Jasper Formal Verification Overview

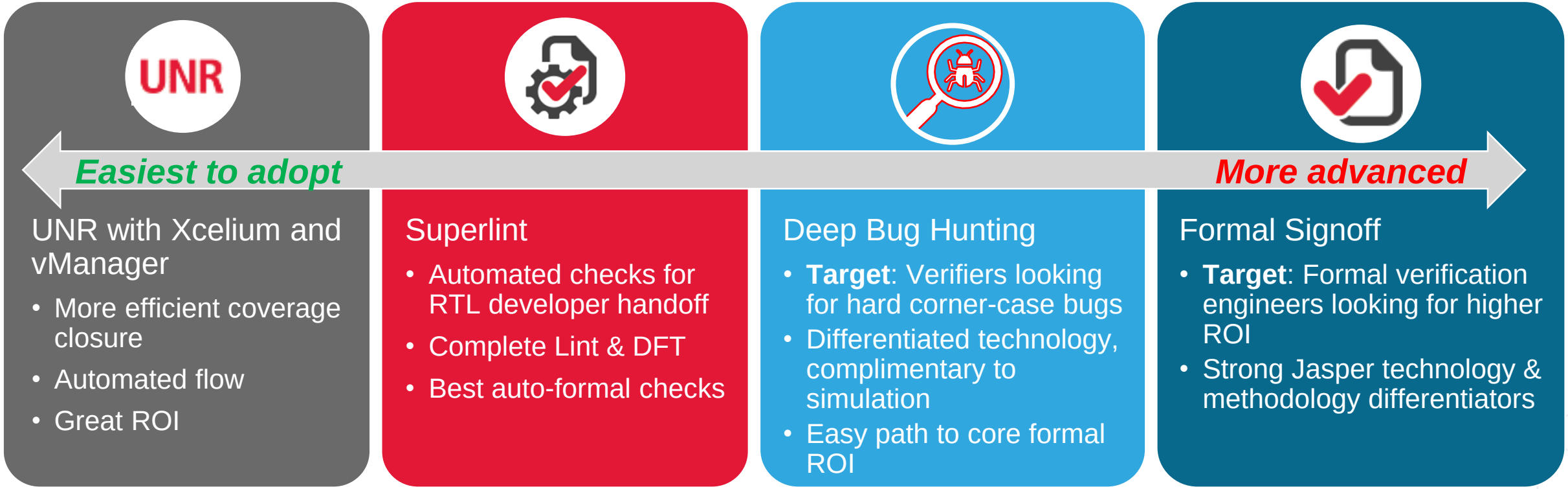
YC Lan, Formal Solutions

Oct. 2022

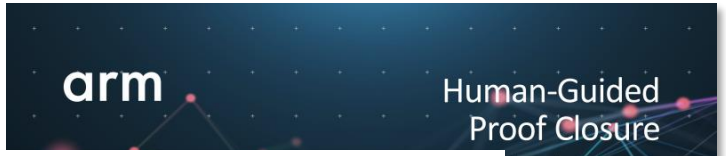
cadence®

Jasper Momentum Continues

- Used by 19 of top 20 semiconductor companies, 40+ new logos in 2021
- Jasper Apps to get started with for verification engineers, designers & formal specialists:



Jasper Formal: New Users and Applications



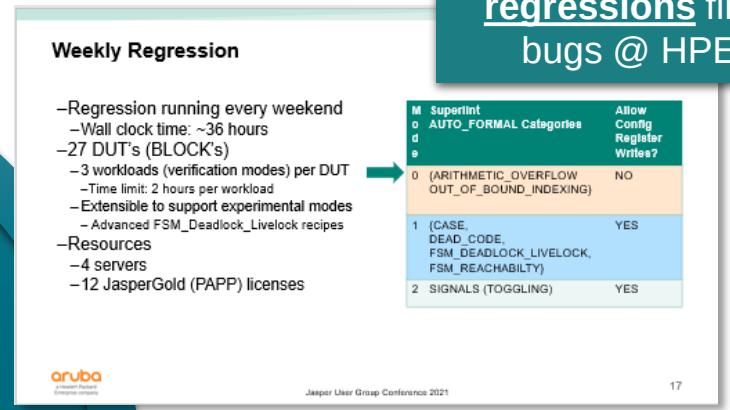
Results

- M-Class processor fetch queue
  - Proof closure of key, end-to-end properties
- M-Class processor pipeline properties
  - 10% more properties proven in regressions
- A-Class processor core
  - Real-bug discovered in the process of discovering helpers (not found by other means)
  - Proof closure of helpers achieved after bug resolved

Converging **end-to-end proofs** on CPUs @ Arm
Best Presentation winner!

Expert Formal

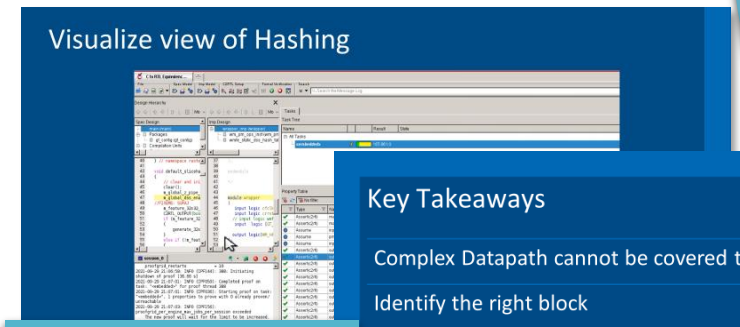
Designer Bring-up

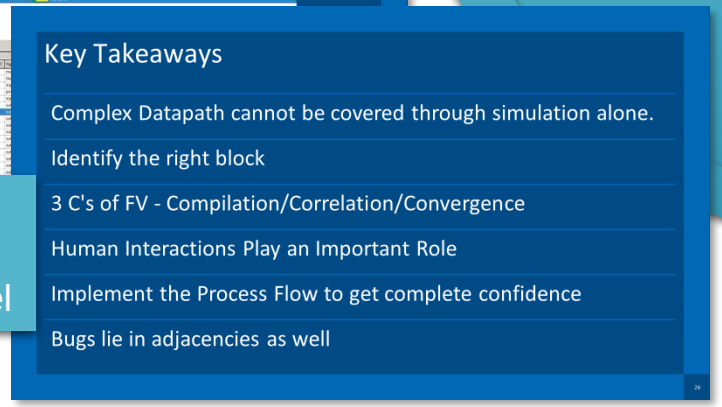


Superlint weekly regressions finding key bugs @ HPE Aruba

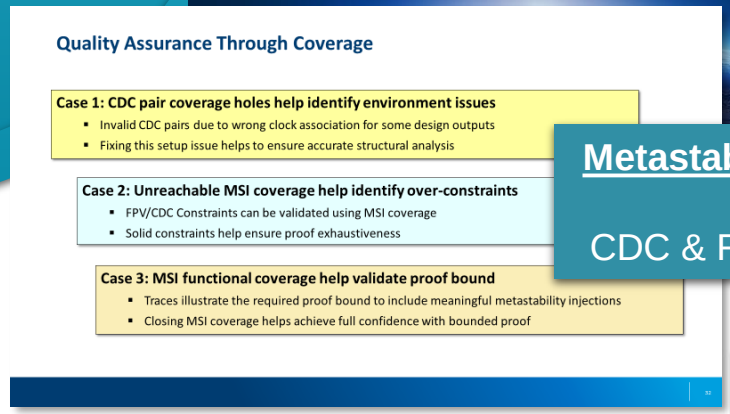
C2RTL Formal

Formal CDC Signoff



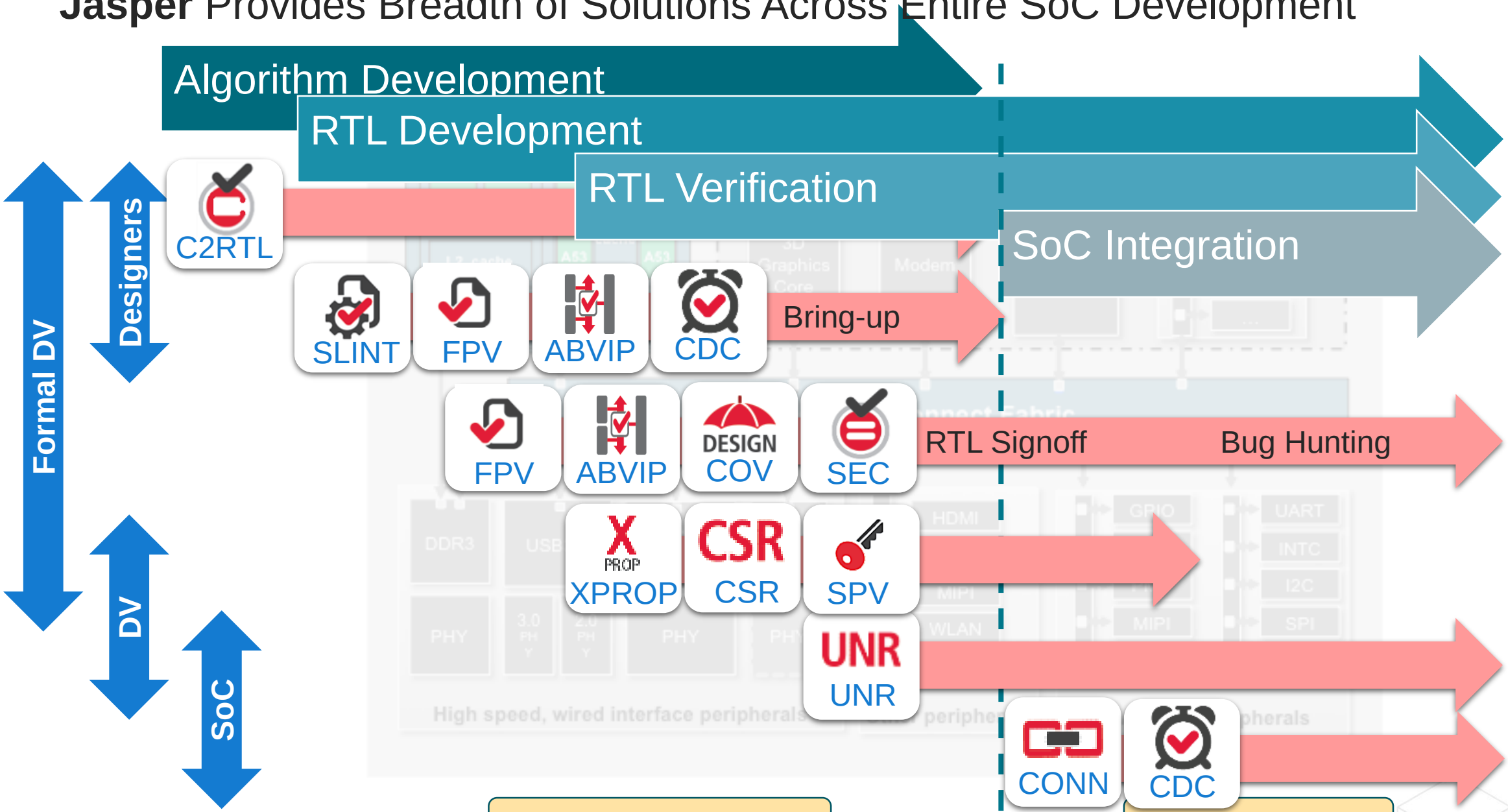


C++ to RTL Datapath verification @ Intel

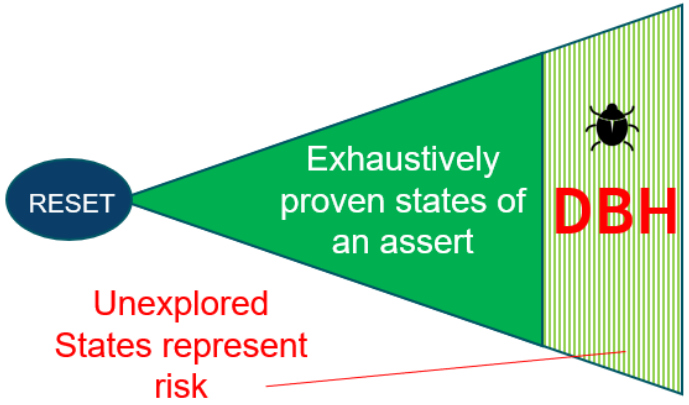


Metastability-aware CDC sign-off
CDC & FPV apps @ Intel

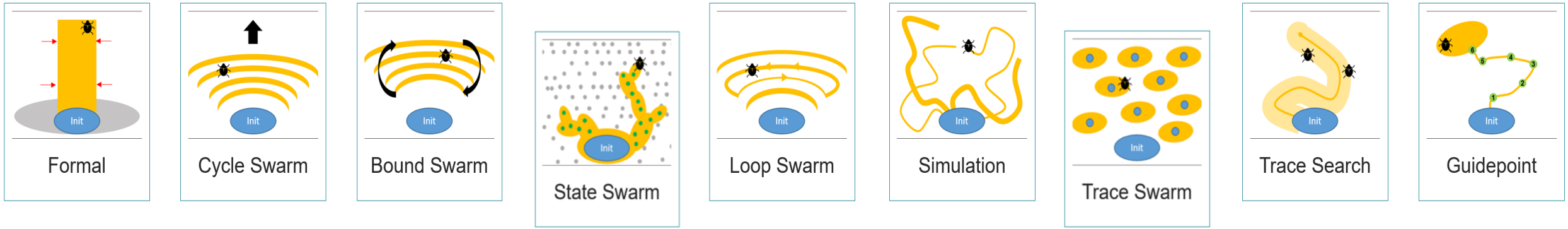
Jasper Provides Breadth of Solutions Across Entire SoC Development



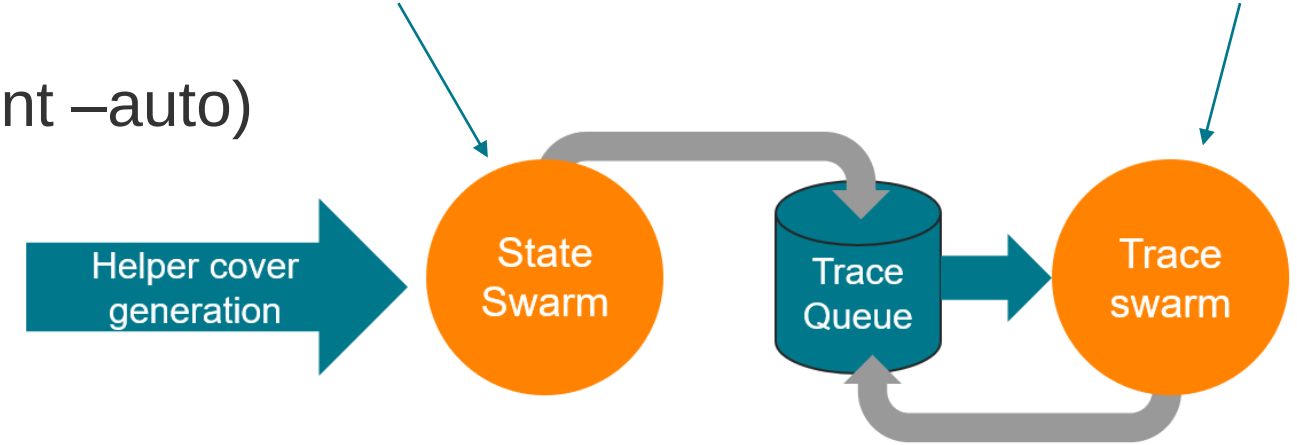
Bug Hunting with Jasper



- Jasper provides range of specialist bug hunting modes
  - Each designed to reach deeper states beyond the proof bound



- Automation (hunt –auto)



Jasper on AWS Cloud (JAWS) and Graviton Support

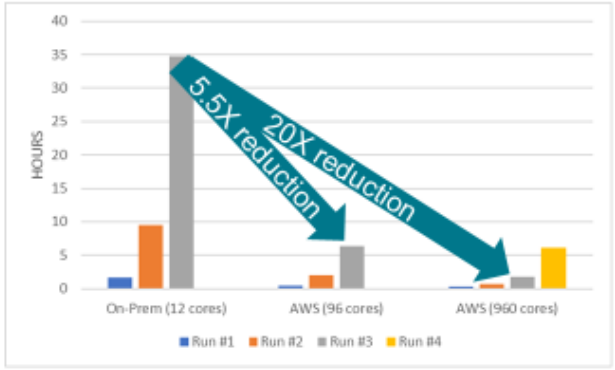
- Cloud makes it economic to use **massive parallelism** to find hard-to-reach bugs
- Arm published great results on AWS Graviton2 in October 2021

JAWS Results

Time for each iteration

STEP	# undet (start)	# undet (end)	time/prop	CORES	minutes
compile					12
iteration #1	343	188	1m	12	85
				96	17
				960	8
iteration #2	188	101	10m	12	470
				96	95
				960	20
iteration #3	101	35	1h	12	1515
				96	258
				960	68
iteration #4	35	28	2h	12	n/a
				96	n/a
				960	262

Total Time



- We ran iterations #1 through #3 on all 3 configurations
- We ran iteration #4 for **6 hours** on AWS 960 core configuration only
  - Estimated runtime **5 days** in-house with 12 cores, 22 hours with 96 cores
  - Completed 7 more properties, with 28 undetermined including 23 useful bounded proofs:
  - Min bound 52 cycles, max bound 978, average bound 189
  - 4 of the 7 determined properties were deep counterexamples (i.e. **security bugs**)

cadence

Cadence JasperGold Performance on AWS Graviton2

In this blog we compare the performance and price to run Cadence's JasperGold formal verification software on AWS Graviton2 compared to x86-based instances.

Tim Thornton

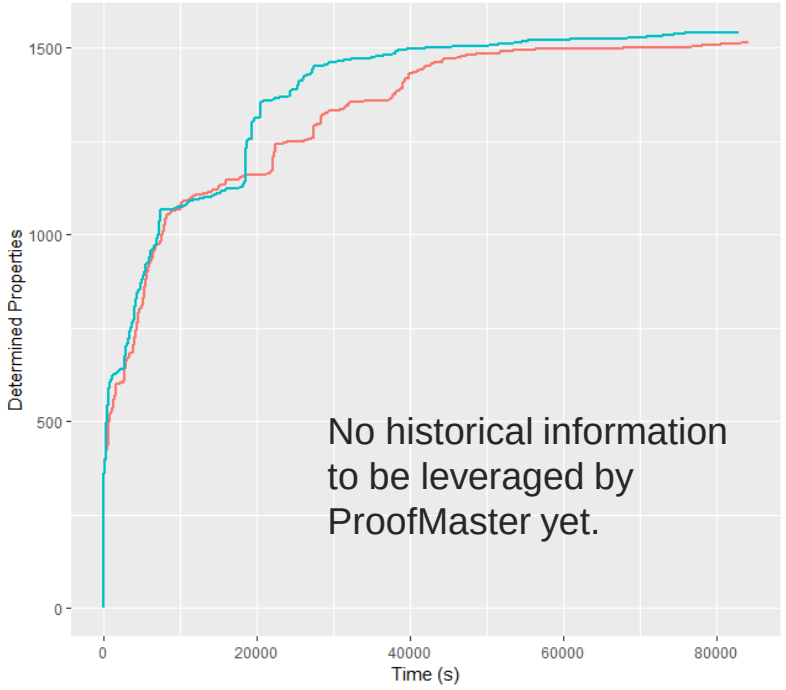
"We found that the x2gd completed our test suite 33% faster than the x1, leading to a cost per run that was 47% less expensive"

cadence

Benchmark Results

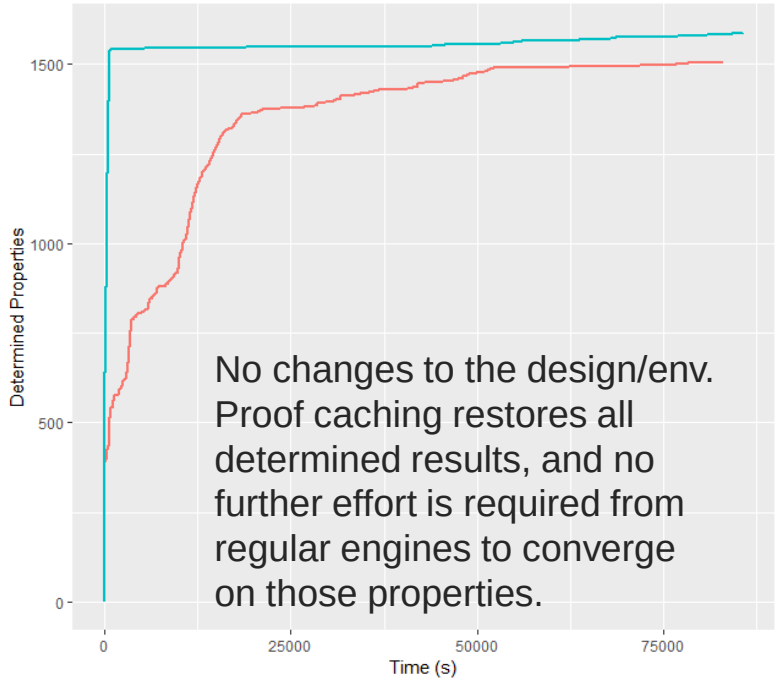
Customer Design Changing Over Time

Design Drop #1 → Design Drop #2 → Design Drop #3 → time



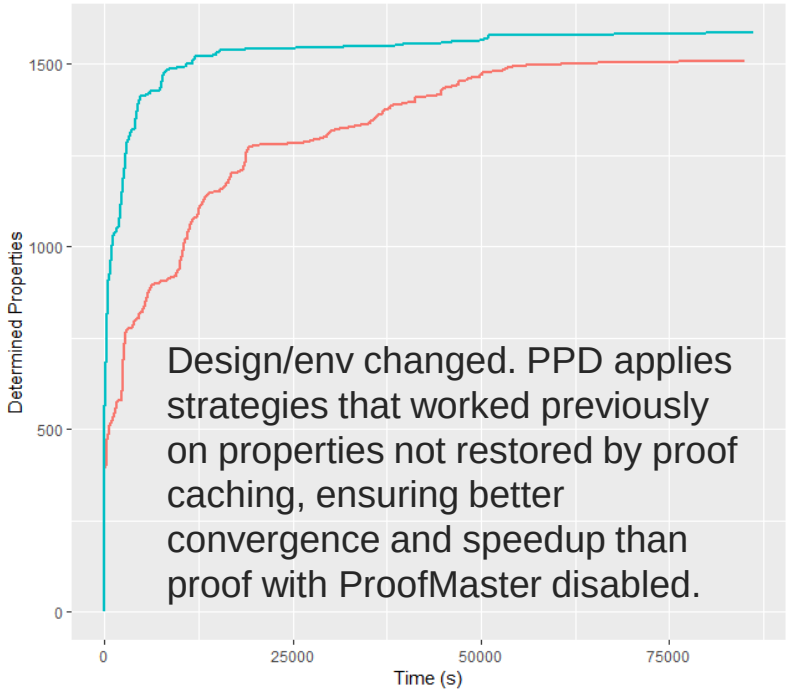
No historical information to be leveraged by ProofMaster yet.

Run	# Determined
ProofMaster OFF	1516
ProofMaster ON	1543



No changes to the design/env. Proof caching restores all determined results, and no further effort is required from regular engines to converge on those properties.

Run	# Determined
ProofMaster OFF	1506
ProofMaster ON	1590

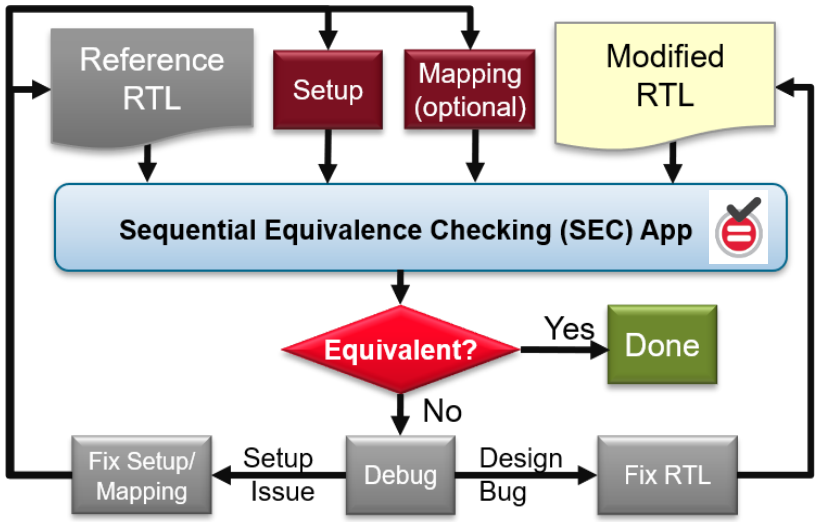


Design/env changed. PPD applies strategies that worked previously on properties not restored by proof caching, ensuring better convergence and speedup than proof with ProofMaster disabled.

Run	# Determined
ProofMaster OFF	1510
ProofMaster ON	1586

Sequential Equivalence Checking App

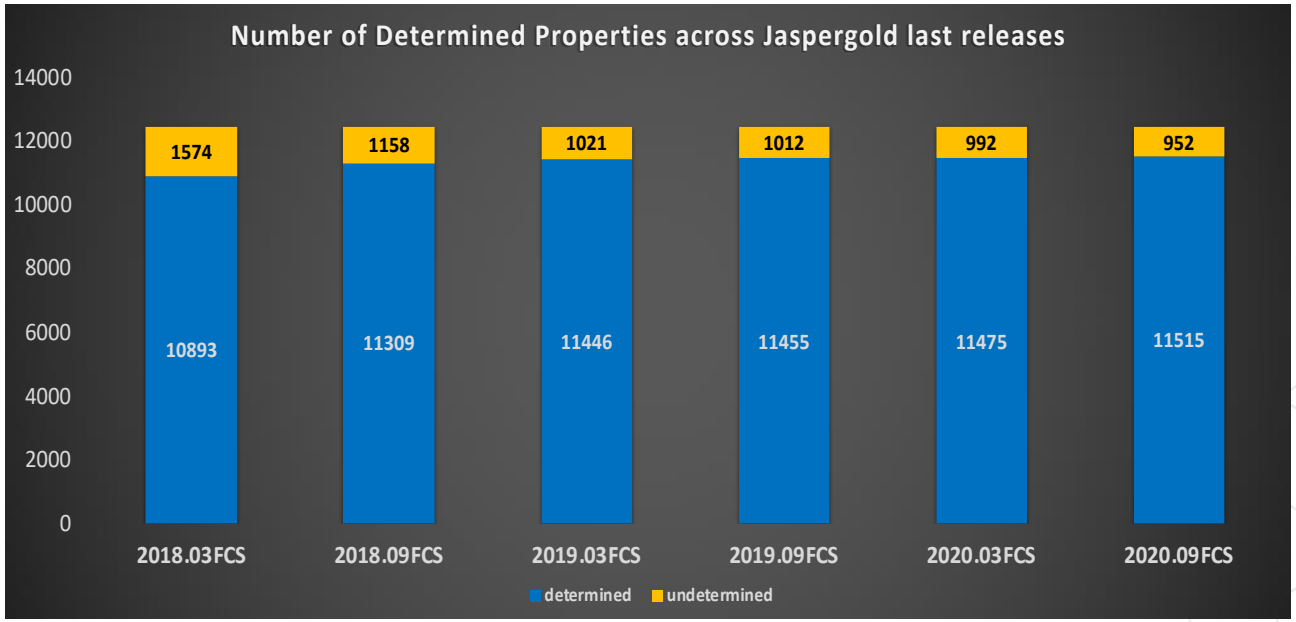
Accelerates design convergence



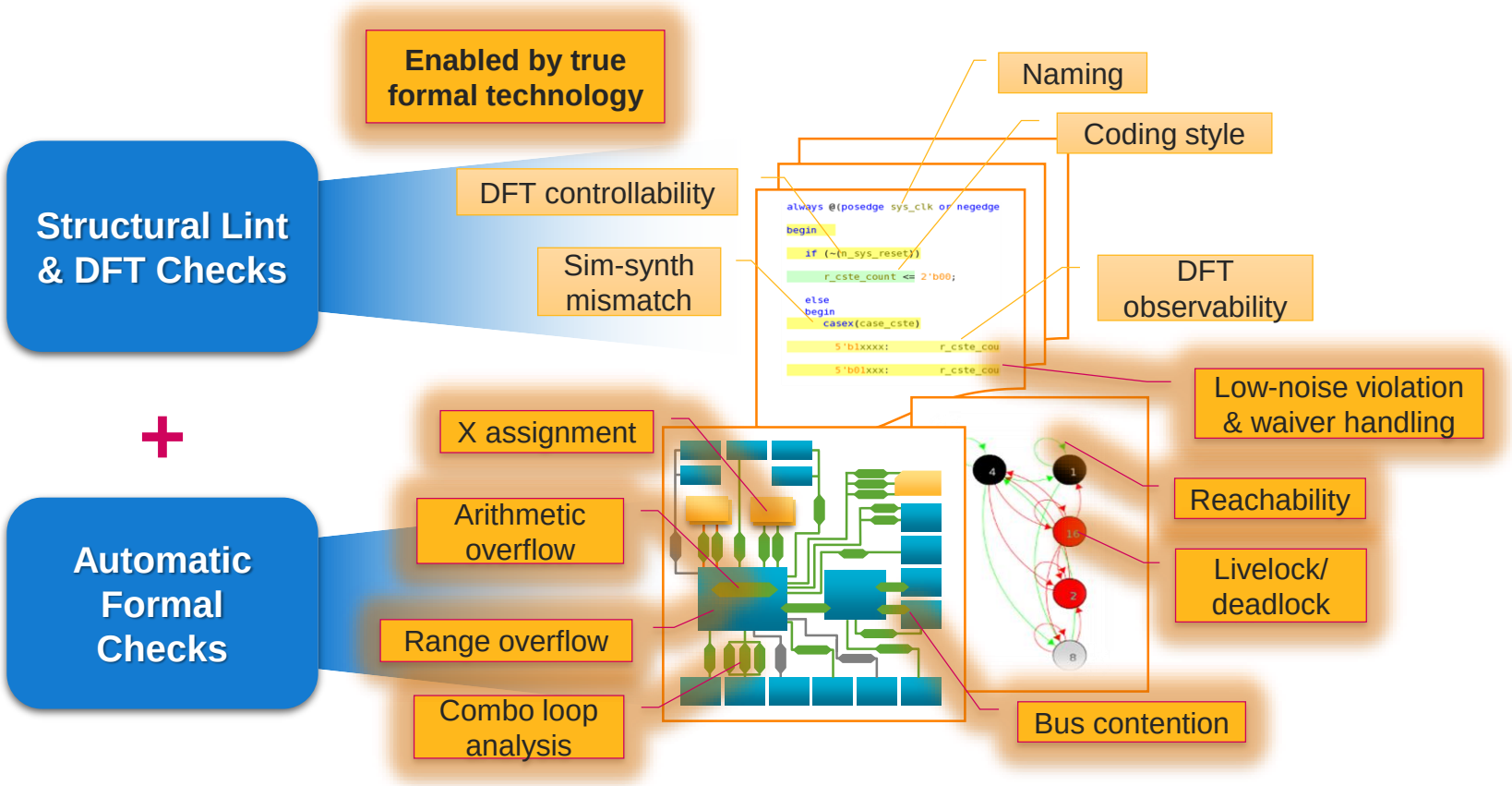
- Sweet-spot use cases:
  - Clock Gating Optimization
  - Pipeline Retiming

What's new?

- Performance and convergence boost using **Proof Cache** and **DBH** technologies
- Over-constraint debug
- Compound signals mapping



Jasper Superlint: Hand-off **Robust Reusable RTL**

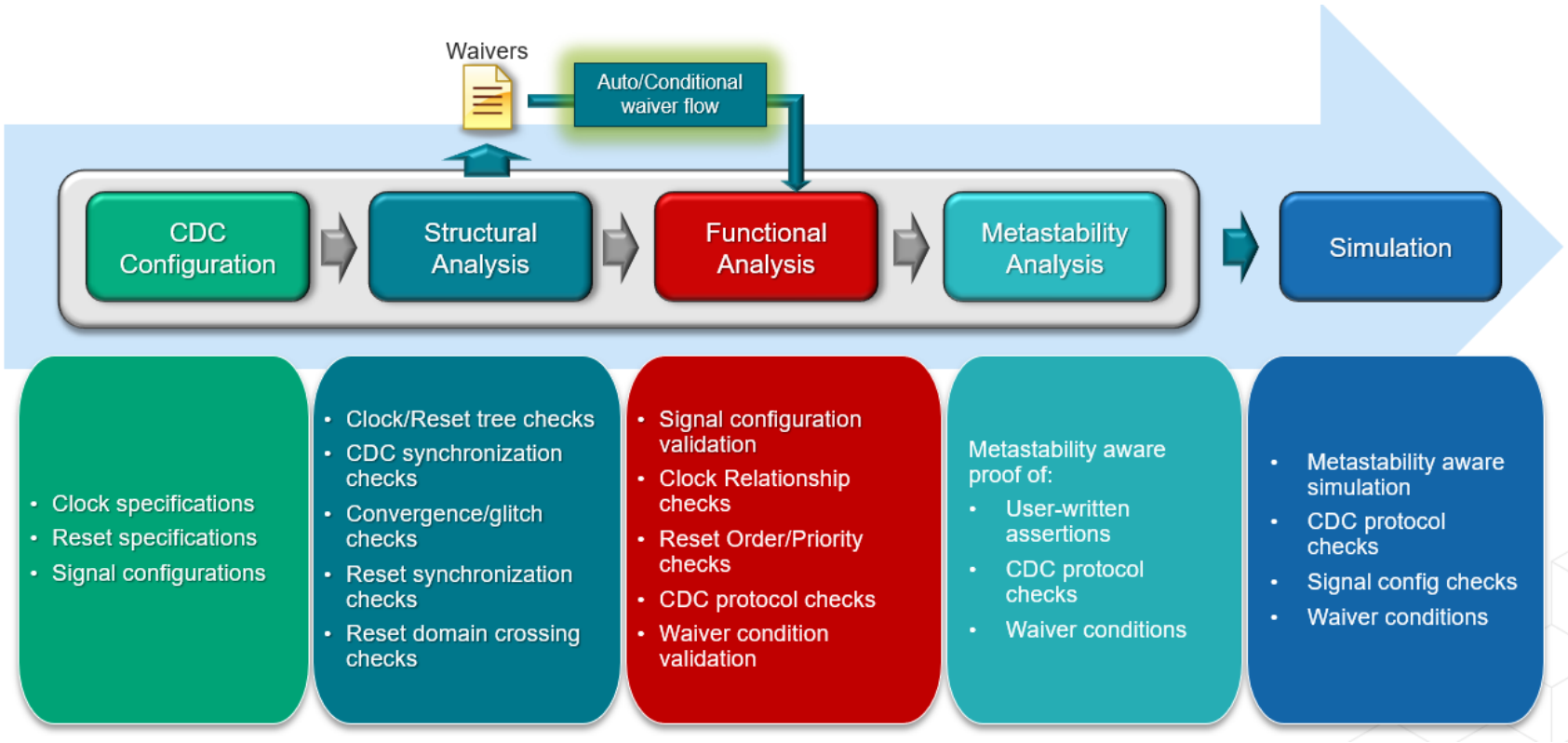


Comprehensive functional checks, violation debug & waiver handling based on best-in-class formal analysis

- **For comprehensive signoff augment with Auto-Formal checks**
- **Jasper™ Superlint is industry leading solution for RTL signoff**

  - ✓ Comprehensive structural LINT and DFT checks
  - ✓ High value auto-formal checks
  - ✓ Easy setup and feature rich analysis and debug environment
  - ✓ Designed to be low noise and high productivity application

Jasper CDC: Hand-off **CDC/RDC-clean RTL**

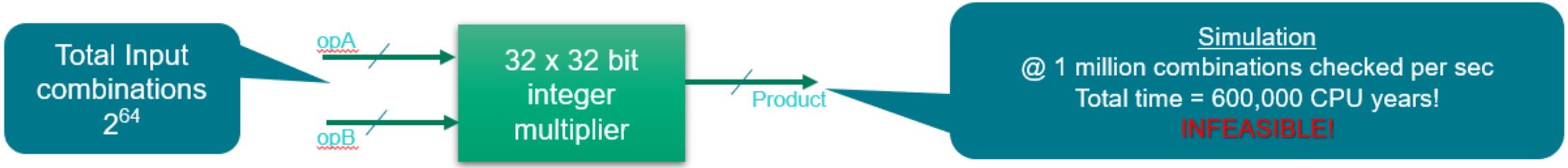


- **Focus beyond structural analysis**
- **Jasper™ CDC App is a holistic CDC/RDC verification solution**

  - ✓ Comprehensive structural checks
  - ✓ Functional CDC/RDC verification
    - Constraint validation
    - Waiver validation
    - CDC protocol verification
  - ✓ Metastability aware verification

The only CDC + RDC solution with industry-leading formal technology for functional checks and violation/waiver handling

Jasper C2RTL Datapath Verification



- Intel's infamous **Pentium FP Division bug** (1994)
  - Corner case: 1 in 9 billion random simulations would produce an inaccurate result
  - Intel recalled faulty processors → cost Intel $475 million *(source: https://en.wikipedia.org/wiki/Pentium_FDIV_bug)*

- Most datapath algorithms developed at a high level in C++ first, RTL designers then use C++ models as a reference while implementing RTL
  - Complex datapath cannot be covered through simulation alone

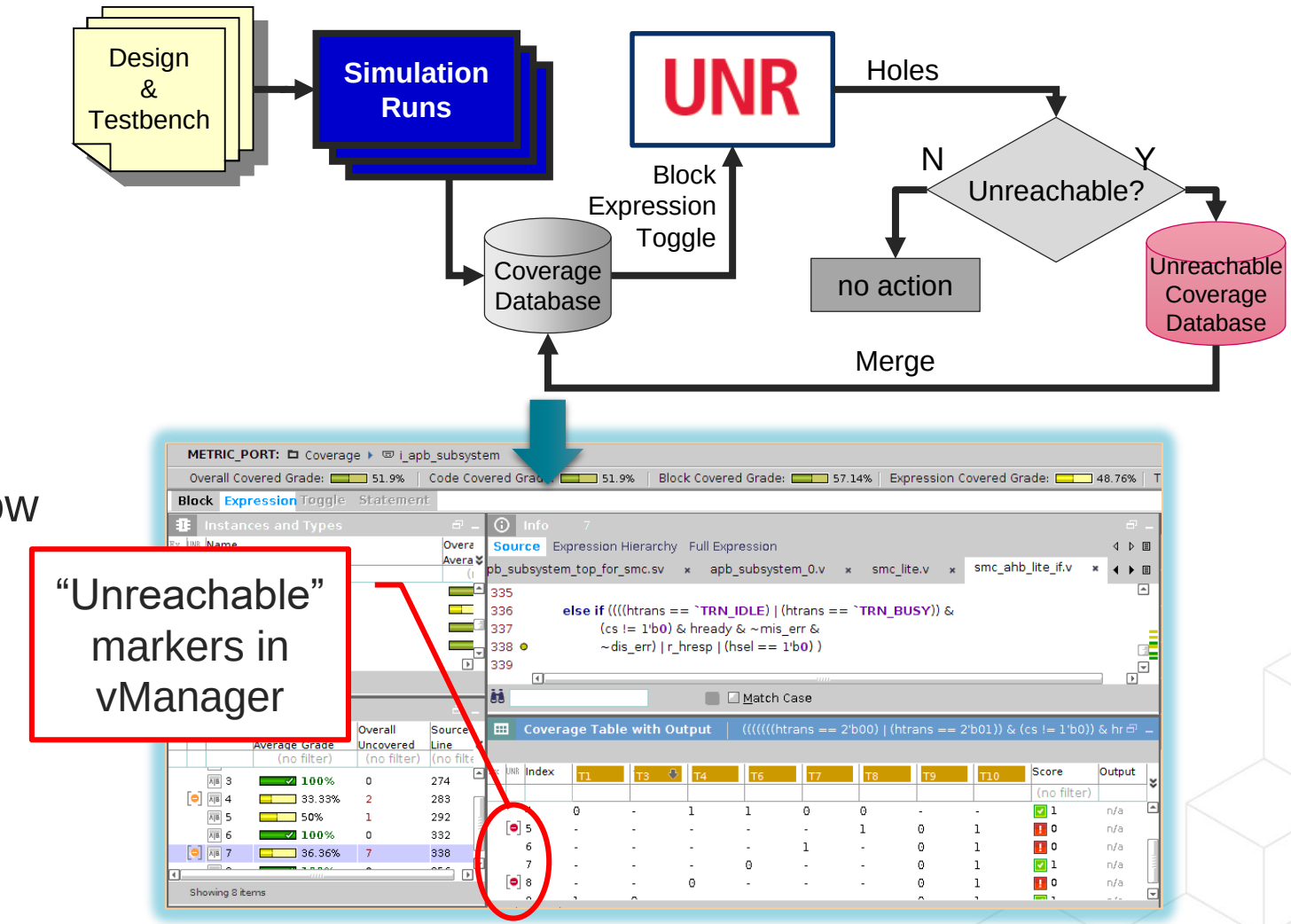
- Data manipulation/transformation algorithm
  - Unit arithmetic operations
    - Integer arithmetic, Floating Point arithmetic
  - Higher level image processing operations / algorithms:
    - ACE / LACE / Matrix multipliers / FFTs / DFTs / Compression / Decompression
  - Encryption / Decryption models
    - Several algorithms like AES, DES, RSA, MD5, etc.

Up to 100X performance improvement	New class of formal engines optimized for checking RTL datapath implementations versus their C/C++ algorithmic specifications Delivers industry-leading performance and capacity to check datapath implementation functionally matches algorithmic intent
Broadest C/C++ specification support	Innovative compilation technology co-developed with University of Oxford Supports latest ANSI C++ standards and common math libraries
Side-by-side C/C++ and RTL debug	Jasper™ Visualize debug technology extended to support C/C++ Enables user to directly compare RTL datapath implementation with C/C++ specification to speed debug and ease root cause analysis

Coverage Unreachability App

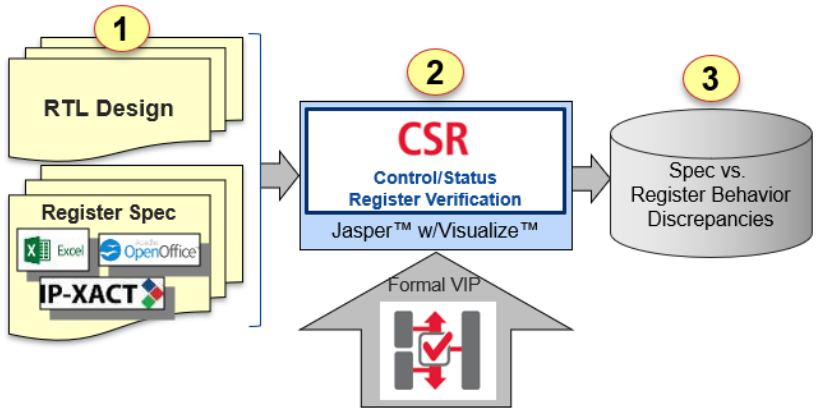
Saves simulation users weeks of time and effort for verification closure

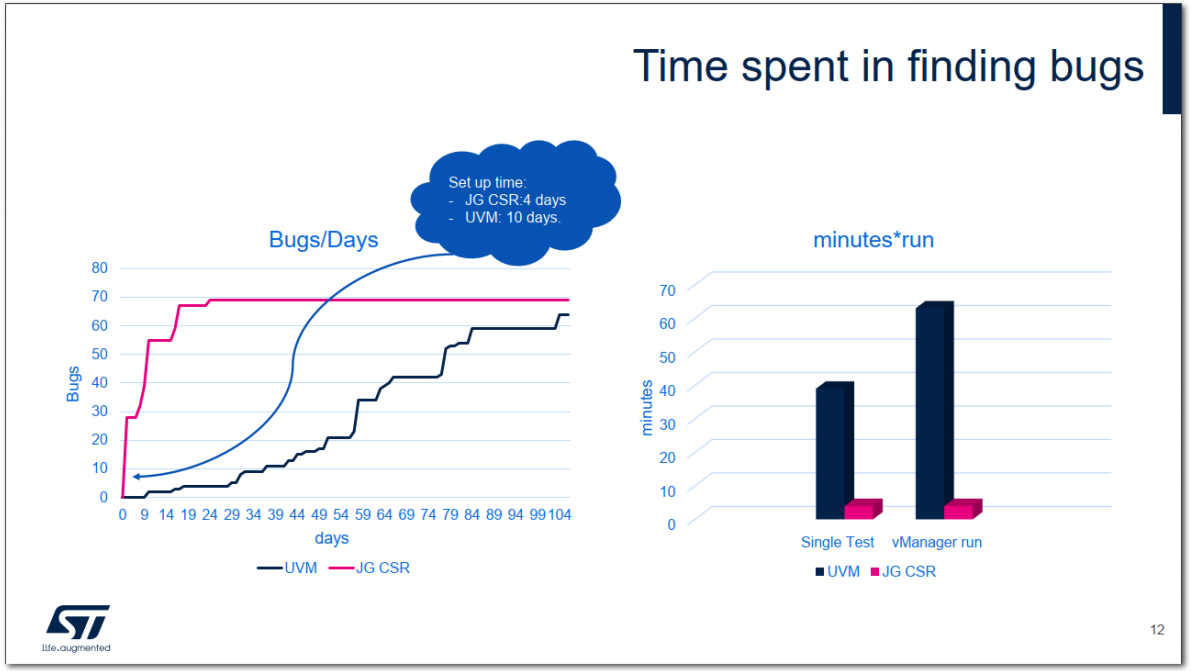
- Inputs: simulation coverage database and RTL
- Output: Unreachable cover points database
- Run by simulation users without formal expertise
- Integrated with vManager to clearly show unreachable coverage points
- Resilient compilation with Xcelium
- Supports all Xcelium modeling languages and setup



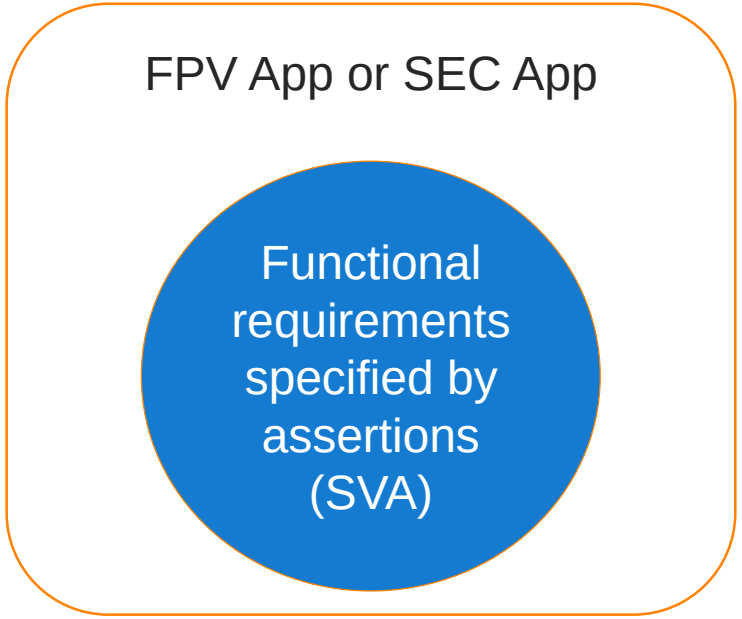
Control Register Verification App

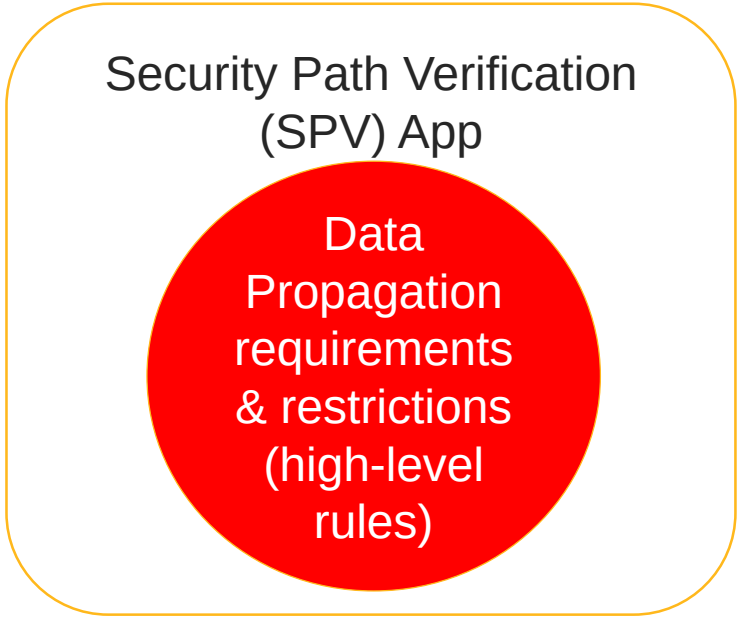
- Control and Status registers (CSRs) is a fundamental element for digital device and need to guarantee the absence of malfunctions.
- UVM:
  - Allows verifying register maps from design top, including bus hierarchy. But many verification objects have to be built at the beginning for verification kick-off. Result depends on the quality of testbench.
  - No way to know how many additional sequence are needed to cover all possible scenarios.
- Jasper CSR
  - Just load CSV/IPXACT and connect bus adapter to start verification.
  - Formal proof of a property provides a guarantee that no simulation will violate the property.





Security: Functional Data Propagation Requirements





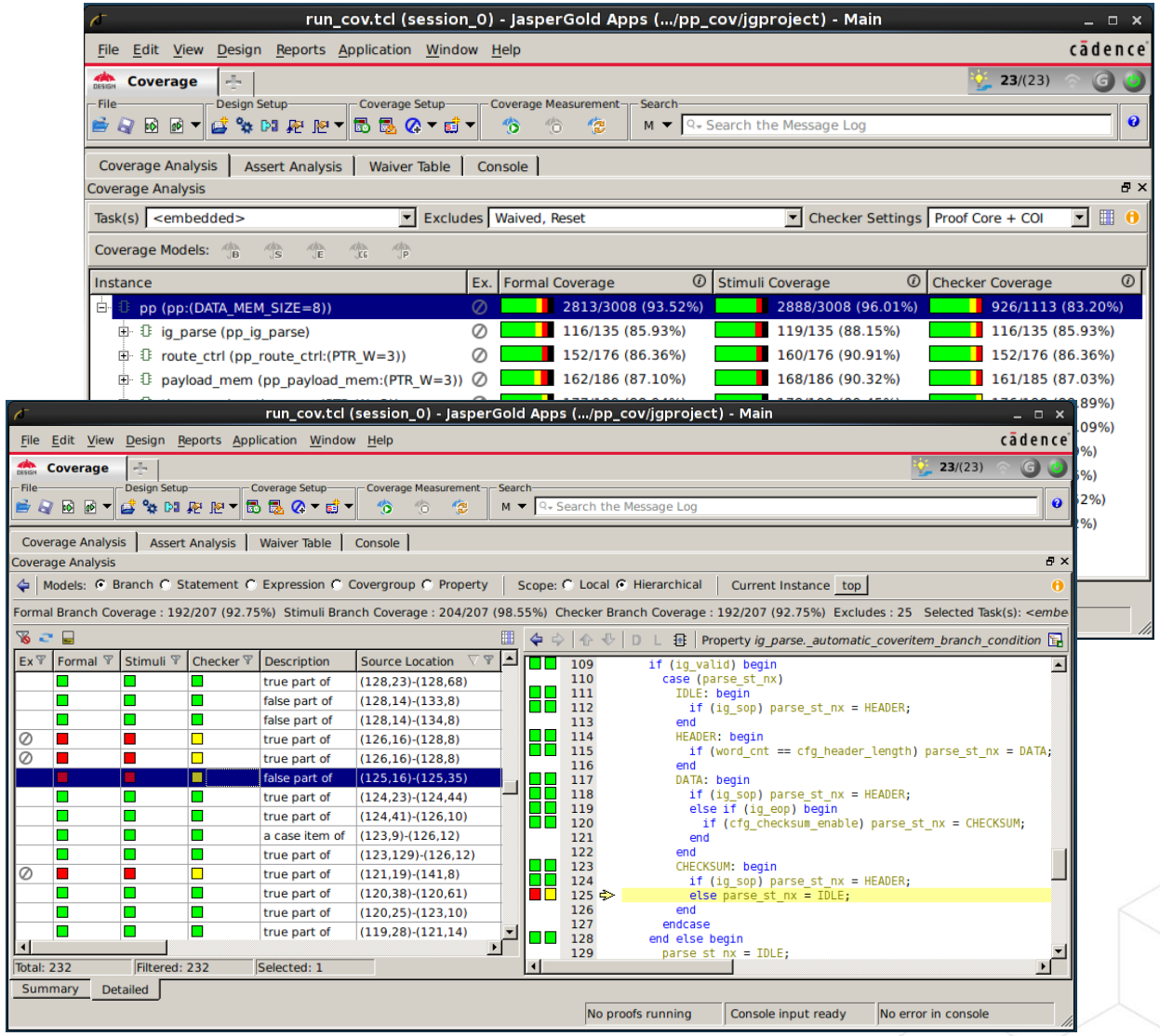
- Examples:
  - System must be reset if a environment monitor trips
  - FSM must never transition to SECURE after reaching TEST or DEBUG states

- Examples:
  - Secure register must not be written by non-secure agent

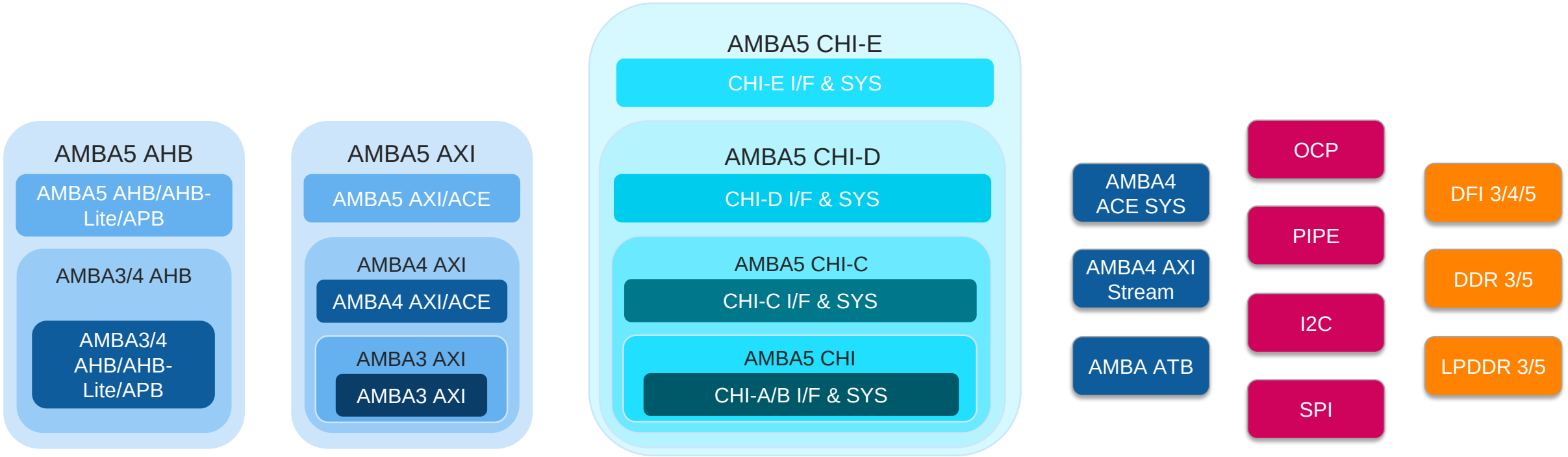
- Other Jasper Apps relevant to Security:
  - **CSR** app verifies integrity of register access policies
  - **FSV** app models direct attacks on internal HW circuitry

Signoff-Quality Formal Coverage

- Intuitive coverage analysis GUI
- Coverage runs independent from proof runs
- Deadcode vs. overconstrained identification
- Formal coverage metric combines stimuli and checker coverage
- Signoff-accurate proof-core coverage
- Mutation coverage mode for extra accuracy



Formal VIP Protocols Update



- Verifies compliance to standard protocols with exhaustive assertion-based verification IP libraries
- Enables automated, encapsulated, plug-and-play capabilities
- Provides quality support for spec-compliant designs

Introducing Jasper University

- Self-paced, virtual or instructor-led classes to get certified on Jasper apps and methodology
- 3rd party, independent management of certifications

Credly

- Benefits
  - Quickly create Jasper Formal expertise in your teams
  - Jumpstart your projects with reference examples
- Check back regularly as more certifications will be added!

https://support.cadence.com/jasperuniversity

Foundational

Intermediate

Advanced

Summary: Best-in-class Jasper Formal Verification Platform

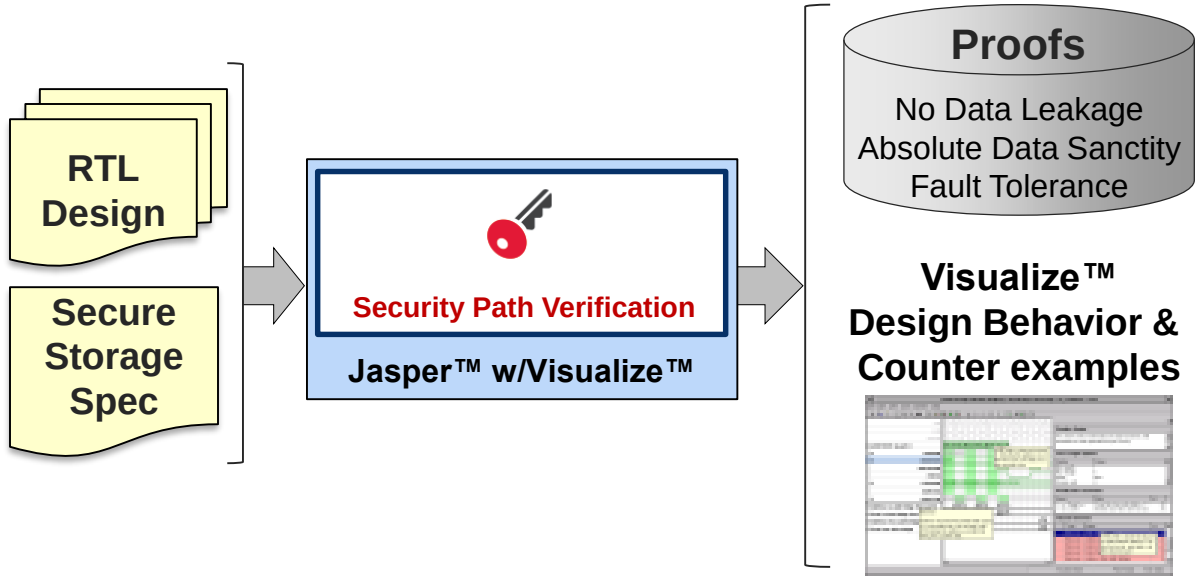
- Jasper™ is the industry's leading formal verification platform
  - Adopted in 19 of the top 20 semiconductor companies
- Fastest and most scalable formal verification solution
  - Proves properties and finds bugs faster, on wider range of bigger designs
  - Largest R&D team by far ensures we stay ahead
- Easiest formal verification solution to adopt
  - Comprehensive range of formal apps that automate property generation for specific tasks
  - Powerful root-cause analysis and design exploration with the Visualize™ environment

Formal Technology Leadership =

- higher verification throughput
- on bigger designs
- with optimal compute resource (in-house or cloud)

Security Path Verification App

Formally prove secure data cannot leak



1. Inputs: RTL and spec. of the secure storage element
2. Run Jasper™ Security Path Verification app
   - App automatically derives & generates all properties
   - Automatically runs special path analysis, optimized formal engine under-the-hood
3. Output: CEXs show data leakage, violations of data sanctity, or vulnerabilities to tampering/faults

Introducing Jasper University

- Self-paced, virtual or instructor-led classes to get certified on Jasper apps and methodology
- 3rd party, independent management of certifications

Credly

- Benefits
  - Quickly create Jasper Formal expertise in your teams
  - Jumpstart your projects with reference examples
- Check back regularly as more certifications will be added!

https://support.cadence.com/jasperuniversity

Foundational

Intermediate

Advanced