riscure

Glitch it if you can: parameter search strategies for successful fault injection

Rafael Boix Carpi[1], Stjepan Picek[2,3], Lejla Batina[2], Federico Menarini[1], Domagoj Jakobovic[3] and Marin Golub[3]

[1]Riscure BV, The Netherlands

[2]Radboud University Nijmegen, The Netherlands

[3]Faculty of Electrical Engineering and Computing, Zagreb, Croatia

CARDIS 2013, Berlin

Agenda

FI parameters problem

Proposed strategies

Findings, conclusions

Future working lines

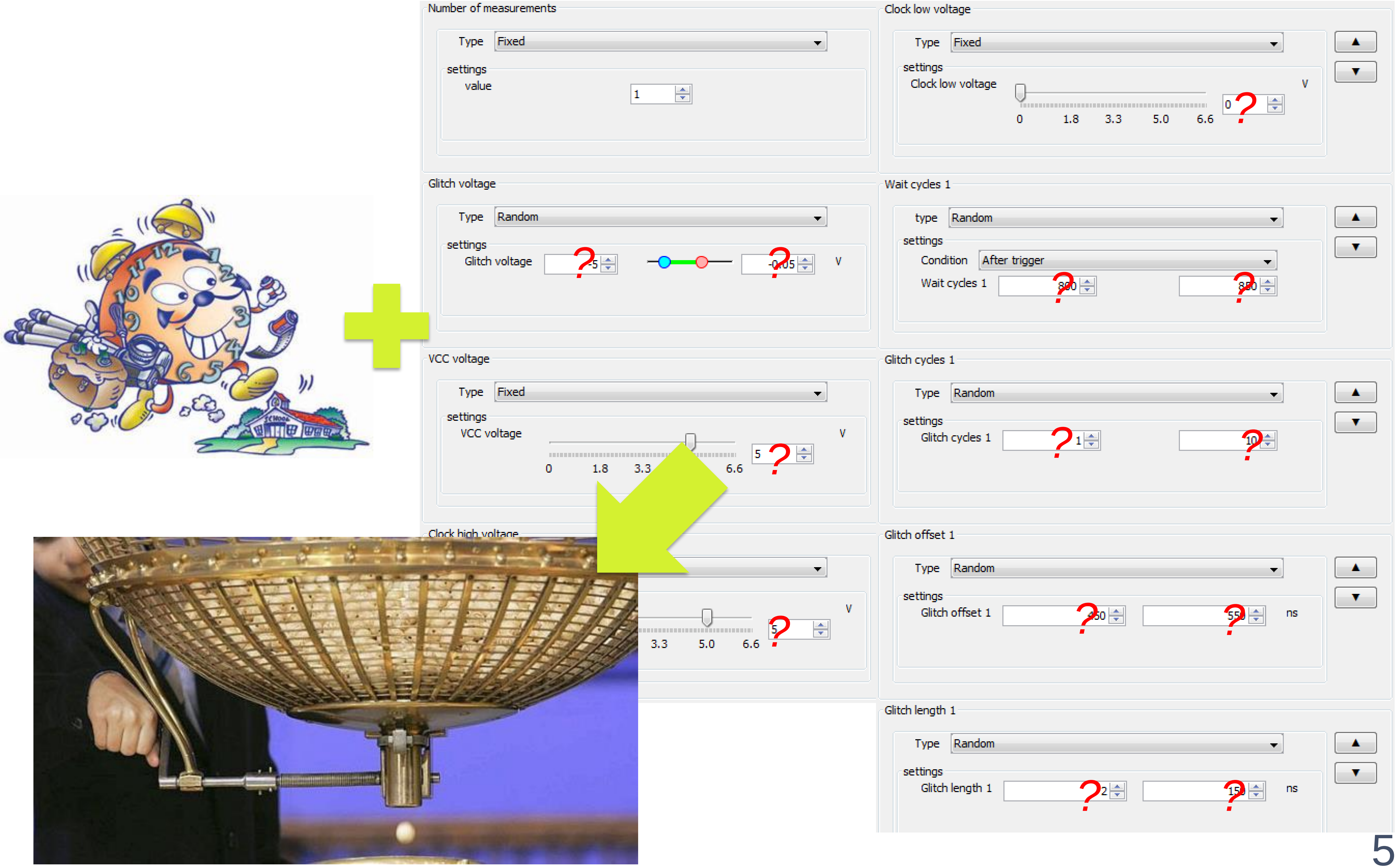
1 FI parameters problem

Proposed strategies

Findings, conclusions

Future working lines

Context of the problem



Number of measurements
Type: Fixed
settings
value: 1

Clock low voltage
Type: Fixed
settings
Clock low voltage: 0 V

Glitch voltage
Type: Random
settings
Glitch voltage: -5 – -0.05 V

Wait cycles 1
type: Random
settings
Condition: After trigger
Wait cycles 1: 800 – 850

VCC voltage
Type: Fixed
settings
VCC voltage: 5 V

Glitch cycles 1
Type: Random
settings
Glitch cycles 1: 1 – 10

Clock high voltage
settings: 5 V

Glitch offset 1
Type: Random
settings
Glitch offset 1: 450 – 550 ns

Glitch length 1
Type: Random
settings
Glitch length 1: 2 – 150 ns

Problem statement

- Can we automatically find good values for parameters **using few measurements**?

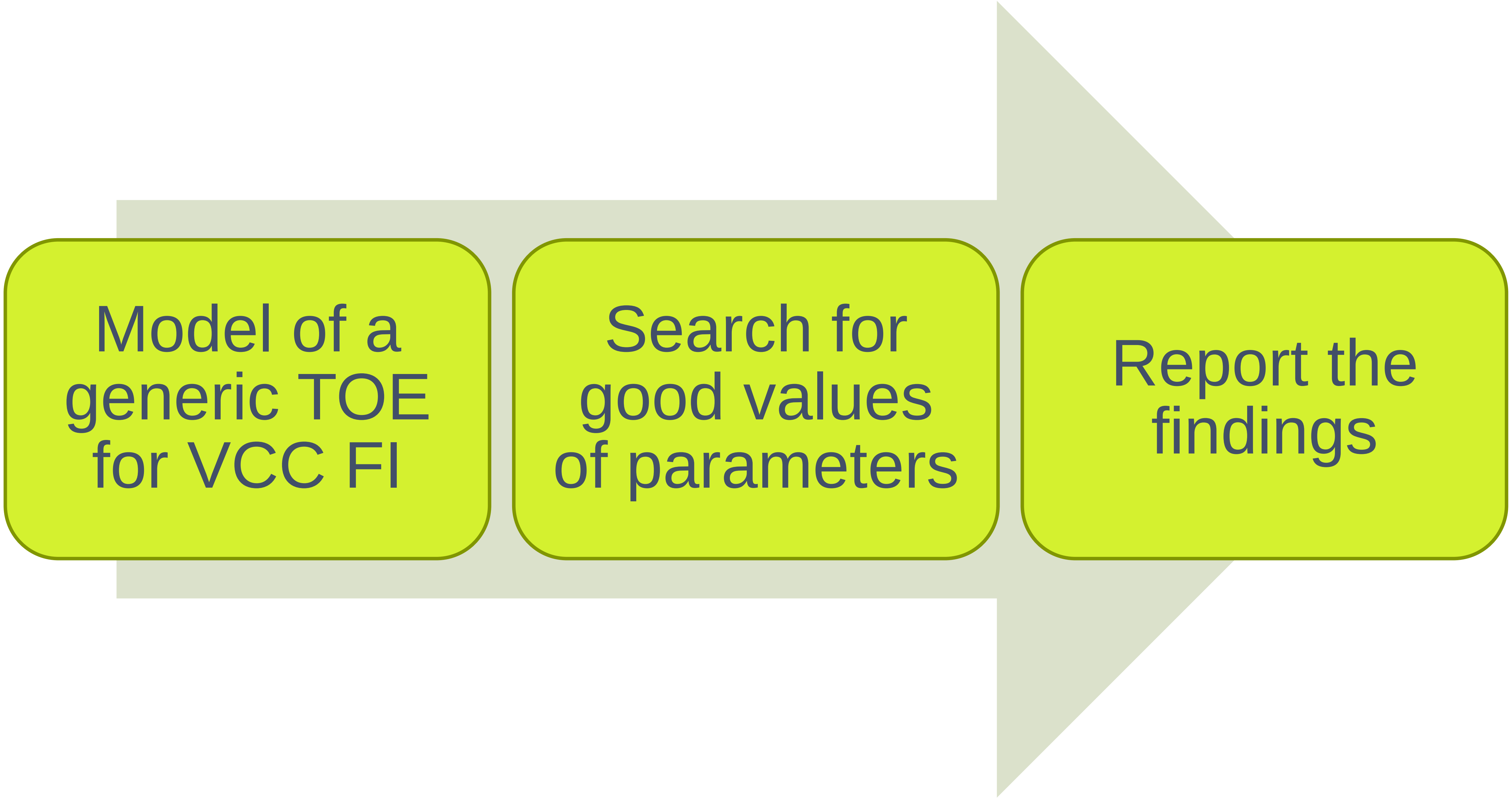
FI Parameters problem

2 Proposed strategies

Findings, conclusions

Future working lines

Roadmap for auto-setting parameters

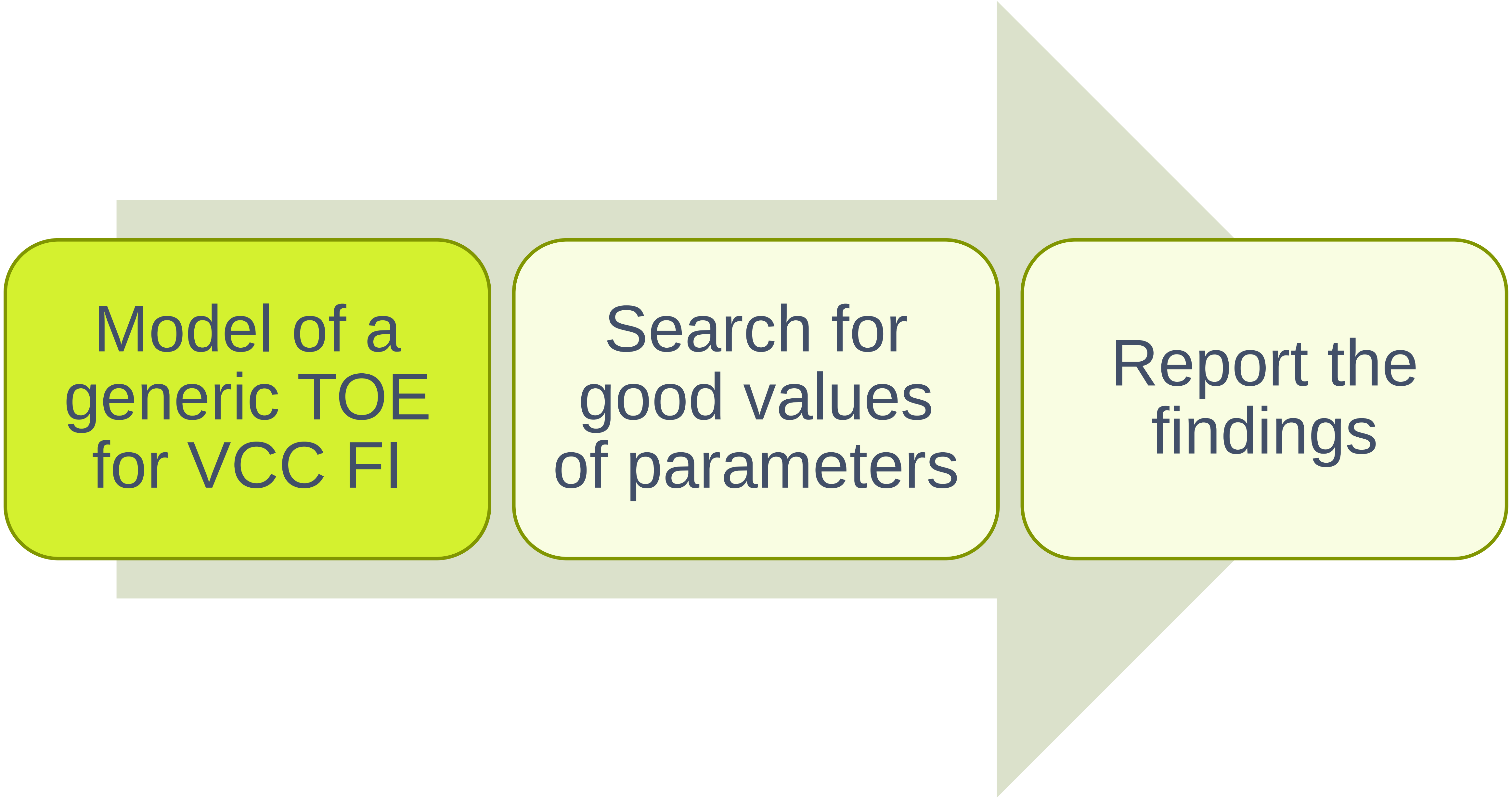


Model of a generic TOE for VCC FI

Search for good values of parameters

Report the findings

Roadmap for auto-setting parameters



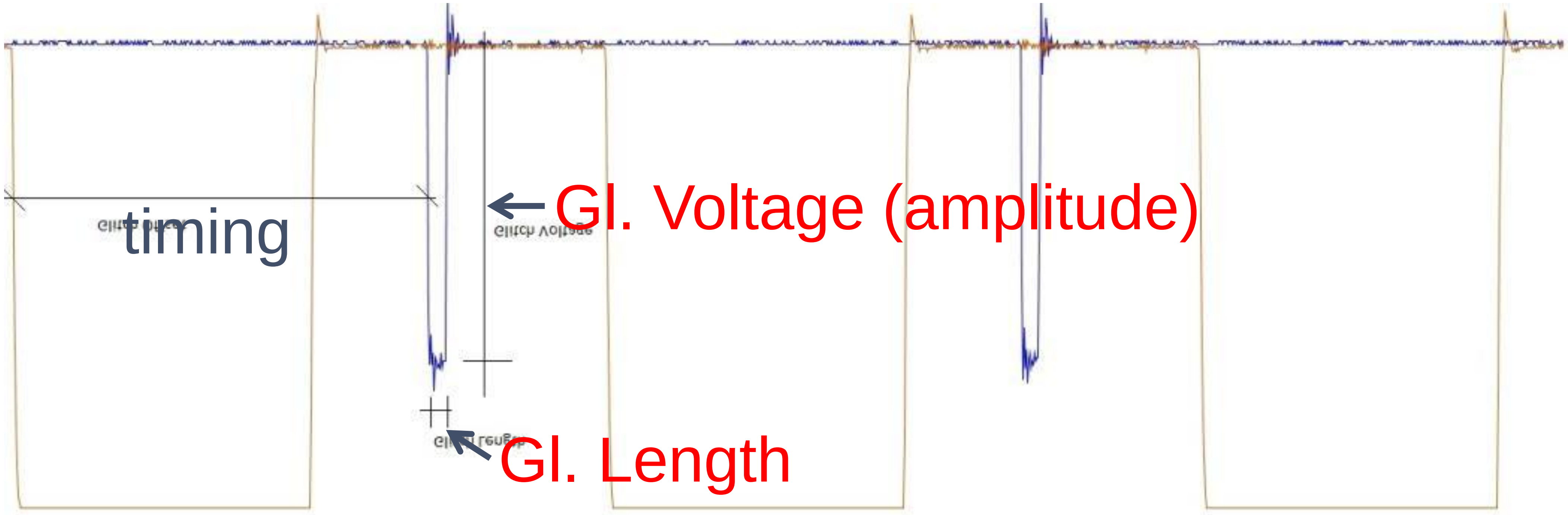
Model of a generic TOE for VCC FI

Search for good values of parameters

Report the findings

What do we know about VCC FI and a generic TOE?

- A glitch:

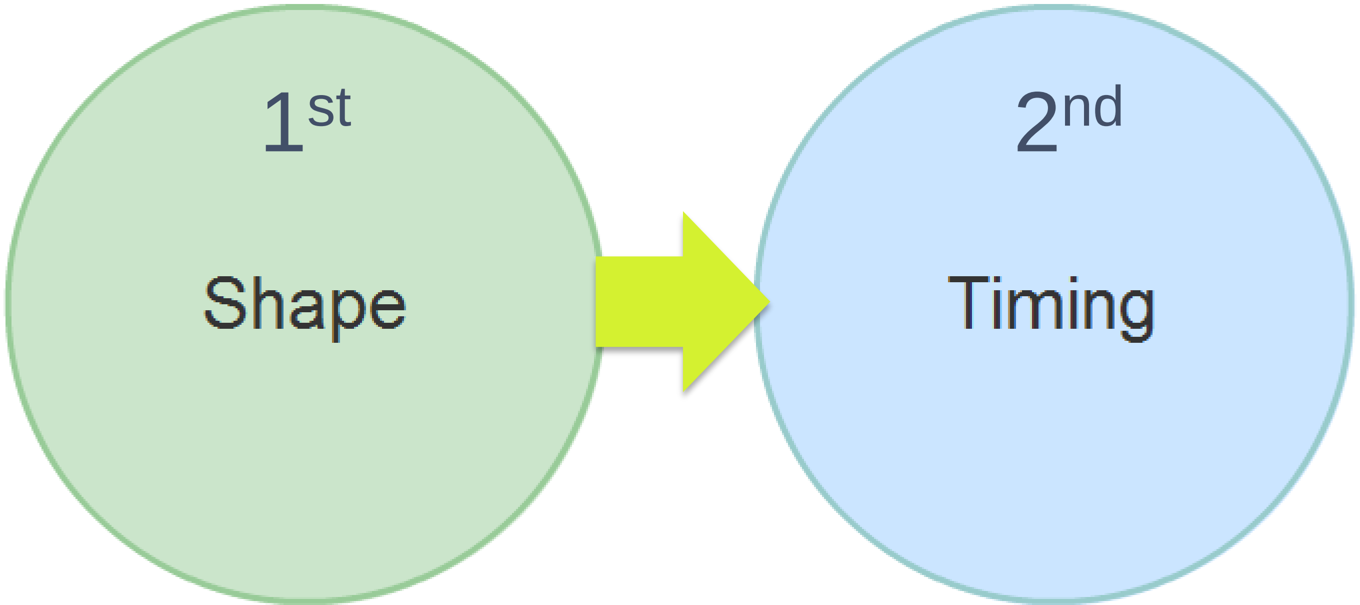


timing

Gl. Voltage (amplitude)

Gl. Length

- Parameter sets



1st

Shape

2nd

Timing

Doing this separation:

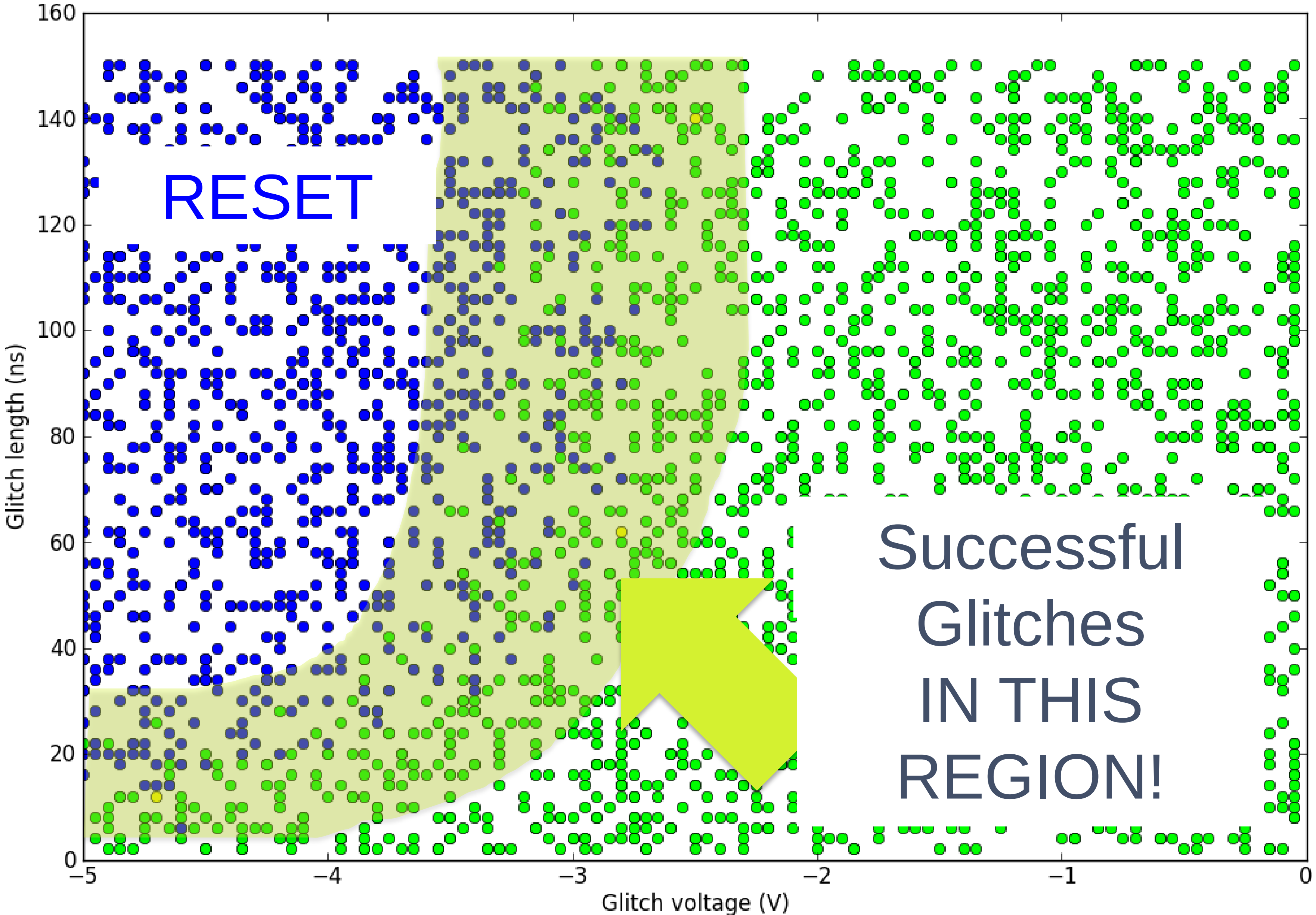
➢ Reduces problem complexity

What do we know about VCC FI and a generic TOE?

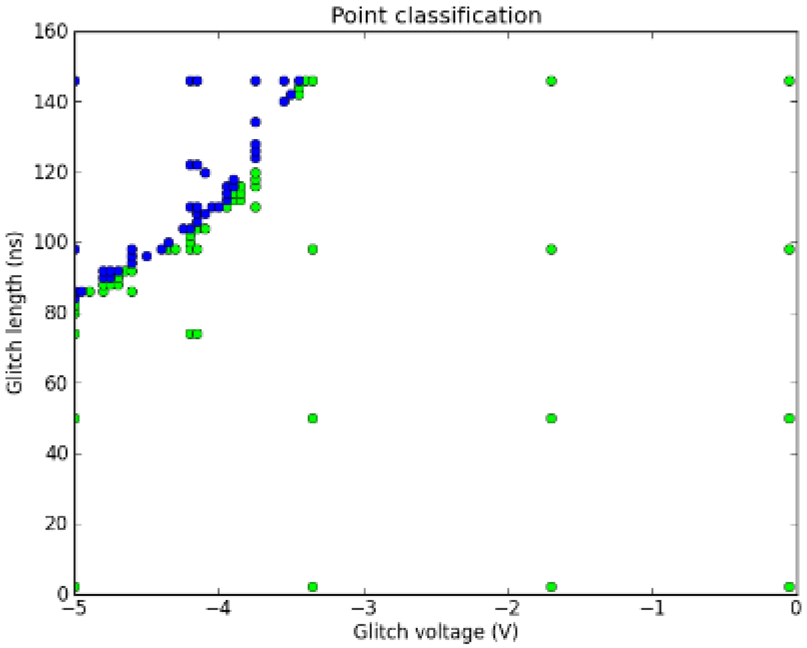
Physical behavior of a generic TOE w.r.t. Shape

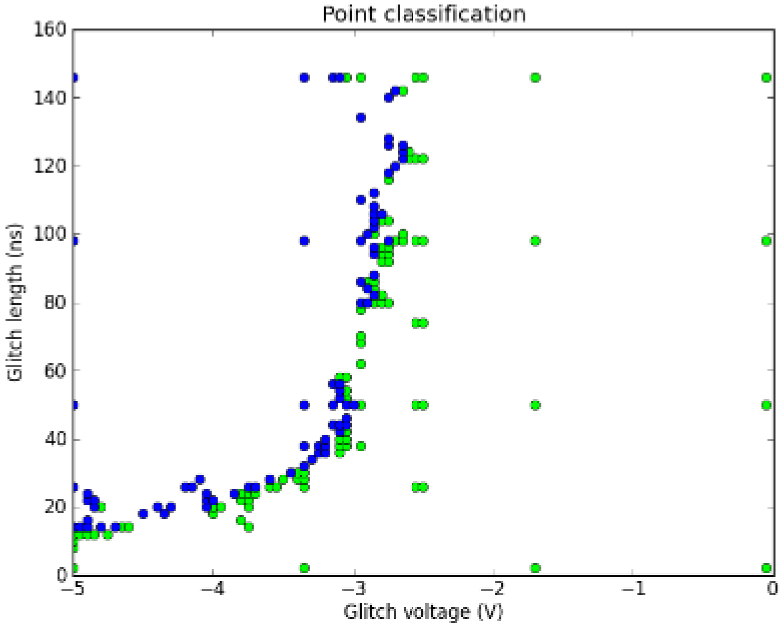
Example: Target A (unprotected smartcard)

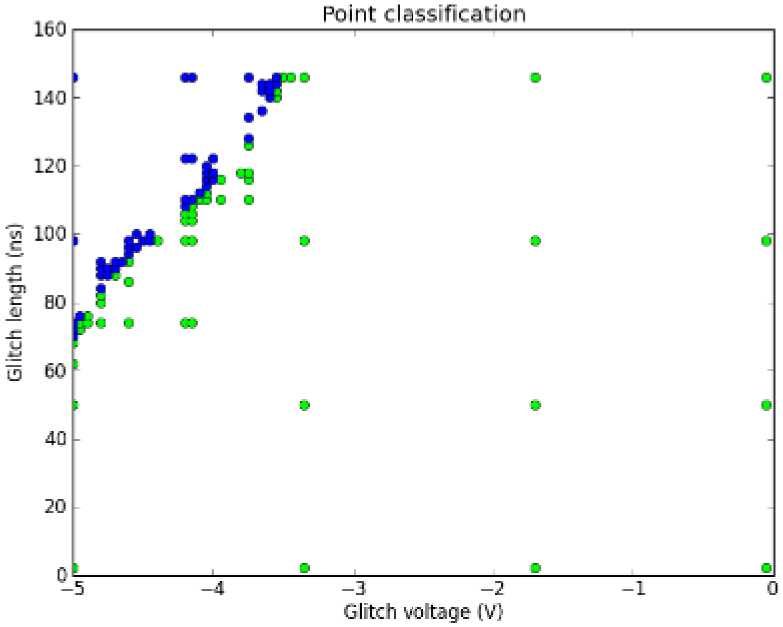
- Glitch Voltage [-0.05,-5]V, gl. Length [2,150]ns
- Timing properties: random values within stable IC operation

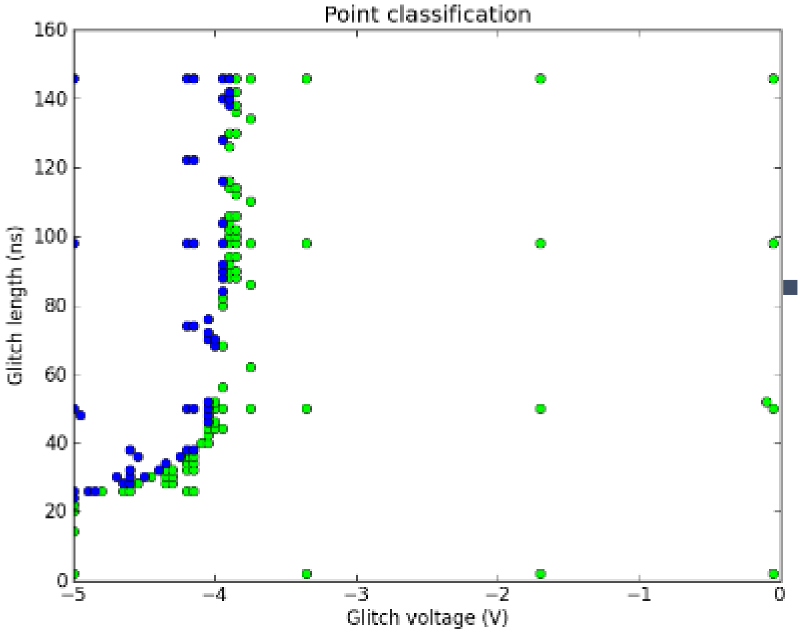


All TOEs we analyzed so far…









…showed this behavior w.r.t.

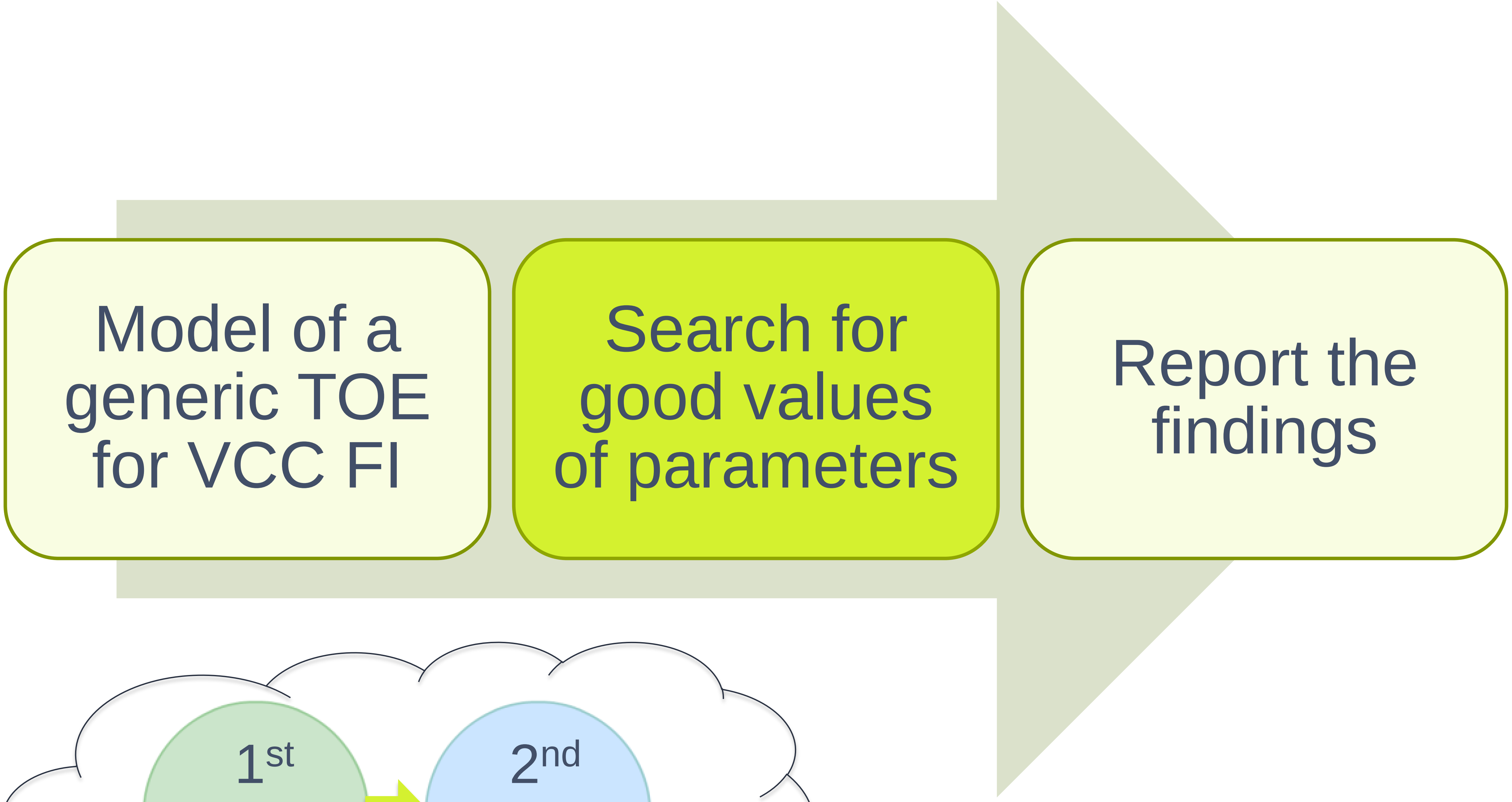
Shape

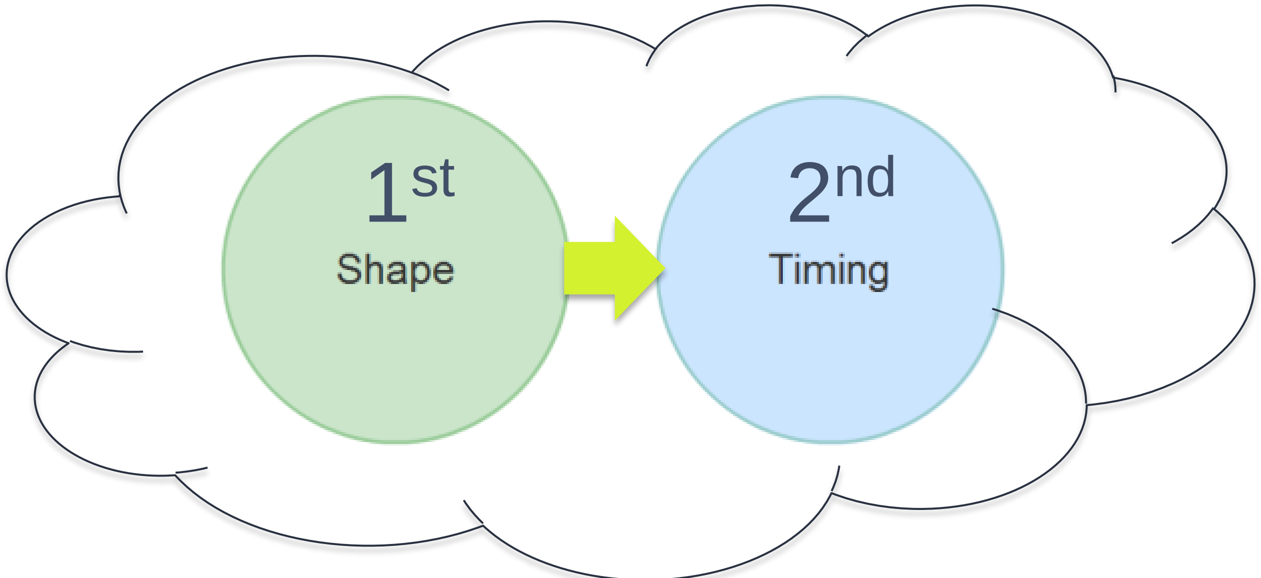
What do we know about VCC FI and a generic TOE?

Physical behavior of a generic TOE w.r.t.

- External clock + predictable code path = PREDICTABLE TIMING
- The rest = UNPREDICTABLE TIMING

Roadmap for auto-setting parameters

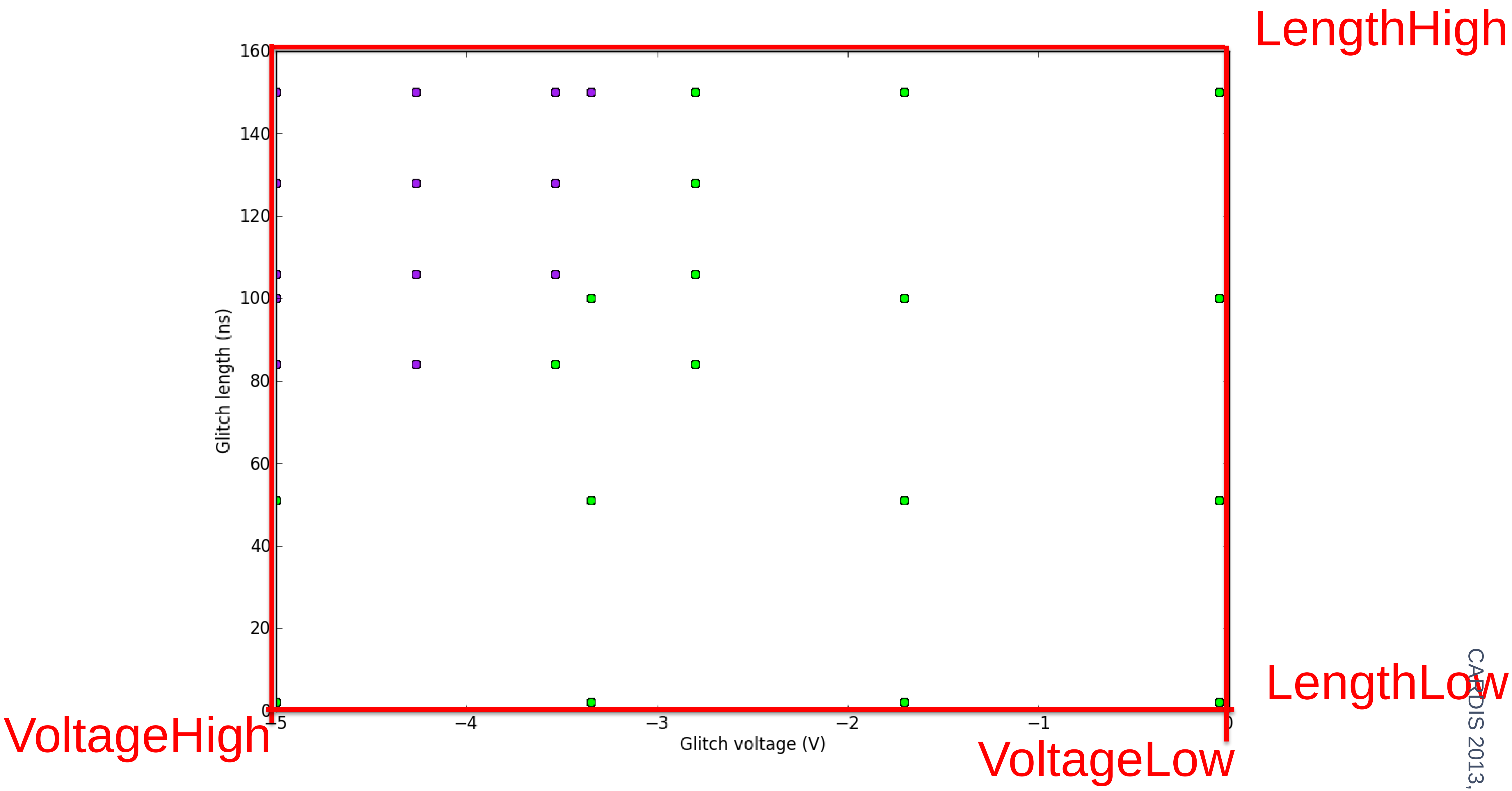

Model of a generic TOE for VCC FI
Search for good values of parameters
Report the findings



Proposed search strategies

- FastBoxing
  - Coarse, proof of concept strategy
- Adaptive zoom & bound
  - Focus on efficiency
- Genetic algorithm
  - Focus on general applicability

Proposed strategy: FastBoxing

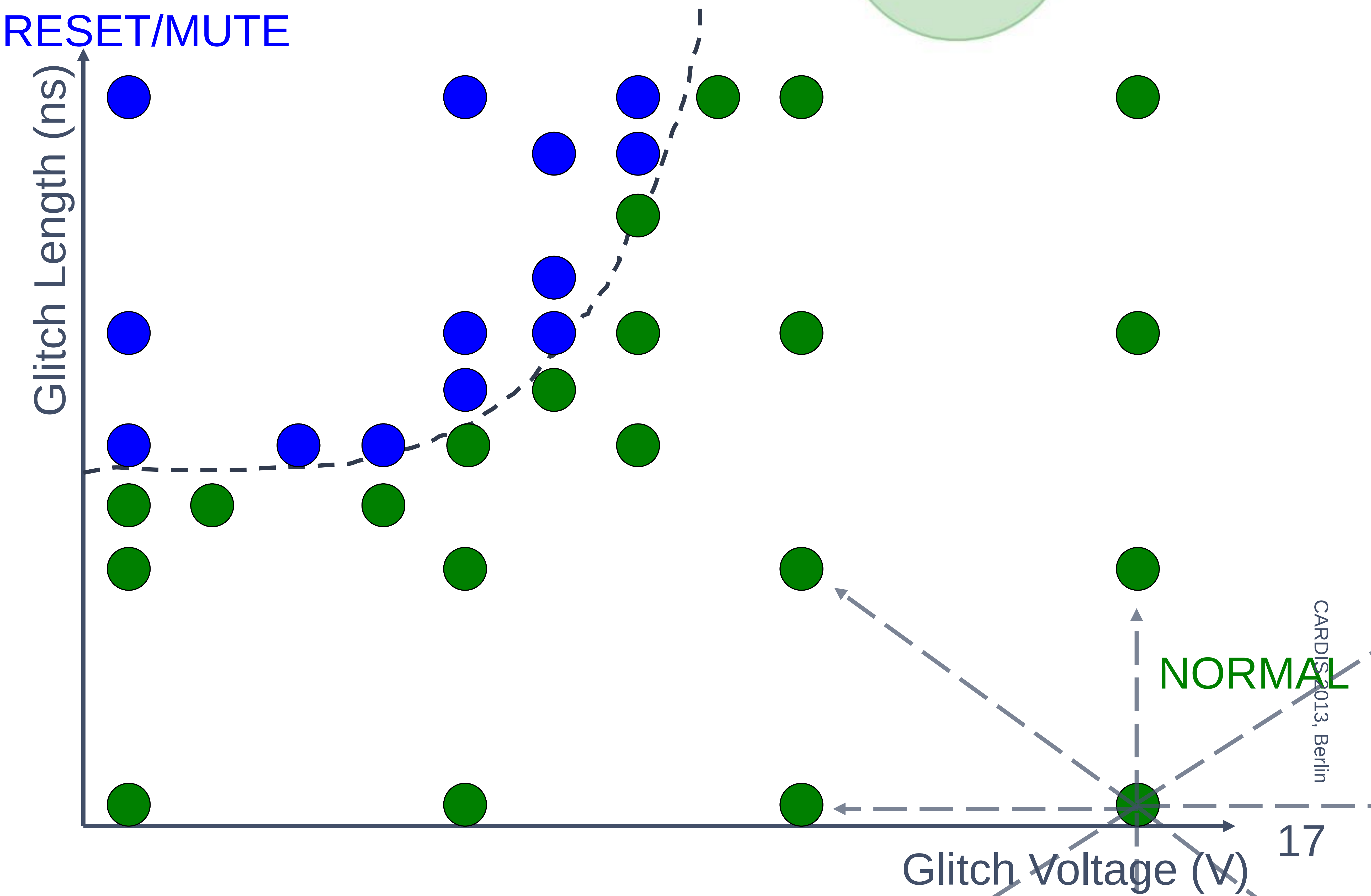


GREEN:=EXPECTED

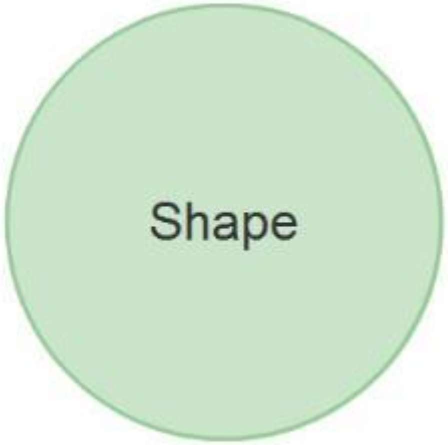
PURPLE:= MUTE

Proposed strategy:
Adaptive zoom & bound

Shape



Proposed strategy 1st stage: Adaptive zoom & bound



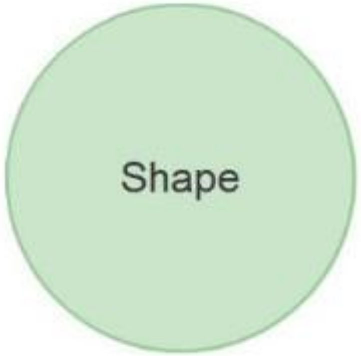
Theoretical performance:

- Number of measurements: 112

Observed performance:

- Protected targets, 1 measurement per point: 128~160
  Unprotected target,1 measurement per point:160~200
- Protected targets, 3 measurements per point: 600~800
- Unprotected target, 3 measurements per point: 800~900

Proposed strategy 1st stage: Genetic Algorithm

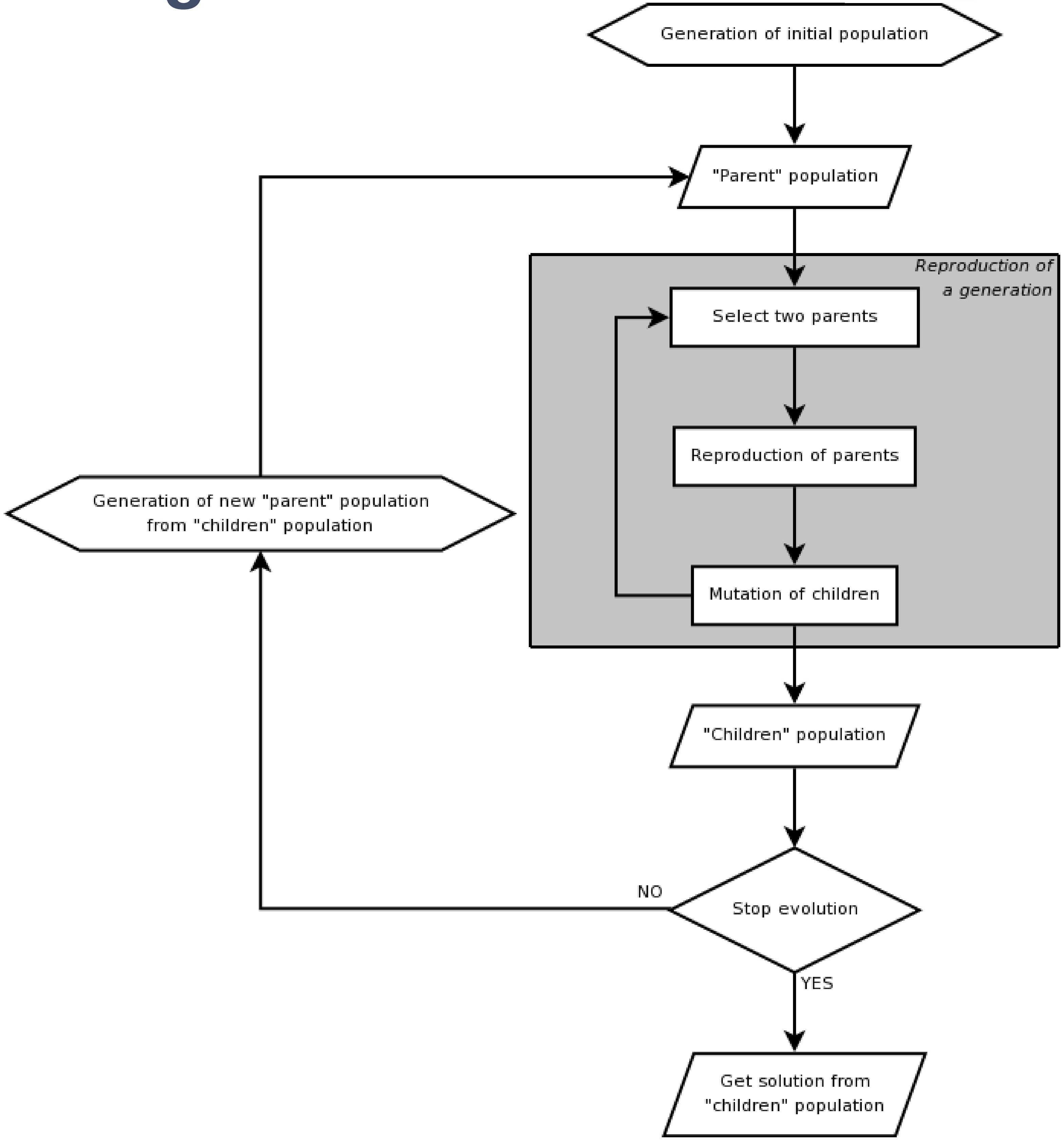


Shape

- Finding correct settings in minimal amount of time can be considered an optimization problem
- We need to map fault classes to fitness values
- Also change the operators to work better for this problem
- We do not look for only one good soultion but for all the solutions that have fitness above treshold value

Proposed strategy 1st stage: Genetic Algorithm

Shape



Generation of initial population

"Parent" population

Reproduction of a generation

Select two parents

Reproduction of parents

Mutation of children

"Children" population

Stop evolution

NO

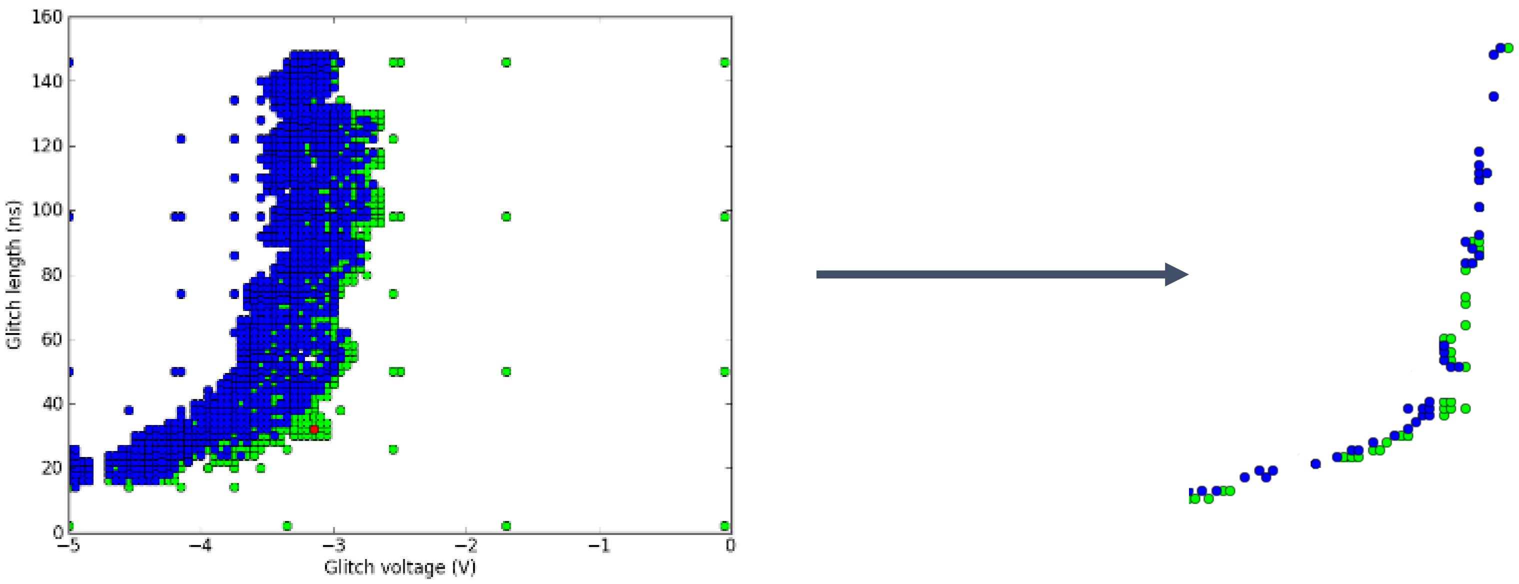
Generation of new "parent" population from "children" population

YES

Get solution from "children" population

2nd search stage: sweep in time domain

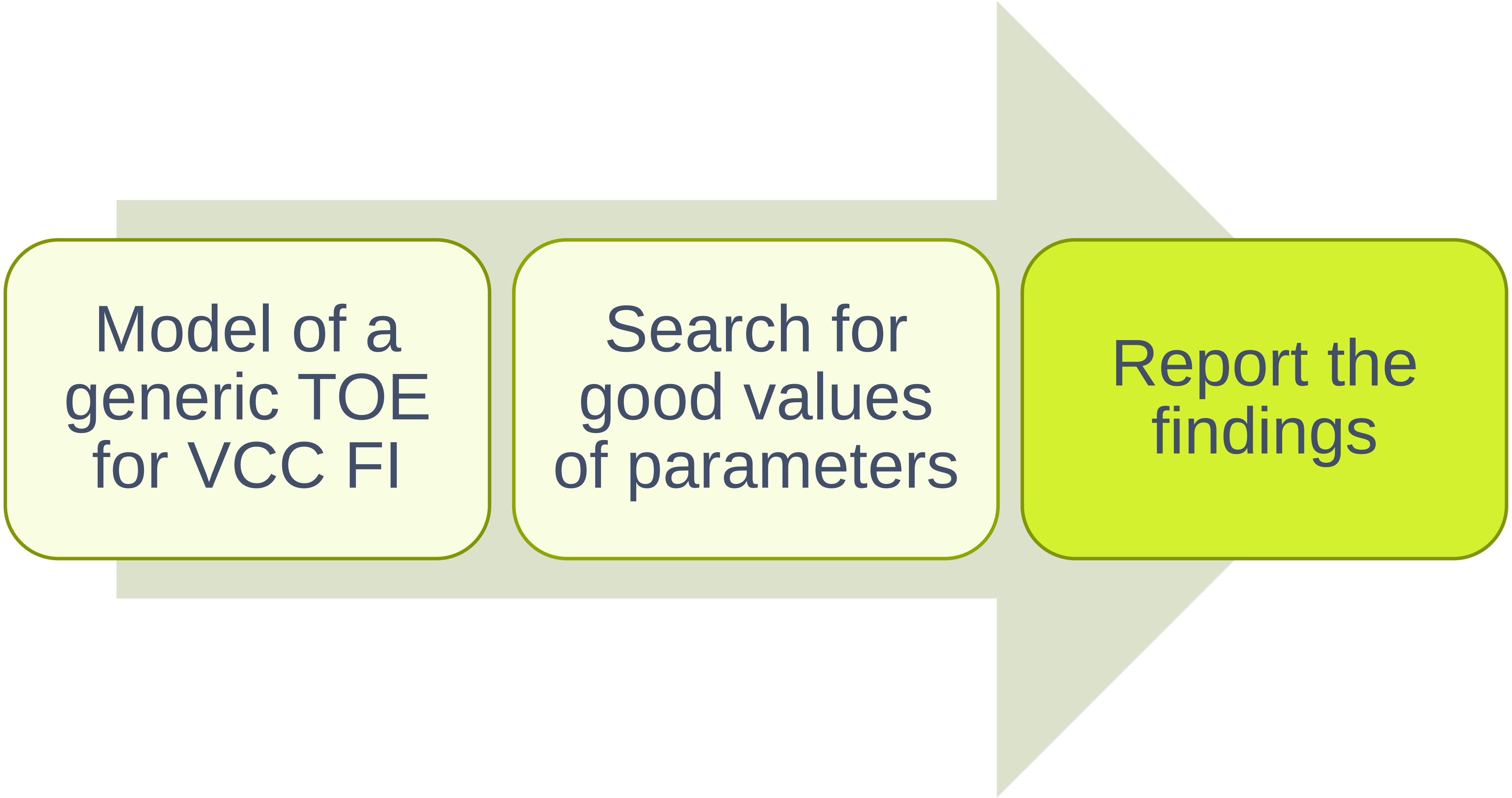
1 - Sample points from the boundary between classes (FastBoxing and Adpative Zoom&bound) or output (GA)



2 – Perform a time sweep:

- Predictable timing: one sweep, minimum step between instants
- Unpredictable timing: multiple sweeps

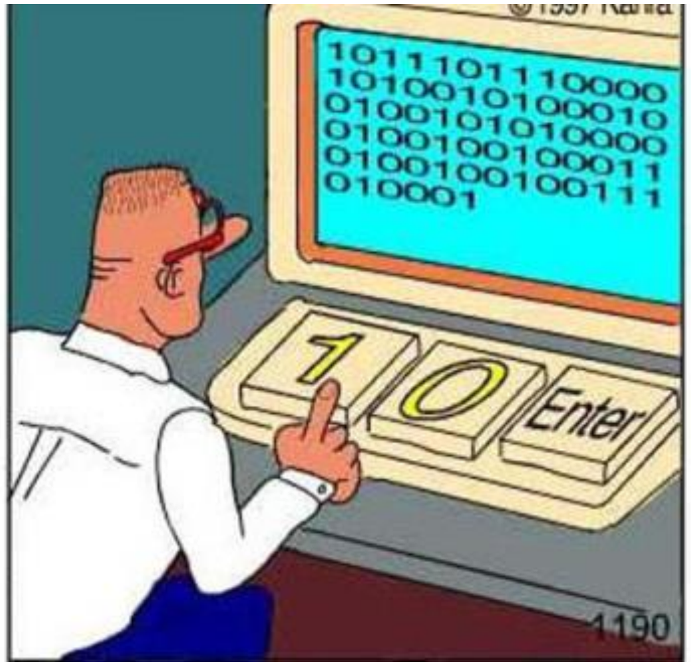
Roadmap for auto-setting parameters



Model of a generic TOE for VCC FI

Search for good values of parameters

Report the findings



FI Parameters problem

Proposed strategies

3 Findings, conclusions

Future working lines

Results: Target A (unprotected TOE)

MonteCarlo search

- 3072 measurements each run
- Successful parameter configurations (median): **0**
- 1 run, 76800 measurements (1.5 days): 11 succesful configs.

FastBoxing search

- 3048 (2048 1st stage+1000 2nd stage) measurements each run
- Successful parameter configurations (median): **9**

Adaptive zoom & bound search

- 1198 (**198** 1st stage+1000 2nd stage) measurements (median)
- Successful parameter configurations (median): **13**

Genetic Algorithm

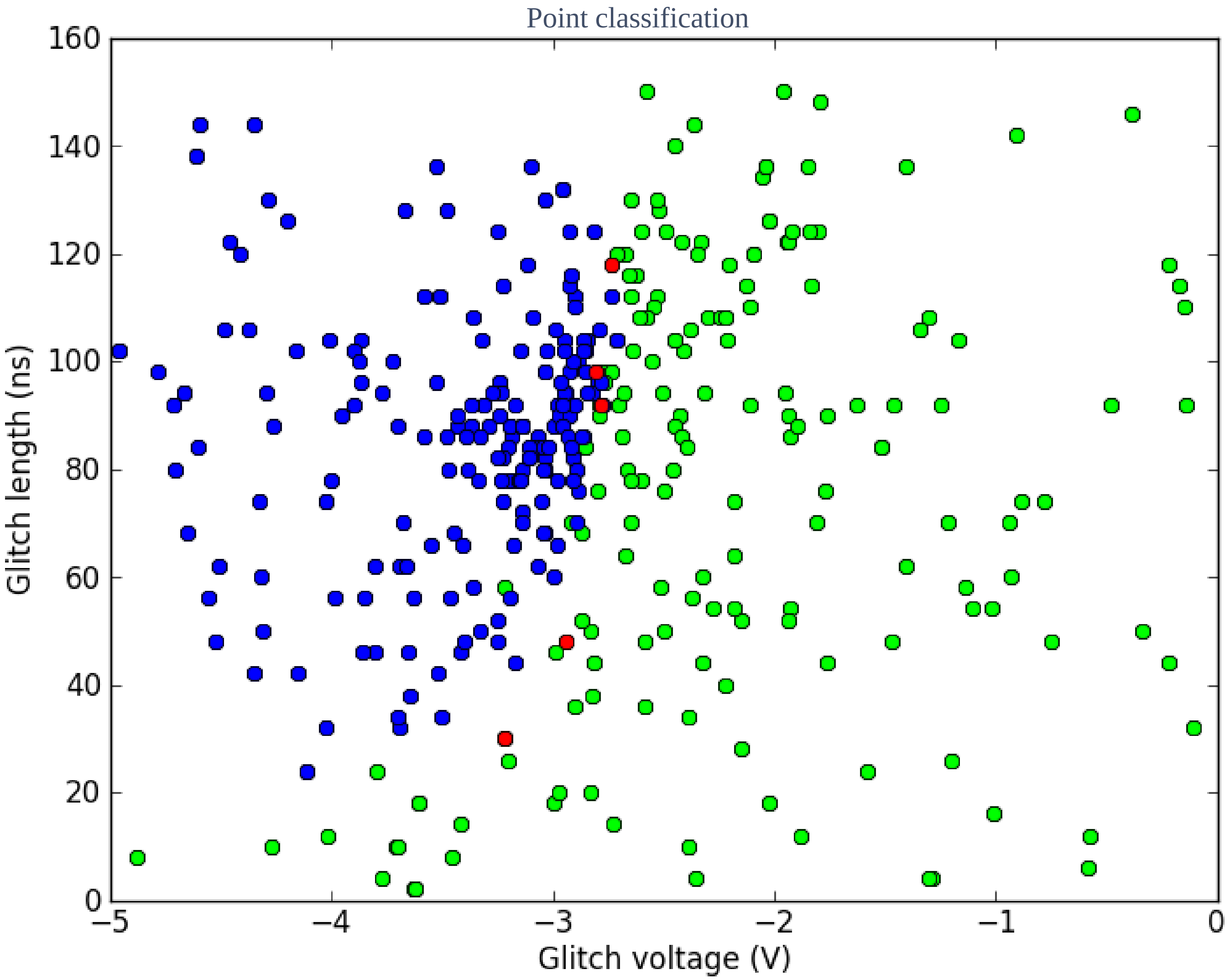
- 2560 (1560 1st stage+1000 2nd stage) measurements each run
- Successful parameter configurations (median): **8**

Results: Target A (unprotected TOE)

- All proposed strategies are more efficient than MonteCarlo search
- Adaptive zoom & bound is the *fastest*
- New idea - go to memetic algorithm
  - Memetic algorithm is a combination of a genetic algorithm and local search
  - It encompasses the advantages of both the Genetic Algorithm and Adaptive zoom & bound.

Results: Target A (unprotected TOE)

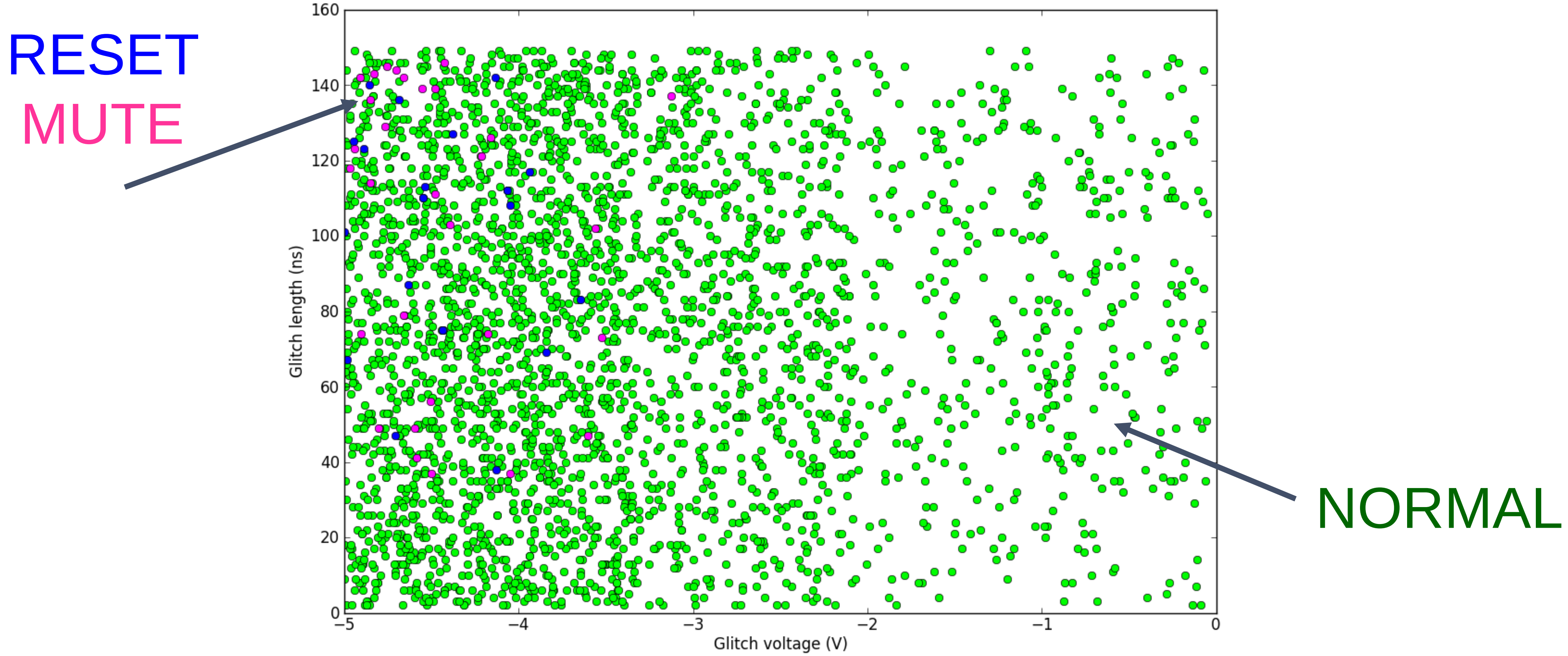
- Sample plot of GA for the Glitch Shape



8 success

Results: Target C (protected smartcard)

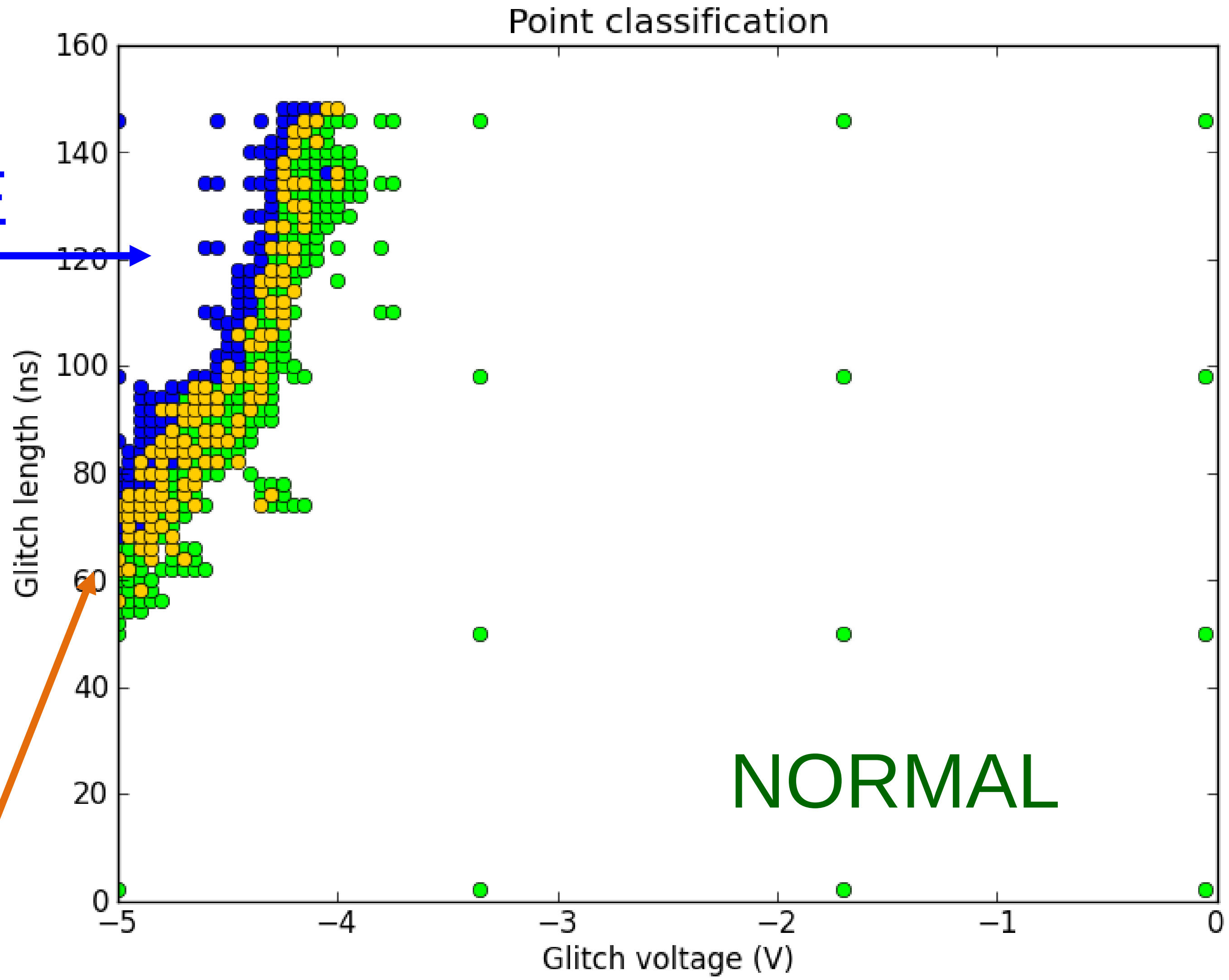
- Plot of MonteCarlo sampling for 2.5 samples of Target C (overlapped)



- Less than 100 resets&mutes
- >6000 measurements yielded nothing interesting

Results: Target C (protected smartcard)

- Plot of Adaptive Zoom & Bound for the Glitch Shape



RESET/MUTE

NORMAL

~600 measurements

ORANGE:=different response types in different time instants

Findings with target C and Adaptive zoom & bound

- Adaptive zoom&bound uses few measurements: usually less than 200 measurements for finding suitable glitch shapes.
- Search is focused in an interesting region for the glitch shape.
- Good information in this explored search space.
- Multiple measurements mitigated the clock jitter effect.
- Results for glitch shape are exportable to different samples of the same device.

Hidden parameters: Successful glitches with respect to…

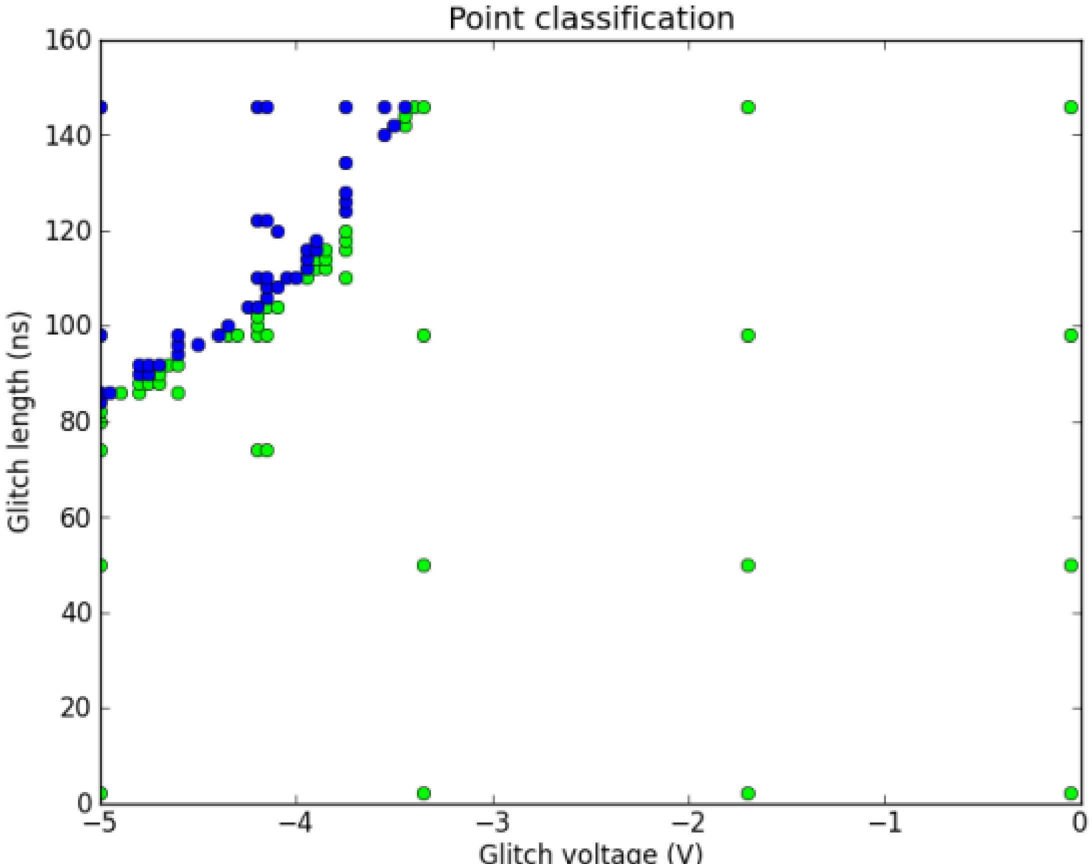
- Number of glitches in consecutive cycles
  - No dependency (in general)
- Frequency
  - No dependency (1~4MHz tested)
- Glitch offset inside clock cycle
  - Only relevant to TOEs running only on external clock.
- Temperature
  - Exists dependency, not controllable with the experimental setup.

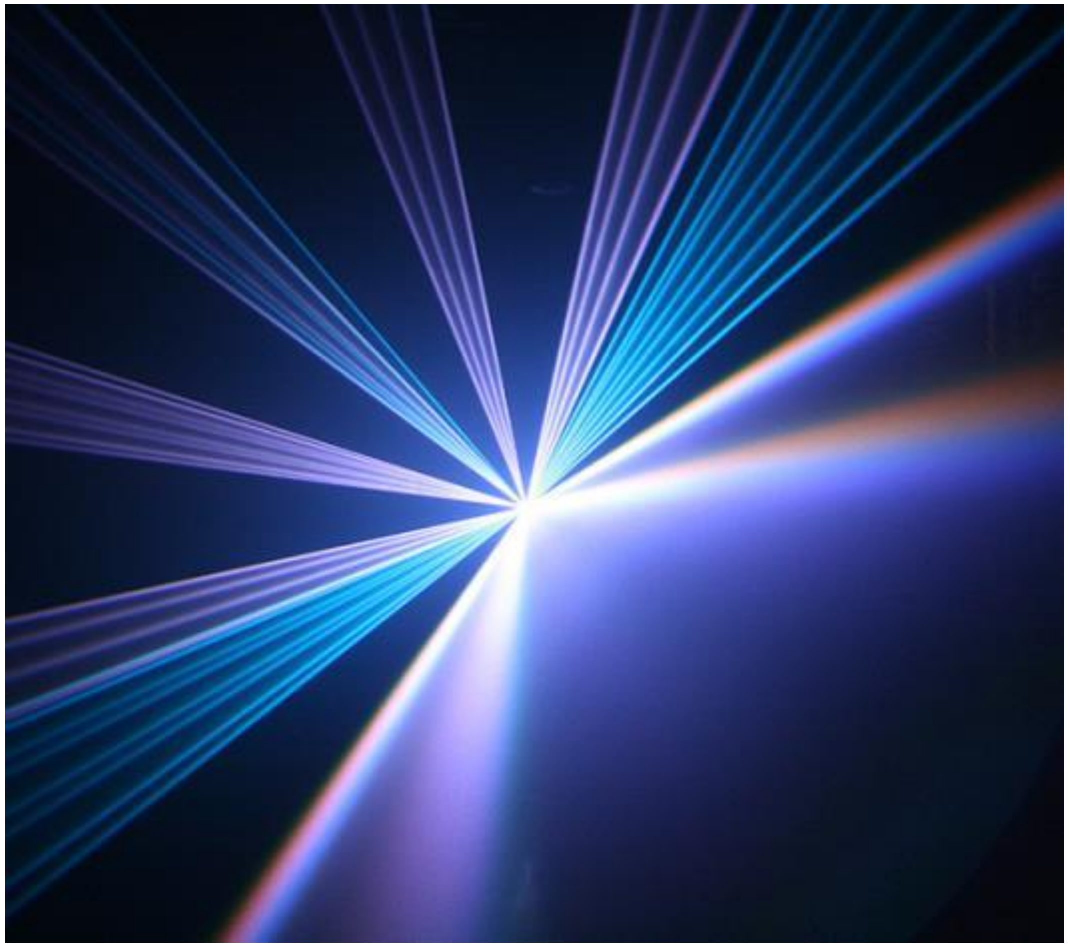
Conclusions

With few measurements, we can get big information.

Glitch shapes found in the boundary between NORMAL and RESET/MUTE are interesting.

Finding this boundary can be performed really fast.





FI Parameters problem

Proposed strategies

Findings, conclusions

4 Future working lines

Future working lines

- Adaptive zoom & bound
  - Implement side channel information in the feedback loop.
- Genetic Algorithm
  - Improvements in the direction of memetic algorithms
- Further testing
  - Extensive testing with other devices: embedded TOEs, more smartcards.

riscure

Challenge your security

Contact: Rafael Boix Carpi
Security analyst & trainer
BoixCarpi@riscure.com

Riscure B.V.
Frontier Building, Delftechpark 49
2628 XJ Delft
The Netherlands
Phone: +31 15 251 40 90

www.riscure.com

Riscure North America
71 Stevenson Street, Suite 400
San Francisco, CA 94105
USA
Phone: +1 650 646 99 79

inforequest@riscure.com