SYNOPSYS®

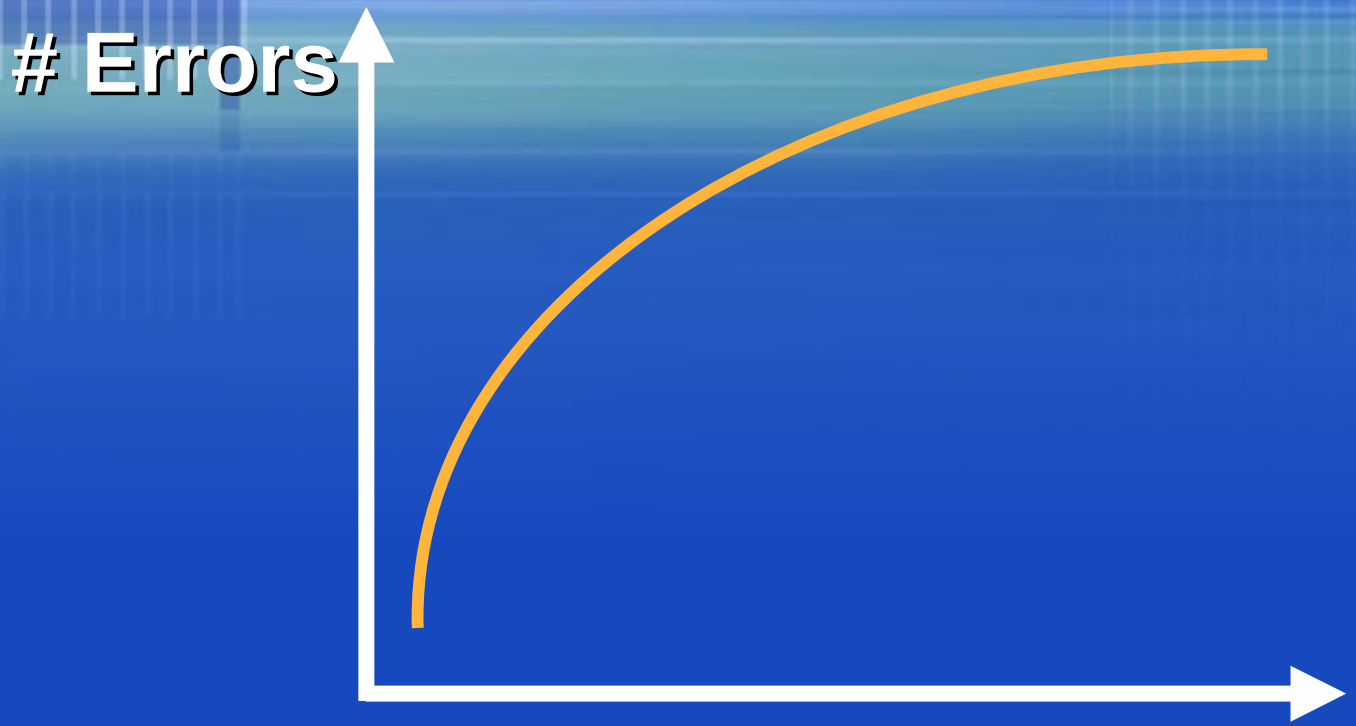
The Expanding Use of Formal Techniques in Electronic Design

Raul Camposano

Chief Technology Officer

Synopsys, Inc.

Why Bother with Formal Techniques?



Traditional simulation provides diminishing returns

SYNOPSYS

Without Formal Verification, A Good Idea...

SYNOPSYS

...Can Disappoint

February 24, 1999

Trouble for Hubble

SYNOPSYS

Another Great Design...

SYNOPSYS

But the Bugs Weren't Found

January 6, 2000

Lockheed Martin Announces Mars Polar Lander Loss Remains a Mystery

SYNOPSYS

The Verification Challenge

Every 18 months:

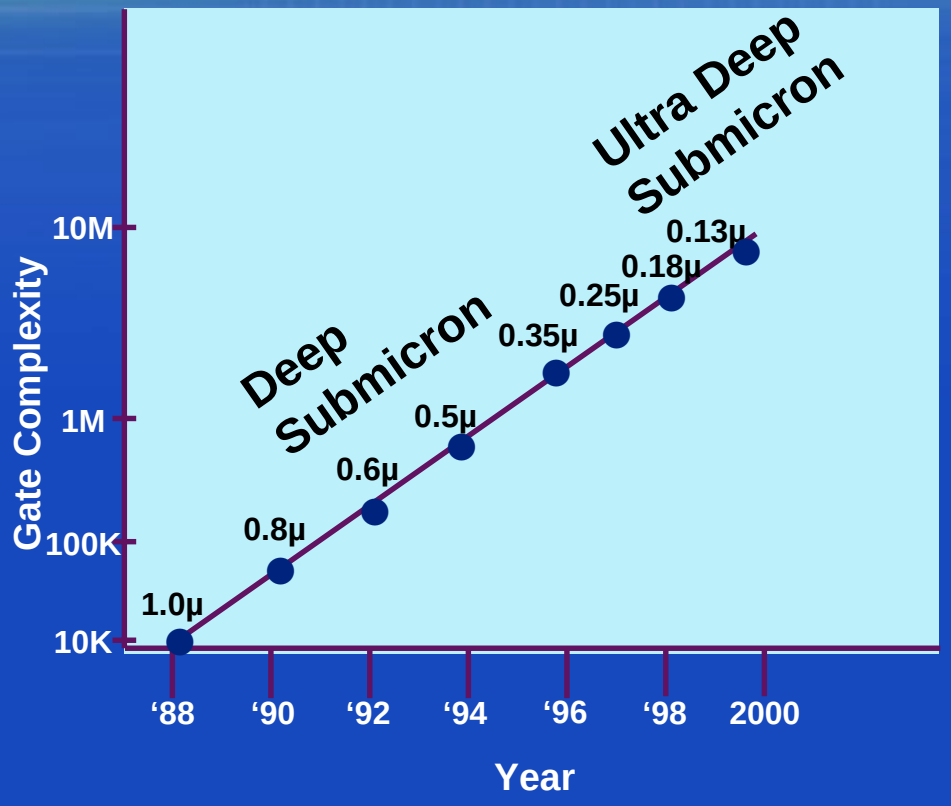
- Gate count doubles
- Vector set grows 10x
- Frequency increases 50%

Benchmark Design

Today:

- 0.18µ
- >500 MHz
- 10 million gates

Moore's Law



SYNOPSYS

Time to Simulate

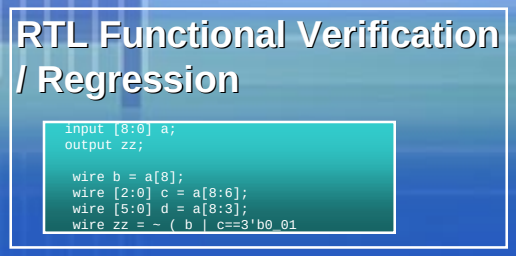
For 200M cycles, today's verification choices:

• 500M cps:	0.4 sec	Actual system HW
• 5M cps:	40 sec	Logic emulator[1] (QT Mercury)
• 500K cps:	7 min	Cycle-based gate accelerator[1] (QT CoBALT)
• 50K cps:	1 h	Hybrid emulator/simulator (Axis)
• 5K cps:	11 h	Event-driven gate accelerator (Ikos NSIM)
• 50 cps:	46 days	CPU and logic in HDL simulator (VCS)
• 5 cps:	1.3 years	Gate-level simulation (VCS)

- How much simulation is enough?

SYNOPSYS

New Static Verification Methodology

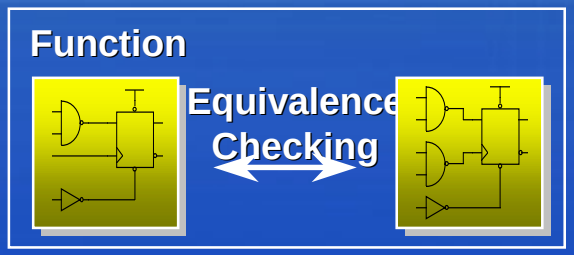


RTL Simulation Regression

- Ensures correct functionality before synthesis

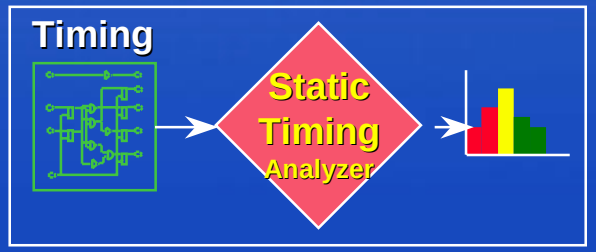
Property Checking

- Guarantees specified properties



Equivalence Checking

- Usually very fast
- Exhaustive
- Focus on the design, not the vectors



STA

- Very fast, large capacity
- Exhaustive
- Signoff quality

SYNOPSYS

Contents

- Static Timing Analysis

- Equivalence checking
- Property checking

SYNOPSYS

What is STA?

- Determines if a circuit meets timing constraints by calculating and timing the critical paths
  - Exhaustive
  - Not dependent on vector stimulus

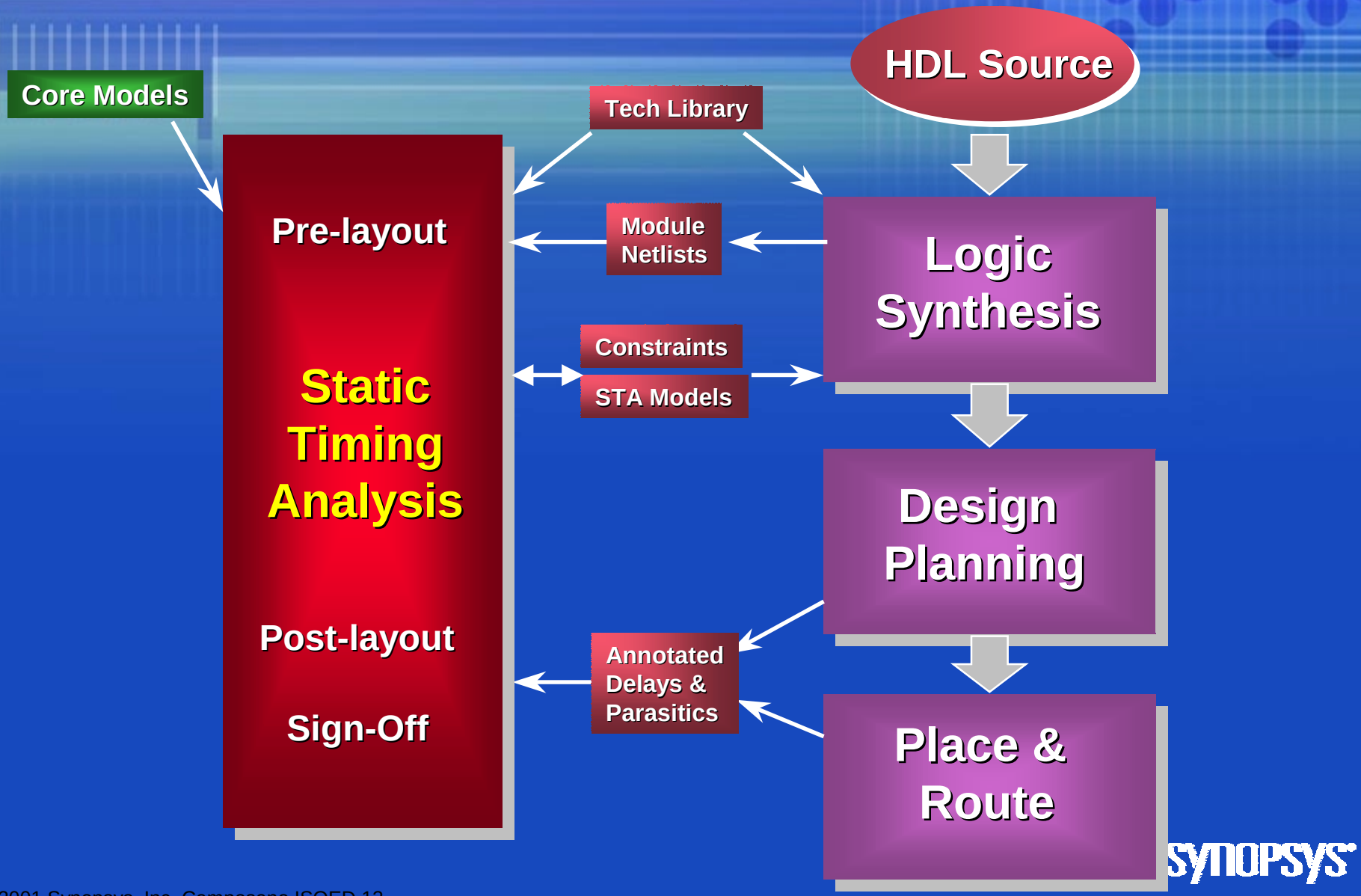
SYNOPSYS

What is STA?

- Up to ***100x*** faster than dynamic simulation
- Comprehensive timing checks
  - Set-up / hold / recovery
  - Minimum period / clock pulse width / skew
  - Clock gating / glitch detection
  - Bus contention / float
  - Unconstrained logic paths
  - More...

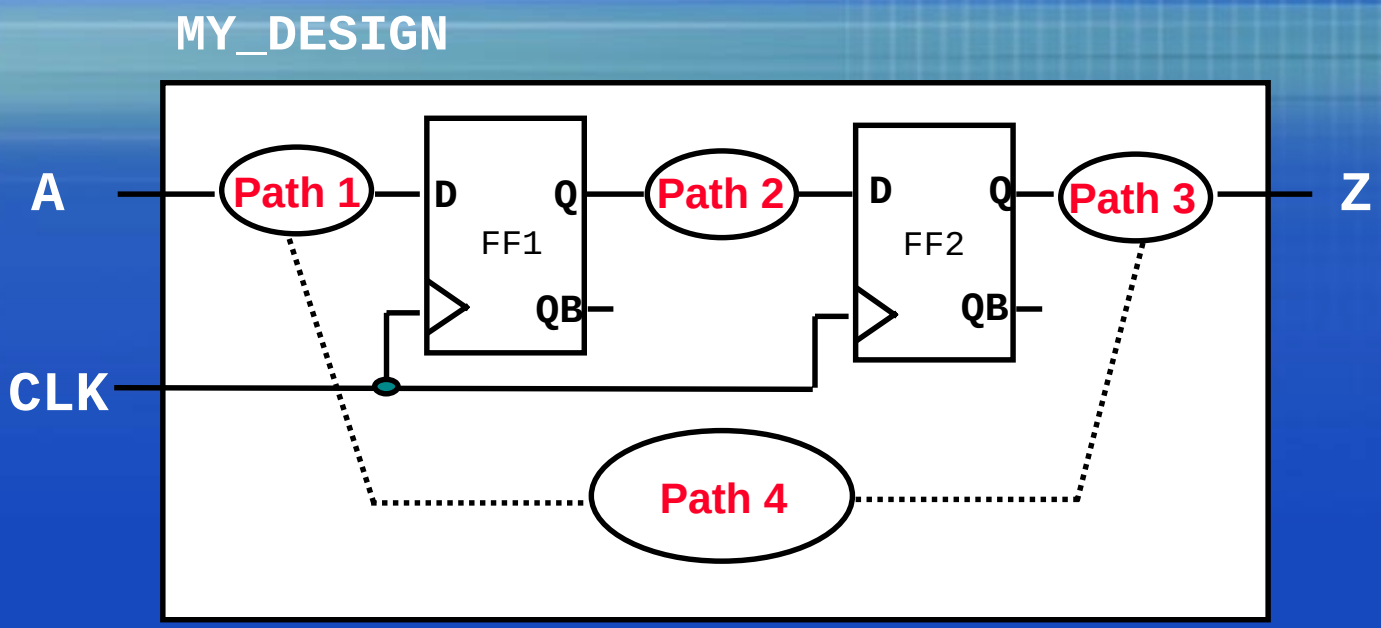
SYNOPSYS

STA in the ASIC Design Flow



SYNOPSYS

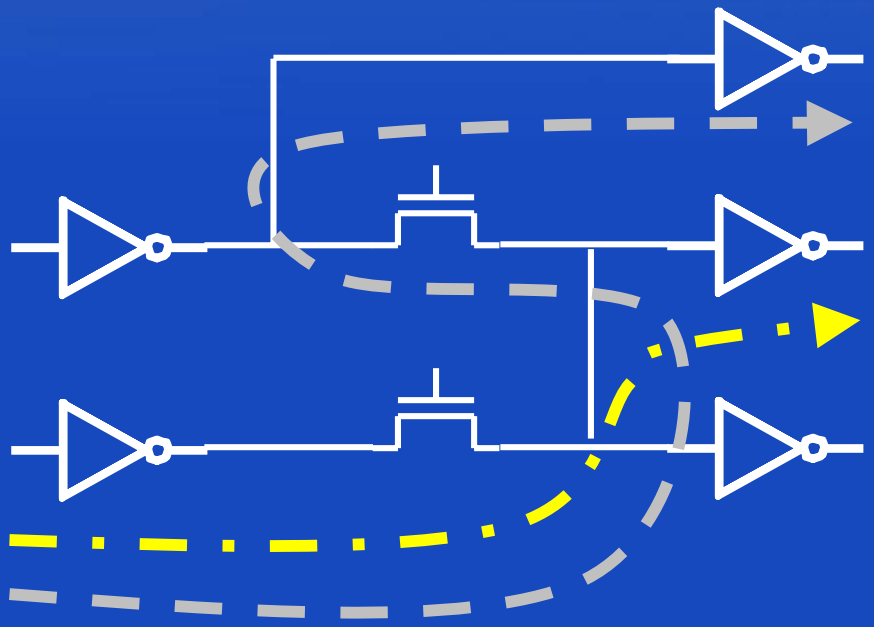
How STA Works



- STA breaks designs into sets of signal paths
- Each path has a start point and an end point

Signal Flow Direction

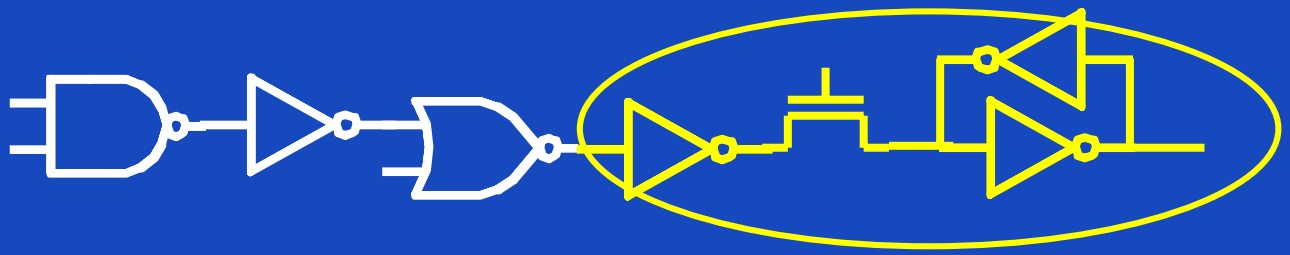
- Eliminates false paths
- Used for logic functions



SYNOPSYS

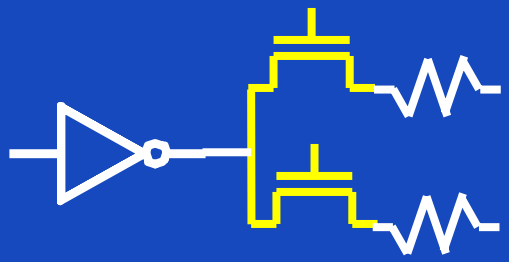
Transistor-Level Delay Calculation

- Group channel-connected transistors
- Consider additional elements that may affect the delay
  - Pass transistors
  - Detailed RC at output nodes



Latch: all transistors considered

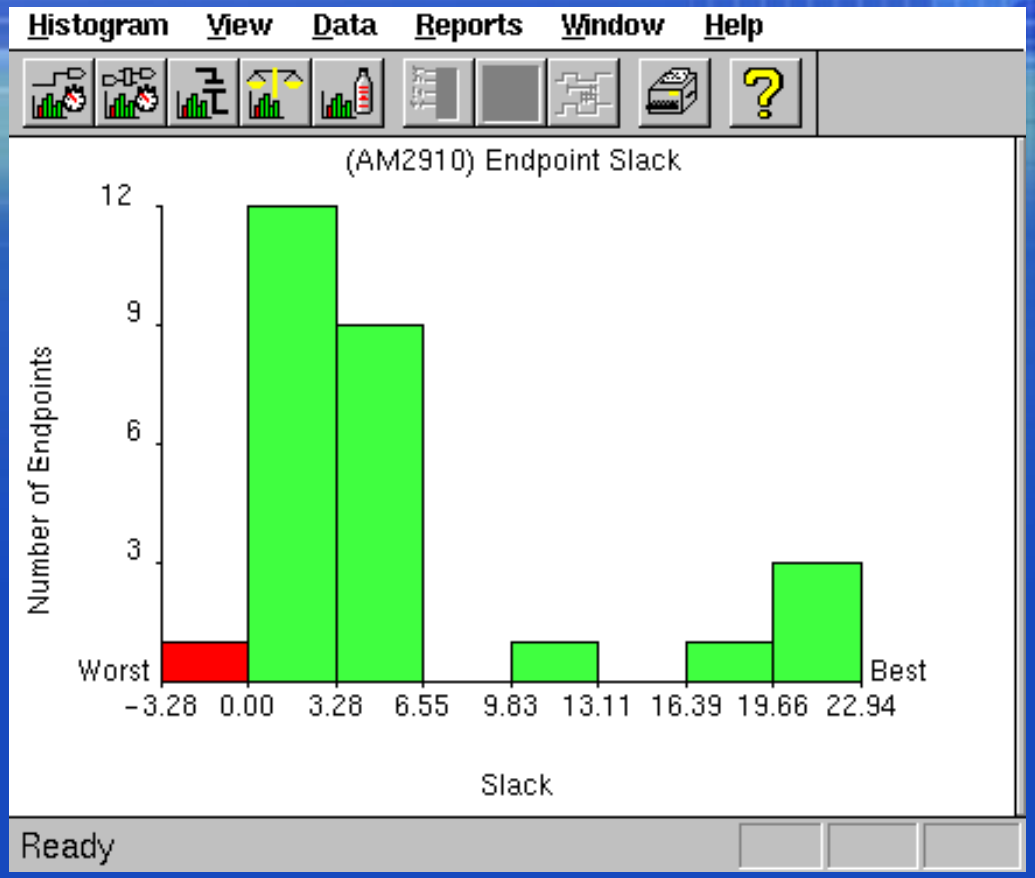
RC Network



Pass Transistors

SYNOPSYS

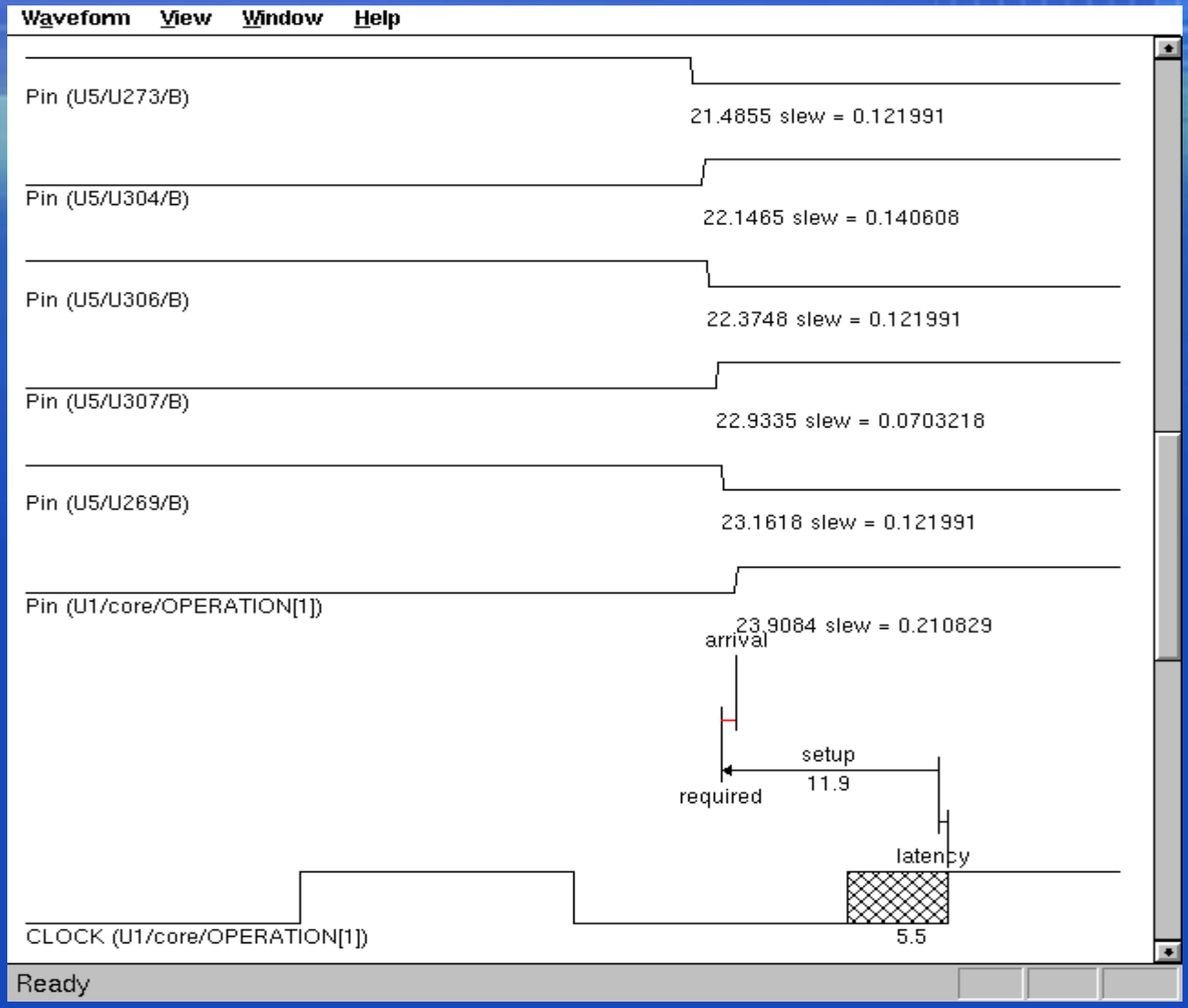
Slack Histogram Example



Timing slack histogram shows slack vs. number of endpoints

SYNOPSYS

Timing Waveform Example



SYNOPSYS

Technical Challenges

- Cannot analyze:
  - Asynchronous logic
  - Analog logic
  - Combinational feedback loops
- Must specify detailed timing information of
  - Internally derived clocks
  - False paths (some)
  - Multi-cycle / zero-cycle paths
  - Functional / test mode info
- Process, voltage, temp variation

SYNOPSYS

Future Challenges for STA

- Cross-talk analysis / signal integrity
  - Smaller geometries, closer nets
  - Can cause signal speed-up or slowdown
- Inductance in delay calculation
- Capacity / performance improvements
  - Growing design sizes: >10M gates

SYNOPSYS

Contents

- Static Timing Analysis
- Equivalence checking
- Property checking

SYNOPSYS

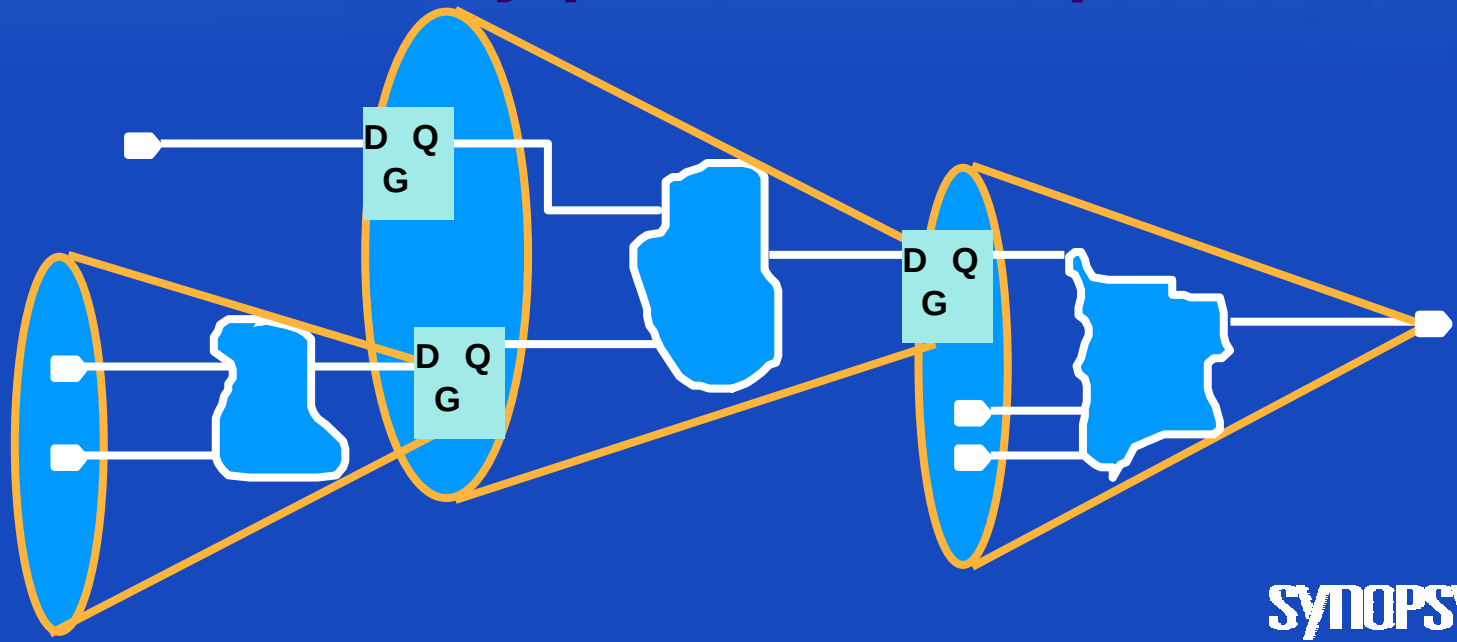
Equivalence Checking

- Equivalence checking verifies whether two designs are functionally equivalent
- Can verify:
  - RTL to RTL
  - RTL to Gates
  - Gates to Gates
- Does not *validate* RTL or Gates

SYNOPSYS

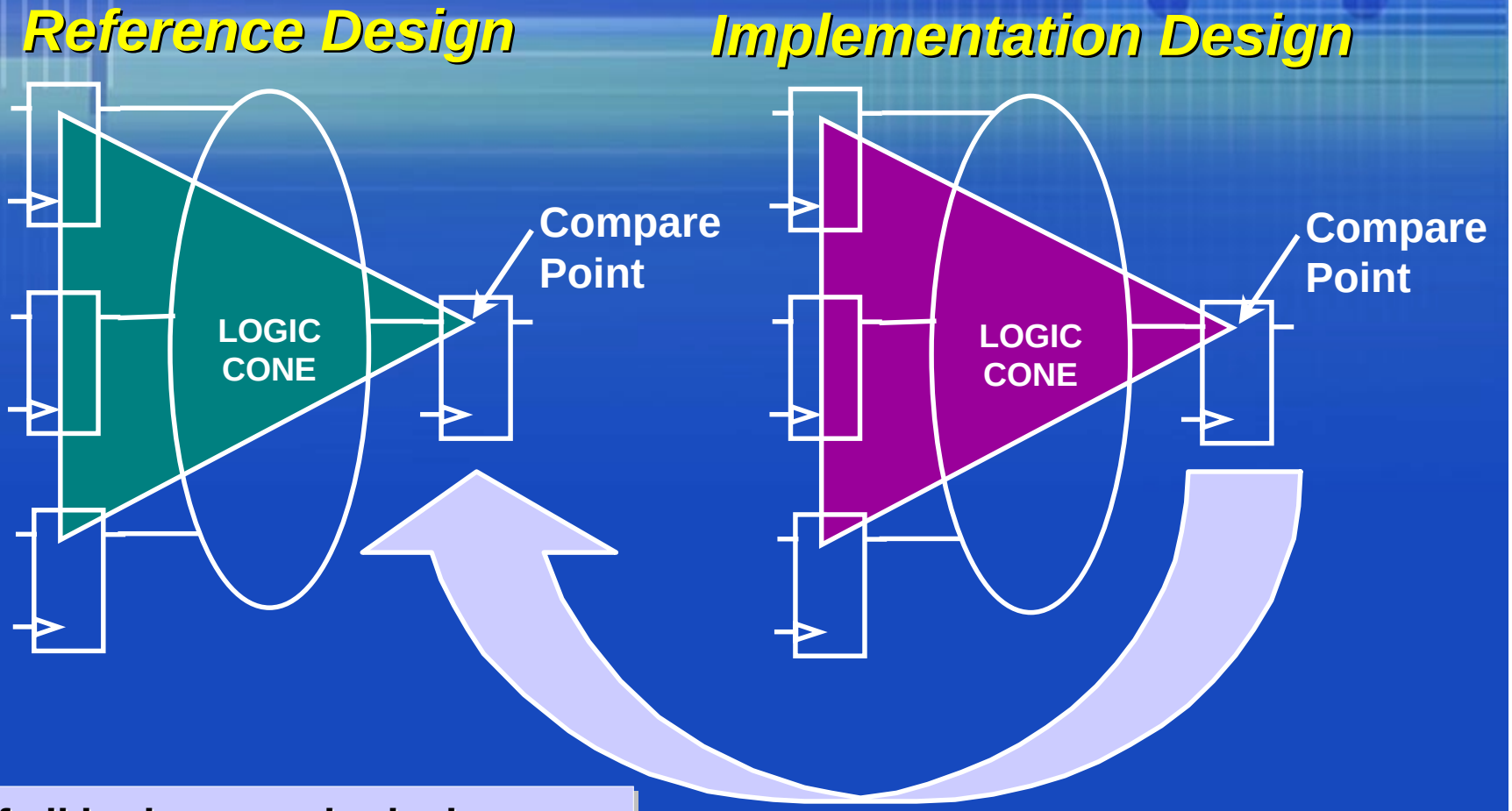
How Does It Work?

- Two logic circuits broken into logic cones
- Corresponding end points (compare points) are matched between the designs
- Equivalence of combinational logic cones is mathematically proved or disproved



SYNOPSYS

How Does It Work?



If all logic cones in design match, designs are equivalent.

Compare Function & State Behavior

SYNOPSYS

Performance & Capacity

Significantly Faster Verification than Gate-level Simulation:

Design Description	Formal Verif. Run Time*	Simulation Run Time
100k flat gates to hierarchical gates	4.5 minutes	hours
440k hierarchical gates to hierarchical gates	12 minutes	days
1.2M flat gates to hierarchical gates	37 minutes	days
1.2M RTL to hierarchical gates	4 hours	days

* Synopsys Formality. Run times vary based on design style.

SYNOPSYS®

Equivalence Checking Challenges

- Modules that are too complex
  - (e.g., large multipliers)
- Timing dependent functionality
  - (e.g., pulse generators)
- Cannot verify added logic is actually correct
  - (e.g., scan chains)
- Initialization
  - (i.e., reset sequence)

SYNOPSYS

Future of Equivalence Checking

- Methodology
  - Clock-gated designs
  - Pipeline retiming
  - Clock trees
  - Black boxes
  - Asynchronous bypass

SYNOPSYS

Contents

- Static Timing Analysis
- Equivalence Checking
- Property Checking

SYNOPSYS

Property / Model Checking

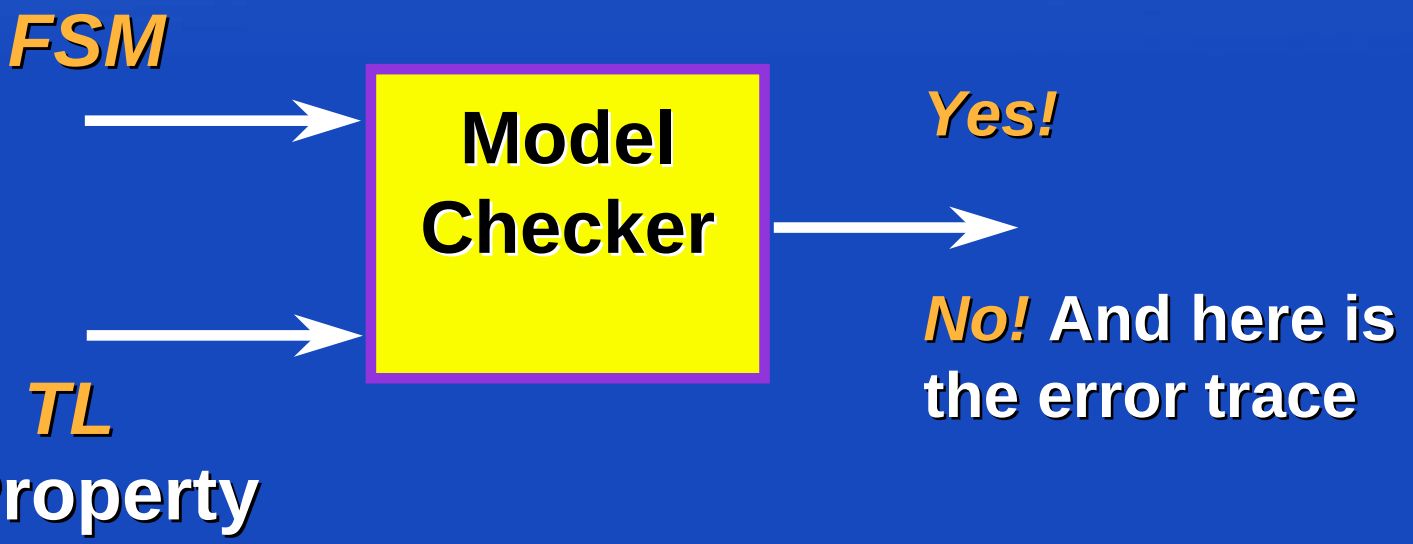
- Verifies that a design does/doesn't conform to a specified property under all possible sets of legal input conditions
- Ideal for verifying a high-level spec with an RTL implementation
- Example: Verify that a bus access will never be granted to two clients at the same time (safety)

SYNOPSYS

Formal Property Verification Example

- Symbolic model checking
  - Most popular formal property verification method

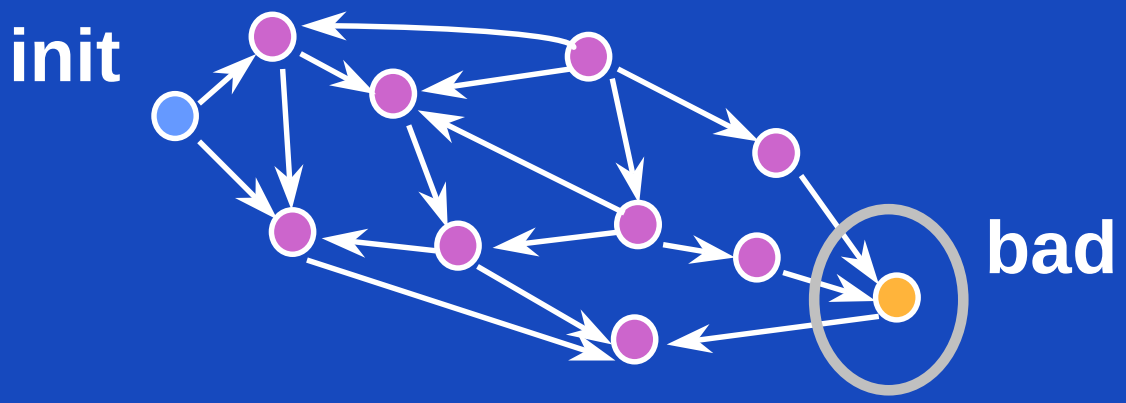
Model of the design



SYNOPSYS

How Model Checking Works

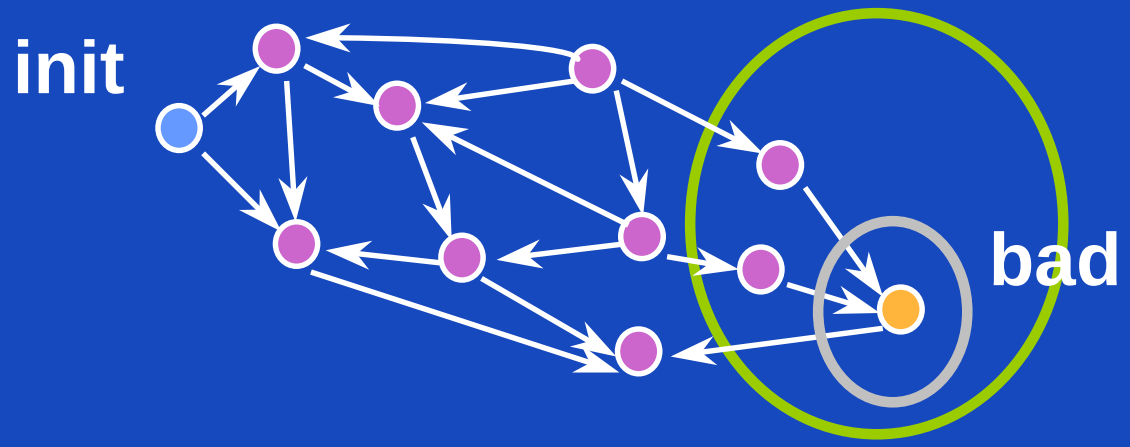
- Model checking algorithm
  - Fix point computation
  - Can the design ever go bad?



SYNOPSYS

How Model Checking Works

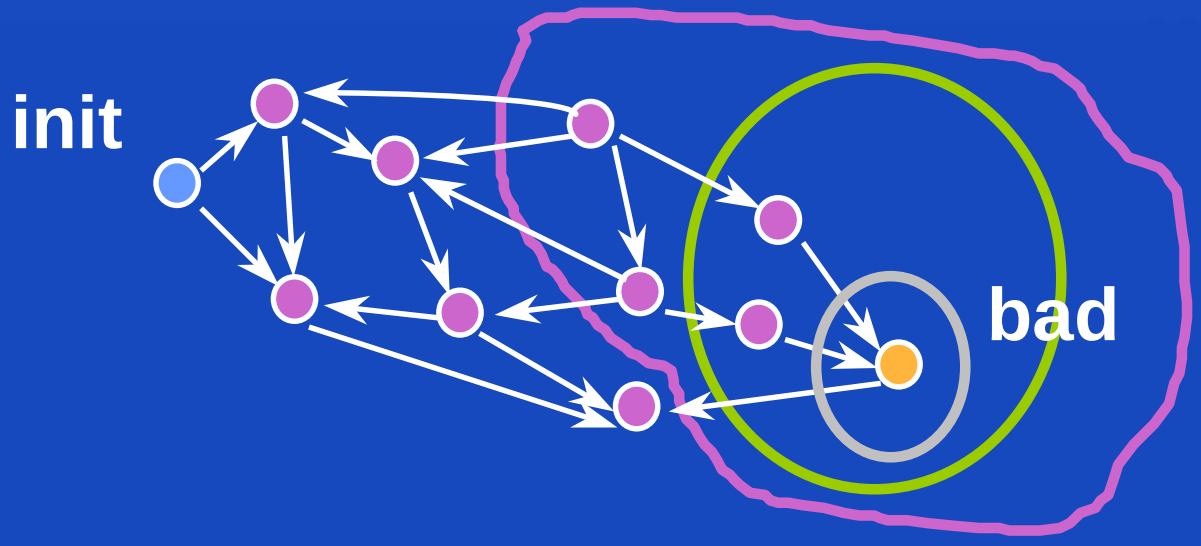
- Model checking algorithm
  - Fix point computation
  - Can the design ever go bad?



SYNOPSYS

How Model Checking Works

- Model checking algorithm
  - Fix point is reached
  - The design can never go bad!



SYNOPSYS

Model Checking

- Pro
  - Exhaustive
- Con
  - Expensive
    - Symbolic computation and representation of all states that can potentially go bad
    - Naïve BDD-based symbolic model checkers can handle around 150 latches
    - 2^{150} states! (10^{78} particles in the universe)
    - Not big enough for industrial designs

SYNOPSYS

Capacity Problem

- Model-checking capacity depends on the techniques used
  - Multiple Analysis Engines
    - SAT
    - BDD
    - ATPG
  - Abstraction
  - Combining Formal techniques with Simulation

SYNOPSYS

Property Verification Results

	Proven	Violated	Unknown	total
User Defined	2	2	2	6
$finish	7	0	0	7
// Illegal state	6	8	4	18
full & parallel_case	81	8	2	91
total	96	18	8	122

Replay these traces to find bugs !!!

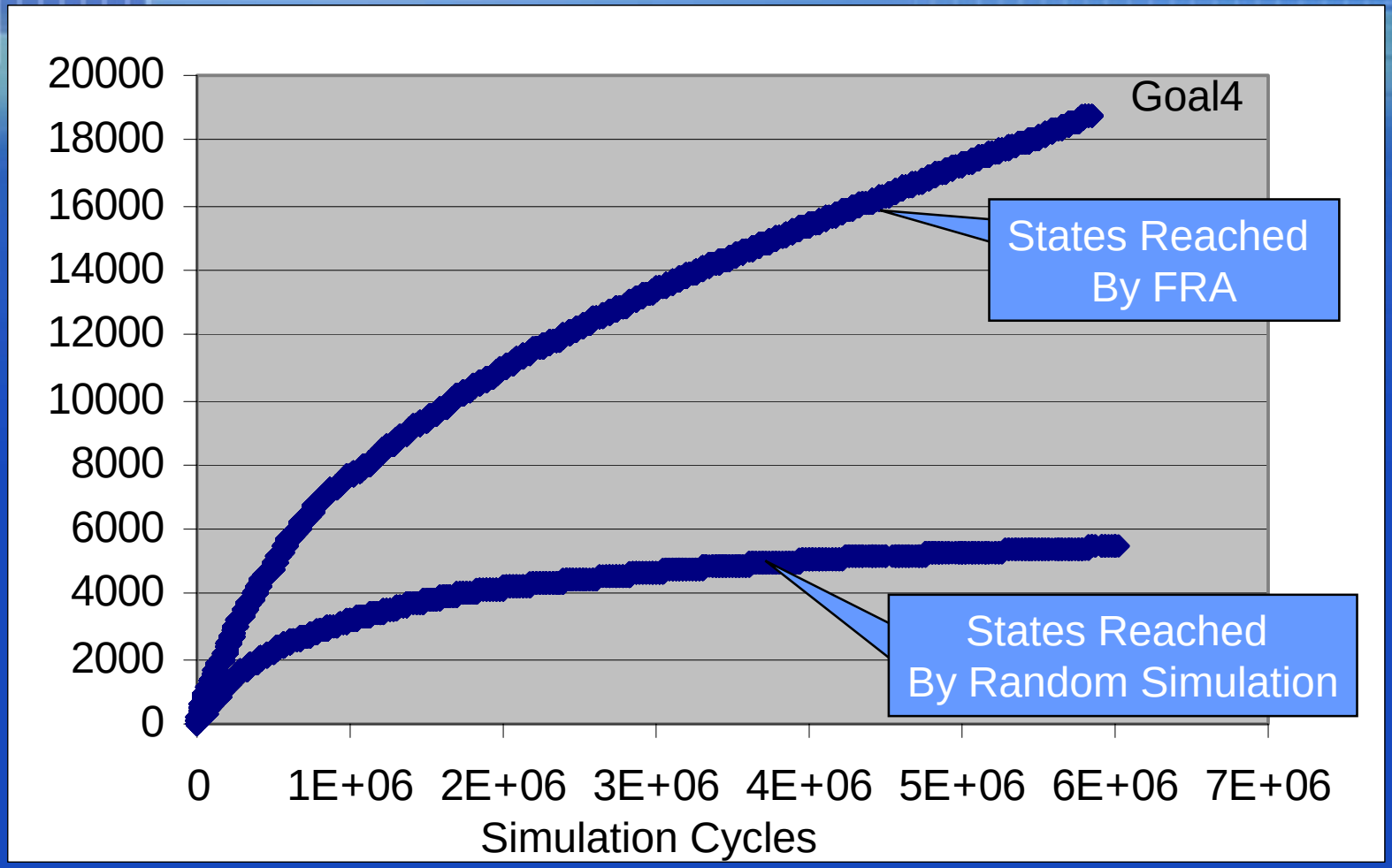
SYNOPSYS

Stimulus Generation: Composite Results

Goalset Name	Nets	Regression Coverage	States Reached	States Unreachable	States Unknown	Search Runtime
goal1	4	13	13	3	0	20m
goal2	4	10	10	6	0	3.5H
goal3	13	269	132	7152	908	59H
goal4	16	246	18780	0	46756	70H
goal5	17	579	6294	94208	30570	10 H
goal6	14	531	213	13056	3115	40H
goal7	17	6555	6193	0	59343	25H
goal8	24	2727	18588	13725632	3032996	24H
goal9	12	247	259	3632	205	22H

SYNOPSYS

Formal Reachability Analysis Assists Random Simulation



SYNOPSYS

Summary

- Formal techniques can eliminate many bugs that traditional simulation doesn't find
- Static timing analysis and equivalence checking are mature formal technologies
- Property checking is an emerging formal verification technology
- Adoption is accelerating

SYNOPSYS

ORDER TODAY
The Sunday Sentinel will contain many interesting special features. Don't fail to order a copy today.

THE MILWAUKEE SENTINEL

HOME EDITION
THE CIRCULATION OF THE SENTINEL ON SUNDAY WAS 53,884

ESTABLISHED 1837—NO. 27,903 TUESDAY EVENING, APRIL 16, 1912—FOURTEEN PAGES PRICE ONE CENT

1,492 OF 2,358 PASSENGERS ON TITANIC LOST; WORLD NOTABLES GO DOWN TO OCEAN GRAVE

BADING IS MAYOR; NONPARTISANS IN; NEW CITY COUNCIL

TO CONTROL CITY FOR CITIZENS IN NEXT TWO YEARS

Bading Is Inaugurated Mayor and Outlines Work in His First Message to Council.

CITY HALL IS FILLED

Spectators Crowd the Chamber Galleries and the New Officials Are Given Continued Ovations.

NEW ALDERMEN APPEAR

Last Words by Socialists Followed by Initial Work by Body Which Takes Up Problems.

Mayor Bading was ushered into office promptly at 12 o'clock Tuesday noon when he became chief executive of the city of Milwaukee.

At the same hour Ald. Joseph P. Carney became city treasurer, while L. M. Koteckl assumed the duties of controller. Mayor Seidel was not present to welcome the new executive. Controller Diets and City Treasurer Whitnall remained on duty and relinquished their offices in a formal manner and wished their successors the "best of luck." The absence of Mr. Seidel was commented upon.

With his secretary, Claude R. Ellis, Mayor Bading walked into the office promptly at 12 o'clock, followed by a host of friends.

"I am glad to see you all," he said, while shaking hands with those who waited for him and applauded as he entered.

Mayor Misses Seidel.

The mayor went direct to his private office and took off his overcoat.

"Where is Emil?" he asked, smiling at

FRANTIC RELATIVES STORM OFFICES OF COMPANY FOR NEWS

New York Stunned by Terrible Disaster to Giant Liner Titanic in Midocean.

MANY BECOME HYSTERICAL

First Authentic News Comes During Evening and Headquarters of Line Are Flooded With Inquiries.

CLAIM REPORTS WITHHELD

Officials Charged With Refusing to Give Out Early Information Regarding Sinking of Ship.

NEW YORK, April 16.—Utterly stunned by the weight of the terrible disaster that followed the loss of the giant liner Titanic on her maiden voyage, New York halted on Tuesday. It was hard to realize that the latest creation of marine architecture, the great steamship which only Monday, when news that it had been in collision was received, was proudly branded by her owners as "unsinkable," now lay below the waters of the Atlantic off the banks of New Foundland and had carried with her much of the flower of American and British manhood.

Not since the French liner Bourgogne was rammed and sent to the bottom with all of her company by the great iron freighter Cromartyshire, on July 2, 1898, have such scenes been witnessed as were enacted at the office of the White Star line on lower Broadway throughout the night and day.

RELATIVES THRONG OFFICE.

A crowd of men, many of them on the verge of tears, and a very few women

TITANIC LOSS RECALLS BIG COLLISION

LAST HOPE FOR MORE SURVIVORS OF TITANIC GONE

Captain of Virginian Reports That He Was Unable to Find Trace of Lifeboats in Icefloes,

CARPATHIA, CARRYING 866 SAVED ON WAY TO NEW YORK

Women and Children Make Up Majority of List of Persons Who Were Not Lost When Liner Sank in Midocean.

BULLETIN.

NEW YORK, April 16.—The New York News Bureau says that a wireless dispatch received from Cape Race Tuesday afternoon, after being relayed from the scene of the wreck of the Titanic, says that "all except 1,237 of the persons on board the Titanic have been accounted for."

This, if true, would indicate that 155 additional have been rescued. The report is not confirmed.

NEW YORK, April 16.—Hope for the safety of passengers of the illfated Titanic, which foundered early Monday morning, off the Grand banks of New Foundland, other than those reported by wireless from the Cuparder Carpathia as en route to this city, was practically abandoned Tuesday afternoon. Latest reports placed only 866 persons, and they were chiefly women and children, on the Carpathia, while even the officials of the White Star line admitted there was practically no hope for the remaining 1,492 of the ship's company of 2,358 souls.

That all would have had a chance of safety had there been lifeboats and rafts enough, was the general belief of navi-

SENT TO ROME BY TAFT; MAY BE LOST ON TITANIC

Maj. Archibald Butt.

As personal and confidential aide he came to President Taft. Maj. Archibald Butt, while determined on leave of absence for recuperation, took with him to

SIMILAR ACCIDENT BEFELL BIG LINER

NEW CITY OFFICIALS

Mayor—Dr. G. A. Bading.
Treasurer—Joseph P. Carney.
Controller—Louis M. Koteckl.

MILWAUKEEAN MAY BE ON DEATH LIST

Prevent Disastrous Design Problems

SYNOPSYS

If They Had Only Used Formal Techniques...

SYNOPSYS


SYNOPSYS®
Your Design Partner
Design
Tools
Services