Safety ≠ Security

A SECURITY EVALUATION OF STATE OF THE ART AUTOMOTIVE MICROCONTROLLERS

Nils Wiersma

May 10, 2017

Radboud University

Introduction

Topic

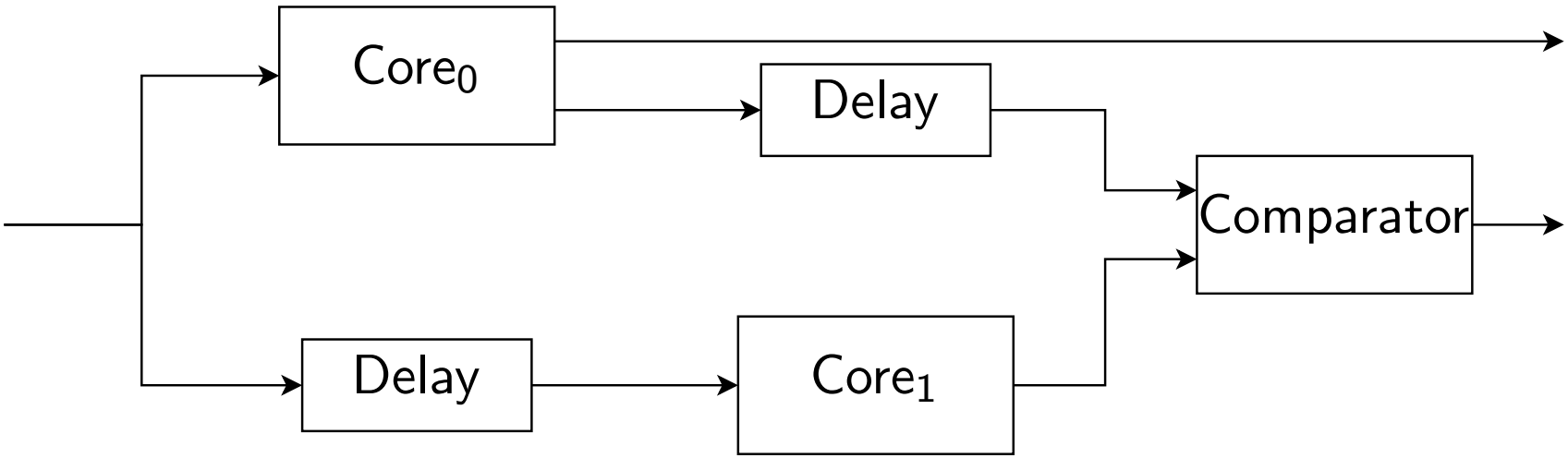
Investigate the security of modern microcontroller units,
used in the automotive industry,
by means of fault injection.

Why the automotive microcontrollers?

- Safety critical
- Fault tolerance
- ISO26262
- Safety mechanisms $\rightarrow$ countermeasures

Safety mechanisms / Countermeasures

Duplicate execution and compare (lockstep)



Safety mechanisms / Countermeasures

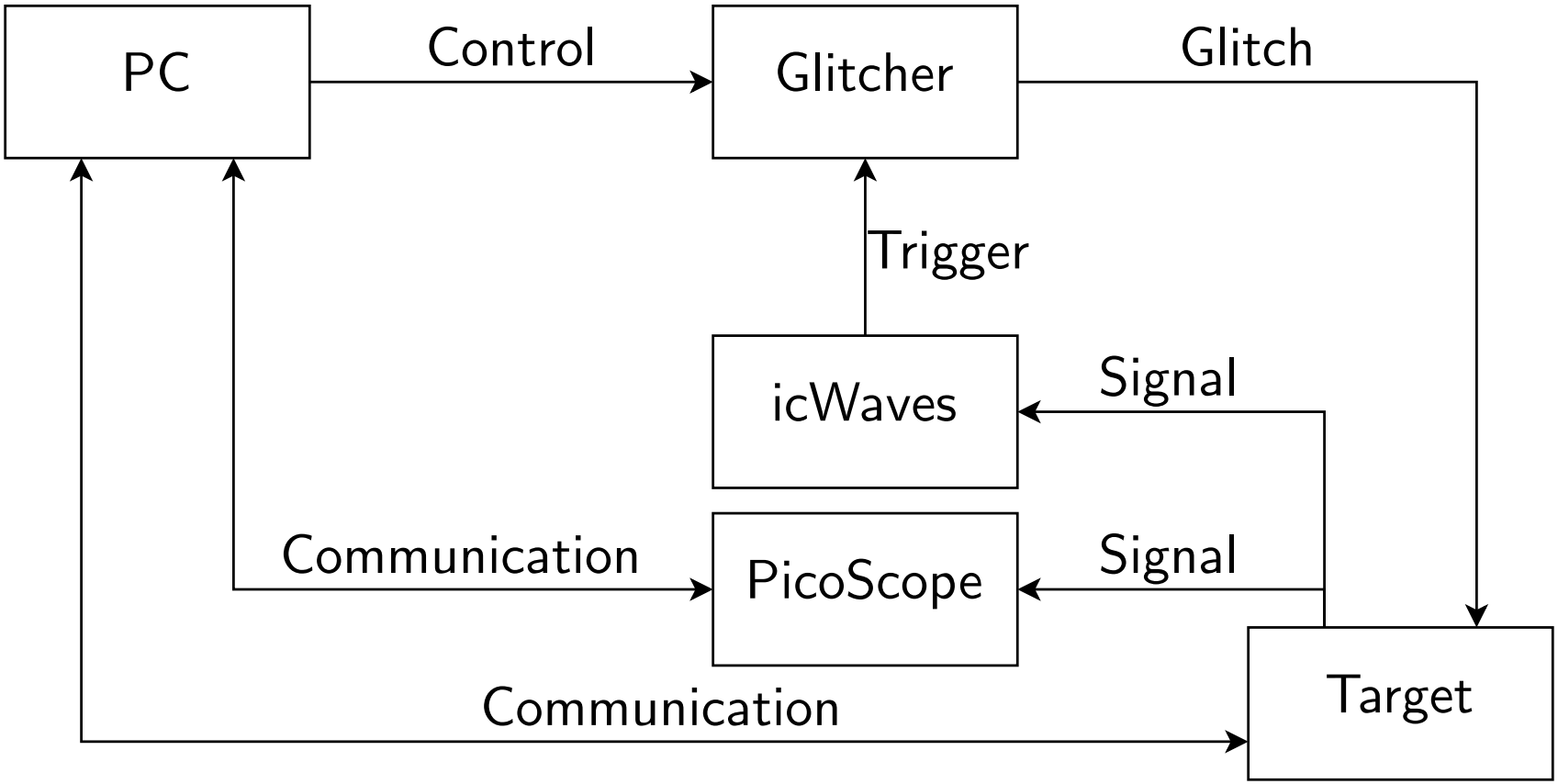
Memory

- Error correction and detection codes
- Memory duplication

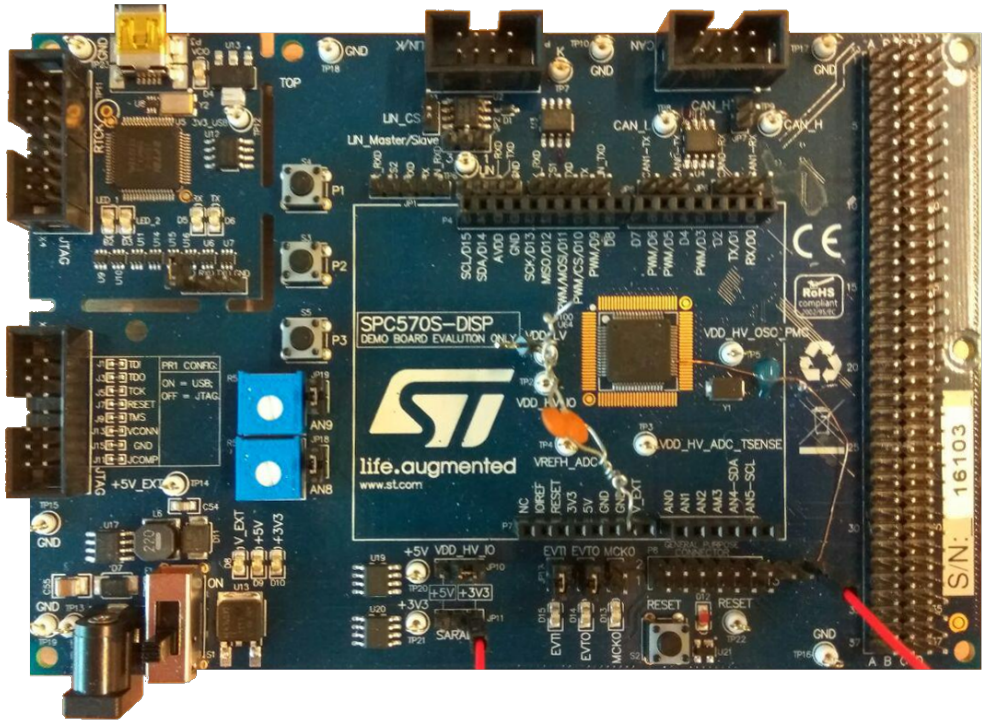
Techniques

- Power
- Electromagnetic

Setup


PC
Control
Glitcher
Glitch
Trigger
icWaves
Signal
Communication
PicoScope
Signal
Target
Communication

Targets

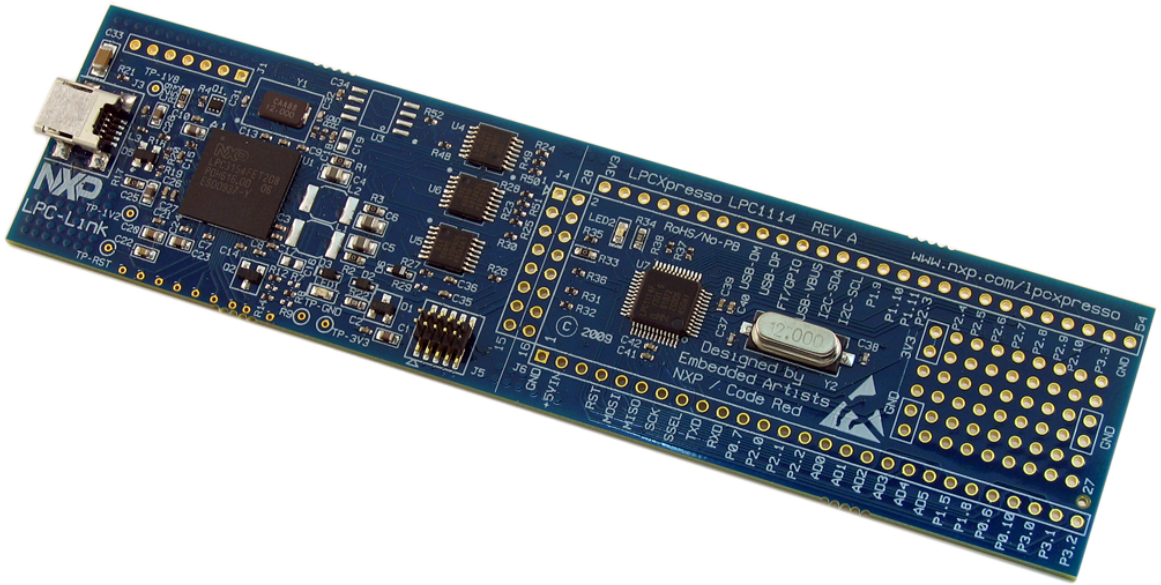


- e200z0h PowerPC 32bit by STMicroelectronics

Targets

- Cortex-R4F ARM 32bit by Texas Instruments

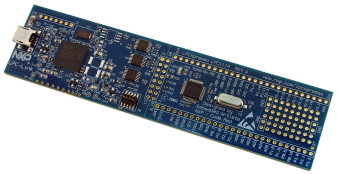
Targets

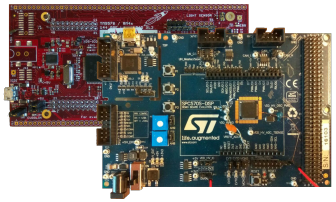


- Cortex-M0 ARM 32bit by NXP (no fancy countermeasures)

Targets

Assurance level Low → High





Category QM ASIL-A ASIL-B ASIL-C ASIL-D

Experiments

- Characterization of targets
- Unlocking debug interface (JTAG)

Characterization

Target firmware under complete control of the attacker

Nice trigger signals

- reduce variables to minimum

Nice output

- classify attempts
- investigate state after fault

Characterization

Experiment 1: unrolled loop of add instructions

```
trigger_high()

ADD r1 #1
ADD r1 #1
ADD r1 #1
ADD r1 #1
ADD r1 #1
ADD r1 #1

trigger_low()
serial_send(r1)
```

Characterization

Experiment 2: simple authentication check

```
flag = 1
trigger_high()

if (flag == 0):
 authenticated()
else:
 not_authenticated()

trigger_low()
```

Characterization

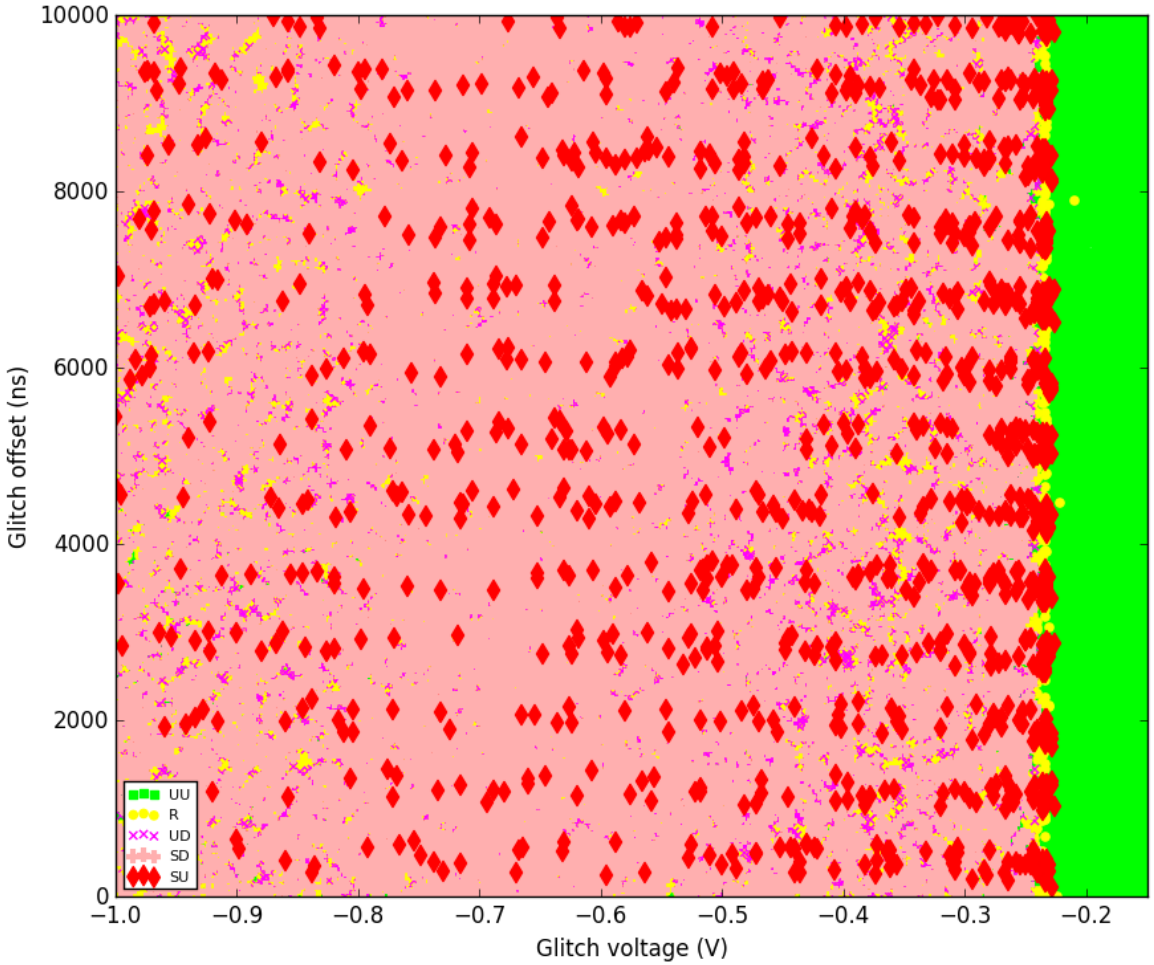
1. Investigate normal behavior through (side) channels
2. Determine rough ranges of values for different parameters
3. Determine fixed values for parameters that yield good results

Characterization

1. Investigate normal behavior through (side) channels
2. Determine rough ranges of values for different parameters
3. **Determine fixed values for parameters that yield good results**

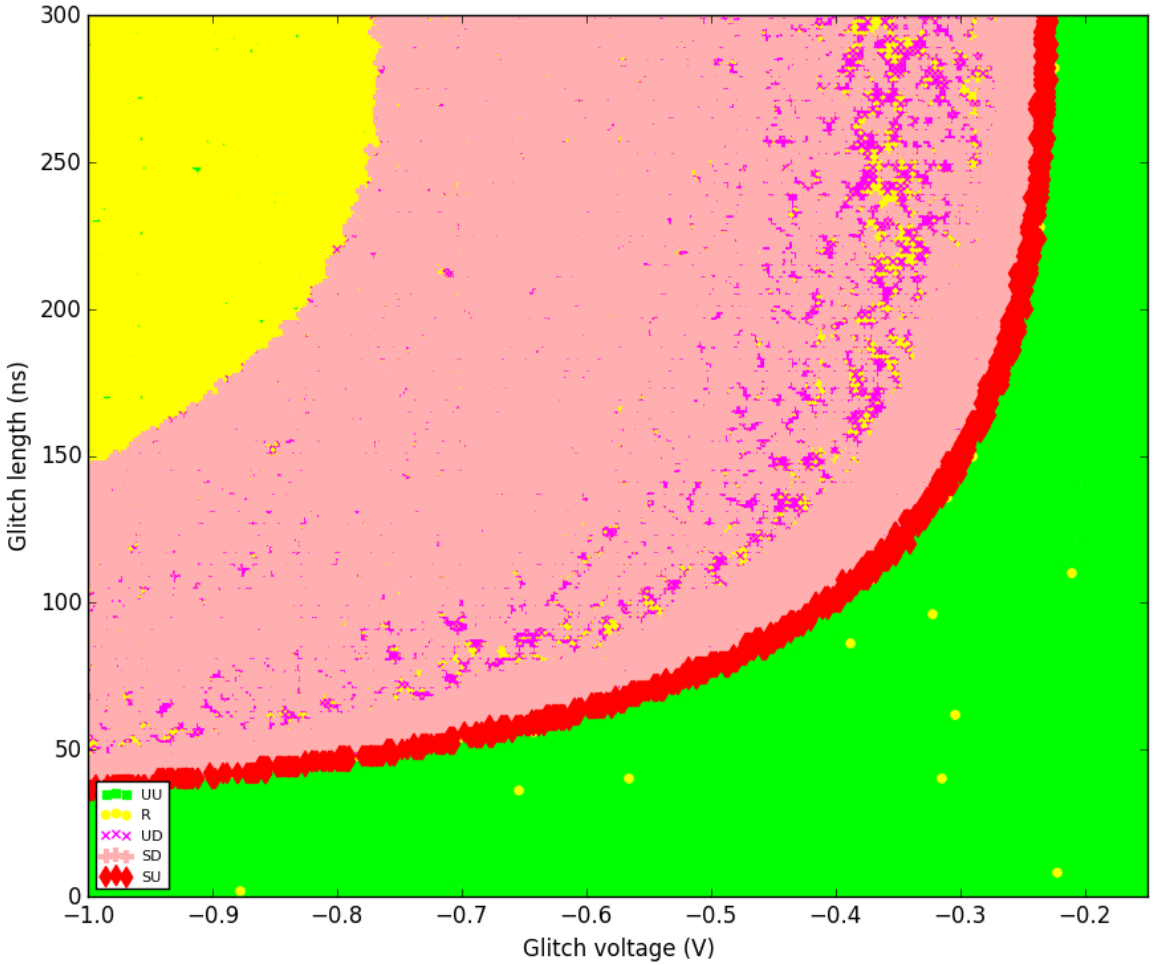
Characterization

TI Power ADD voltage vs. offset



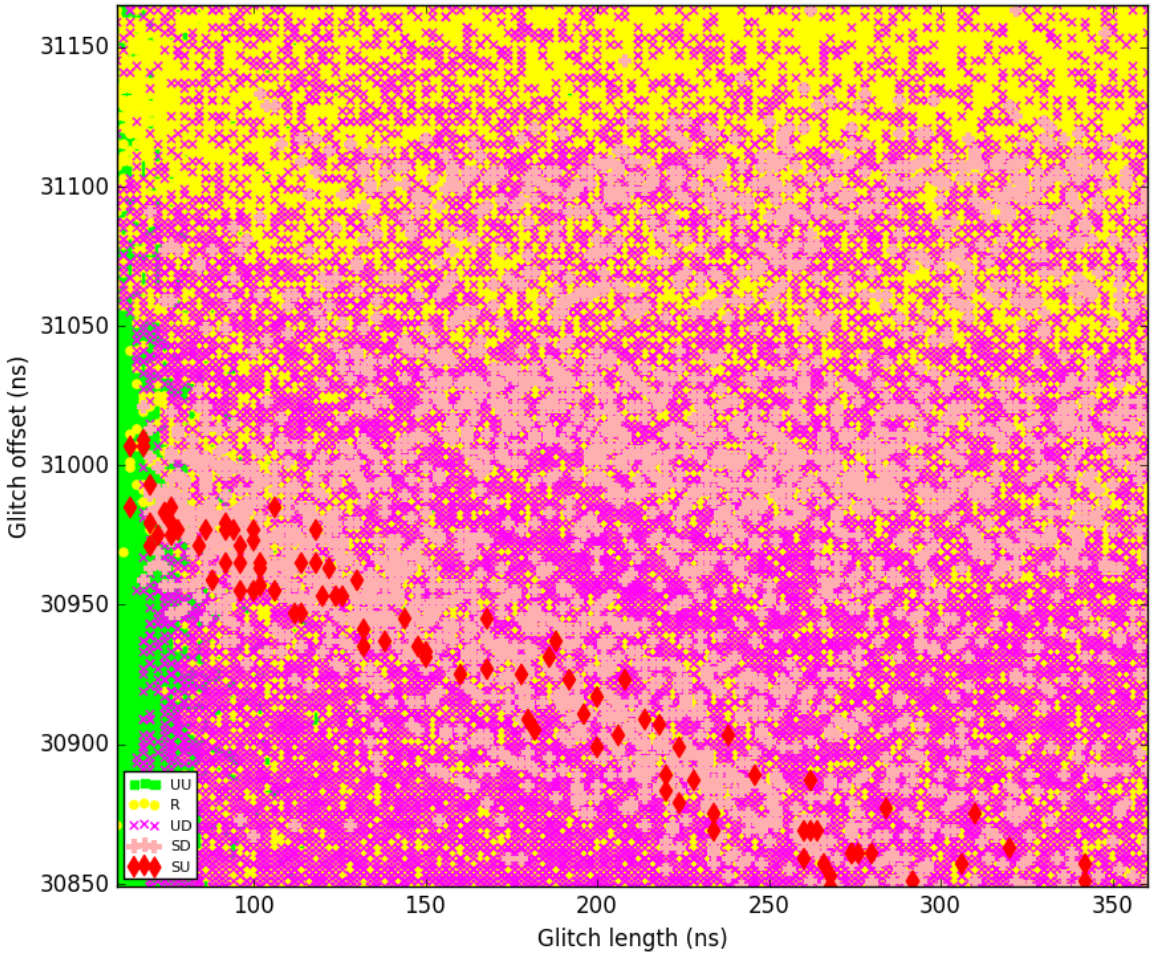
Characterization

TI Power ADD voltage vs. length



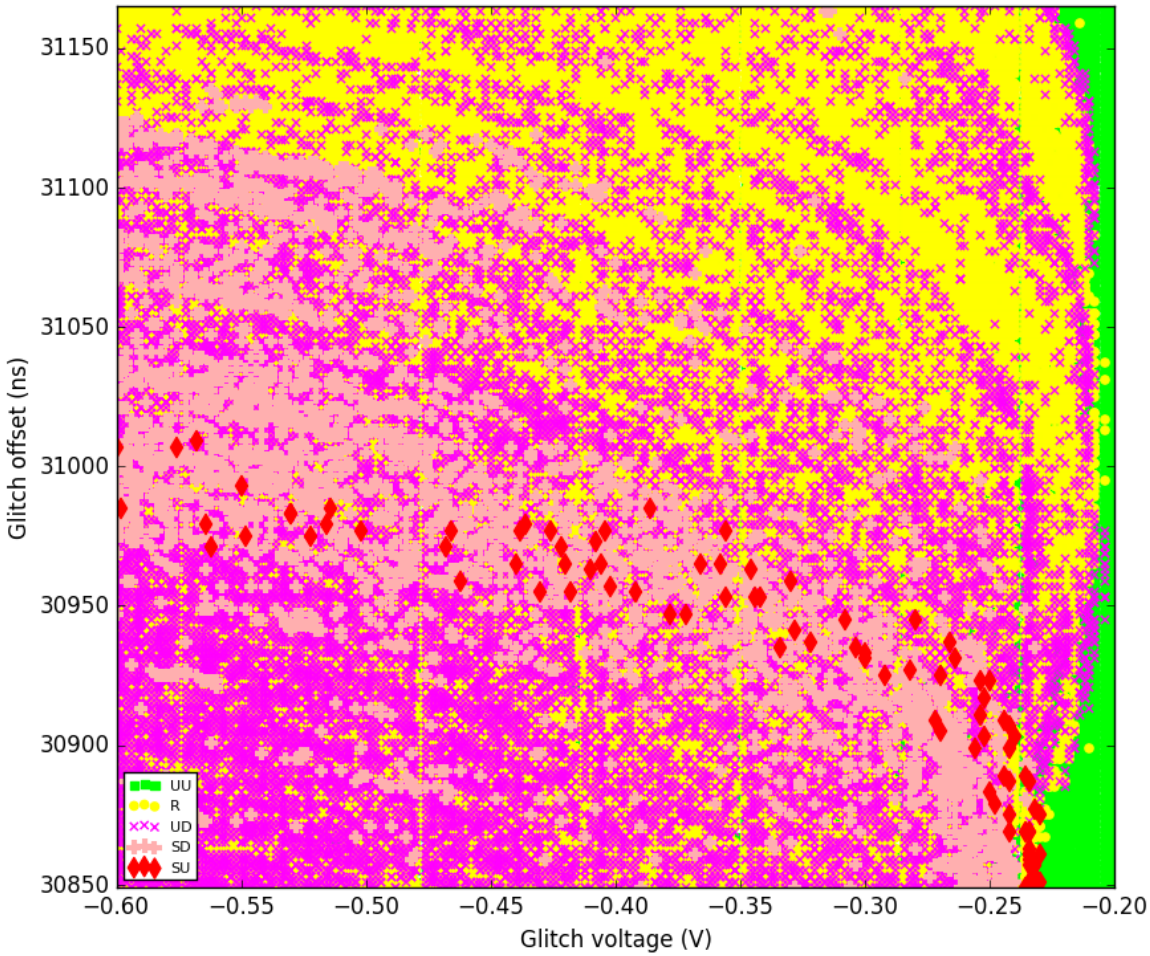
Characterization

TI Power BRANCH offset vs. length



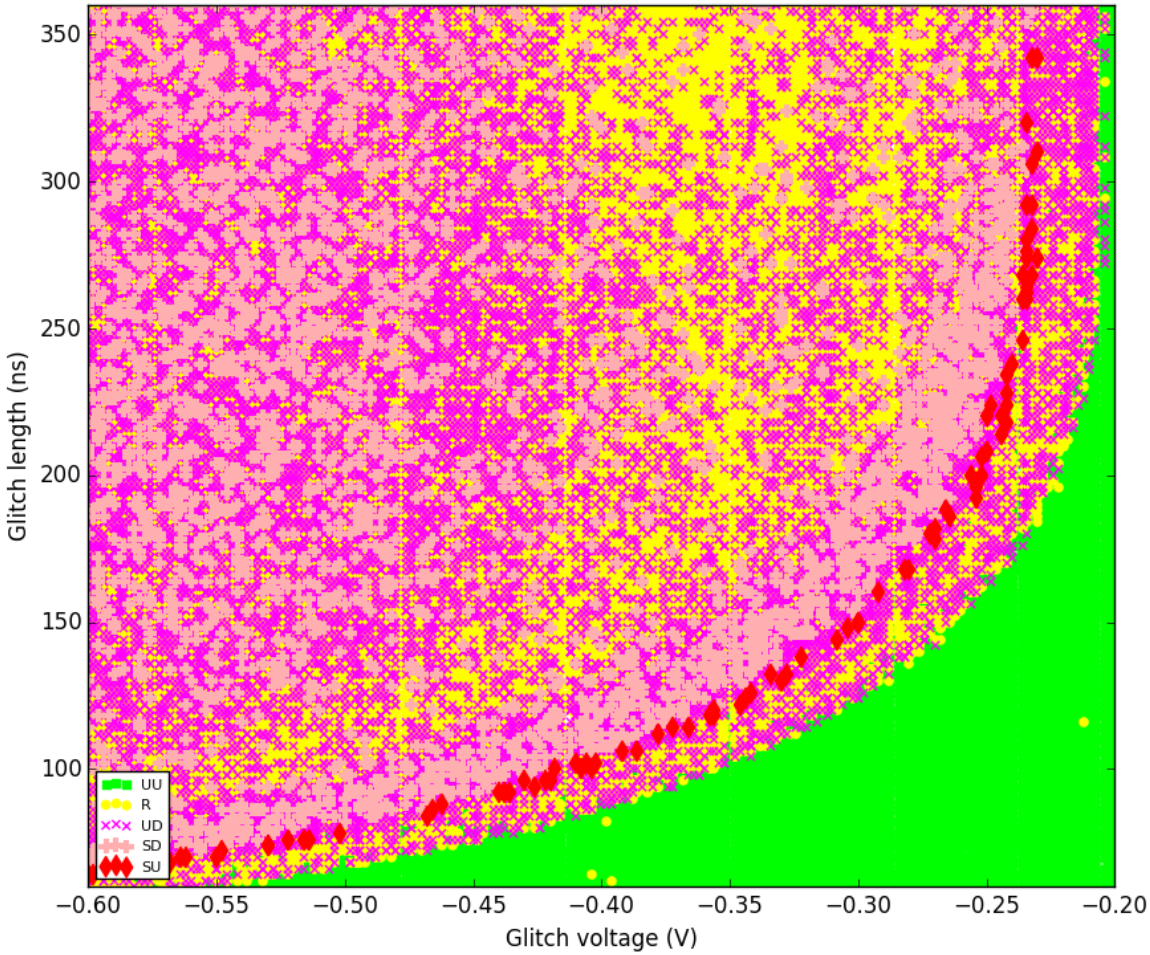
Characterization

TI Power BRANCH offset vs. voltage



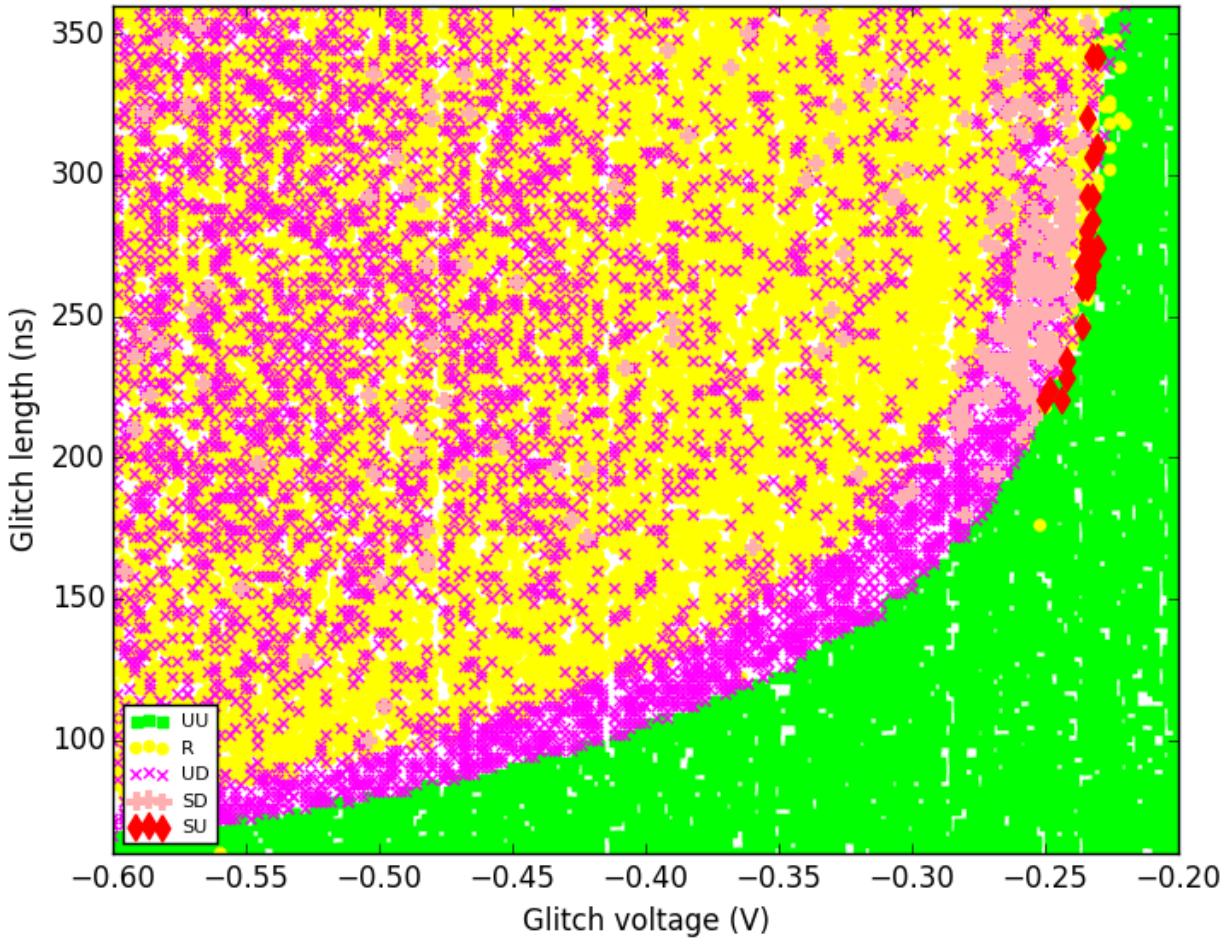
Characterization

TI Power BRANCH length vs. voltage



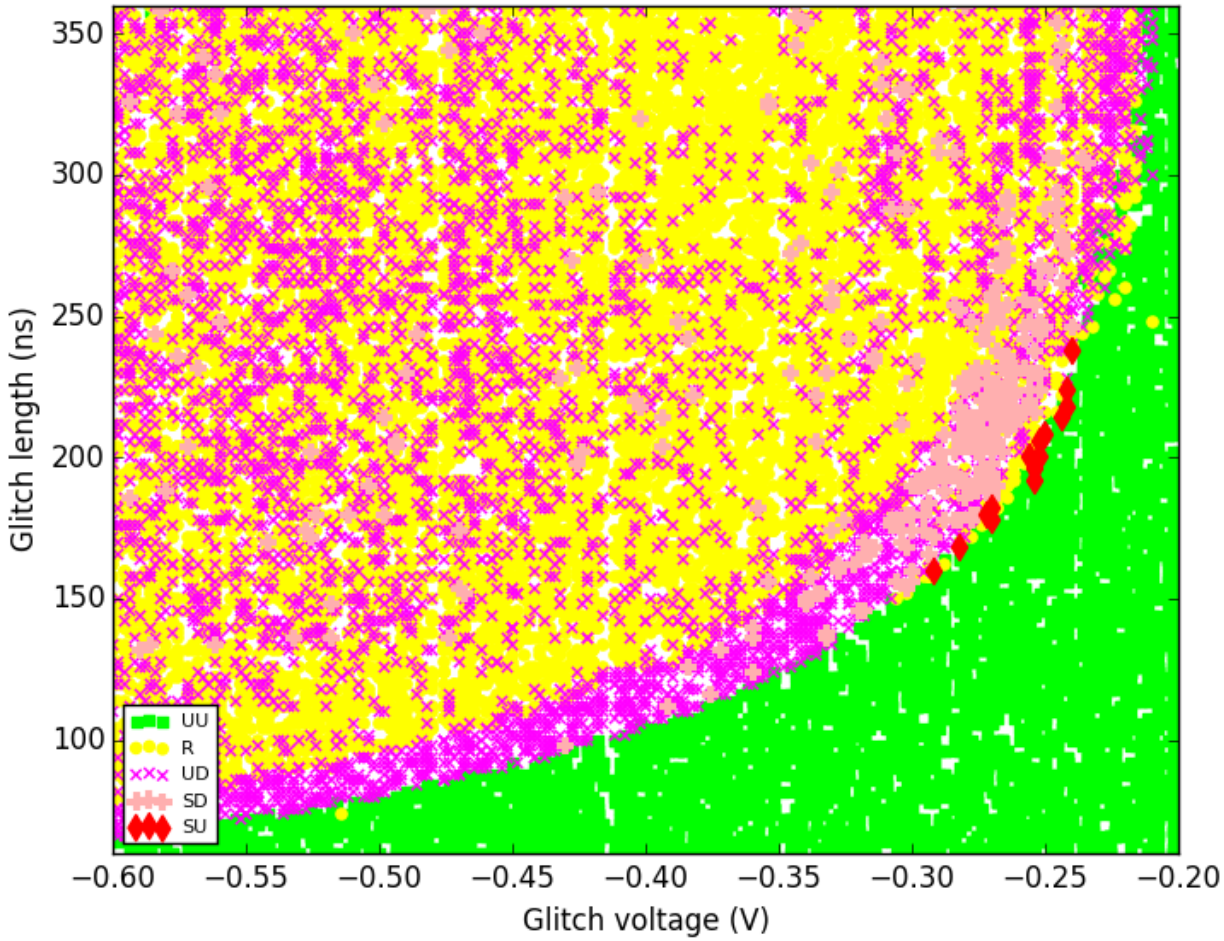
Characterization

TI Power BRANCH length vs. voltage, offset binned (40ns) 1/4



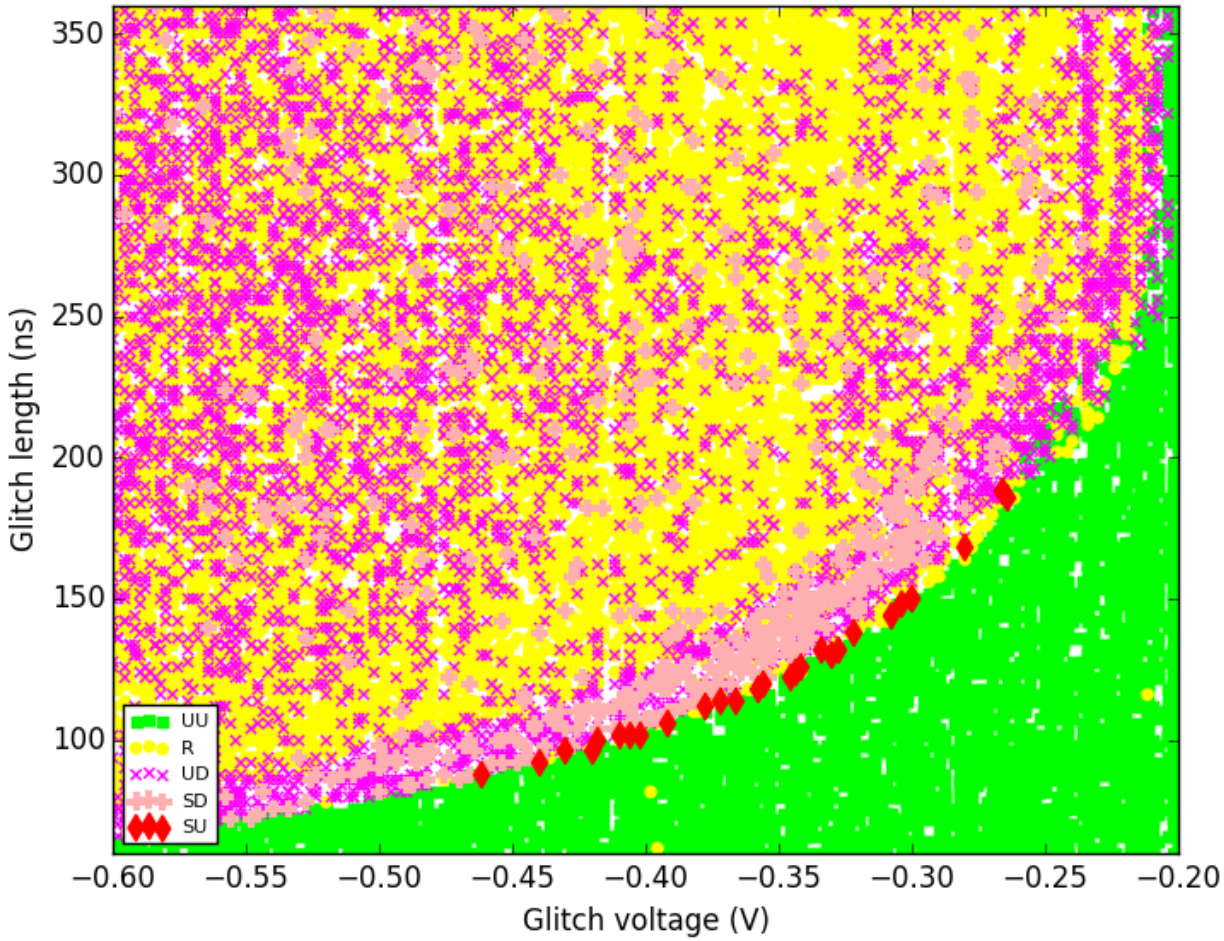
Characterization

TI Power BRANCH length vs. voltage, offset binned (40ns) 2/4



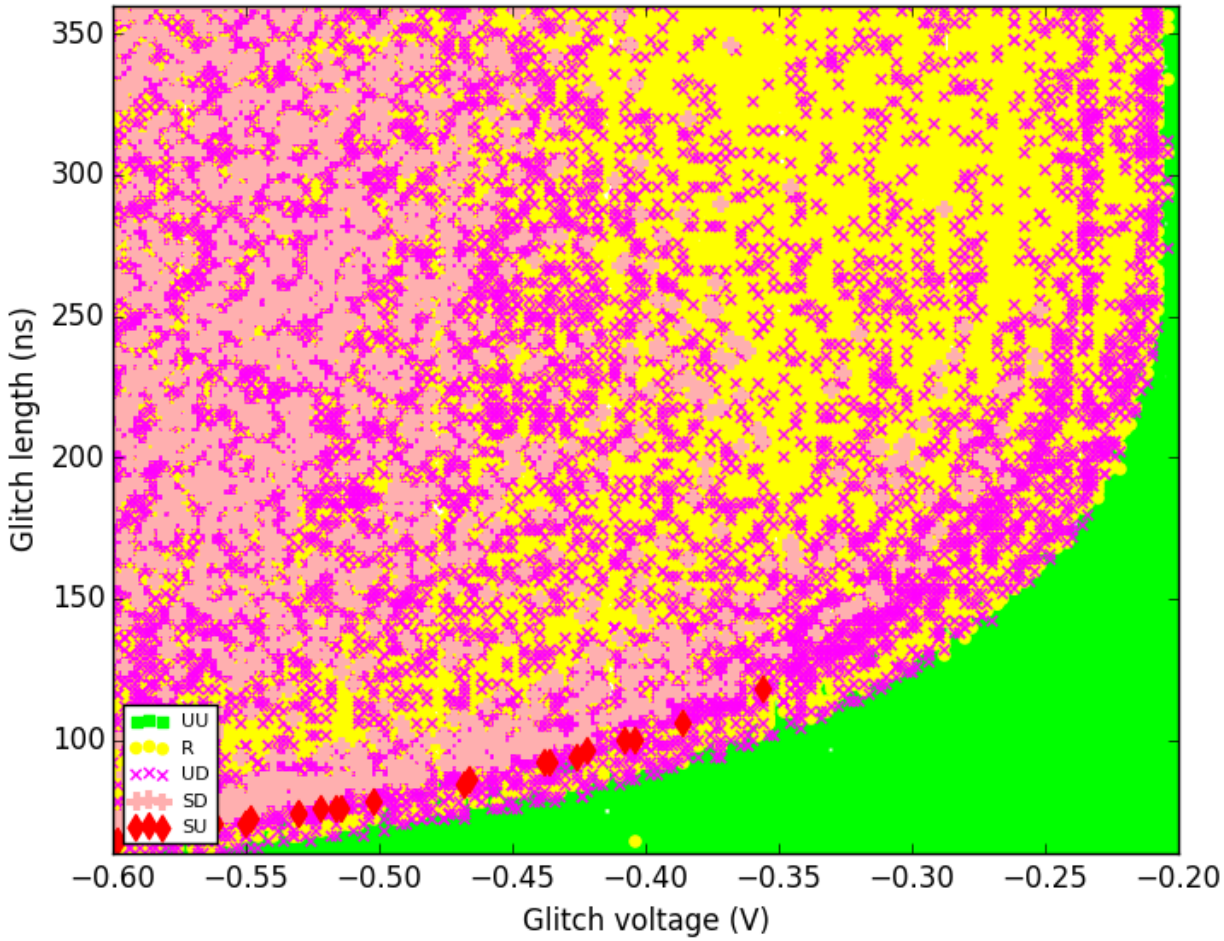
Characterization

TI Power BRANCH length vs. voltage, offset binned (40ns) 3/4



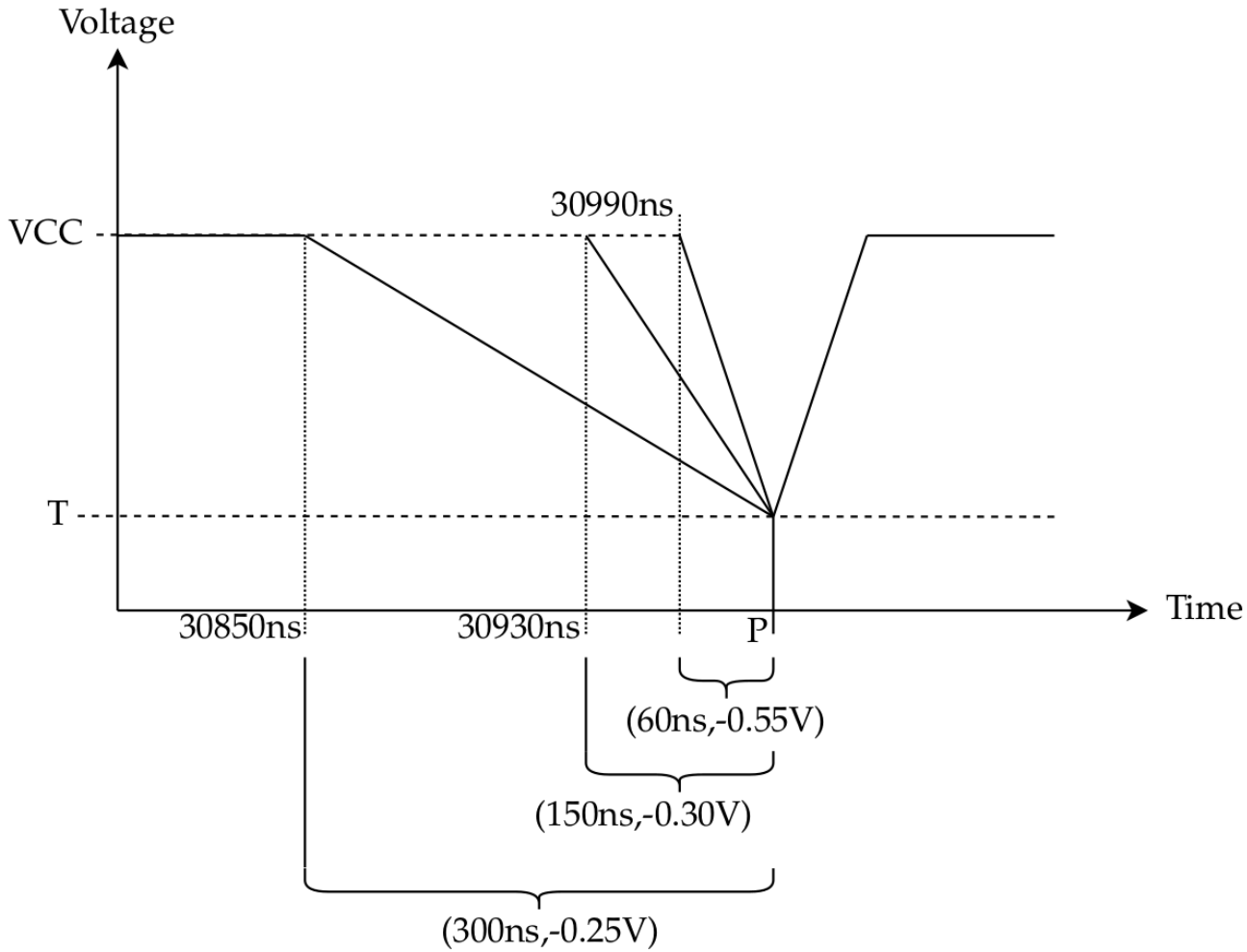
Characterization

TI Power BRANCH length vs. voltage, offset binned (40ns) 4/4



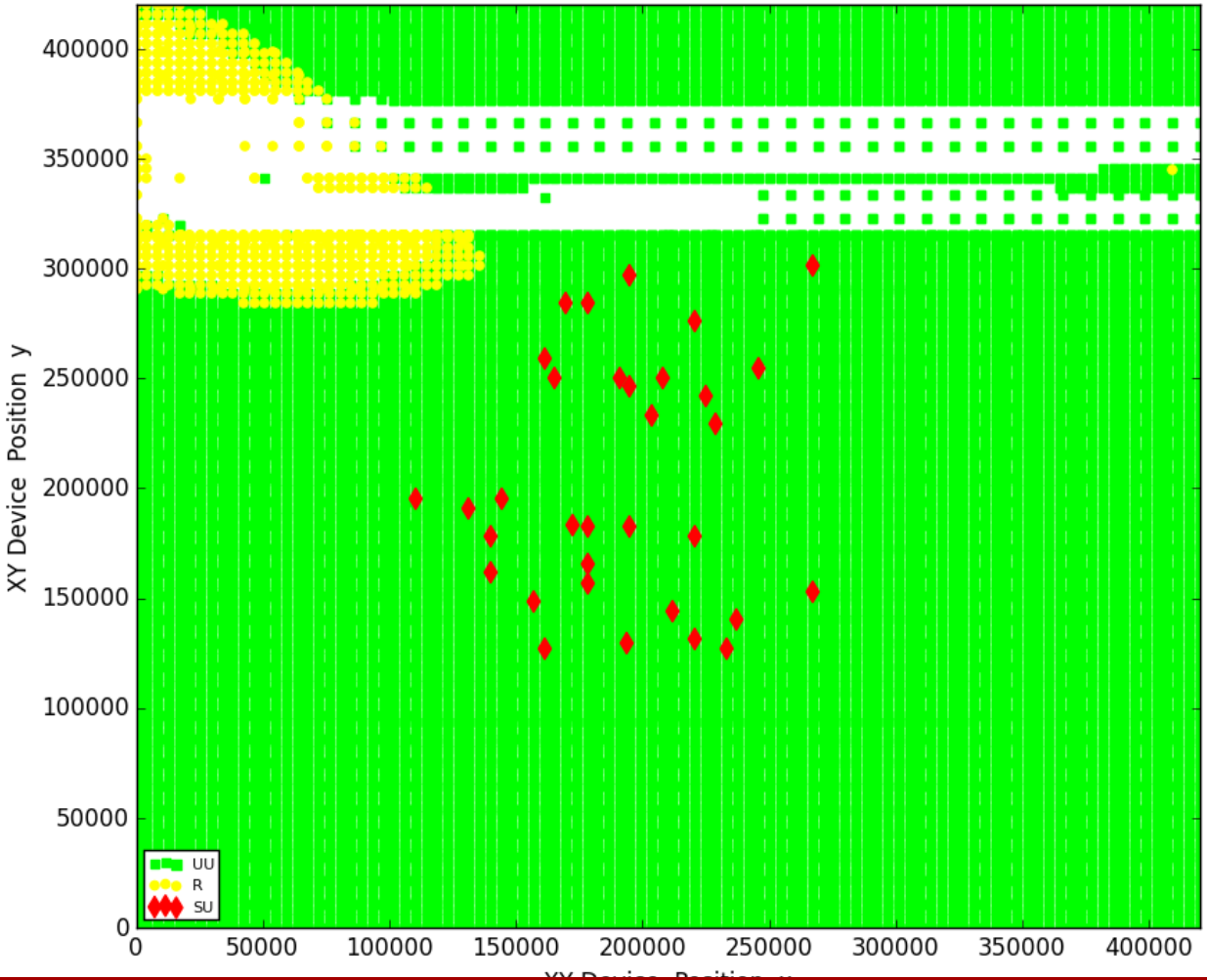
Characterization

Length vs. voltage vs. offset



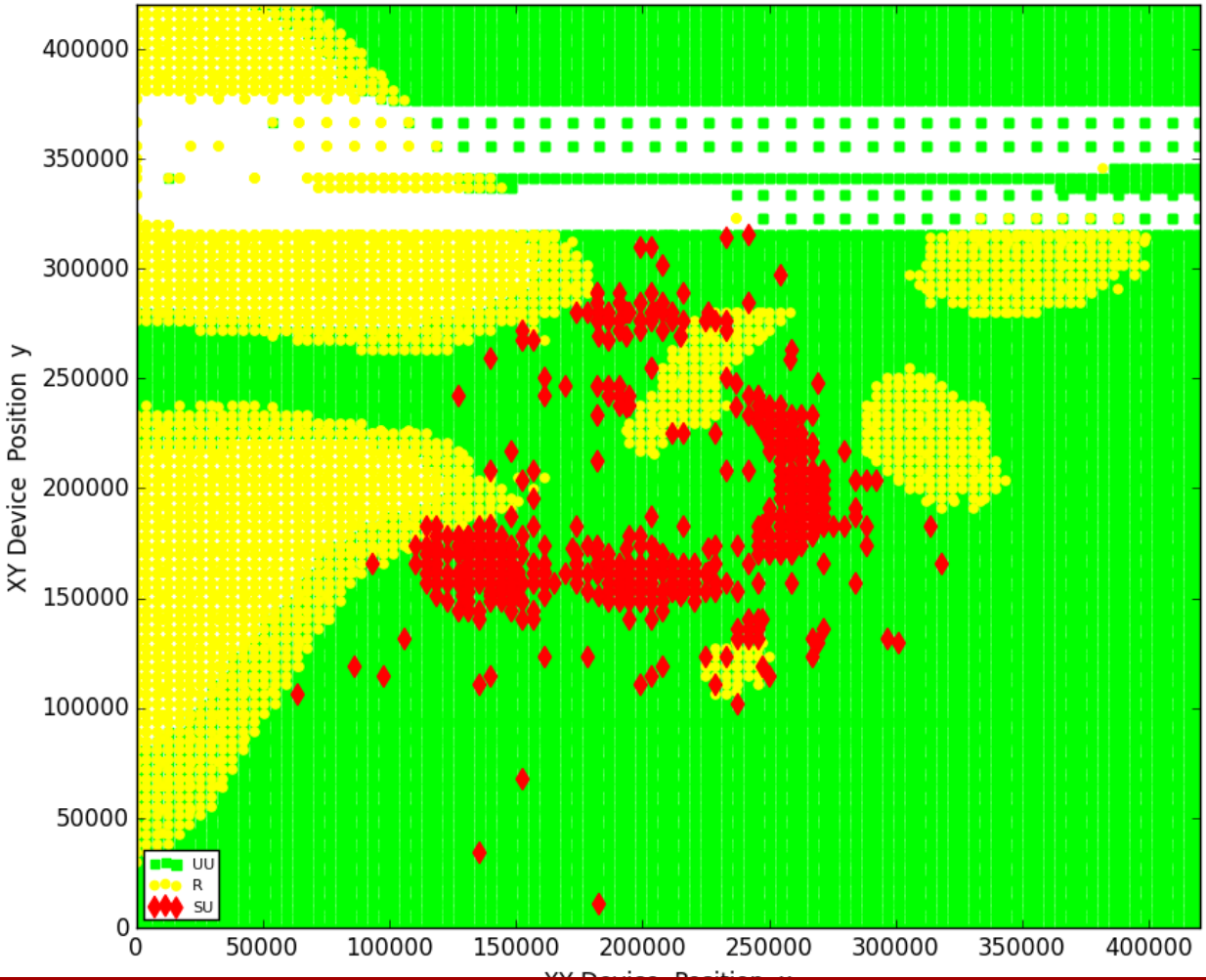
Characterization

ST EM ADD X,Y position, glitch power binned (20%) 1/4



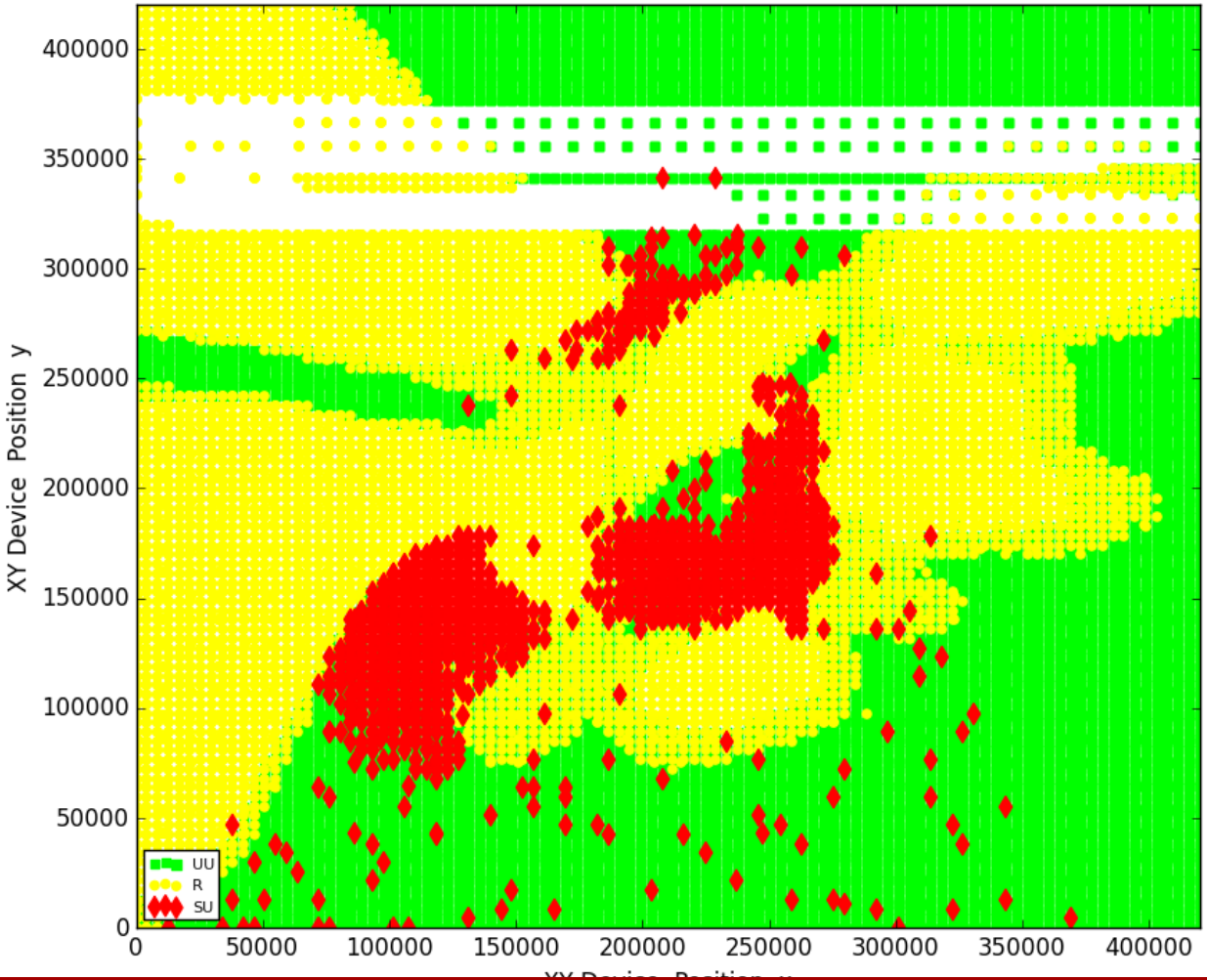
Characterization

ST EM ADD X,Y position, glitch power binned (20%) 2/4



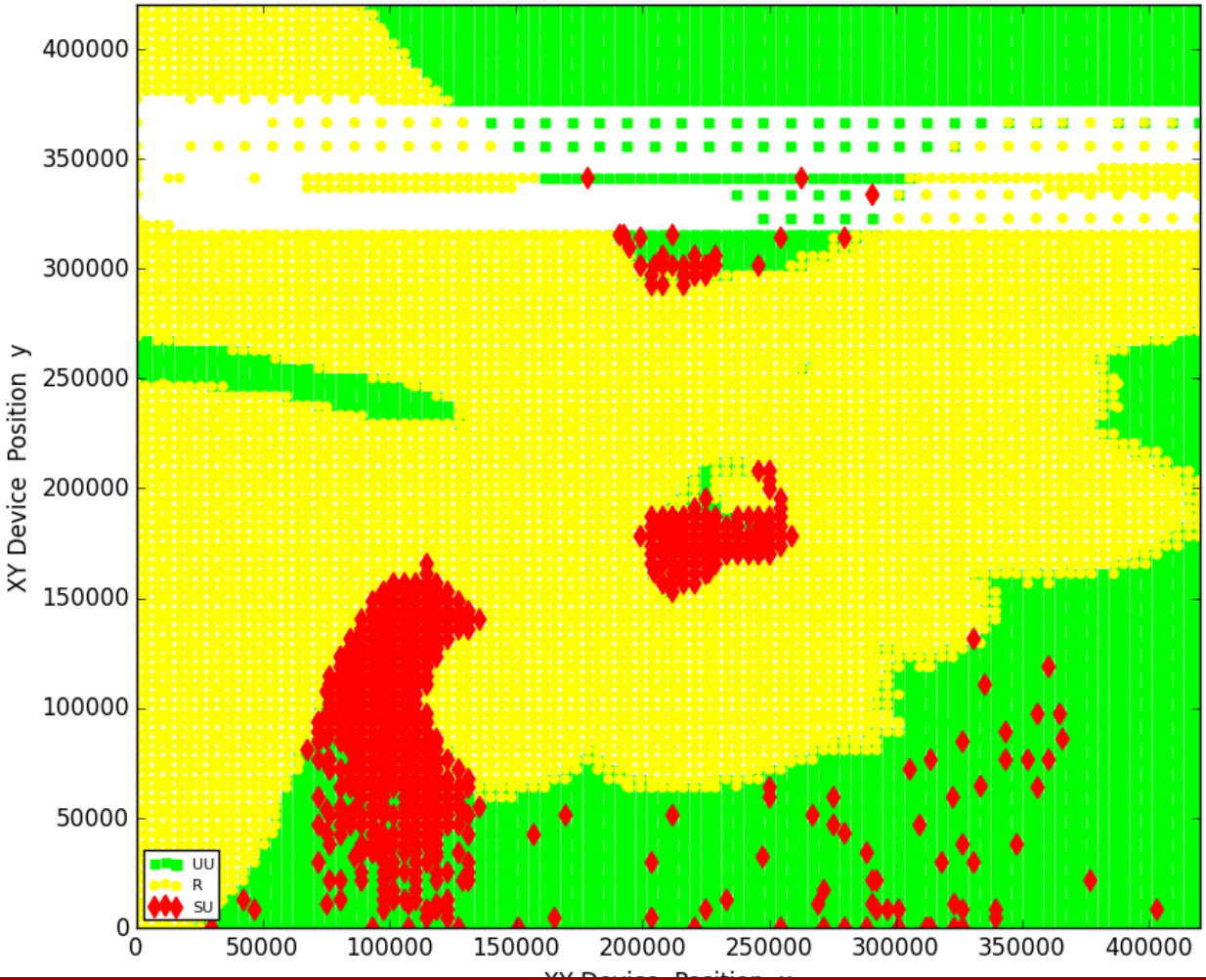
Characterization

ST EM ADD X,Y position, glitch power binned (20%) 3/4



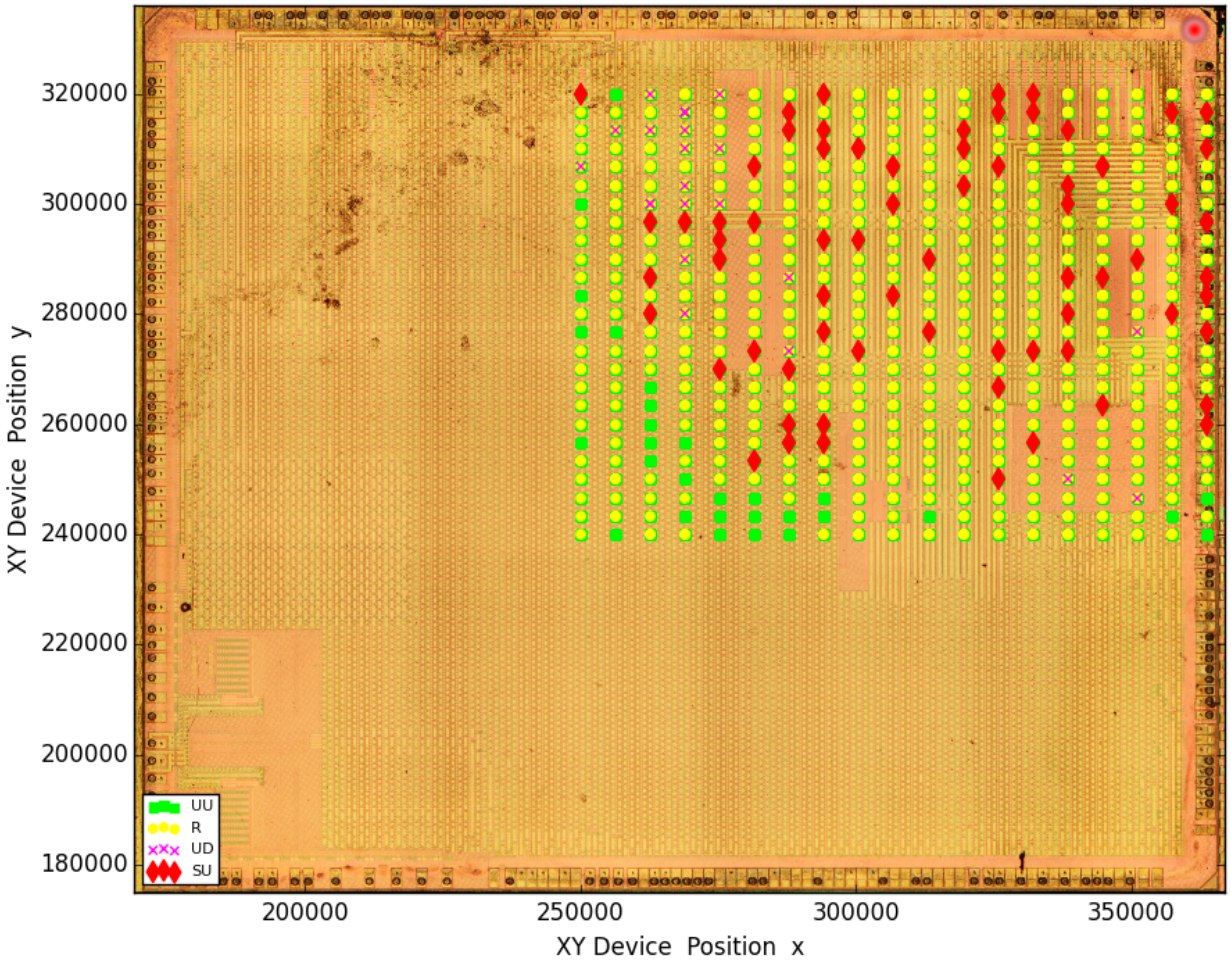
Characterization

ST EM ADD X,Y position, glitch power binned (20%) 4/4



Characterization

TI EM BRANCH X,Y position on die



Characterization

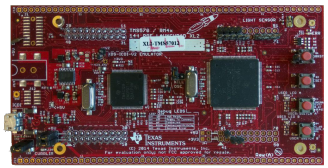
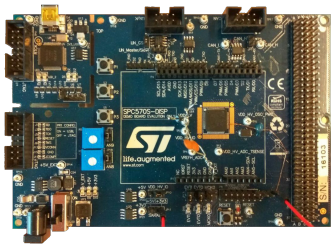
3. Determine fixed values for parameters that yield good results

MORE PLOTSSS

Characterization

Branch experiment results summary

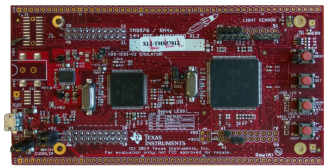
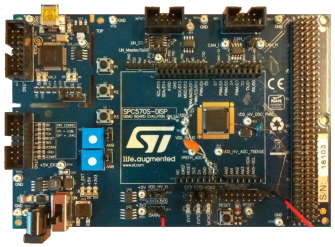
Power

Target	Successful	Detected
 TI	60%	0%
 STM	0%*	0%*

Characterization

Branch experiment results summary

EM

Target	Successful	Detected
 TI	0.2%*	0.07%*
 STM	58%	0%*

Characterization

Comparison of triggered measures in TI

Successful	Detected	Other
0.7%	24%	75%

Lockstep	RAM parity	Flash address parity
98%	21%	27%

JTAG

- Locked, unlockable by providing password
- No knowledge of firmware
- No clear trigger signals available
- No register output to categorize

- Read memory
  - Asset by itself
  - Stepping stone to other assets

JTAG


TMS570 / RM4x
XL2-TMS57012
XDS-ICDI-V2 EMULATOR
LIGHT SENSOR
Debug LEDS
TEXAS INSTRUMENTS
(C) 2014 Texas Instruments, Inc.
For evaluation only; not FCC approved for resale.
USER LED A
USER LED B
USER SWITCH A
USER SWITCH B
ICDI
CURRLIM

JTAG

- JTAG password in memory
- JTAG locking during boot sequence

- Differential analysis of locked and unlocked target
- Inject fault during boot
- Obtain JTAG password for persistent access

JTAG

1. Investigate normal behavior through (side) channels
2. Determine rough ranges of values for different parameters
3. Determine fixed values for parameters that yield good results

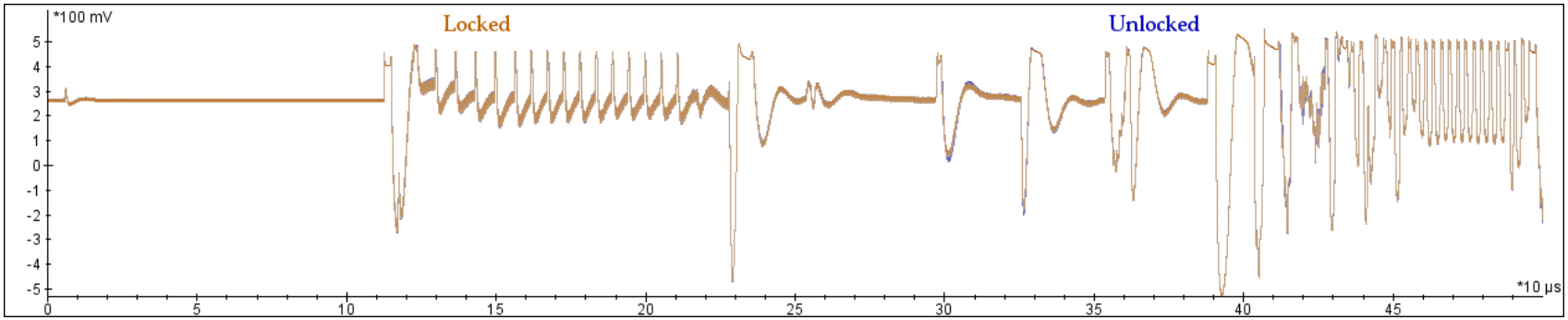
JTAG

1. **Investigate normal behavior through (side) channels**
2. Determine rough ranges of values for different parameters
3. Determine fixed values for parameters that yield good results

(thank you Fatih!)

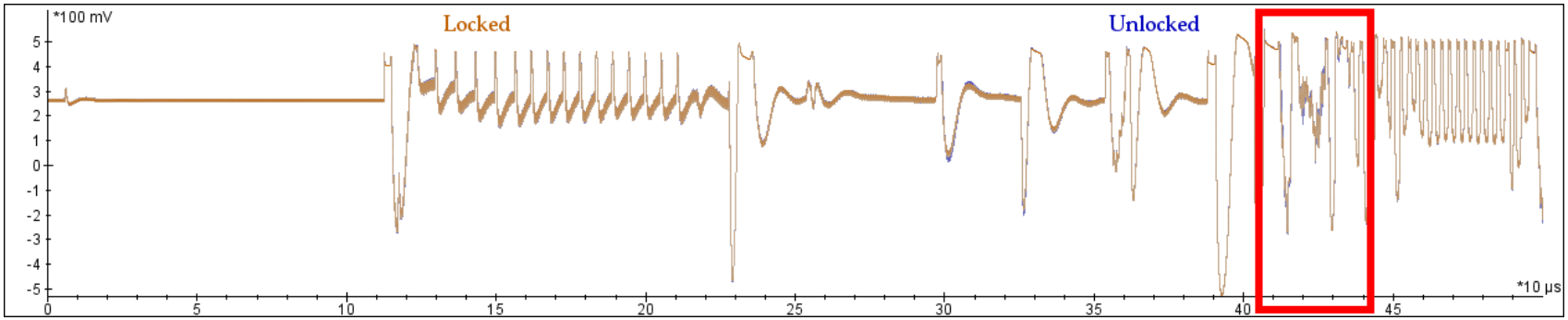
JTAG

1. Investigate normal behavior through (side) channels



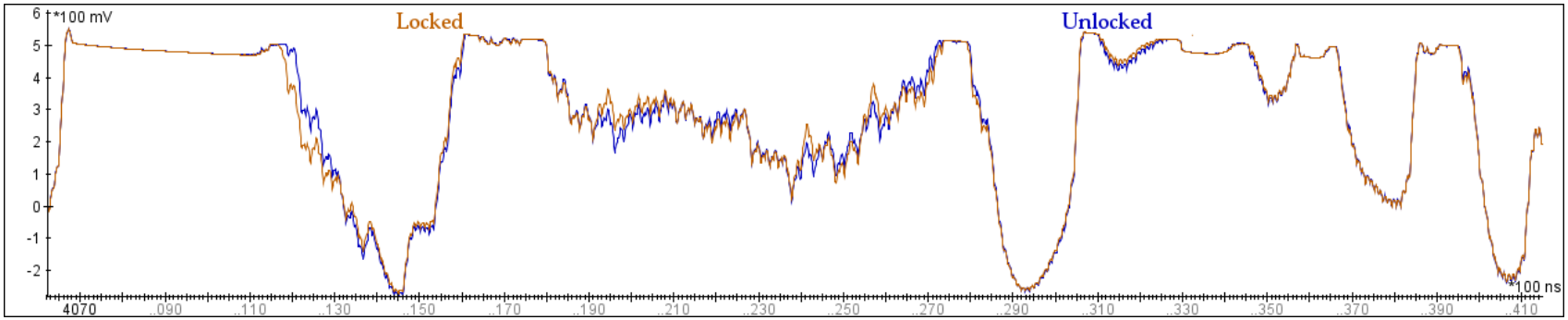
JTAG

1. Investigate normal behavior through (side) channels



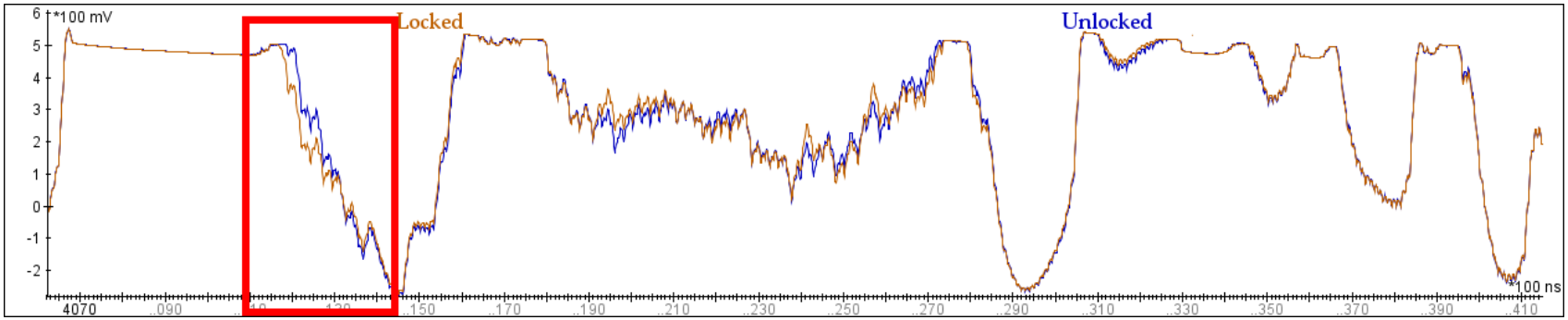
JTAG

1. Investigate normal behavior through (side) channels



JTAG

1. Investigate normal behavior through (side) channels

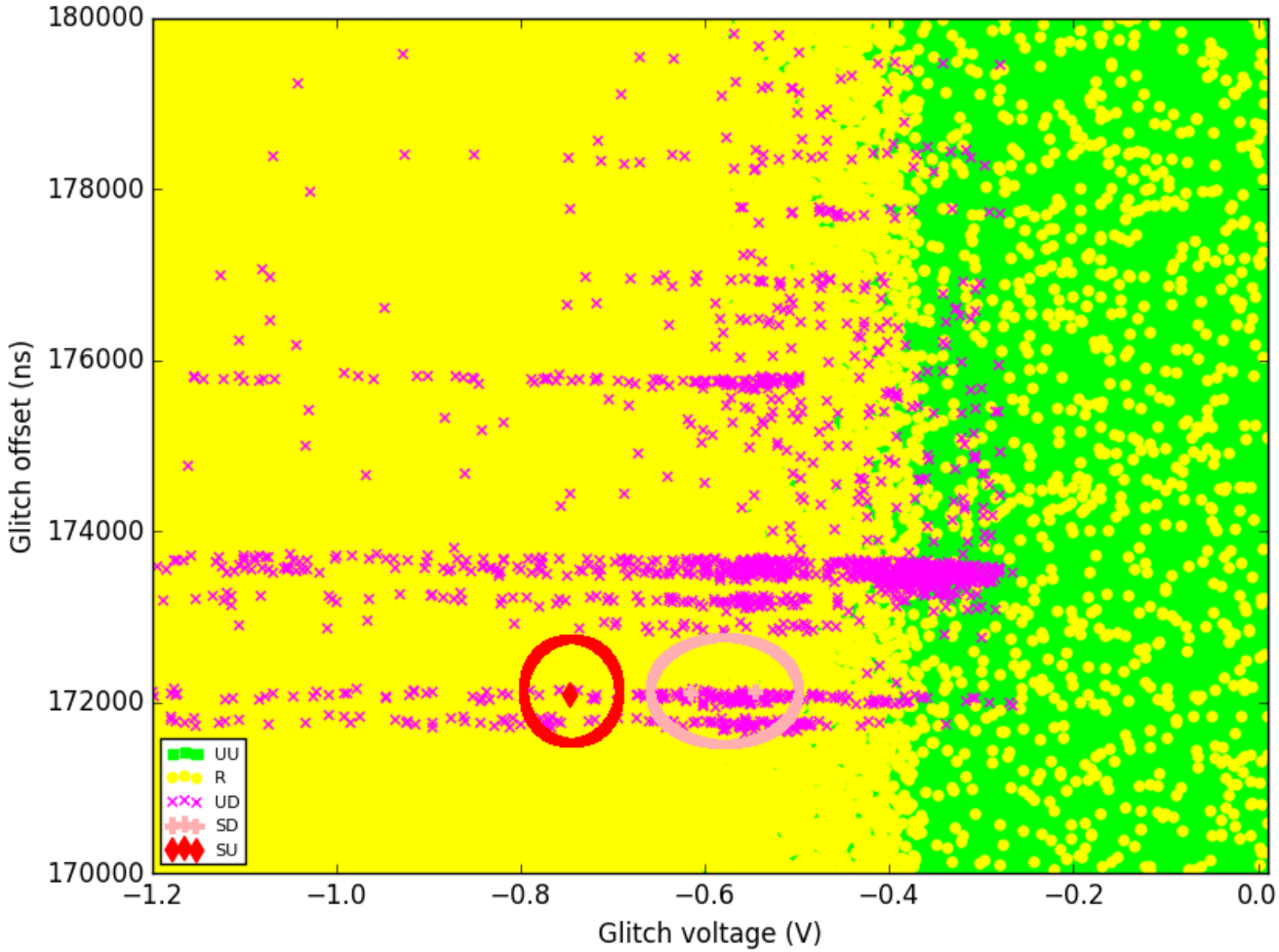


JTAG

1. Investigate normal behavior through (side) channels
2. Determine rough ranges of values for different parameters
3. **Determine fixed values for parameters that yield good results**

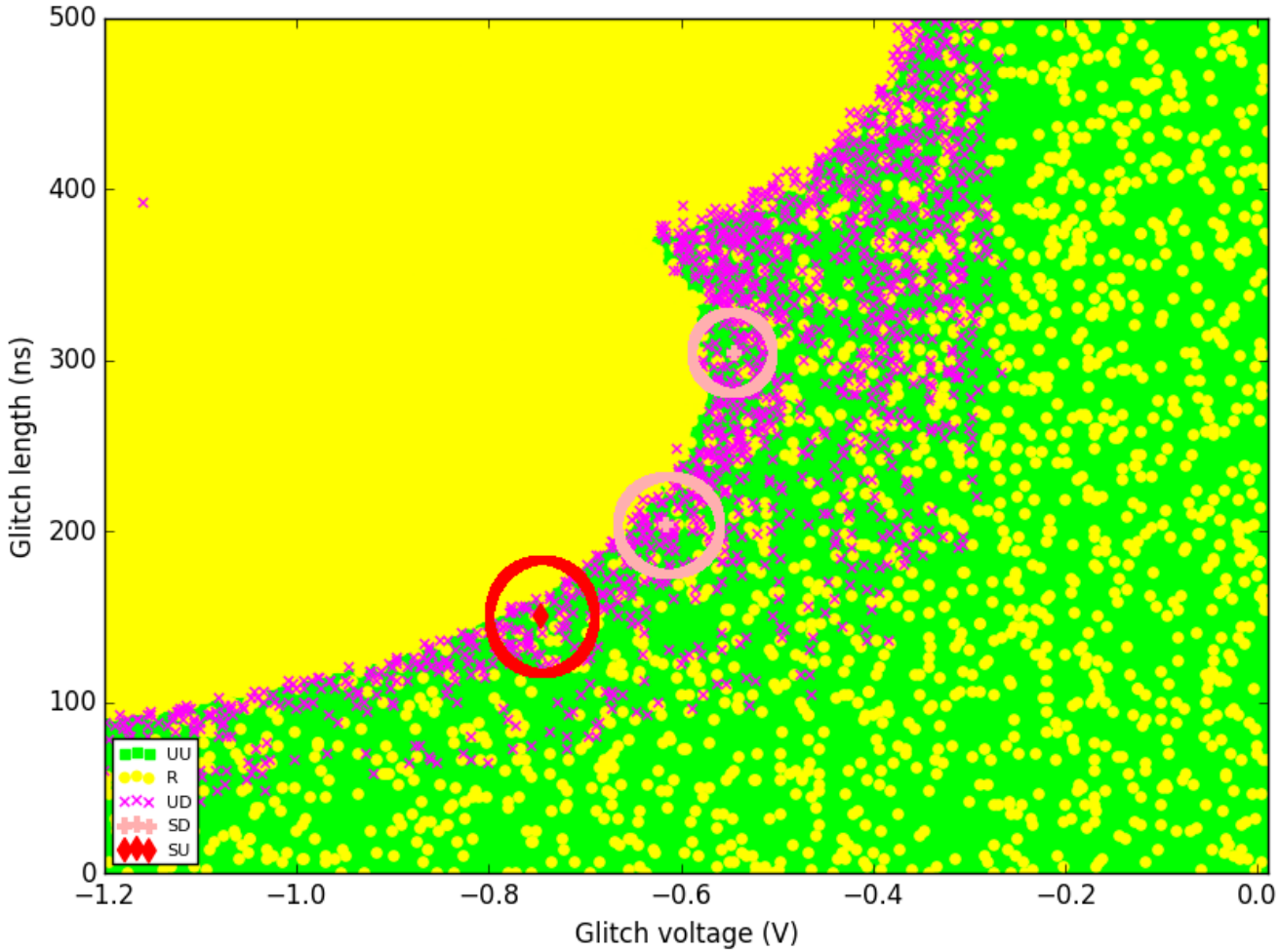
JTAG

TI power JTAG offset vs. voltage

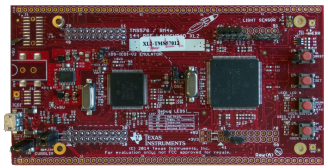


JTAG

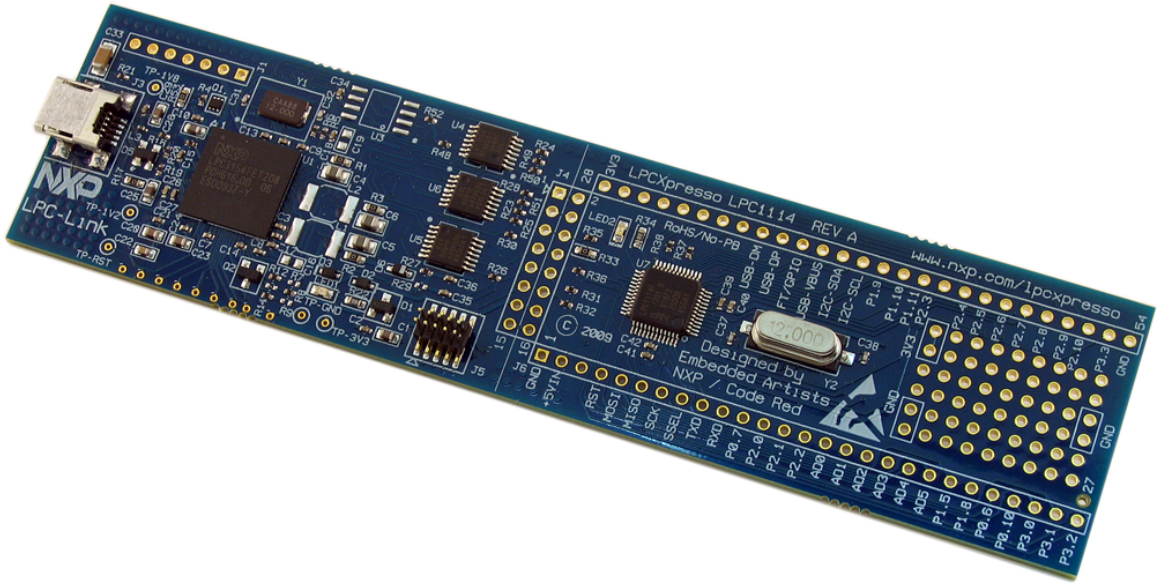
TI power JTAG length vs. voltage



JTAG

Target	Successful	Detected
 TI (power)	1.4%	4.5%

JTAG



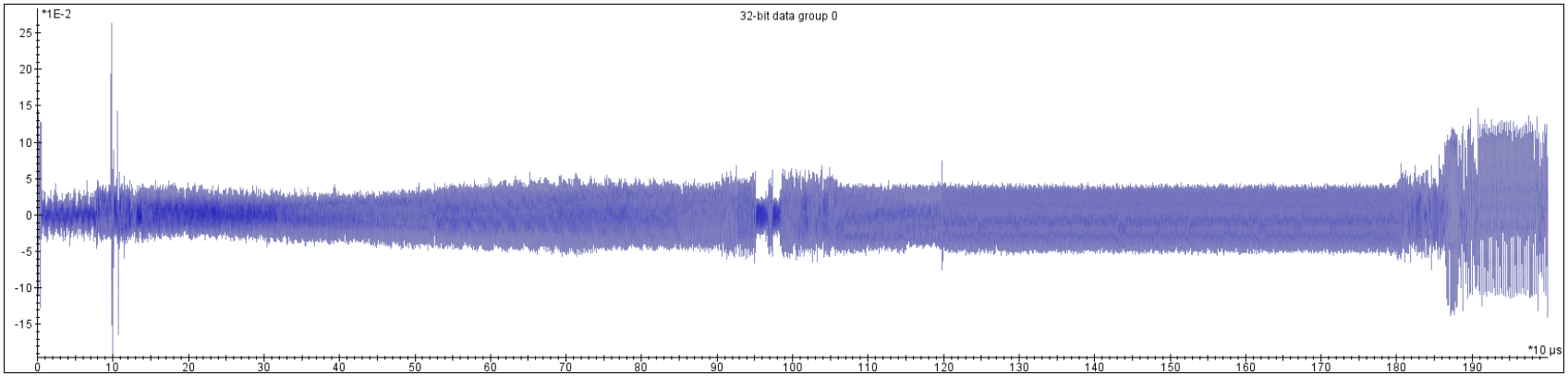
(done by Ramiro)

JTAG

- Correlation analysis by repeatedly changing bits in the password

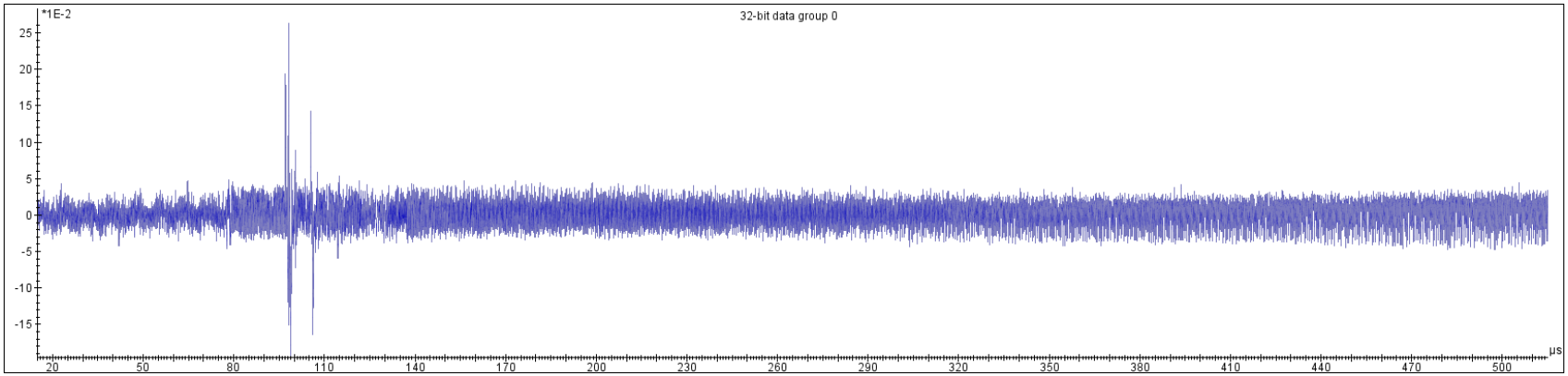
JTAG

1. Investigate normal behavior through (side) channels



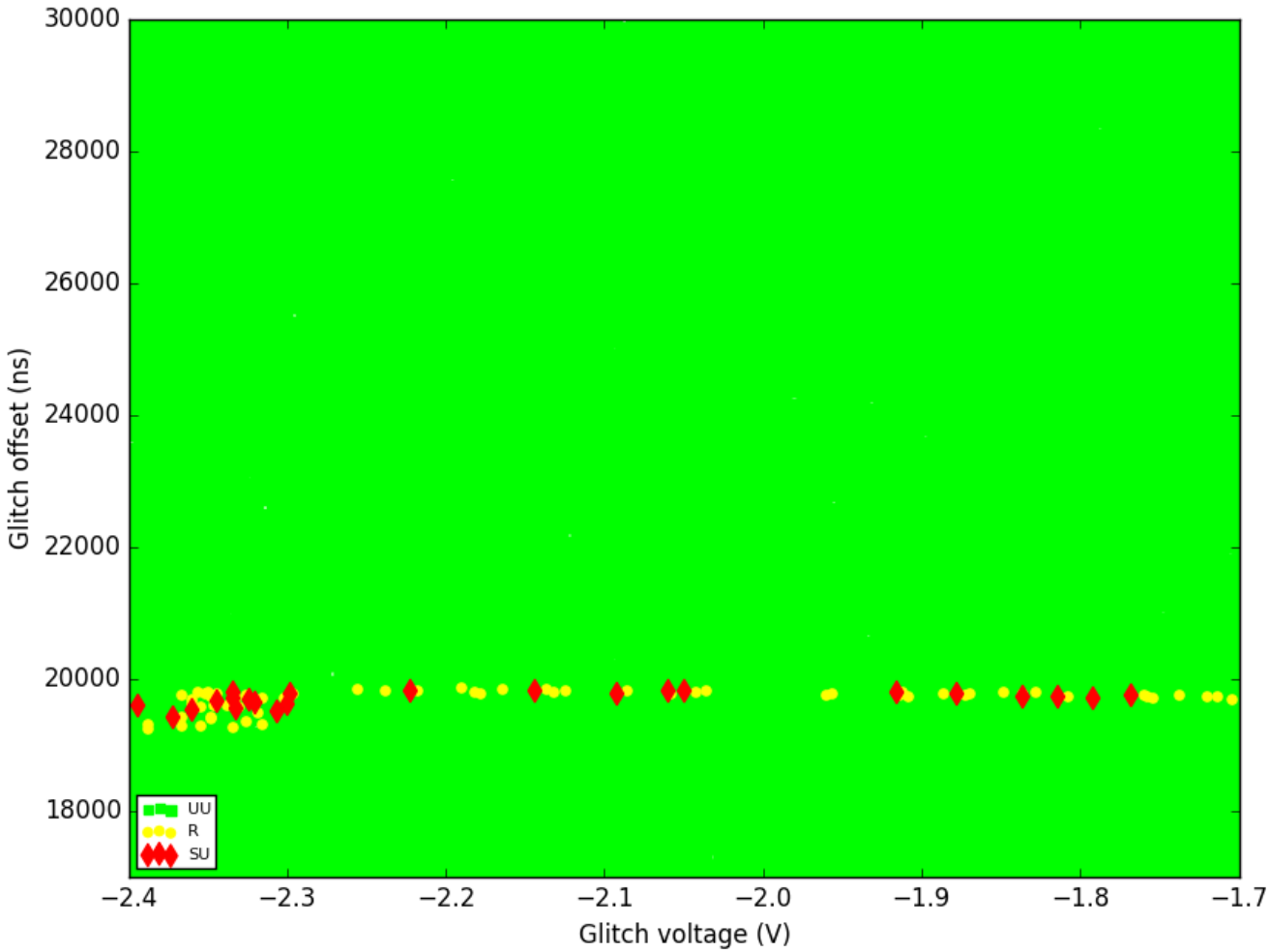
JTAG

1. Investigate normal behavior through (side) channels



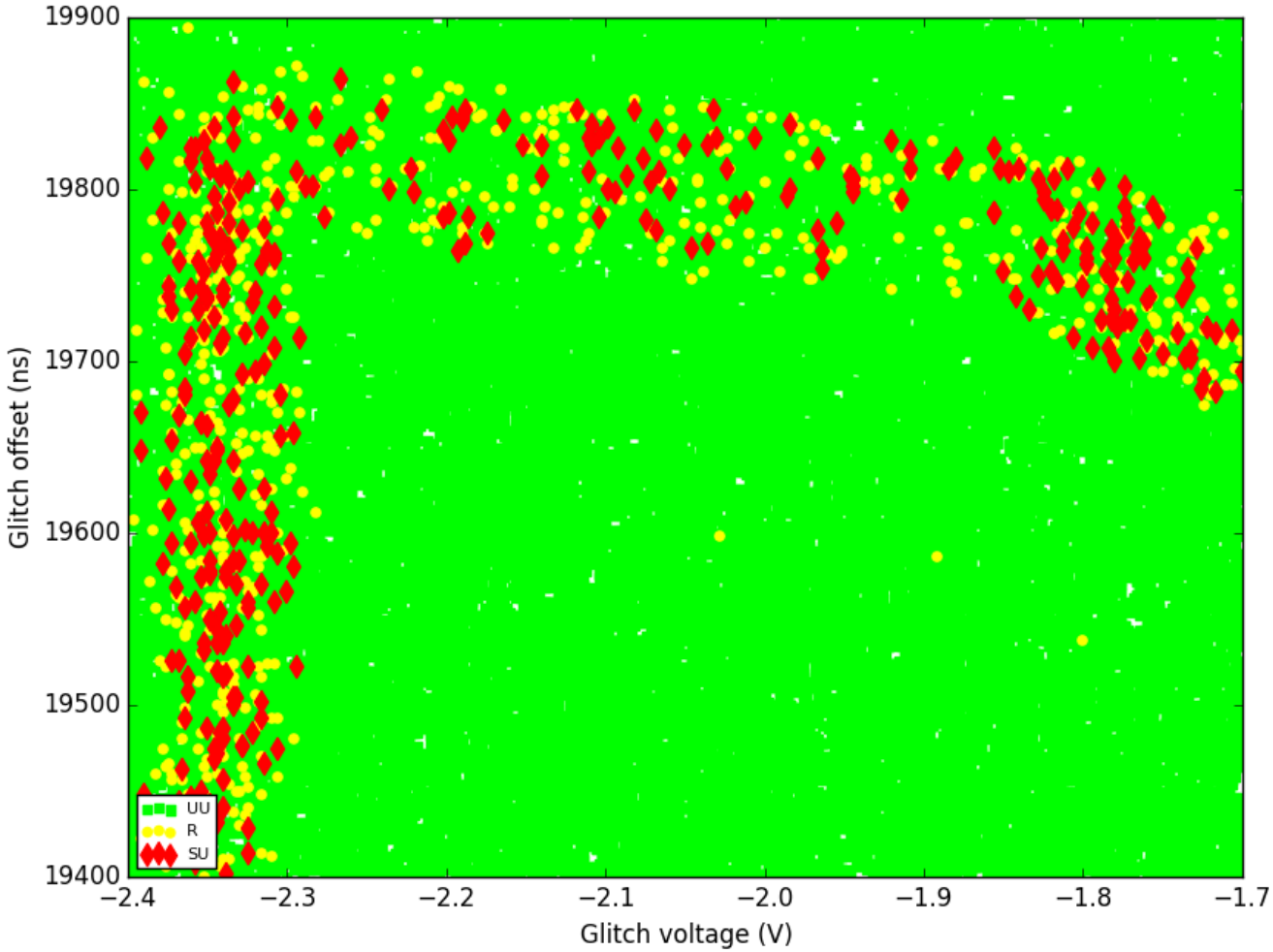
JTAG

NXP power JTAG offset vs. voltage



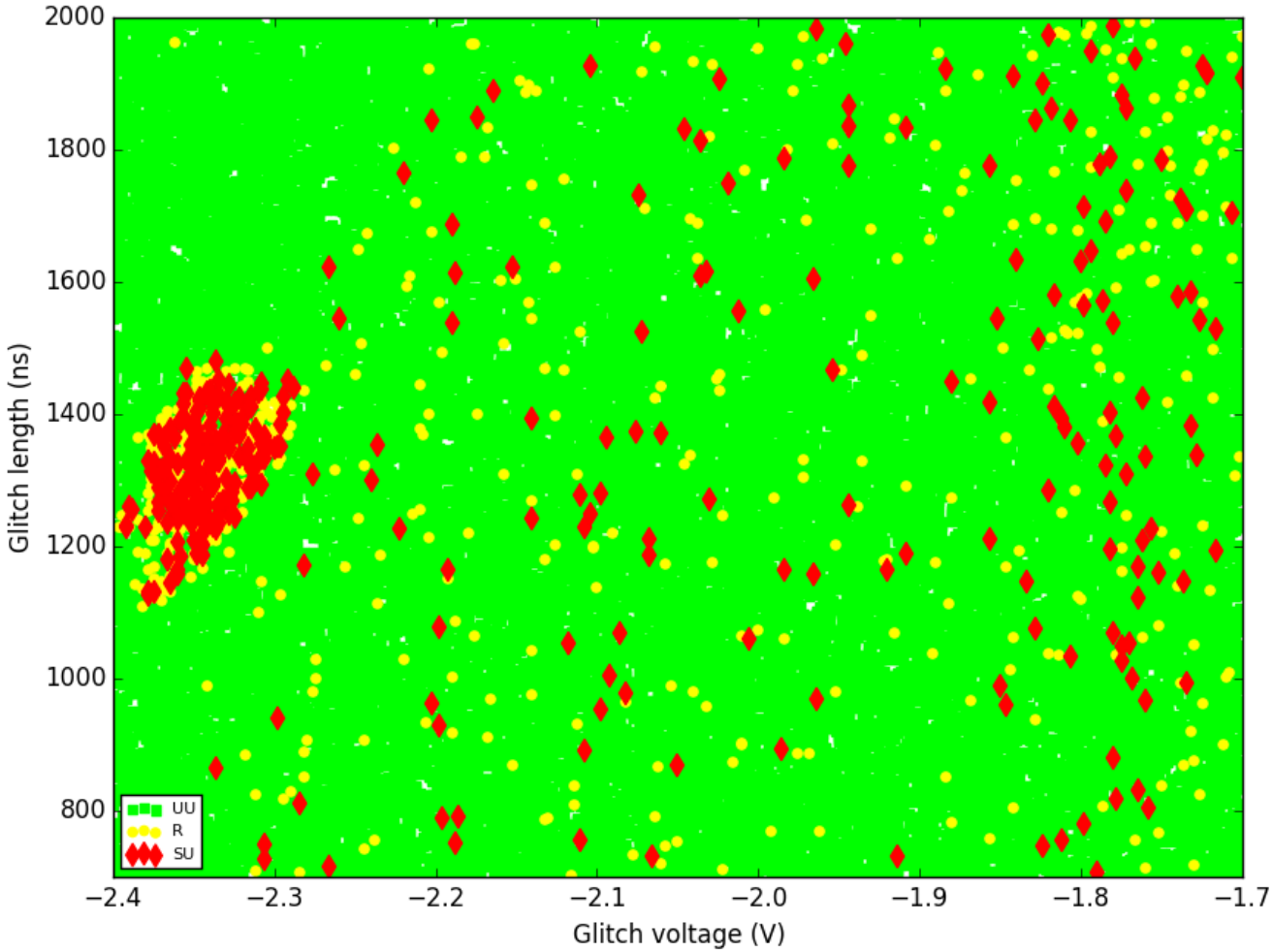
JTAG

NXP power JTAG offset vs. voltage



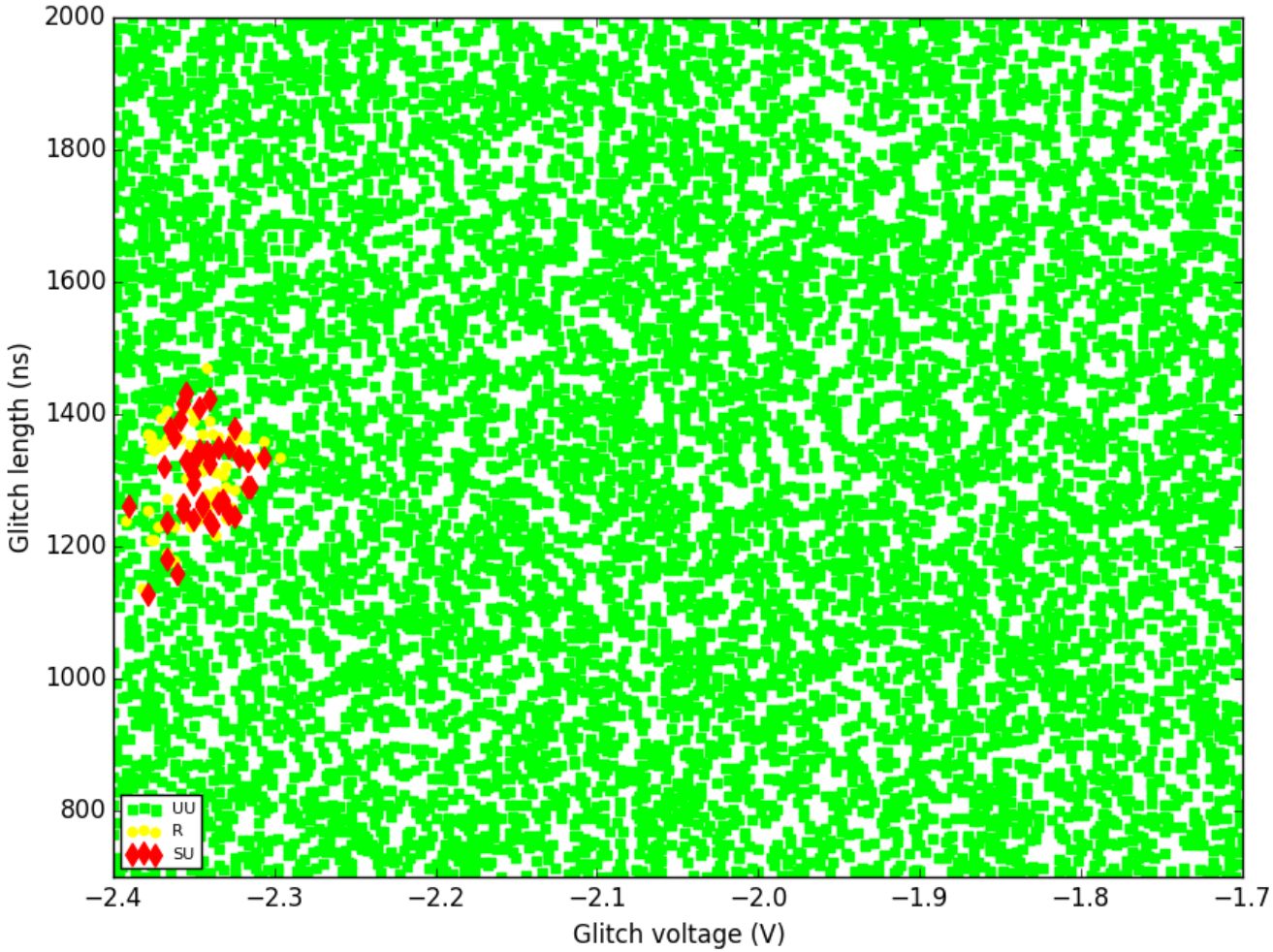
JTAG

NXP power JTAG length vs. voltage



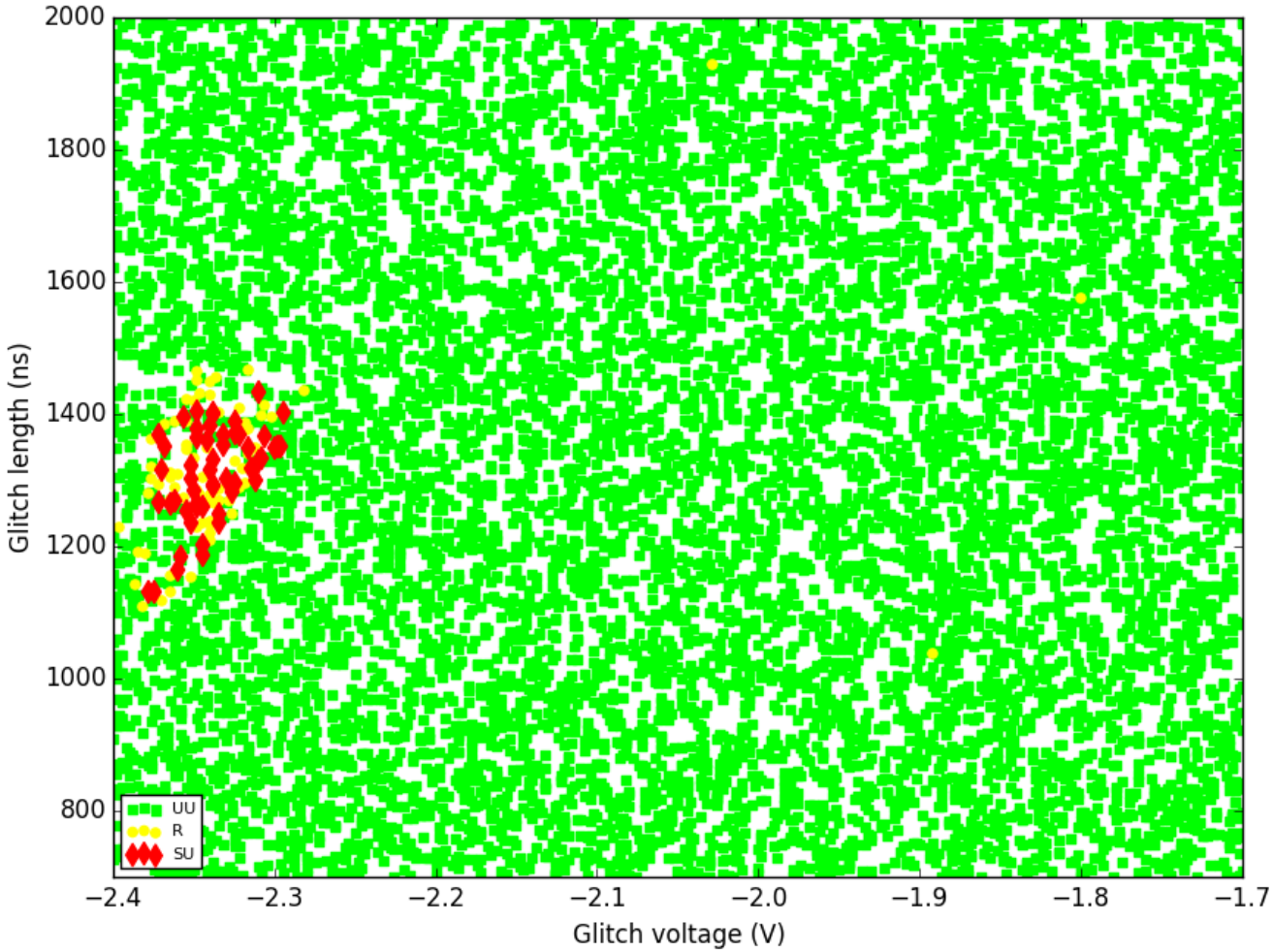
JTAG

NXP power JTAG length vs. voltage, binned offset (125ns) 1/4



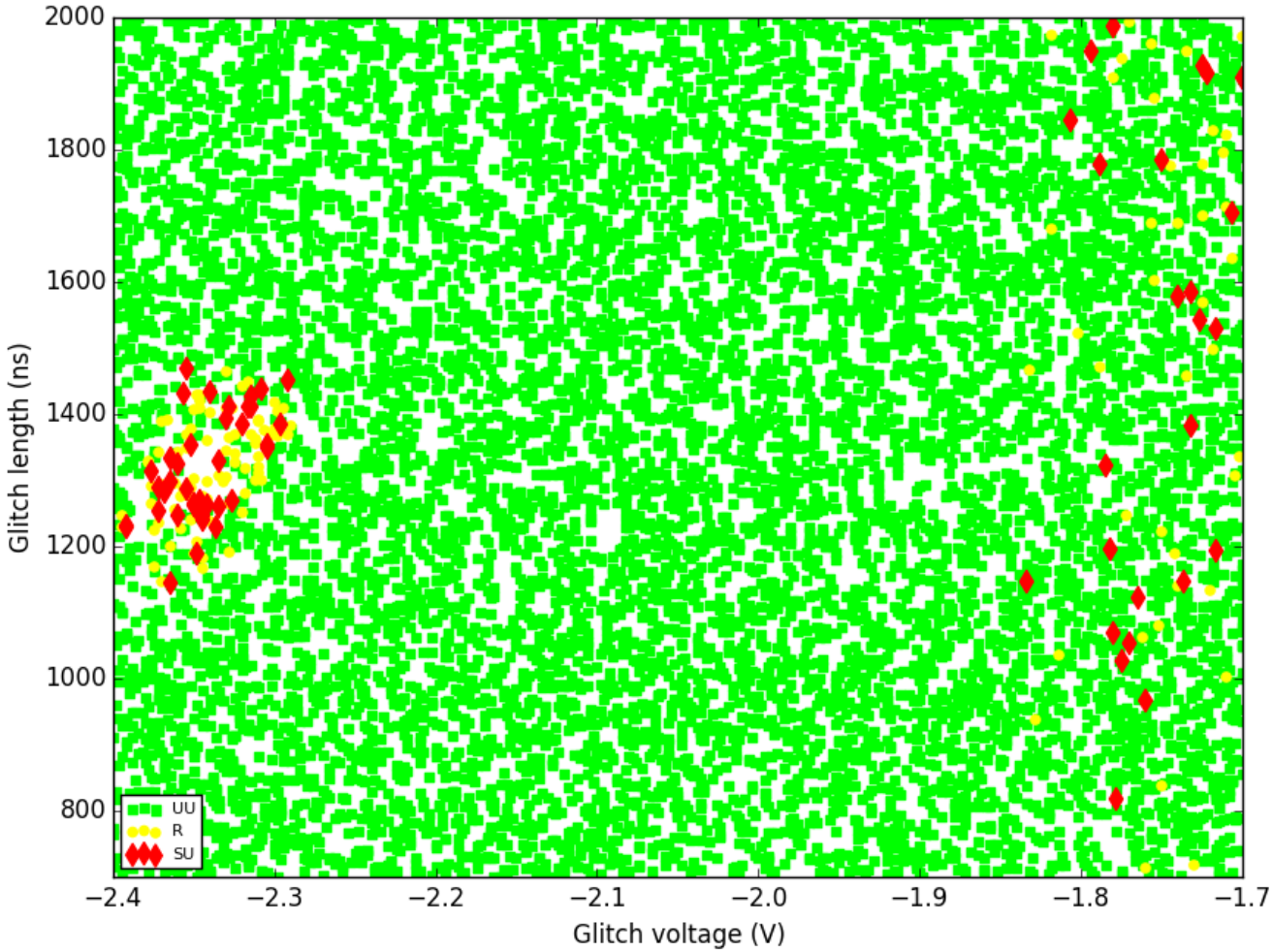
JTAG

NXP power JTAG length vs. voltage, binned offset (125ns) 2/4



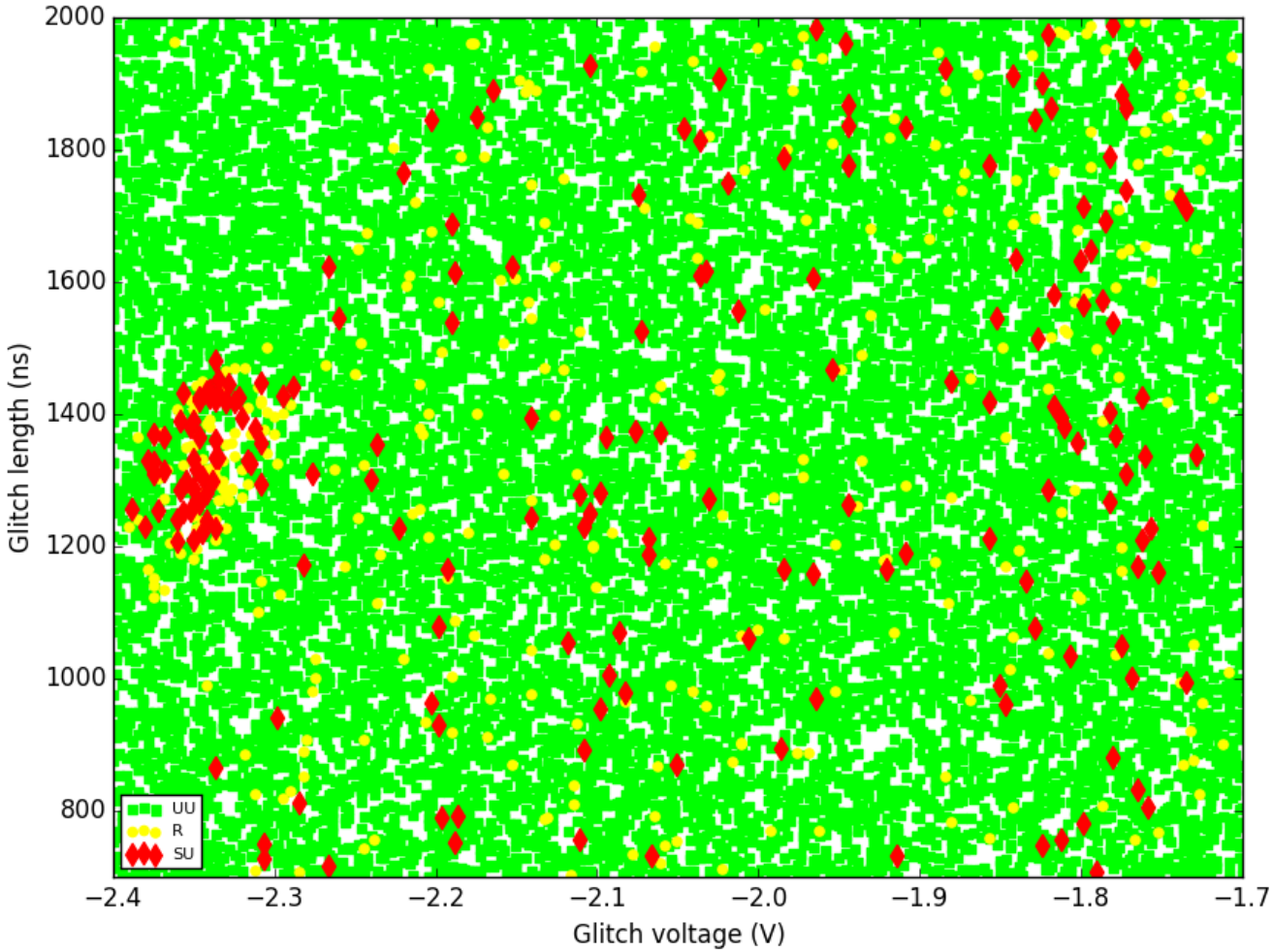
JTAG

NXP power JTAG length vs. voltage, binned offset (125ns) 3/4

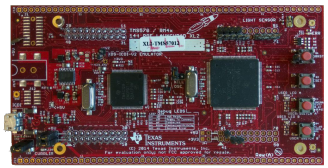
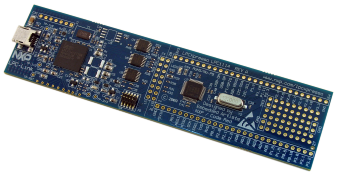


JTAG

NXP power JTAG length vs. voltage, binned offset (125ns) 4/4



JTAG

Target	Successful	Detected
 TI (power)	1.4%	4.5%
 NXP (power)	80%	0%*

Conclusions

- These specific hardware countermeasures not good enough for detection by themselves
- Of the mechanisms, lockstep most effective as countermeasure
- Proper mitigation requires additional measures, either additional in hardware or in software

TODO

- Present findings at ESCAR USA (June)
- Produce paper to submit to FDTC (June, September)
- Perform JTAG experiments on STMicro target (the blue one)
- Experiment with popular automotive protocols (UDS)

TODO (open)

- Test other targets (Infineon TRI(!) core lockstep)
- Test actual ECUs
- Create automotive pinata-like board
- Expand data on used targets (more extensive EM on TI target)
- Investigate relationship between countermeasure parameters and detection rate
- Investigate effect of adding software countermeasures