Trust Your Hardware by Physical Inspection

Matthias Ludwig (IFAG CSS M CS)
2023-01-24

About This Talk

The Bad

Reverse Engineering

The Good

› IP infringement
› Malicious modification (HTs)

› Benchmarking
› **Physical Verification**

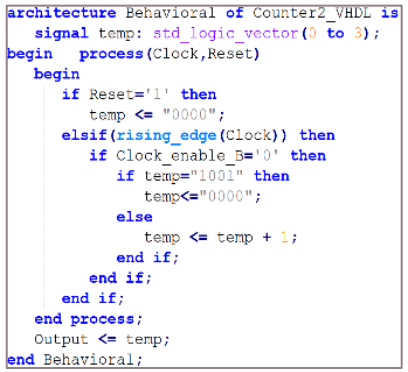
This talk

How to use RE / physical inspection to generate trust?

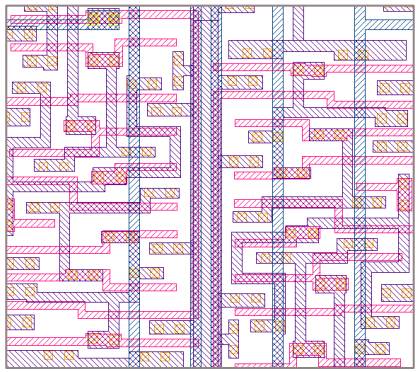
Table of contents

Trust & Security Threats Along the Distributed Value Chain

Design phase 2 3 | Fabrication phase 2 3 | Market

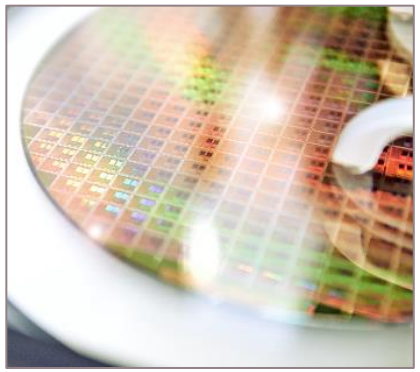


RTL 1

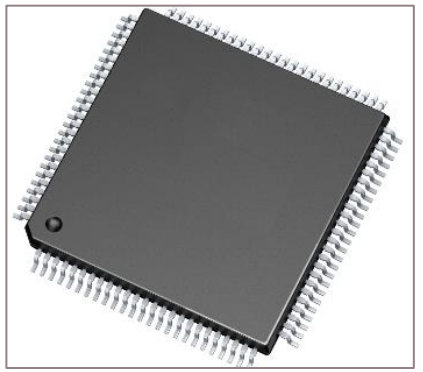


Layout 1

Photo masks 1



Wafer 1

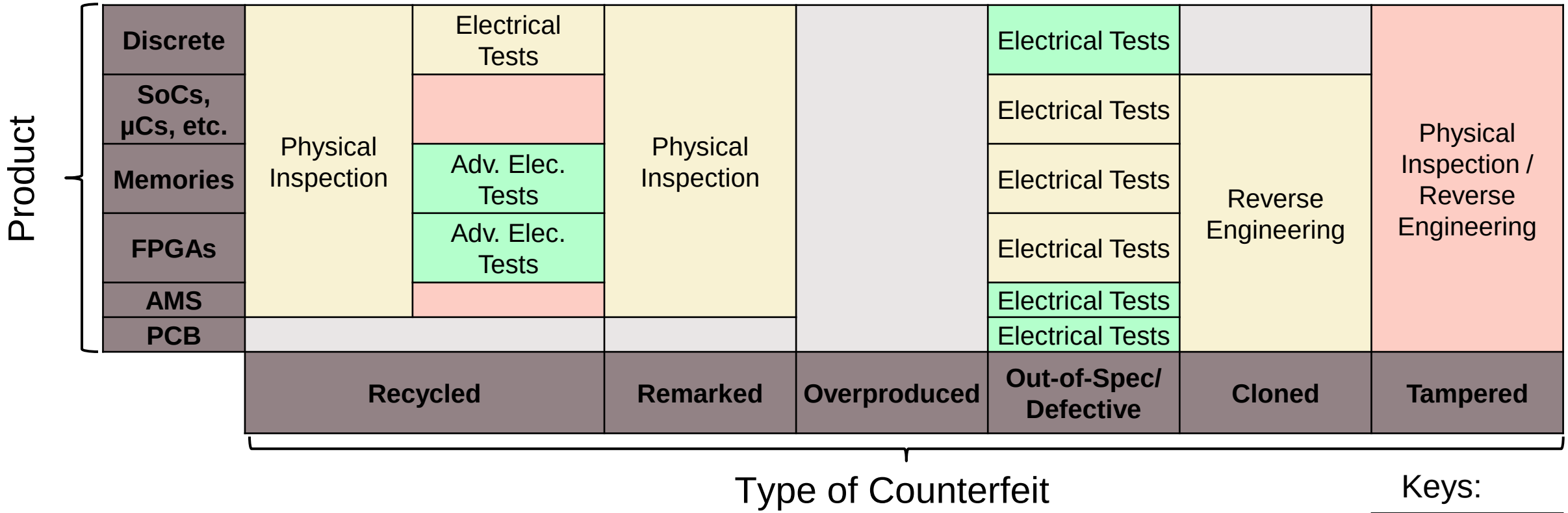


Product 2 3

Security threats due to outsourcing of design and fabrication to third parties:

1. **Hardware Trojans**: Insertion of malicious modifications
2. **IP stealing**: Extraction of intellectual property
3. **IC counterfeiting**: cloning, recycling, overproduction, etc.

Counterfeit *Landscape* 3

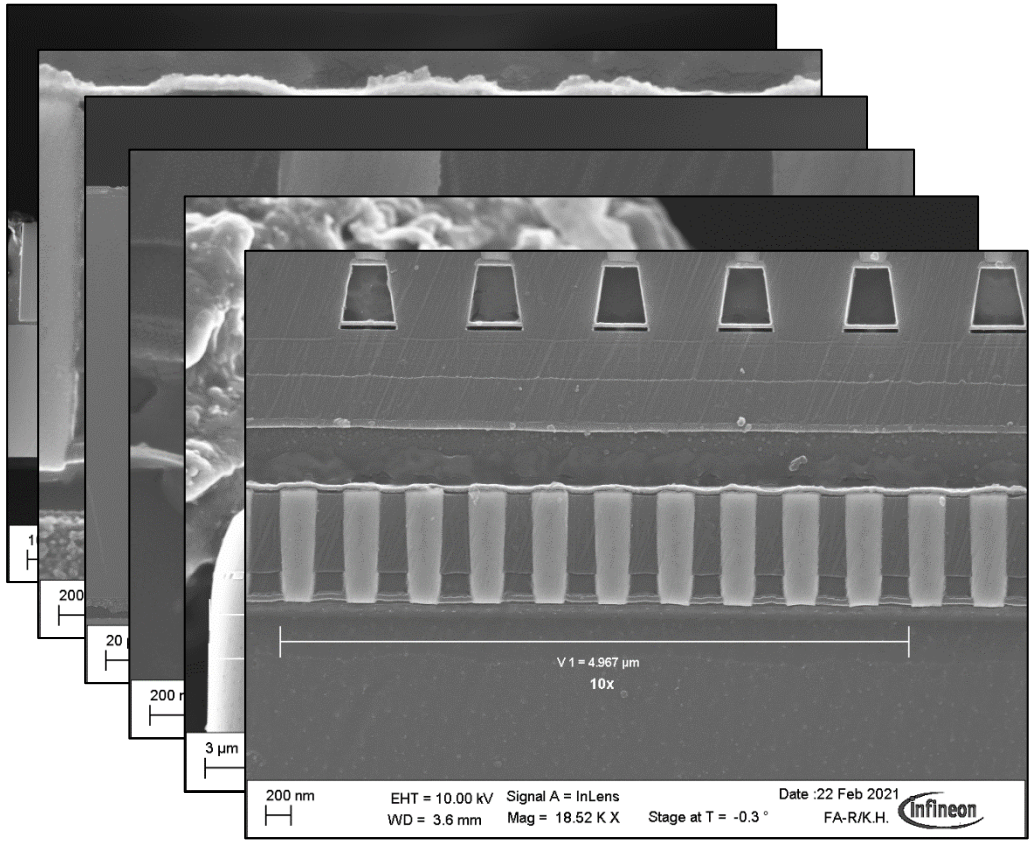


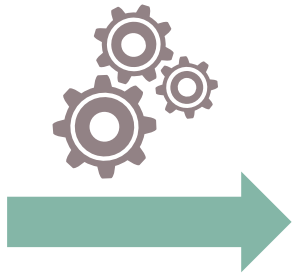
Keys:

N/A
Good
Needs Improvement
Unexplored or Inadequate

D. Forte, R.S. Chakraborty: Counterfeit Integrated Circuits: Threats, Detection, and Avoidance; Tutorial CHES2018

Visual Abstract of Our Approach





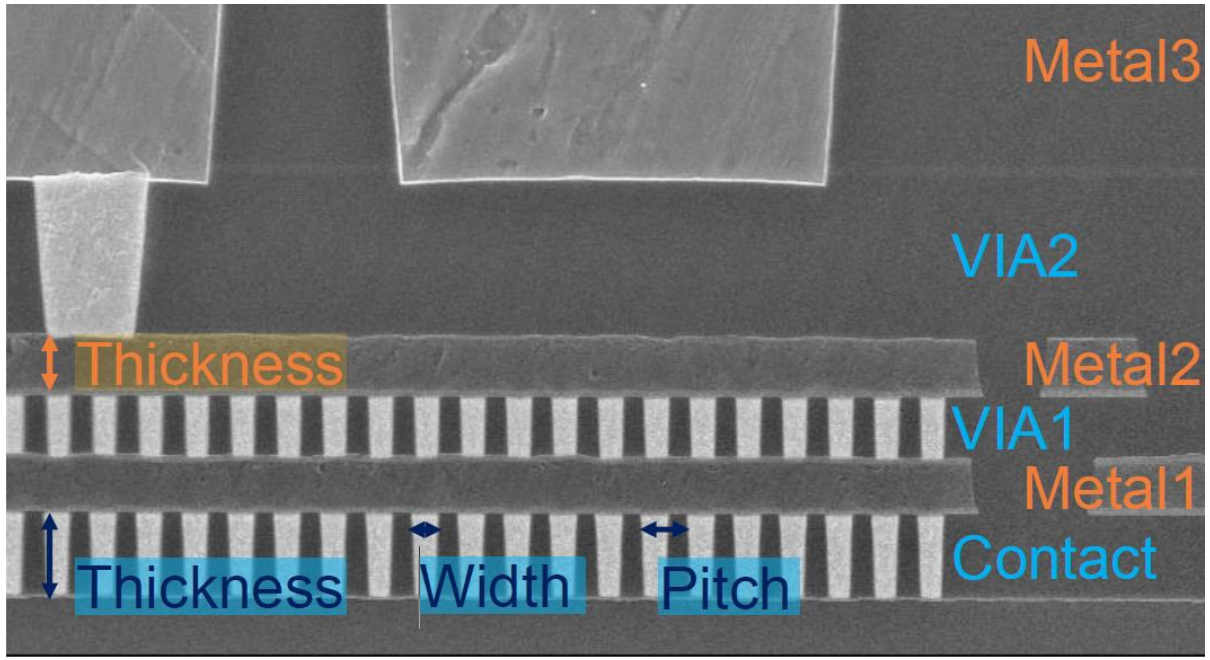
Tech_A21_180;
No counterfeit

Front-end Features

› List of characteristic features

Stage	Feature	Property
FEOL	Polysilicon_N	$[\text{Pitch, Thickness, Width}]_N$
	Shallow Iso	Type, Thickness
	Deep Trench	Type, Depth, Width
BEOL	Contact	Pitch, Thickness, Width
	Metal_N	$[\text{Pitch, Thickness}]_N$
	VIA_N	$[\text{Pitch, Thickness, Width}]_N$
	Type	{Copper, Alu/Tungsten}
General	Substrate	{e.g. Bulk-Si, SOI, GaN}
	Misc.	e.g. Passivation, Die Thickness

› Example: BEOL



Technical Implementation

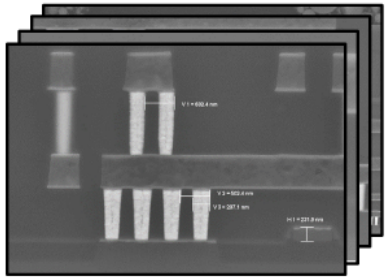
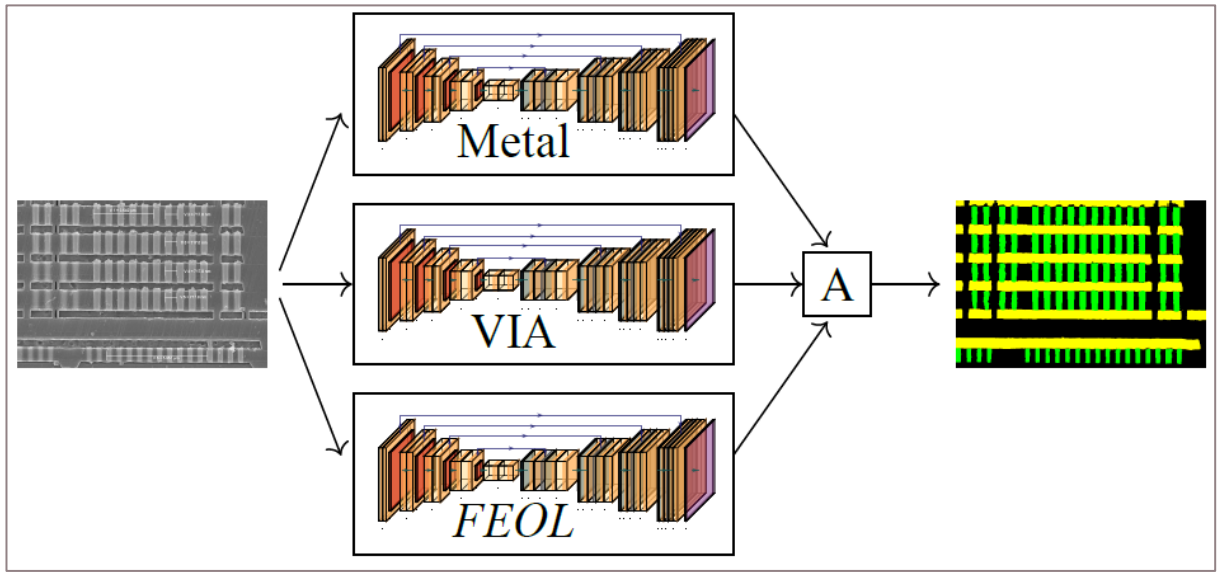


Image Segmentation

Data Interpretation

Counterfeit ✓ ⩒ ✗




```
1:  function FCheckForCounterfeit(Images, Meta, I)
2:      for all Images do
3:          SufficientQuality ← FImageQuality
4:          if SufficientQuality == TRUE then
5:              T_i ← FMeasurement(Image_i, Meta_i)
6:              T'_i ← FRegistration(Image_i, Meta_i)
7:          end if
8:      end for
9:      M ← FMerging(T')
10:     IsCounterfeit ← FProof(M, I)
11:     Return IsCounterfeit
12: end function
```

$$F(M,I) = \frac{1}{N_o} \cdot \sum_{i=1}^{N} f(M_i, I_i)$$

Example Images

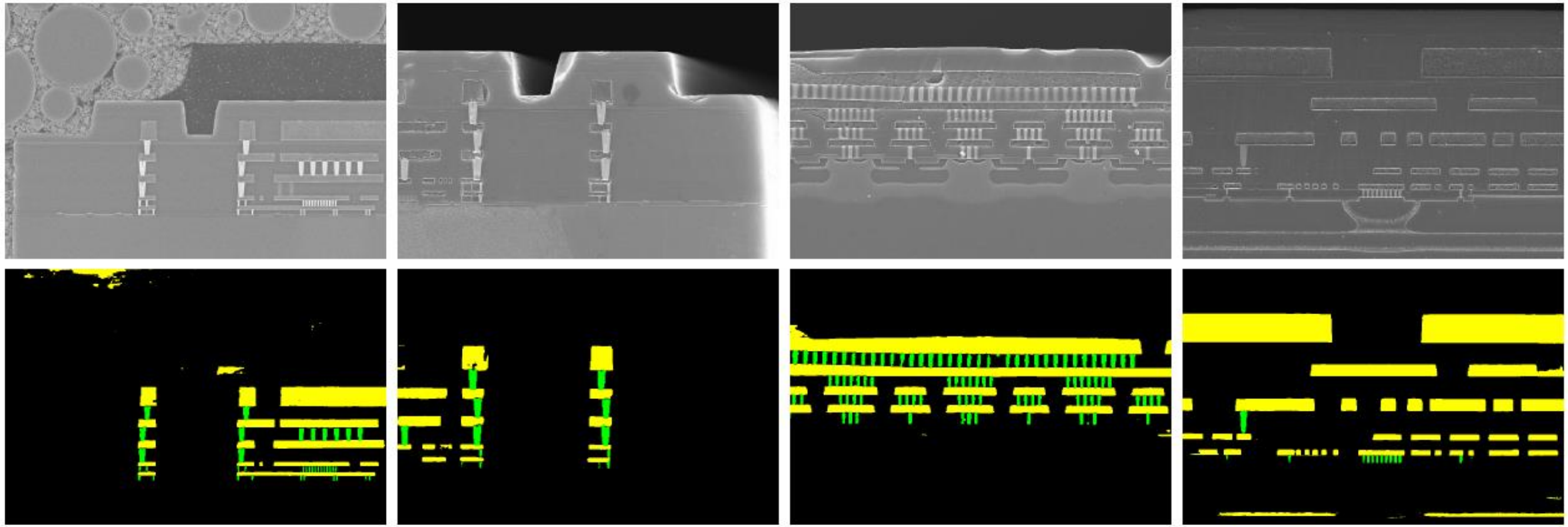


Fig. 9: Four example SEM cross-section images of semicondcutor devices and their segmented counterparts. They correspond to ID 2, 3, 4, and 6 from table IV and depict a comparable zoom level.

Counterfeit Experiment

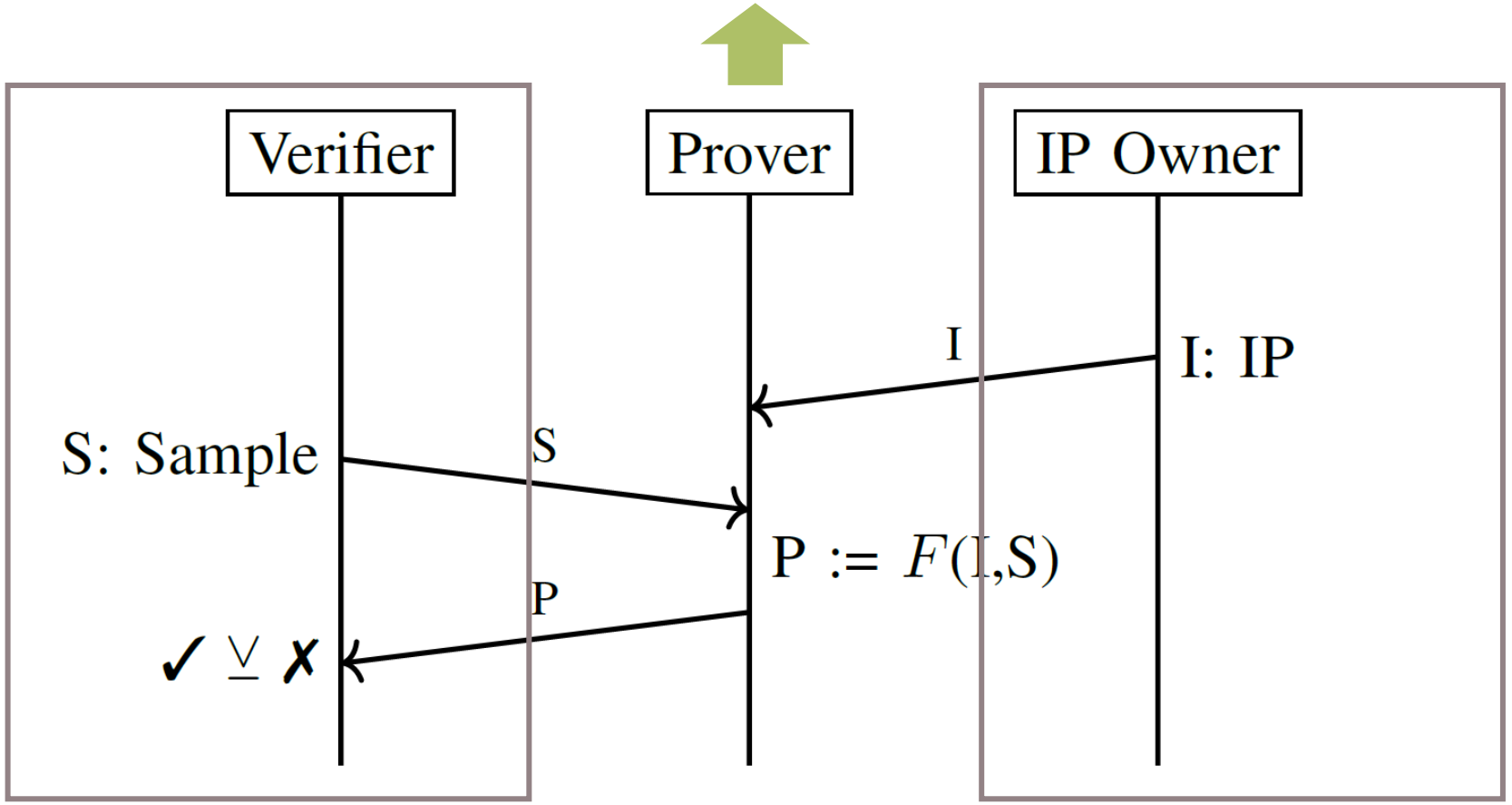
ID	CF	Images	Pitch, Thickness, Width [nm]; Contact	Thickness [nm]; M1; M2; M3; M4; M5; M6; M7	Pitch, Thickness, Width [nm]; V1; V2; V3; V4; V5; V6	Distance (F)	Is CF?
1	✗	30	430, 877, 182	604; 506; 506; *874*; *879*	{470, 807, 308; n.a., 861, 484; n.a., *395*, n.a.}	0.10	✗
2	✗	27	491, 938, 244	646; 708; 1385; 1395; 3325	{495, 1061, 245; n.a., 2404, 571; 1957, 2307, 822; n.a., 2393, 571}	0.04	✗
3	✗	19	459, 812, 194	645; 757; 1553; 1456; 3650	{503, 1068, 194; n.a., 2455, 777; n.a., 2375, 777; n.a., 2423, 1096}	0.16	✗
4	✓	53	477, 899, 214	613; 664; 813; 1108	{495, 762, 232; 523, 777, 214; 719, 938, 232}	**1.18**	✓
5	✗	25	488, 865, 207	669; 687; 3271	{494, 633, 208; 2162, 1773, 1229}	0.08	✗
6	✗	31	505, 890, 219	675; *2216*; *723*; 1468; 1426; *3298*	{506, 986, 255; n.a., 1064, n.a.; n.a., 2638, 851; n.a., 936, 2426; *n.a., 2447, n.a.*}	0.26	✗
7	✗	28	424, 758, 157	641; 715; 777; 1296; 1259; *8740*; 3037	{493, 994, 195; 502, 629, 129; 613, 1901, 301, 3168, 2074, 667; 2901, 1815, 815; 2901, 1889, 667}	0.21	✗

- Approach is robust to measurement errors
- Forged device was confidently detected

What Is Missing?

› Trusted third-party
› Prover meets requirements of *Verifier* and *IP Owner*

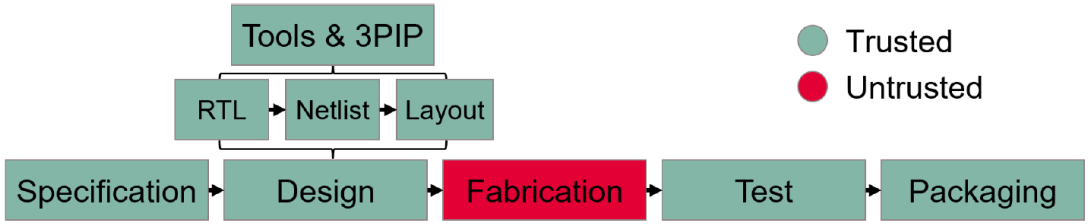
› Costumer

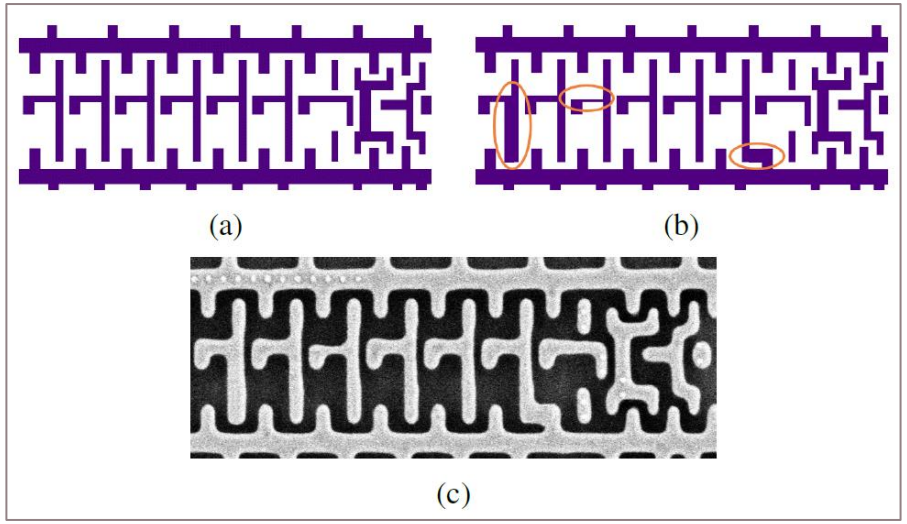


› Foundries
› IDMs

Motivation 1

› Assumed Threat Model

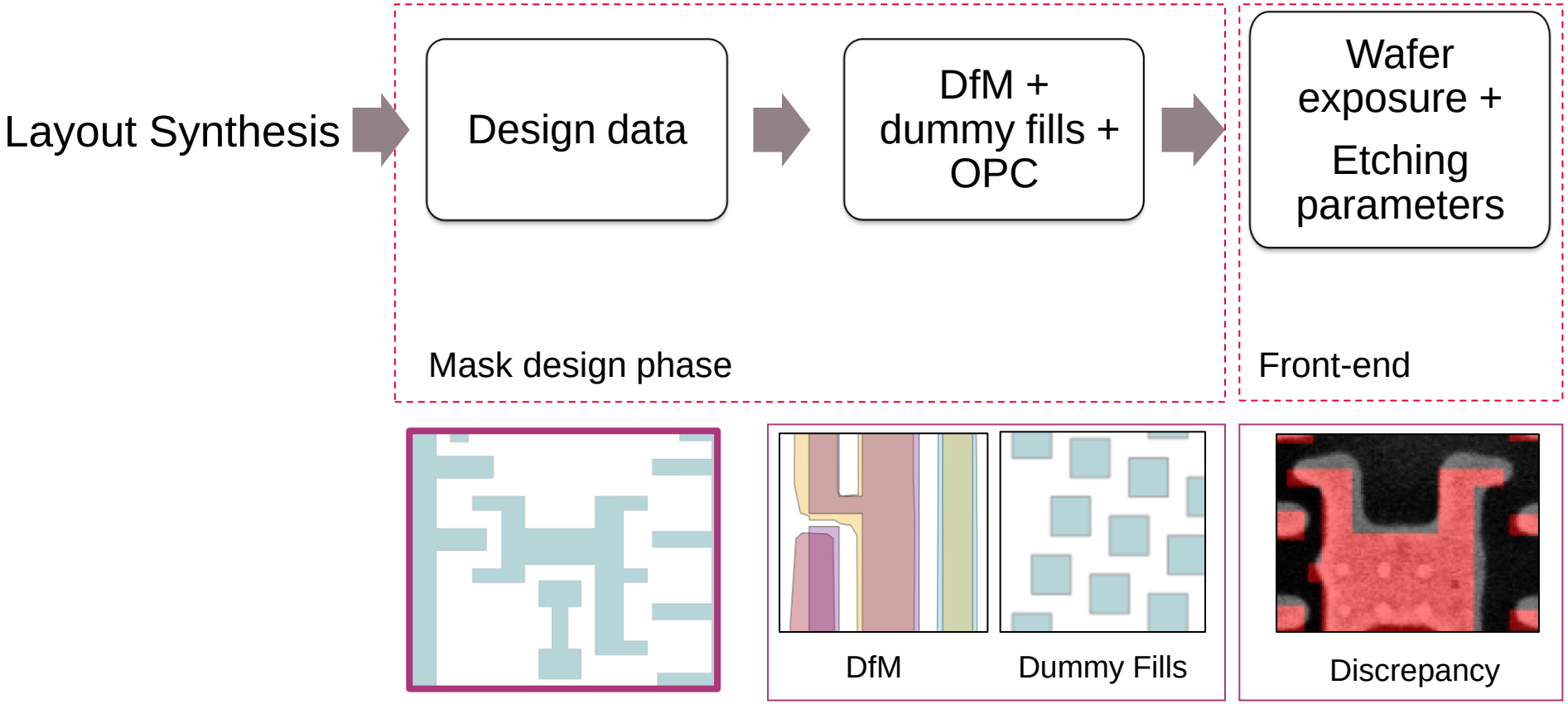




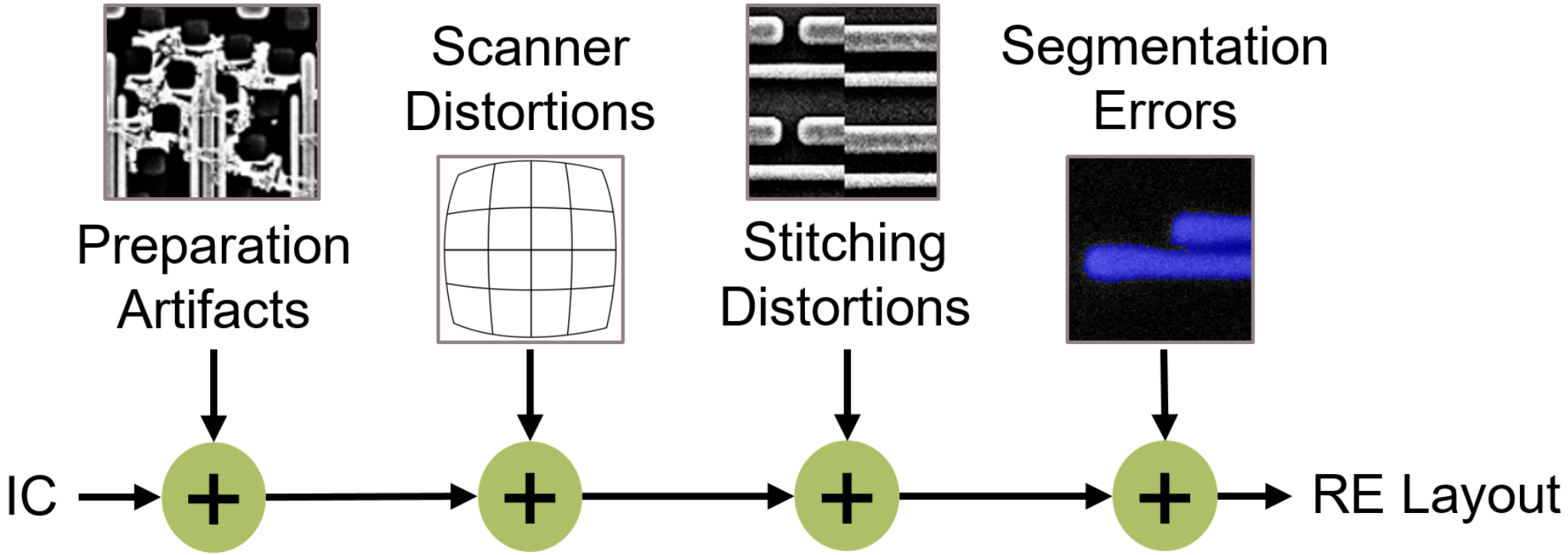
› **Verification and Validation (V&V) Framework**

› **Reverse Engineering Process Assessment**

Physical Layout Post-Processing

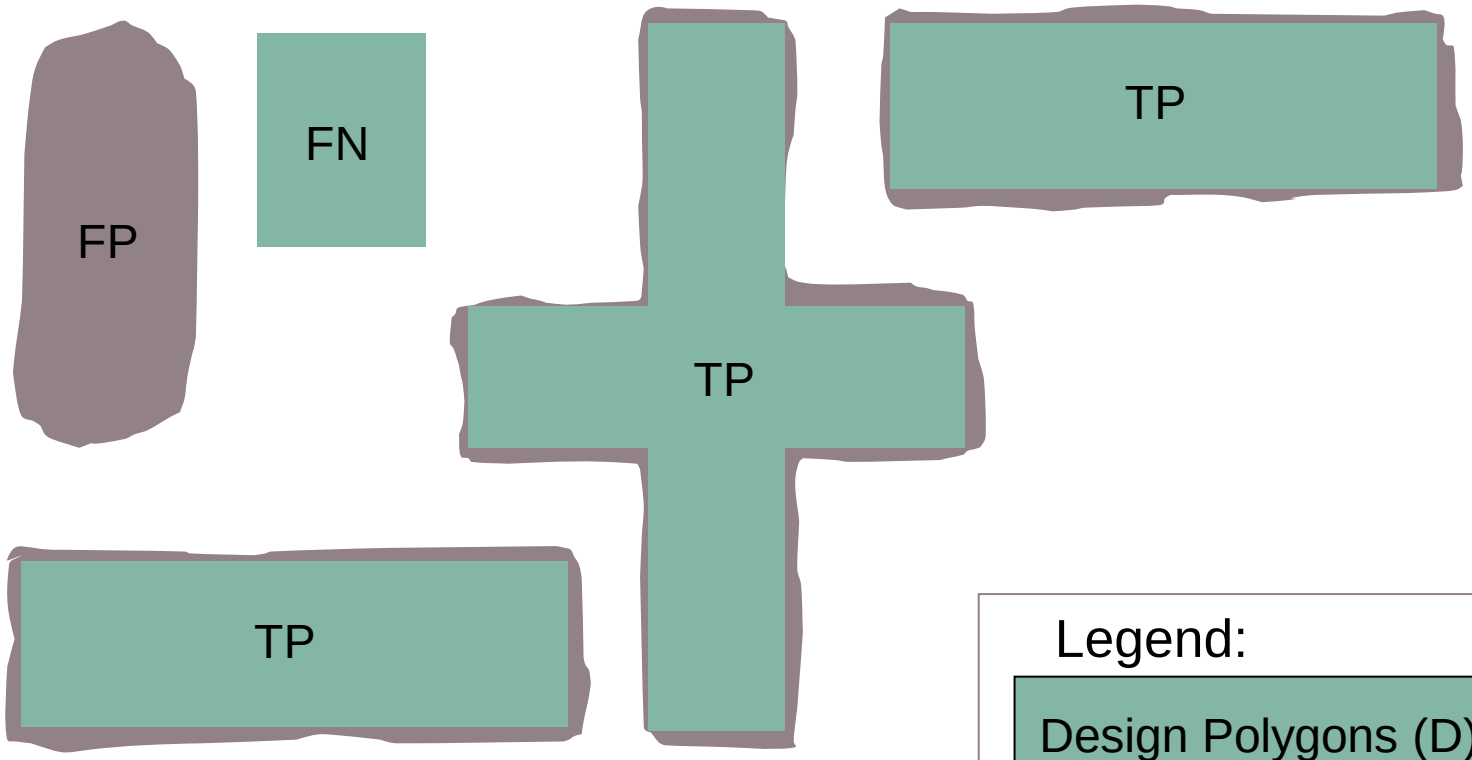


Reverse Engineering Process “Error Function“



Pre-Requisite: Scoring Figures

› Example Polygon Set

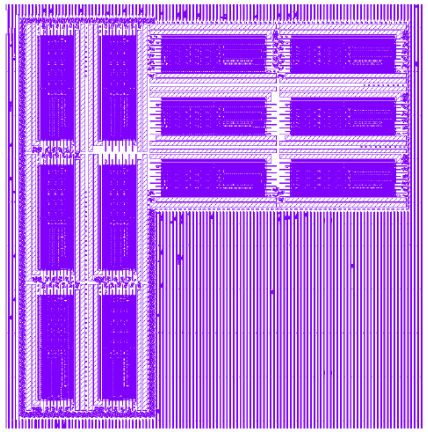


$$\text{Precision: } P = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

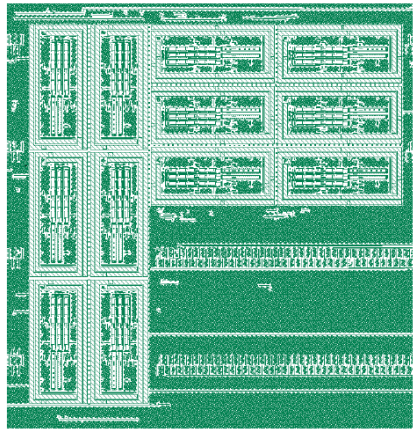
$$\text{Recall: } R = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

$$F_1 \text{ Score: } F_1 = 2 \cdot \frac{P \cdot R}{P + R}$$

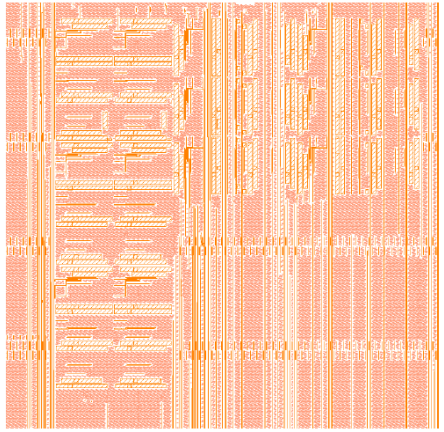
Physical Verification: Layout Data



(a) GDSII excerpt of Metal 1

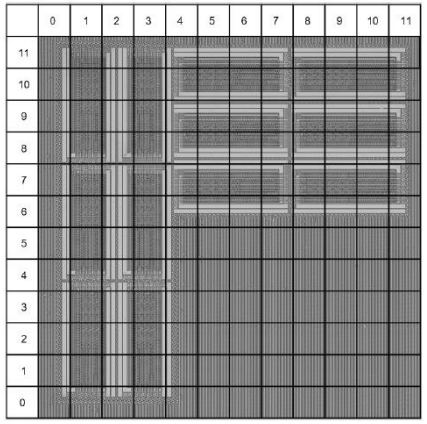


(b) GDSII excerpt of Metal 2

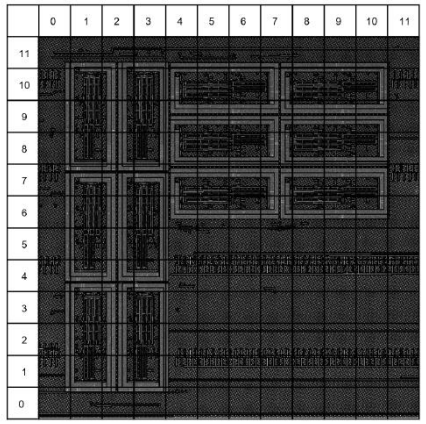


(c) GDSII excerpt of Metal 3

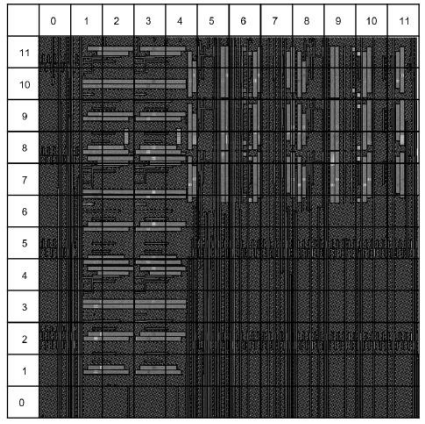
Figure 5: Physical layout of the evaluated test sample.



(a) Mosaic of Metal 1

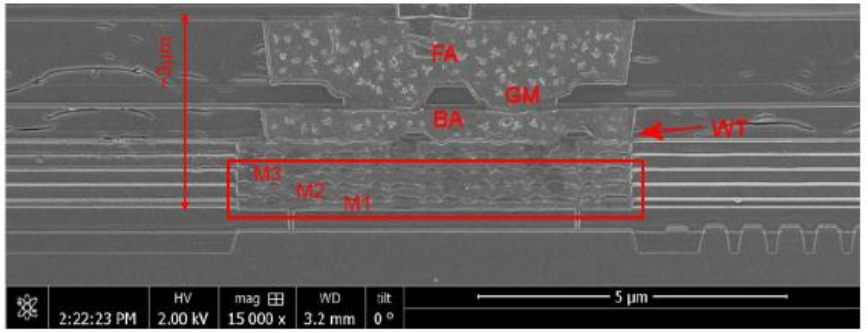


(b) Mosaic of Metal 2

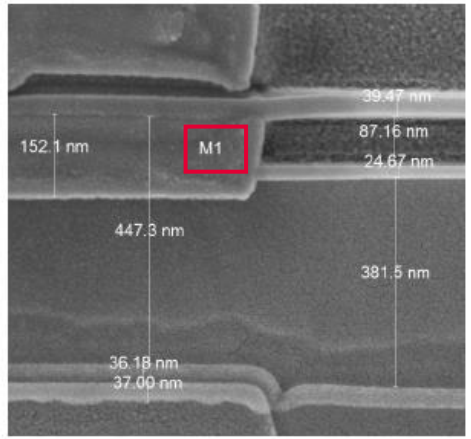


(c) Mosaic of Metal 3

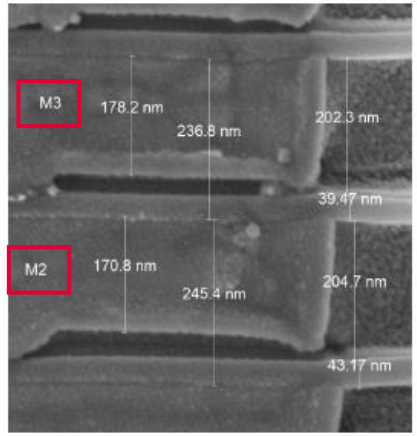
Figure 7: Scanned layers of the 40 nm test sample. The grid indicates the individual SEM scans.



(a)



(b)



(c)

Physical Verification: Results

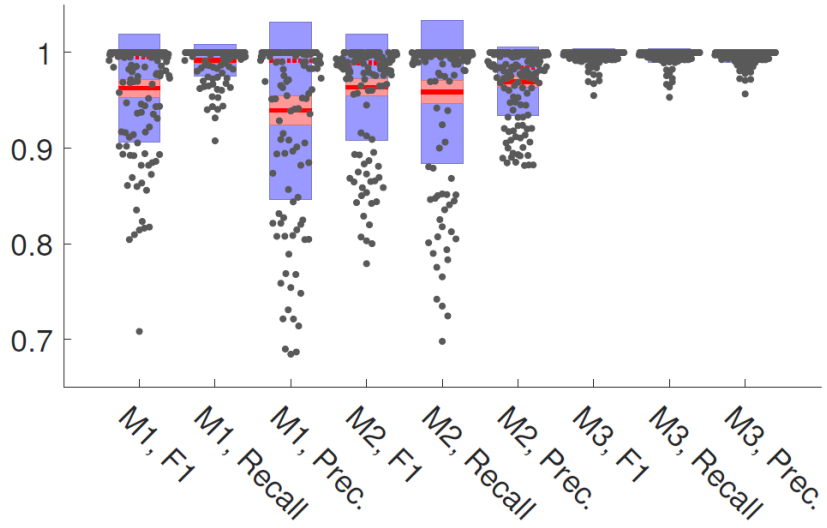
Equal Scanner Settings: Scanner type: *Raith CS150 Two*; Detector: *ET-SE*; Field of view: *16.0µm*; Pixel Size: *4.0nm*; Pixel dwell time: *6.0µs*; Image resolution: *16Mpx* (4000 x 4000); Bit depth: *8 Bit*; Grid: *12 x 12*

	Scanner Settings		Image Processing			
Layer	Acc. Volt.	Focus	Stitching Method	Pre-Processing	Segmentation Method	Post-Processing
Metal 1	3.5 kV	4.96 mm	NCC (local), MLE (global)	Median Filter (1 x), Kernel: 5 x 5	Edge Detection, gradient oriented flood-fill	Vertex simplification, Deletion ($<70\,\mathrm{Px}^2$)
Metal 2	7.0 kV	4.95 mm	NCC (local), MLE (global)	Median Filter (7 x), Kernel: 5 x 5	Thresholding	Vertex simplification, Deletion ($<100\,\mathrm{Px}^2$)
Metal 3	7.0 kV	5.00 mm	NCC (local), W-LMS (global)	Median Filter (3 x), Kernel: 5 x 5	Edge Detection, gradient oriented flood-fill	Vertex simplification, Deletion ($<100\,\mathrm{Px}^2$)

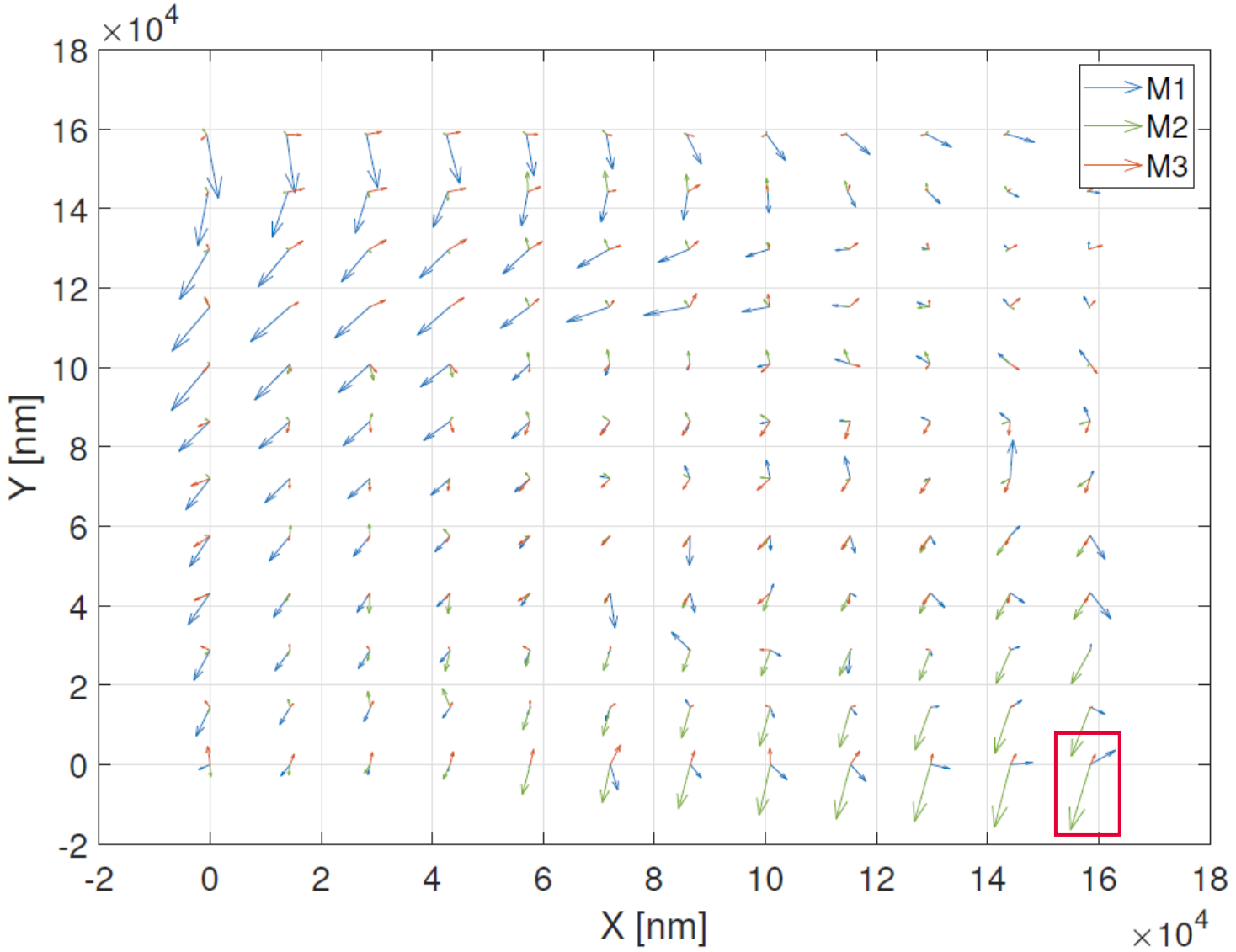
	Without *DfM*			With *DfM*			No. of polygons	
Layer	F1 Score(%)	Precision(%)	Recall(%)	F1 Score(%)	Precision(%)	Recall(%)	GDS	RE
Metal 1	92.54	89.55	95.73	95.70 (+3.18)	92.63 (+3.08)	99.03 (+3.30)	30,386	32,486
Metal 2	95.00	95.13	94.87	97.92 (+2.92)	98.05 (+2.92)	97.79 (+2.92)	46,429	46,302
Metal 3	97.16	97.15	97.18	99.66 (+2.50)	99.64 (+2.49)	99.67 (+2.49)	44,680	44,693

- Only statistically evaluated via polygon features
- *Normal* mode without user input

- Technology-specific DfM measures considered
- Larger area for RE polygons allowed

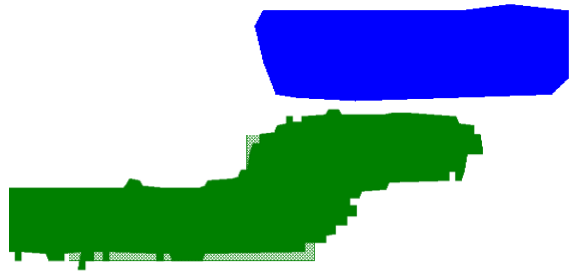


2D Mosaic Aberrations

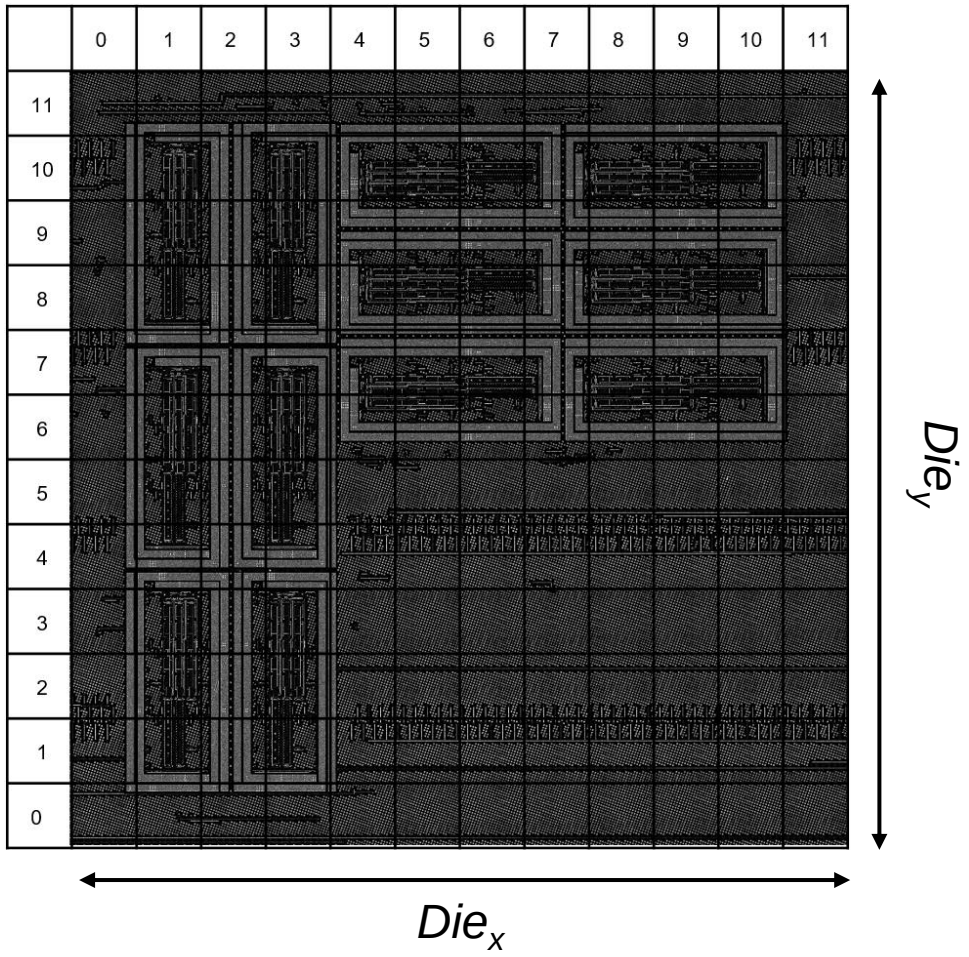


	Deviation [nm]
M1 Avg.	19
M1 max.	56
M2 Avg.	13
M2 max.	65
M3 Avg.	8
M3 max.	18

- Minimum dimensions on M1 and M2 are 70 nm
- **Consequence:** 3D Alignment not possible



Scan Time Evaluation

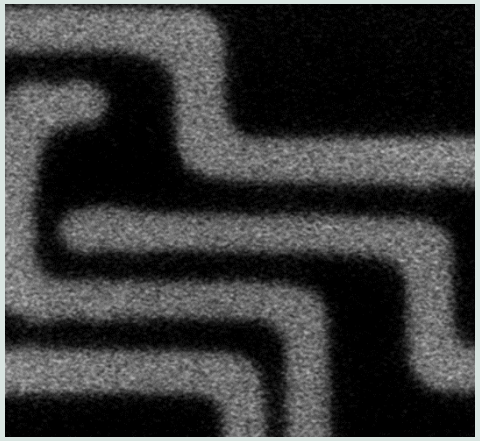
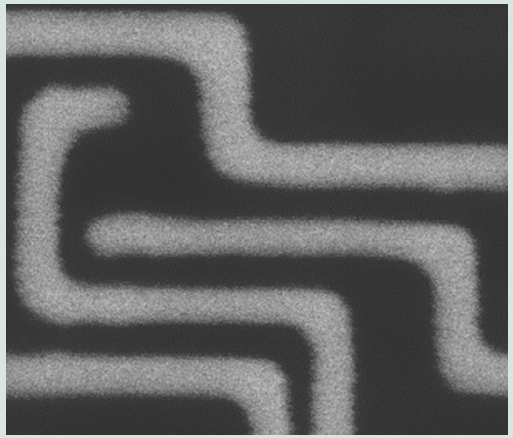
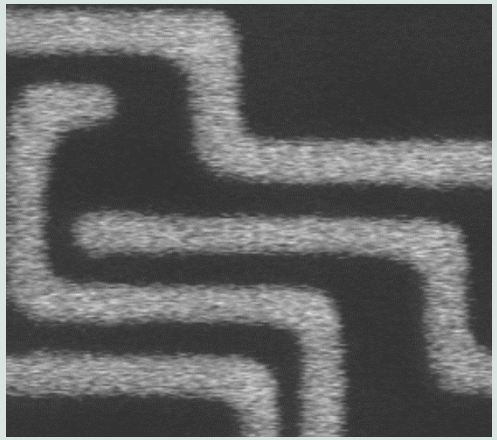


$$T_{Total} = k \cdot \frac{Die_x \cdot Die_y}{Res^2} \cdot t_{dwell}$$

- *k:* Factor of processing overhead
- Die_x: Die-length in x-direction [m]
- Die_y: Die-length in y-direction [m]
- *Res:* Resolution per pixel [m/px]
- t_{dwell}: Dwell time per pixel [s/px^2]

FoM Comparison

	F1-Score	Precision	Recall	IoU	Measured Time
CS150 Two (t_{dwell}: *6 µs)*	**97.59%**	96.63%	98.57%	6.08%	03h 46min 11s
eSCAN 2018 (t_{dwell}: *30 ns)*	**98.10%**	97.61%	98.59%	6.46%	00h 10min 12s
eSCAN 2018 (t_{dwell}: *500 ns)*	**99.04%**	98.84%	99.24%	5.49%	00h 28min 25s

CS150 Two *t_{dwell}: 6 µs*	**eSCAN 2018** *t_{dwell}: 500 ns*	**eSCAN 2018** *t_{dwell}: 30 ns*
		

Conclusion

Counterfeit detection possible through evaluation of technological device features.

Full V&V workflow to handle **DfM, manufacturing**, and **RE process variations**.

Sample preparation and distortion-free mosaicking still **major bottle-necks** especially for larger areas and advanced technology nodes.

Part of your life. Part of tomorrow.

References (On Counterfeit Detection)

1 Ludwig, M.; Lippmann, B.; Bette, A.-C. & Lenz, C.
Demo: A Fully Automated Process for Semiconductor Technology Analysis through SEM Cross-Sections
25th International Conference on Pattern Recognition (ICPR), **2021**

2 Ludwig, M.; Purice, D.; Lippmann, B.; Bette, A.-C. & Lenz, C.
Towards Fully Automated Verification of Semiconductor Technologies
Artificial Intelligence for Digitising Industry - Applications, River Publishers, **2021**, 147-160

3 Pollach, M.; Schiegg, F.; Ludwig, M.; Bette, A.-C. & Knoll, A.
Boundary Enhanced Semantic Segmentation for High Resolution Electron Microscope Images
2022 30th European Signal Processing Conference (EUSIPCO), **2022**

4 Purice, D.; Ludwig, M. & Lenz, C.
An End-to-End AI-based Automated Process for Semiconductor Device Parameter Extraction
Industrial Artificial Intelligence Technologies and Applications, River Publishers, **2022**, 53 - 72

5 Ludwig, M.; Bette, A.-C.; Lippmann, B. & Sigl, G.
Counterfeit Detection by Semiconductor Process Technology Inspection (accepted)
28th IEEE European Test Symposium, IEEE, **2023**

References (On Layout Verification)

1

Singla, A.; Lippmann, B. & Graeb, H.
Verification of Physical Chip Layouts Using GDSII Design Data
2019 IEEE 4th International Verification and Security Workshop (IVSW), IEEE, **2019**, 55-60

2

Lippmann, B.; Unverricht, N.; Singla, A.; Ludwig, M.; Werner, M.; Egger, P.; Duebotzky, A.; Graeb, H.; Gieser, H.; Rasche, M. & Kellermann, O.
Verification of physical designs using an integrated reverse engineering flow for nanoscale technologies
Integration, Elsevier BV, **2020***, 71*, 11-29

3

Ludwig, M.; Lippmann, B. & Unverricht, N.
Zachäus, C. & Meyer, G. *(Eds.)*
Enabling Trust for Advanced Semiconductor Solutions Based on Physical Layout Verification
Intelligent System Solutions for Auto Mobility and Beyond, Springer International Publishing, **2021**, 87-103

4

Ludwig, M.; Bette, A.-C. & Lippmann, B.
ViTaL: Verifying Trojan-Free Physical Layouts through Hardware Reverse Engineering
2021 IEEE Physical Assurance and Inspection of Electronics (PAINE), IEEE, **2021**, 1-8