black hat
USA 2022

Tunable Replica Circuit for Fault-Injection Detection

Daniel Nemiroff

Carlos Tokunaga

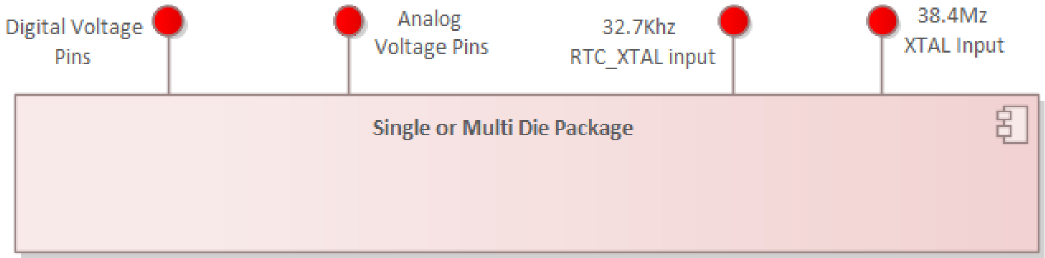
black hat®
USA 2022

- Fault-Injection Attack Basics
- Dive into the TRC (Tunable Replica Circuit)
- Why and How Intel Integrated the TRC
- TRC Calibration and Validation
- Conclusions and Productization

Non-Invasive FI Attacks

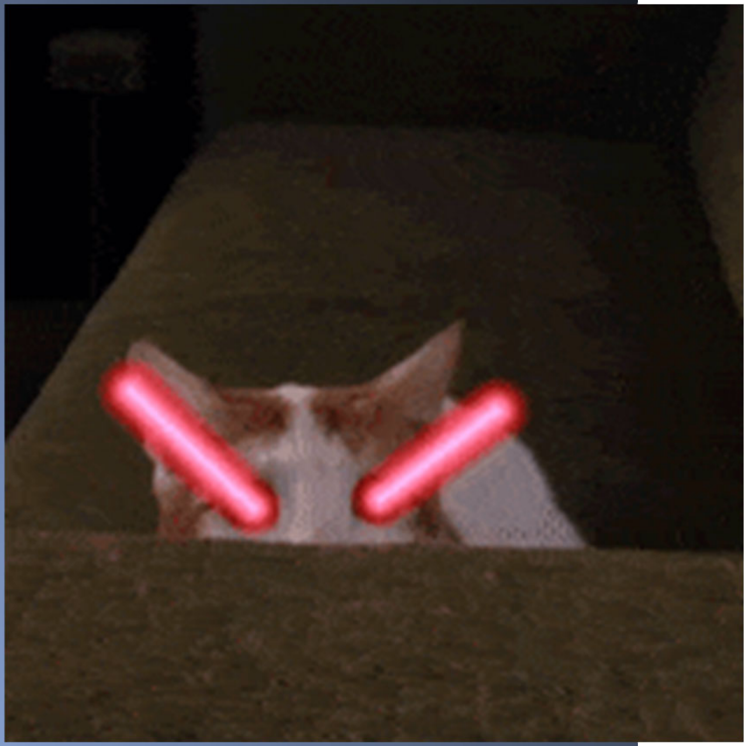
- This briefing covers the fault-injection detection circuit, known as the TRC (tunable replica circuit).
- Our focus is non-invasive FI attacks, where modification of the package is out of scope, this includes:
- Voltage attacks
- Clock attacks
- EM (electro-magnetic radiation) attacks
- Thermal attacks

Non-Invasive FI Attacks



As they are exposed at the package-level, clock and voltage pins are the primary non-invasive attack surface.

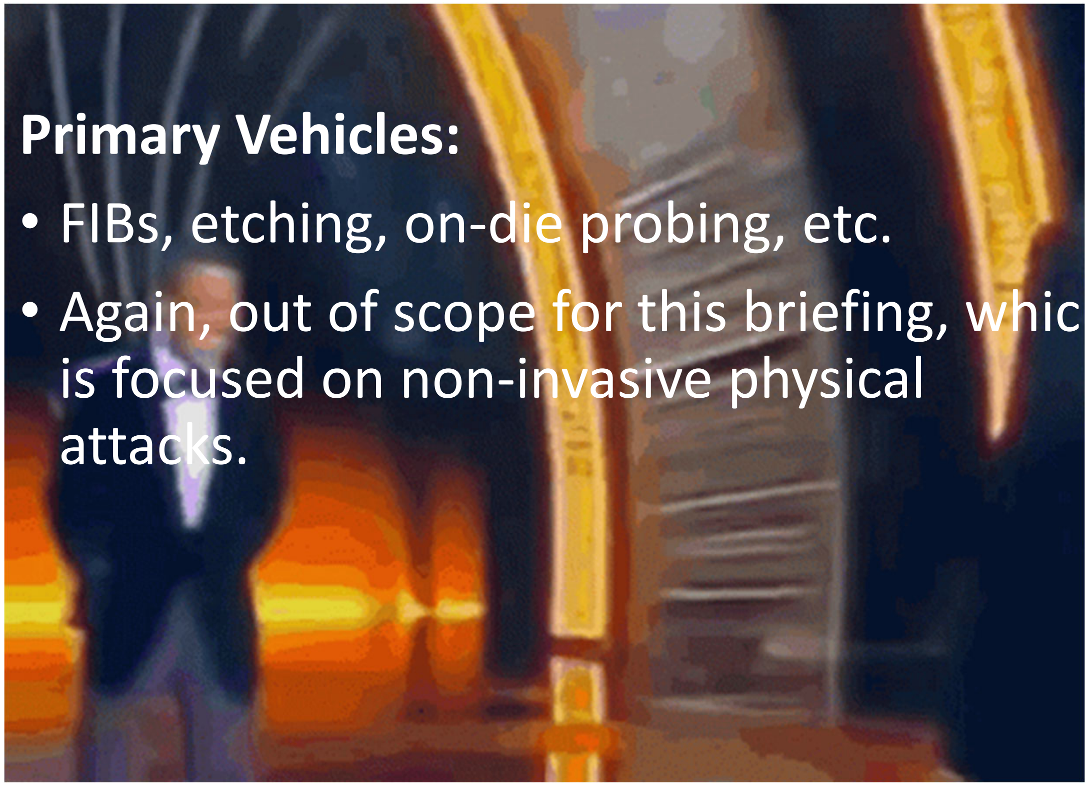
Semi-Invasive FI Attacks



- Lasers are a primary semi-invasive threat, because they require a package de-lid.
- However, research shows attacks from the side of a package can be done, without a de-lid.
- These attacks are out of scope for this briefing.

To Complete the Circle . . .

. . . Invasive Physical Attacks



Primary Vehicles:

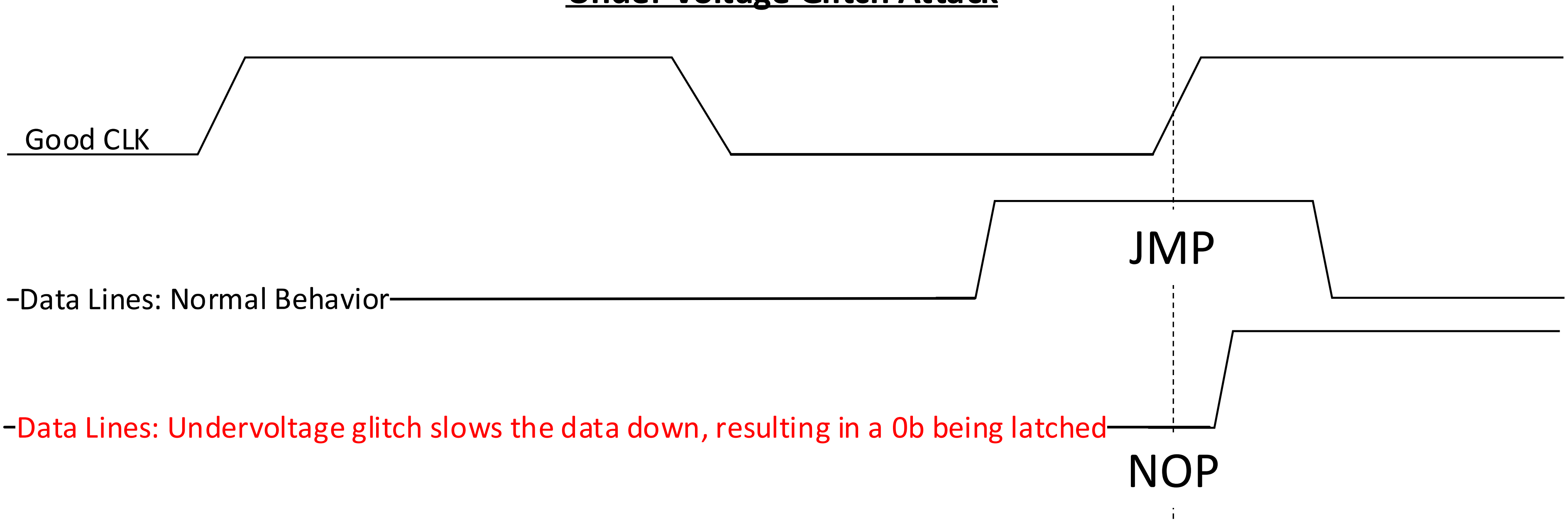
- FIBs, etching, on-die probing, etc.
- Again, out of scope for this briefing, whic is focused on non-invasive physical attacks.

What is the Attacker is Trying to Accomplish with FI?

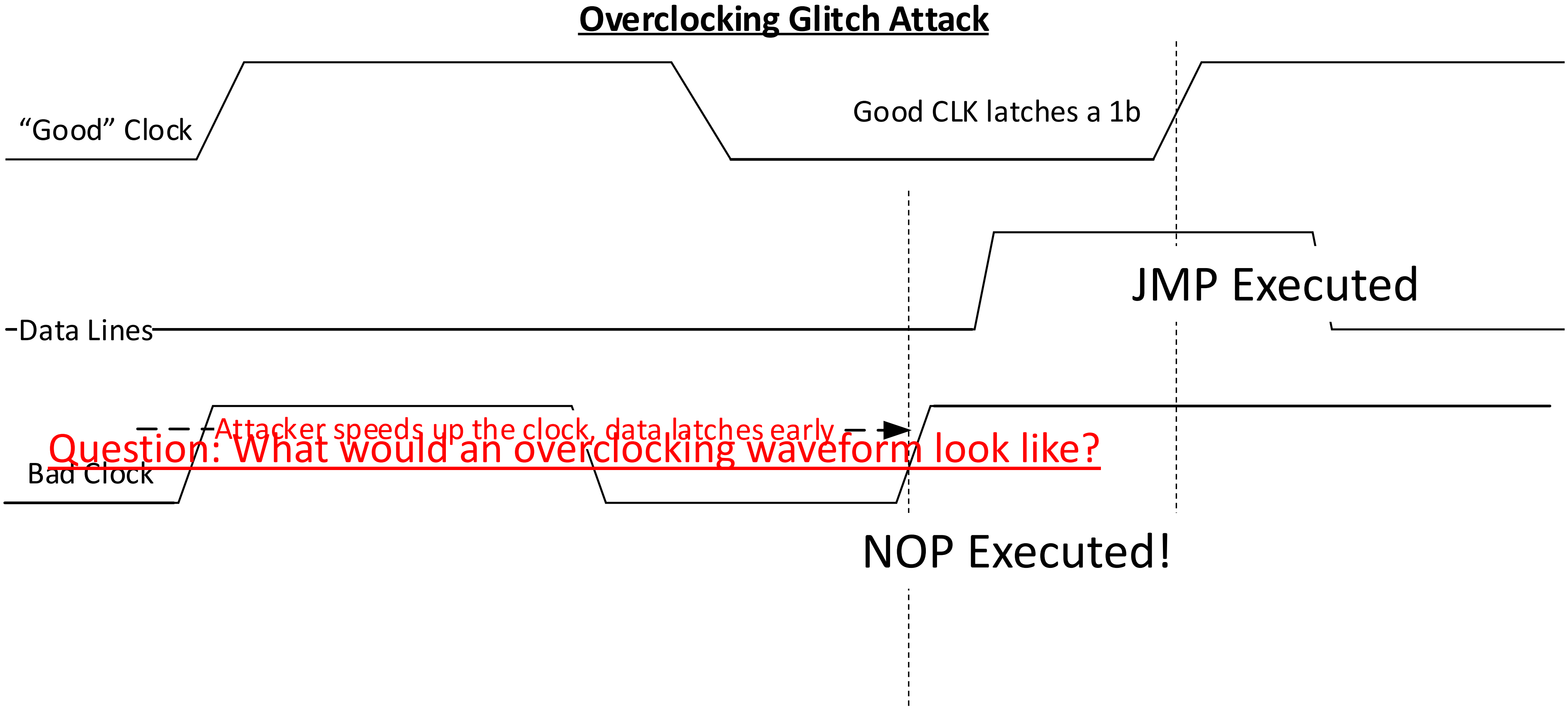
- Using FI, a common goal of the attacker is to cause circuit timing to fail, without causing the platform to crash.
- When circuit timing fails, data can be latched too early or too late.
- In many cases, latching data early causes 0x00 to be latched.
- In the context of a CPU or uC, when glitched at just the right time, an attack can cause a NOP to be latched, instead of a JMP.
- In fixed-function crypto engines, real keys could be replaced, etc.
- In fabrics and busses, I/O devices could latch data or bus addresses too early/late.

Voltage Glitch Impact on Timing

Under-voltage Glitch Attack


Good CLK
Data Lines: Normal Behavior
JMP
Data Lines: Undervoltage glitch slows the data down, resulting in a 0b being latched
NOP

Clock Glitch Impact on Timing

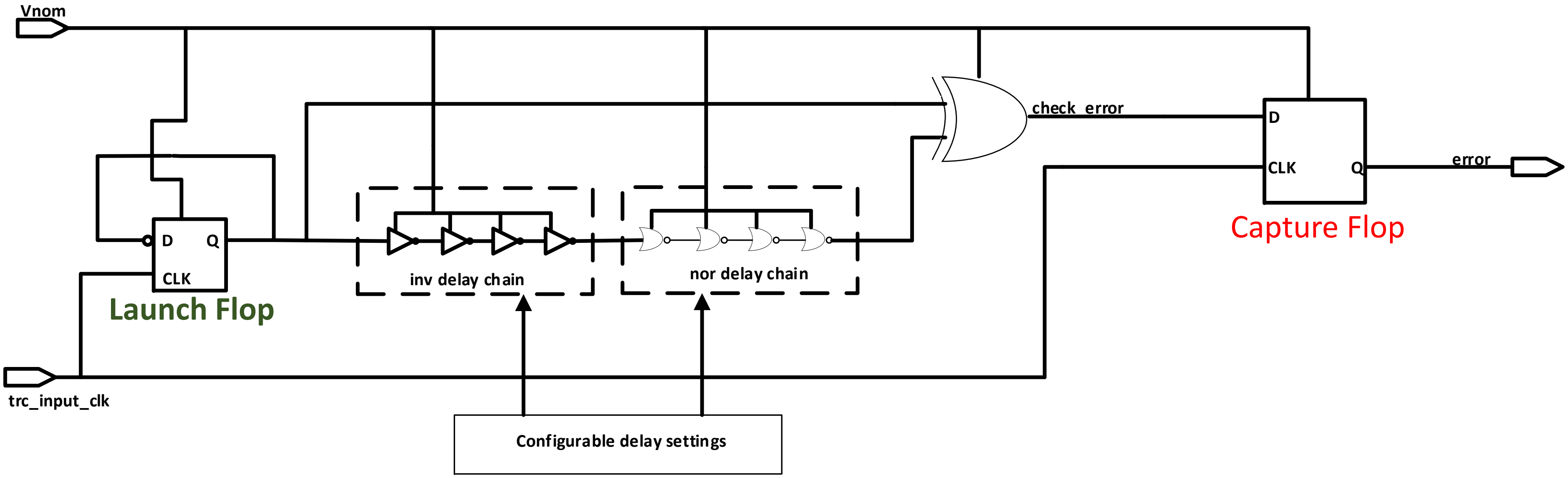


Question: What would an overclocking waveform look like?

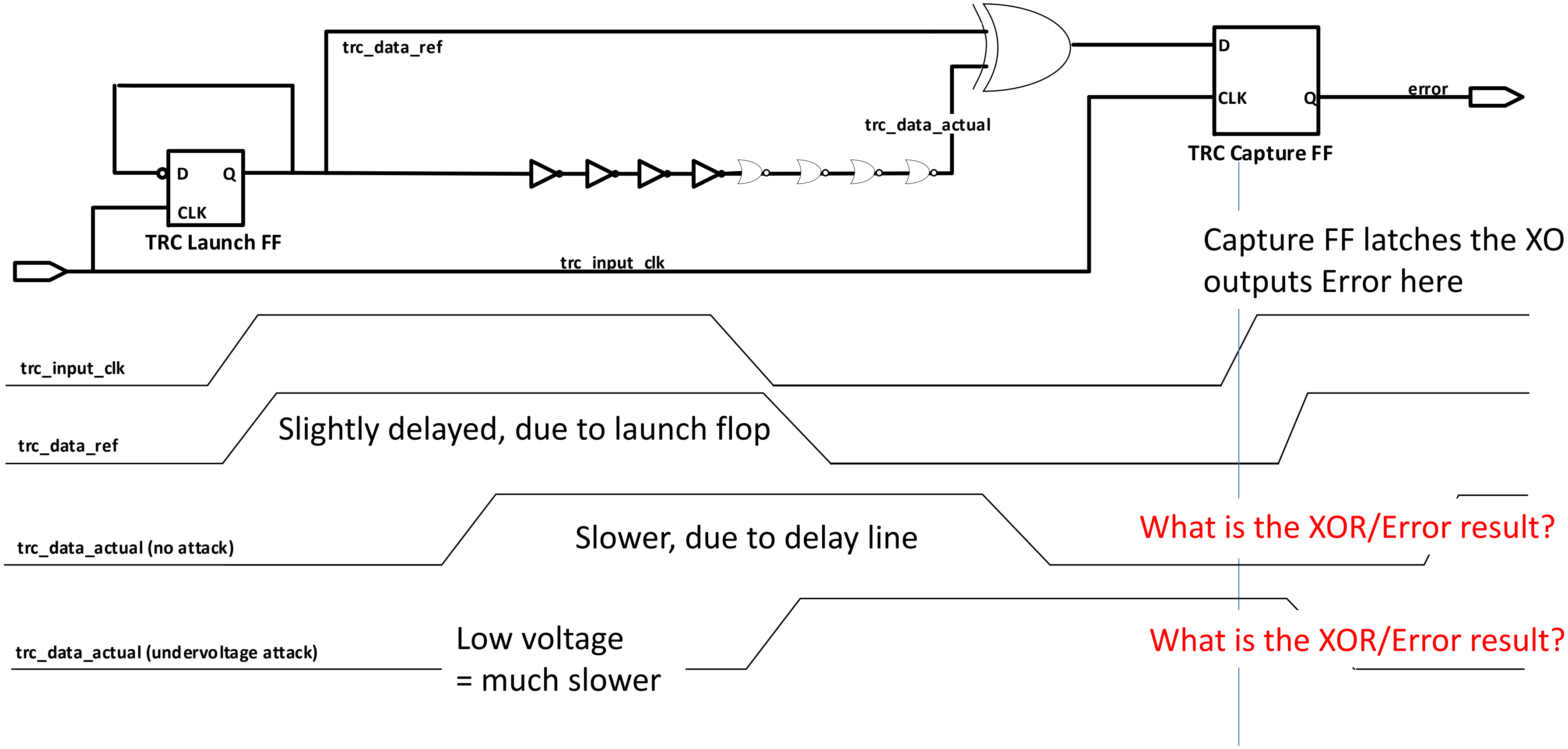
- Fault-Injection Attack Basics
- Dive to the TRC (Tunable Replica Circuit)
- Why and How Intel Integrated the TRC
- TRC Calibration and Validation
- Conclusions and Productization

The TRC (Tunable Replica Circuit)

- The TRC was designed to mitigate aging in silicon by analyzing circuit timing.
- It consists of a **launch flip-flop**, a tunable delay chain, and a capture flop.
- The capture flop detects when a signal exits the delay chain at the wrong speed.
- Since FI often seeks to induce timing violations, the TRC can help detect FI attacks.



Deeper Dive into TRC Behavior



Capture FF latches the XOR, & outputs Error here

Slightly delayed, due to launch flop

Slower, due to delay line

What is the XOR/Error result?

Low voltage
= much slower

What is the XOR/Error result?

Why Intel Selected the TRC

Traditional FI detection circuits are dedicated analog voltage-level detectors, analog clock monitors and thermal sensors, so why did we choose the TRC:

1. The TRC was a proven technology at Intel, analog circuits would be new.
2. The TRC can help detect multiple attacks (clock, voltage, EMFI, temp).
3. The TRC is a digital circuit, easy to port to future process nodes.
4. The TRC is small in die area.

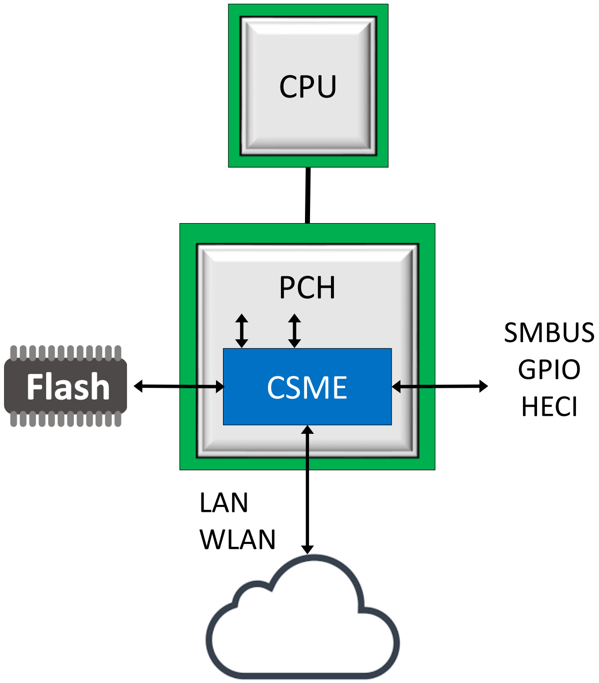
Advantages of Traditional Analog FI Sensors:

- Precision
- Independent Detection of Attacks → The TRC will not detect if both voltage and clock frequency increase.

black hat
USA 2022

- Fault-Injection Attack Basics
- Dive to the TRC (Tunable Replica Circuit)
- Why and How Intel Integrated of the TRC
- TRC Calibration and Validation
- Conclusions and Productization

What Is CSME?



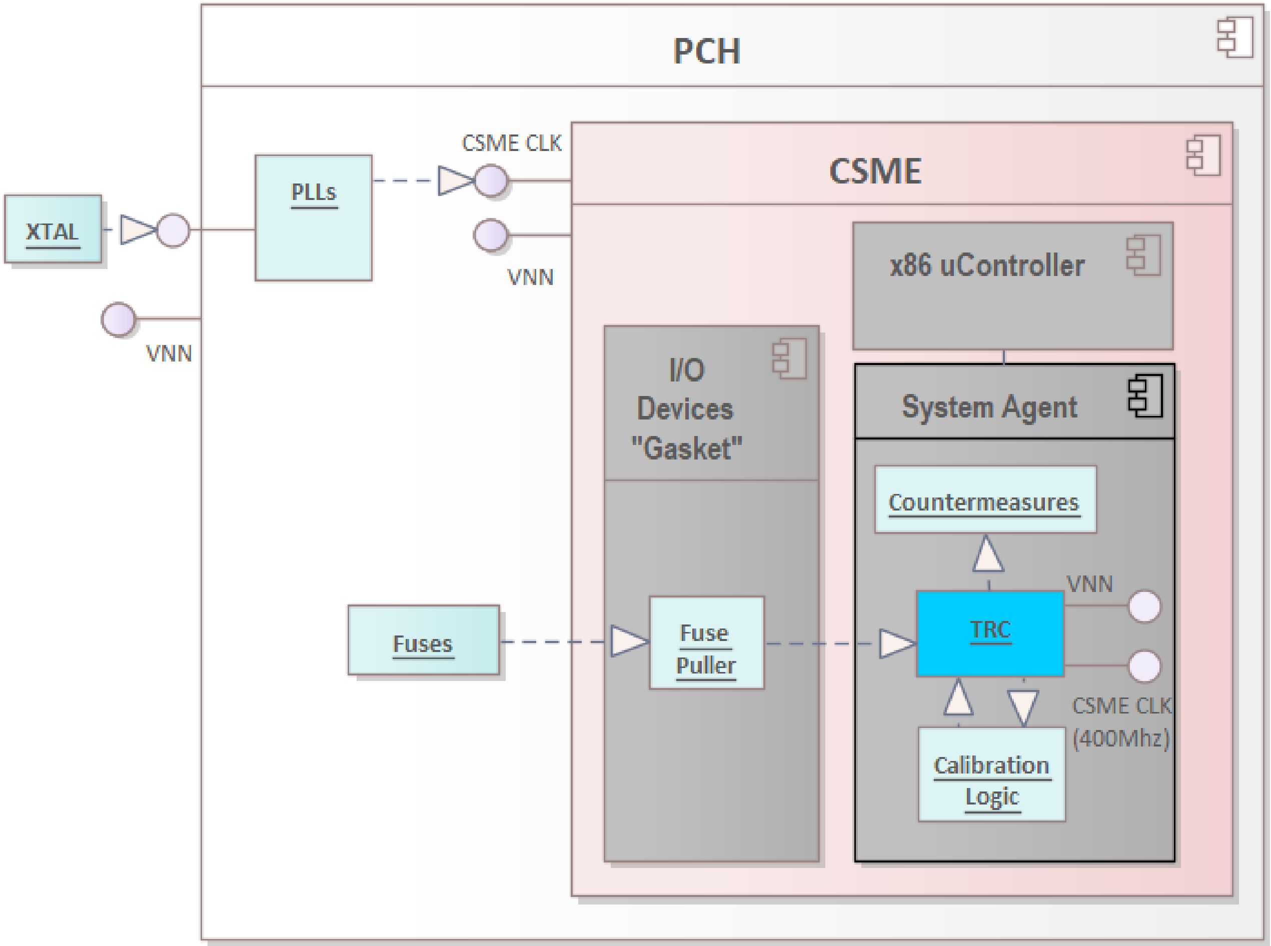
CSME is an embedded subsystem in Platform Controller Hub (PCH)

- Stands for **C**onverged **S**ecurity & **M**anageability **E**ngine
- Standalone low power Intel processor with dedicated Hardware (HW)

CSME is Root of Trust of the platform

- Provides an isolated execution environment protected from host SW running on main CPU
- Executes CSME Firmware (FW)

TRC Integration into CSME



Details for the CSME-TRC

- The TRC is integrated into the system agent partition of CSME.
- The CSME-TRC monitors the power and clock coming into CSME, to help protect all portions of CSME from an attack.
- When the TRC detects a glitch, it invokes countermeasures that result in a CSME reset. The rest of the SoC is not impacted.
- The TRC is on the same reset line as all CSME HW, and if CSME is on, the TRC is monitoring this power.
- If CSME is power-gated, the TRC is also power-gated.

Why Integrate the TRC?

- Physical attacks have become cheaper to mount with FI equipment available for purchase or rent.
- Intel views security as an evolutionary process with a roadmap of incremental and meaningful countermeasures . . . the TRC is an example of this roadmap.
- Additionally, CSME has supported a TCG compliant TPM2.0 HW starting in 2015.
- It has been our goal to make this the most capable and feature-rich TPM2.0 on the market.
- In order to compete with discrete TPM devices, physical attack mitigations, like the TRC, are required.

- Fault-Injection Attack Basics
- Dive to the TRC (Tunable Replica Circuit)
- Why and How Intel Integrated of the TRC
- TRC Calibration and Validation
- Conclusions and Productization

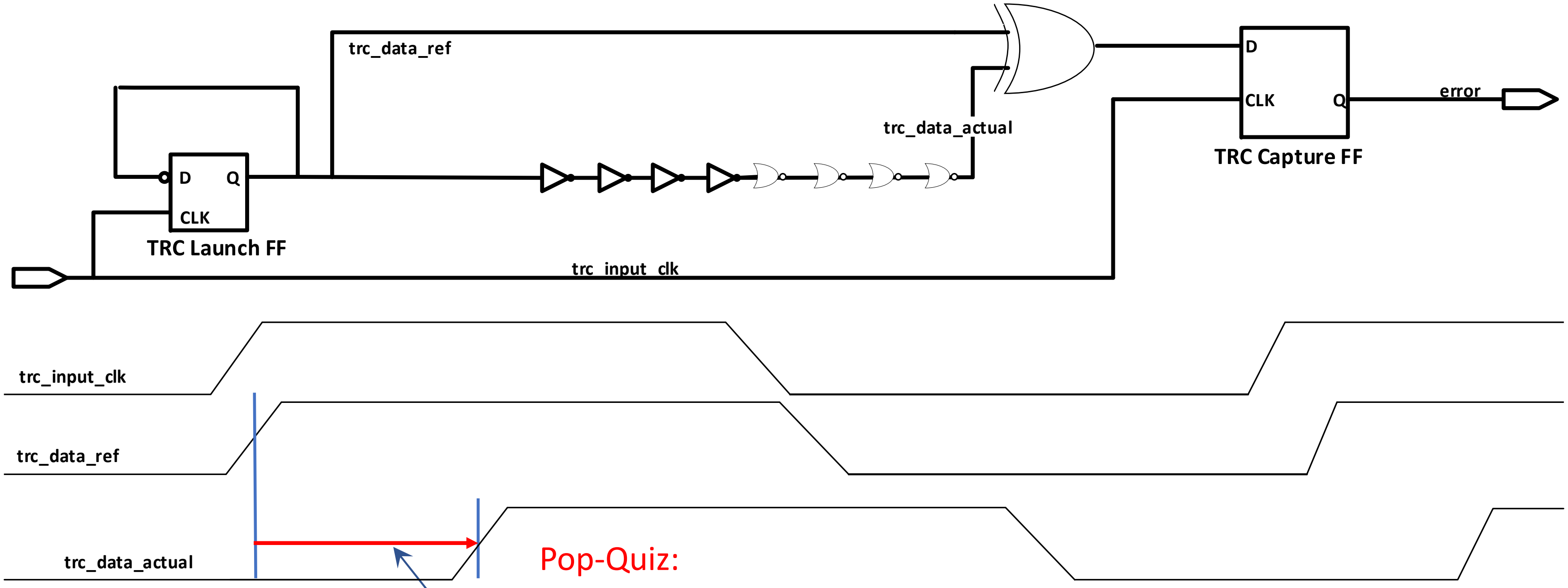
Calibrating the TRC to Detect an Attack

- Circuits fail timing at a specific point on a Voltage/Frequency curve.
- At a fixed frequency, we know what voltage the circuits will fail.
- This point is called vGlitch, calculated using pre and post-silicon data.

➢ **vGlitch is global to each product**

- *TRC calibration is the act of converting vGlitch to a TRC delay and fusing that configuration into silicon.*
- To ensure the calibration is correct, a sample of parts from multiple process corners are fused and run through false-positive and fault-injection testing.
- If any parts fail either test, the recipe is modified, and the process starts over.
- Once no failures occur, the calibration determined to be correct and high-volume manufacturing can begin.

TRC Waveforms and Calibration



Pop-Quiz:
Identify the Delay that corresponds to vGlitch

This is the Delay, corresponding to vGlitch, that is fused into each part

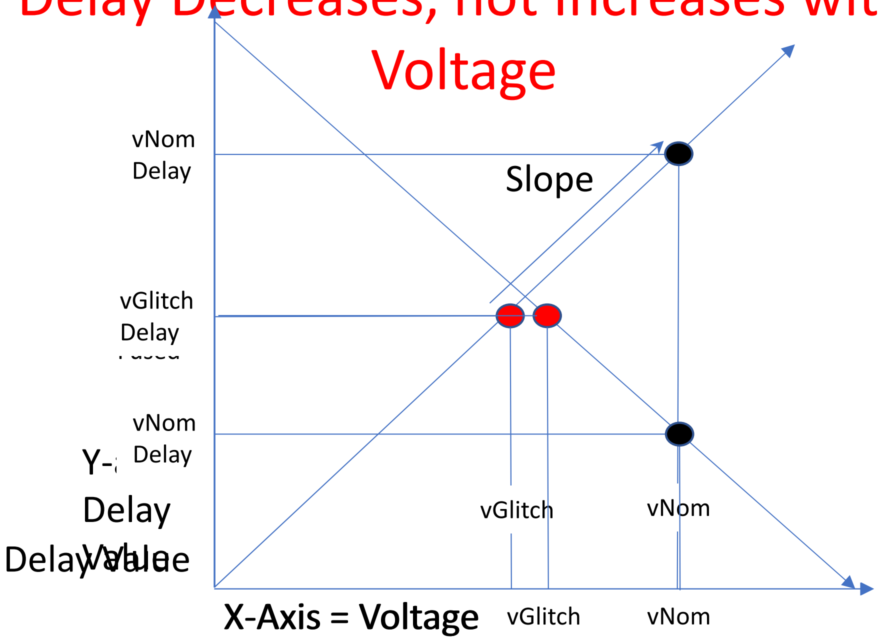
How is the Per-Part vGlitch Delay Found?

1. At first-silicon we calculate the slope associated with a Voltage/Delay curve, common to all parts.
2. In HVM (high-volume manufacturing) each part's TRC outputs to HVM testers the TRC delay at nominal voltage.
3. Using the Voltage/Delay slope, testers calculate the TRC delay (for each part) at vGlitch (using the below equation) and fuse this into silicon.

vGlitchDelay = vNomDelay – (vGlitch / Slope)

- (vGlitch / Slope) is a constant
- vNomDelay is per-part data, captured in HVM

Delay Decreases, not Increases with Voltage



Pop Quiz: What is wrong with the graph?

Fault-Injection Testing

black hat USA 2022

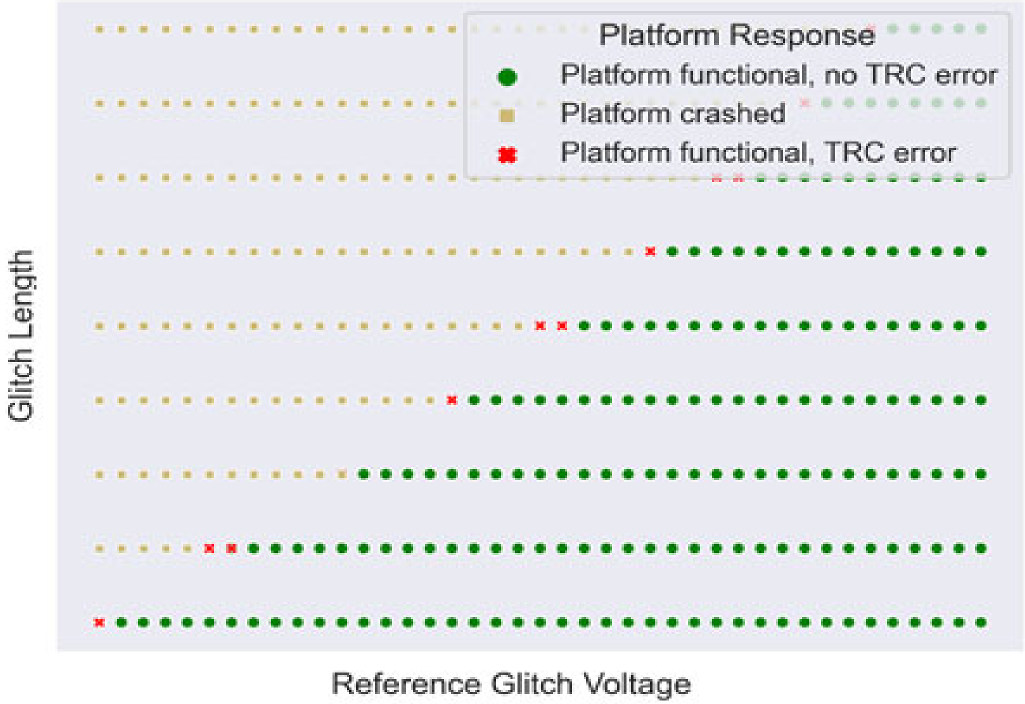
FI voltages are driven from a generator for varying pulse-widths.

The band of red X's highlights the TRC's detection capability.

The region of functionality before the SoC crashes is where an FI exploit will focus, as the objective is to change the state of the system without crashing.

It is critical the red X band be present, proving the TRC is calibrated to detect voltage glitches before they begin crashing the SoC.

As can be seen, in the first pass of testing, the TRC missed some glitches.



TRC Calibration Tuning

The TRC failed initial testing; the red X band did not exist at every glitch length, indicating that the calibrated delay code was set too low.

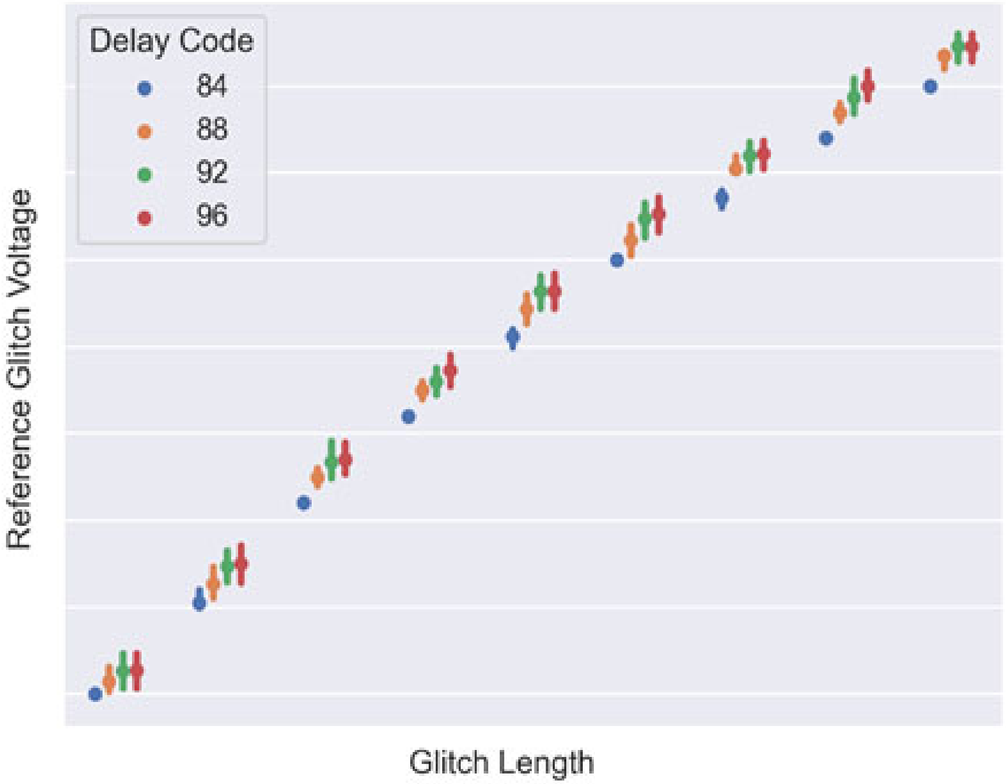
To fine tune the calibration we repeated the glitch scan, schmooing the delay codes.

For a given glitch length, the width of the red X band was measured and plotted, as shown.

The initial delay code was 84.

Increasing the delay from 84 to 92 allowed the TRC to detect glitches in a larger range for a given glitch length.

There was no meaningful detection capability when going to a delay of 96.



- Fault-Injection Attack Basics
- Dive to the TRC (Tunable Replica Circuit)
- Why and How Intel Integrated of the TRC
- TRC Calibration and Validation
- Conclusions and Productization

Testing Results and Productization

- From these (second pass) results we determined the initial batch of TRCs were calibrated too conservatively with vGlitch too low.
- Accordingly, we modified the value of vGlitch.
- New parts were calibrated, fused and (once again) sent through false-positive and FI testing.
- This time, the TRC detected attacks at all glitch lengths while recording no false-positives.
- Based on this data, we locked in this new calibration recipe for all 12th Gen Intel® Core™ (ADL) silicon and committed the TRC to high-volume manufacturing.

Riscure Engagement

- To further gain confidence in the TRC and gain additional insight into FI testing, we contracted with Riscure to evaluate the TRC.
- We submitted multiple 12th Gen Intel® Core™ parts with the TRC to Riscure for clock, voltage and EMFI testing.
- In the end, Riscure was unable to successfully execute a FI attack against CSME, concluding, “In all cases the successful glitches were detected by the implemented countermeasures”

Acknowledgements

Thanks to the engineers who contributed to the TRC at Intel!

- Matias Leonetti
- Swetha Basani
- Parthiv Trivedi
- Sivakumar Ramakrishnan
- Joseph Friel
- Mohamad Faiz Mohd Faridh
- Nanda G Kumar Kalavai
- Masahide Kakeda
- Avinash Varna
- Habib Shawal

Source Citations

GIF citations:

- Slide #3
  - Lightning GIF, from - https://an-crazy.tumblr.com/post/65952328112
  - Big Ben GIF, from - https://gifs.alphacoders.com/gifs/view/75109
  - Magneto GIF, from - https://media.giphy.com/media/xTiQyrLULEB9EBfAwo/giphy.gif
  - Fire GIF, from - https://tenor.com/search/louise-fire-gifs
- Slide #4
  - Cat lasers GIF, from - https://www.wearepercolate.com/
- Slide #5:
  - Will Smith Slap GIF, from - https://www.xavierdegraux.be/
- Slide #6:
  - Muppet Fire GIF, from - https://tenor.com/search/beaker-fire-gifs

Legal Disclaimer

Intel provides these materials as-is, with no express or implied warranties.

All products, dates, and figures specified are preliminary, based on current expectations, and are subject to change without notice.

Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at https://www.intel.com.

Some results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.

Intel and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.

intel®