Trace-based timing fault localization with supply voltage sensor

Miho Ueno, Masanori Hashimoto, Takao Onoye

Osaka University

{ueno.miho, hasimoto, onoye}@ist.osaka-u.ac.jp

Outline

2

Outline

3

Background

Electrical timing fault

- is a bug that arises even though the circuit is logically correct and is caused by dynamic events

- arises only a certain situation and its reproduction is difficult

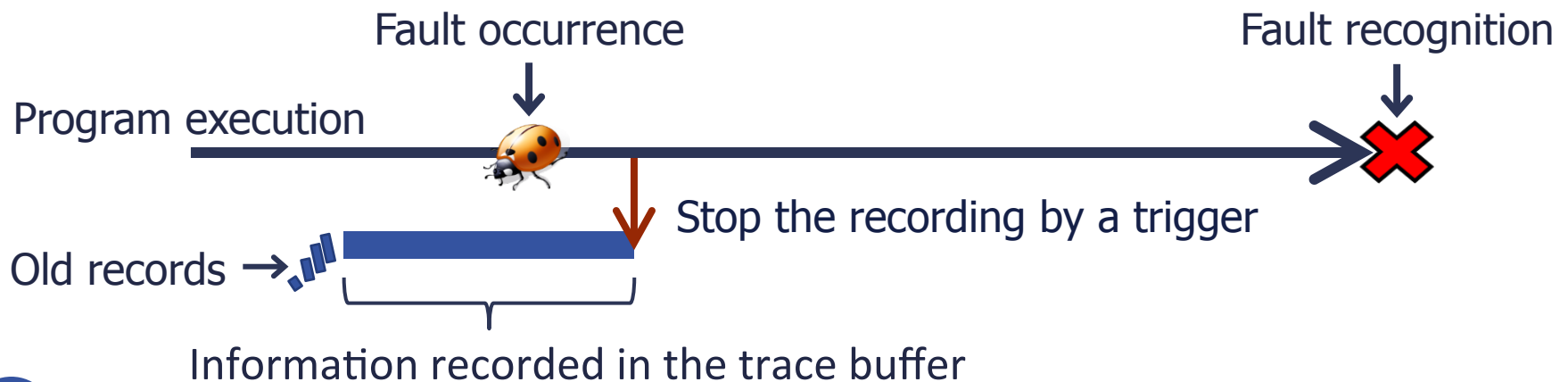⇒It is hard to debug the electrical timing fault.

Dynamic events

Supply noise

Temperature gradient
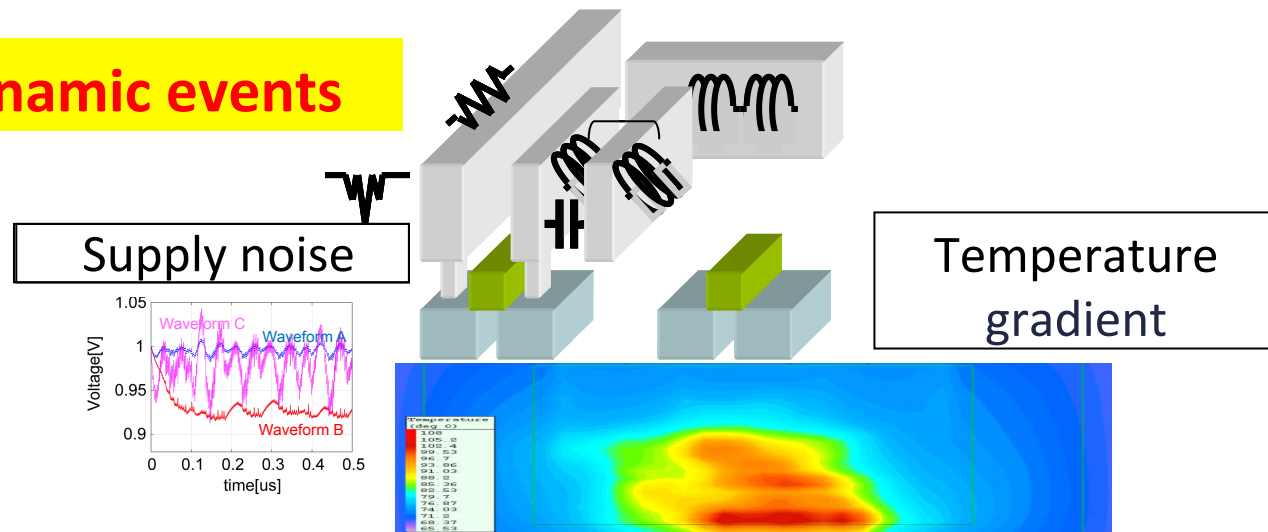
Trace-based fault localization system

Trace buffer[1] records circuit signals and status at every cycle.

× Trace buffer involves additional area overhead.

A trigger signal ⟶ crucially important

- is generated after a fault occurs.

- prevents to overwrite the fault information.

Fault occurrence

Fault recognition

Program execution

Stop the recording by a trigger

Old records →

Information recorded in the trace buffer

[1] M. Abramovici, P. Bradley, K. Dwarakanath, P. Levin, G. Memmi, and D. Miller, "A reconfigurable design-for-debug infrastructure for SoCs," *DAC*, pp. 7–12, 2006.

5

Trigger quality

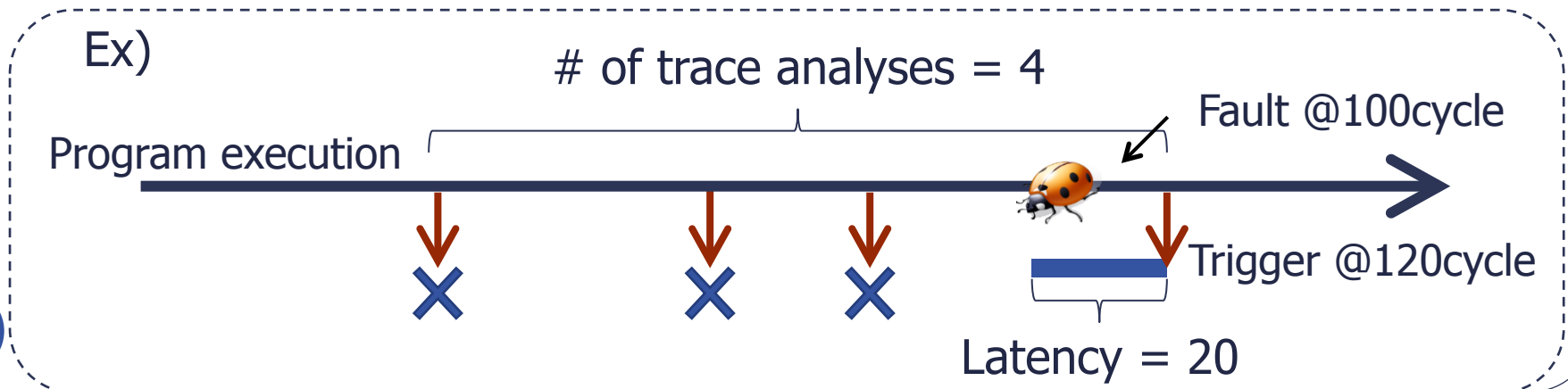1. Latency

- Time interval between timing fault and trigger.

- Shorter latency is desirable.

2. # of trace analyses

- # of traces to check if a timing faults is included until a trace captures the target timing fault.

- Smaller number is desirable.

Ex)

# of trace analyses = 4

Program execution

Fault @100cycle

Trigger @120cycle

Latency = 20

Objective

- Trigger quality is very important
  - for area overhead.
  - for fault localization efficiency.
- Conventionally logical events are used as triggers (e.g. deadlock and segmentation fault [2]).
  - ×Electrical timing faults can be recorded only when the fault influence appears as a logical event.
  - ×It takes a long time for appearance.

Objective

Directly observe power supply noise and improve trigger quality.

[2] Sung Boem Park, Ted Hong, and Subhasish Mitra, "Post-Silicon Bug Localization in Processors Using Instruction Footprint Recording and Analysis (IFRA)," *IEEE Trans. on CAD*, pp. 1545-1558, 2009

Outline

1. Background and objectives
2. Proposed timing fault localization system
3. Supply voltage sensor
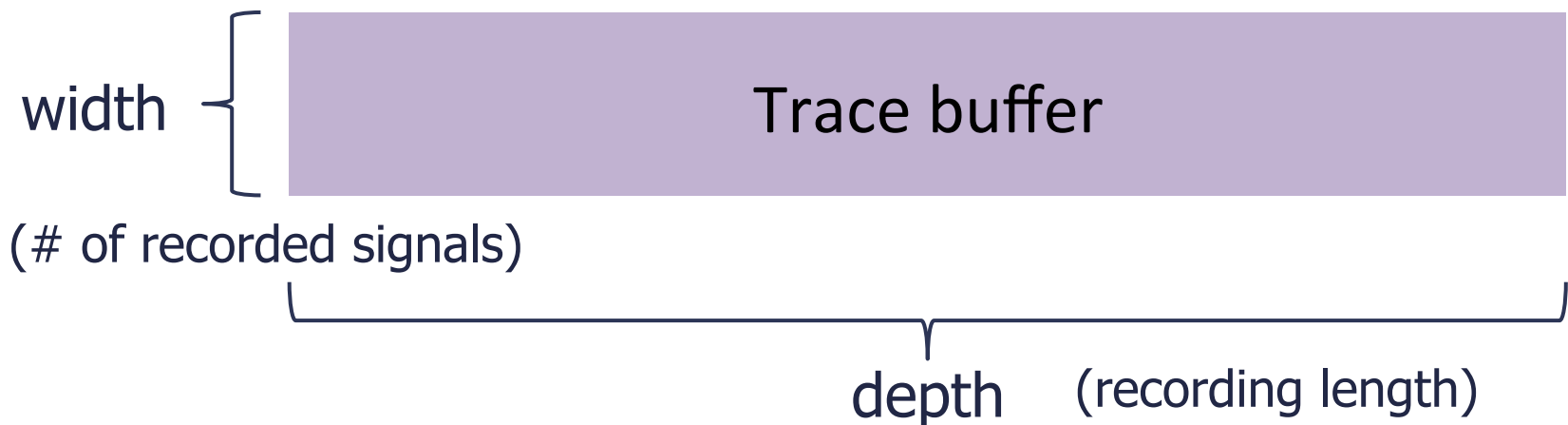4. Evaluation of fault localization performance
5. Conclusion

8

Proposed timing fault localization system

- Proposed system consists of trace buffer, trigger generator and supply voltage sensor.

Circuit under test (CUT)	Trigger generator	Supply voltage sensor

Some internal signals to record

Trigger

Sensing data
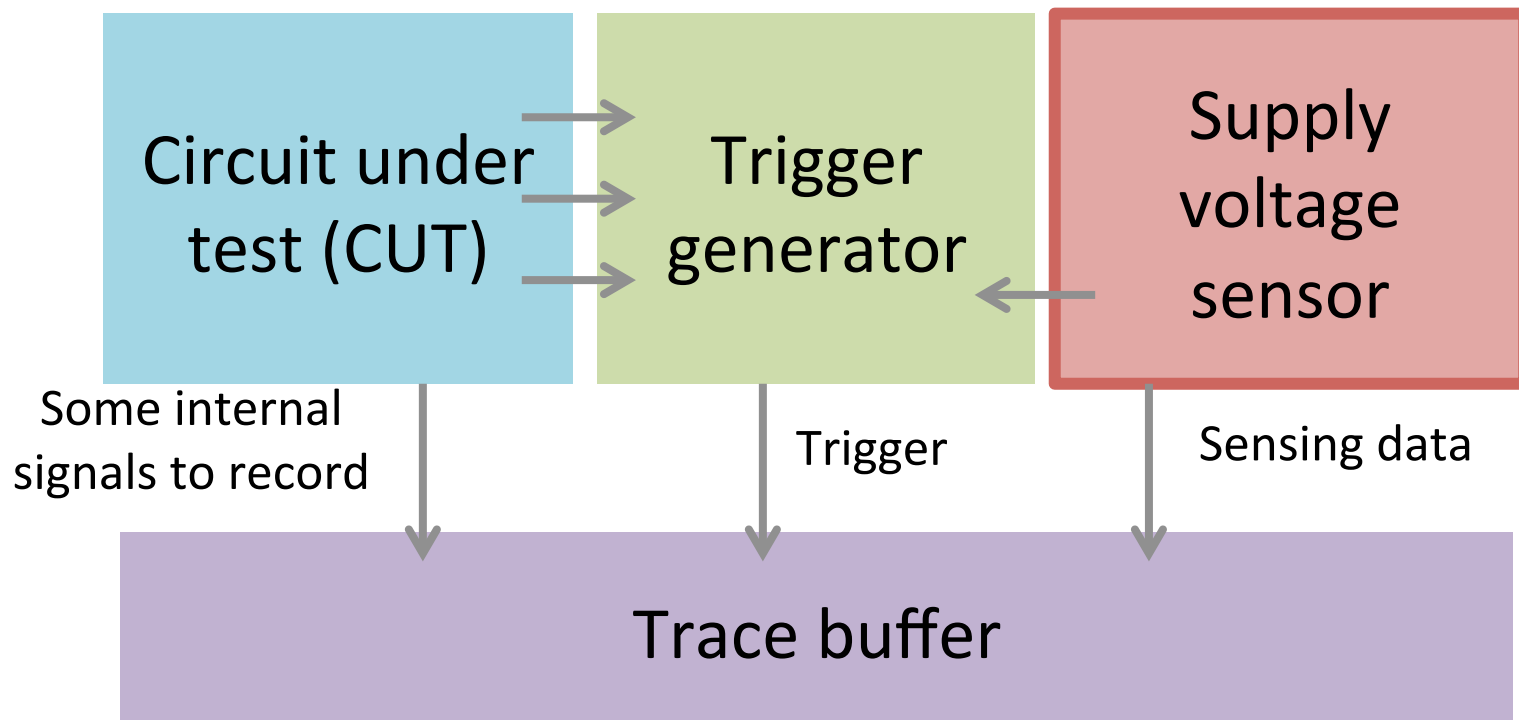
Trace buffer

Trace buffer

- Trace buffer aims to store the information which is useful for localizing electrical timing faults.

- Both width and depth of the trace buffer must be minimized for area overhead reduction.

⇔Fault localization efficiency, i.e. # of trace analyses is maintained.

width {
[Trace buffer]

(# of recorded signals)

depth (recording length)

Supply voltage sensor

Provides supply voltage information to trigger generator and trace buffer.

- Sensor should measure cycle-by-cycle supply voltage fluctuation, since a timing fault occurs depending on supply voltage within the corresponding cycle.

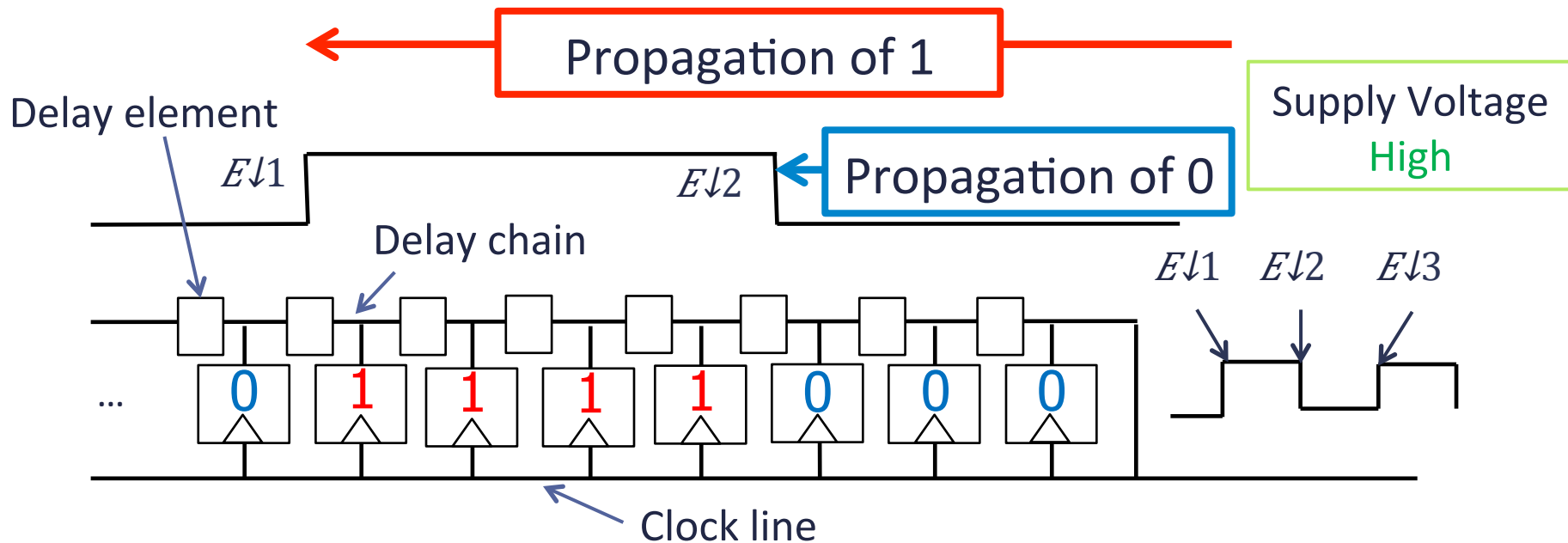- To immediately exploit sensing results for trigger generation, real-time sensing is demanded.
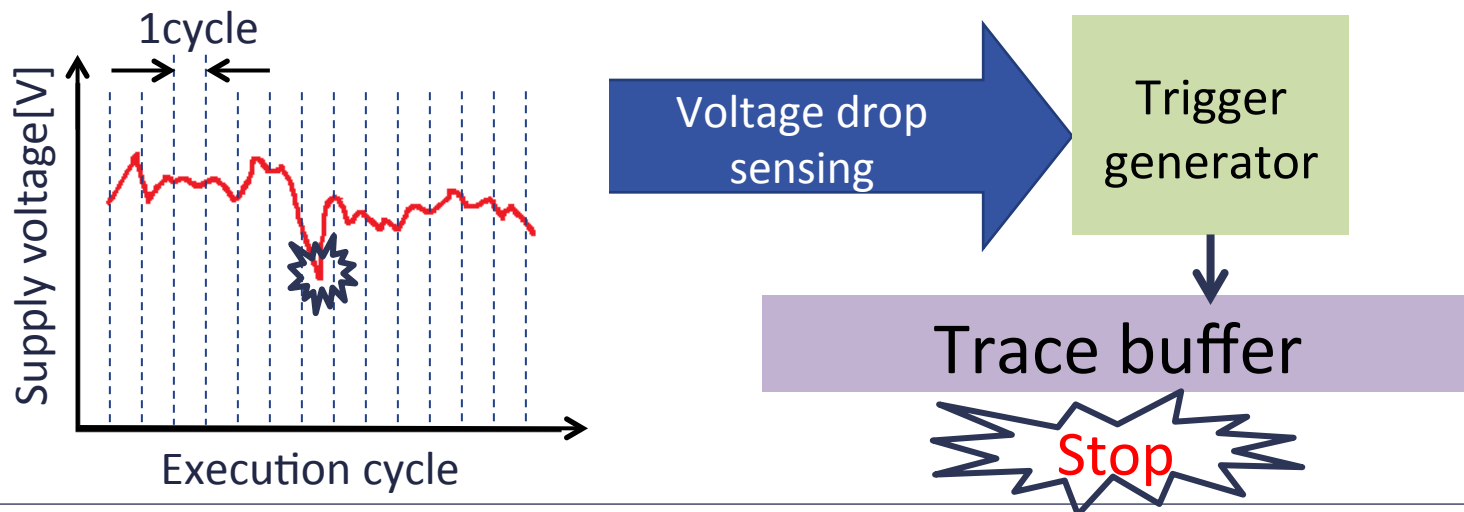
Outline

12

Sensor structure and operation

Supply voltage sensor consists of a delay chain and TDC (Time to Digital Converter).

Latch the signal at $E{\downarrow}3$

- Distance of $E{\downarrow}1$ propagation (N_{passed}) represents Vdd.
- Every cycle and one-shot sensing is achieved.

Sensor structure and operation

Supply voltage sensor consists of a delay chain and TDC (Time to Digital Converter).

$E{\downarrow}1$ $E{\downarrow}2$

Supply Voltage
Low

$E{\downarrow}1$ $E{\downarrow}2$ $E{\downarrow}3$

… 0 0 0 1 1 1 0 0

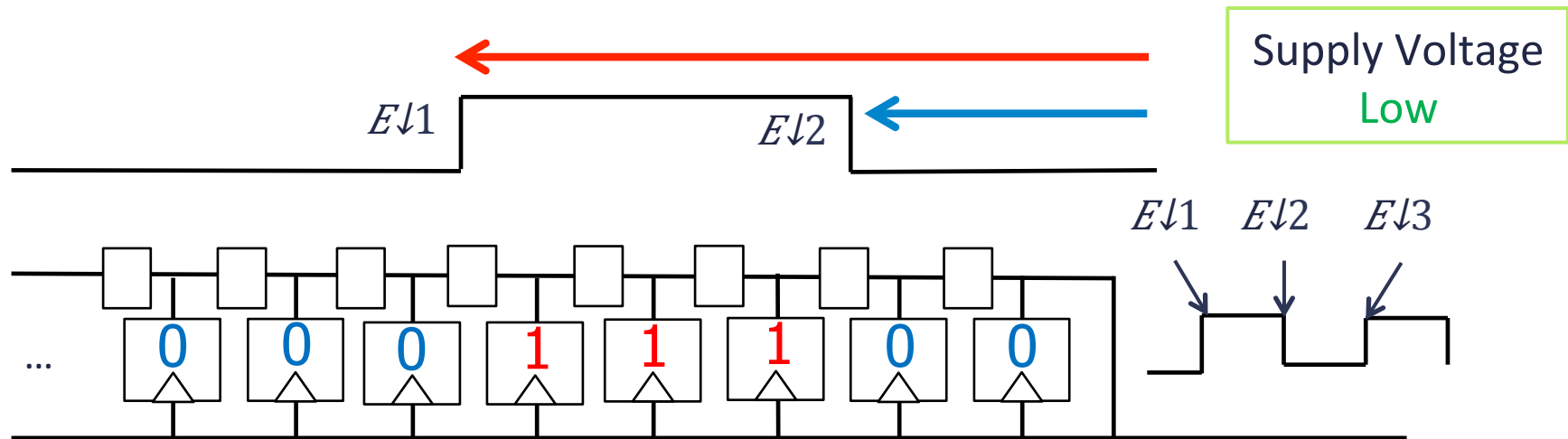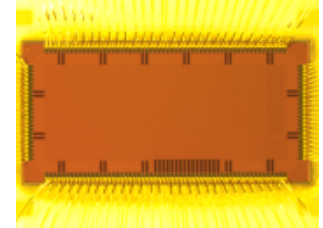## Latch the signal at $E{\downarrow}3$

- Distance of $E{\downarrow}1$ propagation (N_{passed}) represents Vdd.
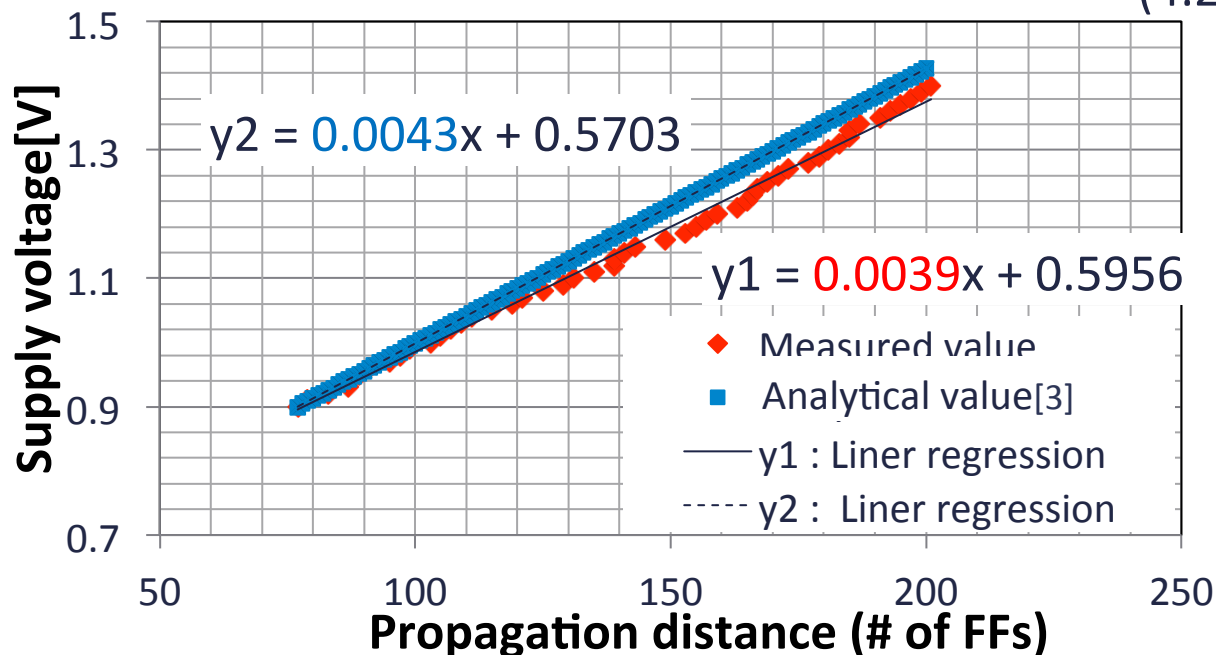- Every cycle and one-shot sensing is achieved.

14

Measured voltage resolution

Supply voltage sensor w/ 256-stage TDC

- is implemented on a 65-nm process test chip.
- occupies 0.138% of the test chip.

Test chip
(4.2mm ×2.1mm)

$y2 = 0.0043x + 0.5703$

$y1 = 0.0039x + 0.5956$

- ◆ Measured value
- ■ Analytical value[3]
- —— y1 : Liner regression
- ---- y2 : Liner regression

Supply voltage[V] (y-axis)

Propagation distance (# of FFs) (x-axis)

Voltage resolution of 3.9mV

[3] Miho Ueno, Masanori Hashimoto, and Takao Onoye, "Real-Time Supply Voltage Sensor for Detecting/Debugging Electrical Timing Failures," in *Proc. of IEEE IPDPSW*, pp. 301-305, 2013
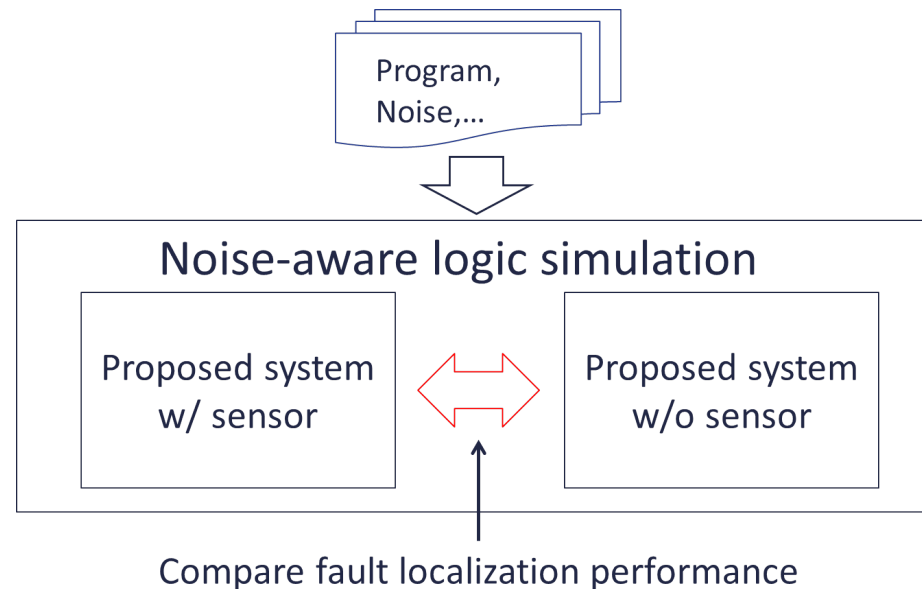
15

Outline

16

Evaluation environment

- To reproduce noise-induced timing faults, a gate-level logic simulation framework that considers dynamic supply noise is developed.

- We used
  - TOSHIBA MeP processor as a CUT.
  - three MiBench programs (SHA1, CRC32, dijkstra).

Program, Noise,...

Noise-aware logic simulation

Proposed system w/ sensor		Proposed system w/o sensor

Compare fault localization performance

An example of simulation result

An electrical timing fault occurred when the voltage dropped to a low value of 0.823V.

Simulation result (dijkstra)

Timing fault at 58735 cycle
Supply voltage : 0.823V

(Y-axis: Supply voltage [V], X-axis: Execution cycle)
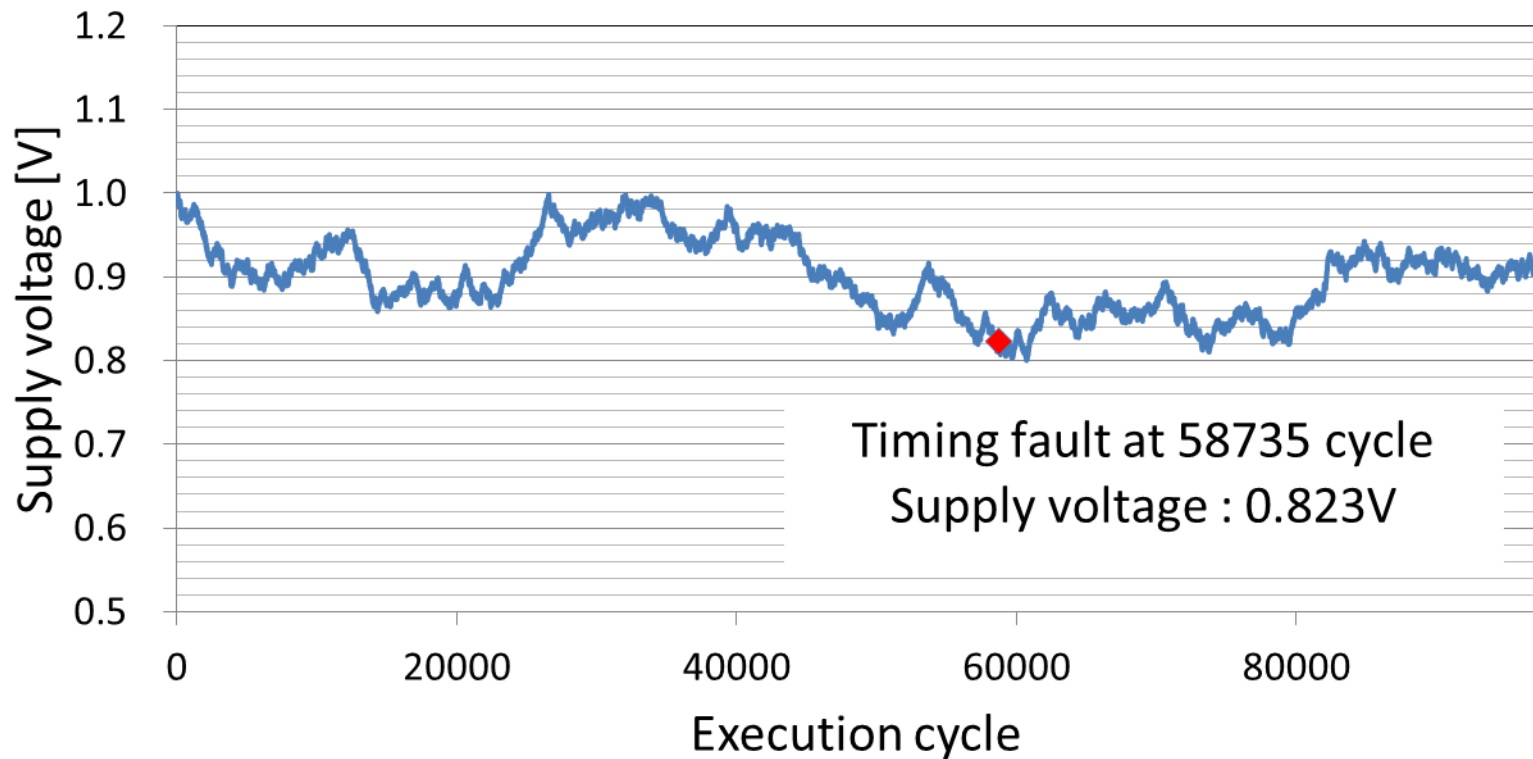
Setup for trigger quality evaluation

Trigger setting

- Threshold value of supply voltage.
    - (Any, ≤ 0.96, ≤ 0.92, ≤ 0.88, ≤ 0.84, ≤ 0.80)
- Instruction executing in the CUT.
    - Instructions supposed to activate timing-critical paths were selected.
    - For example, for instructions (ret, lw, sw, jmp) were selected from dijkstra program.

AND

Comparison to trigger based on logical event

- Memory access error, Exception handling etc.

Reminder: Metrics of trigger quality

1. **Latency**
- Time interval between timing fault and trigger.
- **Shorter** latency is desirable.

2. **# of trace analyses**
- # of traces to check if a timing faults is included until a trace captures the target timing fault.
- **Smaller** number is desirable.

Ex)

# of trace analyses = 4

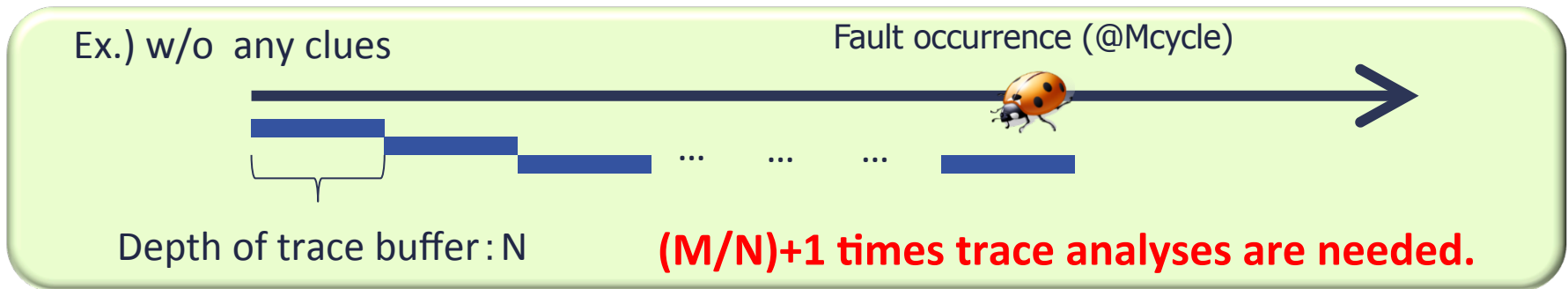Program execution

Fault @100cycle

Trigger @120cycle
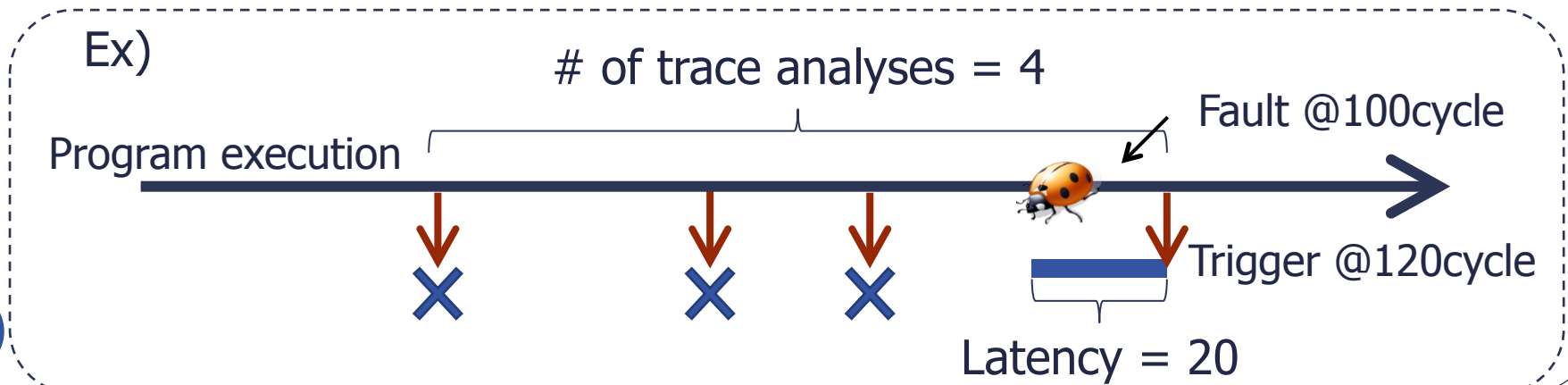
Latency = 20

Trigger quality improvement (dijkstra)

Voltage Condition	Instruction Condition							
	ret		lw		sw		Jmp	
	# of trace analyses	Latency	# of trace analyses	Latency	# of trace analyses	Latency	# of trace analyses	Latency
Any	461	26	10,439	52	4,502	2	318	140
≤0.96	354	26	8,886	52	3,754	2	262	140
≤0.92	237	1/13	6,075	1/45	2,583	1/25	179	1/21
≤0.88	121	26	2,386	52	1,196	2	95	140
≤0.84	36	26	232	52	183	2	15	140
≤0.80	0	N/A	0	N/A	0	1,977	0	N/A

# of trace analyses can be significantly reduced thanks to voltage sensor.

Comparison to logical event trigger

Logical events were observed in all three programs.

- Trigger activation w/ logical events was not useful.
  - Fault localization must be carried out without any clues.

Ex.) w/o any clues

Fault occurrence (@Mcycle)

... ...

Depth of trace buffer : N

(M/N)+1 times trace analyses are needed.

For example, supposing buffer depth is 16,

- \# of trace analyses is 3671.
- w/ a trigger setting of "sw" and "≤0.84", it becomes 183.

\# of trace analyses is reduced to 1/20.

Trigger sweep policy

Repeating trace analyses w/ different trigger settings, we have two policies in sweeping priority.

A) Fix instruction and change **voltage threshold first**.

B) Fix voltage threshold and change **instruction first**.

Trigger condition priority (dijkstra program)

- Voltage threshold
  - 0.80V → 0.84V → 0.88V → 0.92V → 0.96V →Any

- Instruction
  - ret → lw → sw → jmp
    - This order is decided by the frequency of timing violation in the program.

Compare # of trace analyses with policy A) and B) .

Evaluation result of trigger sweep policy

I. **Trace buffer depth is 100.**

- Policy A) : # of trace analyses is 38.
- Policy B) : # of trace analyses is 41.

← comparable

II. **Trace buffer depth is 2.**

- Policy A) : # of trace analyses is 56,879.

- Policy B) : # of trace analyses is 2,090. ← superior

In this case, we should change **instruction condition** first before raising voltage threshold.

Outline

1. Background and objectives
2. Proposed timing fault localization system
3. Supply voltage sensor
4. Evaluation of fault localization performance
5. Conclusion

Conclusion

We proposed a timing fault localization system with a supply voltage sensor.

- Supply voltage sensor
  - could provide cycle-accurate voltage variation.
  - had 4mV voltage resolution on a 65-nm test chip.
- Proposed system w/ a voltage sensor
  - was helpful for reducing trace buffer depth.
  - reduced # of trace analyses and improved efficiency of timing fault localization.
- Future work includes evaluation of more complex trigger condition with a number of test programs.