PicoEMP

A Low-Cost EMFI Platform Compared to BBI and Voltage Fault Injection using TDC and External VCC Measurements

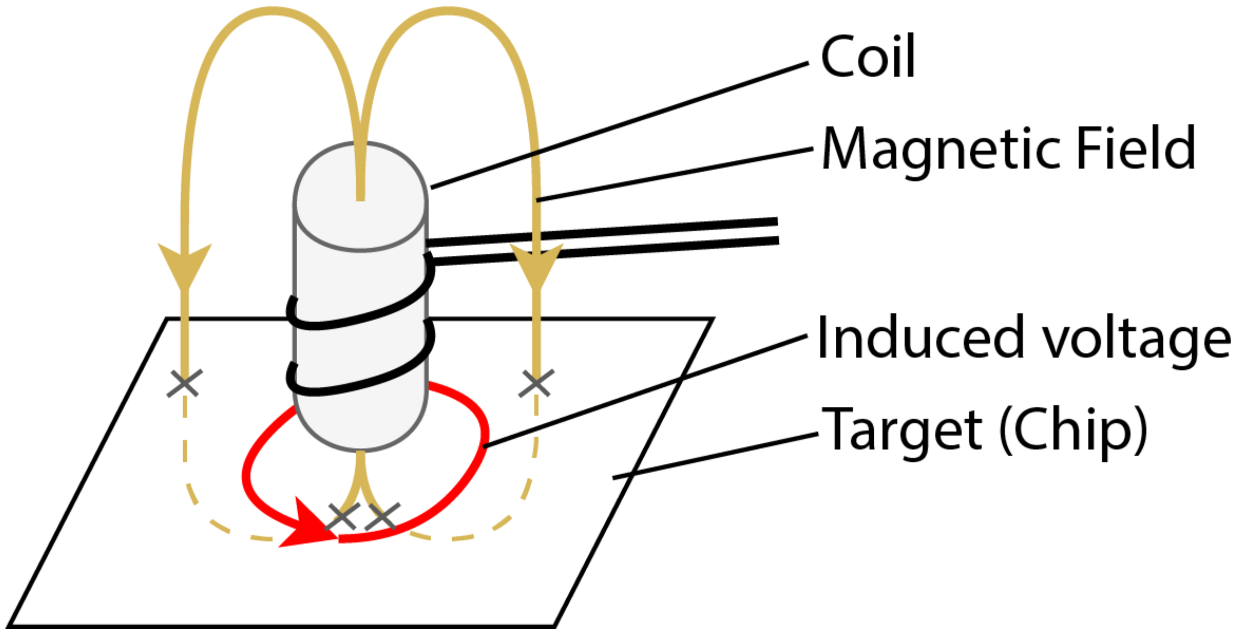
Colin O’Flynn

NewAE Technology Inc. & Dalhousie University

Topics

- EMFI Tools & Building Low-Cost Tools
- TDC for On-Die Voltage Measurement
- Comparing EMFI, Voltage-FI, and BBI

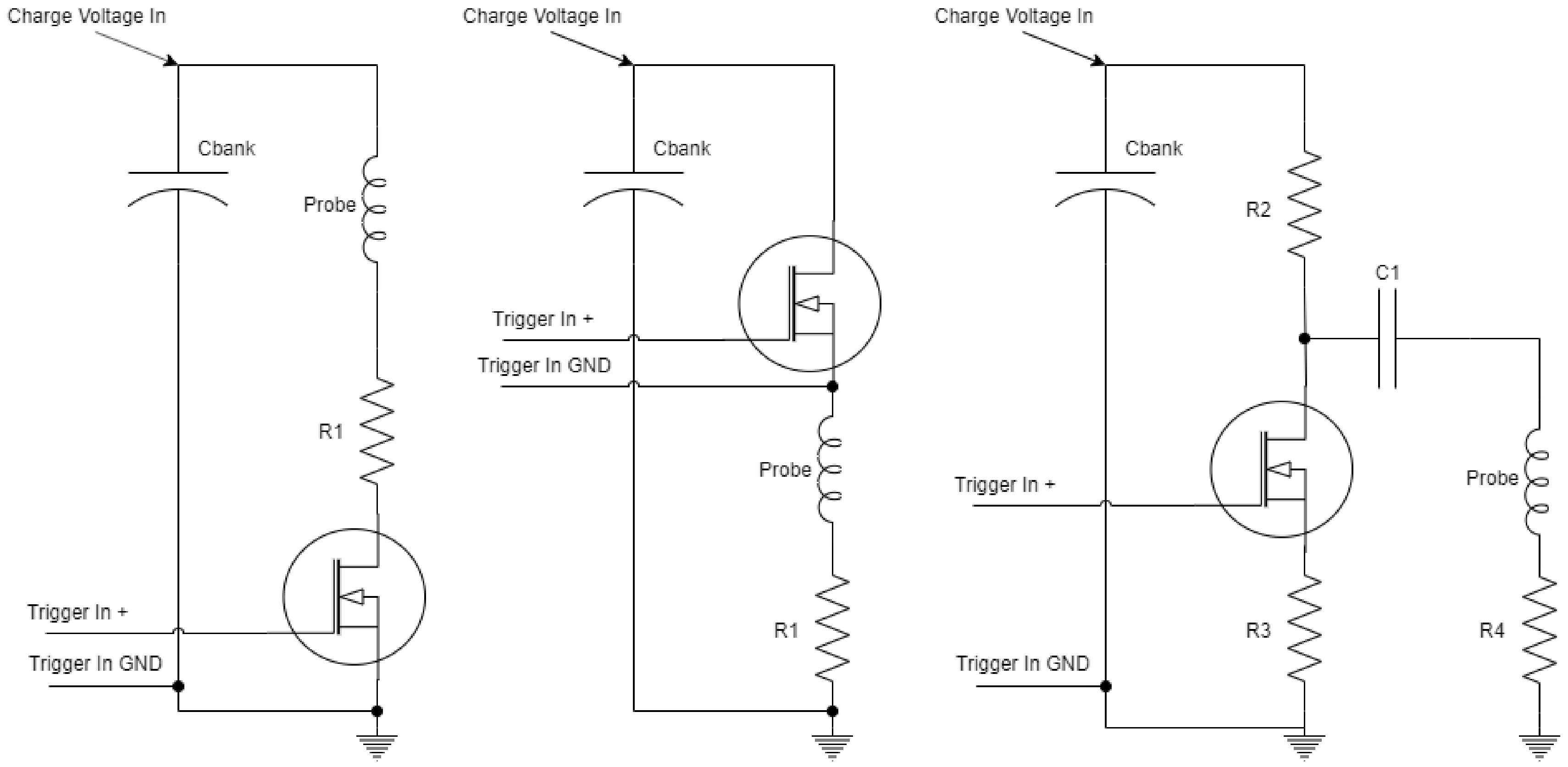
EMFI Tooling



EMFI Architectures

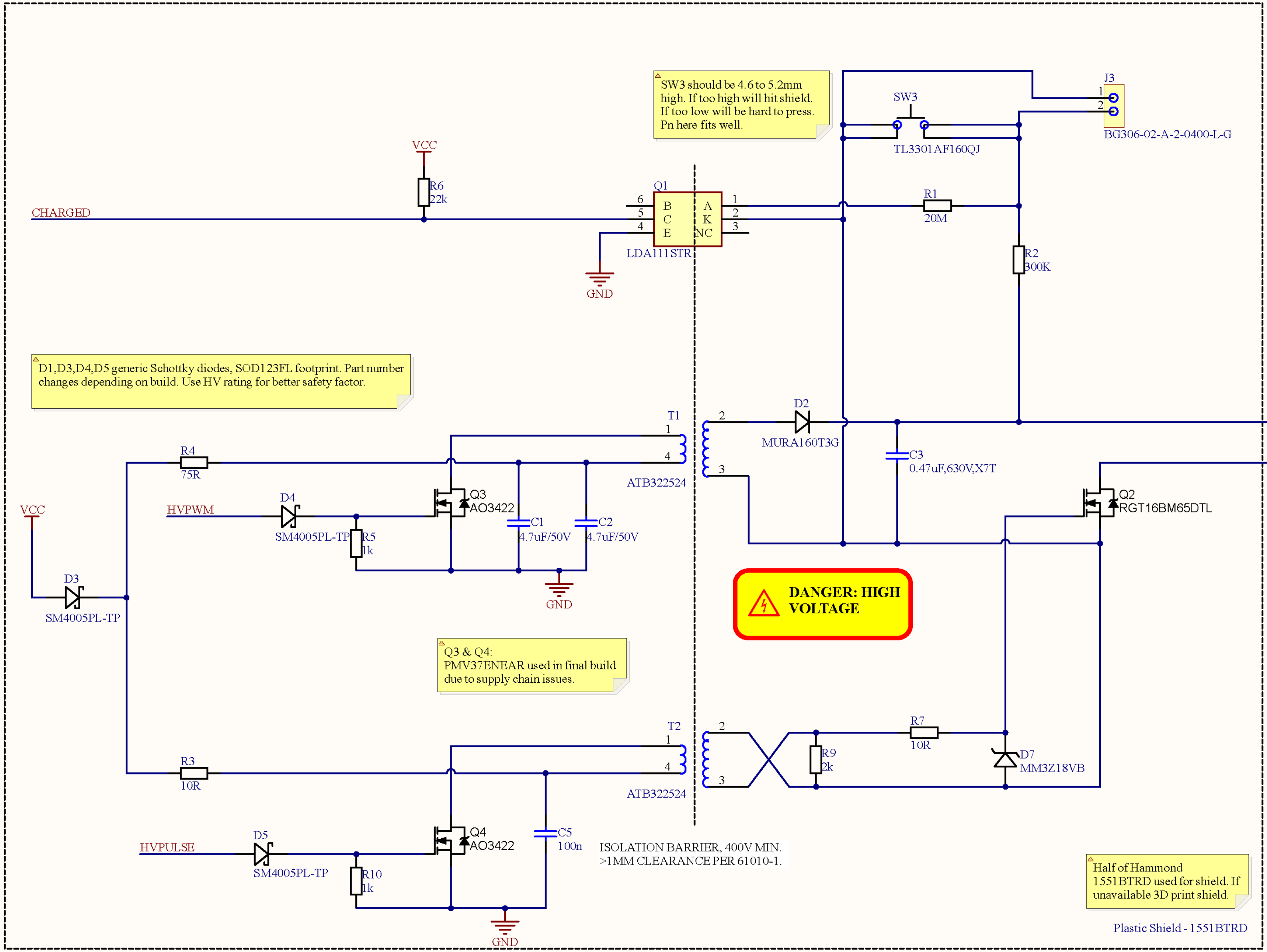
Direct Drive EMFI

Coupled Drive EMFI



Low-Side Switching

High-Side Switching



SW3 should be 4.6 to 5.2mm high. If too high will hit shield. If too low will be hard to press. Pn here fits well.

D1,D3,D4,D5 generic Schottky diodes, SOD123FL footprint. Part number changes depending on build. Use HV rating for better safety factor.

DANGER: HIGH VOLTAGE

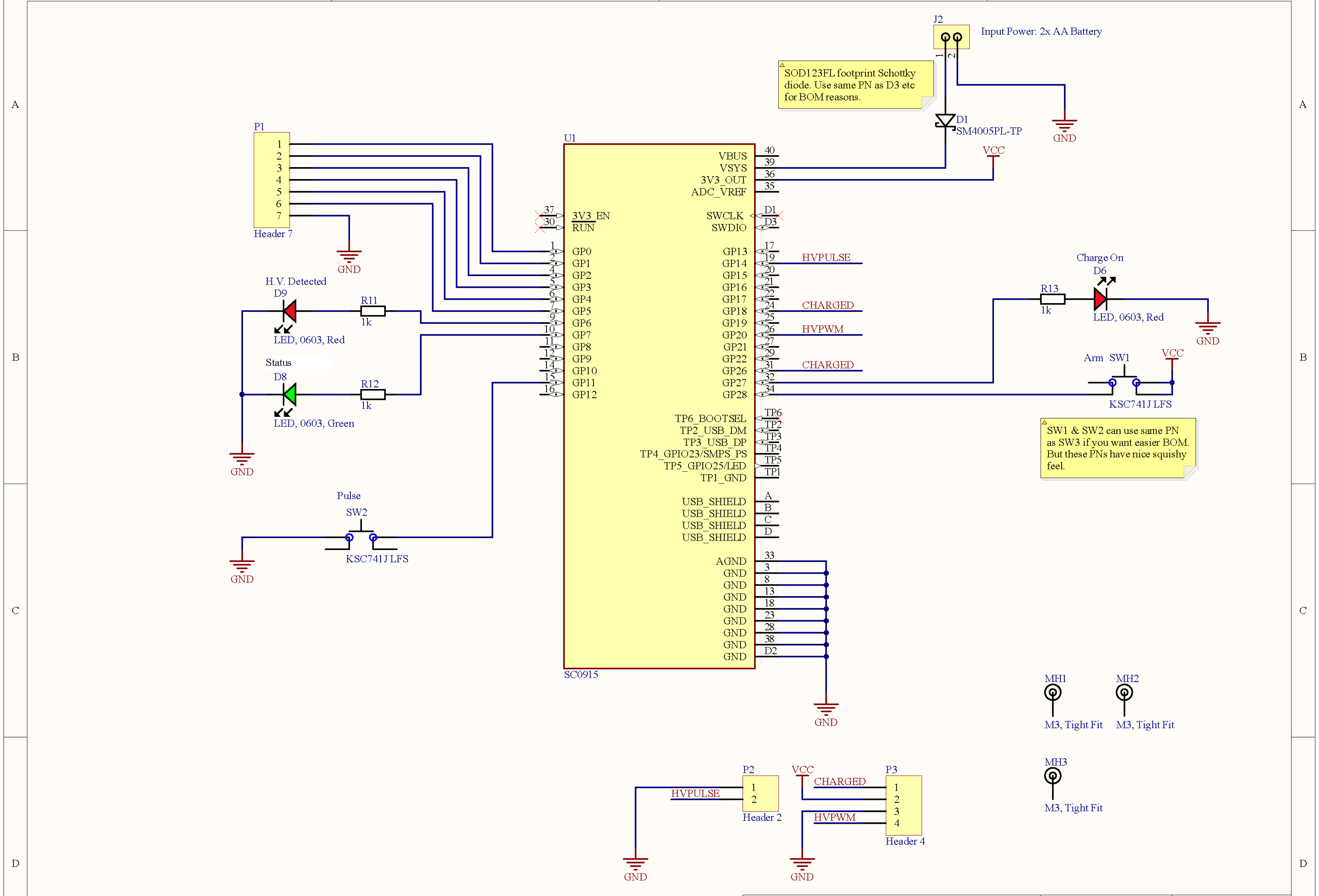
Q3 & Q4:
PMV37ENEAR used in final build due to supply chain issues.

ISOLATION BARRIER, 400V MIN.
>1MM CLEARANCE PER 61010-1.

Half of Hammond 1551BTRD used for shield. If unavailable 3D print shield.

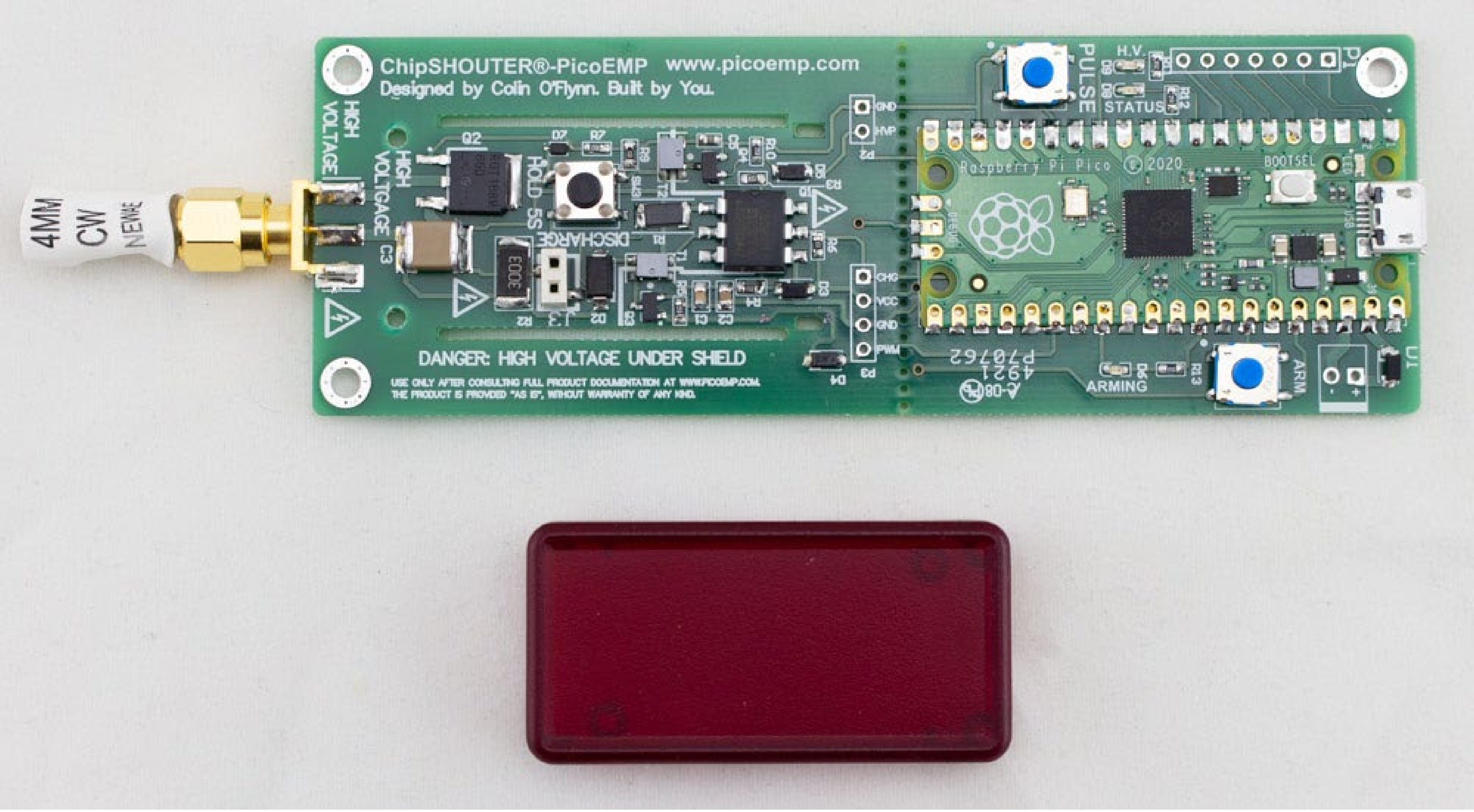
Plastic Shield - 1551BTRD

Title: **High Voltage Circuitry**		Approved: YES	
Rev: 04	Project: PicoEMP .	License: CC BY-SA 3.0	
Date: 2021-12-16 Time: 8:53:16 PM	Sheet 1 of 2	Copyright © NewAE Technology Inc.	NewAE.com
File: chipshouter-pico-hv.SchDoc		Copyright (C) Colin O'Flynn, 2021	

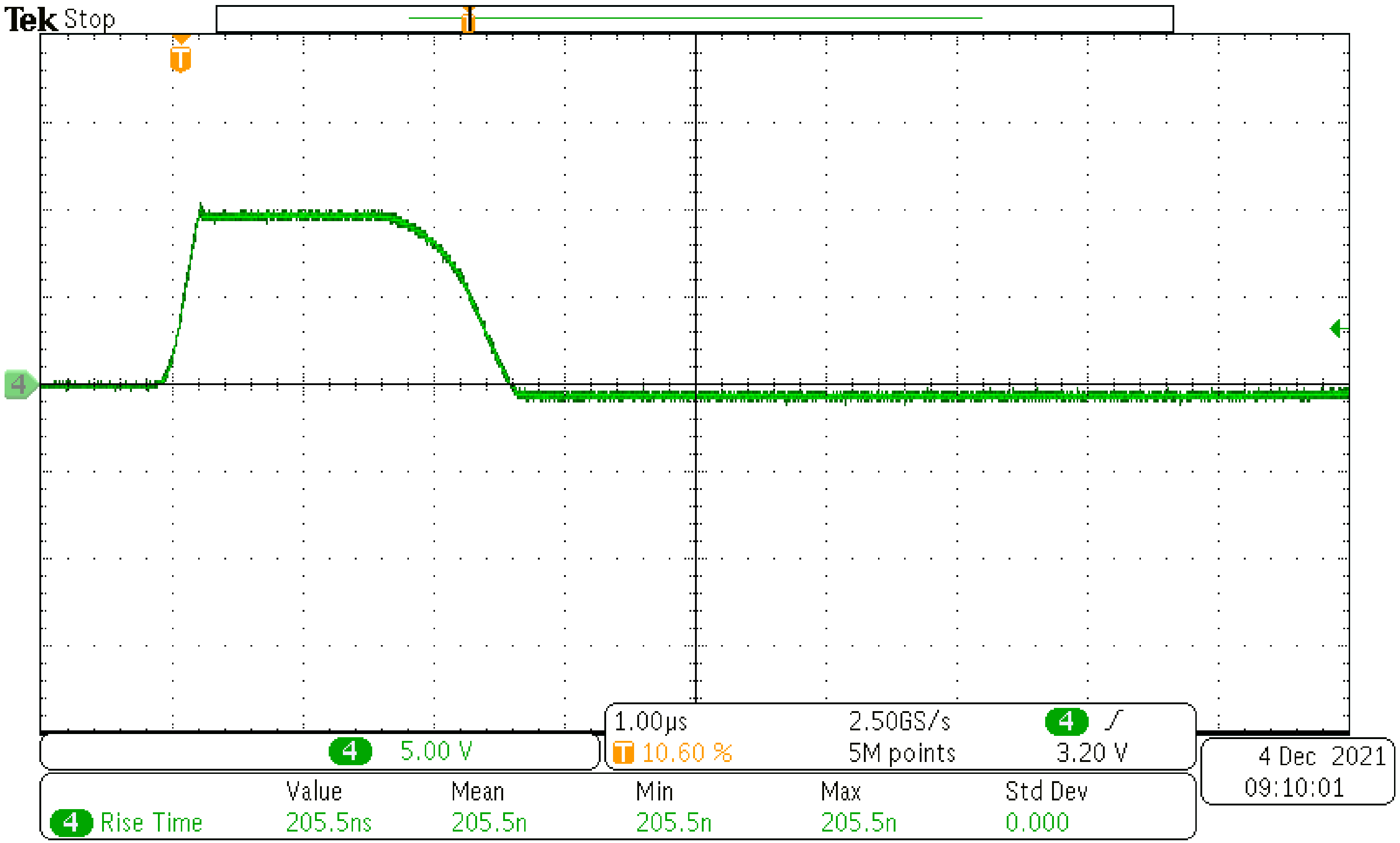


Title: **RP2040 Microcontroller**		Approved: YES	NewAE Technology
Rev: 04	Prqject: PicoEMP .	License: CC BY-SA 3.0	
Date: 2021-12-16	Time: 8:53:16 PM Sheet 2 of 2	Copyright © NewAE Technology Inc.	NewAE.com
File: chipshouter-pico-mcu.SchDoc		Copyright (C) Colin O'Flynn, 2021	

Implementation

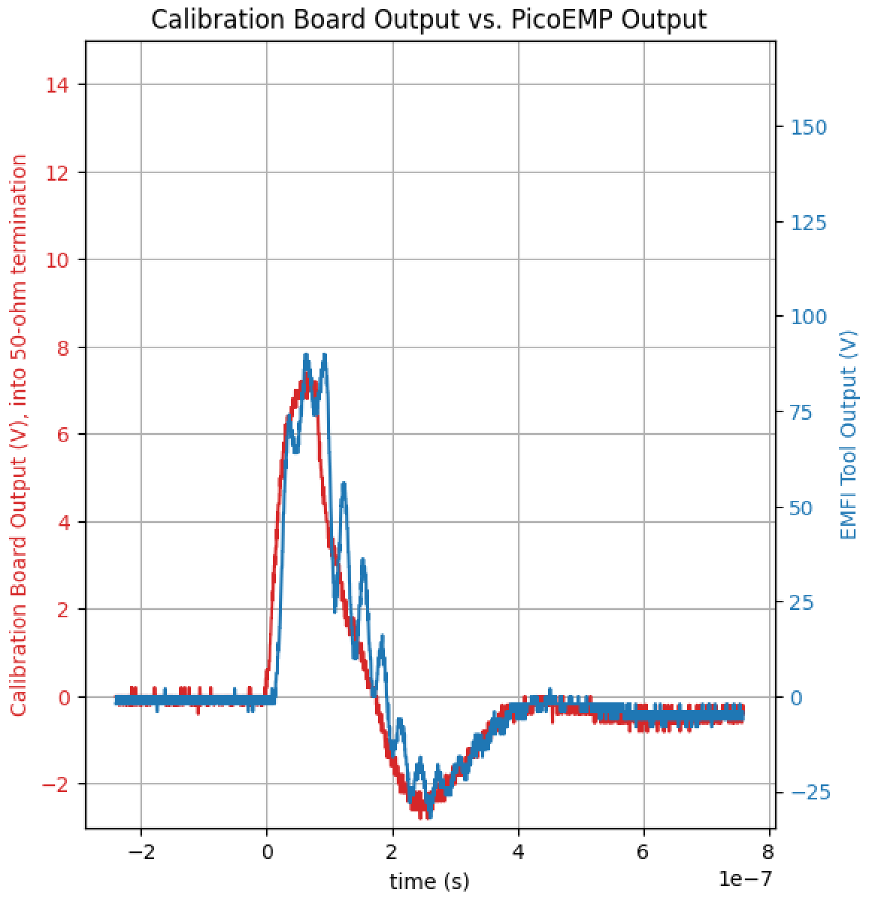

ChipSHOUTER®-PicoEMP www.picoemp.com
Designed by Colin O'Flynn. Built by You.
HIGH VOLTAGE
HOLD 5S
DISCHARGE
PULSE
H.V.
STATUS
Raspberry Pi Pico © 2020
BOOTSEL
DANGER: HIGH VOLTAGE UNDER SHIELD
USE ONLY AFTER CONSULTING FULL PRODUCT DOCUMENTATION AT WWW.PICOEMP.COM.
THE PRODUCT IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND.
ARMING
ARM
4MM
CW
NEW

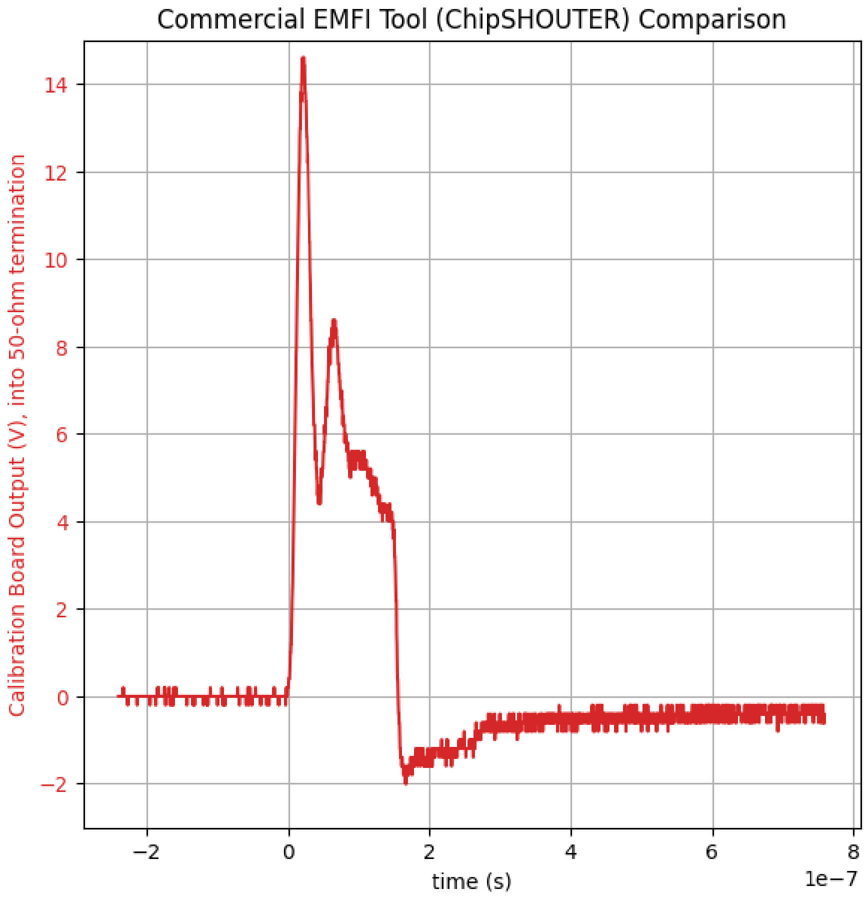
Gate Drive Waveform



	Value	Mean	Min	Max	Std Dev
4 Rise Time	205.5ns	205.5n	205.5n	205.5n	0.000

Pulse Comparison





Pi on Pi Violence

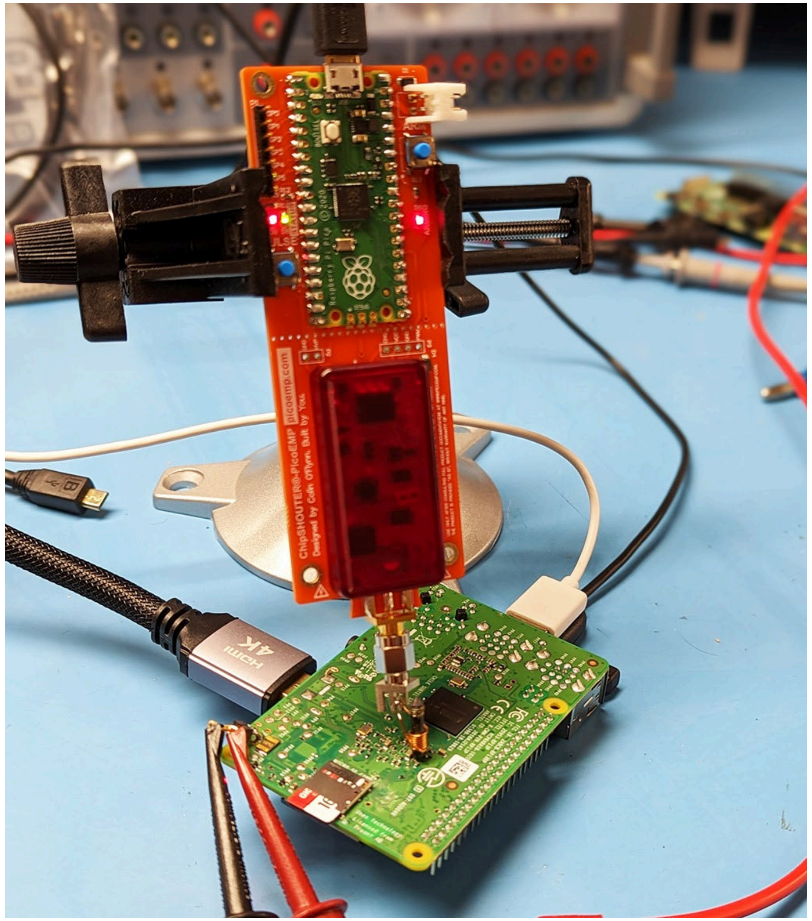
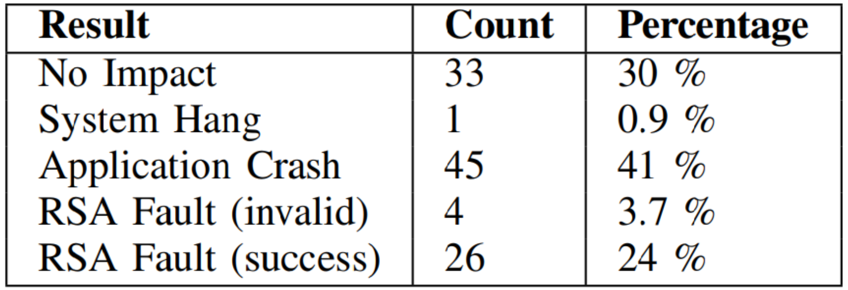
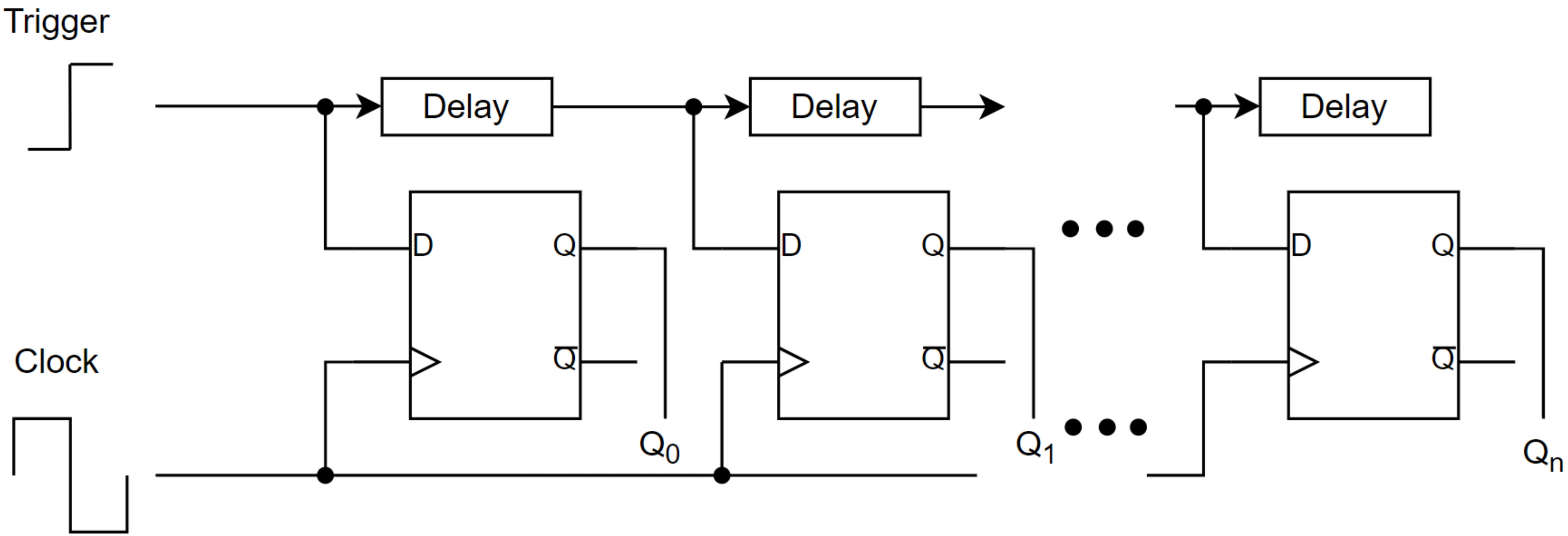


Table I: Results of RSA Fault Attack on Raspberry Pi 3B+

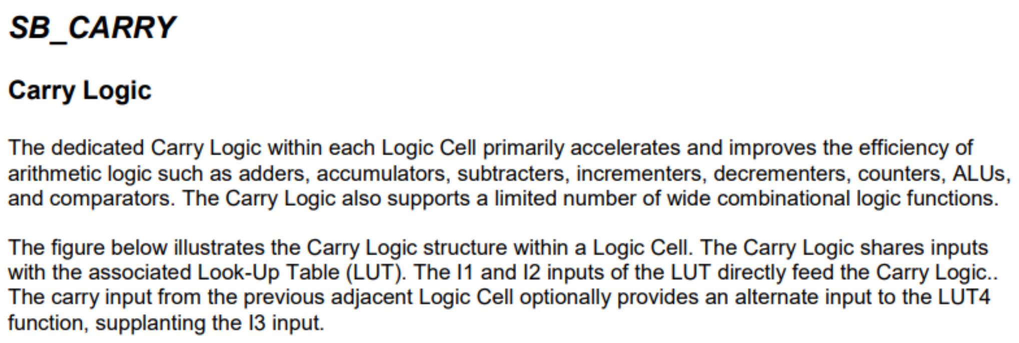


Result	**Count**	**Percentage**
No Impact	33	30 %
System Hang	1	0.9 %
Application Crash	45	41 %
RSA Fault (invalid)	4	3.7 %
RSA Fault (success)	26	24 %

Time to Digital Converter (TDC)



TDC on iCE40



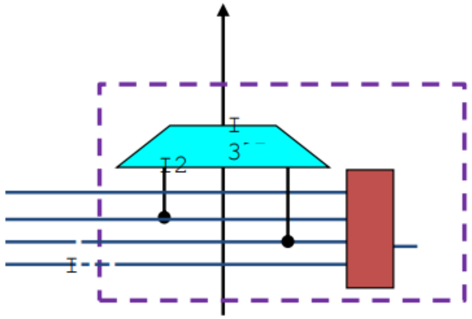
SB_CARRY

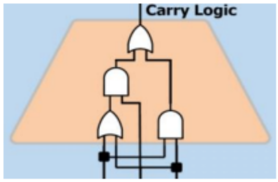
Carry Logic

The dedicated Carry Logic within each Logic Cell primarily accelerates and improves the efficiency of arithmetic logic such as adders, accumulators, subtracters, incrementers, decrementers, counters, ALUs, and comparators. The Carry Logic also supports a limited number of wide combinational logic functions.

The figure below illustrates the Carry Logic structure within a Logic Cell. The Carry Logic shares inputs with the associated Look-Up Table (LUT). The I1 and I2 inputs of the LUT directly feed the Carry Logic.. The carry input from the previous adjacent Logic Cell optionally provides an alternate input to the LUT4 function, supplanting the I3 input.

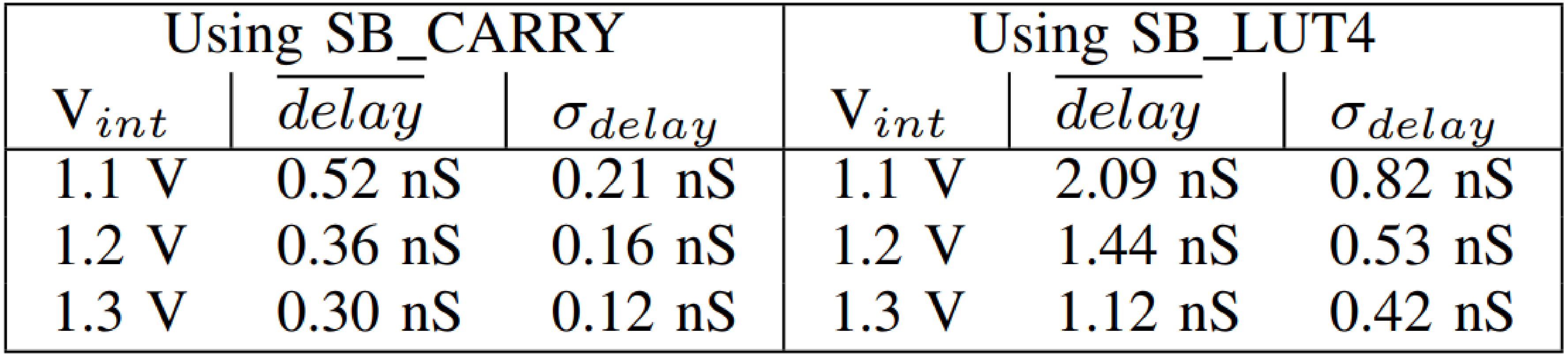
Carry Logic Structure within a Logic Cell





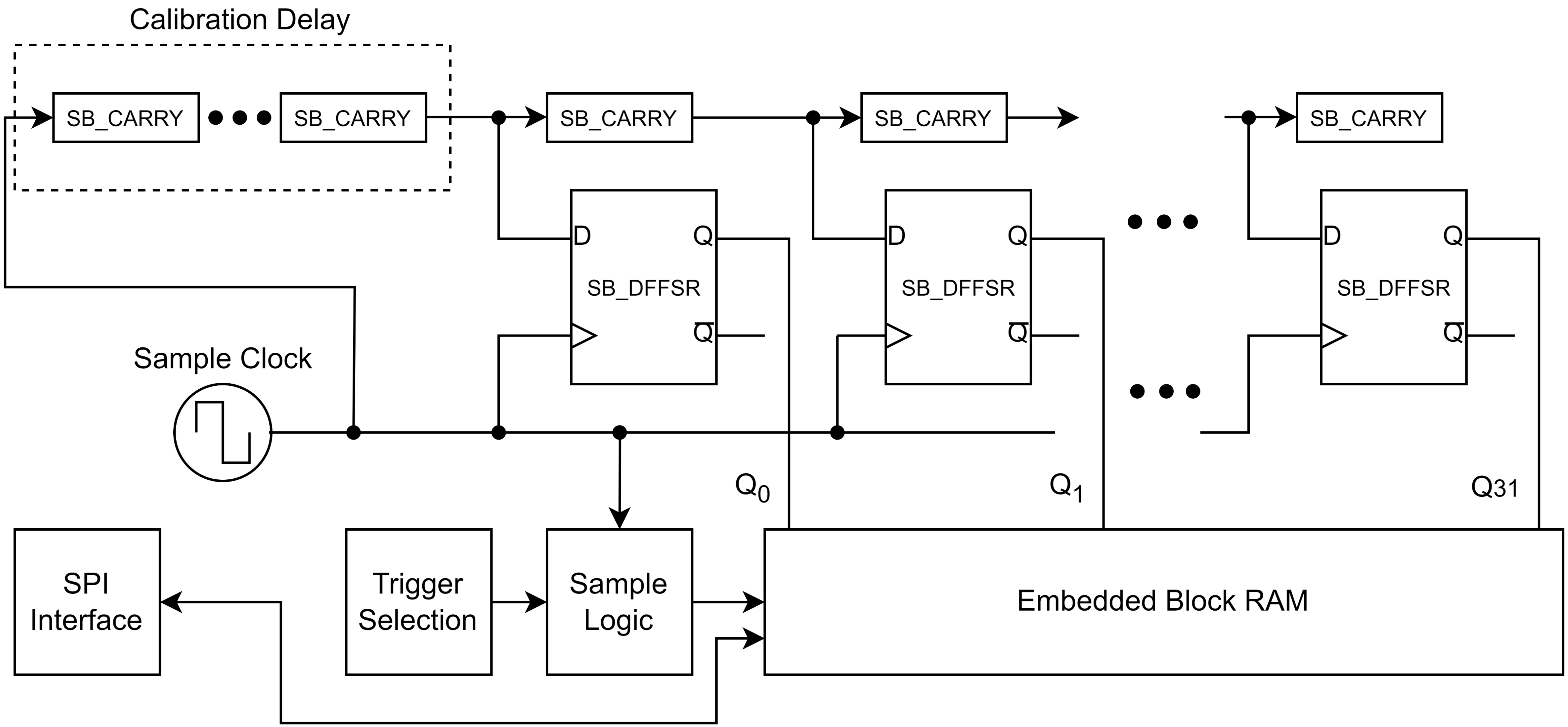
Delay Element Sensitivity

Table II: iCE40 Delay Element Measurements



Using SB_CARRY			Using SB_LUT4		
V_{int}	$\overline{delay}$	σ_{delay}	V_{int}	$\overline{delay}$	σ_{delay}
1.1 V	0.52 nS	0.21 nS	1.1 V	2.09 nS	0.82 nS
1.2 V	0.36 nS	0.16 nS	1.2 V	1.44 nS	0.53 nS
1.3 V	0.30 nS	0.12 nS	1.3 V	1.12 nS	0.42 nS

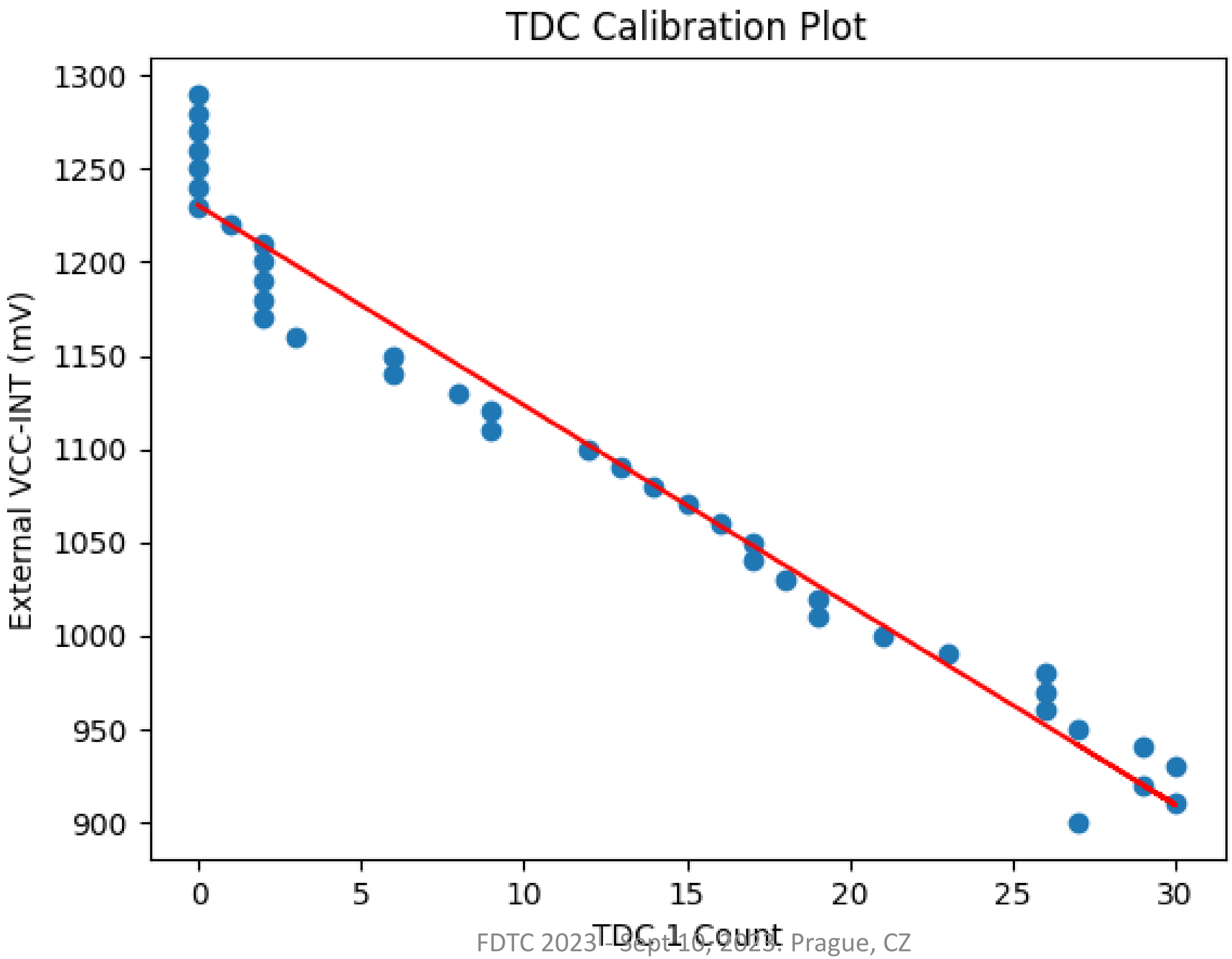
TDC on ICE40


Calibration Delay
SB_CARRY
SB_CARRY
SB_CARRY
SB_CARRY
SB_CARRY
D
Q
SB_DFFSR
Q̅
D
Q
SB_DFFSR
Q̅
D
Q
SB_DFFSR
Q̅
Sample Clock
Q_0
Q_1
Q31
SPI Interface
Trigger Selection
Sample Logic
Embedded Block RAM

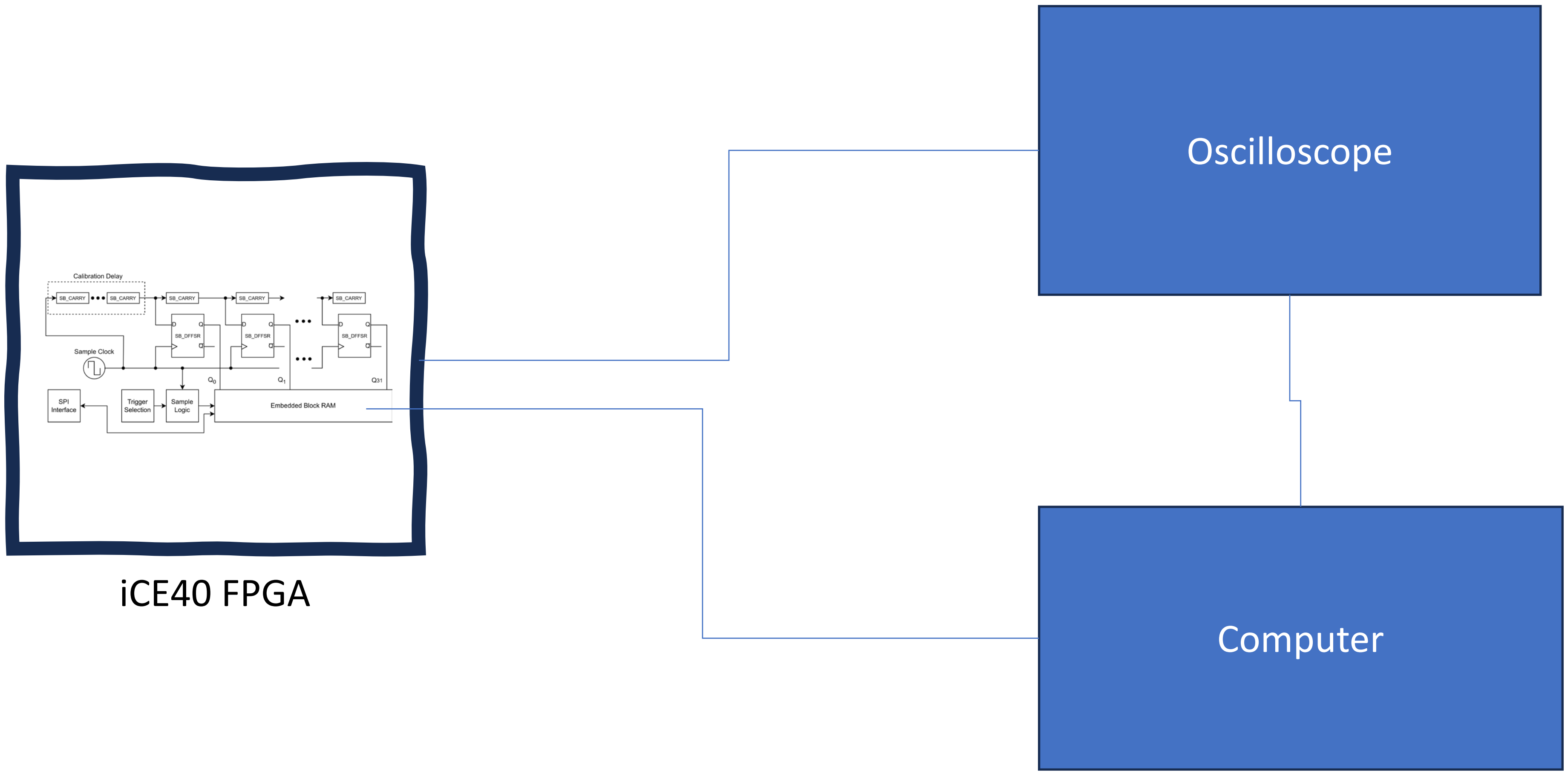
Rebuilding TDC

- Can rebuild the TDC in seconds thanks to Yosys!
- Allows modification of the delay elements without needing tricky (and glitchable) state machine.

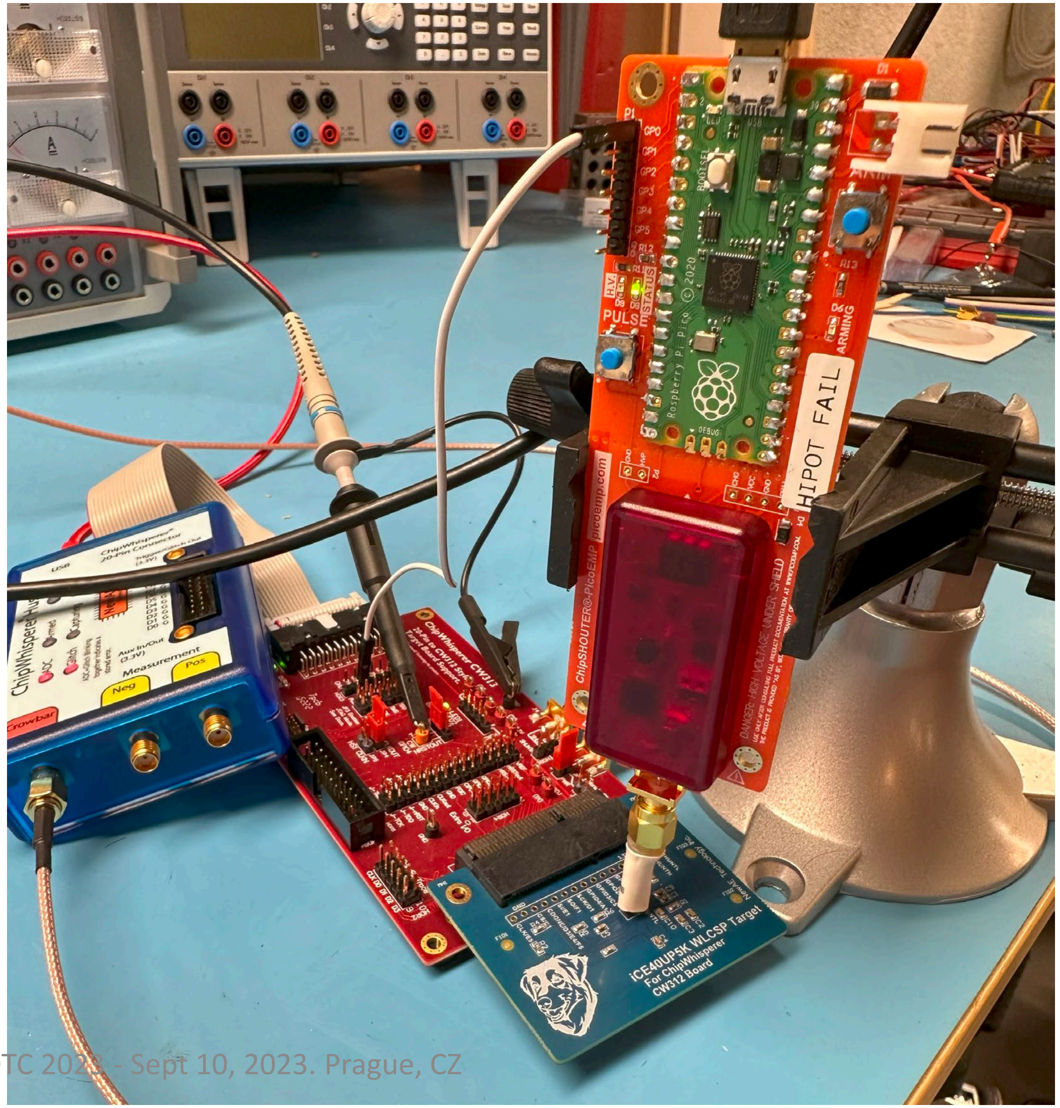
TDC Results - Calibration



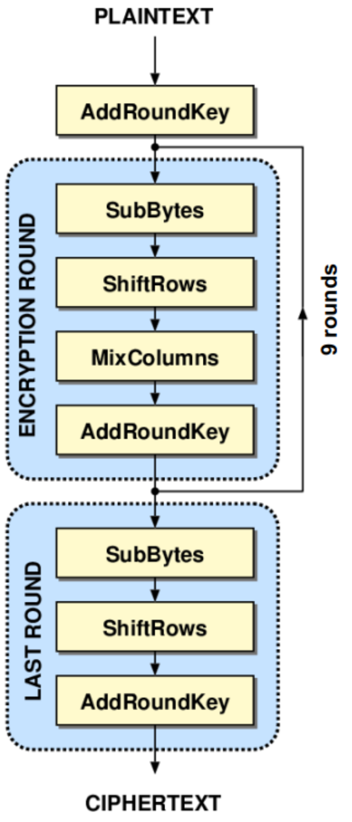
Internal & External Voltage Measurements



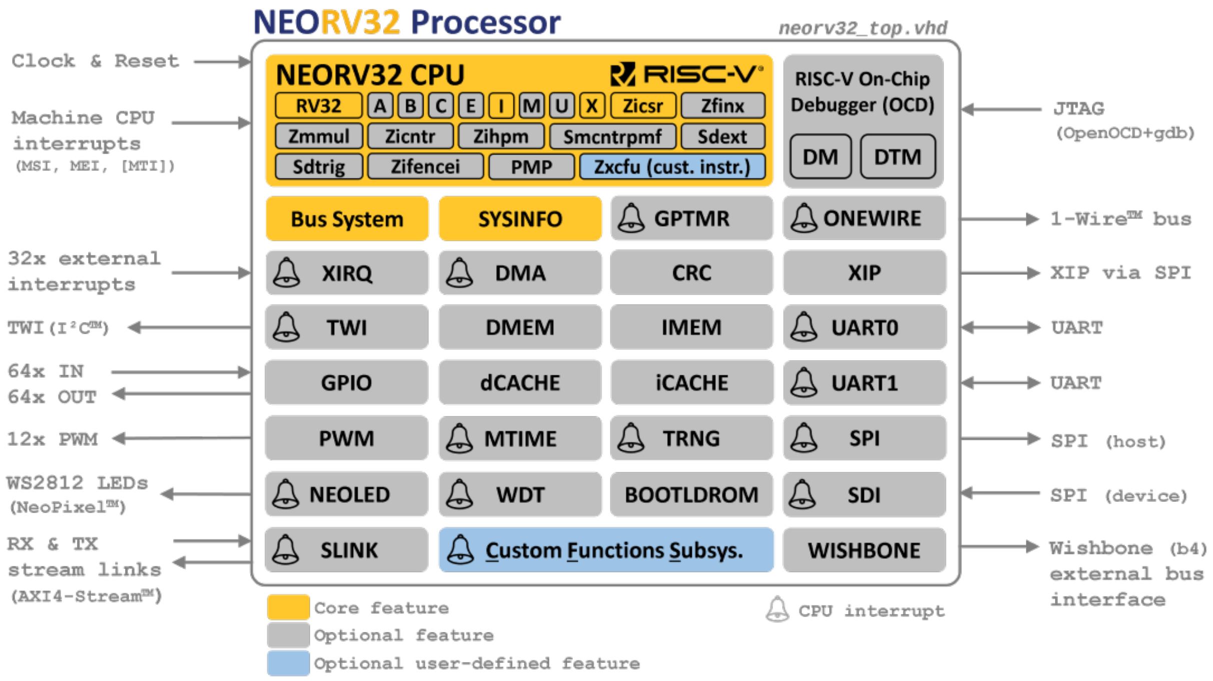
TDC / PicoEMP Measurement Setup



Practical Tests

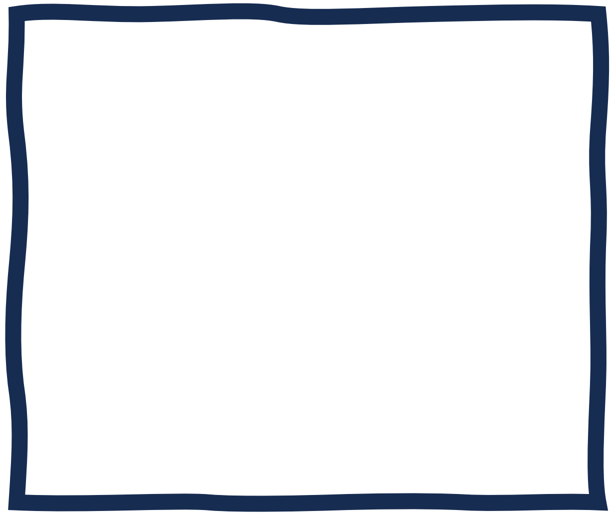


Hardware AES



RISC-V Soft-Core, Loop Test

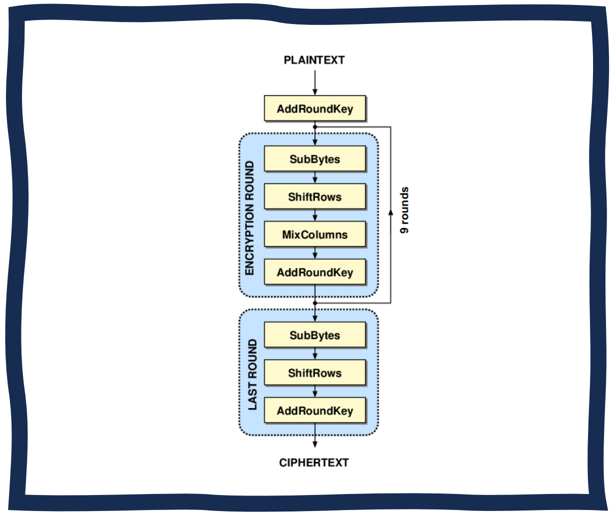
Internal Measurement of Practical Tests



iCE40 FPGA

- The TDC is reloaded and measurement taken after finding an “effective” glitch setting/location.
- Does not require *any* touching of the setup, so no movement occurs.
- Reloading happens <1 second

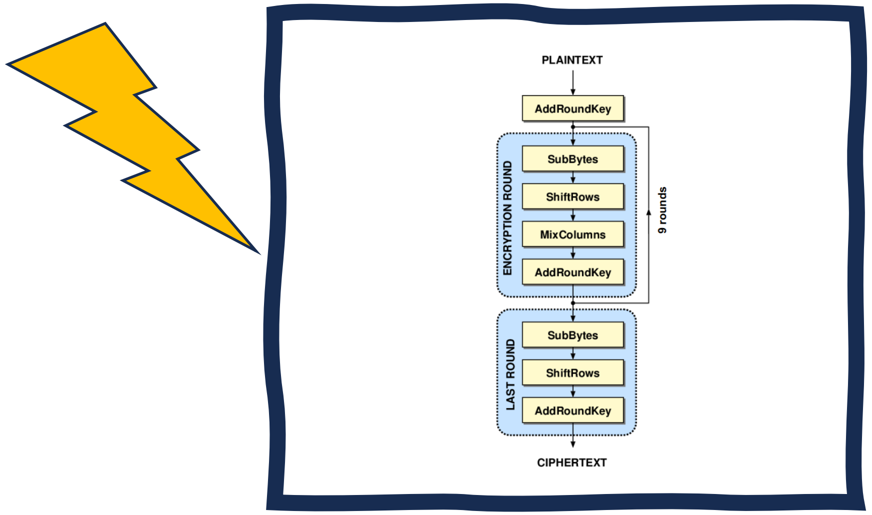
Internal Measurement of Practical Tests



iCE40 FPGA

- The TDC is reloaded and measurement taken after finding an “effective” glitch setting/location.
- Does not require *any* touching of the setup, so no movement occurs.
- Reloading happens <1 second

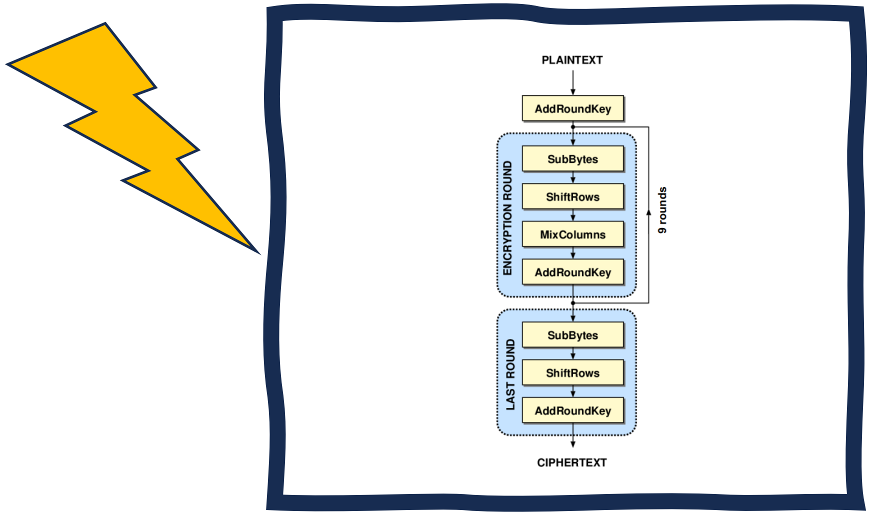
Internal Measurement of Practical Tests



iCE40 FPGA

- The TDC is reloaded and measurement taken after finding an “effective” glitch setting/location.
- Does not require *any* touching of the setup, so no movement occurs.
- Reloading happens <1 second

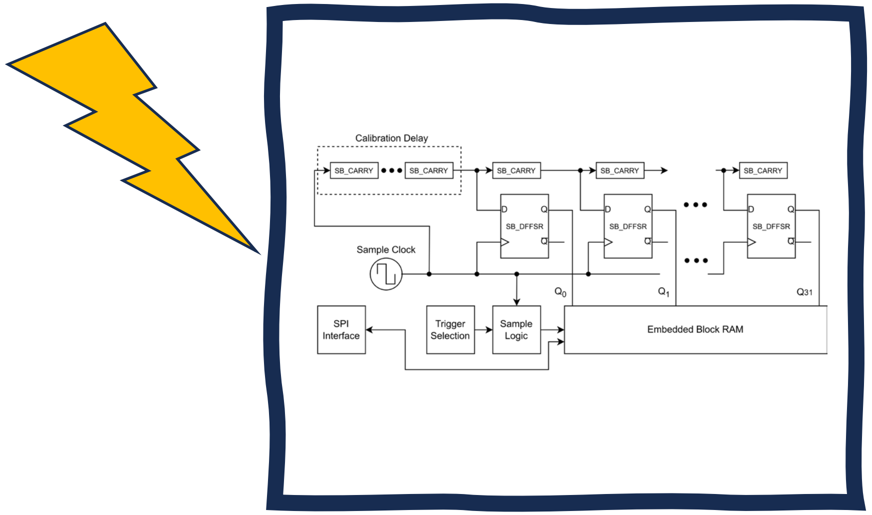
Internal Measurement of Practical Tests



iCE40 FPGA

- The TDC is reloaded and measurement taken after finding an “effective” glitch setting/location.
- Does not require *any* touching of the setup, so no movement occurs.
- Reloading happens <1 second

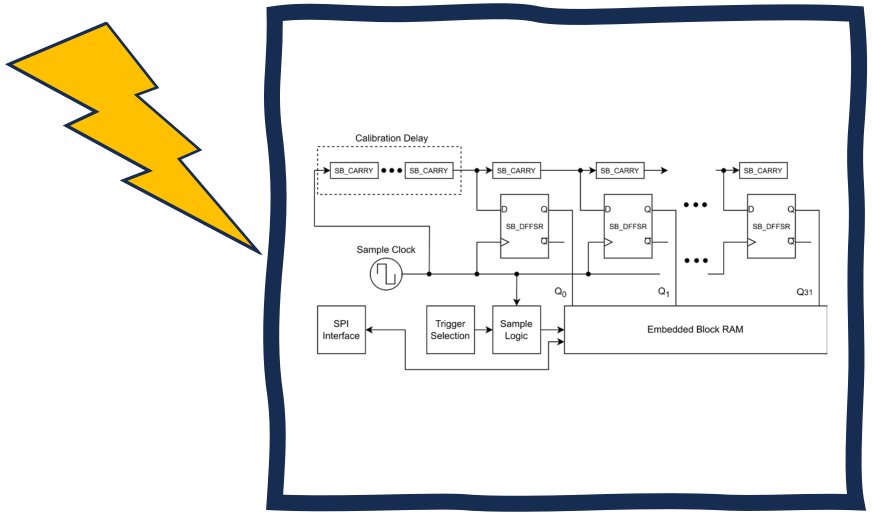
Internal Measurement of Practical Tests



iCE40 FPGA

- The TDC is reloaded and measurement taken after finding an “effective” glitch setting/location.
- Does not require *any* touching of the setup, so no movement occurs.
- Reloading happens <1 second

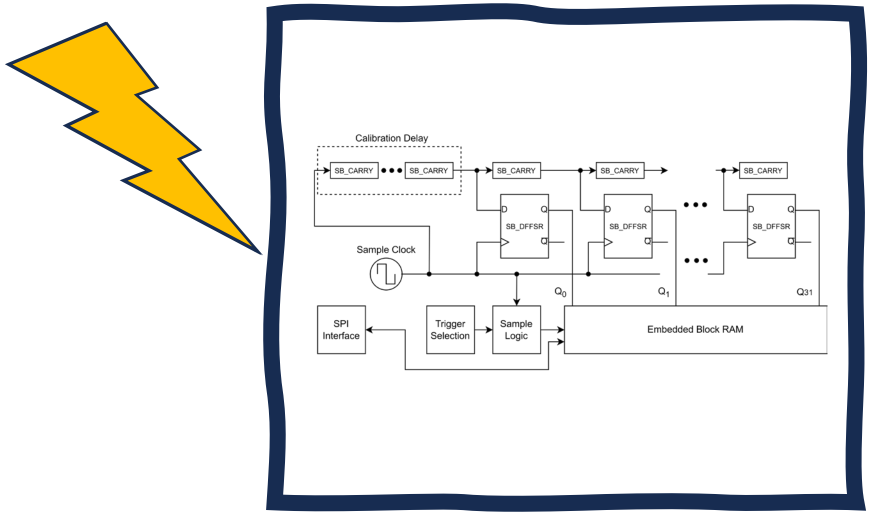
Internal Measurement of Practical Tests



iCE40 FPGA

- The TDC is reloaded and measurement taken after finding an “effective” glitch setting/location.
- Does not require *any* touching of the setup, so no movement occurs.
- Reloading happens <1 second

Internal Measurement of Practical Tests



iCE40 FPGA

- The TDC is reloaded and measurement taken after finding an “effective” glitch setting/location.
- Does not require *any* touching of the setup, so no movement occurs.
- Reloading happens <1 second

Hardware AES

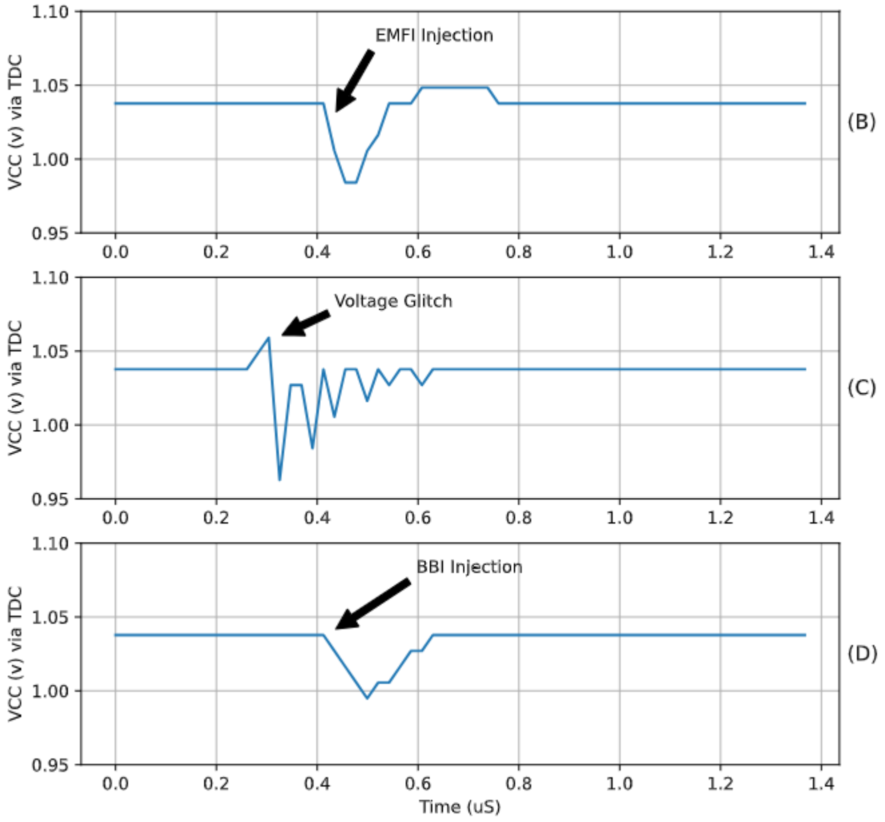


Figure 13: Measurements of the VCC-INT power rail using TDC during hardware AES operations.

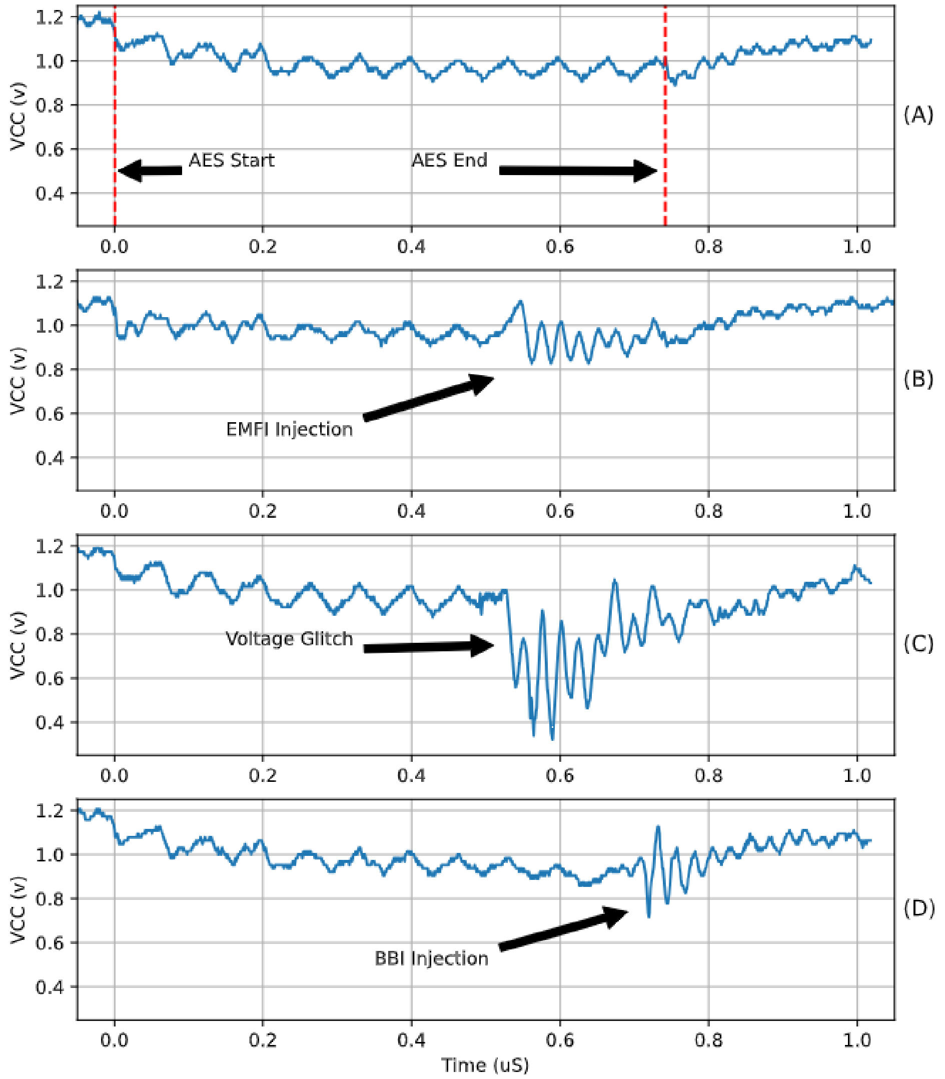


Figure 12: Measurements of the VCC-INT power rail using external oscilloscope during hardware AES operations.

RISC-V Core

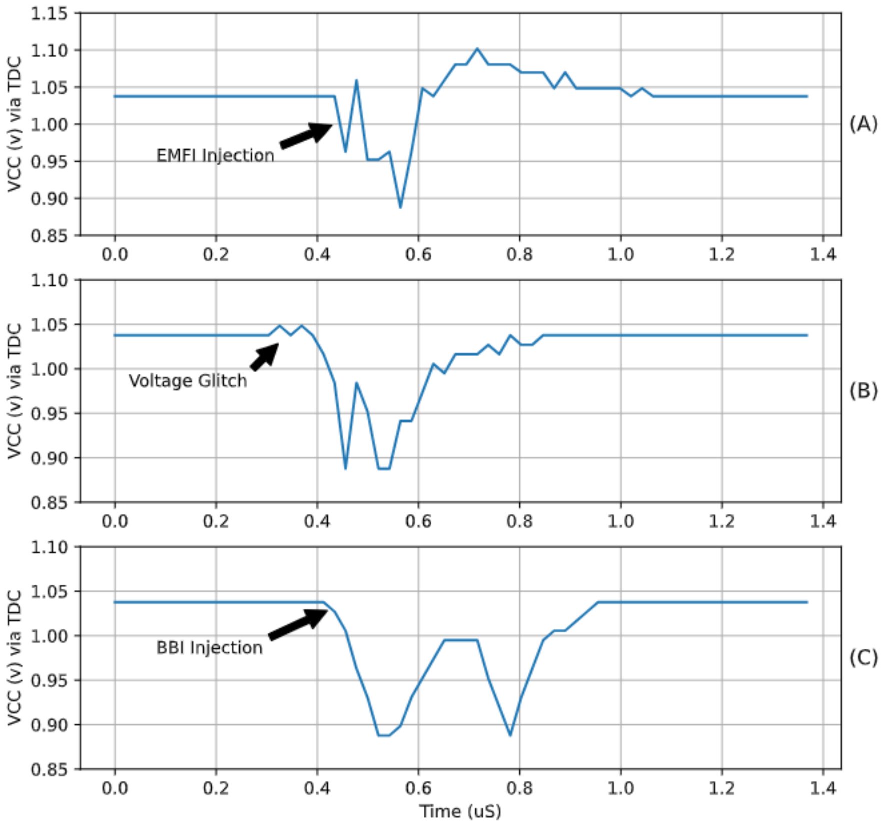


Figure 15: Measurements of the VCC-INT power rail using TDC during RISC-V soft-core operation.

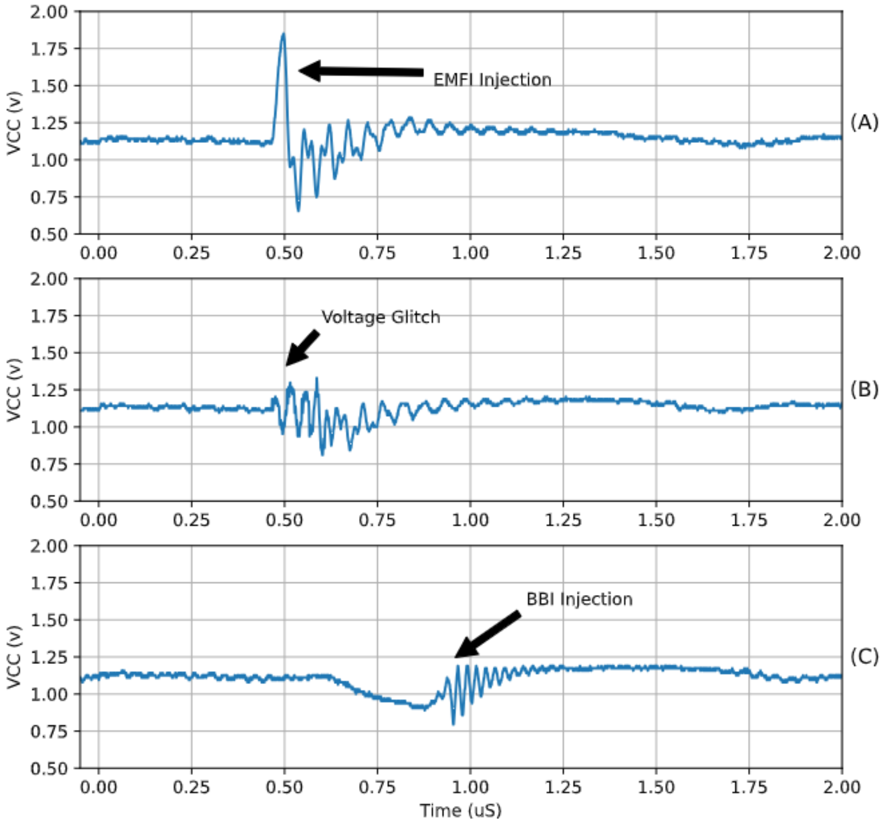
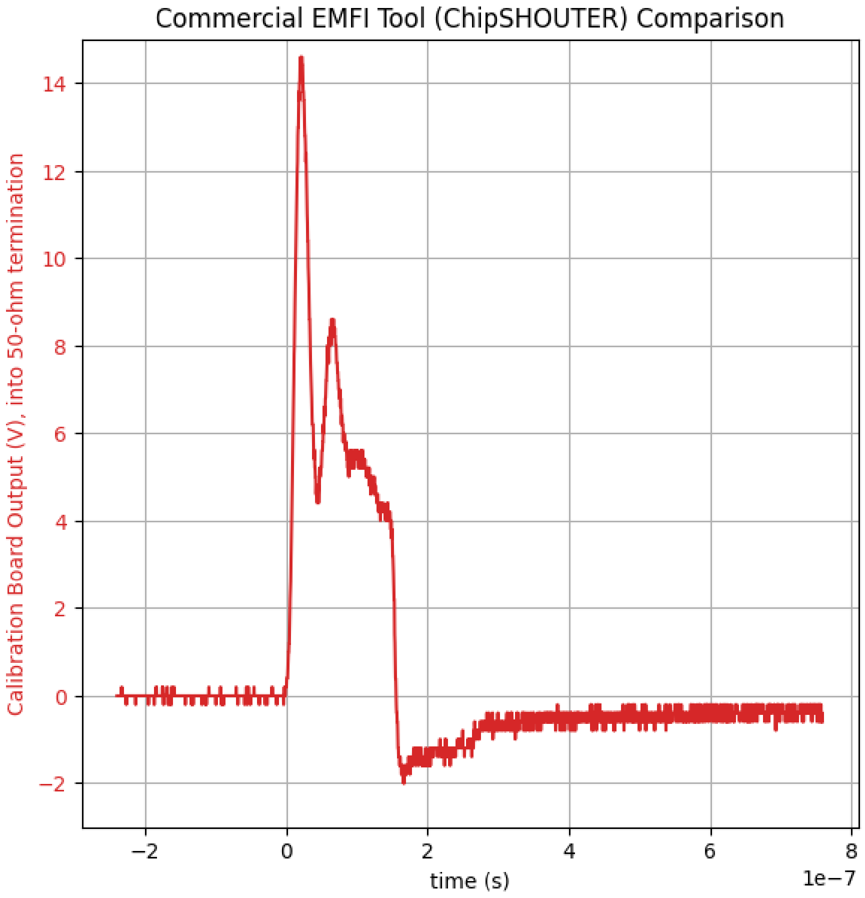
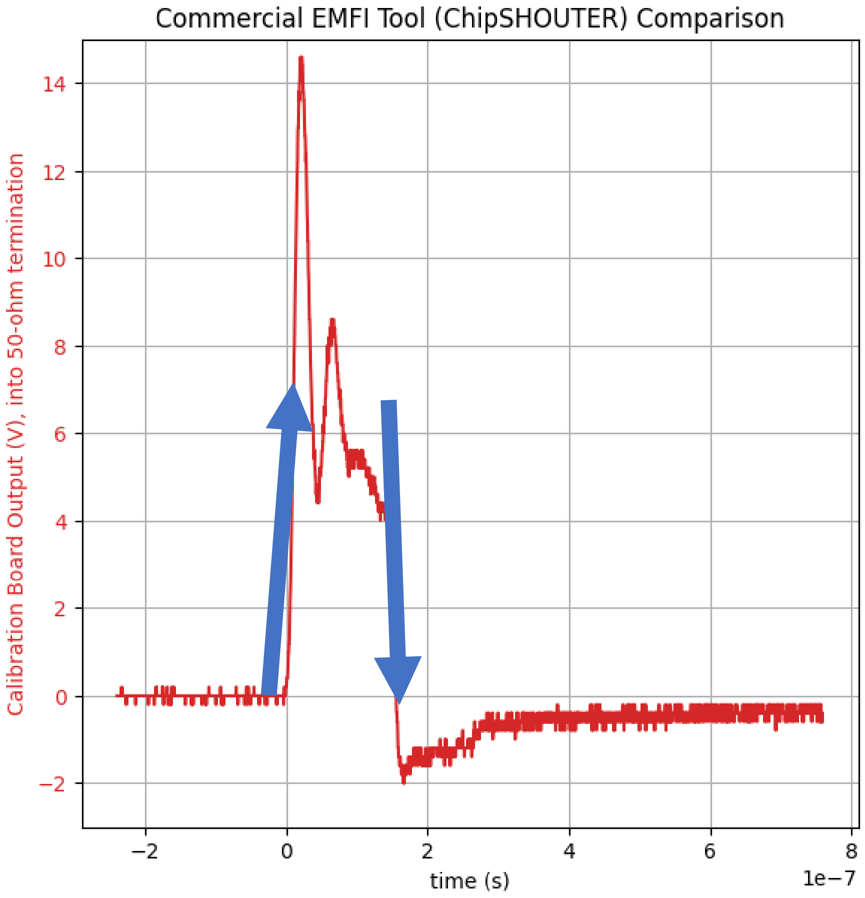


Figure 14: Measurements of the VCC-INT power rail using external oscilloscope during RISC-V soft-core operation.

EMFI Width?


Commercial EMFI Tool (ChipSHOUTER) Comparison
Calibration Board Output (V), into 50-ohm termination
14
12
10
8
6
4
2
0
−2
−2
0
2
4
6
8
1e−7
time (s)

EMFI Width?


Commercial EMFI Tool (ChipSHOUTER) Comparison
Calibration Board Output (V), into 50-ohm termination
14
12
10
8
6
4
2
0
−2
−2
0
2
4
6
8
time (s)
1e−7

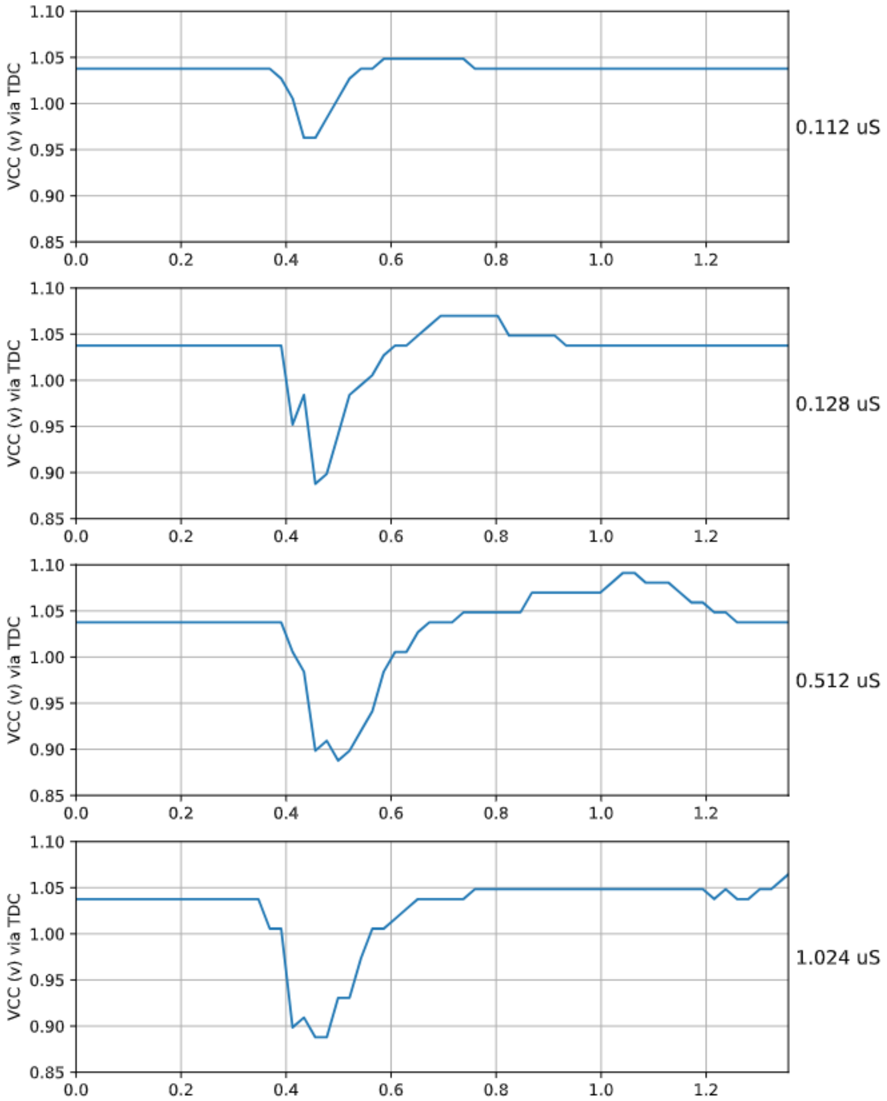


Figure 17: Comparison of EMFI Pulse Width, measured using TDC on VCC internally.

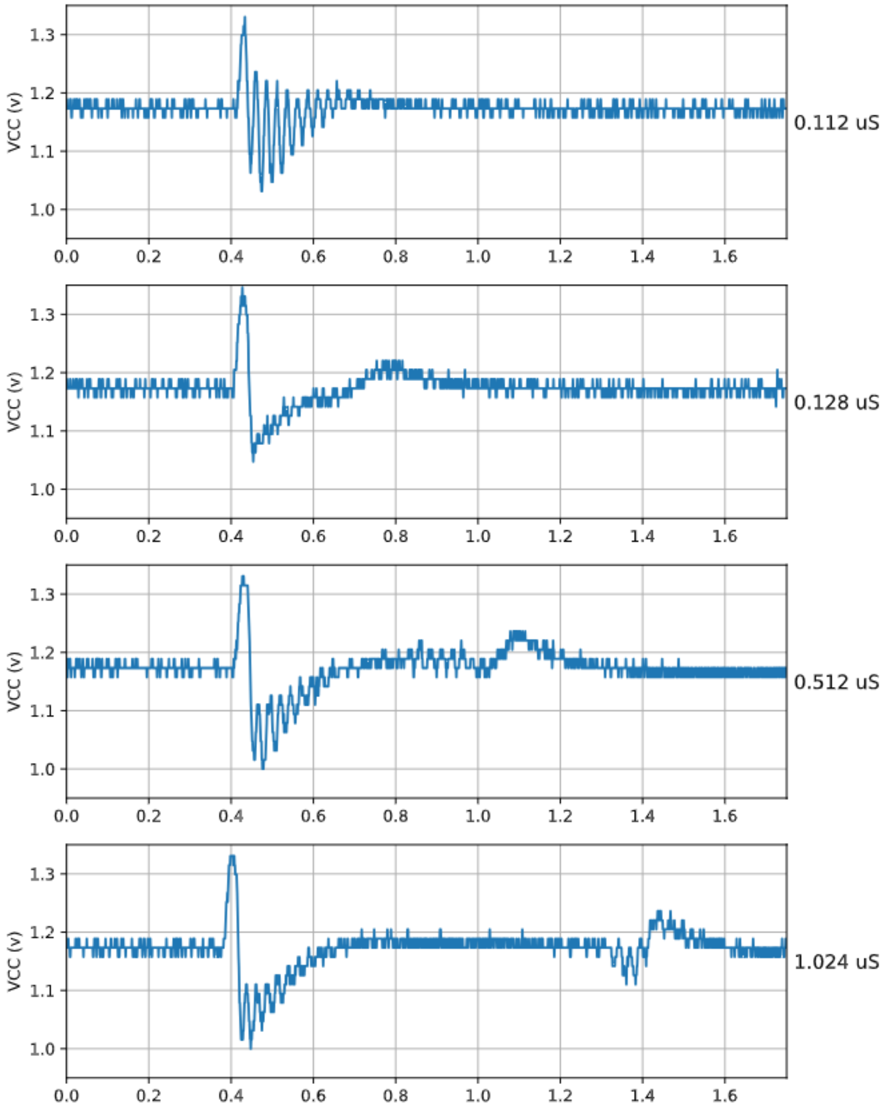


Figure 16: Comparison of EMFI Pulse Width, measured using oscilloscope on VCC externally.

Effective vs. Ineffective Glitches

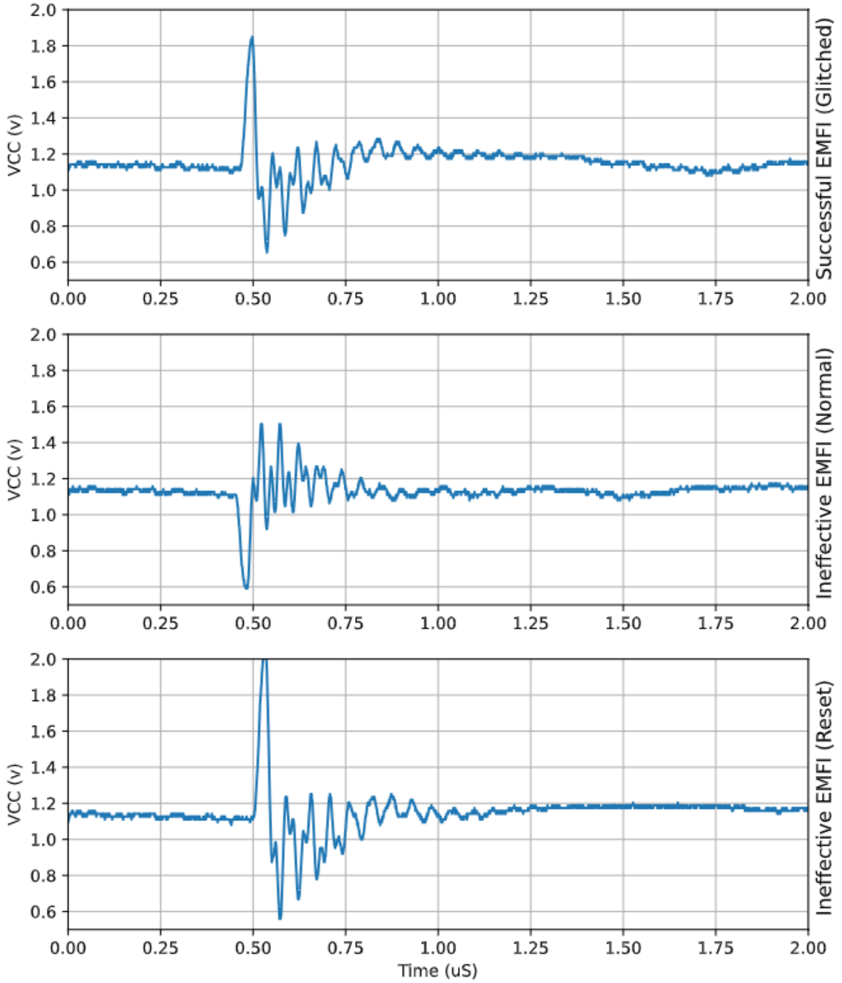


Figure 18: Comparison of EMFI pulses as measured on VCC-INT for effective & ineffective glitches.

Effective vs. Ineffective Glitches

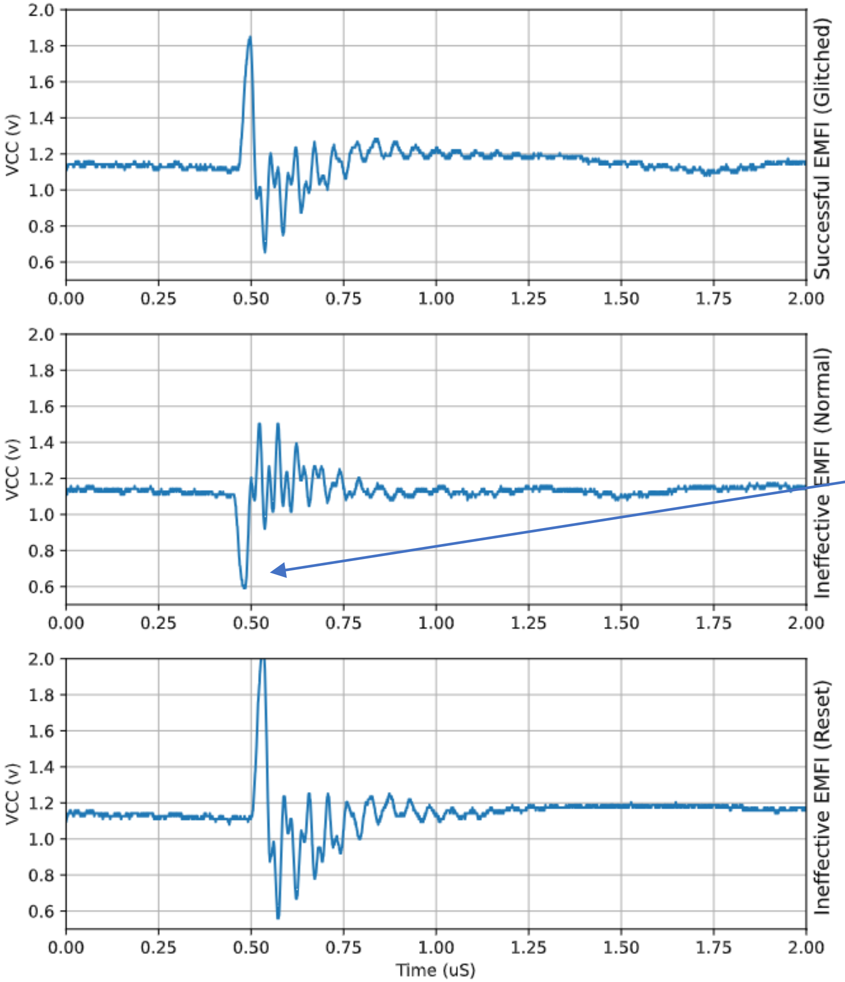
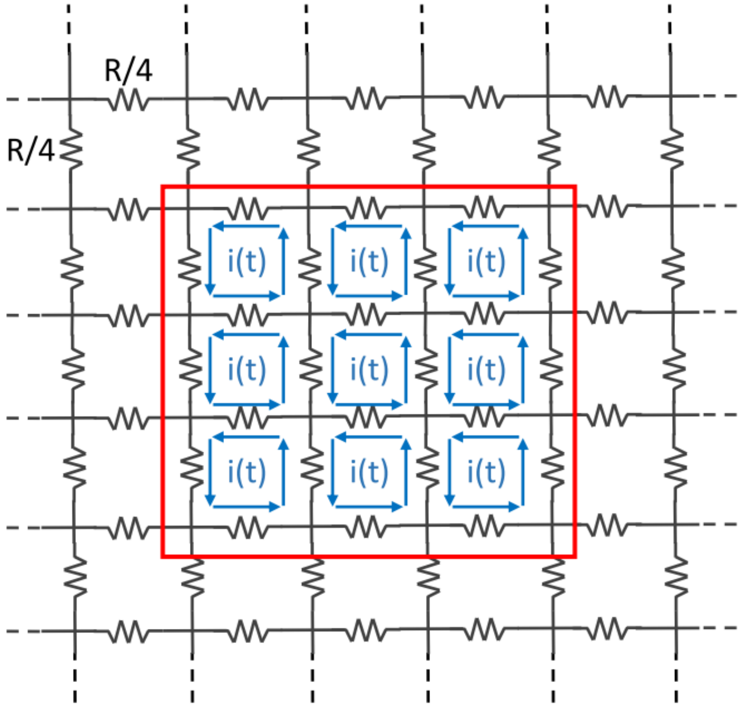


Figure 18: Comparison of EMFI pulses as measured on VCC-INT for effective & ineffective glitches.



M. Dumont; M. Lisart; P. Maurine. Modeling and Simulating Electromagnetic Fault Injection. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 2020

Conclusions & Questions

- PicoEMP is a low-cost EMFI tool, with a safety-focused design.
- TDC implemented in an iCE40 FPGA provides a useful calibration and exploration artifact.
- We can use this to demonstrate the link between EMFI, Voltage Glitching, and BBI.
- We can also link external power measurements with internal (TDC) measurements.

colin –AT– oflynn.com