Evaluating the Effectiveness of 2OE Methods to Mitigate Specific Supply Chain Risks

Brendan Foran
Electronics and Photonics Laboratory
The Aerospace Corporation

4/22/2021

© 2021 The Aerospace Corporation

Outline

- Why we are evaluating second order effects testing methods
- What second order effects are and who are the players
- Aerospace’s FPGA-based Test bed
- Results and analyses
- Conclusions

Acknowledgements

- Carl Boone, Dmitry Veksler, Sean Stuart – conducted all data collection and analysis
- Vikram Rao, Garrett Chan, and Salam Zantout – developed the FPGA code with Trojans insertions
- Paiboon Tangyunyong (Sandia) helped us to understand, adapt, and evolve on his PSA method
- Richard Ott (AFRL) encouraged participation with JFAC-ASSESS Working Group
- Rebecca McKenna (Aerospace) for encouragement via the Verification Sciences & Engineering program
- Much of this work has also been funded by The Aerospace Corporation’s iLab Ventures program

Evolving Reliability Needs

- Changing perspectives for space missions
  - *Commercial and broader nation-state access*
  - *Increased focus on resiliency and agility*

- Pressure to use state of the art (SOTA) and commercial off the shelf (COTS)
  - *Commercial vs. space-qualified parts reliability*
  - *Changes risk and vulnerability aspects critical to hardware security*

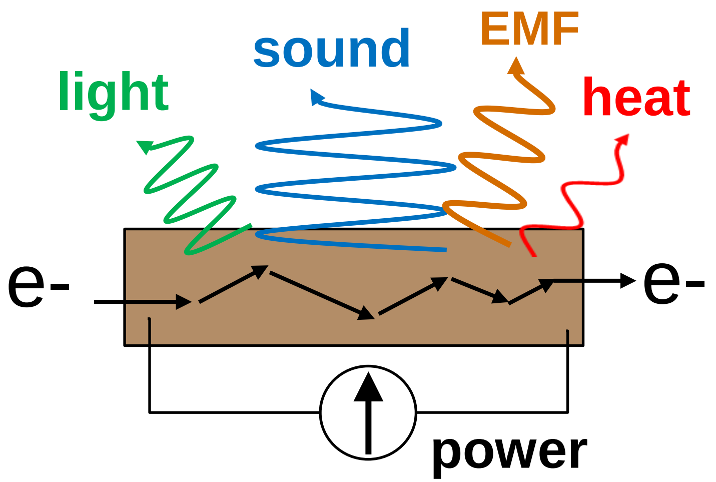
- Speeding technology insertion
  - *Model based systems engineering (MBSE) and Digital Engineering (DE)*
  - *Test in flight and continuous product improvement*

- Changing Trust, hardware assurance and program protection perspective
  - *Connection to OSD T&AM, MINSEC and DARPA activities*
  - *Need new ways to screen parts for variability and vulnerabilities to mitigate risk*

Quantitative Assessment of Second Order Effects (2OE) Capabilities

2OE testing has been proposed for screening counterfeits and reliability escapes

- 2OE are characteristics beyond the purpose-designed functionalities
  - *Related to physical implementations: design and manufacturing*
  - *Power absorption, emission of energy as devices operate*

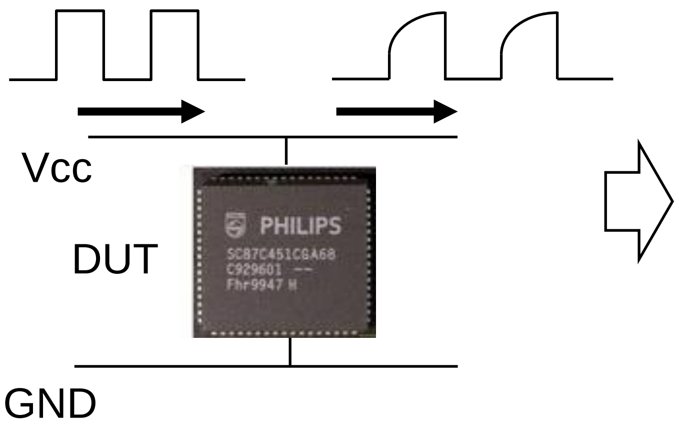


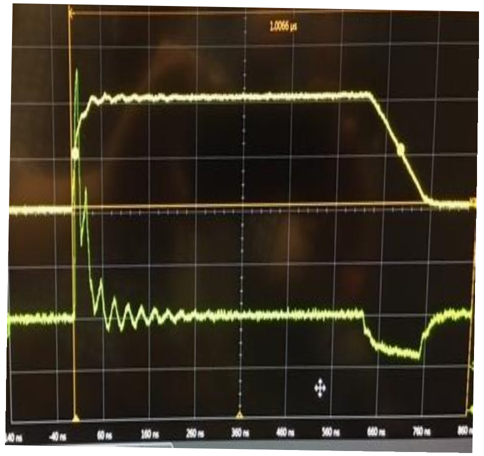
- Second Order Effects (2OE) can identify physical changes
  - *Different chips or “same chip” ported to a new node or fab-process, or packaging modifications,*
  - *Radiation exposure, aging and wear-out damage*

Aerospace has focused R&D to understand limitations and paths to optimize 2OE methods

Broad Range of 2nd Order Effects "Systems"

- Battelle's Barricade™
  - *power waveforms collected under various test conditions*
- Lincoln Laboratories' SICADA™
  - *power side channel analysis for test vectors*
- Nokomis' ADEC™
  - *RF emissions collected under various test conditions*
- Robson Technologies
  - *analyzes curve trace data*
- Sandia's Power Spectrum Analysis (PSA)
  - *"off-normal" power signatures via sub-threshold square wave injection*





- Also: PFP Cybersecurity, ABI Sentry, Aprel EM-Isight, and Applied Research Associates, PRISM, …?

- What types of signals are collected, under what stimuli, how data is sorted, compared, and used to make decisions
  - *Many offer sample-specific system "training" to optimize their methods*

- AFRL-led JFAC "ASSESS Working Group"
  - *Evaluating 2OE systems via 1) standardized test articles, 2) systematic and controlled test strategy, and 3) common metrics*

- DMEA "Machine Vision Technologies" pilot program @ UMD-CALCE:
  - *"Applications of Machine Learning and Machine Vision to Determine the Authenticity and Security of Microelectronics Parts…"*

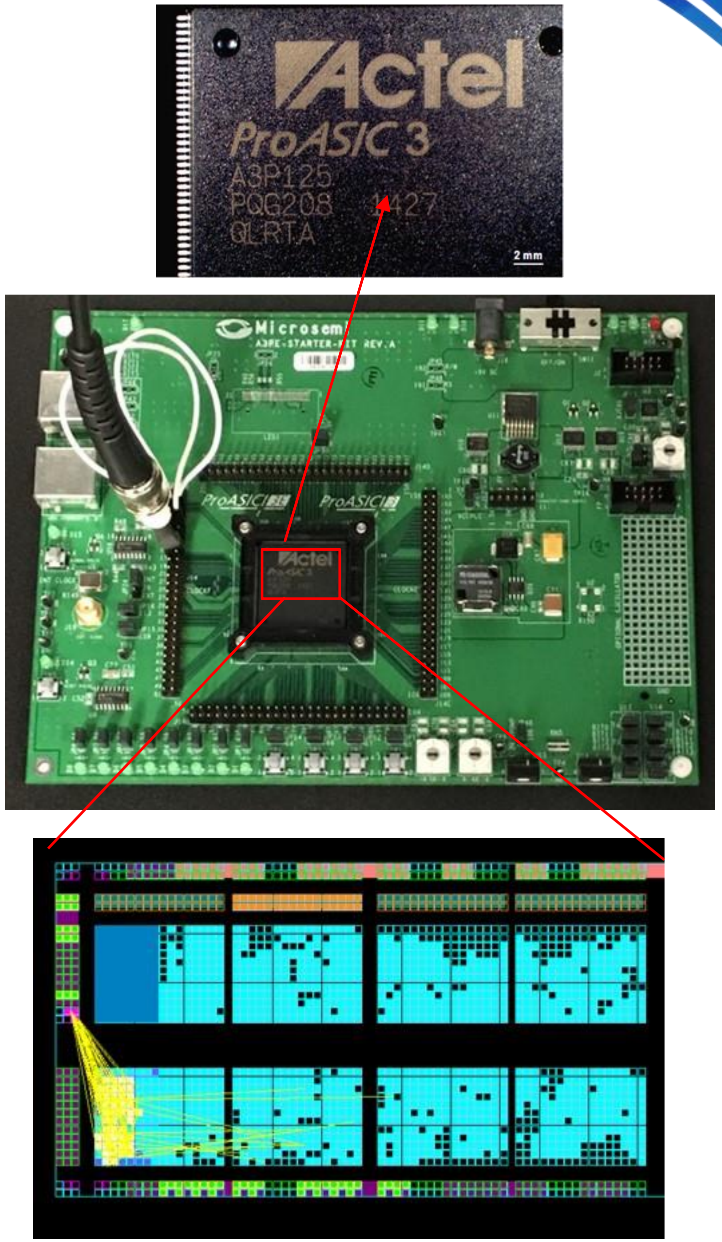
Aerospace's FPGA-Based 2OE Test-bed

- Suitable FPGA: Microsemi ProASIC-3 (A3P125)
  - *Flash-type configuration bits stay programmed when powered off*

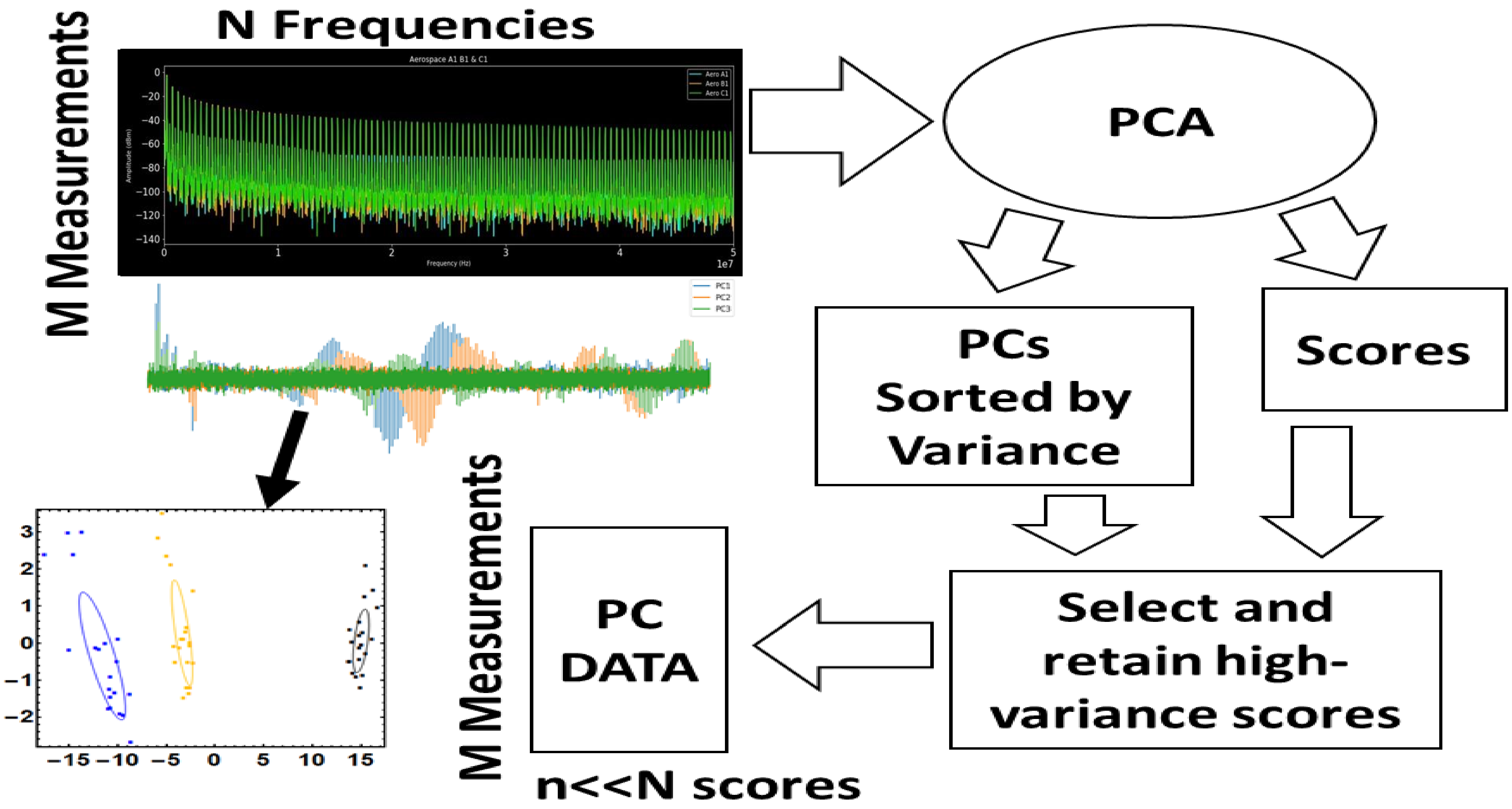
- Host circuit modified by hardware Trojans of variable functionality (trigger and payload), size, and layout:
  - *<u>Golden SpaceWire (SW): 60% of FPGA resources used</u>*
  - *<u>SW + Large Trojan: 90% of the FPGA used (30% HT)</u>*
  - *<u>SW + Small Trojan: 62% of the FPGA used (2% HT</u>*

- Allows for rapid testing of 2OE for many modified circuits
  - *No need to fabricate lots of differently modified ASICs*
  - *Easily cycle through experimental conditions: input voltage, frequency, data sampling, binning and averaging*

- Caveat: circuits in an FPGA aren't one-to-one with ASIC implementation and 2OE detectability could differ significantly



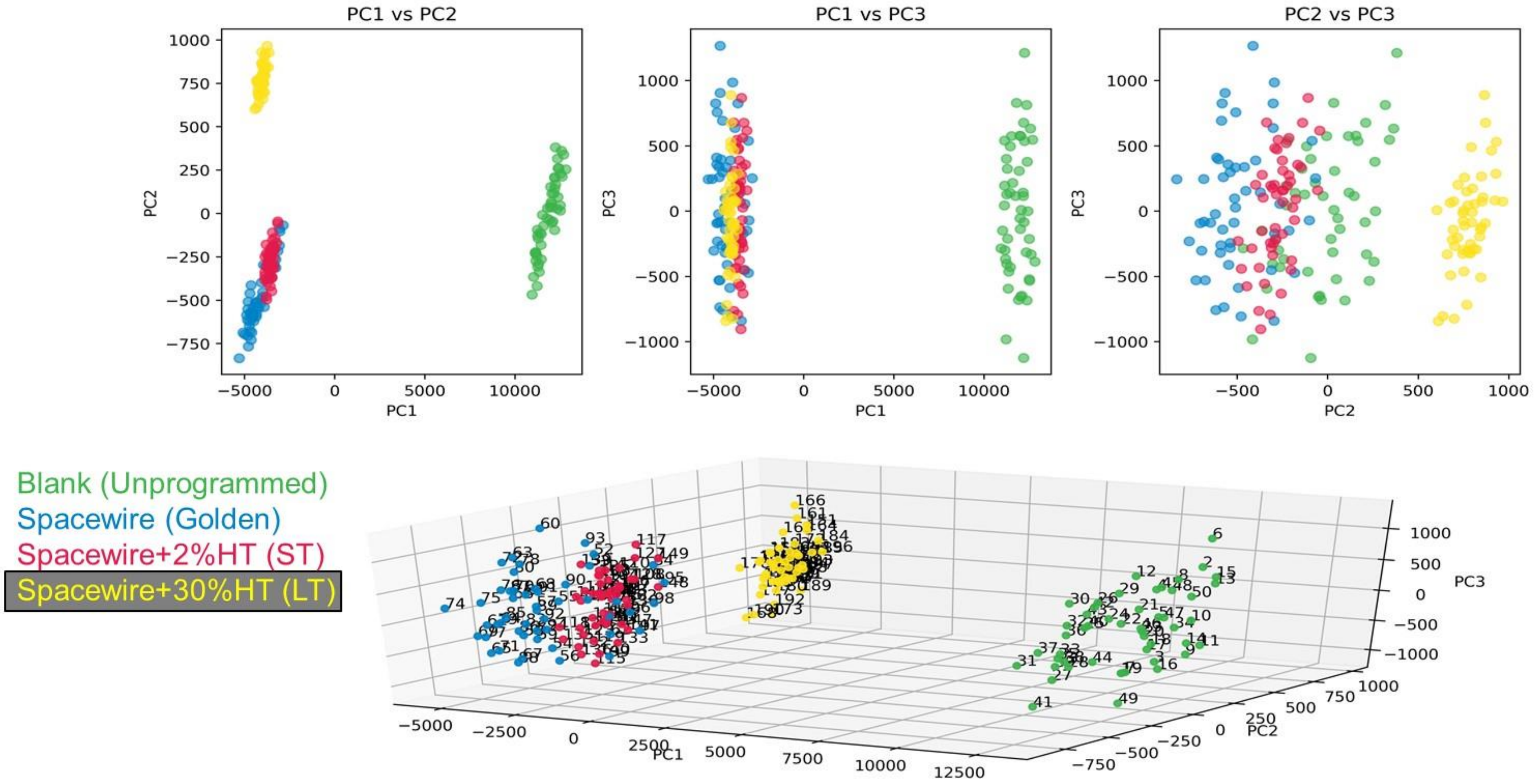
Power Spectrum Analysis Method adapted from Pai et al., (Sandia)



Principle Component Analysis (PCA) enables dimensionality reduction transforming high-dimensional data to a new set of basis vectors that best describe maximum variance in the data

First Results from one FPGA "reloaded in the test socket each time"

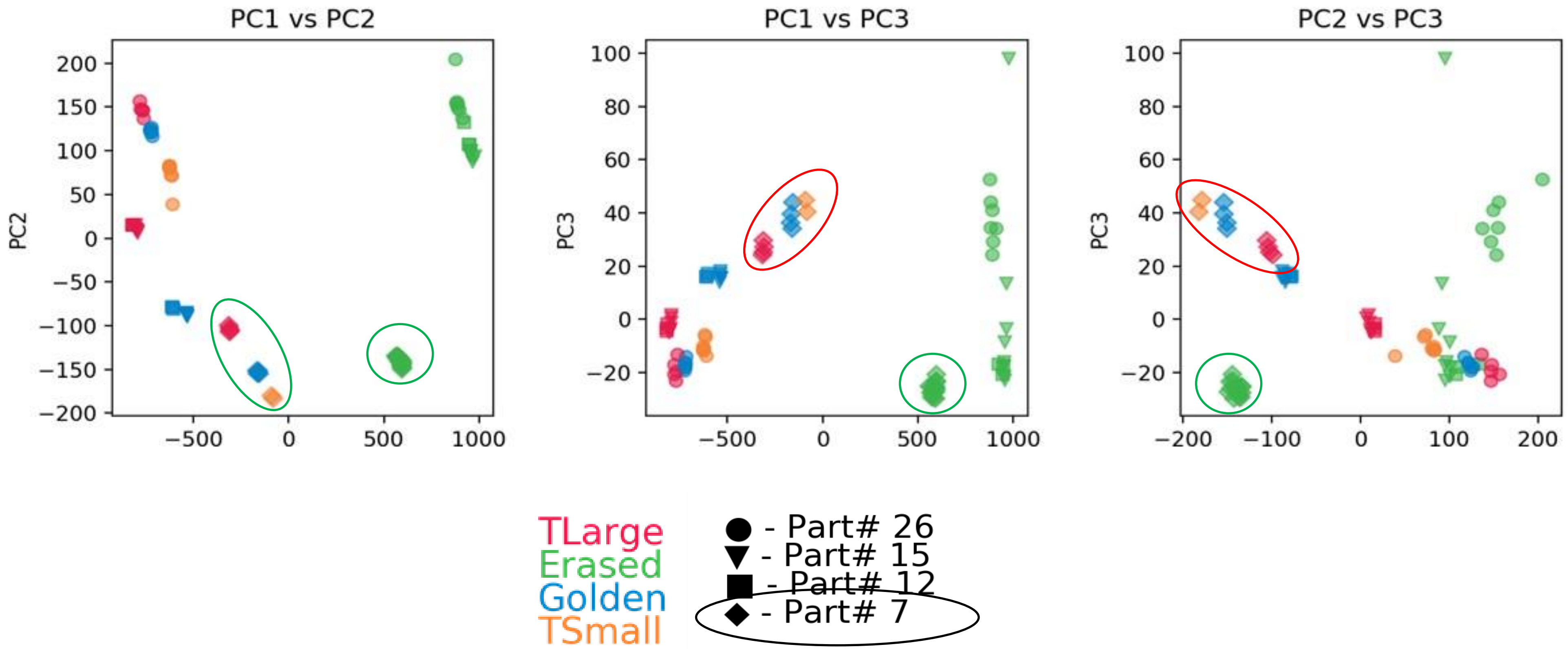
50 measurements made for each program state



PC1 separates the four "states" well, but significant overlap for Golden and 2%...

Next we used several FPGAs

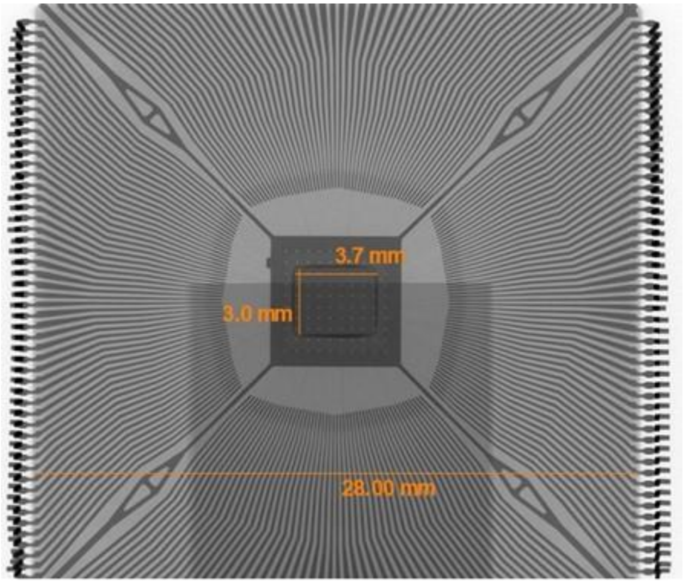
Parts reinserted into test socket for each 2OE measurement

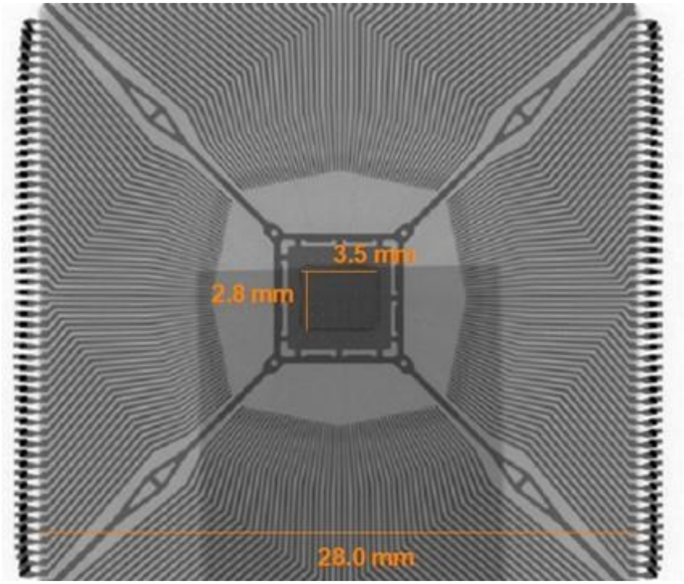


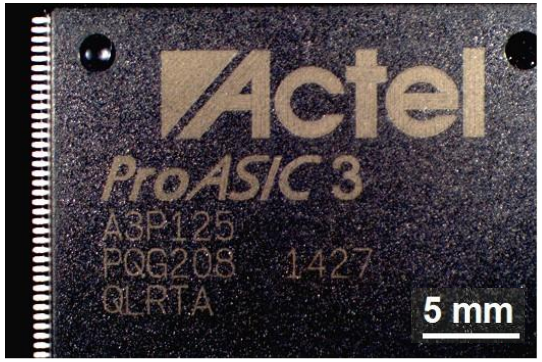
- ***Physical loading-unloading of the created variation as much as our Trojan modifications***
- ***But also, clustering of different parts suggested something more happening***

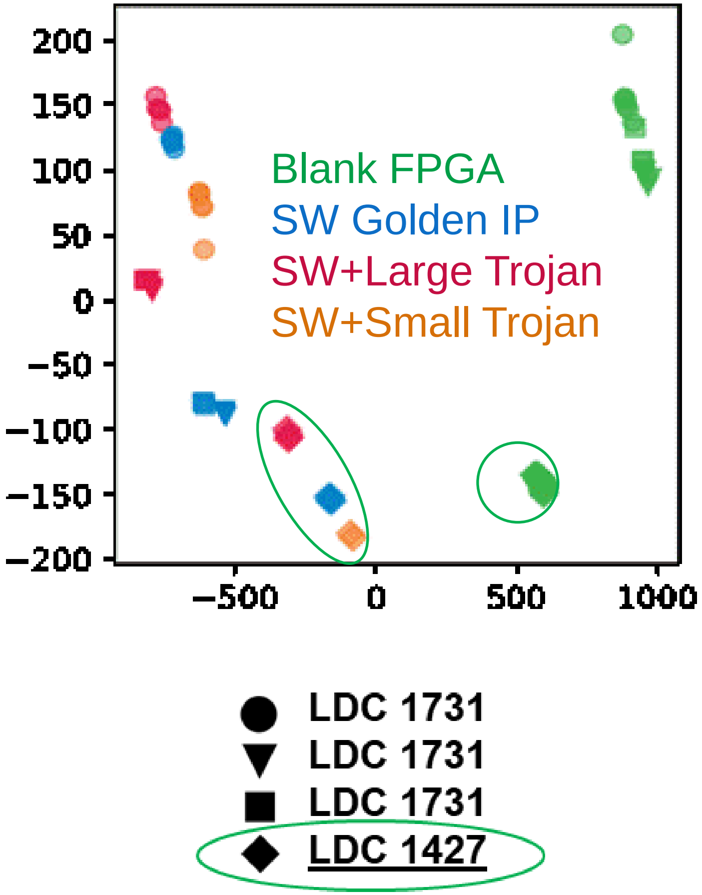
Big “modifications” are easy to detect

Detecting changes in die, package lead frames… and test-socket insertion





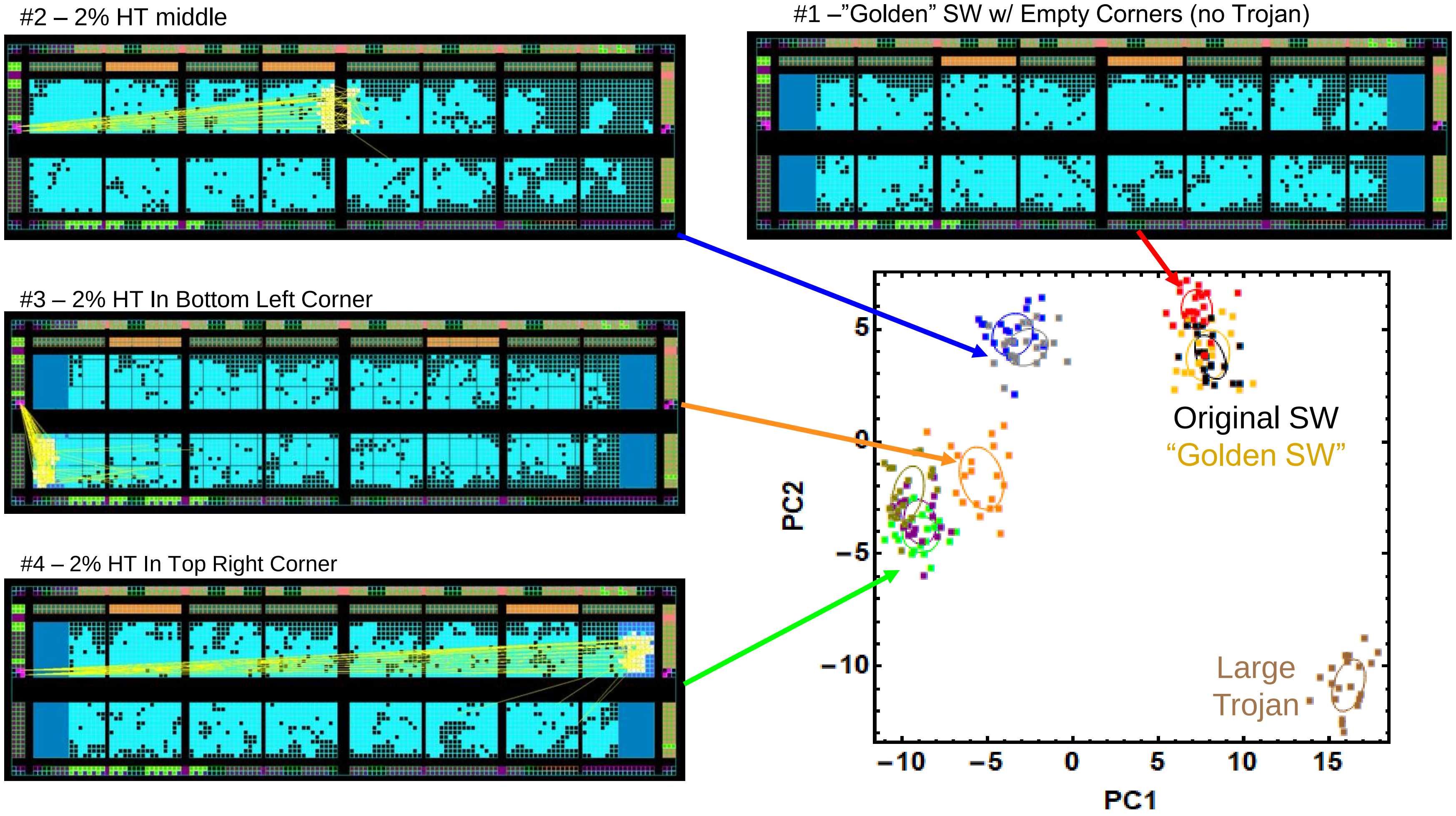




Changed manufacturing between different lot date codes (3 years apart)

Sticking to one FPGA, programmed and 2OE tested in place

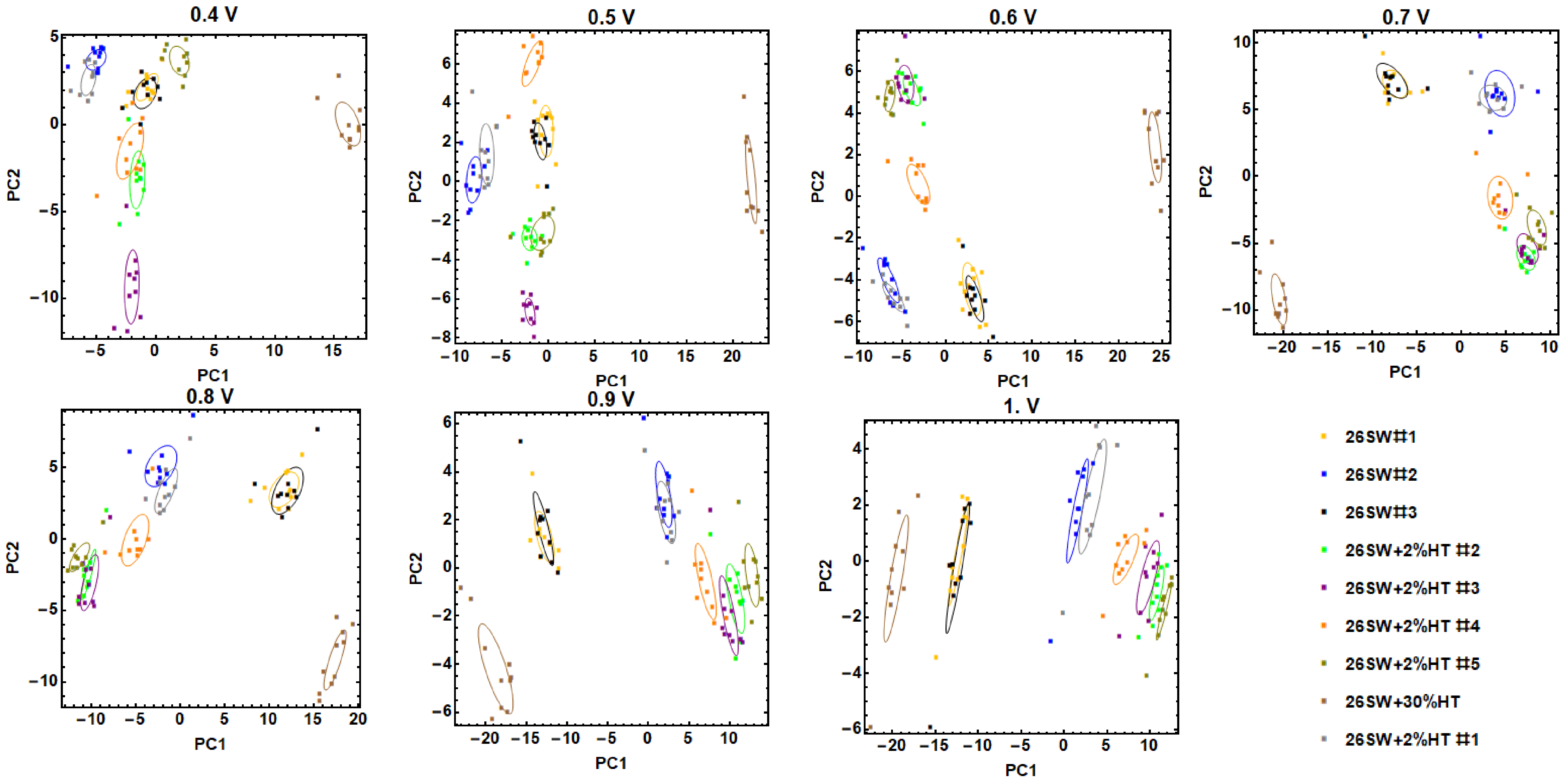
- changes in physical location (place and routing) of a small hardware Trojan



The quantification of separability warrants an accepted standardized metric

PCA Analysis of Data at Different Voltages

Testing for optimal excitation conditions



0.7 V was optimal "separability" of the different circuits studied in our FPGA-based testbed

What do they say about statistics?

t-squared distance and p-value

$$t_{x-y}^2 = \left(\bar{\vec{x}} - \bar{\vec{y}}\right)^T \hat{\sigma}_{xy}^{-1}\left(\bar{\vec{x}} - \bar{\vec{y}}\right)$$

Mahalanobis Distance

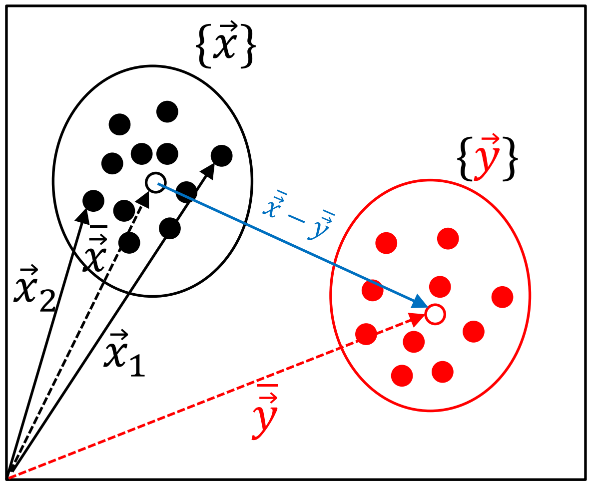
$$L_M = \left(\bar{\vec{x}} - \bar{\vec{y}}\right)^T \hat{\sigma}_x^{-1}\left(\bar{\vec{x}} - \bar{\vec{y}}\right)$$

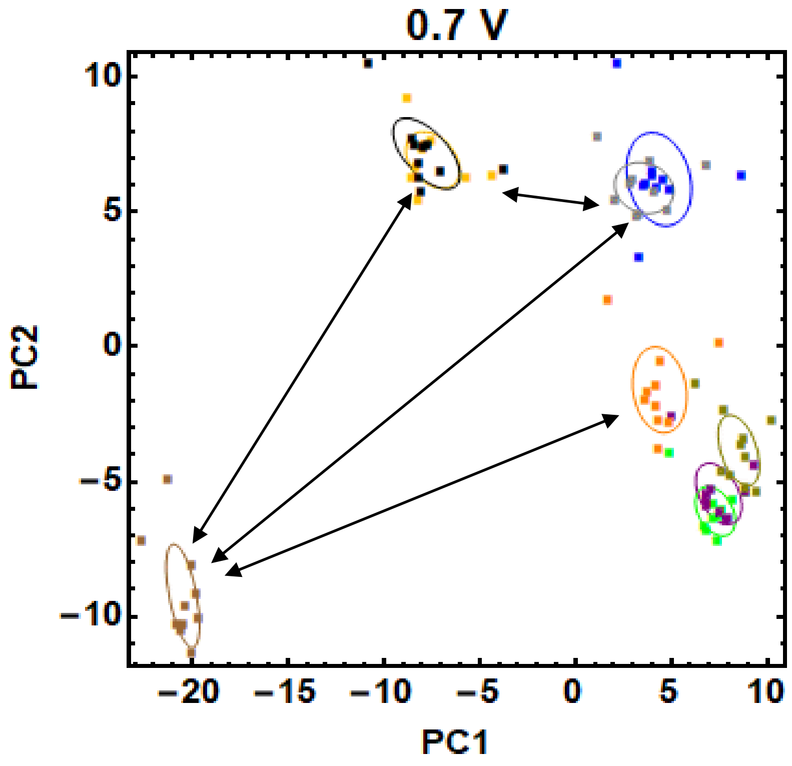
chi-square

$$\chi^2 = \left|\bar{\vec{x}} - \bar{\vec{y}}\right|^2|$$

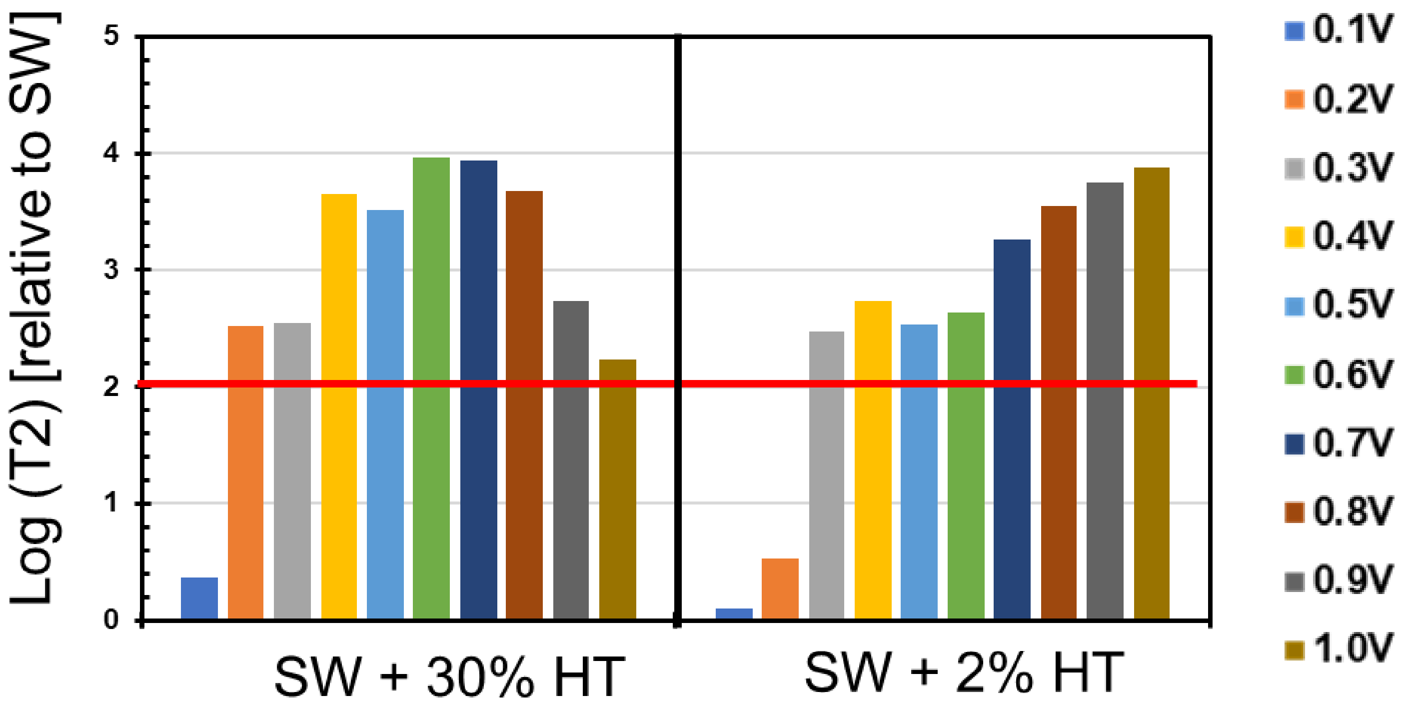
Advanced Methods:

- Neural networks and other classifier algorithms have different ways of assessing performance… **Confusion Matrices**



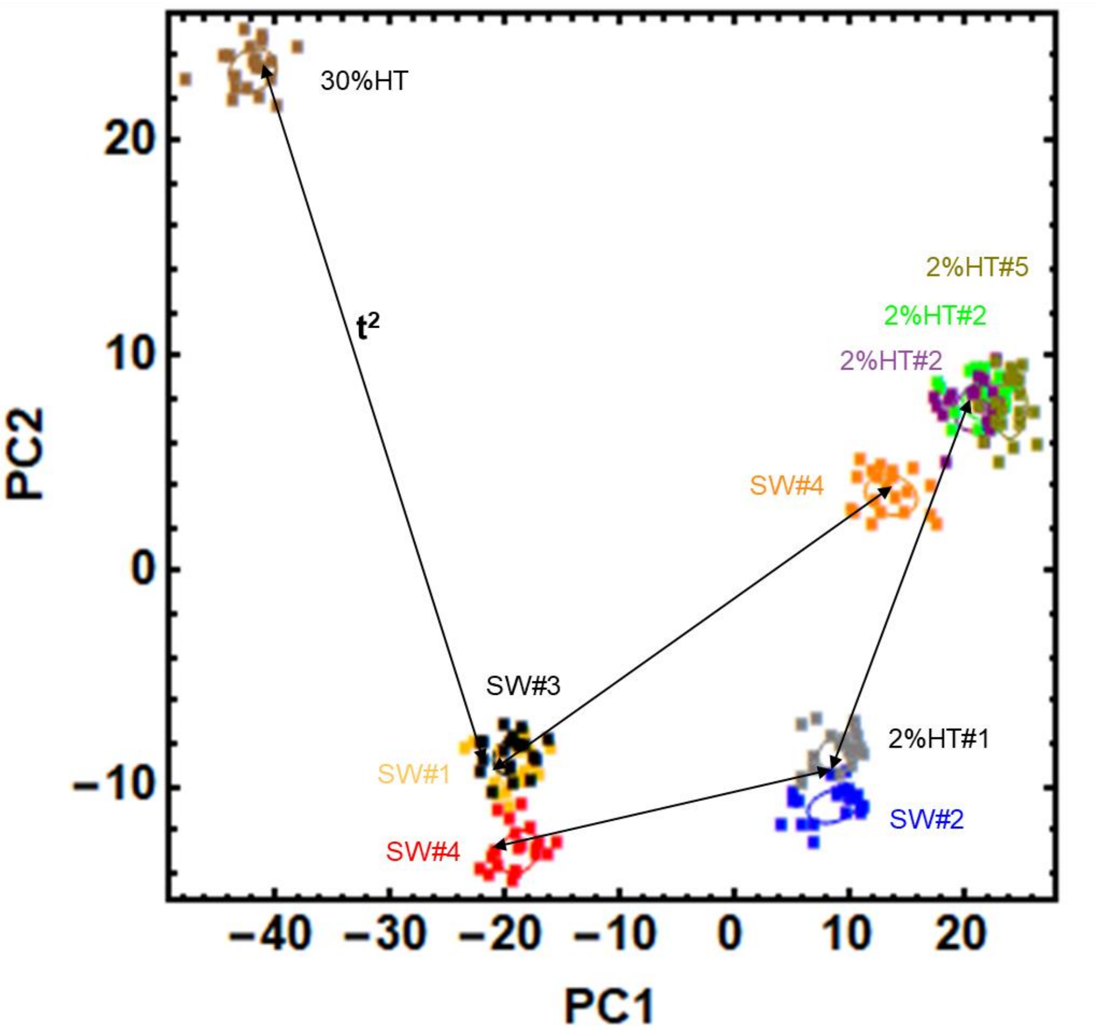


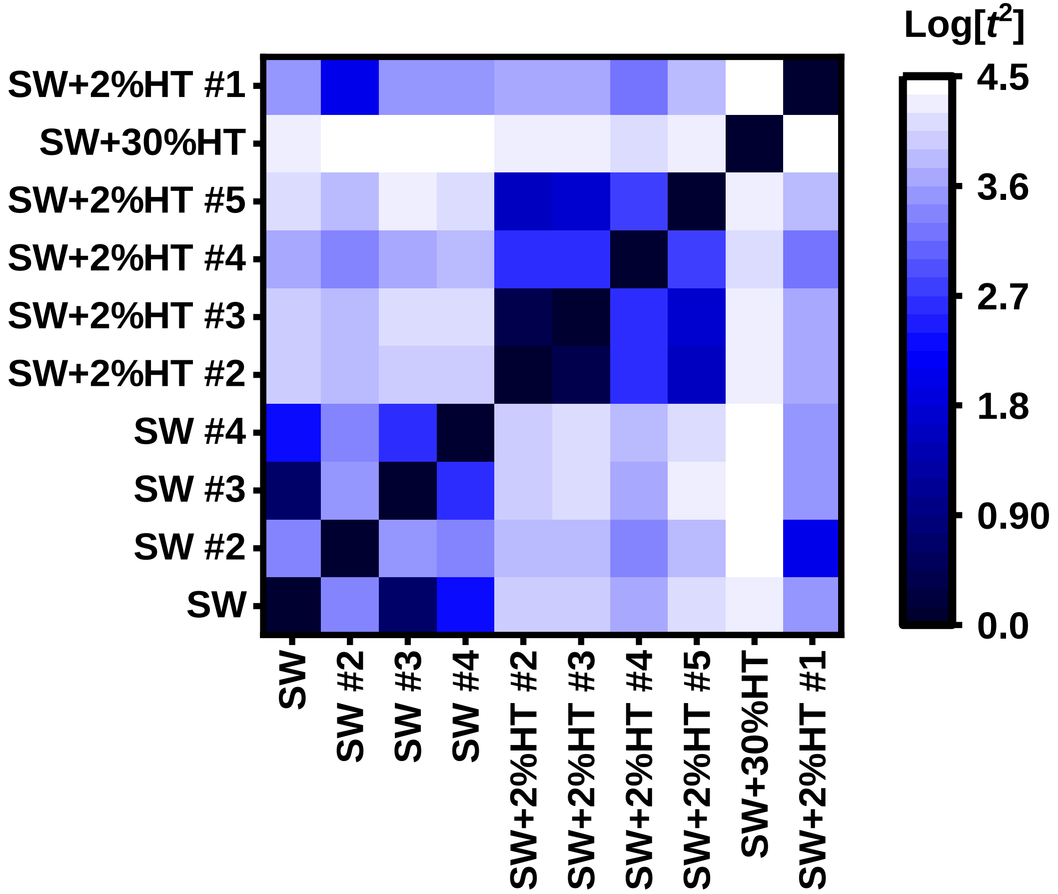
T^2 values highlight optimized methods (input voltages)



- *30% HT was easier to identify than the 2% HT, but interestingly this 2% variant became easier to detect at higher voltages while the 30% HT was optimized at 0.6 V.*
- *Could automate use of T2 values for optimization across other 2OE data collection parameters for specific parts-pairs issues.*

PCA Plot and T^2 distances between clusters for single FPGA data

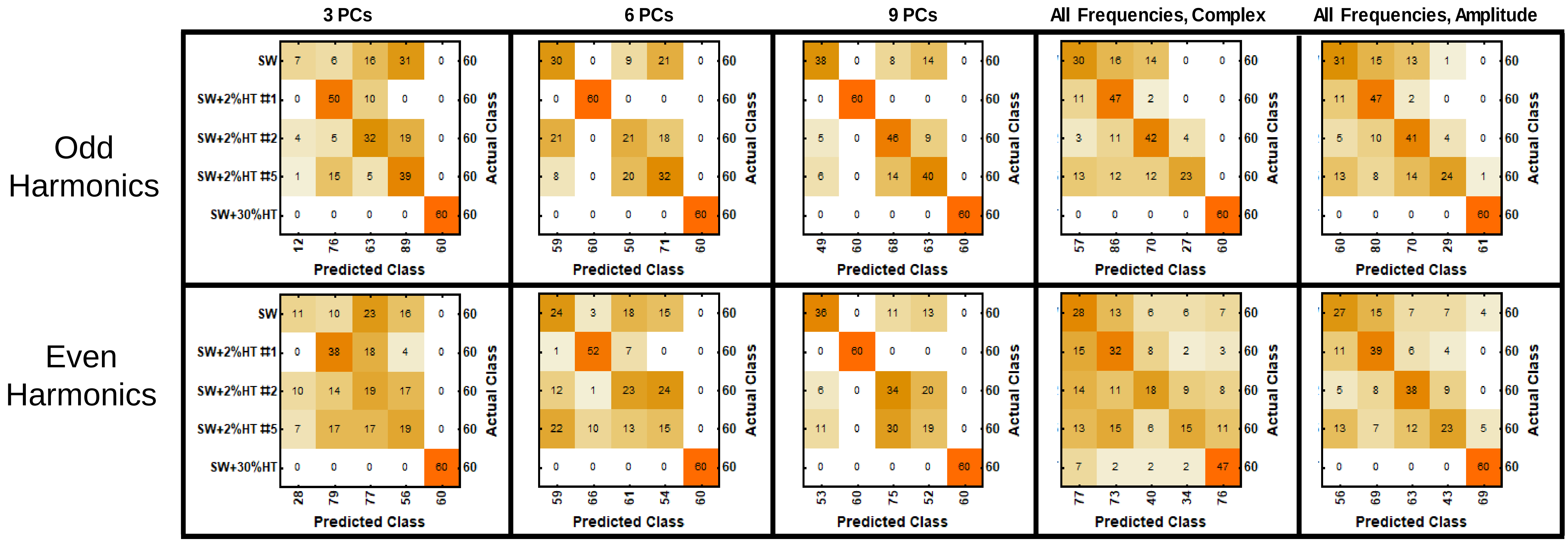




Methods optimization should consider the value of improving sensitivity to different modifications

Machine learning was used to identify optimal data dimensionality

Example confusion matrices present results from linear regression for different data subsets



- ***Support vector machines and neural networks were also tested, but linear regression performed well as a classifier algorithm for these data subsets and it did so with much lower training times***

Conclusions

- Our Trojan insertions and modified-PSA methods provide a test case to study quantified mitigation
  - *We are still working to understand the physical basis for detectability of specific modifications*
- One 2OE method may be fine for detecting one type of problem but may be inadequate for identifying a different problem
  - *Problem = part type + defect*
  - *Method = data collection + data analysis*
  - *Noise = data that does not help identify a problem*
  - *Noise is reduced by optimization of data collection method OR by data analysis (filtering, data reduction, P/F criteria)*
- Big differences in parts may be easy to detect, but might also be easily detected by other means
- Quantifying detectability of an unknown/untested modification is still a big problem
  - *Knowing how to optimize a 2OE method for a specific type of part/problem pairing*
  - *Connecting 2OE methods to physical properties and measurement physics for detecting specific problems is key*