

Trojan Scanner

Navid Asadi

Physical Inspection and Attacks on ElectronicS (PHIKS)



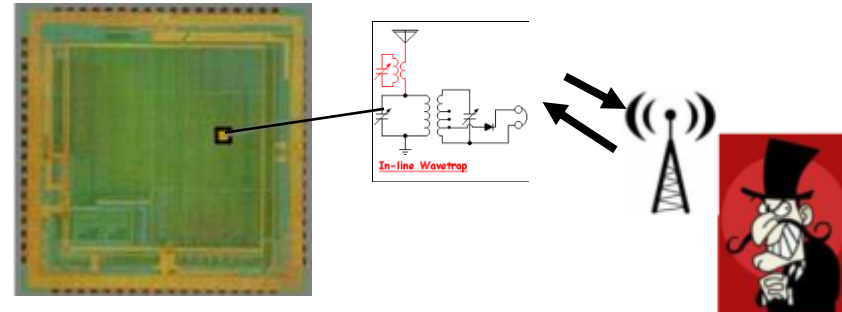
Hardware Trojan as a Threat

❑ Hardware Trojan:

- Malicious addition, deletion or modification to existing circuit elements.

❑ What Hardware Trojans can do?

- Reduce the reliability to cause early failure
- Hijack to control or change the functionality
- Leak sensitive information (Encryption keys)

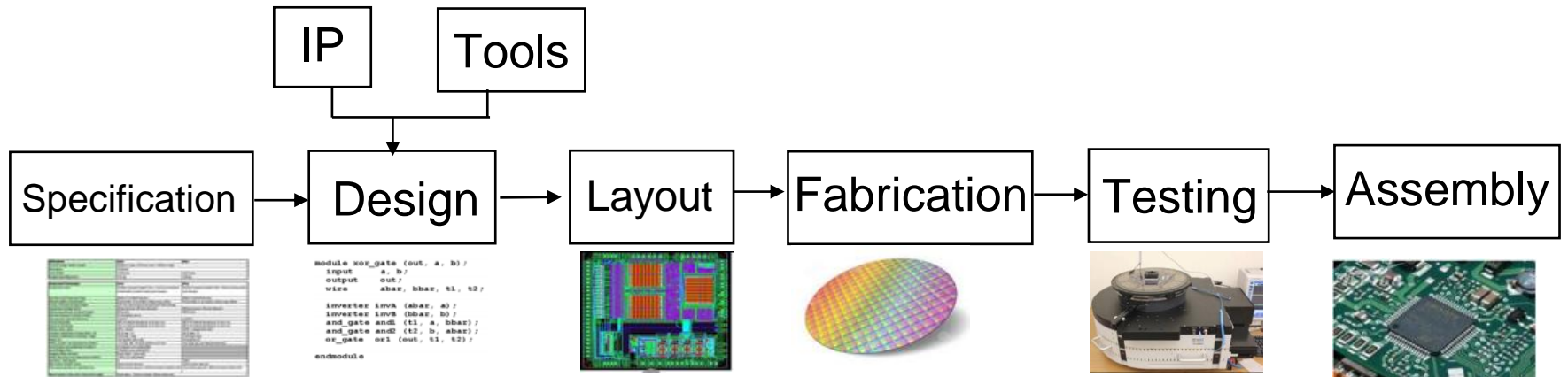


❑ Targeted Applications

- IoT devices (Home automation – Google Home, Alexa, Security cams, locks)
- Aerospace & Military applications
- Civilian applications like Aviation, Security, Healthcare, Financial...and many more

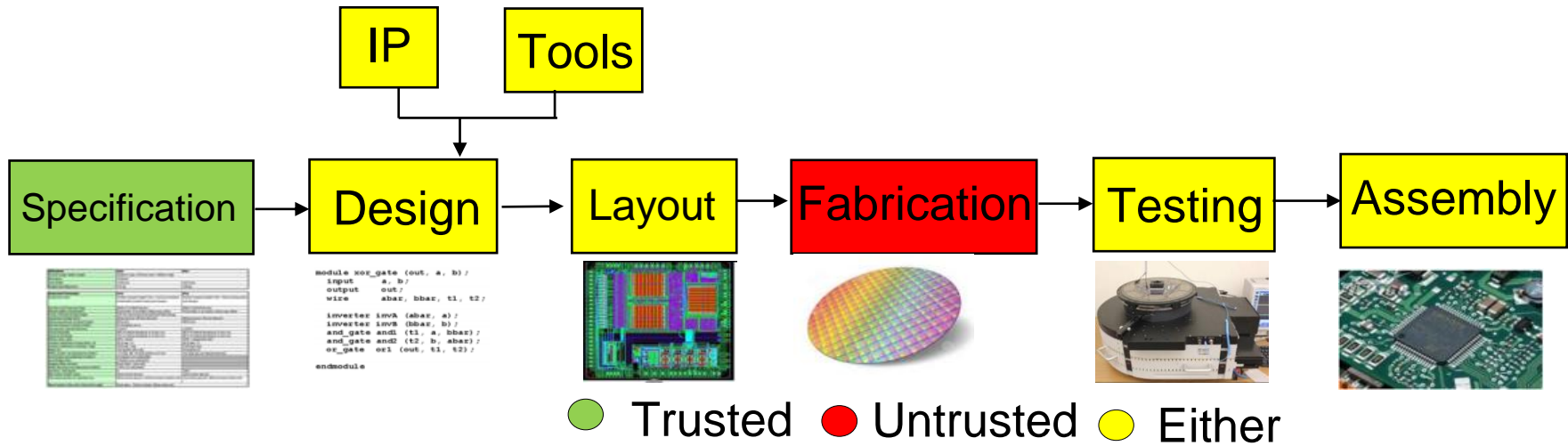


Introduction: Horizontal Business Model



- The economics of the semiconductor industry today have created a 'horizontal' business model.
- Cost of maintaining top-end fab prohibitively expensive ~ \$\$ Billions.
- Foundries at advanced nodes are almost exclusively off-shore today.

Trust Issues in Design, Fabrication, etc.



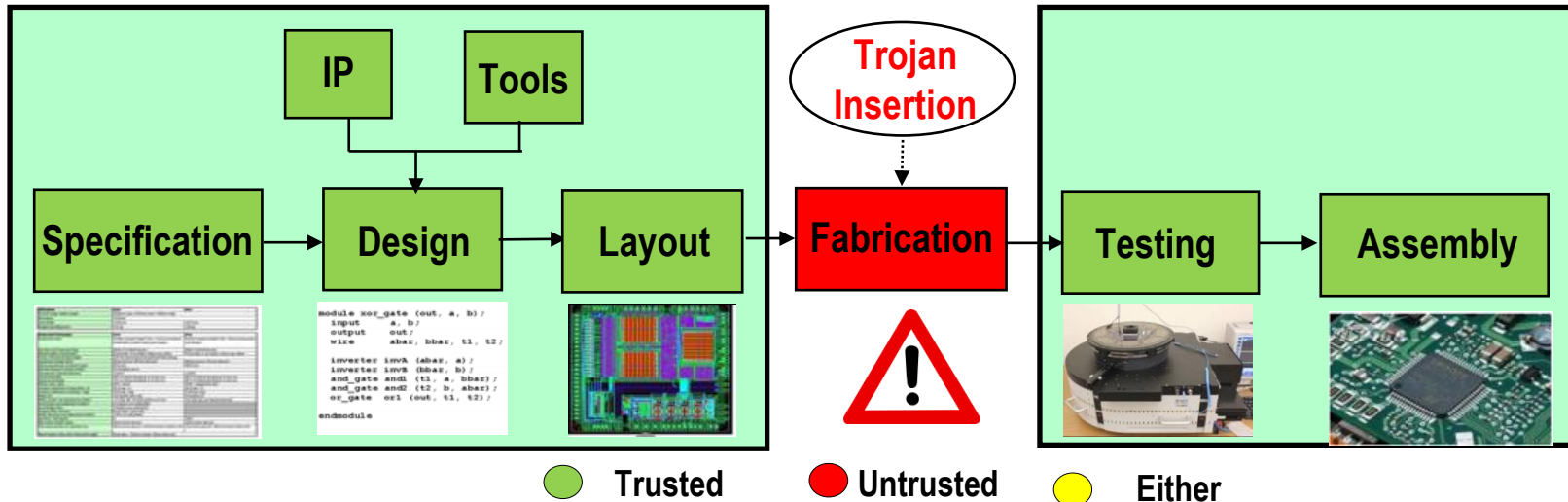
• Trust Issues

- Foundry receives (almost) everything from design house
 - GDSII layout ⇒ Netlist, Test Vectors
- A design house has little to no control over an off-shore foundry.

• Threats

- IC Threats
 - Overproduction
 - **Trojan Insertion**
- IP Threats
- Out-of-Spec/Defective Products

Trojan Problem for Government



Trust Issues

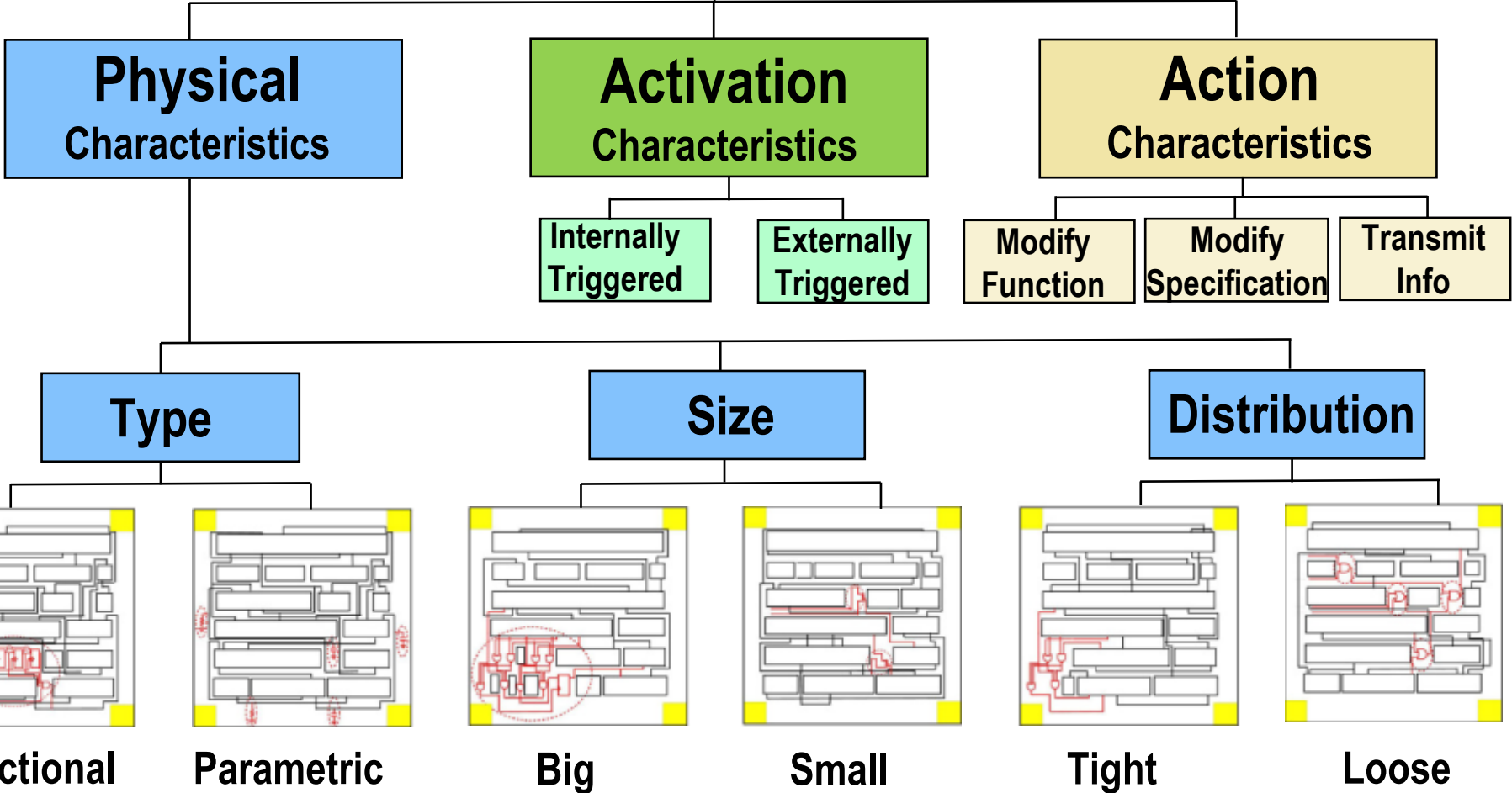
- Foundry receives (almost) everything from design house
 - GDSII layout ⇒ Netlist, Test Vectors
- A design house has little to no control over an off-shore foundry.

Threats

- IC Threats
 - Overproduction
 - **Trojan Insertion**
- IP Threats
- Out-of-Spec/Defective Products

Taxonomy of Hardware Trojans

Trojan Classification



Trojan Detection Techniques

Trojan Detection Approaches

Destructive

Full chip
Reverse Engineering

Non - Destructive

Run -Time Monitoring

Resource
Utilization

On Chip
Sensors

Reconfigurable
Computing

Test Time

Logic Test

Side Channel Analysis

Timing &
Delay

Quiescent
Current

Transient
Current

EM
Radiation

Multiple
Parameters

Trojan Detection Techniques

Trojan Detection Approaches

Destructive

Full chip
Reverse Engineering

Time Consuming
Most Effective

Non - Destructive

Run -Time Monitoring

Resource
Utilization

On Chip
Sensors

Reconfigurable
Computing

Test Time

Logic Test

Side Channel Analysis

Timing &
Delay

Quiescent
Current

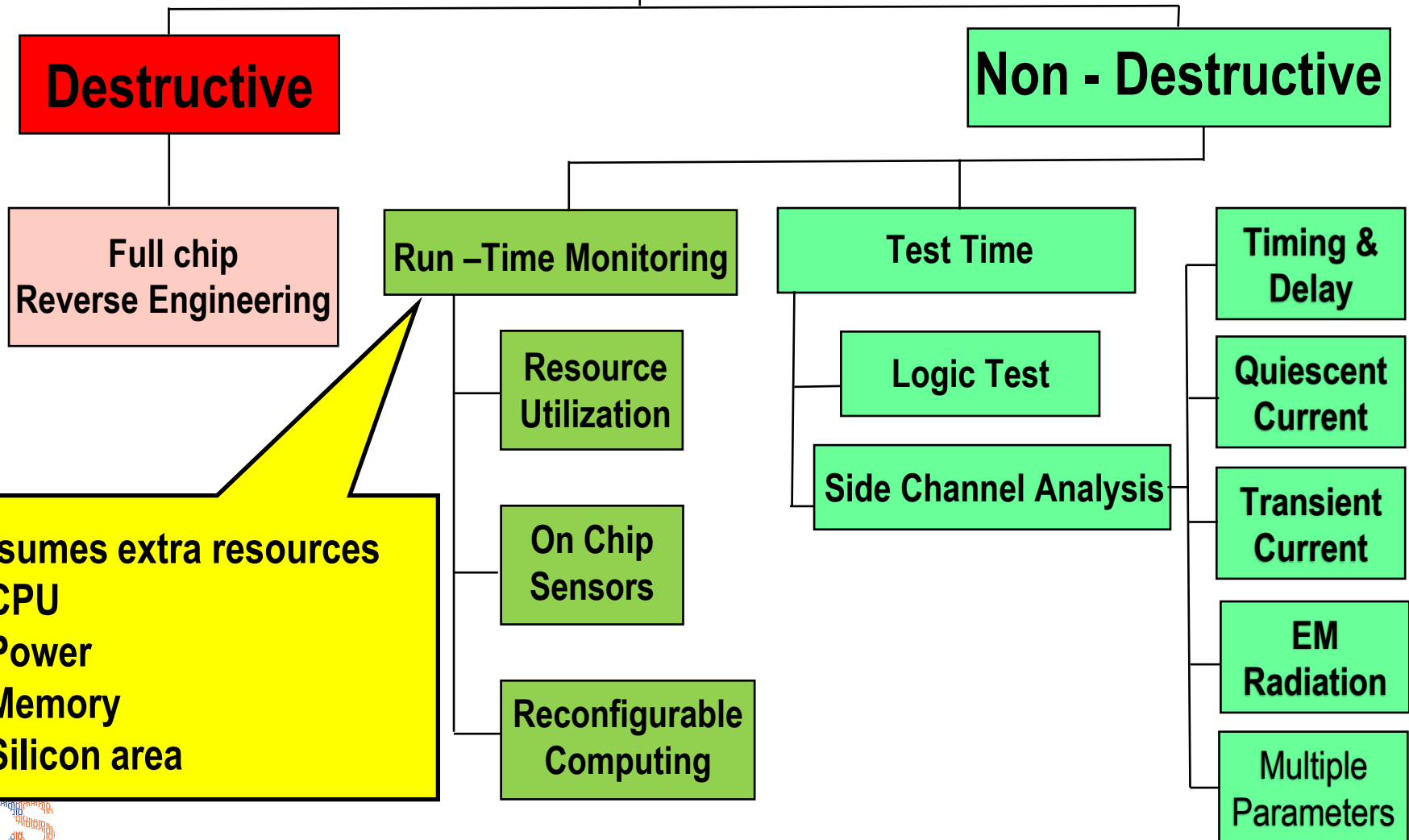
Transient
Current

EM
Radiation

Multiple
Parameters

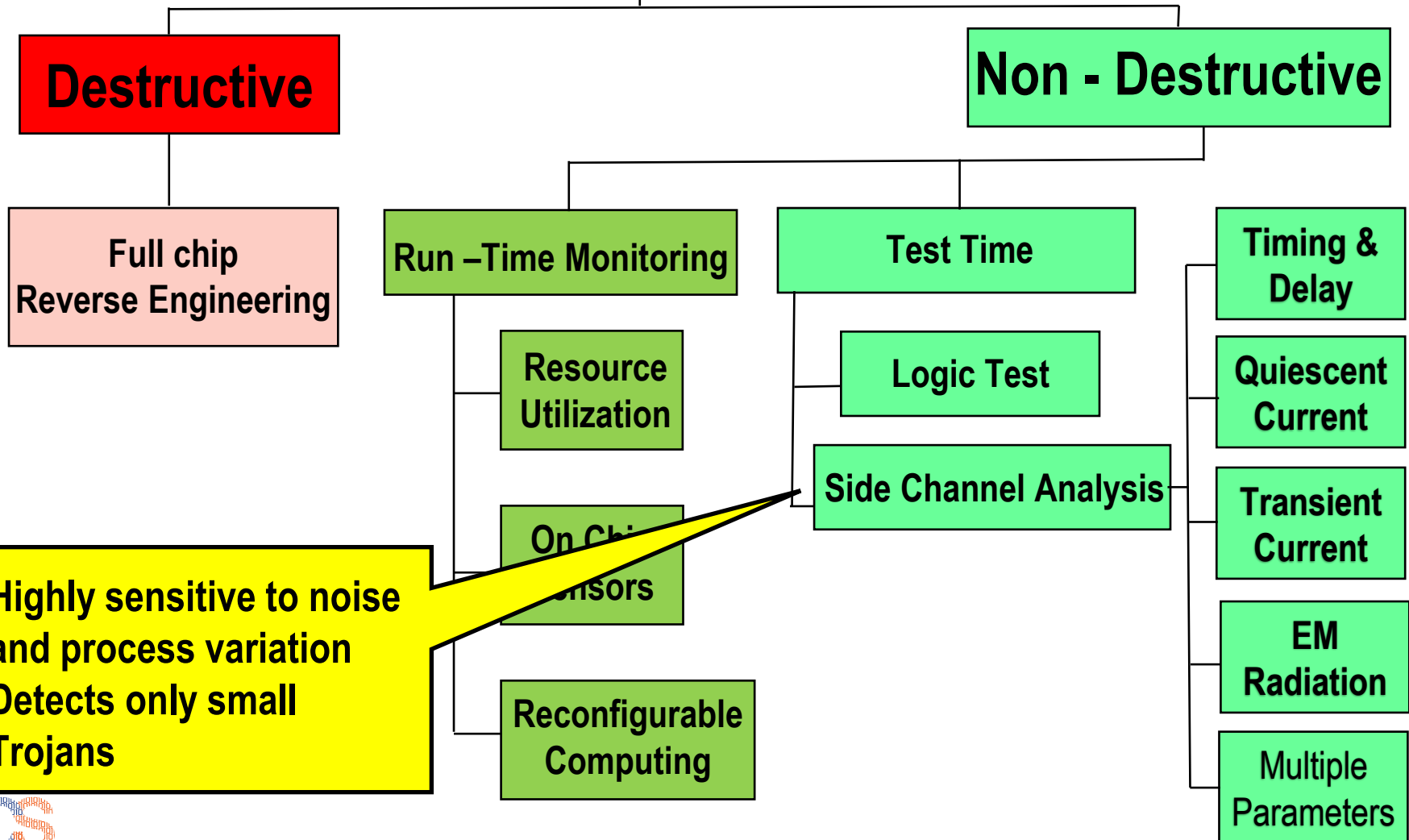
Trojan Detection Techniques

Trojan Detection Approaches

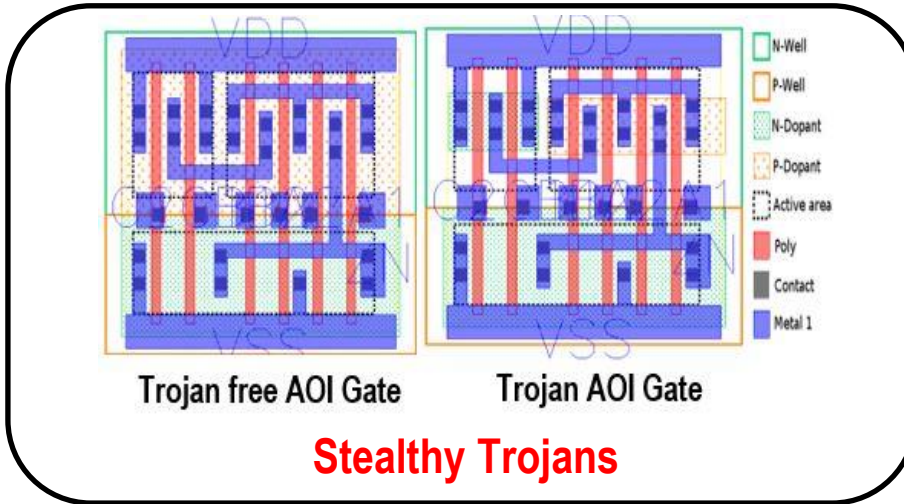
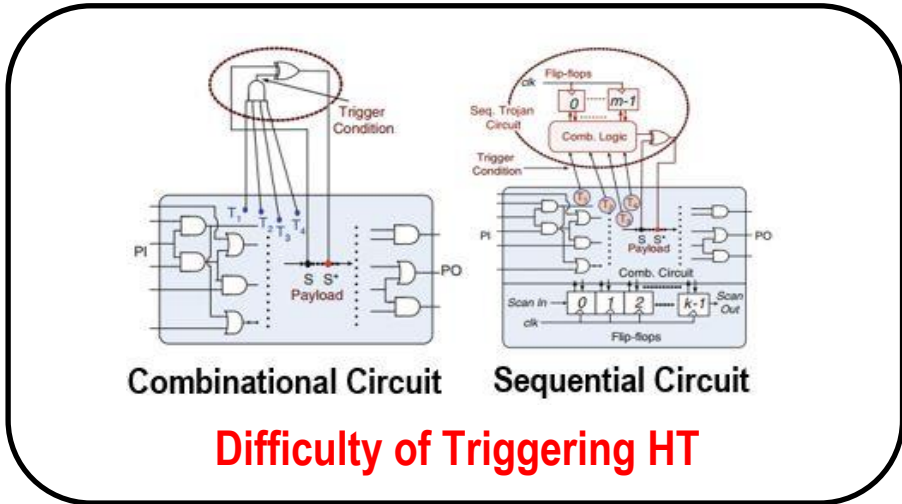
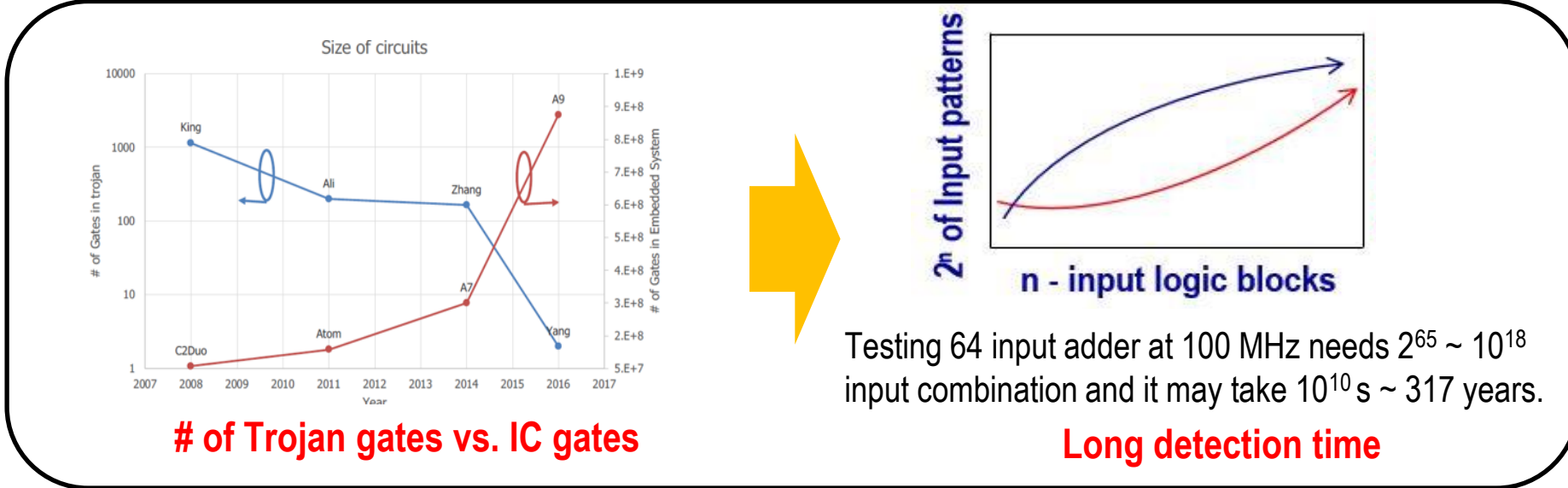


Trojan Detection Techniques

Trojan Detection Approaches



Next Generation Trojans - Challenges



We need a super fast and reliable HT detection technique

Hardware Trojans and their Footprints

Trojan Type	Implemented by	Payload
AES-T100	Flip Flops & XOR	Leaking LC circuit
AES-T400	Modulating unused pin on chip	Transmitting key bits
AES-T1800	Shift Register	Increased power
AES - T600	Shift Register & Two Inverters	Leakage current
B15-T100	6 Logic Cells Inserted	Reducing clock frequency
B19-T300	Counter Circuit	Manipulation of address bus
Basic RSA - T200	Disable encoding on RTL level	Denial of service
RS232-T1800	Chain of Invertors	No Info in benchmark
EthernetMAC10GE-T100	Critical path is widened / narrowed	Reliability Impact
EthernetMAC10GE-T200	Part of clock tree is widened	Reliability Impact
EthernetMAC10GE-T300	Part of clock tree is narrowed	Reliability Impact
EthernetMAC10GE-T400	Narrowing power lines	Reliability Impact
EthernetMAC10GE-T500	Narrowing ground lines	Reliability Impact
EthernetMAC10GE-T600	Making design susceptible to crosstalk	Denial of service

In an IC, all Hardware Trojans leave their footprints on either Active or Metal Layer!!

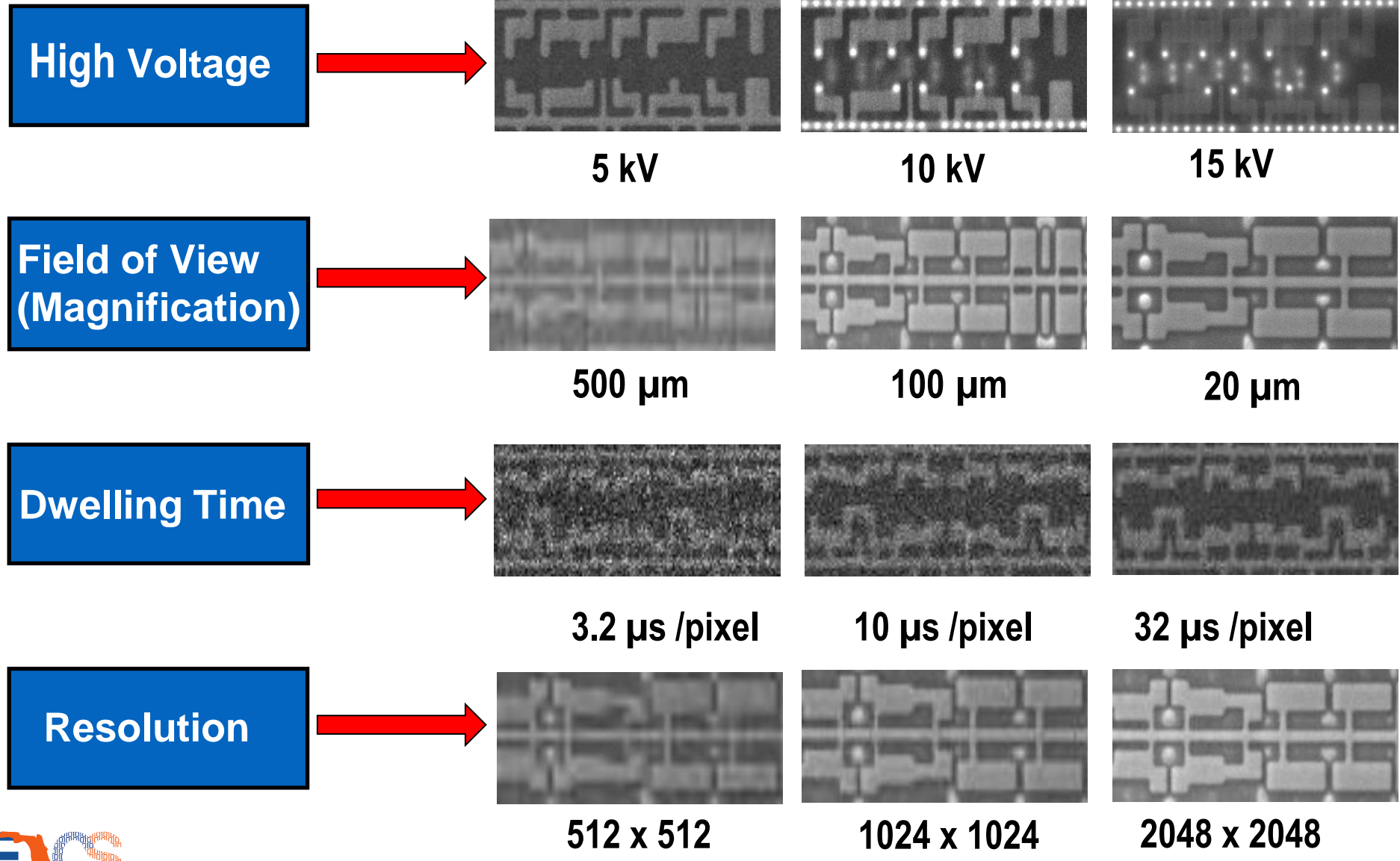
Source: Unique hardware Trojans from the list of 94 Trojans reported at TrustHub

SEM Imaging Time Table

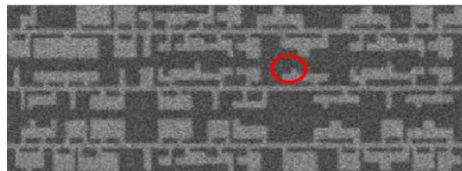
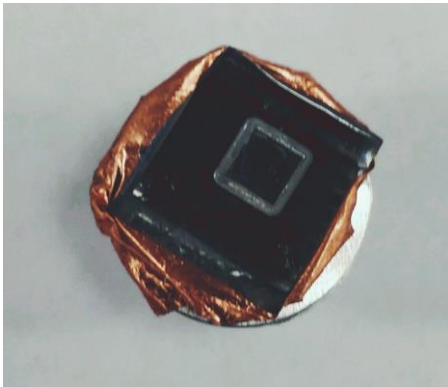
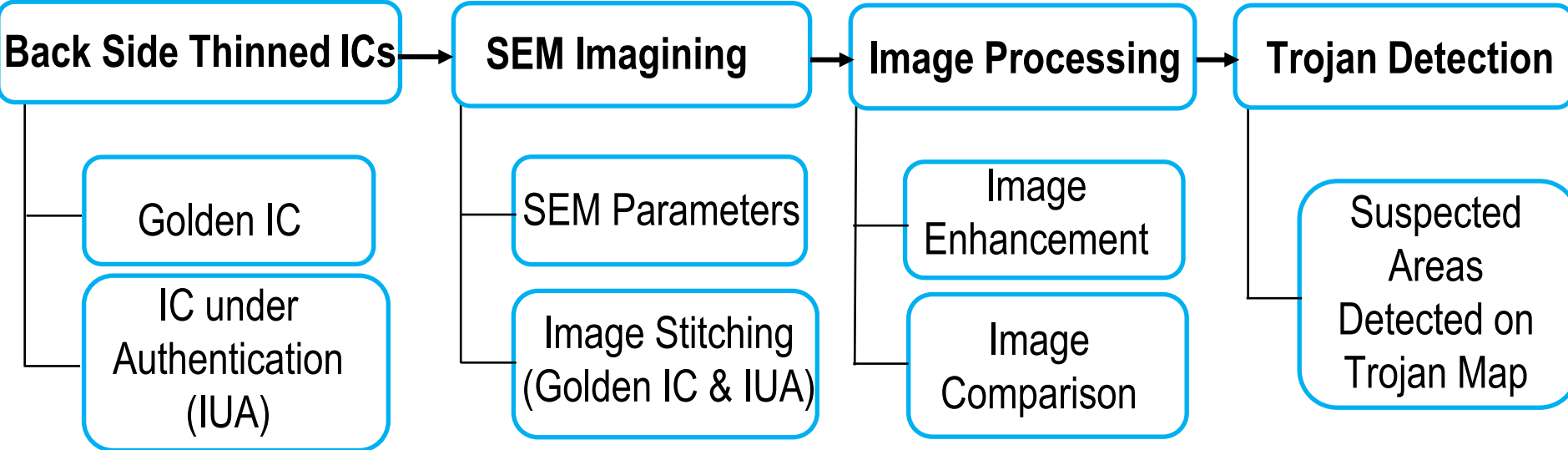
Technology node: 130nm; Chip size: 1.5mm x 1.5 mm

Scanning Speed & Resolution	1500um x 1500um	500um x 500um	100um x 100um	20um x 20um
3 (1.0 μs/Pixel)				
(512 x 512)	1 sec	9 sec	3 min 45 sec	1 hr 33min 45 sec
(1024 x 1024)	2 sec	18 sec	7 min 30 sec	3 hr 7 min 30 sec
(2048 x 2048)	6 sec	54 sec	22 min 30 sec	9 hr 22 min 30 sec
4 (3.2 μs/Pixel)				
(512 x 512)	1 sec	9 sec	3 min 45 sec	1 hr 33 min 45 sec
(1024 x 1024)	4 sec	36 sec	15 min 10 sec	6 hr 13 min 10 sec
(2048 x 2048)	14 sec	2 min 5 sec	52 min 5 sec	21 hr 42 min 5 sec
5 (10.0 μs/Pixel)				
(512 x 512)	5 sec	45 sec	18 min 45 sec	7 hr 48 min 45 sec
(1024 x 1024)	22 sec	3 min 18 sec	1 hr 22 min 30 sec	1 d 10hr 22 min 30sec
(2048 x 2048)	1 min 25 sec	6min 25 sec	5 hr 18 min 45 sec	5 d 12 hr 48 min 45 sec
6(32 μs/Pixel)				
(512 x 512)	11 sec	1 min 30 sec	36 min	15 hr
(1024 x 1024)	43 sec	6 min 30 sec	2 hr 45 min	1 d 21 hr 5 min
(2048 x 2048)	2 min 52 sec	24 min	10 hr 45 min 10 sec	11 day 1 hr 30 min
7 (100.0 μs/Pixel)				
(512 x 512)	32 sec	4 min 48 sec	2 hr	2 days 2 hours
(1024 x 1024)	2 min 6 sec	18 min 54 sec	7 hr 52 min 30 sec	8 d 4 hr 25 min 6 sec
(2048 x 2048)	7 min 54 sec	1 hr 11 min 6 sec	1 d 5 hr 37 min 30 sec	30 d 20 hr 37 min 30 sec

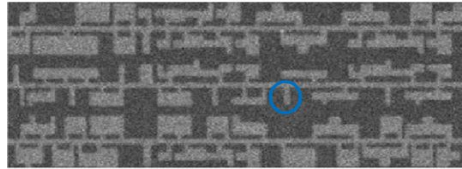
SEM Image Collection



Trojan Scanner: Golden Chip



(a)



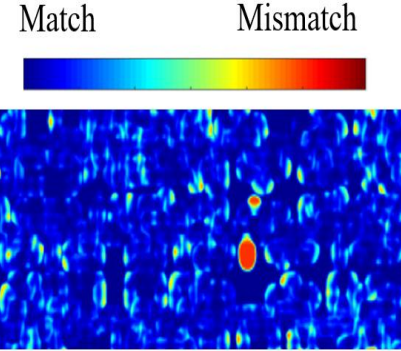
(b)



(c)




(d)

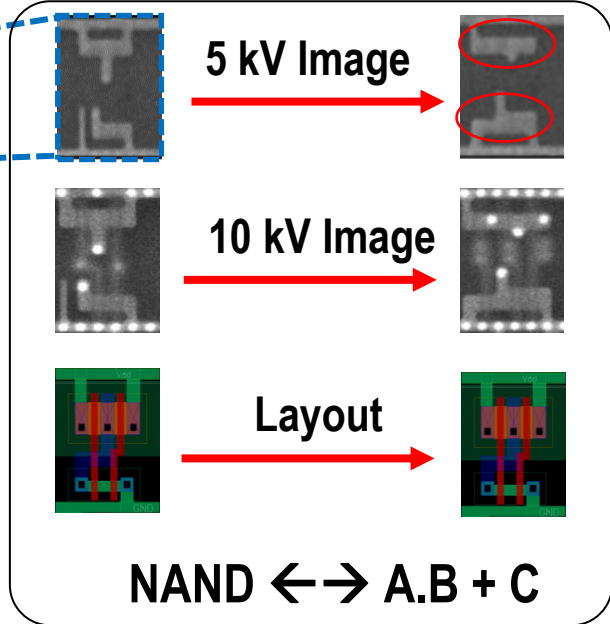
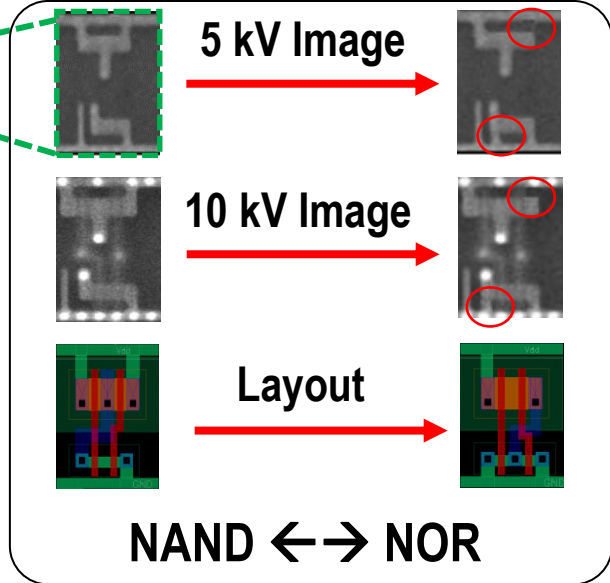
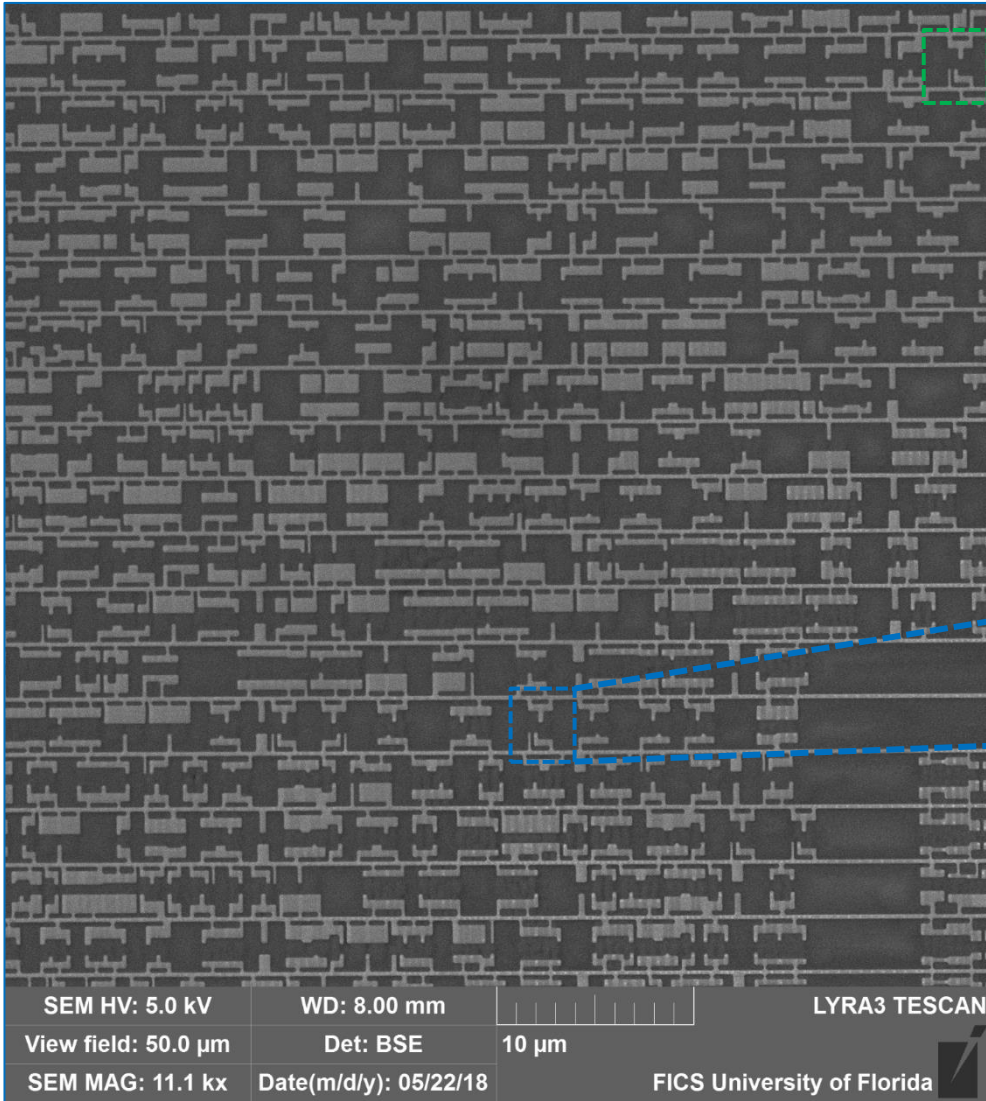


(e)

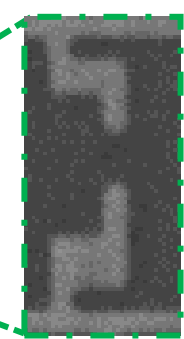
Case Study of Trojan & Footprints on ICs

Size of Change	Change Type		Footprint
<p style="color: red; font-weight: bold; text-align: center;">Smallest</p> <div style="text-align: center;">  </div>	Modification	NAND \leftrightarrow NOR	Active Region
		NAND \rightarrow A.B+C (or any custom logic)	Active Region
		Splitting active P well \rightarrow P + N well	Active Region
		Changing number of inputs	Active Region
		Resizing 1x \rightarrow 2x	Active Region
		Interconnects / Power / GND - Thinning	Metal Layer 1
	Camouflage Cells	NOR \leftrightarrow NAND	Metal layer 1
	Insertion / Deletion	Invertor NOT	Active Region
		NAND / NOR	Active Region
	Biggest		Capacitor

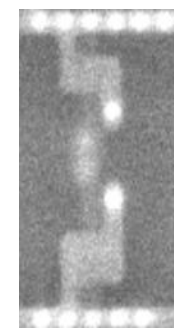
Modification of Logic Gates



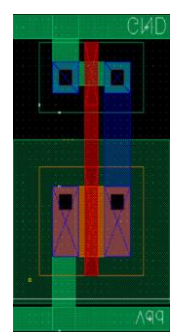
Insertion Based Trojans



5 kV Image

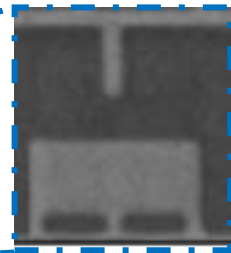


10 kV Image

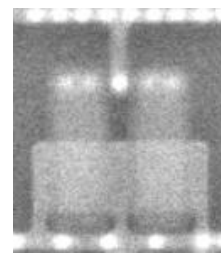


Layout

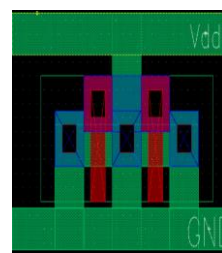
Inverter* NOT Gate



5 kV Image



10 kV Image



Layout

MOS Capacitor#

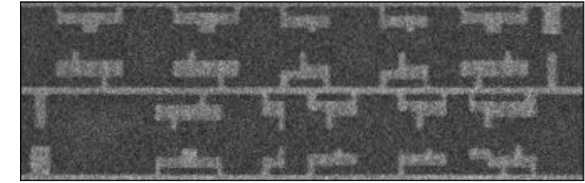
SEM HV: 5.0 kV	WD: 8.00 mm	LYRA3 TESCAN
View field: 50.0 μm	Det: BSE	
SEM MAG: 11.1 kx	Date(m/d/y): 05/22/18	FICS University of Florida

*Capacitor as a Trojan Implemented : A2: Analog Malicious Hardware by Yang et. Al

#Trojan RS232-T1800 Implemented using two Inverters – Trust Hub

a. Original SEM Image

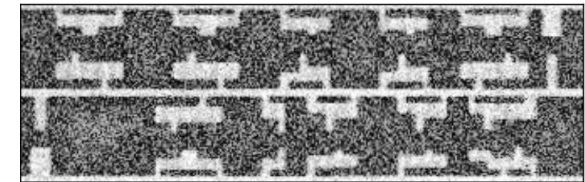
Scan the whole die as fast as possible while capturing sufficient feature details to compare with the layout.



(a)

b. Histogram Equalization

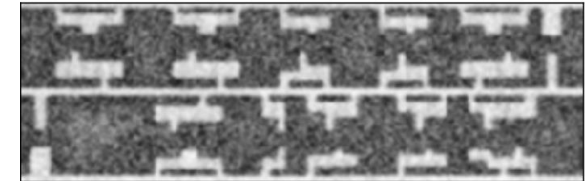
Increase contrast of doping regions in SEM image for better feature detection.



(b)

c. Gaussian Filtering

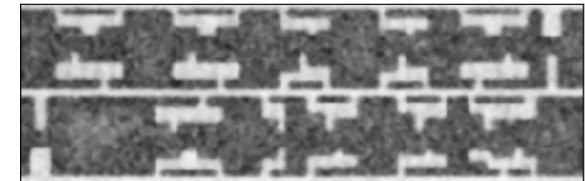
A 5x5 Gaussian filter is applied to remove the Gaussian noise in SEM image.



(c)

d. Median Filtering

A 3x3 median filter is applied to effectively remove noise and preserve the edge information to detect every unique footprint of a logic cell.



(d)

e. Thresholding

Segmenting SEM image into a binary image to separate the dark background and the foreground active region shape.



(e)

Trojan Detection

Slowest

Speed: 32 μ s /pixel

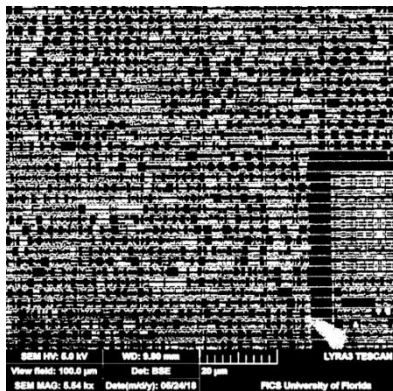
Speed: 10 μ s /pixel

Fastest

Speed: 3.2 μ s /pixel

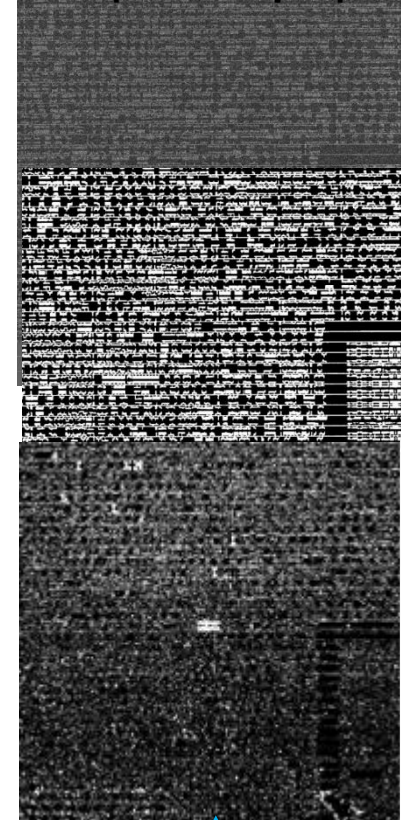
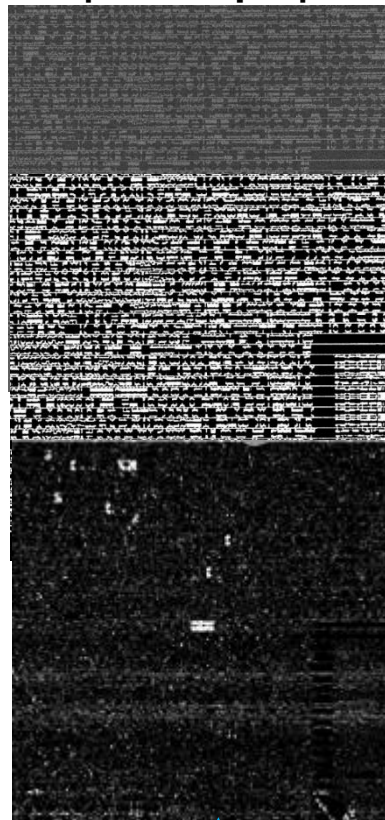
Filtering Denoising

Thresholding



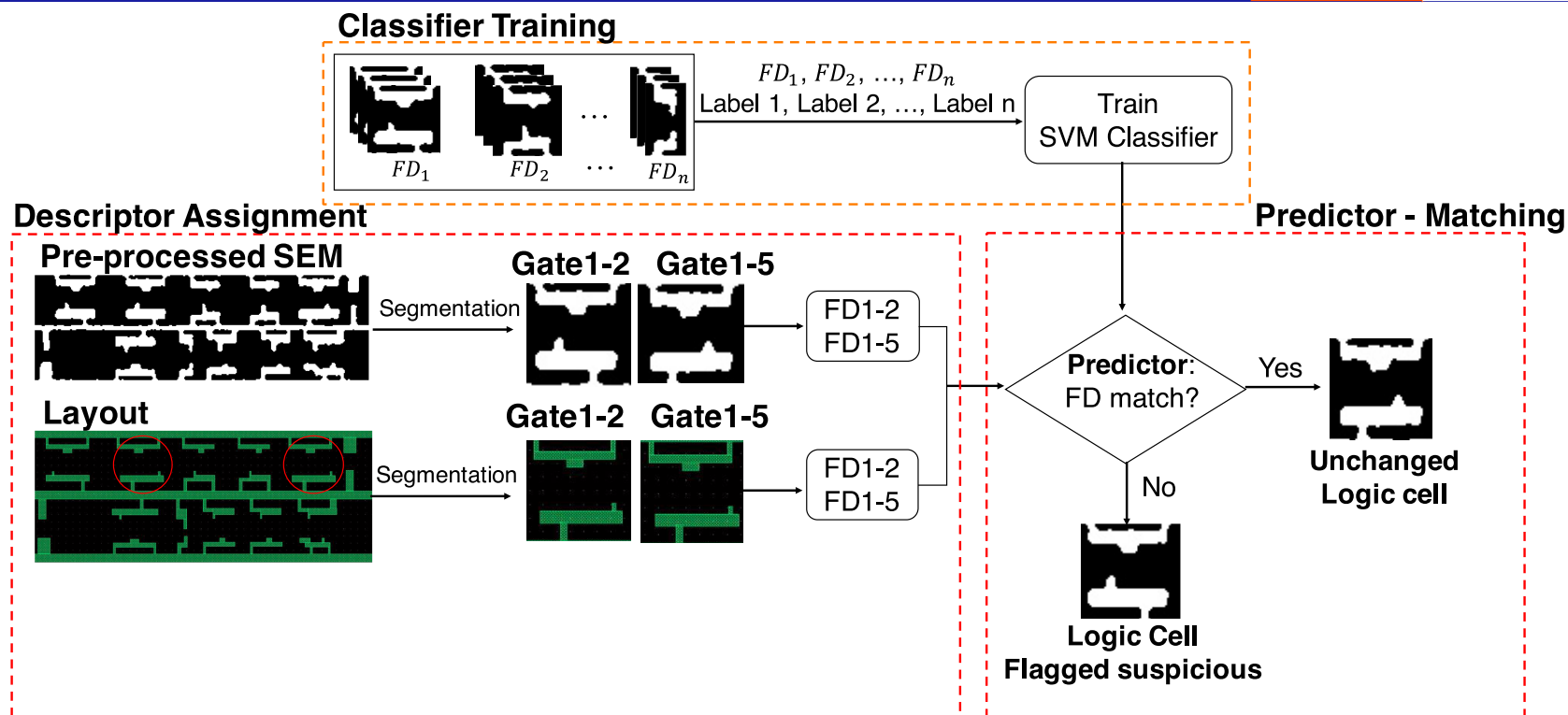
Golden IC

SSIM



$$SSIM(x, y) = l(x, y) \cdot c(x, y) \cdot s(x, y)$$

Trojan Scanner: Golden Layout



1. Descriptor Assignment

Assigning Fourier descriptor (FD) to every unique logic cell from SEM Image and Layout.

2. Classifier Training

Training machine learning model using different variations of a logic cell to account for imaging and manufacturing.

3. Predictor Matching

A machine learning based predictor matches the SEM and layout descriptors to detect a change.

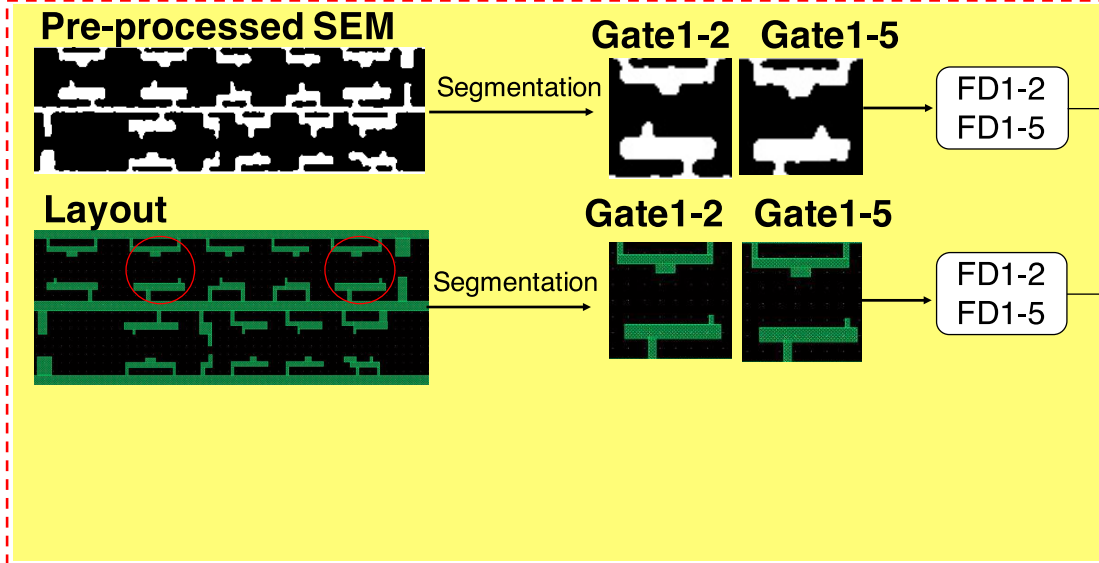
Descriptor Assignment

Assigning descriptor to every unique logic cell from SEM Image and Layout.

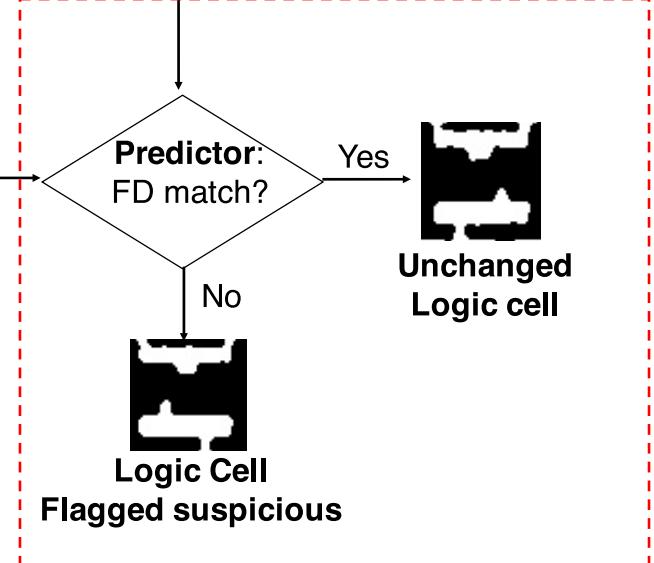
Classifier Training



Descriptor Assignment



Predictor - Matching



Descriptor Assignment --- Fourier Descriptor

- Obtain cell's mask by binary thresholding.
- Obtain contour of the mask based on the pixel difference of the shape edge.
- Obtain shape signature: The distance between contour centroid and contour coordinates.
- Calculate Fourier transform of shape signature:

$$f[k] = DFT(C[n]) = \frac{1}{N} \sum_{n=0}^{N-1} C[n] e^{\left(\frac{-j2\pi kn}{N}\right)}, \quad k = 0, 1, \dots, N - 1 \quad (1)$$

where $f[k]$ is the Fourier transform of the k^{th} coordinate and $C[n]$ is the contour.

- Combine upper and lower Fourier descriptors for the whole gate:

$$FD_g = [f_{upper}[k], f_{lower}[l]], \quad k = 0, 1, \dots, N - 1 \quad \text{and} \quad l = 1, 2 \quad (2)$$

where f_{upper} and f_{lower} is upper and lower half of logic cell respectively.



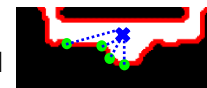
(Logic cell)



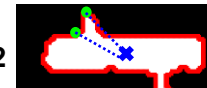
(a. Cell mask)



(b. Contour Mask)

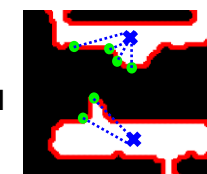


FD₁₁



FD₁₂

(c. Shape signature)

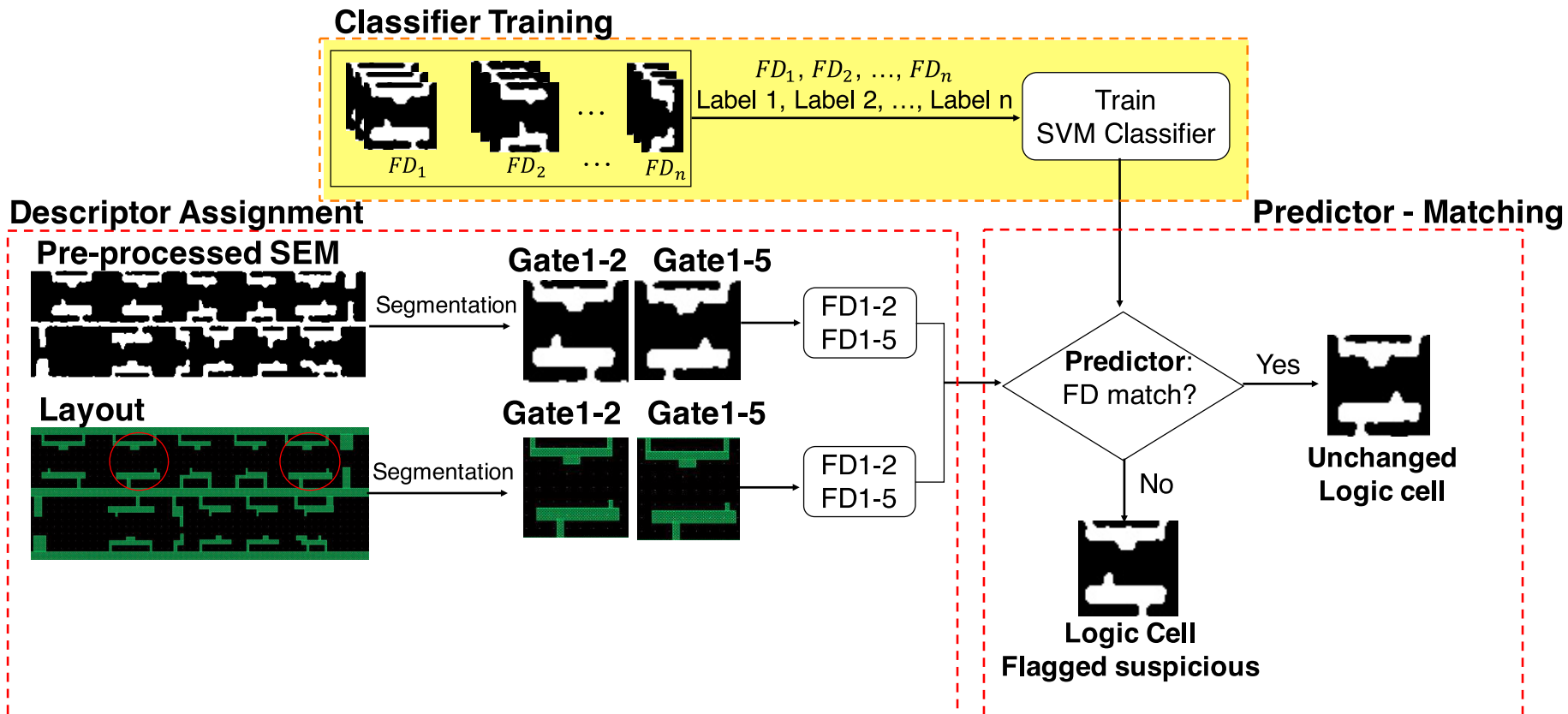


FD₁

(e. Combined FD)

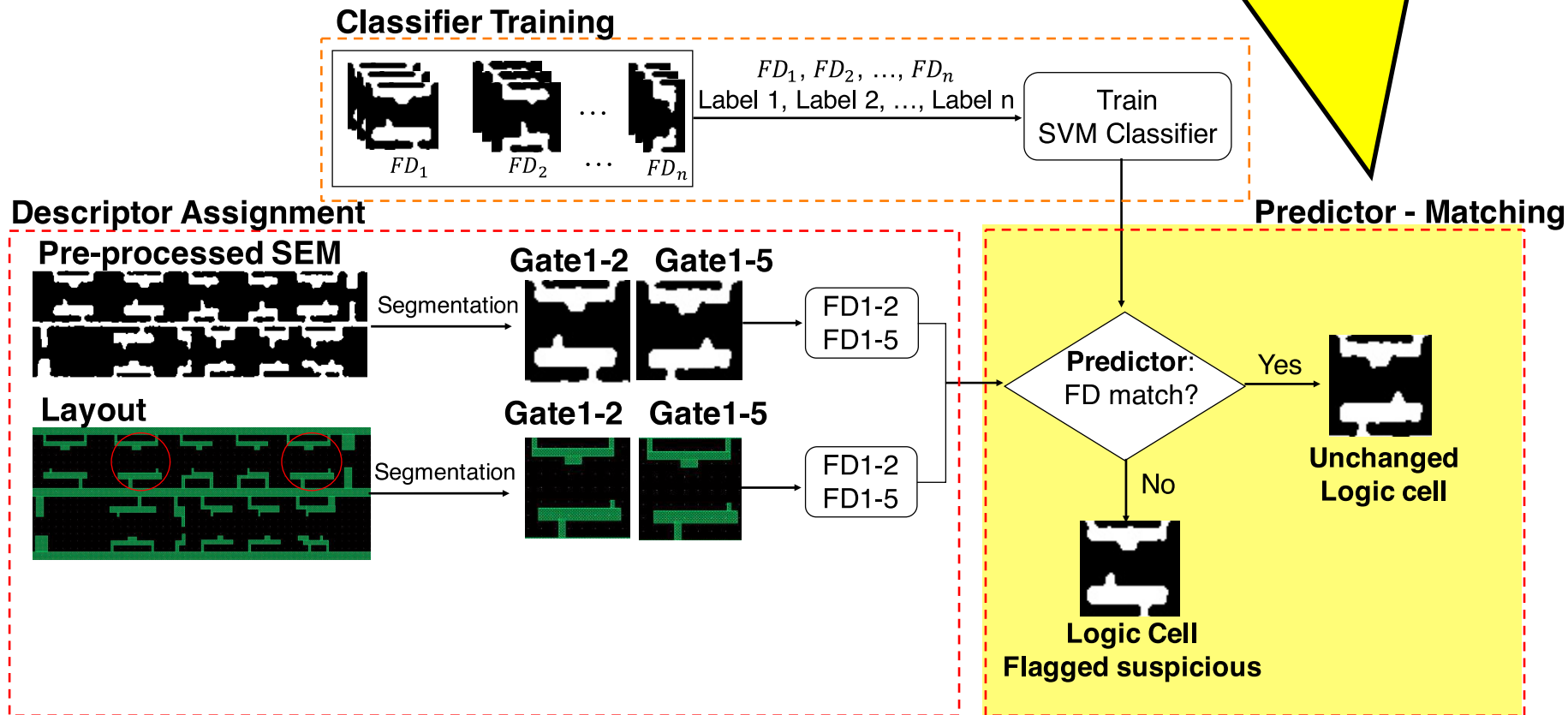
Classifier Training

Training machine learning model using different variations of a logic cell to account for imaging and manufacturing.

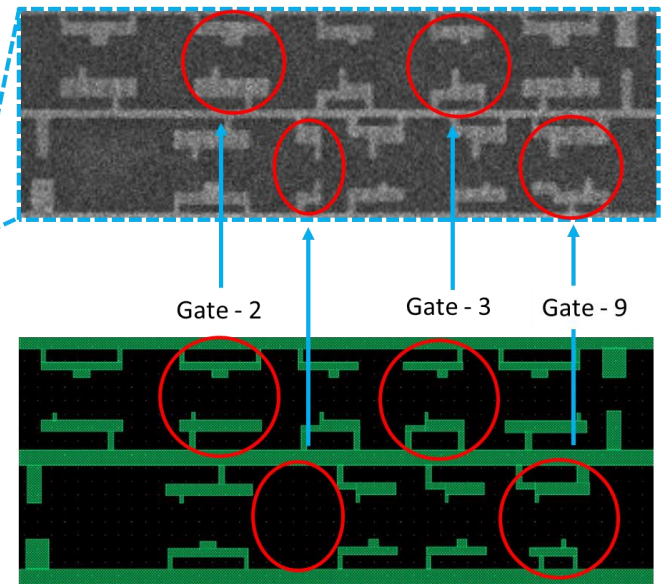
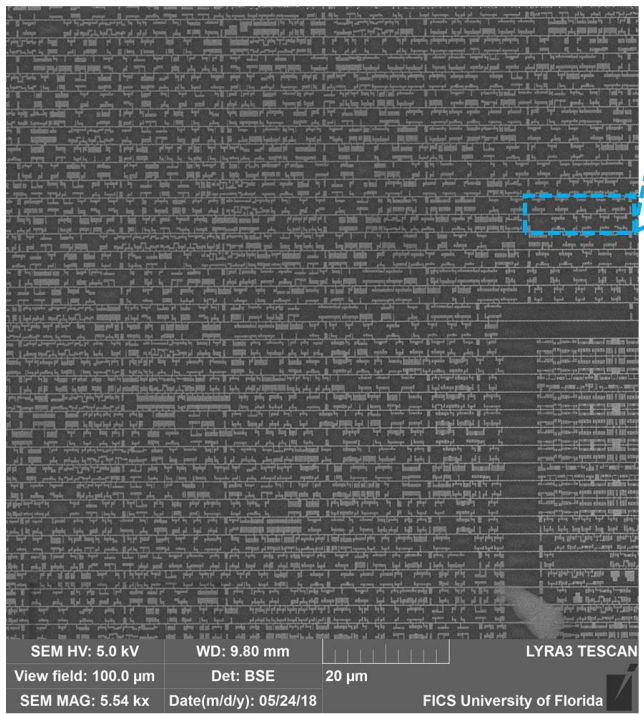


Predictor Matching

A machine learning based predictor matches the SEM and layout descriptors to detect a change.



Layout vs. SEM Image Comparison

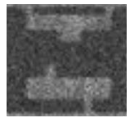


Layout showing doping region layers

1	2	3	3	2	4
5	X	6	7	8	9

Layout cell labels

Location 1: Row1, Cell 2



Detected: Modified Gate
 ↓
 not as Gate 2
Modification 1

Location 2: Row1, Cell 4



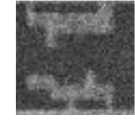
Detected: Modified Gate
 ↓
 not as Gate 3
Modification 2

Location 3: Row2, Cell 4



Existing: Gate (2)
 ↓
Insertion

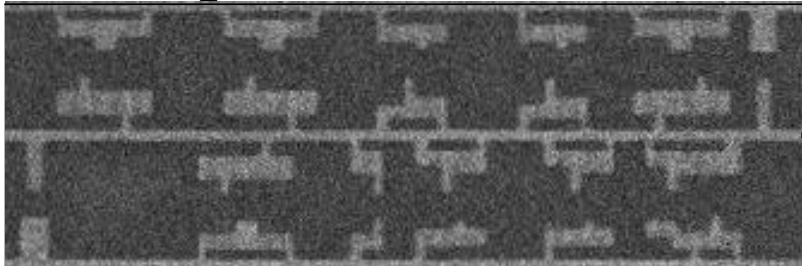
Location 4: Row2, Cell 7



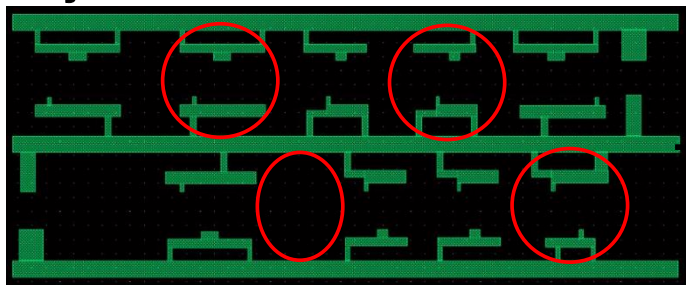
Detected: Modified Gate
 ↓
 not as Gate 9
Modification

Layout vs. SEM Image Comparison

SEM Image



Layout



Output Report

	✓	▲	✓	▲	✓	✓
✓	✓	✓	⊙	✓	✓	▲

- ✓ Clean
- ▲ Modified
- ⊙ Insertion/Deletion

1. Modification of logic cell

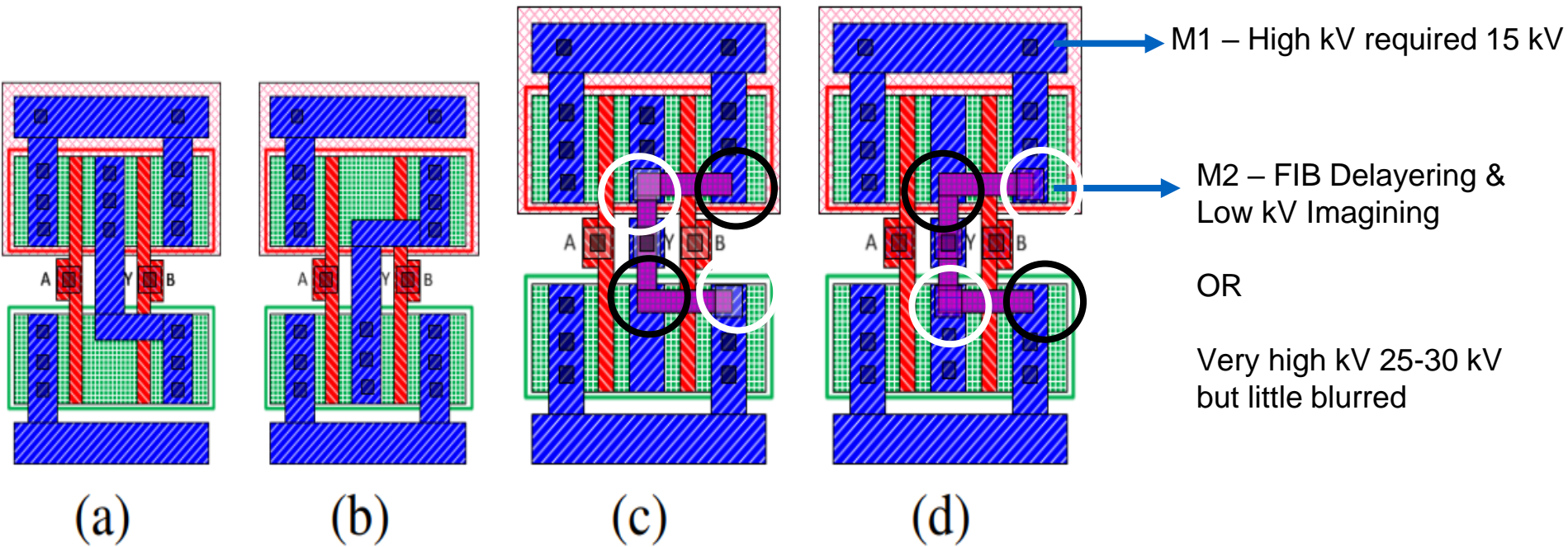
Logic cells encircled Location at 1, 2 and 4 are modified to emulate Trojan and successfully detected as change.

2. Insertion of logic cell

Logic cell insertion at empty space location 3 is detected as an insertion.

Trojan Scanner Challenges

Camouflage Cells Detection



Standard cell layout of regular 2-input (a) NAND and (b) NOR gate.
Camouflaged standard cell layouts of 2-input (c) NAND and (d) NOR gate.

RE vs Trojan Scanner

Reverse Engineering vs Trojan Scanner

	Full Reverse Engineering	Trojan Scanner
# of samples required	50-100	1
Detected Trojans	All Types	All types except reliability Trojans
Processing time	Months	hours
Functionality extraction	Required	Not required
Gate Identification	Required	Not required

Summary of Detection Methods

Hardware Trojans	Logic Test	Power SCA	Delay SCA	Run Time	Trojan Scanner
Functional	Maybe	Maybe	Maybe	Maybe	✓
Parametric	✗	✓	✓	✗	✓
Big	Maybe	✓	Maybe	✓	✓
Small	✓	✗	✓	Maybe	✓
Tight	✓	✓	✓	Maybe	✓
Loose	✓	Maybe	✓	Maybe	✓

- **IEEE transaction on image processing: Image Quality Assessment: From Error Visibility to Structural Similarity**
- **ACM TODAES: Hardware Trojans: lessons learned after one decade of research**
- **IEEE design & test of computers: A survey of hardware Trojan taxonomy and detection**