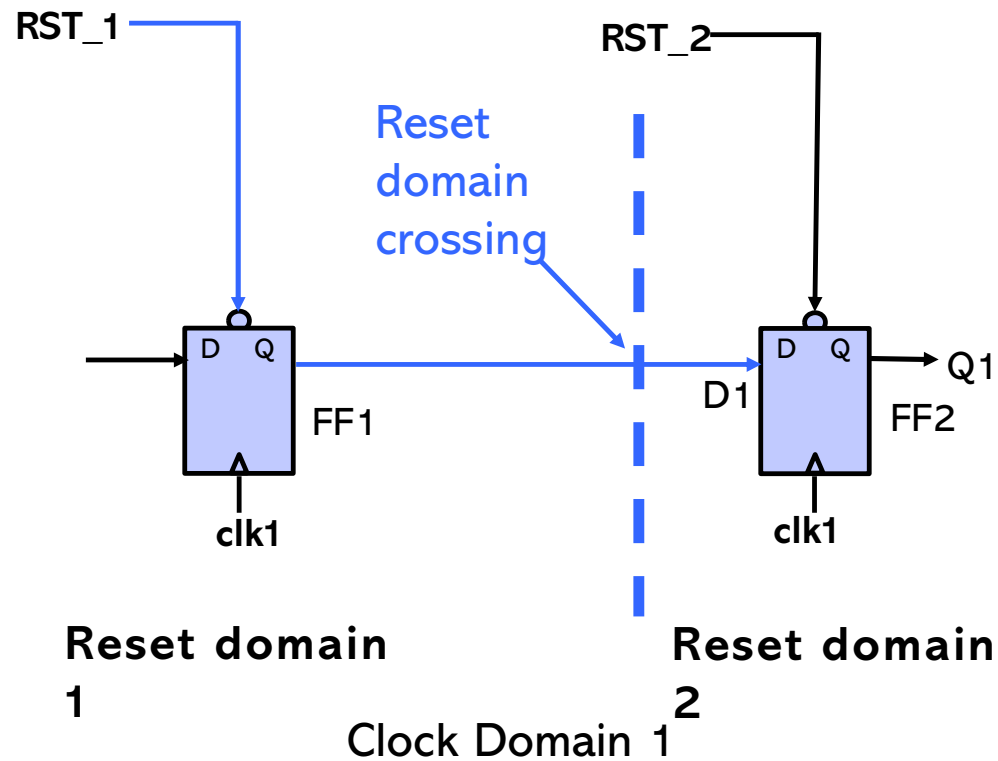
Safe Reconvergence



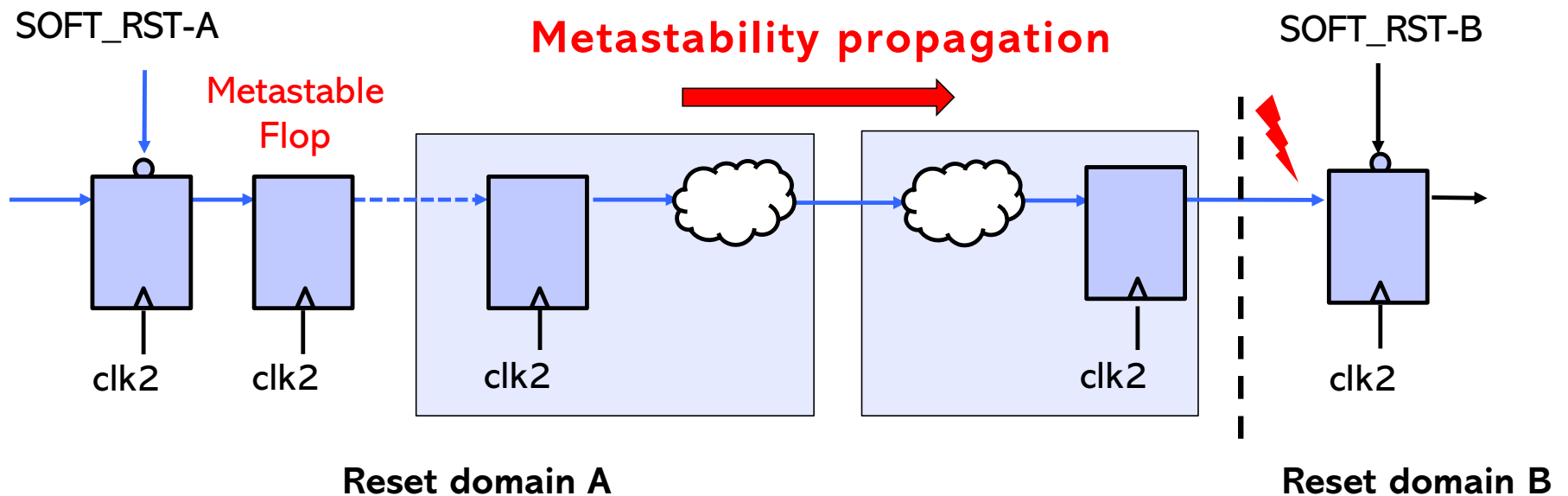
Safety from Glitch Hazards



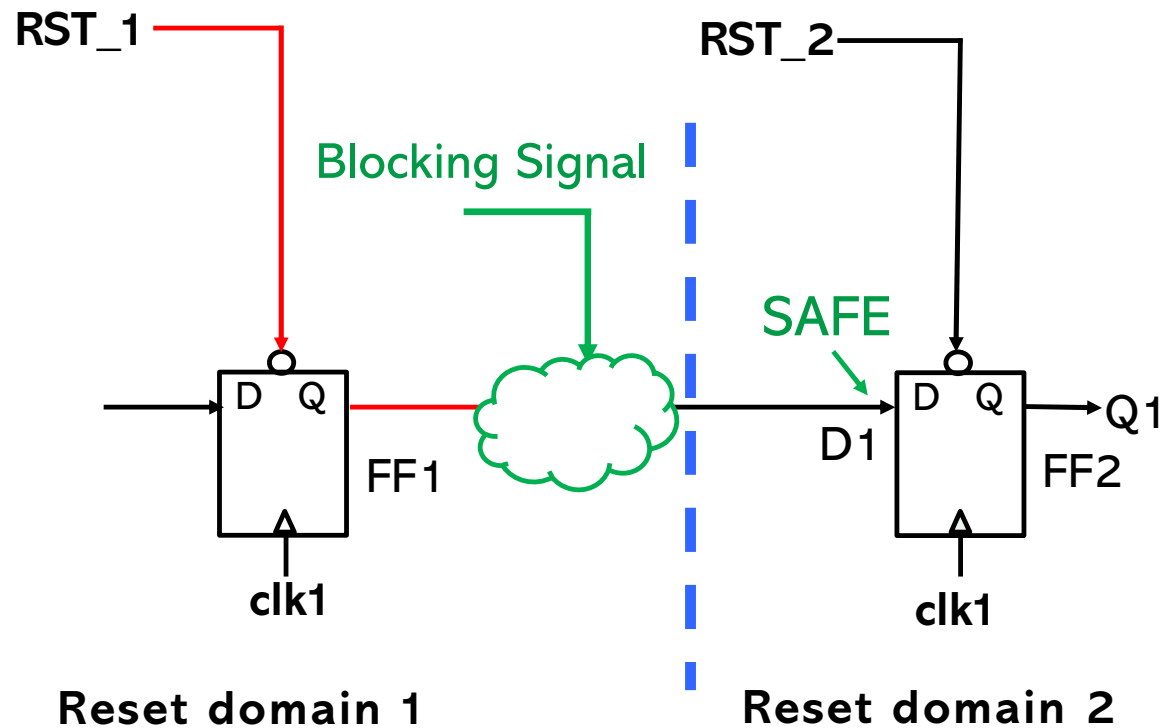
No Reset Metastability



No Reset Metastability

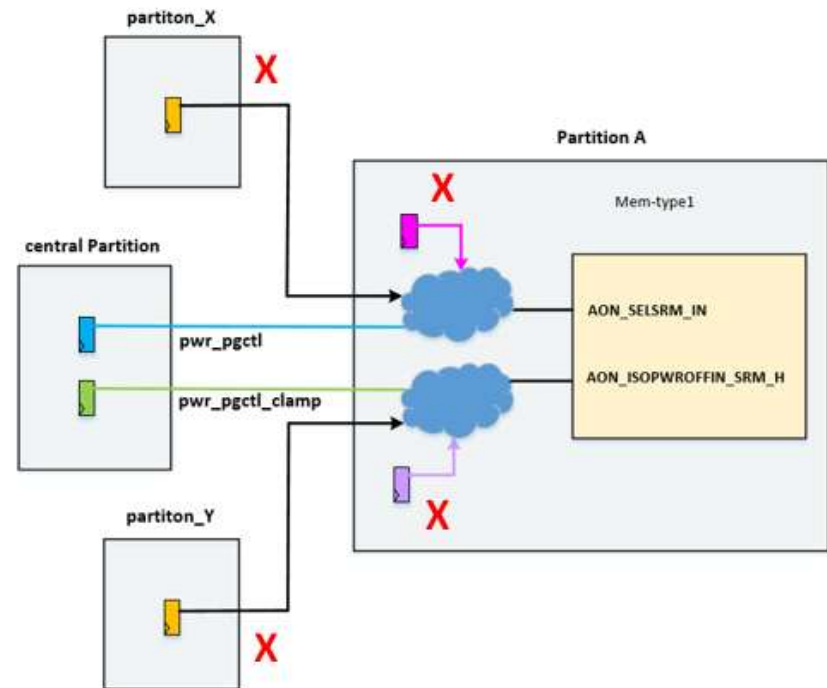


No Reset Metastability

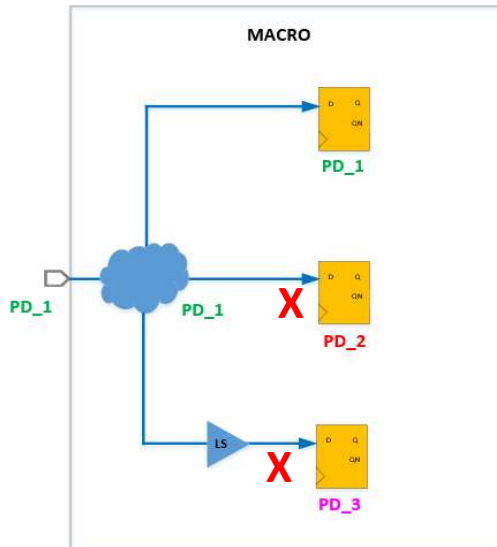


Power Logic Verification

Check memory inputs in a partition are driven without any extra connections by power and clamp PGCTL pins respectively from one central partition



Power Isolation Verification

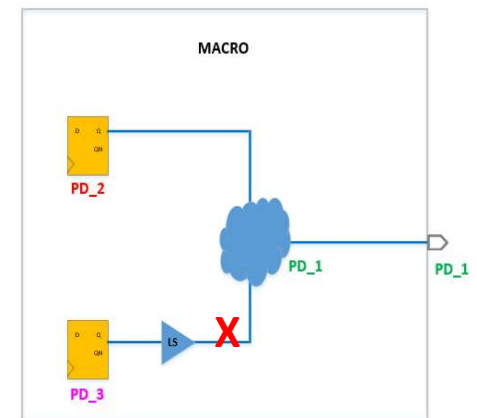


Check that any input of the macro can only drive FFs in the same power domain

- `create_group -name GRP1 -module {MACRO} -all_inputs`
- `trace_all_paths -rule POWER_ISOLATION_DIFFERENT_PD -from_group GRP1 -source_pd`

Check that any output of the macro can only be driven by FFs in same power domain

- `create_group -name GRP2 -module {MACRO} -all_outputs`
- `trace_all_paths -rule POWER_ISOLATION_DIFFERENT_PD -to_group GRP2 -destination_pd`

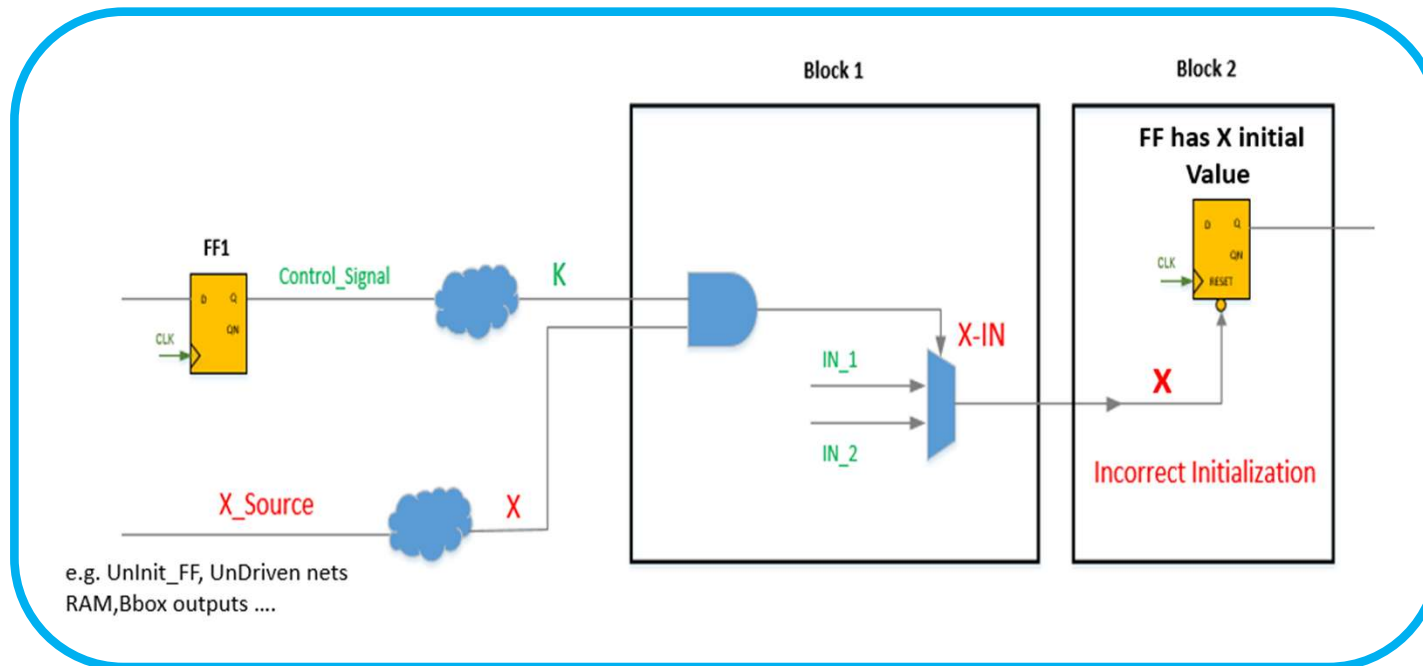


Design Initialization

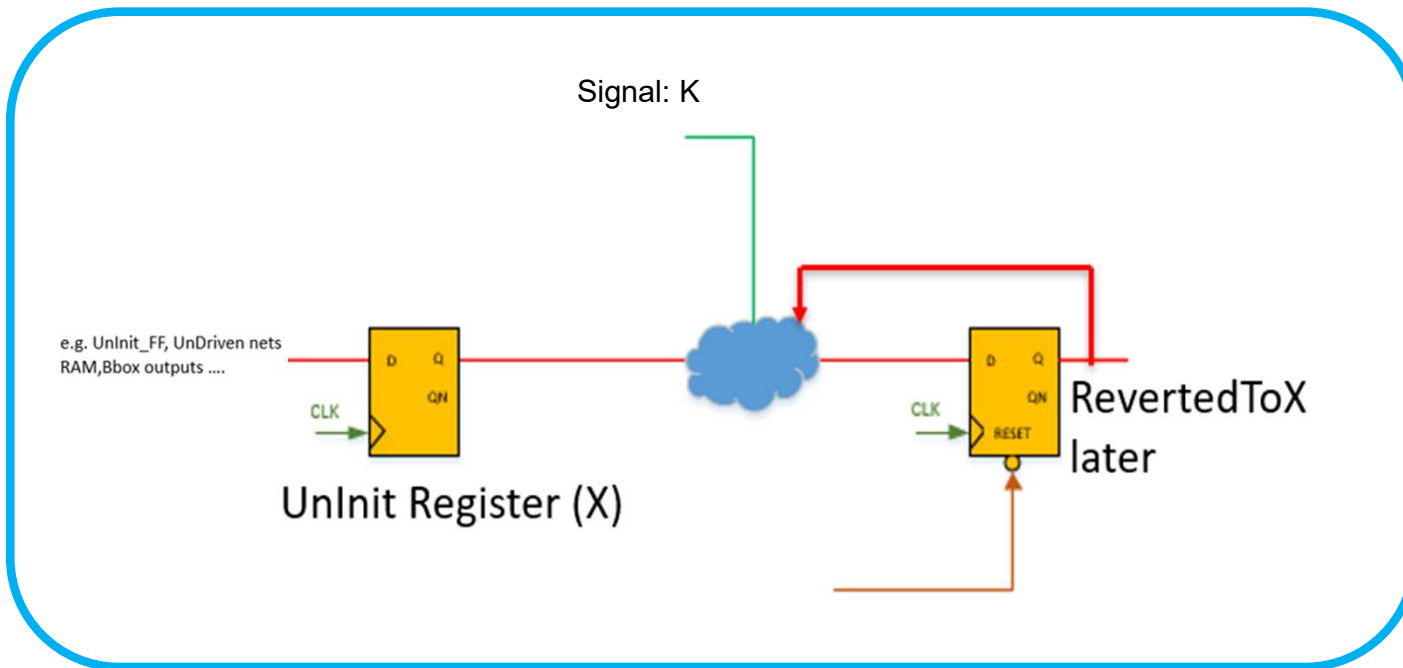
- How to catch uninitialized and incorrectly initialized FFs ?
- How to ensure upfront that RTL is not X Optimistic ?
- Ensure design does not have long initialization latency and desire to reduce it effectively ?



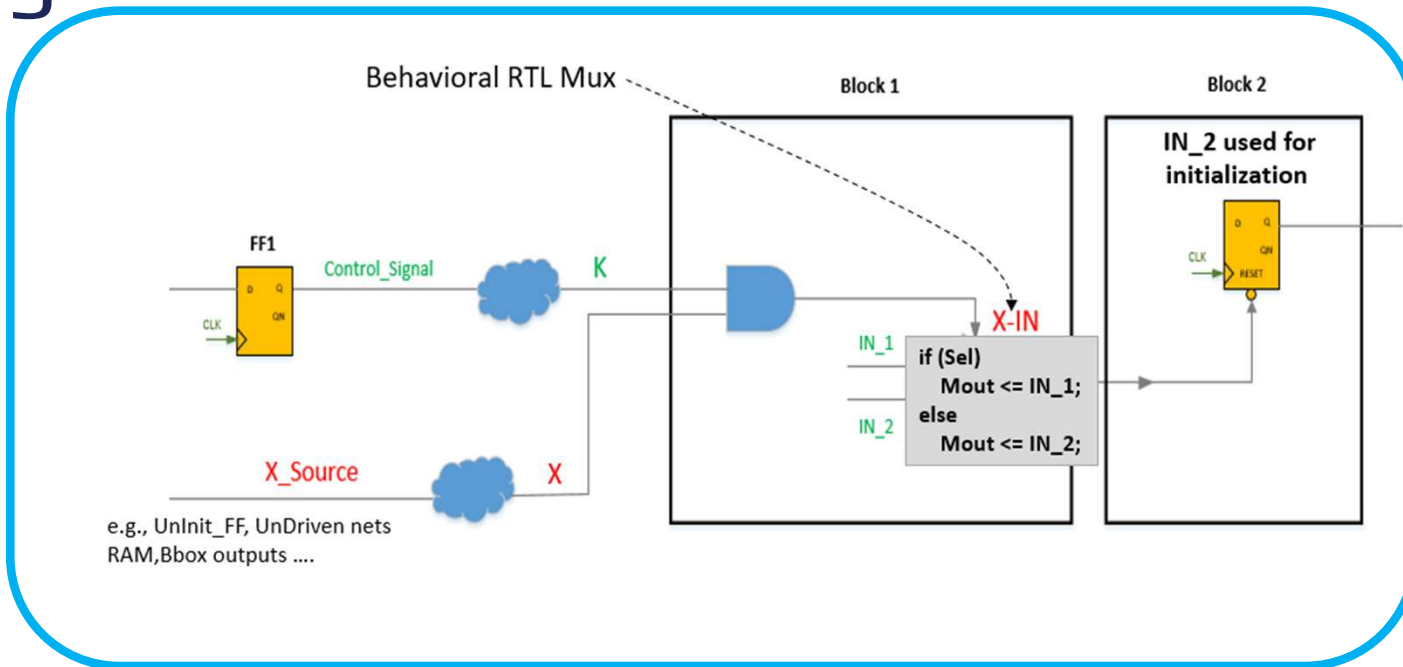
Incorrect Design Initialization (1)



Incorrect Design Initialization (2)



X-Optimistic Code Breaks Downstream Logic



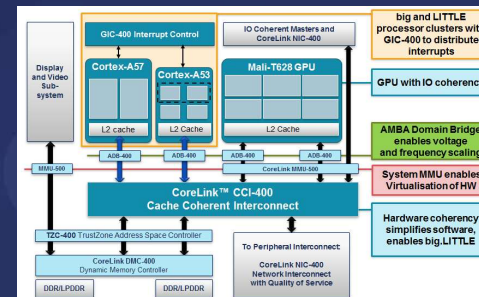
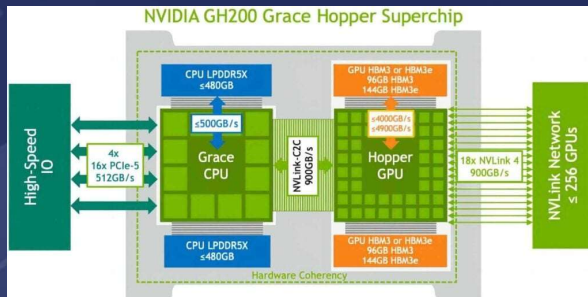
Automatic & Low-noise Static Tools are Imperative to Success

- Automatic setup enable out of the box setup and reduce cost
- Automatic checks speed up bug detection
- Automatic checks mitigate risks early through **scalable, systematic verification** — from individual IP blocks to **full-chip** designs.
- Low noise is imperative as large noise discourages detailed analysis can causes issues to slip through

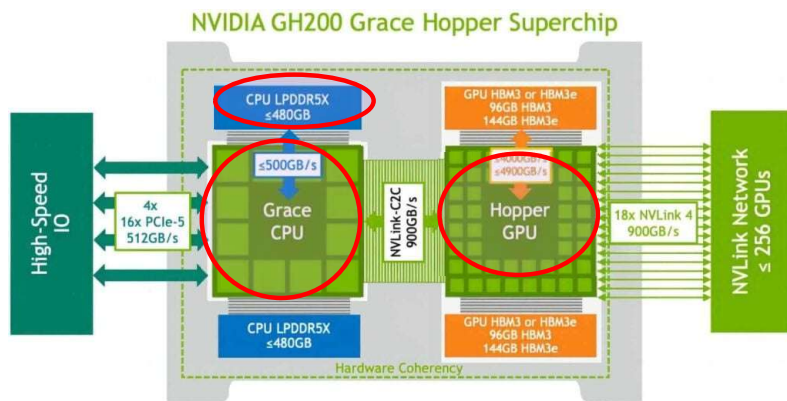
2026
DESIGN AND VERIFICATION™
DVCON
CONFERENCE AND EXHIBITION
UNITED STATES

SANTA CLARA, CA, USA
MARCH 2 - 5, 2026

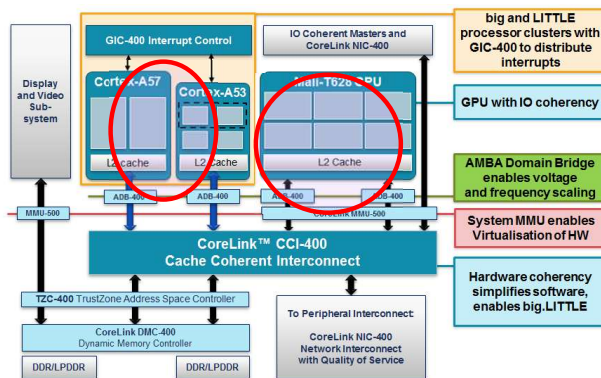
CPU/GPU Verification Challenges



CPU/GPU Verification Challenges



- Side-channel vulnerabilities (e.g., Spectre, Meltdown) arise from speculation, caches, and timing.
- Correct handling of exceptions, interrupts, and privilege levels must be validated across all instruction flows
- Root of Trust Verification



Security Vulnerabilities Risk for All CPU

Types

Meltdown and Spectre: 'worst ever' CPU bugs affect virtually all computers

Everything from smartphones and PCs to cloud computing affected by major security flaw found in Intel and other processors - and fix could slow devices

Security experts find vulnerability in ARM's memory tagging extensions

by Bob Yirka, Phys.org

ENDPOINT SECURITY

GhostWrite Vulnerability Facilitates Attacks on Devices With RISC-V CPU

GhostWrite is a RISC-V CPU vulnerability that can be exploited to gain full access to targeted devices.

New SLAP & FLOP Attacks Expose Apple M-Series Chips to Speculative Execution Exploits

Intel's latest security update has this 'big warning' for AMD and Nvidia customers

According to the report, AMD had "4.4x more firmware vulnerabilities in their hardware root-of-trust" and "1.8x more firmware vulnerabilities in their confidential computing technologies" compared to Intel. The company also criticised Nvidia in the GPU category, stating that it only had high-severity vulnerabilities (18) in 2024.

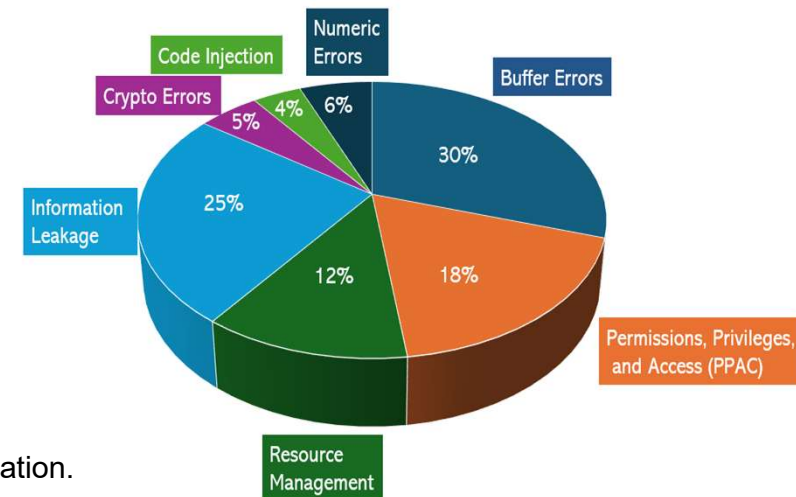
Security Becoming Core Part Of Chip Design – Finally

One of the big changes for hardware and system security is a recognition that it's no longer someone else's problem. What used to be an afterthought is now a competitive edge that needs to be baked into a design at the architectural level.

The High Cost of Security Vulnerabilities in Chips

Missing a security flaw can cost tens of millions of dollars—a critical business risk

- Direct Financial Costs 💰
 - Cyberattack & Ransomware – Data breaches & extortion risks.
 - Remediation & Incident Response – Investigations & recovery efforts.
 - Revenue Loss – Business disruptions & customer fallout.
- Indirect Financial Costs ⚠️
 - Downtime & Operational Disruptions – Impacting productivity & supply chain.
 - Regulatory & Legal Penalties – Compliance violations & lawsuits.
- Strategic Consequences
 - Loss of Competitive Advantage – A compromised product damages innovation.
 - Erosion of Trust – Customer & partner confidence declines.



Source: Data from MITRE/NIST

Hardware security signoff is crucial

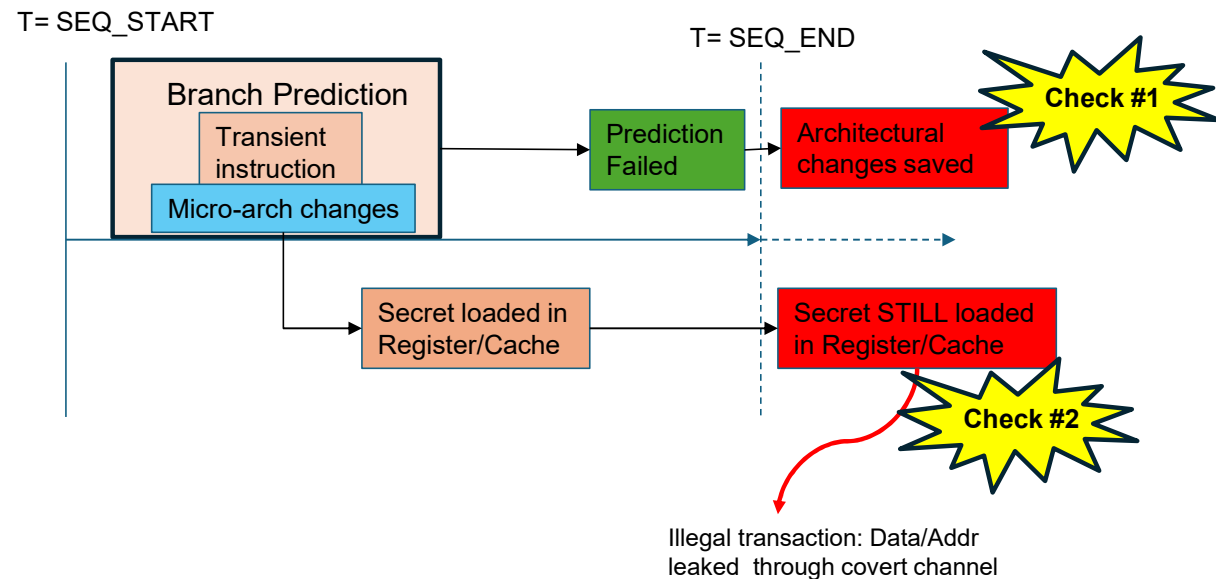
Speculative Execution Vulnerabilities

Leakage Scenario

Expose architecturally restricted data

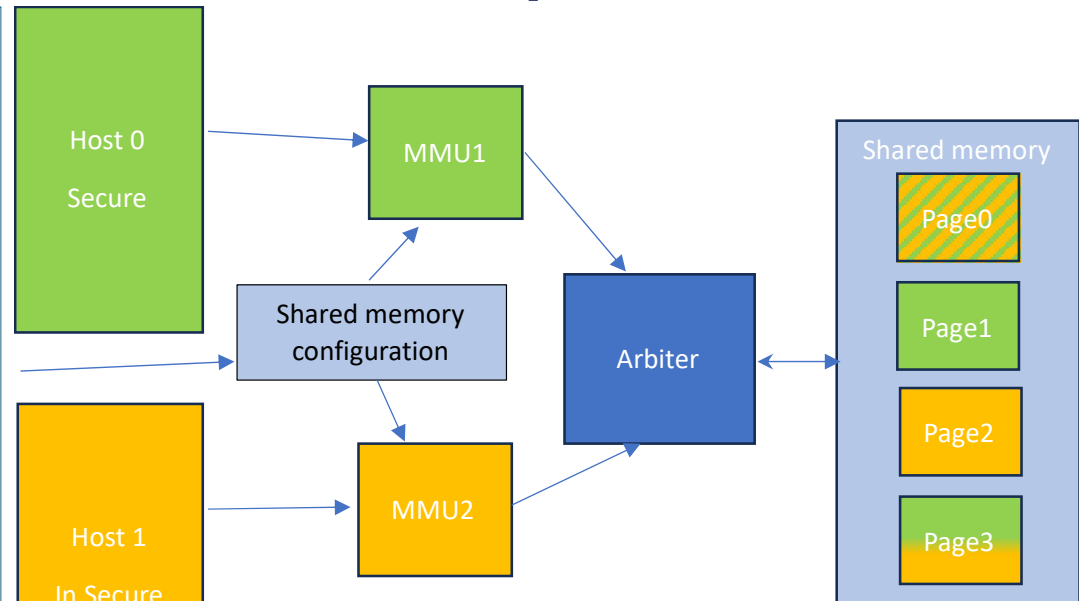
Allow predictor training in one domain to influence behaviour in another domain

Caused by stale/incorrect data forwarding



Privilege Access in Multi CPU System

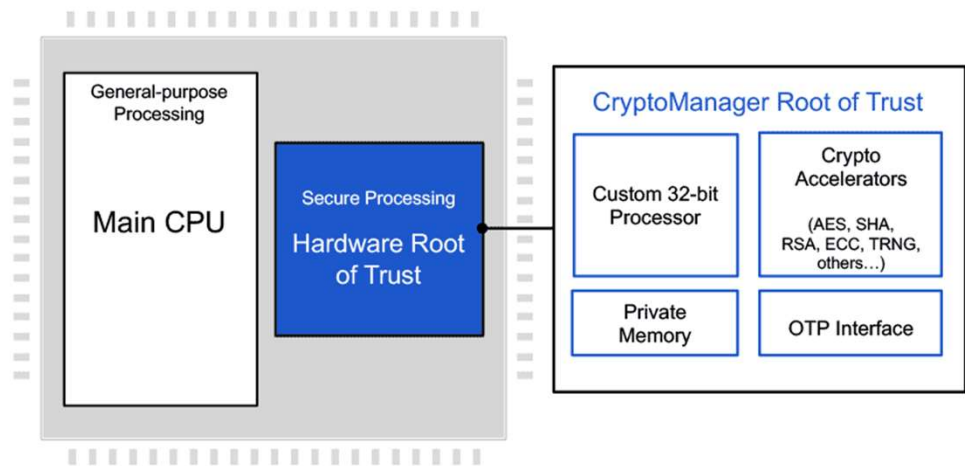
- Host0 and Host1 share the memory
 - Host0: Secure
 - Host1: Insecure.
- Shared Memory: 4 pages
- MMU's configures page is read or write to/from a host.
- Example configuration in the MMU's:
 - Page 0 is shared RW and accessible by both
 - Page 1 is exclusive RW to Host0
 - Page 2 is exclusive RW to Host1
 - Page 3 is mailbox RW by Host0, read only by Host1
- Configuration is written into the shared memory configuration block via a sequence of writes from an external entity.



Sample Check: Insecure Host-1 should not have any interaction with Page-1 when valid RW transaction is happening between secured Host-0 and Page-1.

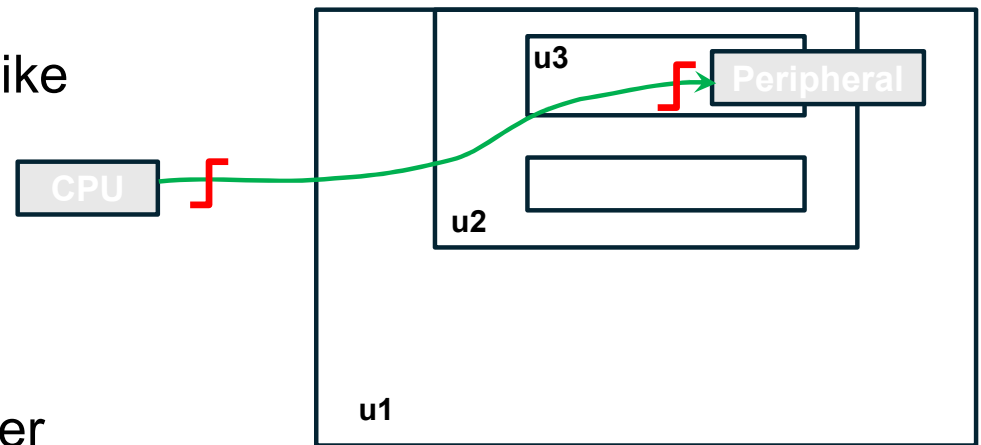
CPU- Hardware Root Of Trust

- Secure Key Storage
 - Key material must be stored securely to prevent compromise, as the exposure of cryptographic keys can lead to systemic security failures.
- Side Channel Detection
 - Hardware is often susceptible to side channel attacks where attackers glean sensitive information



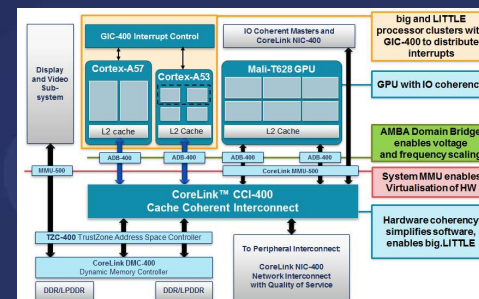
Interrupt Verification

- Specific connectivity register based
- Can propagate through special cells like synchronizers
- Polarity of connection important
- No additional drivers or receivers
- Mask the interrupt under certain conditions
- Read and clear interrupt status register that generated the interrupt signal
 - WI/WO acknowledgment depending on interrupt type
 - Unmask the interrupt under certain conditions

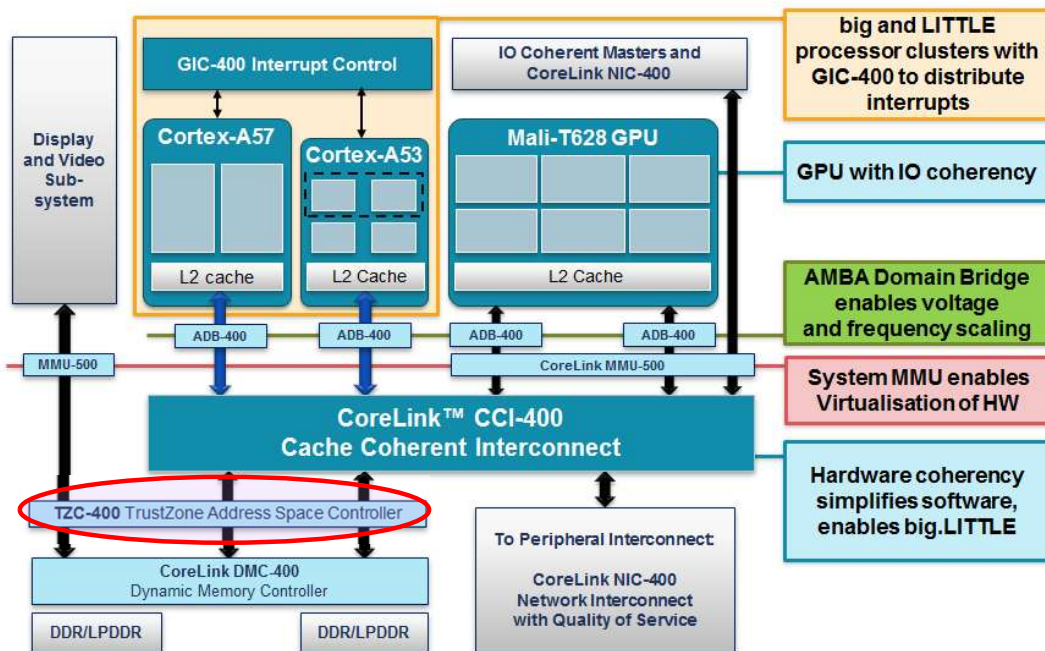


SANTA CLARA, CA, USA
MARCH 2 - 5, 2026

The diagram illustrates the NVIDIA GH200 Grace Hopper Superchip architecture. It features a central 'Grace CPU' (represented by a green grid) and a 'Hopper GPU' (represented by a green grid). The CPU is connected to two 'CPU LPDDR5X <480GB' memory blocks. The GPU is connected to two 'GPU HBM3 or HBM3e' memory blocks, each with '96GB HBM3' and '144GB HBM3e' capacities. Data flow between the CPU and GPU is managed by an 'NVLink-C2C 900GB/s' interface. The entire chip is connected to a 'High-Speed IO' block on the left and an 'NVLink Network < 256 GPUs' block on the right. The network connection is specified as '18x NVLink 4 900GB/s'. A dashed green box labeled 'Hardware Coherency' encompasses the CPU, GPU, and their respective memory blocks.

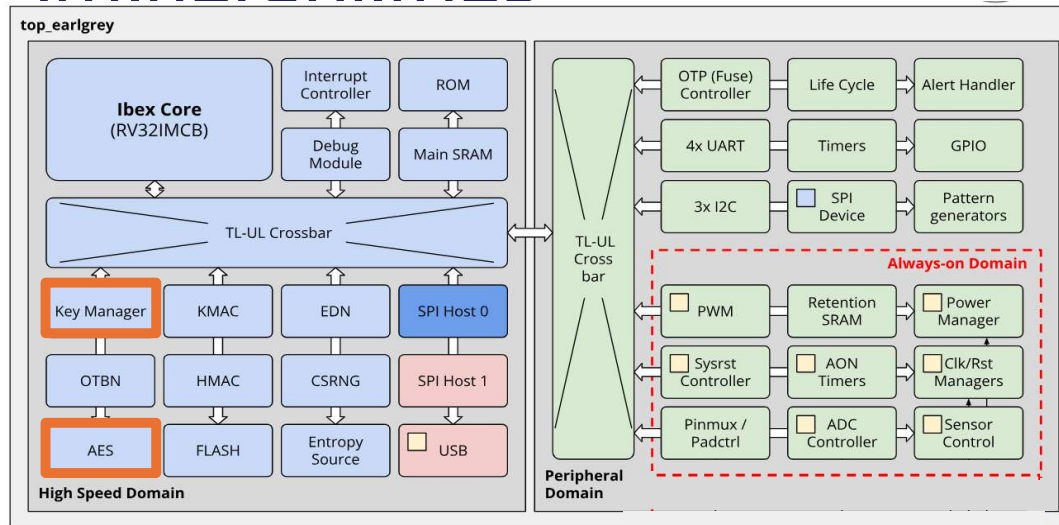


Security IPs – Verification Challenges



- Security (TrustZone, TZC-400)
 - World separation: Normal world vs Secure world must be strictly isolated.
 - Illegal access prevention: Verifying that GPU/DMA cannot access secure-only memory.
 - Corner case: Speculative loads/stores bypassing TZC checks.

Crypto Cores, AES, Key Manager Security Vulnerabilities



Abstract Data Transactions

Illegal data transfer: Confidential
→ Exposed

Valid data transfer: Exempt →
Exposed

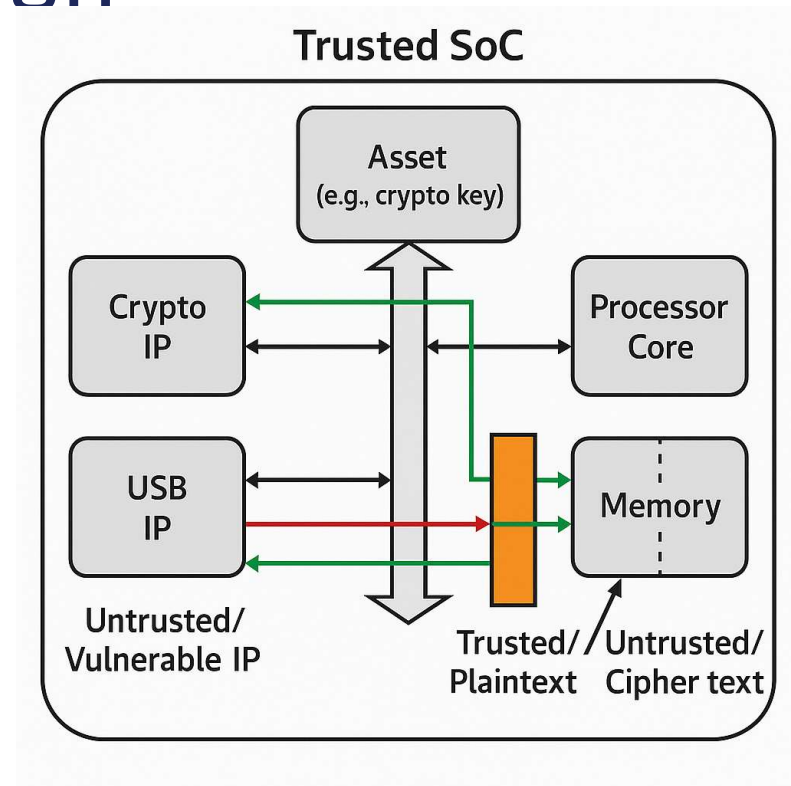
Illegal data transfer: Confidential
→ Exempt

Valid data transfer:
Confidential → Encrypted → Exempt

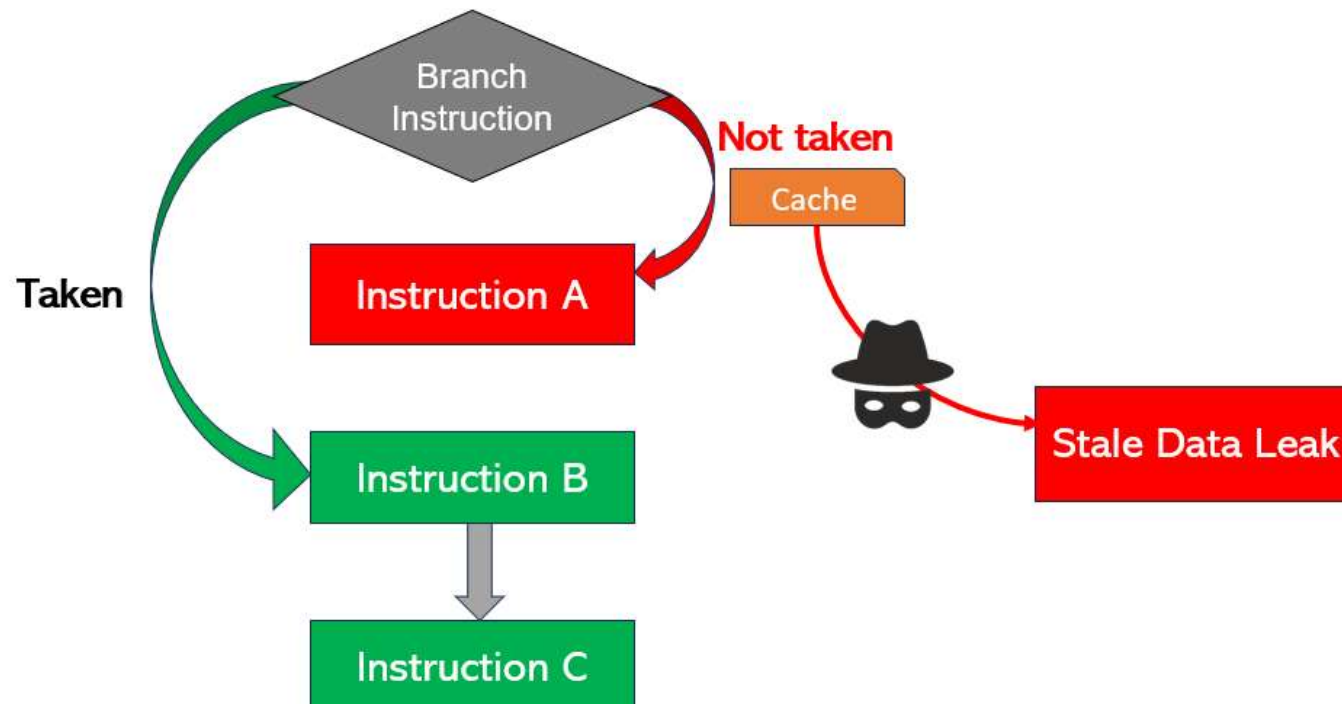
- Encryption/Decryption block
- Partition assets: Confidential, Exempt, and Exposed signals
 - Confidential signals hold secure data
 - Exposed signals are world readable
 - Exempt signals hold post-encryption data

Illegal Access Prevention

- Only Allowed Host can access
- Access permissions can be static or configurable



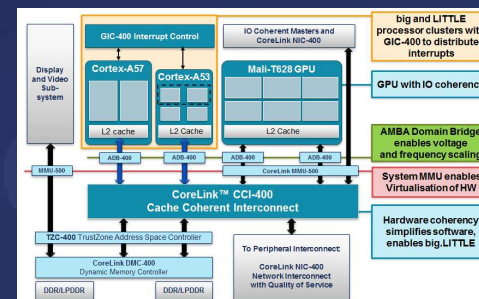
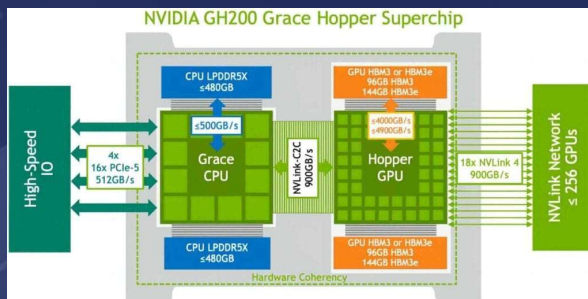
Speculative Load/Store Verification



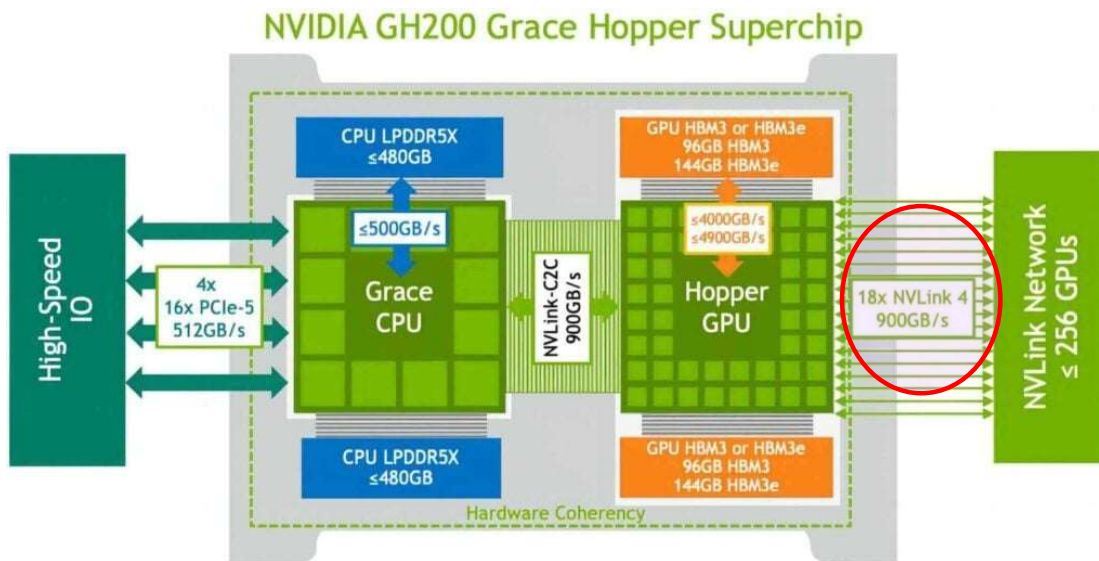
2026
DESIGN AND VERIFICATION™
DVCON
CONFERENCE AND EXHIBITION
UNITED STATES

SANTA CLARA, CA, USA
MARCH 2 - 5, 2026

Interconnect Verification Challenges



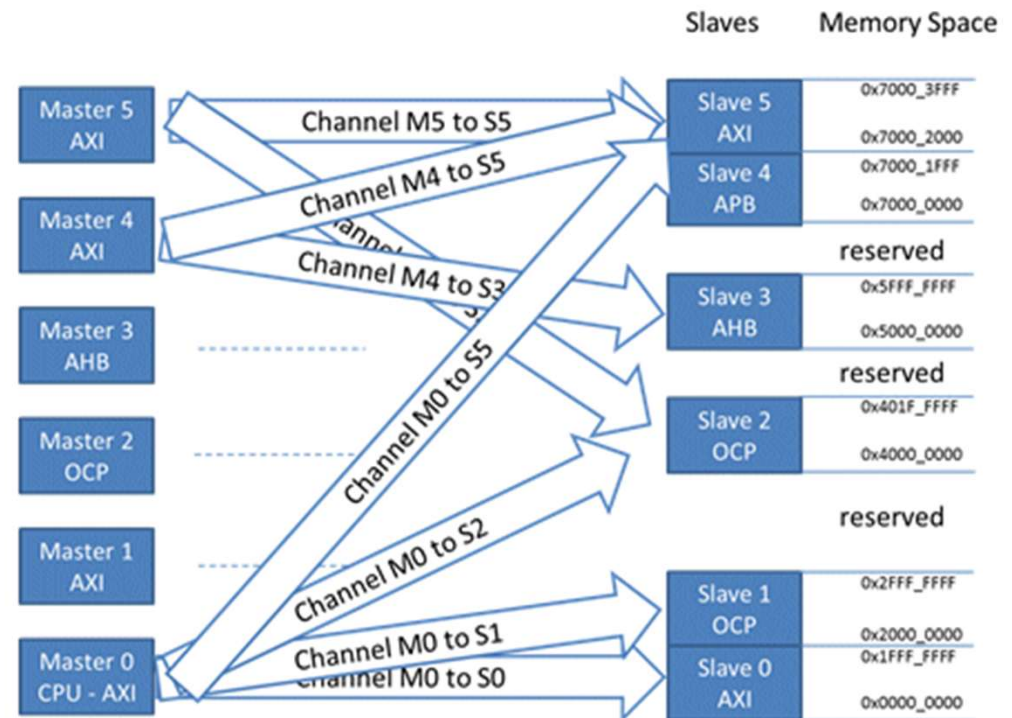
Interconnect Verification



- Data Integrity Verification
- Address Mapping Verification
- Routing Configuration Verification
- Quality of Service
- Security Access Verification

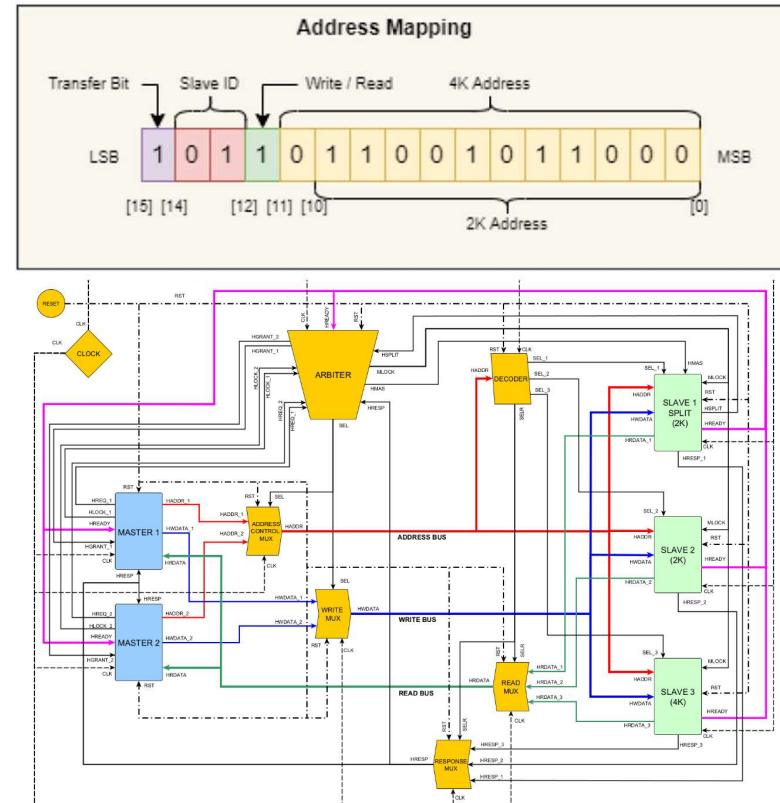
Interconnect Verification

- Reachability Verification
 - A particular master connected to slave
 - Protocol ports connected correctly
 - Connections through complex sequential logic (bridges etc.)
 - Negative verification – masters not connected to slaves as per specification



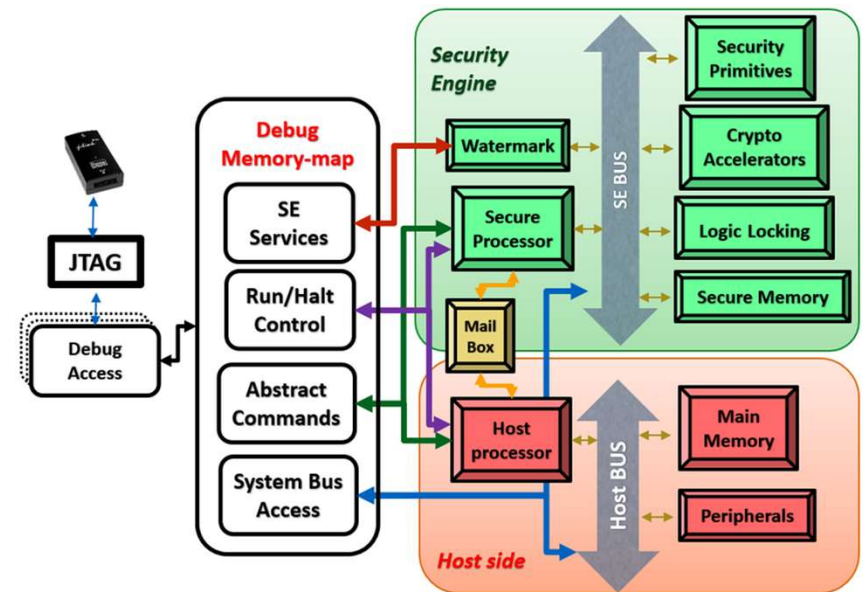
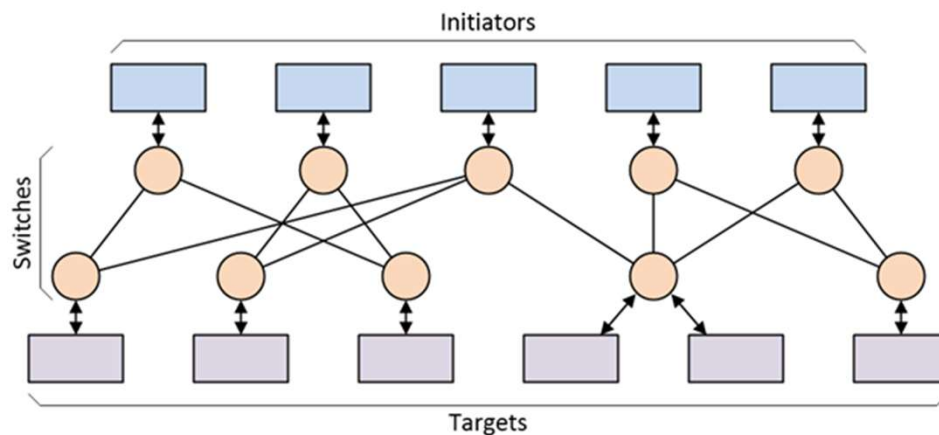
Address Mapping Verification

- Simple Data transfer
 - Master1 requests for bus access
 - Check
 - One cycle later Master1 granted bus access
 - Master1 deploys address and control data on address bus
 - Check
 - Sel pin toggles high for slave, HWDATA gets master DATA one cycle later
 - One cycle later HWRITE goes high and HRESP = 00 (meaning Ok transfer)



Secure Access Verification

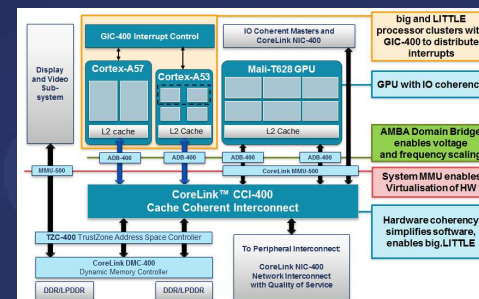
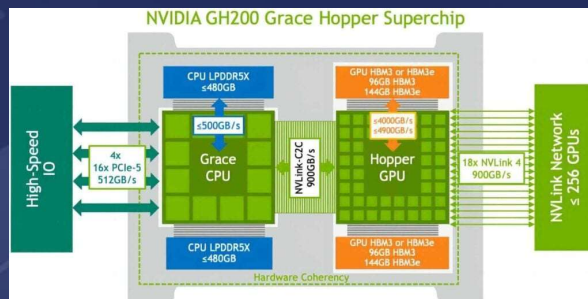
- Secure Interconnect initiator, target access
- Debug interface protection



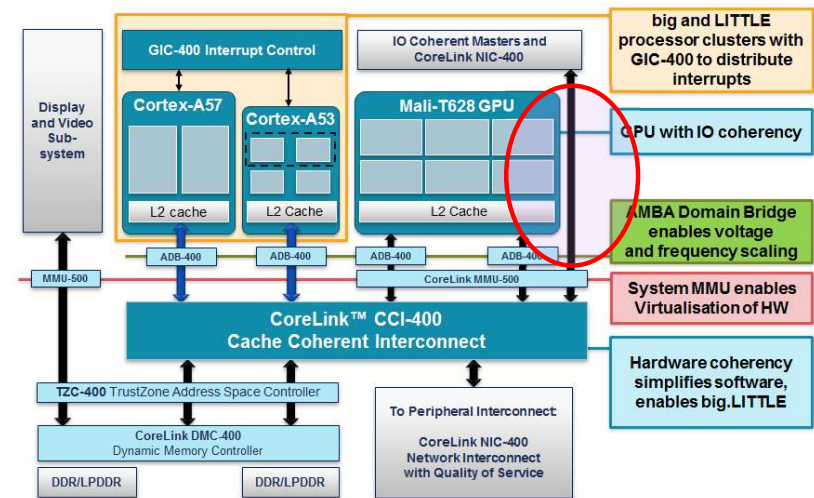
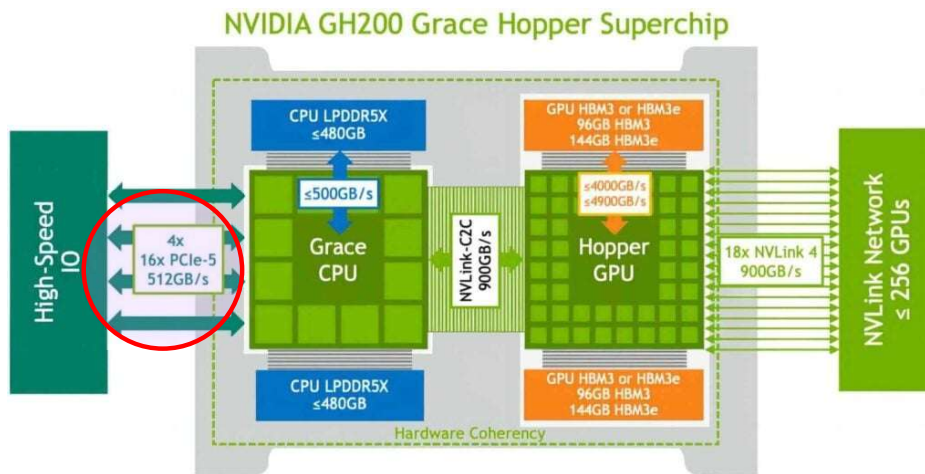
2026
DESIGN AND VERIFICATION™
DVCON
CONFERENCE AND EXHIBITION
UNITED STATES

SANTA CLARA, CA, USA
MARCH 2 - 5, 2026

IO Verification Challenges

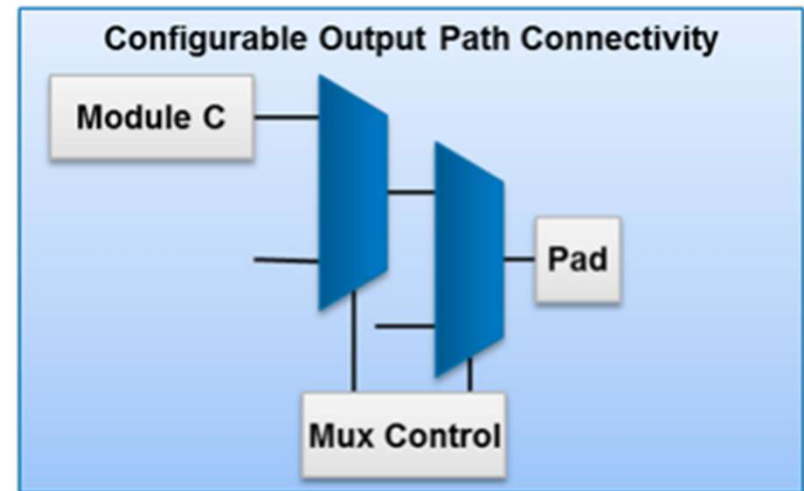
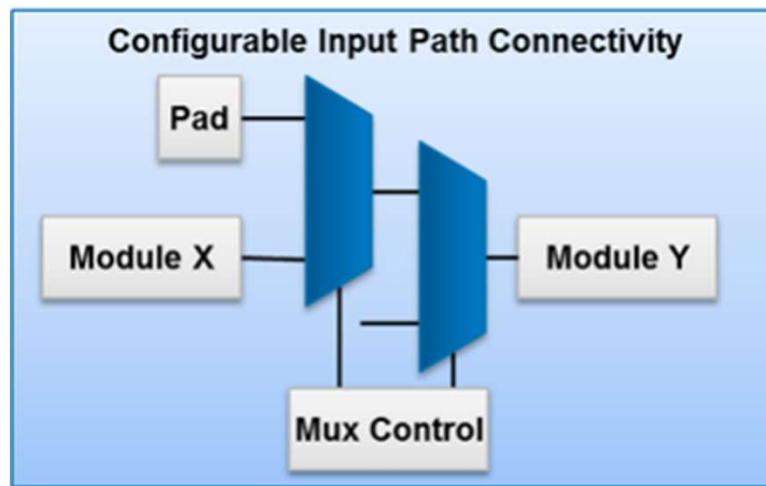


IO Verification



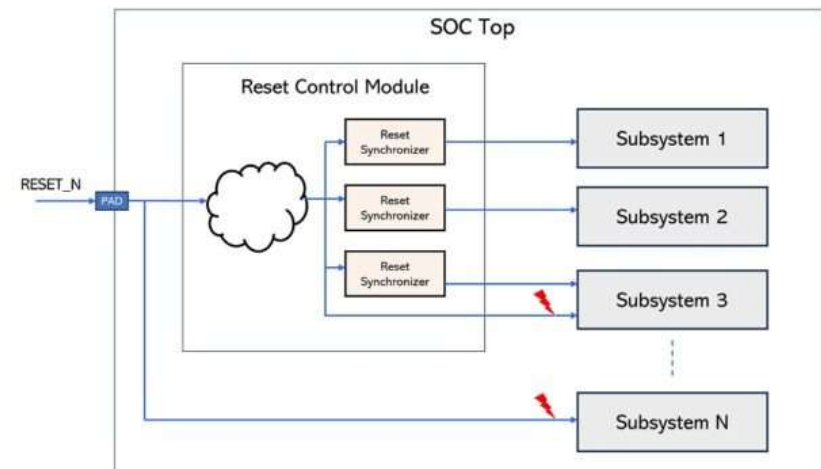
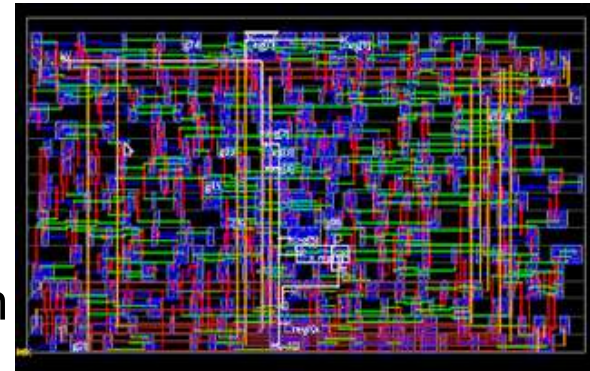
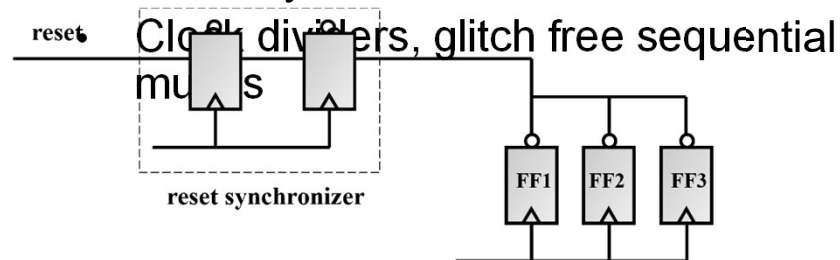
IO Verification

- Source to Destination connection
 - Based upon conditions



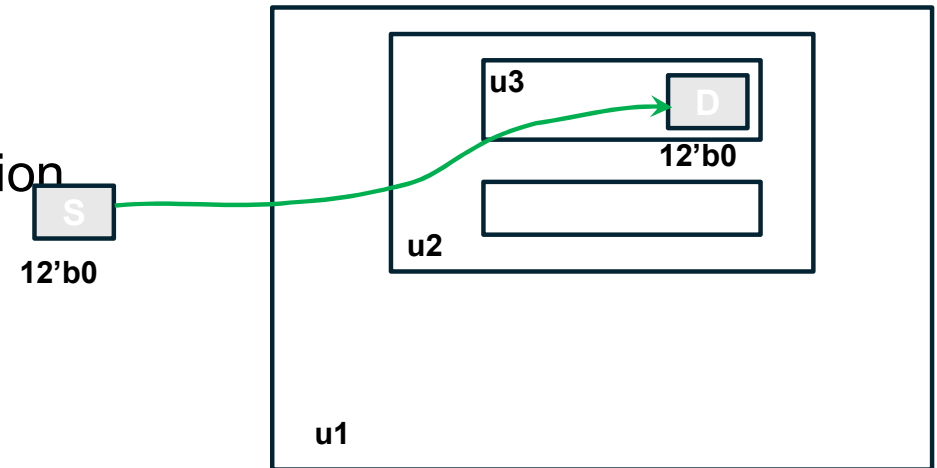
IO Global Signals

- Reset, Clock and Global signals
 - Connected to all the flops in the design
 - Millions of paths
 - Polarity is important
 - Can propagate through specialized cells
 - Reset synchronizers



IO Registers Verification

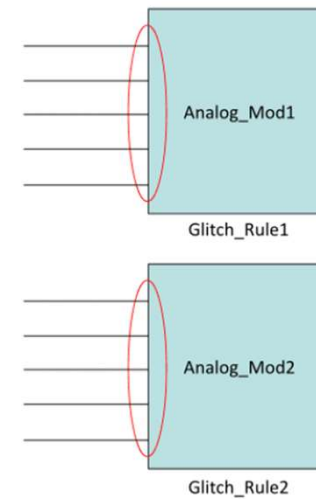
- System Registers, Configuration registers
 - Specific connectivity register based
 - Can propagate through sequential
 - Not just connection, value propagation also important



IO A/D Interface Glitch Verification

```
create_group -name AM1_IN -module Analog_Mod1 -all_inputs  
set_no_glitch -to_group {AM1_IN} -rule Glitch_Rule1
```

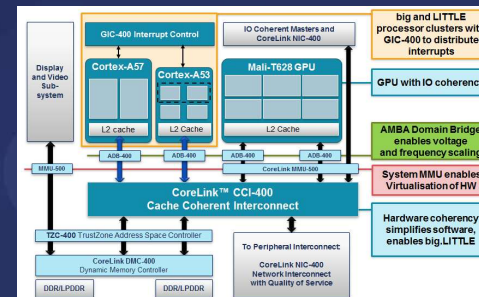
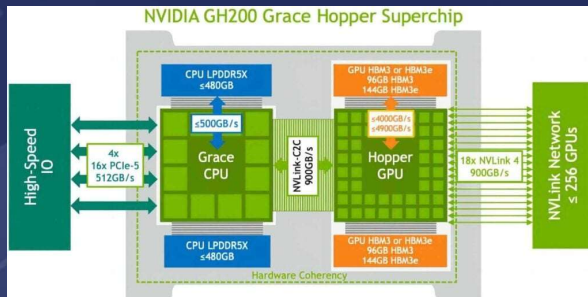
```
create_group -name AM2_IN -module Analog_Mod2 -all_inputs  
set_no_glitch -to_group {AM2_IN} -rule Glitch_Rule2
```



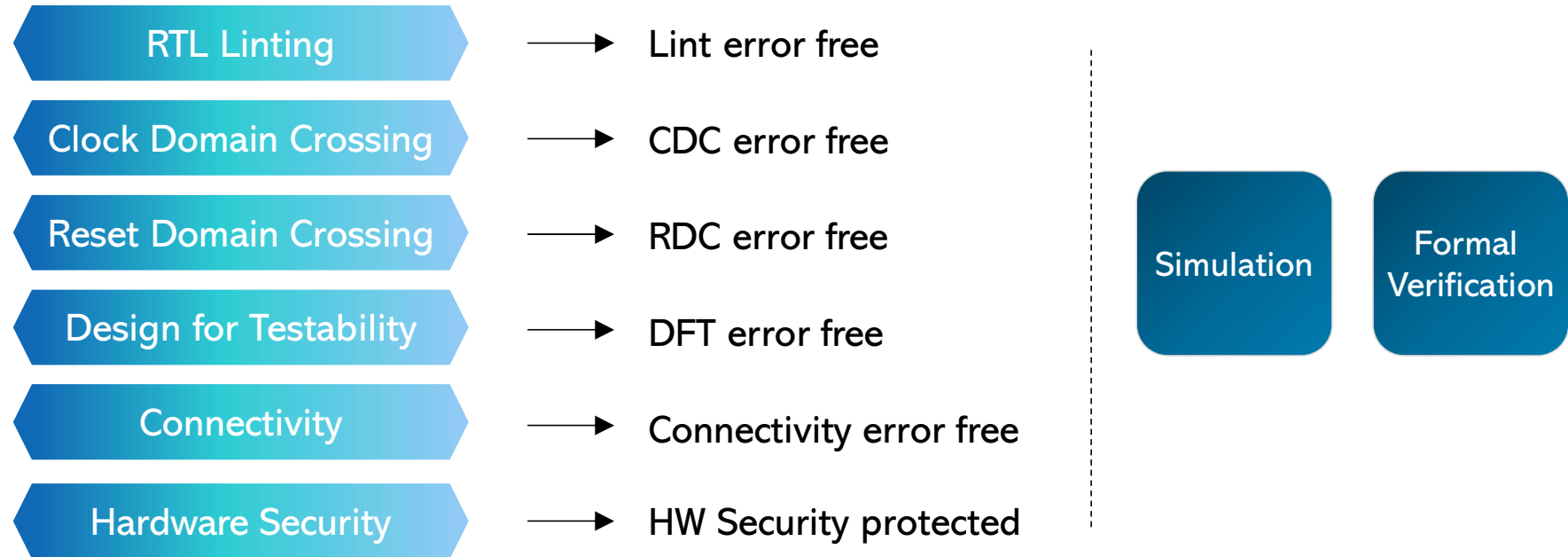
2026
DESIGN AND VERIFICATION™
DVCON
CONFERENCE AND EXHIBITION
UNITED STATES

SANTA CLARA, CA, USA
MARCH 2 - 5, 2026

Addressing These Challenges with Static Signoff

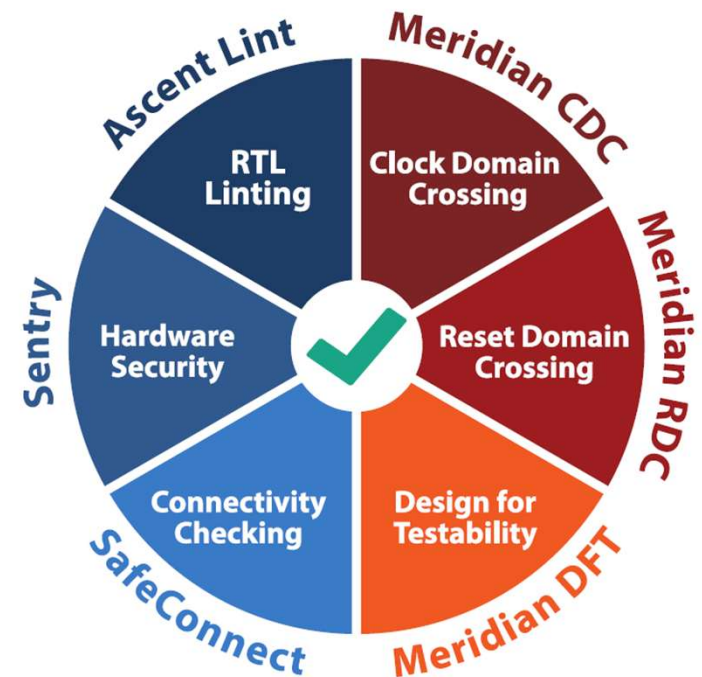
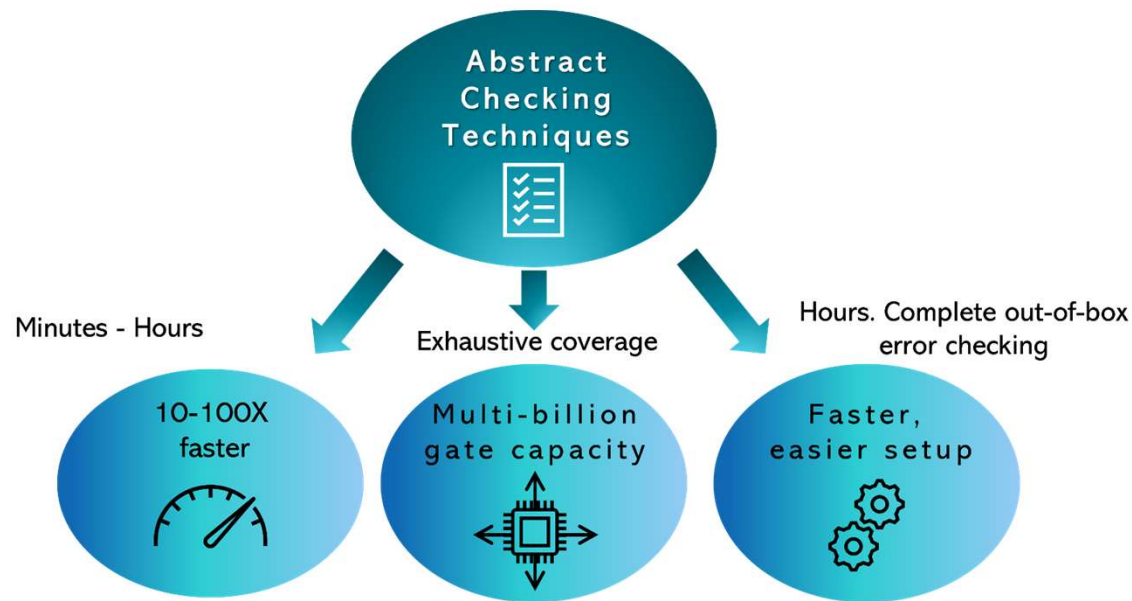


Static Signoff Paradigm is Expanding



Simulation and Formal have their role to play
**Use Static Signoff effectively and judiciously to
make verification faster, more predictable, and tape-out chips without risk**

Signoff with Static



Where Our Technology Is Adding Value

SPACEX

WD Western
Digital®

Google

icsense
THE IC DESIGN COMPANY

paloalto
NETWORKS®

SAMSUNG

MI maxim
integrated™

JARIET
Technologies

NVIDIA®

dialog
SEMICONDUCTOR

NEC

MARVELL™

ORACLE

MicroVision

TARANA

gyrfalcon
technology

FORTINET®

Microsoft

knowles

PETAIO

HAILO
Empowering Intelligence

CERAGON

NAVSEA
NAVAL SEA SYSTEMS COMMAND

U.S. ARMY

Materials Magic
Hitachi Metals

SatixFy

D E Shaw Research

Esperanto
TECHNOLOGIES

Viasat
HARRIS®

LOCKHEED MARTIN

AVI

Valens

2026
DESIGN AND VERIFICATION™
DVCON
CONFERENCE AND EXHIBITION
UNITED STATES
SANTA CLARA, CA, USA
MARCH 2 - 5, 2026

QnA

