2019 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Formal Bug Hunting with “River Fishing” Techniques

Mark Eslinger, Mentor

Ping Yeung, Mentor

accellera SYSTEMS INITIATIVE

Mentor® A Siemens Business

2019 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Agenda

- What is River Fishing
- Traditional approach
- River fishing approach
- Results
- Design bugs
- Summary

accellera SYSTEMS INITIATIVE

TAKEMEFISHING.org

Learn To Fish & Boat | Where To Fish & Boat | State Info | Get Licensed

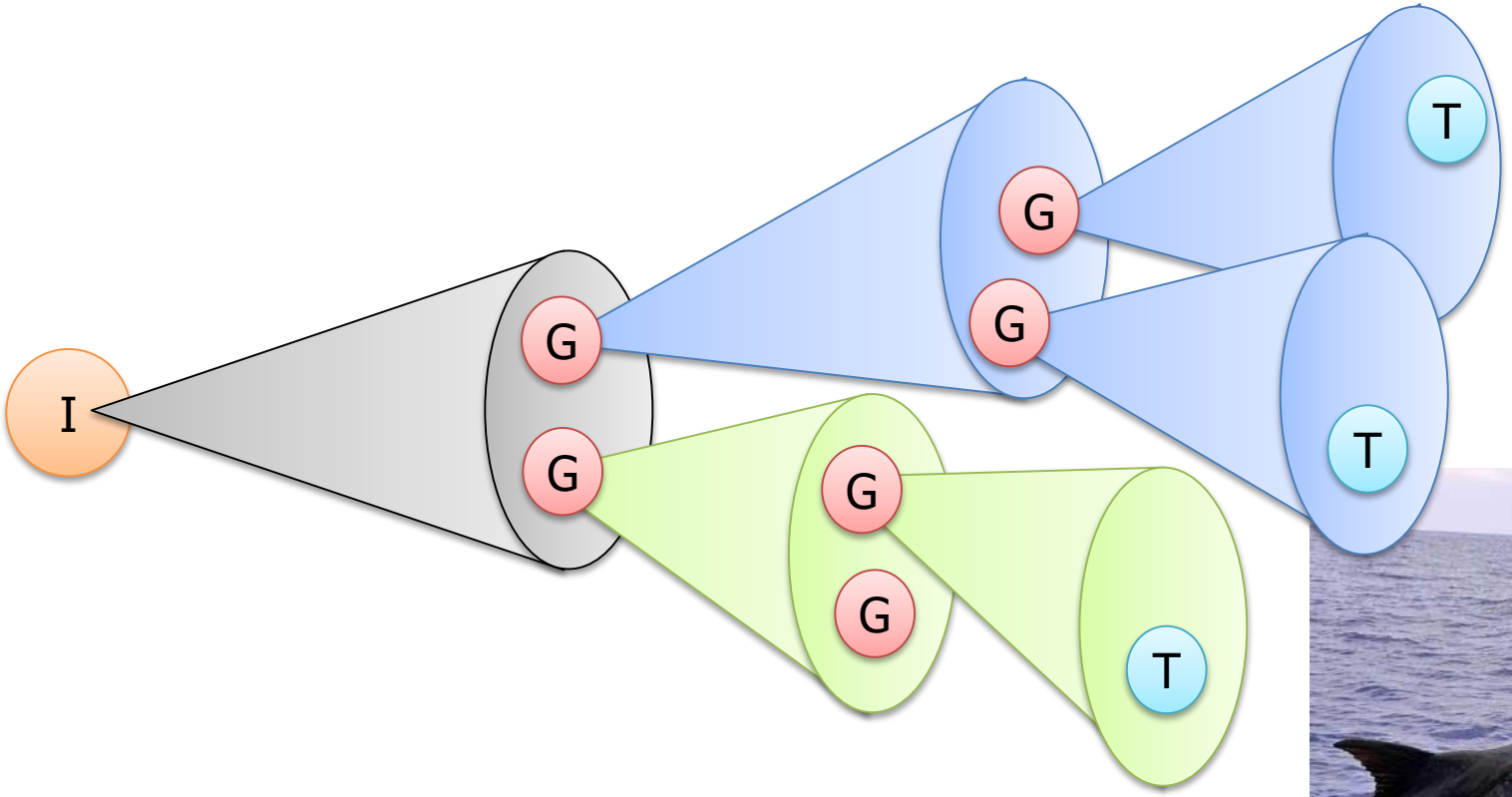
Home > Learn to Fish & Boat > Freshwater Fishing > Best Freshwater Fishing > River Fishing

River Fishing

Many anglers consider river fishing to be one of the most relaxing freshwater fishing experiences because it doesn't require much gear, and can easily be done from a canoe, kayak, or while wading. Find river fishing tips and more information.

www.takemefishing.org/freshwater-fishing/types-of-freshwater-fishing/river-fishing

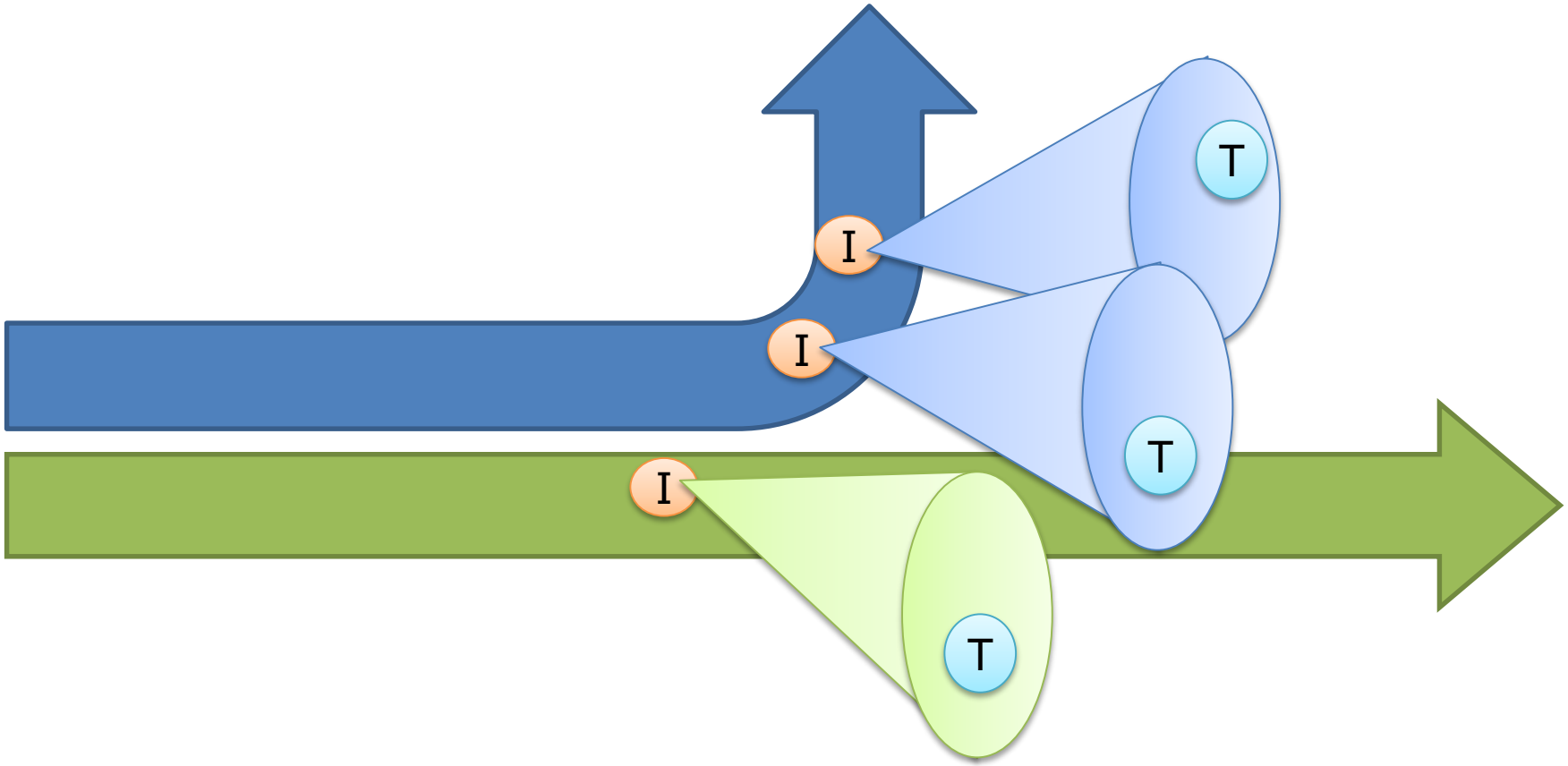
Waypoints, Goal-posting, Cover-points



- [1] Richard Ho, et al., “Post-Silicon Debug Using Formal Verification Waypoints,” DVCon 2009
- [2] Blaine Hsieh, et al., “Every Cloud - Post-Silicon Bug Spurs Formal Verification Adoption,” DVCon 2015

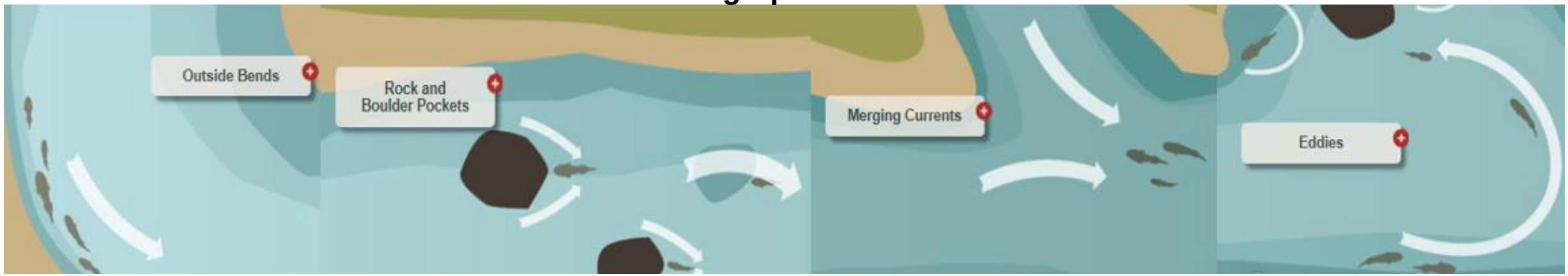
River Fishing

- Launching formal verification from interesting fishing spots
- “Selection of initial states for formal verification,” US7454324.



Formal Bug Hunting with “River Fishing”

Fishing Spots



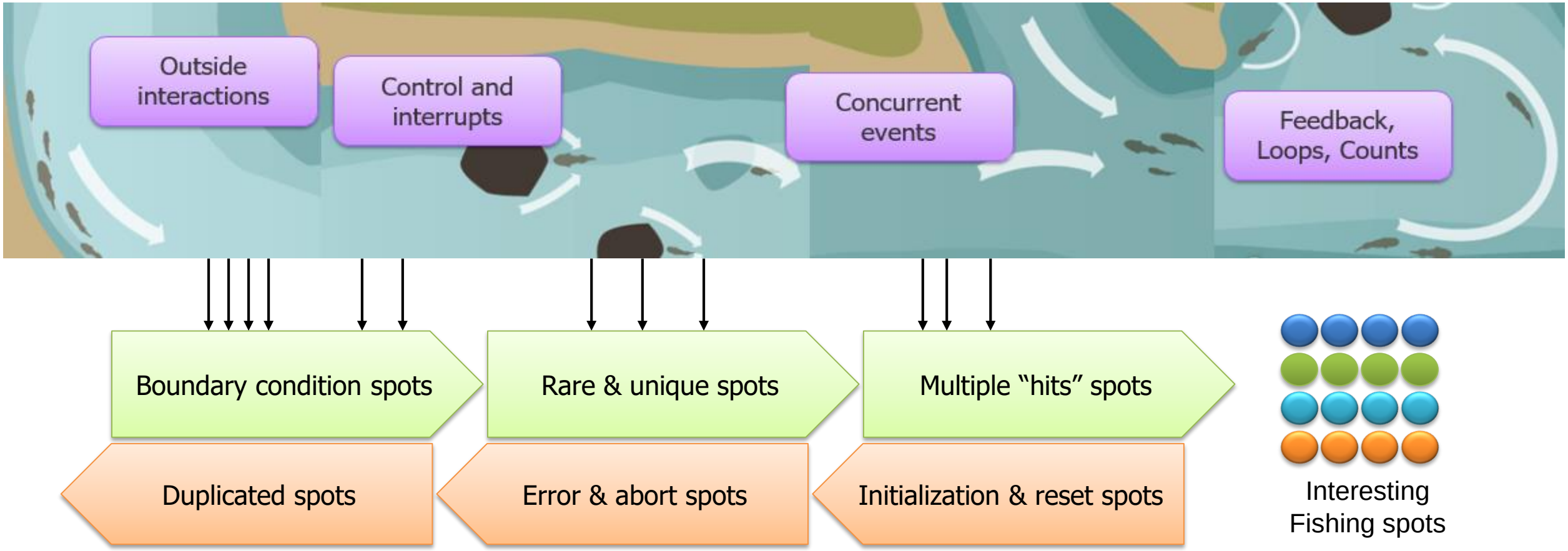
Bug Hunting Spots

Identify “fishing spots”

Outside interactions	Inter-module communication and standard protocol interfaces
Control and interrupts	FSMs, bus controllers, memory controllers, flow charts, algorithmic controls
Concurrent events	Arbiters, interrupts, schedulers, switches, multiplexing logics etc
Feedback, loops, and counts	FIFOs, timers, counters, data transfers, bursting, and computations
Assert and cover properties	fan-in cones of the user properties are great coverpoints and sub-goals

- “Selection of initial states for formal verification,” US7454324

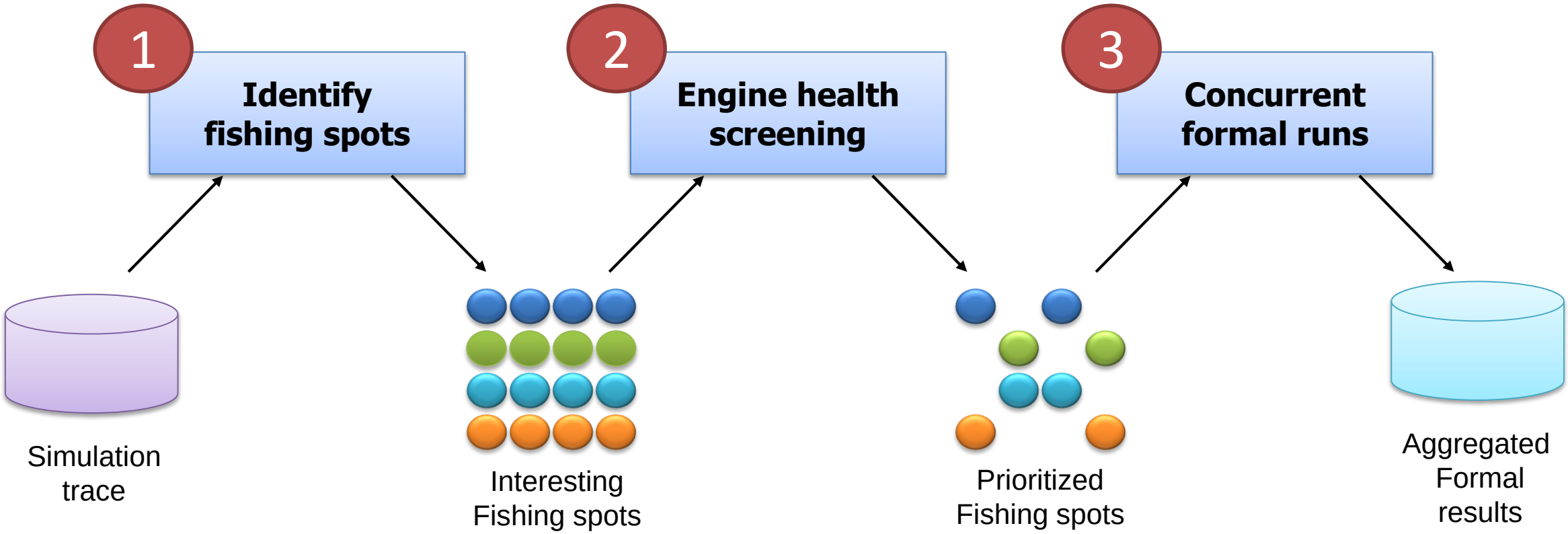
Identify “fishing spots”



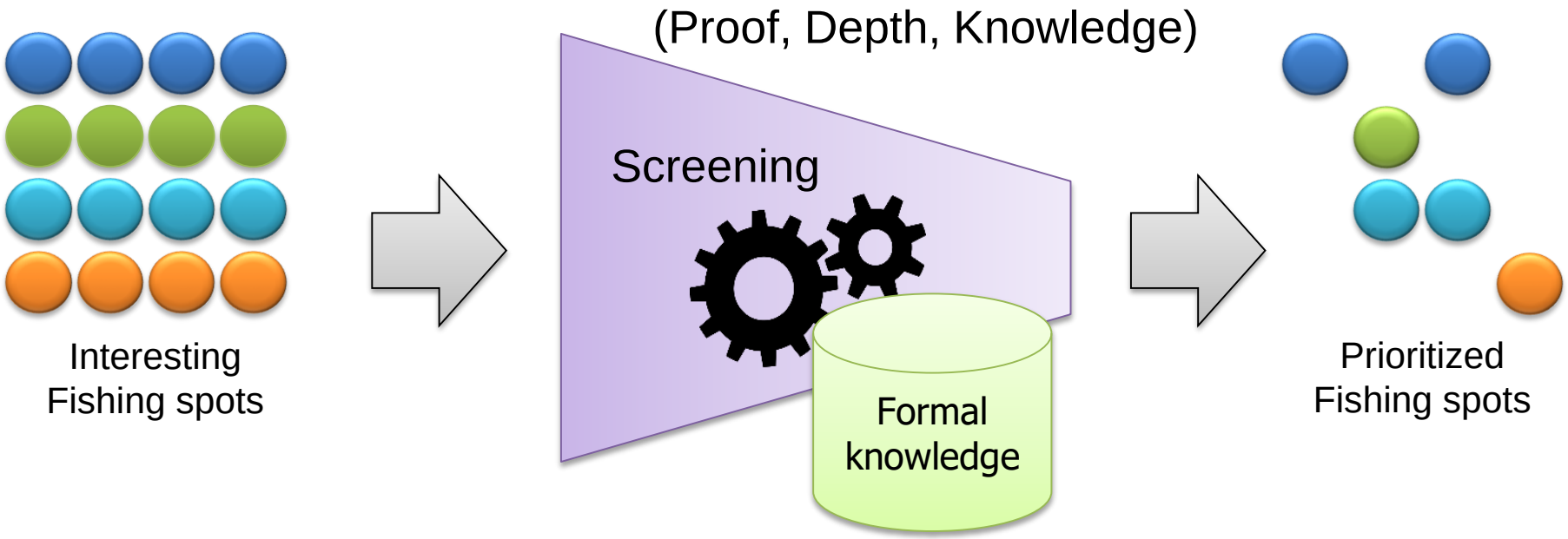
- “Selection of initial states for formal verification,” US7454324

The 3 Major Steps

- The “river fishing” formal bug hunting methodology consists of:

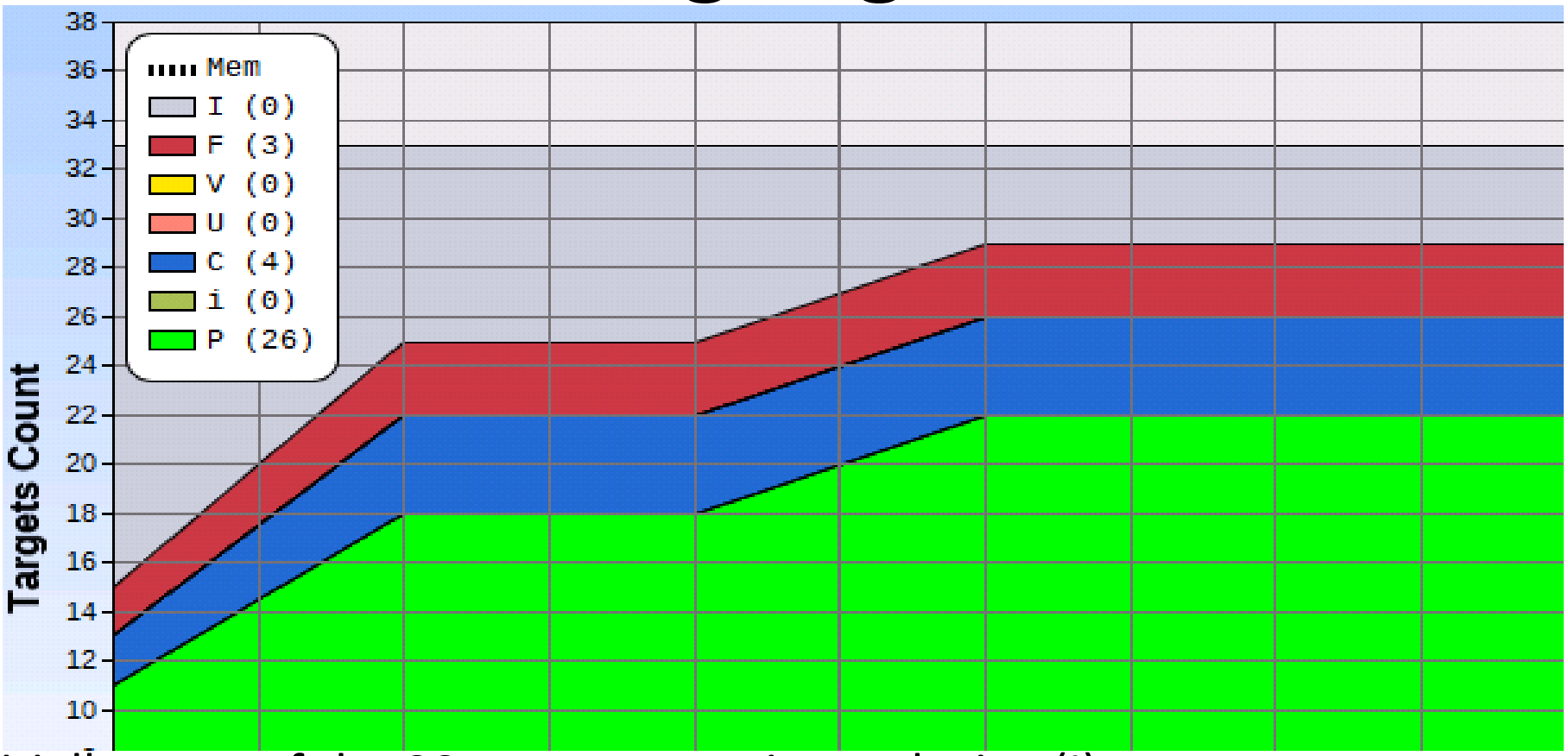


Screening with Engine Health



- Formal engine health:
  - Formal targets concluded (proven/fired/covered/uncoverable)
  - Sequential depth explored or cone of influence analyzed
  - Formal knowledge and engine setting acquired

Monitoring Engine Health



- Initially most of the 33 targets were inconclusive (I).
- With multi-cores running concurrently, formal verification gradually verified the targets into one of the following catalogs: firing (F), vacuous (V), uncoverable (U), covered (C), and proof (P).

Formal engine knowledge snapshot

#	# Proven / Unsatisfiable		# Fired / Satisfied		# Inconclusive Targets		
	Safety	Vacuity	Safety	Vacuity	Good	Fair	Poor
0*	14	0	0	0	N/A	N/A	N/A
7*	168	8	102	236	N/A	N/A	N/A
10*	29	0	0	0	51	18	9
12*	0	0	0	0	75	2	1
17*	0	0	0	0	78	0	0

- The “Proven/Unsatisfiable” columns show which engines solve the safety/vacuity checks.
- The “Fired/Satisfied” columns show which engines generate the counterexamples.
- The “Inconclusive Targets” columns (Good, Fair, Poor) show the individual engine health
- Engine 7 is very productive in finding a lot of proofs and firings.
- Engine 0 (the housekeeping engine) and Engine 10 have found some proofs.
- Engines 12 and 17 haven’t been contributing to the results

Results

Block-Level Results

Block	Targets	Fishing Spot S0	Fishing Spot ∑ SP
Block De	12	12 C, depth 23	12 C, depth 23
Block Pc	71	66 C + 5 I, depth 134	71 C + 0 I, depth 256
Block Cp	81	60 C + 21 I, depth 65	79 C + 2 I, depth 161

C: proven/fired/covered/uncoverable. I: inconclusive targets

Results

Block-Level Results

Block	Targets	Fishing Spot S0	Fishing Spot ∑ SP
Block De	12	12 PF, depth 23	12 PF, depth 23
Block Pc	71	66 PF/CU + 5 I, depth 134	71 PF/CU + 0 I, depth 256
Block Cp	81	60 PF/CU + 21 I, depth 65	79 PF/CU + 2 I, depth 161

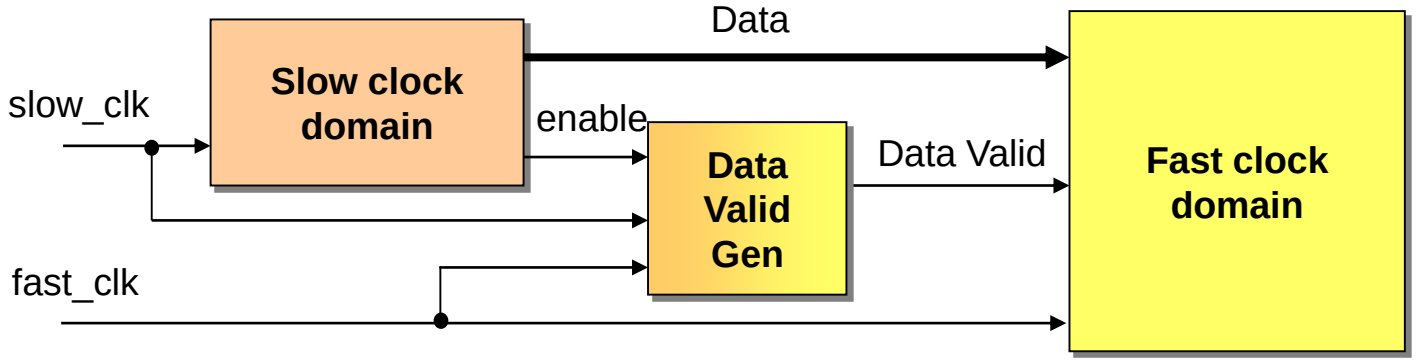
Sub-System Level Results

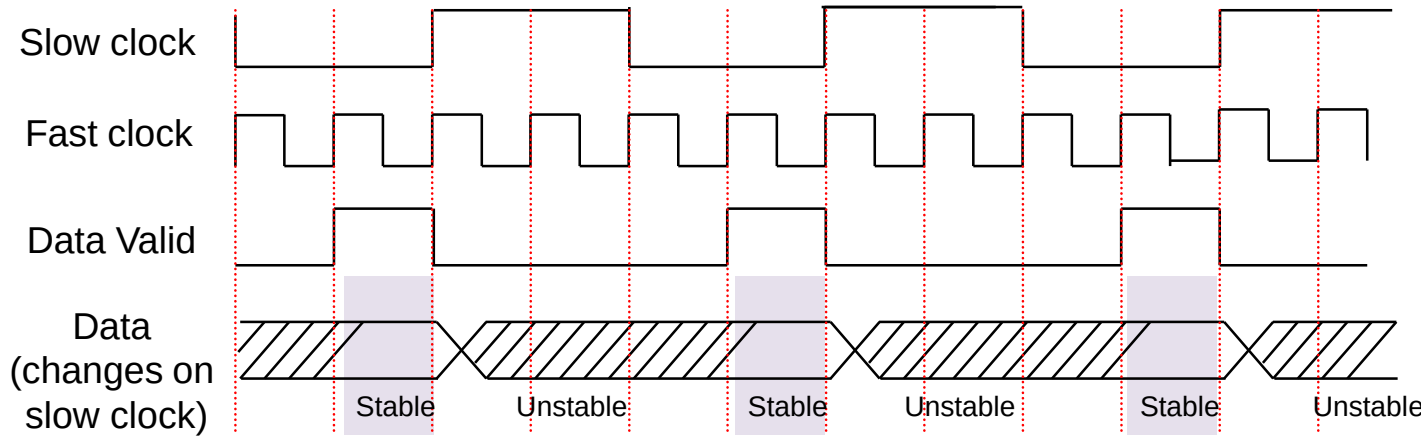
Design	Targets	First stage	Fishing spot S0	Fishing spot ∑ SP
Design Ct	2356	2319 PF/CU + 37 I 15 min	2338 PF/CU + 18 I 24 hours	2349 PF/CU + 7 I 24 hours
Design Pb	15205	15126 PF/CU + 79 I 15 min	15154 PF/CU + 51 I 24 hours	15161 PF/CU + 44 I 24 hours

PF/CU: proven/fired/covered/uncoverable. I: inconclusive targets

Case #1: Design Interface Bugs

- Ratio-synchronized Data Sampling
  - Sub-systems are running at slower frequencies
- Assertions
  - Ensure the data is sampled at the right time
- Bug
  - The fast clock domain samples the data at the end of a slow clock period
  - In some corner cases, Data Valid condition is not checked
  - As a result, the data is sampled at the incorrect time, and corrupted data is registered

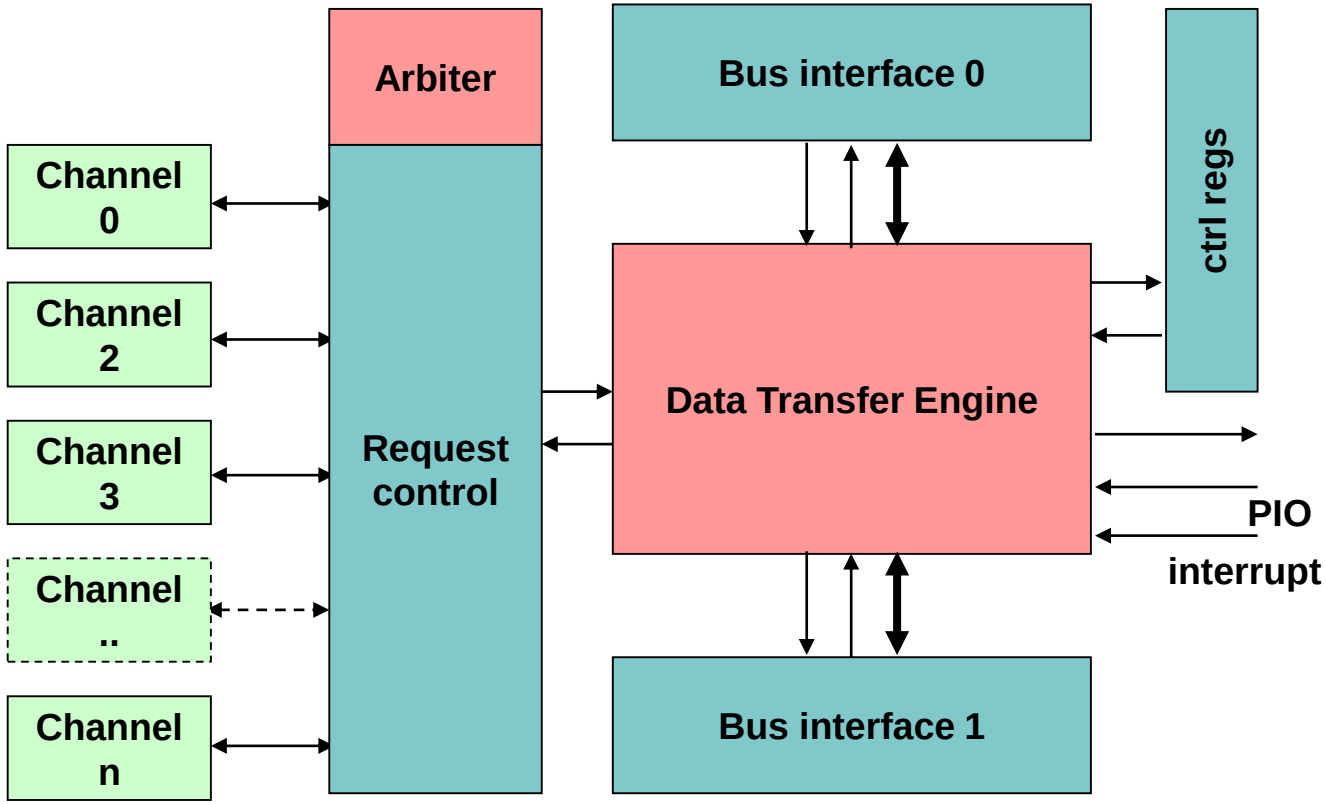




Data must be sampled at the correct time

Case #2: Data Transfer Controller

- DMA Controller
  - DMA Controller in WLAN/PDA design
- Assertions
  - Monitors for on-chip bus interfaces
  - Pointer manipulation, allocation and de-allocation
- Bug
  - Channels are set up to handle data with priority
  - When >1 channels finish the transfer at the same time
  - One address pointer is de-allocated twice, while the other is not de-allocated
  - Causes memory leak and data corruption



Summary

- Simulation and formal methodologies can be used together to accelerate the verification of complex designs.
  - Leverage what has been learned or achieved in one for the other
  - Some companies have already made organizational changes
- *River fishing* technique
  - leverages the functional simulation activities and starts formal verification from interesting fishing spots in the simulation traces.
  - Identify and extract a set of good fishing spots from the simulation traces
  - Screen and prioritize the fishing spots using formal engine health
  - Launch and monitor multiple formal runs on the computing servers

2019 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

Thank you

accellera SYSTEMS INITIATIVE