FICHSA 2019

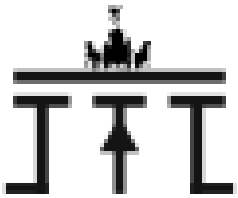
Contactless Fault Isolation in ICs

=

Trailblazer of Hardware Attacking

C. Boit

Technische Universität Berlin
Germany



Semiconductor Devices

Intro: Among the side channel attacks…

Side channel attacks of digital ICs are evaluating analog signals that come with the digital data stream…

(Differential) Power Analysis

Timing Analysis

Electro Magnetic Analysis

Fault Injection (part of CFI)

Light emission (part of CFI)

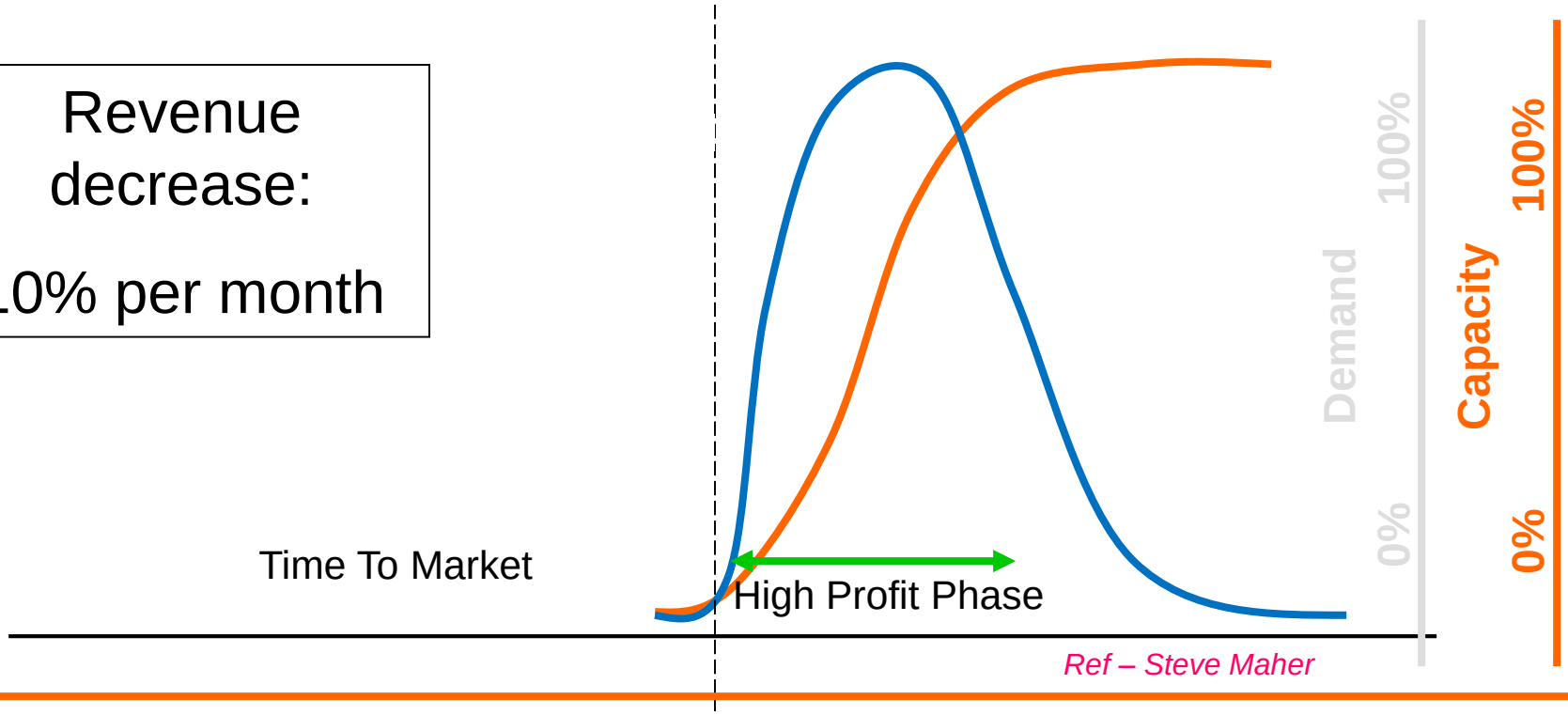
CFI is a much wider field of techniques made for a purpose in IC development

What makes CFI one of the highest hardware security risks?

Time to Market: Critical Factor in IC Development

Revenue decrease:

10% per month

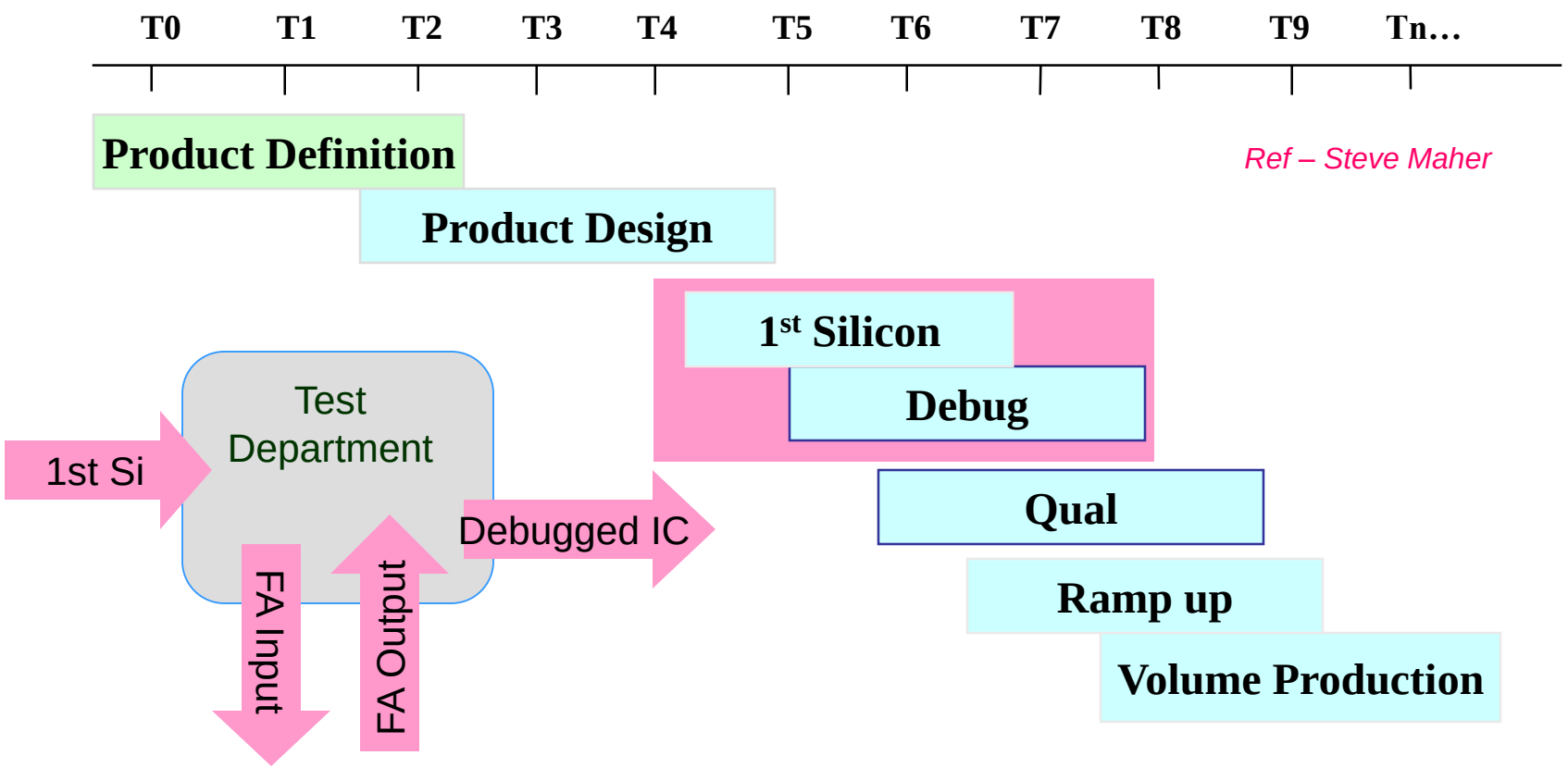


Time to market reduction:

Acceleration of design, technology development, ramp up and…

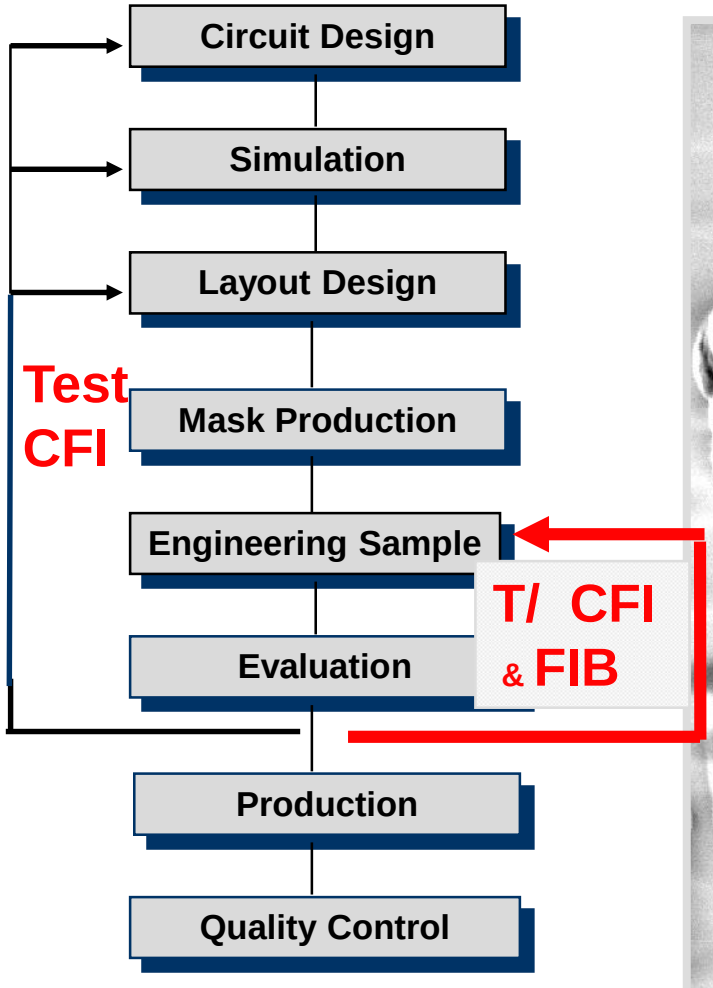
debug (readiness of tests & CFI techniques to new product)

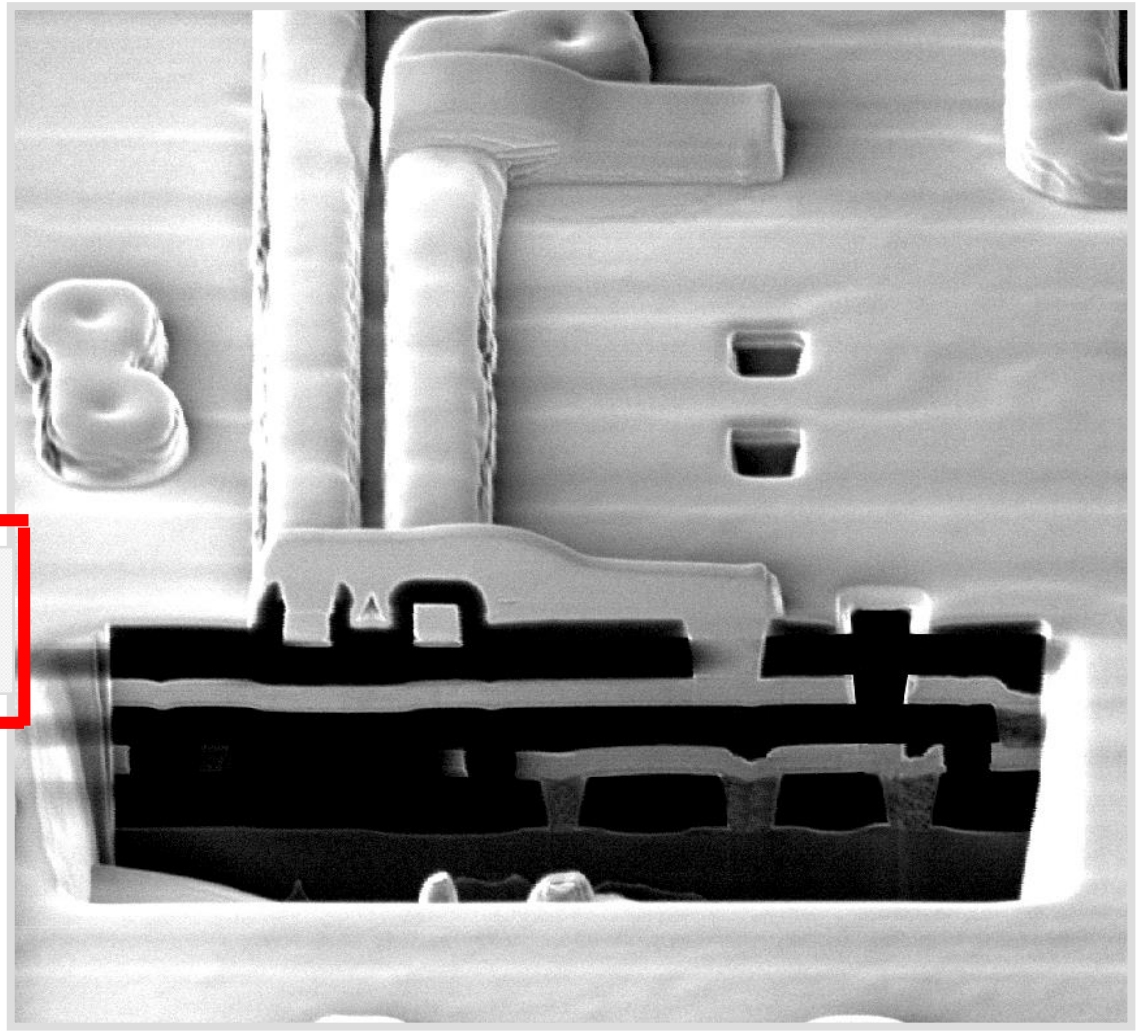
IC Development Process Silicon Debug



Test shows performance of IC
If spec fails, redesign is necessary
Where? Contactless Fault Isolation will tell

Debug with Test, CFI & FIB Circuit Edit





Source: Infineon

Why is CFI one of the highest hardware security risks?

It is not just another side channel access

It has been created for an own pupose within IC delopment

Time to market and performance optimization depend on professional CFI as integrated in IC development process

IC debug and Failure Analysis have their agenda to match shrinking node size into nanoscale

→ now, let‘s have a look into the history and today‘s agenda

Outline

Why contactless Fault Isolation in ICs

Technology Node and CFI Evolution

The Benefits of CFI Backside Approach

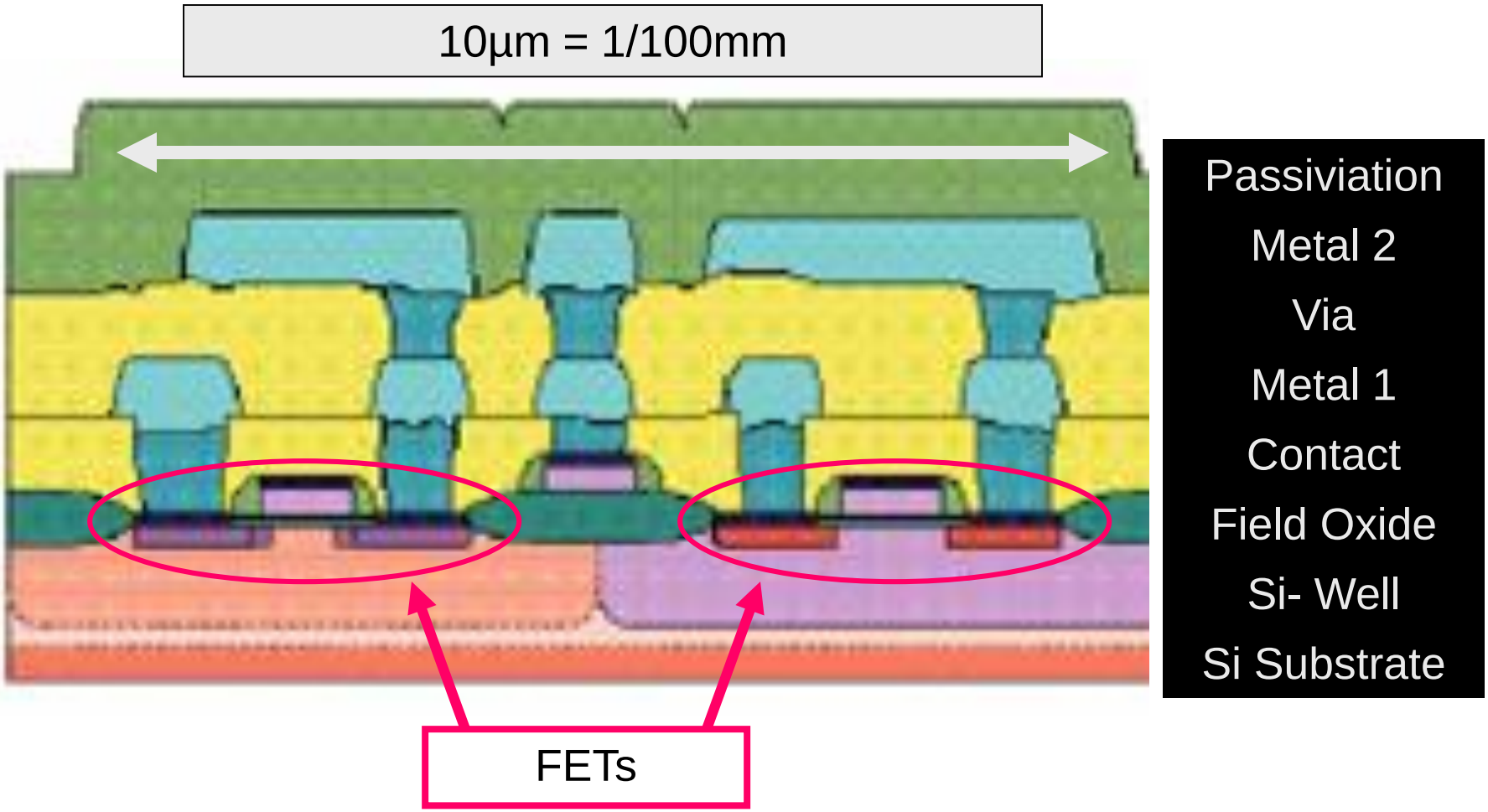
Relevant CFI Techniques and Attack Risks

IoT Roadmap: Nanoscale FinFET & Low Power

CFI will prevail and the Attack Risk with it

Backside Protection

IC of 1µm Node Technology (~1990)

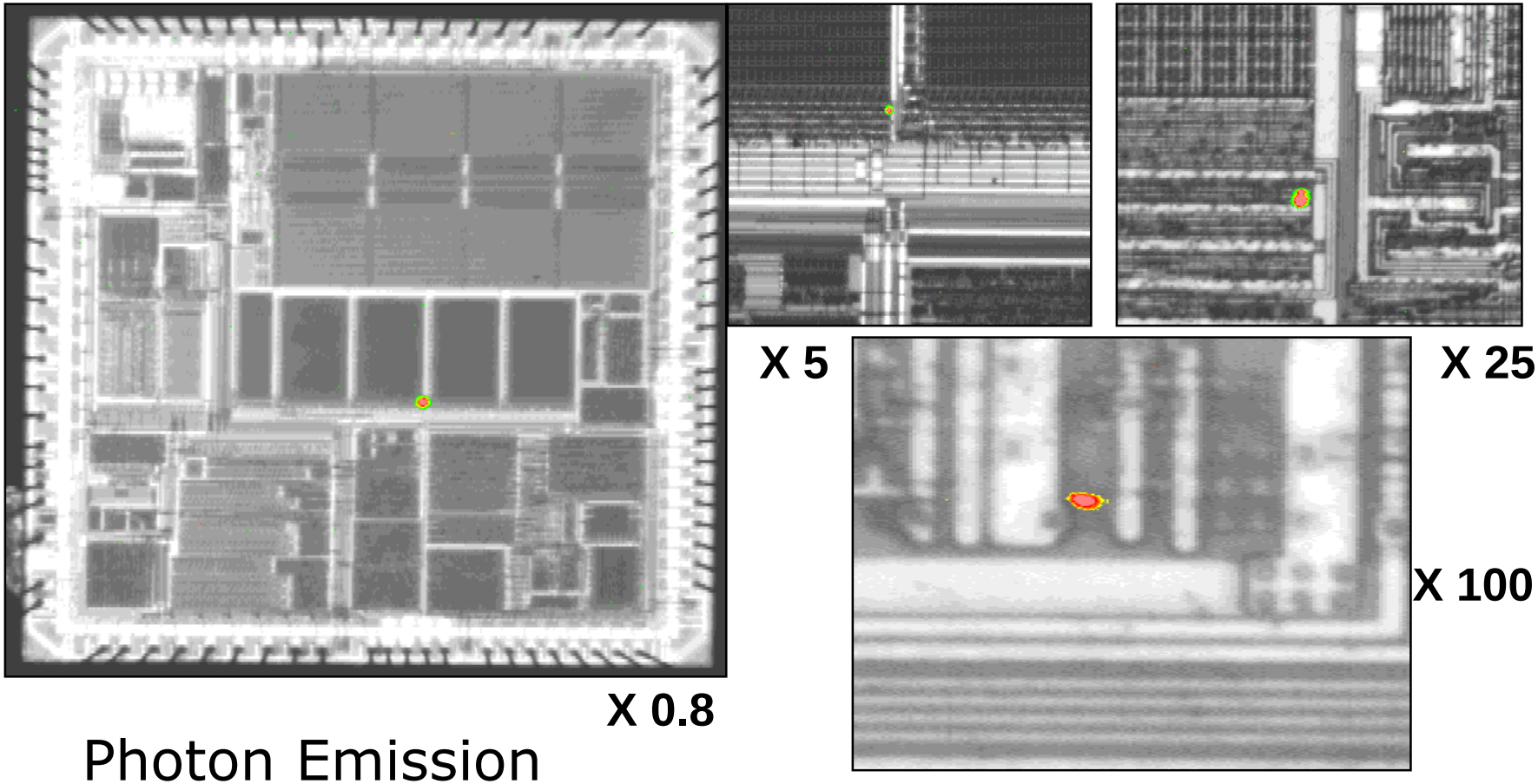


IC Contactless Fault Isolation (CFI)

R ≈ 0.61λ/NA NA: Numerical Aperture

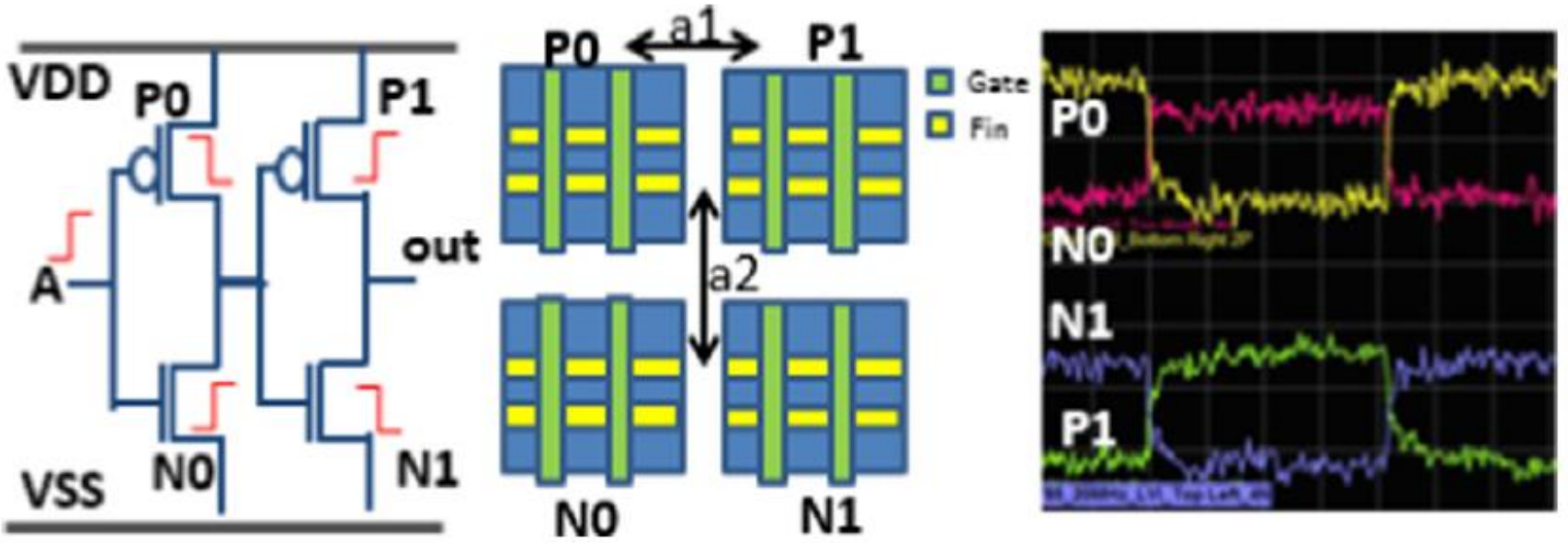
λ: Light wavelength (NIR: ≈ 1μm)

NA= sinα: Aperture of Objective (<1)



Photon Emission

IC Contactless Probing (subject to CFI as well)



Understanding spatial resolution of laser voltage imaging

V.K. Ravikumar[a,b,*], G. Lim[b,c], J.M. Chin[b], K.L. Pey[a], J.K.W. Yang[a]

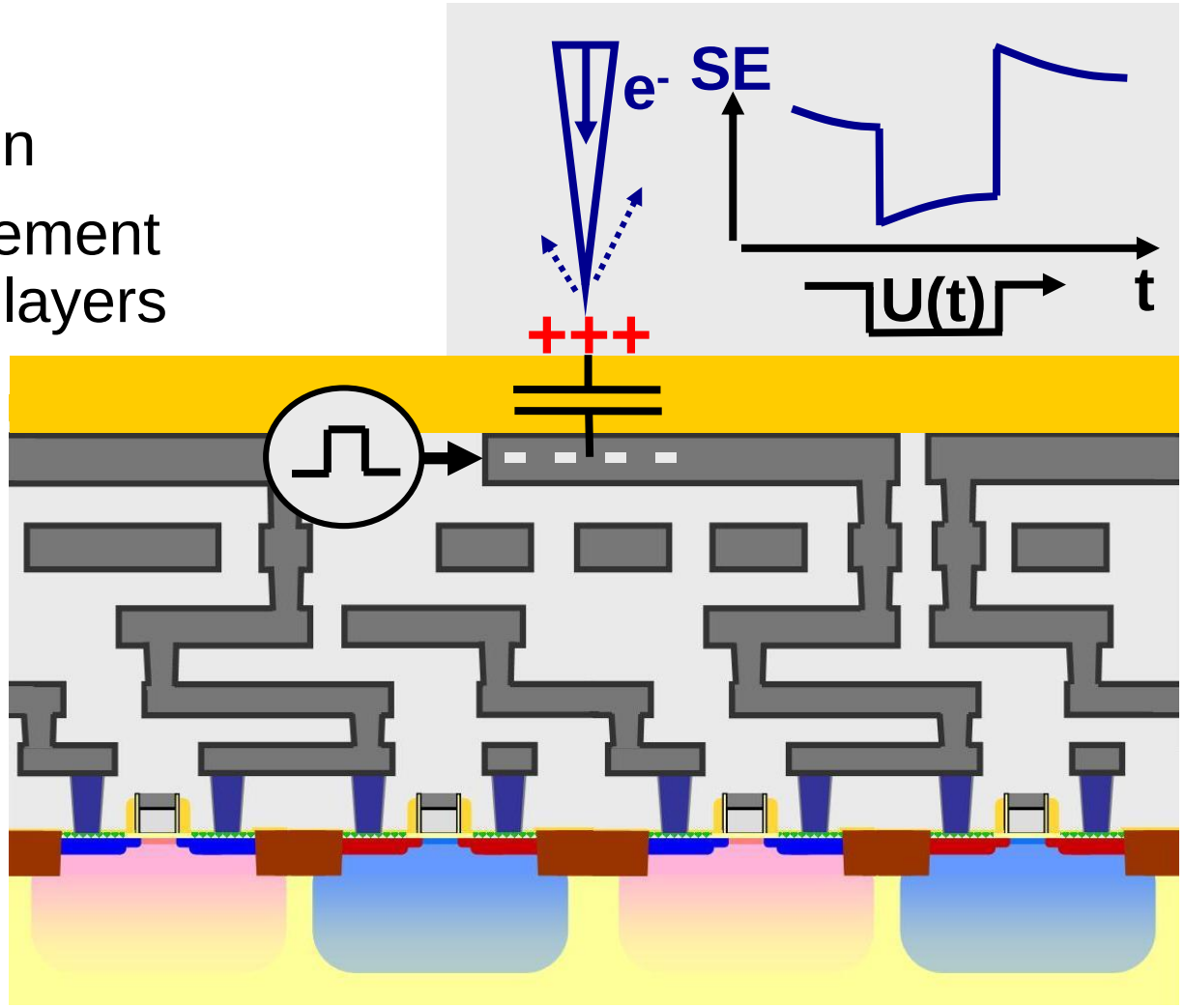
[a] *Singapore University of Technology and Design, Singapore*
[b] *Advanced Micro Devices Singapore Pte Ltd, Singapore*
[c] *Nanyang Technological University, Singapore*

ESREF 2018

Frontside Electron-Beam-Probing

- non invasive
- high time resolution
- fast signal acquisition
- quantitative measurement
  - only on uppermost layers

Logical waveform = timing analysis !!



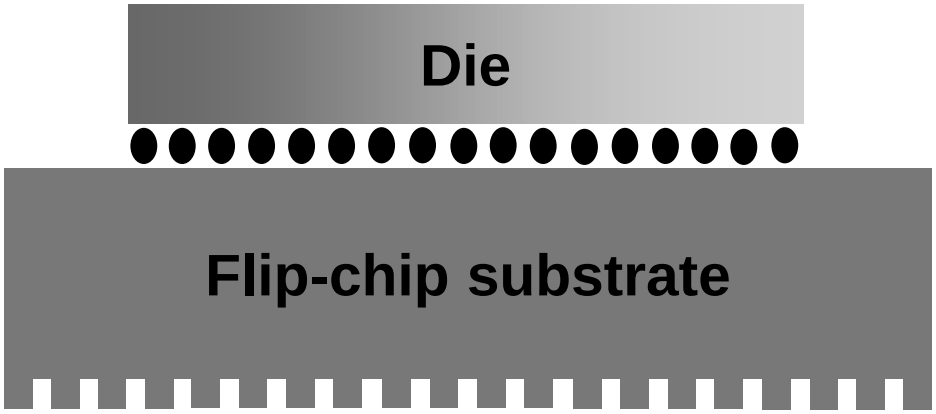
R ≈ λ/(2NA)

λ E Beam: 0.1nm

(100V, De Broglie)

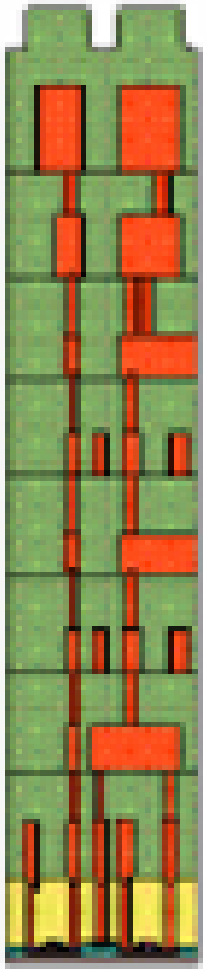
Real resolution: 10nm

Process Access: Through Silicon Backside



New Packages: Flip Chip

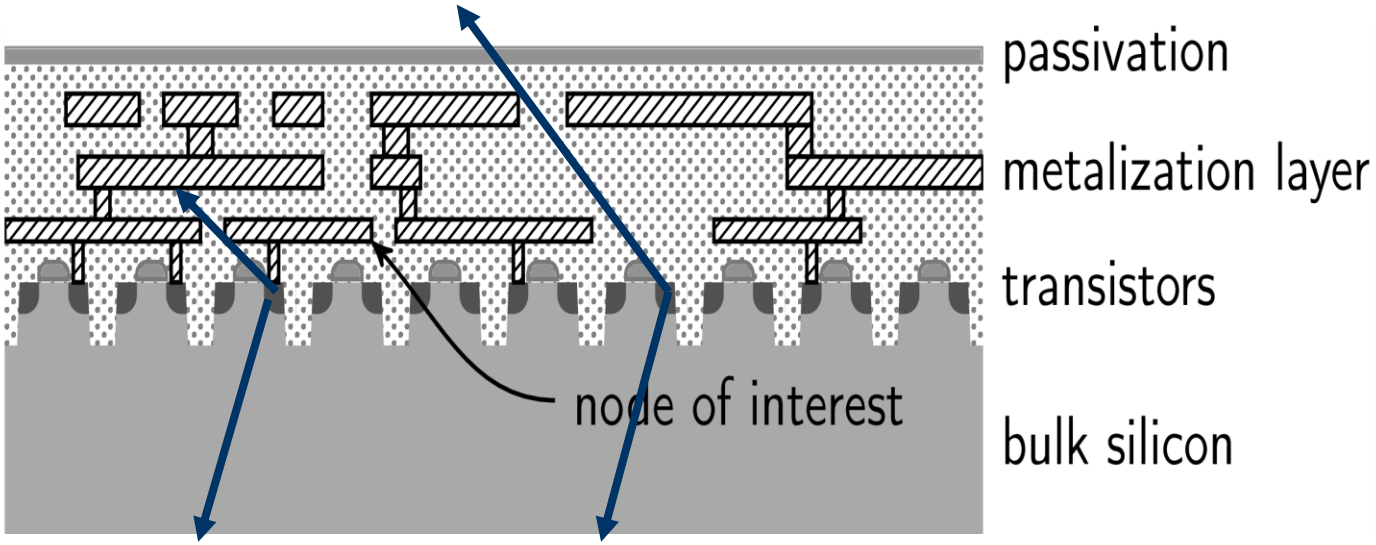
Data taken from Fujitsu



New Technologies: Multiple Interconnect Levels

Compare Information Level Frontside and Backside

Optical interaction through frontside: each node has individual signature due to interconnect intransparency

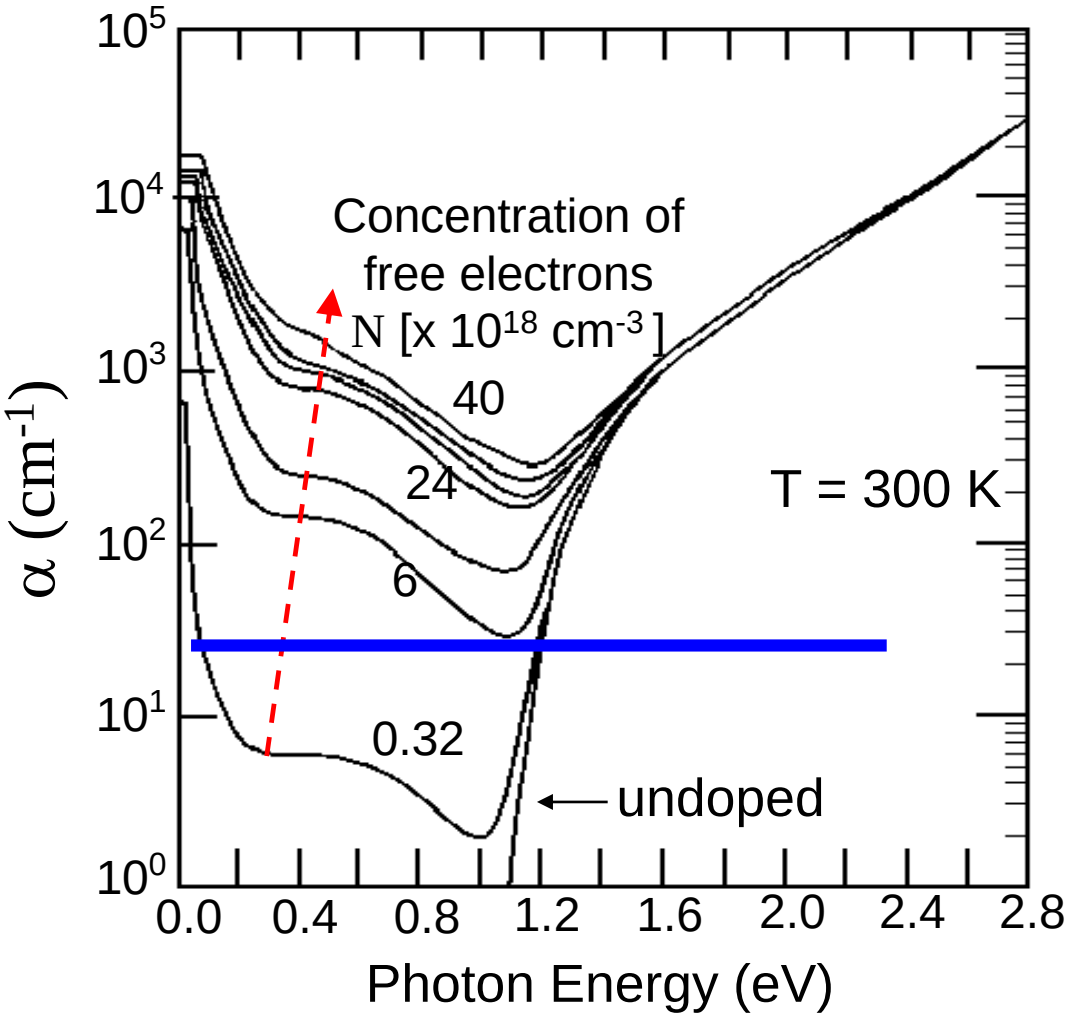


Access through chip backside: all nodes show same interaction scenario …and compare quantitatively! Read out much more precise

Backside Access & Optics

Sufficient transmission through Si good for die thickness of 500µm

Soref et al., IEEE J. of Quant. Elec., Vol. QE-23, No.1, January 1987



From backside, all nodes act alike

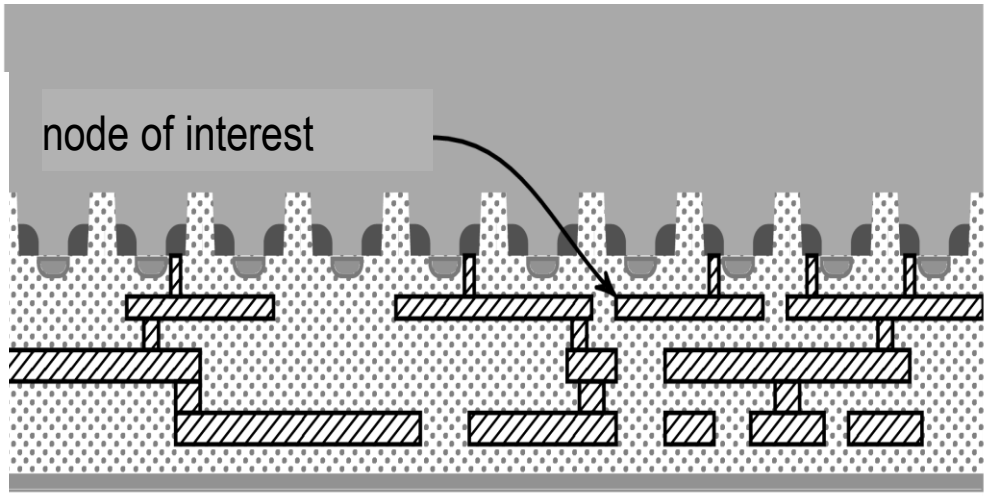
Backside point of view….

Bulk silicon

Transistors

Metallization Layer

Passivation



…is from now on interaction surface for CFI

In A Nutshell

- Contactless signal tracking mandatory in IC development
- Contactless signal tracking = Physical Interaction
- Today physical interaction needs to access chip through backside = optical techniques play major role
- Backside access allows to compare signal quantitatively = new level of precision in signal reconstruction

Outline

Why contactless Fault Isolation in ICs

Technology Node and CFI Evolution

The Benefits of CFI Backside Approach

Relevant CFI Techniques and Attack Risks

IoT Roadmap: Nanoscale FinFET & Low Power

CFI will prevail and the Attack Risk with it

Backside Protection

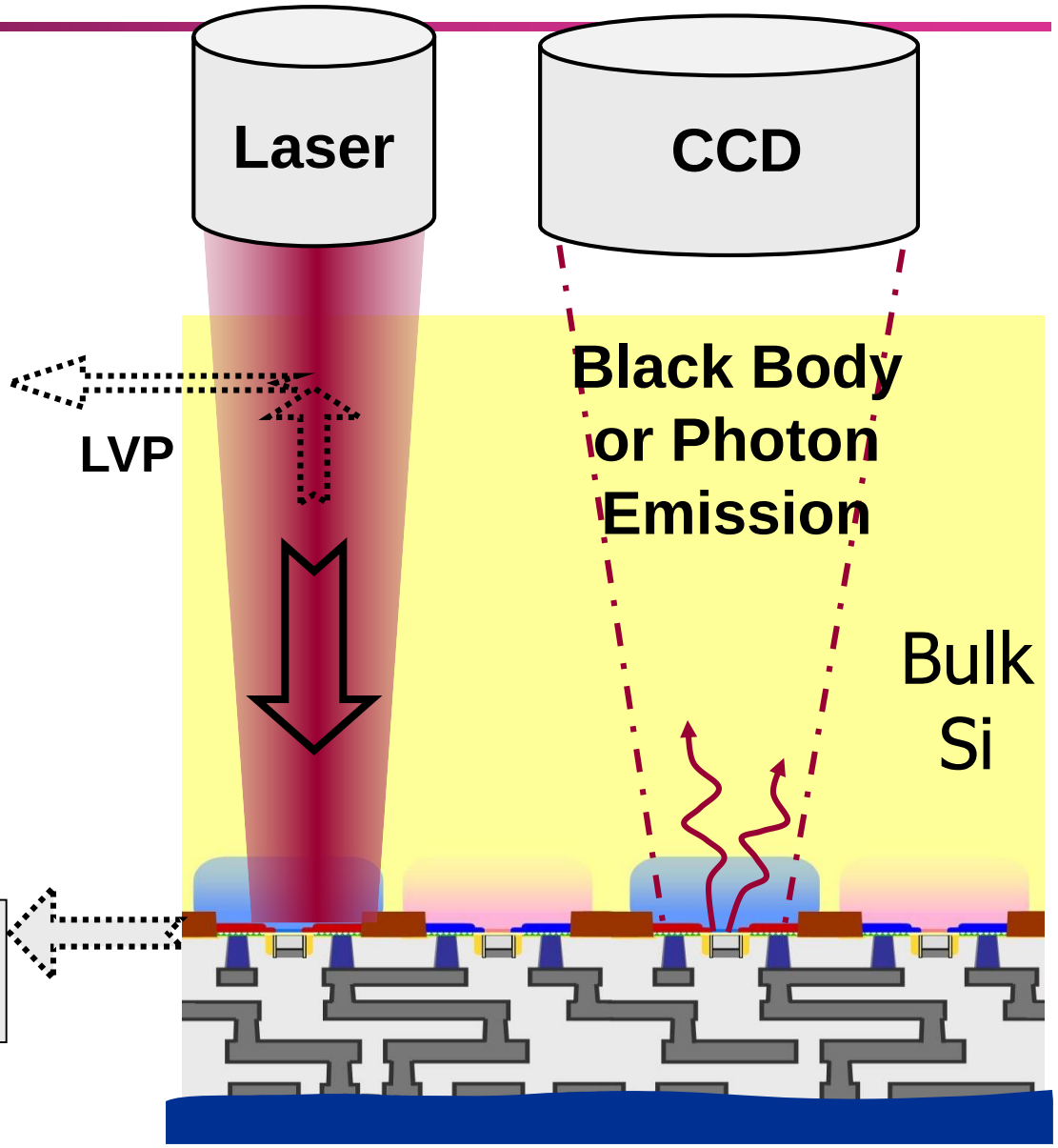
Optical Backside Circuit Analysis

- Time Res. Photon Emission: Rise and Fall Events of Pattern

- Laser Voltage Probing: Quantitative Voltage Waveform

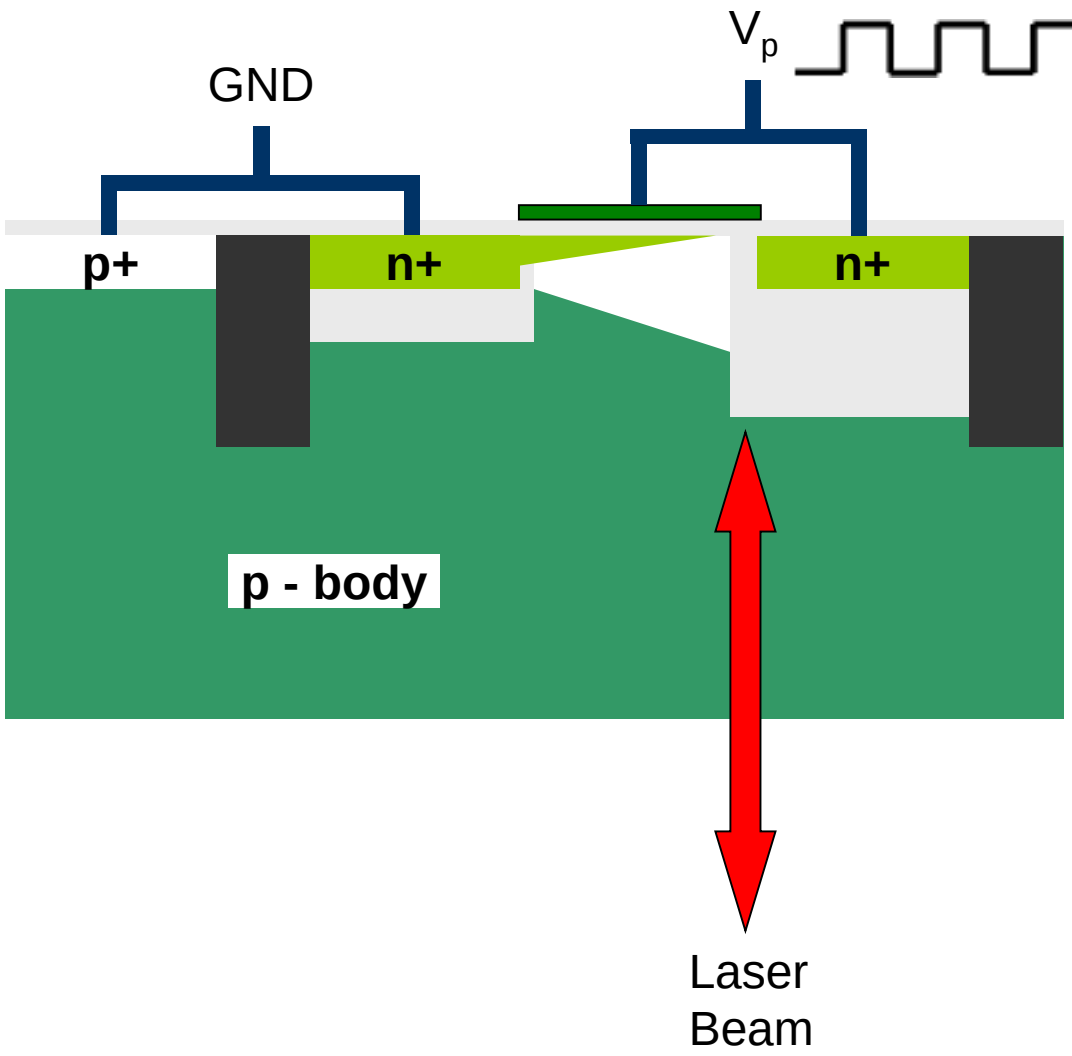
- Laser Stimulated Delay Variation: Tester Pass / Fail Decision

Laser Stimulated Electrical Signal



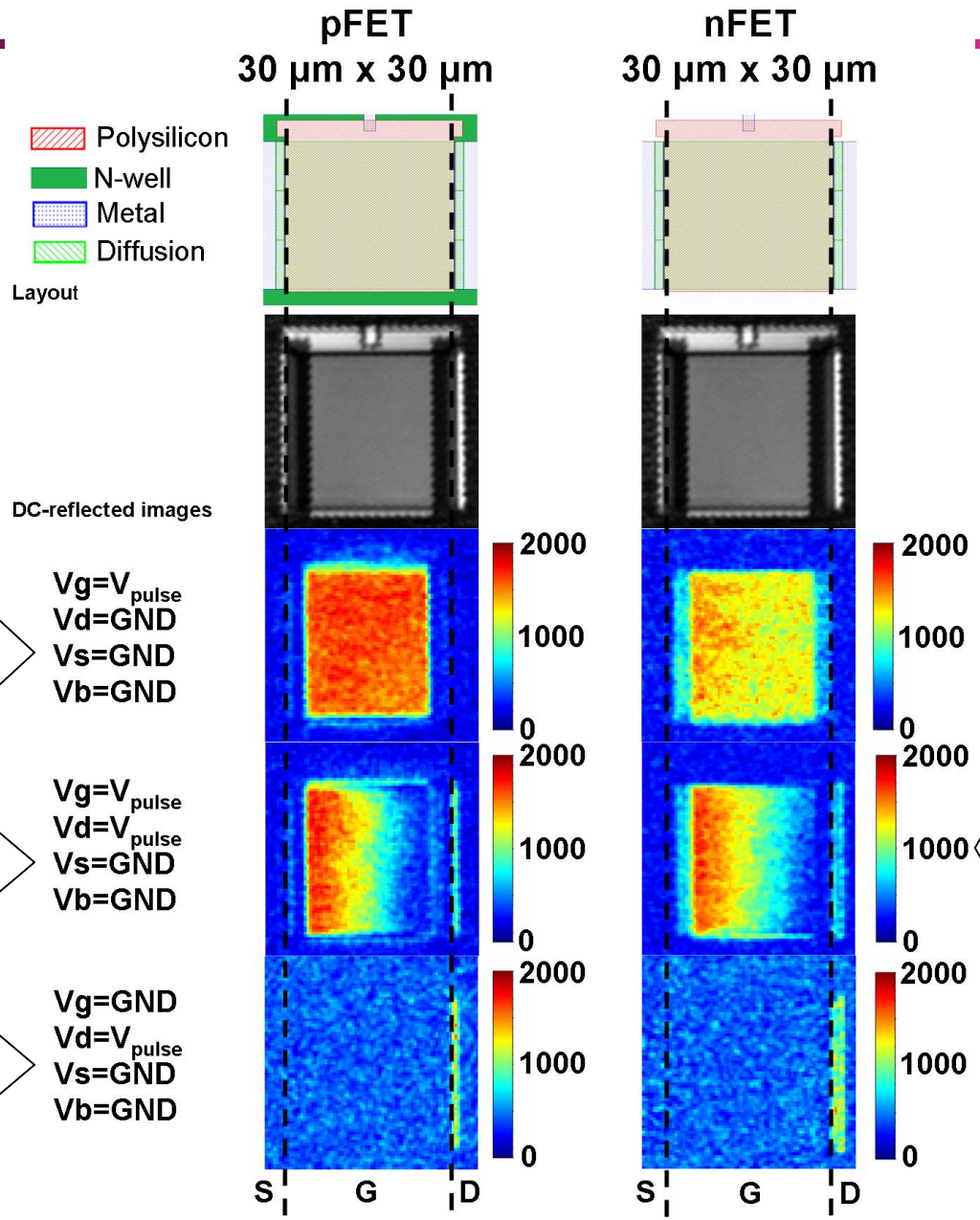
Reflectance Modulation Imaging / Principles
Laser Voltage Imaging (LVI), Electro-Optical Freq.Modul. (EOFM)

Logical waveform = timing analysis !!



- The reflected light modulation due to:
- Varying Charge Density
  - In the channel region
- Varying space charge layer
  - In the pinch off region
  - In the drain-junction region

LVI / EOFM on large-area FETs

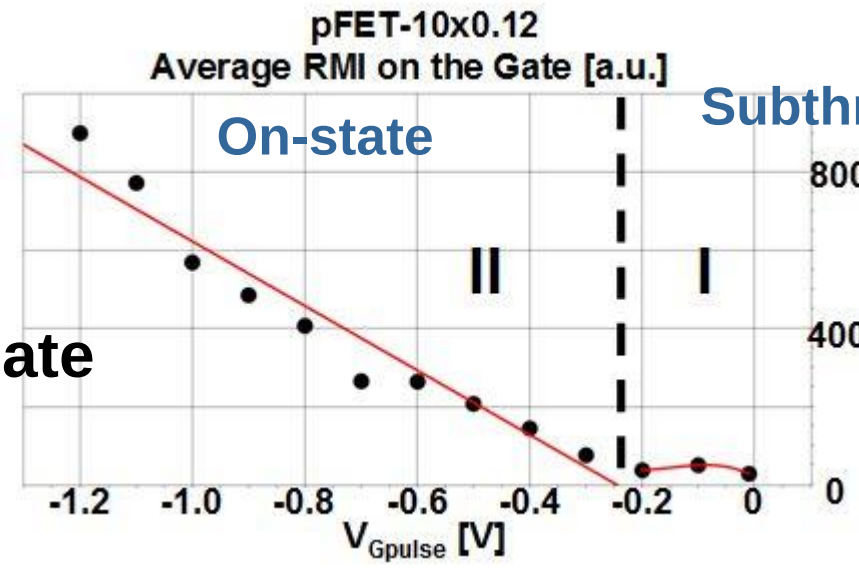


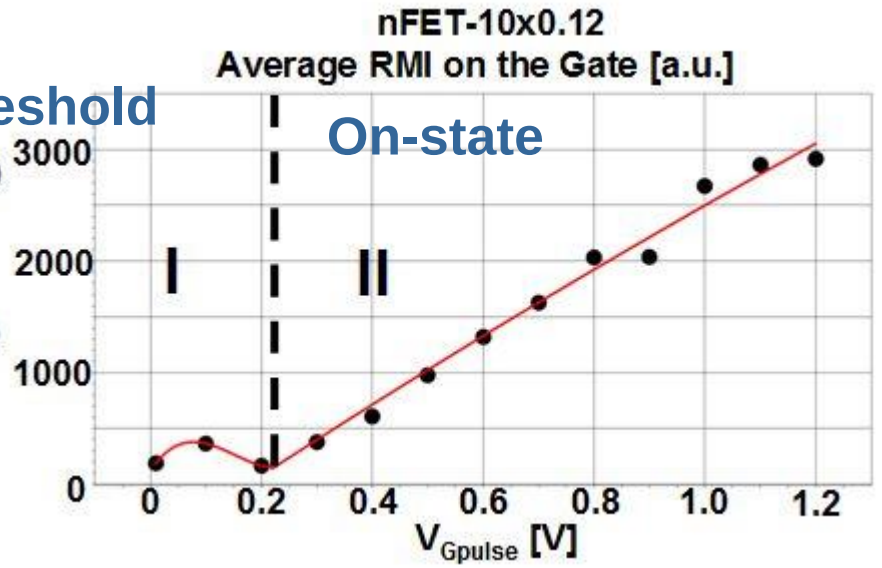
Pinch off: Channel decreases towards drain, no significant space charge signal in pinch off region

EOP / LVP: Signal Linear with Supply Voltage: No Limit for Low Power Technologies

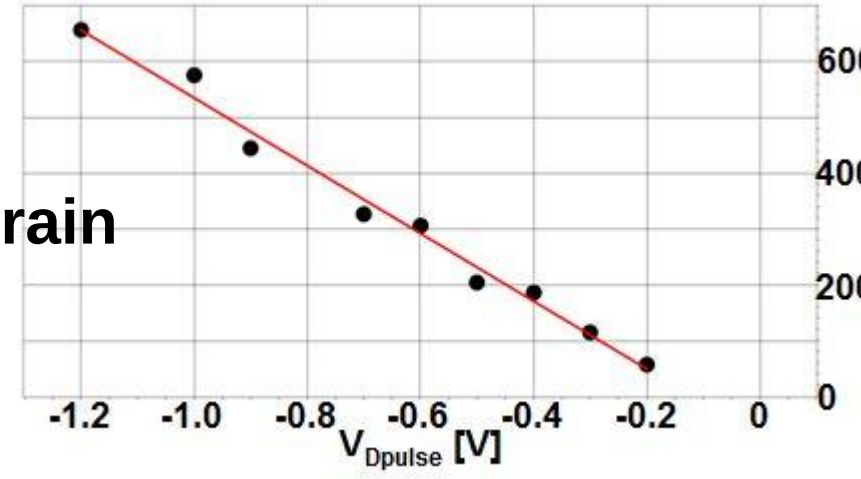
PFET **NFET**

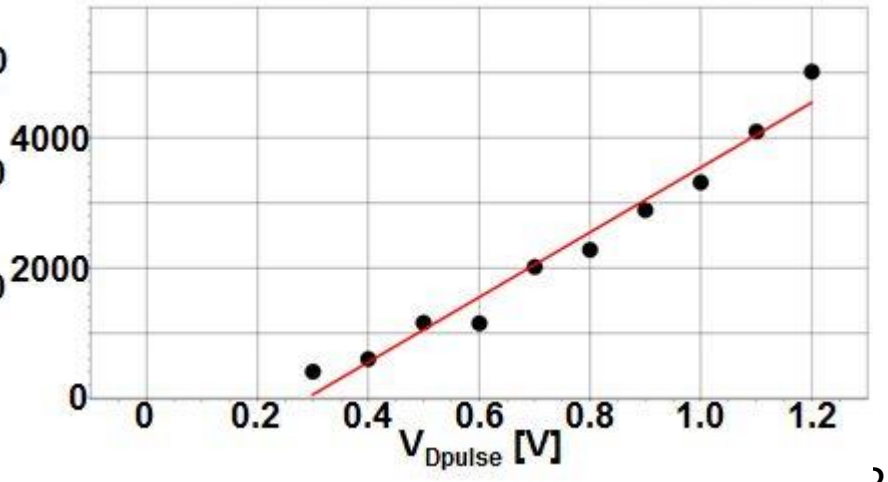
Gate





Drain





21

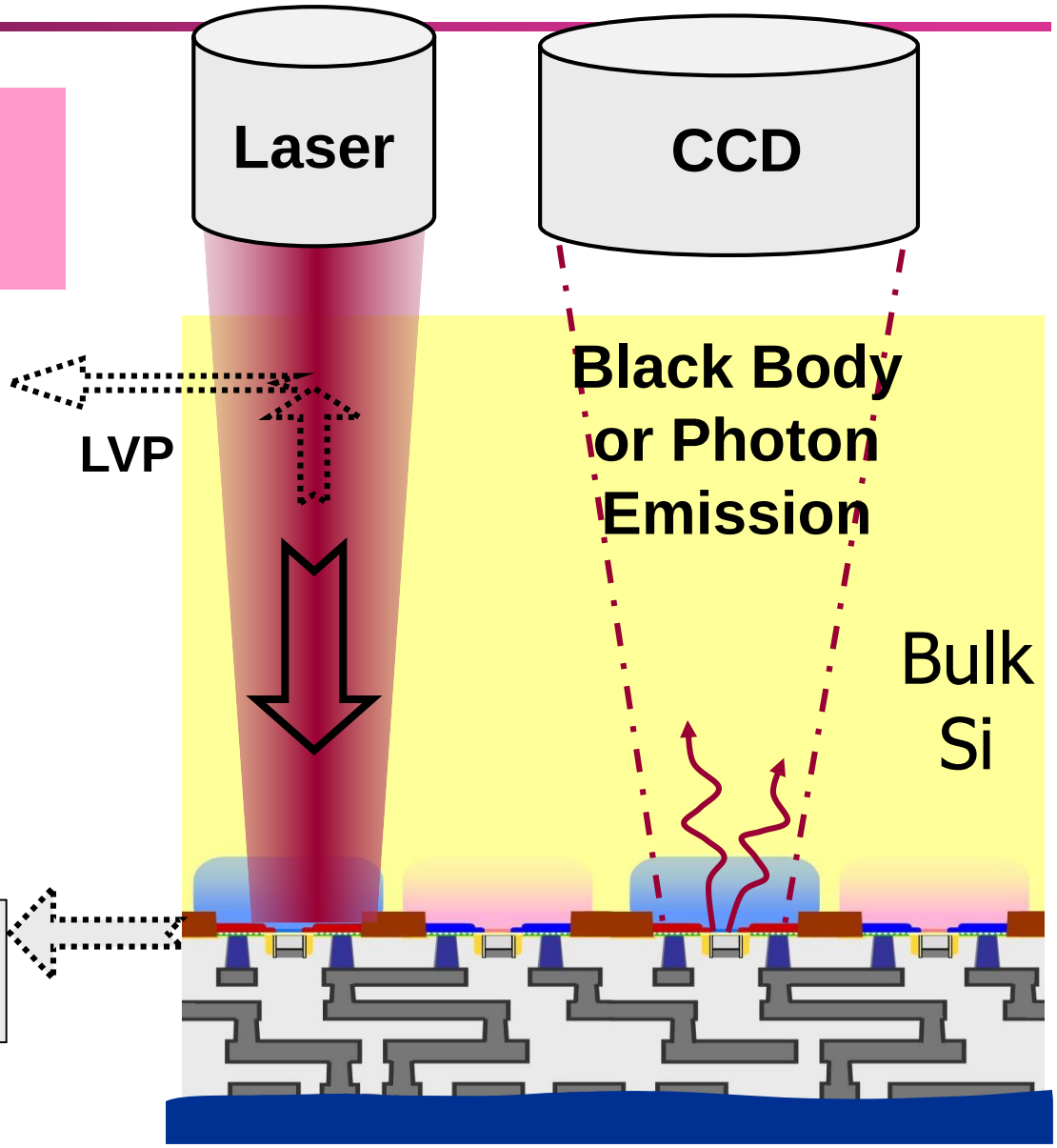
Optical Backside Circuit Analysis

- Time Res. Photon Emission: Rise and Fall Events of Pattern

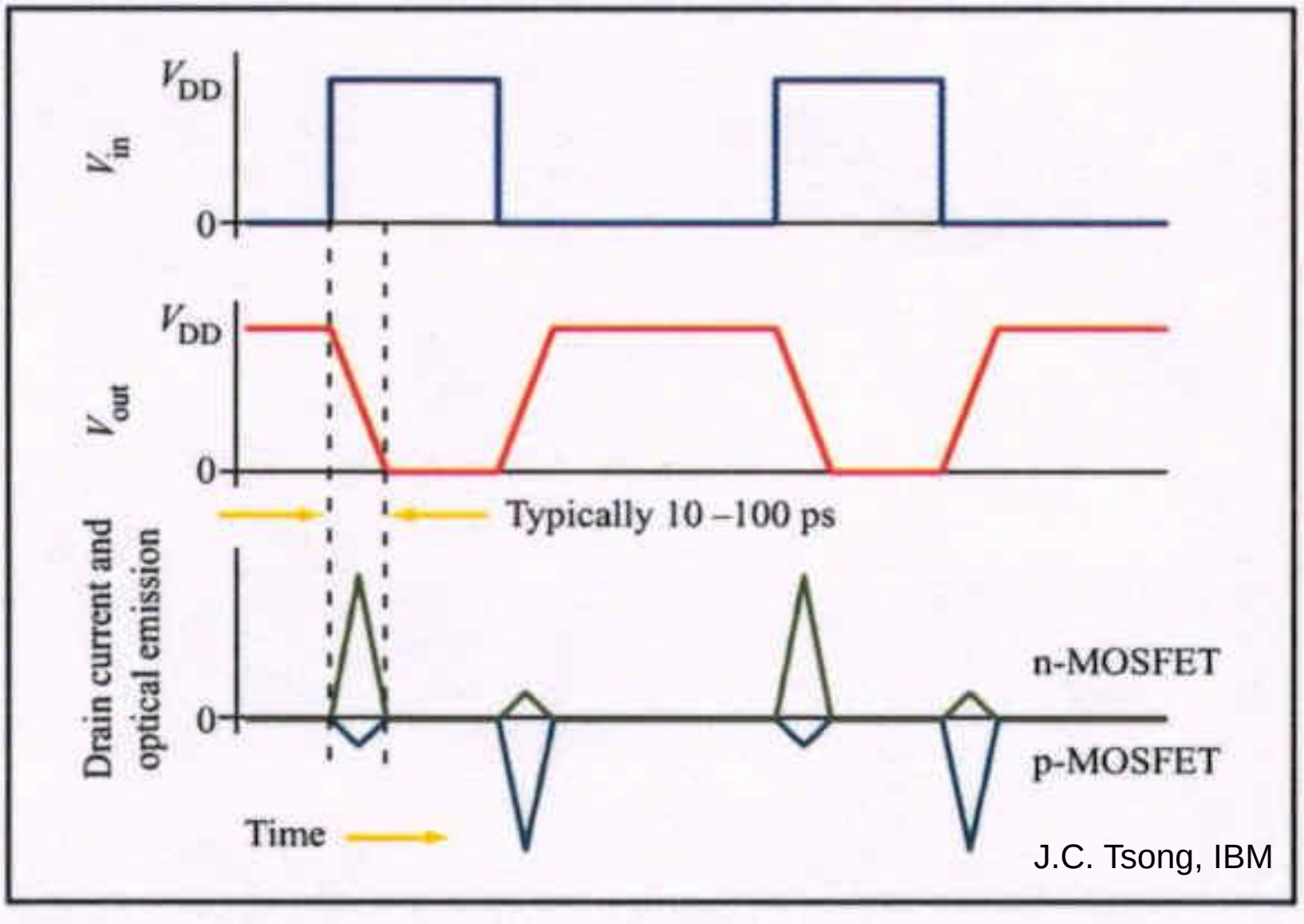
- Laser Voltage Probing: Quantitative Voltage Waveform

- Laser Stimulated Delay Variation: Tester Pass / Fail Decision

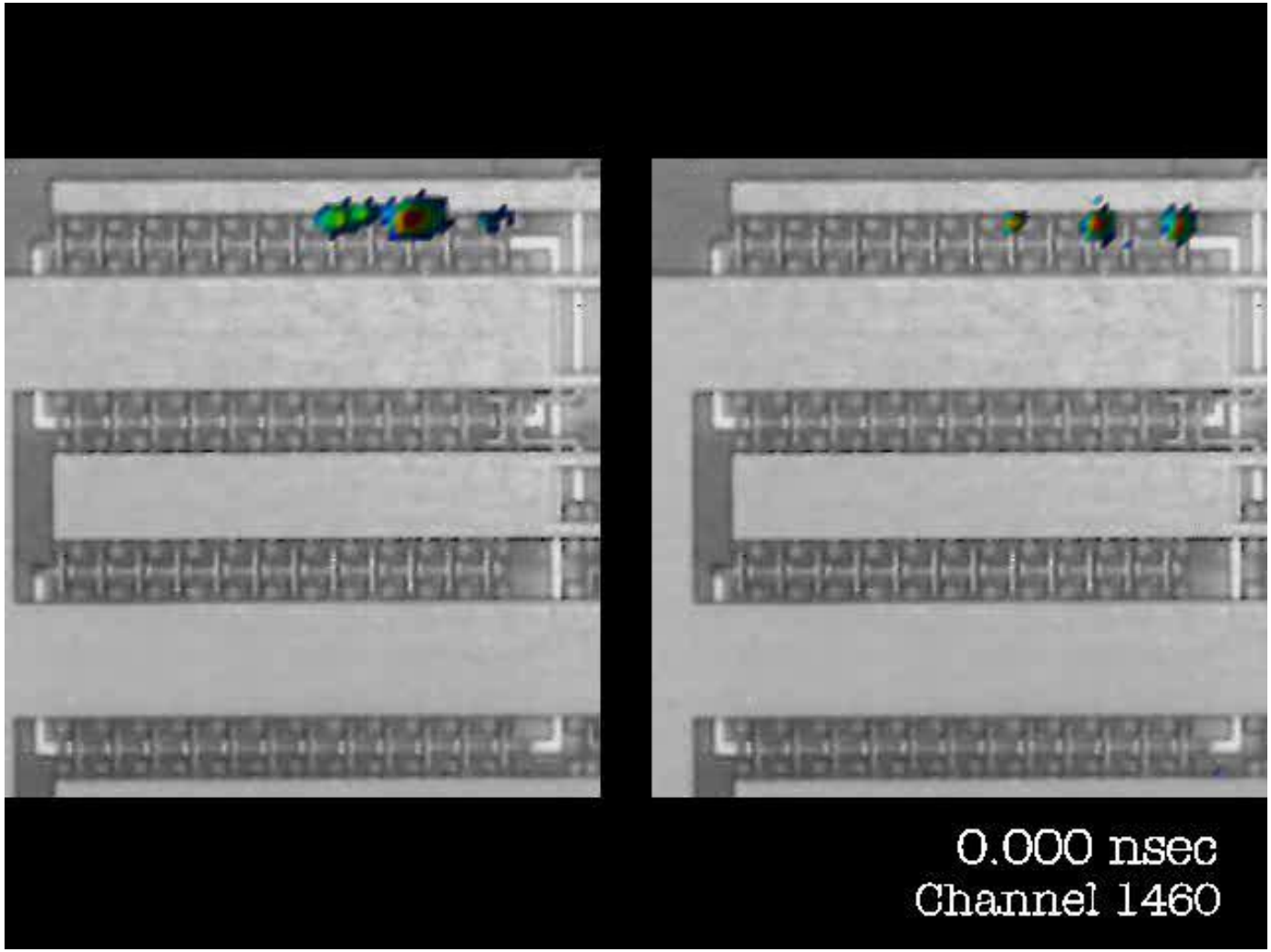
Laser Stimulated Electrical Signal



Photon Emission in CMOS Inverter



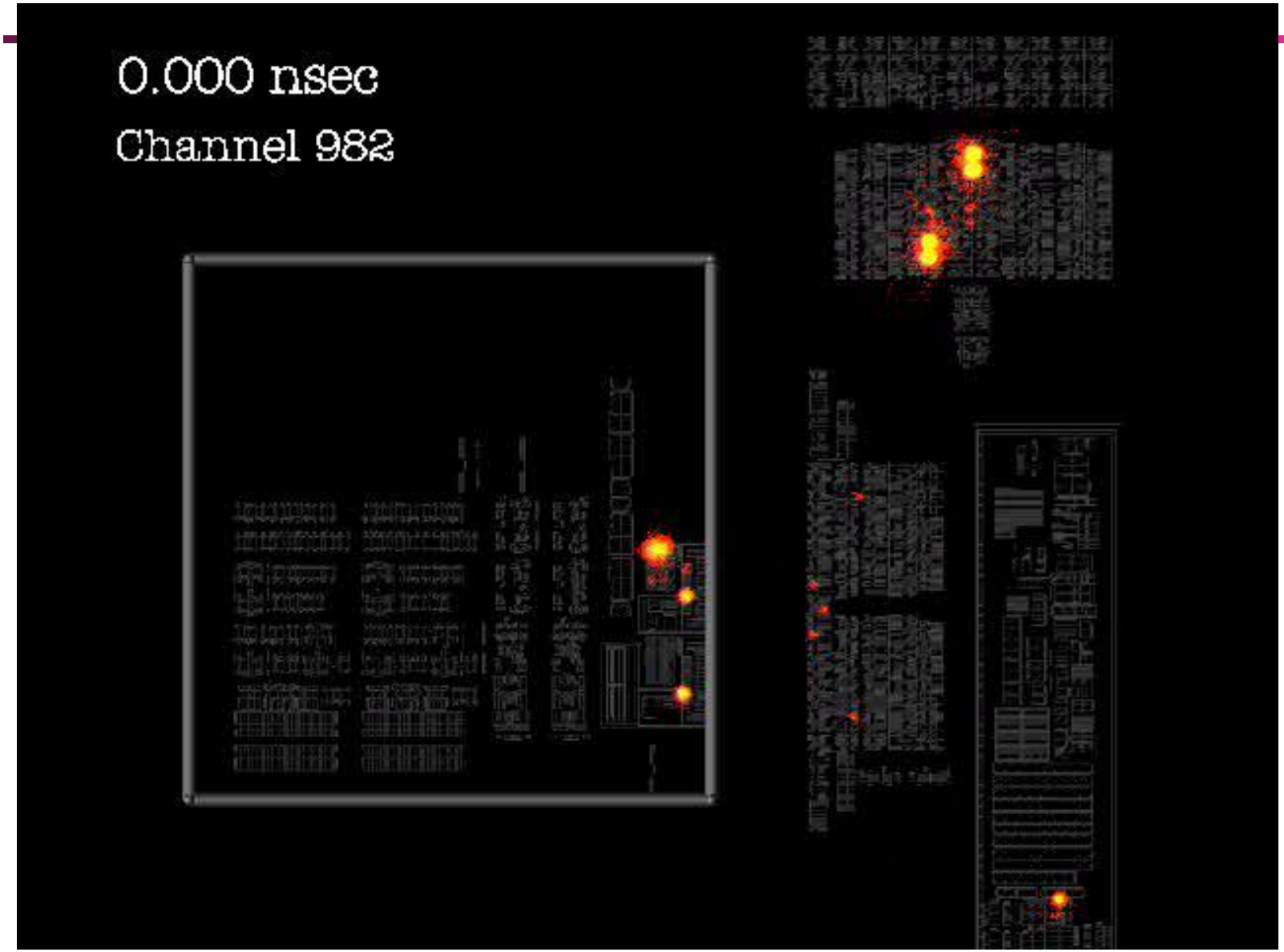
TRE in Ring Oscillator - Demonstrator



Coutesy IBM / Richard Ross

...impossible with frontside detection

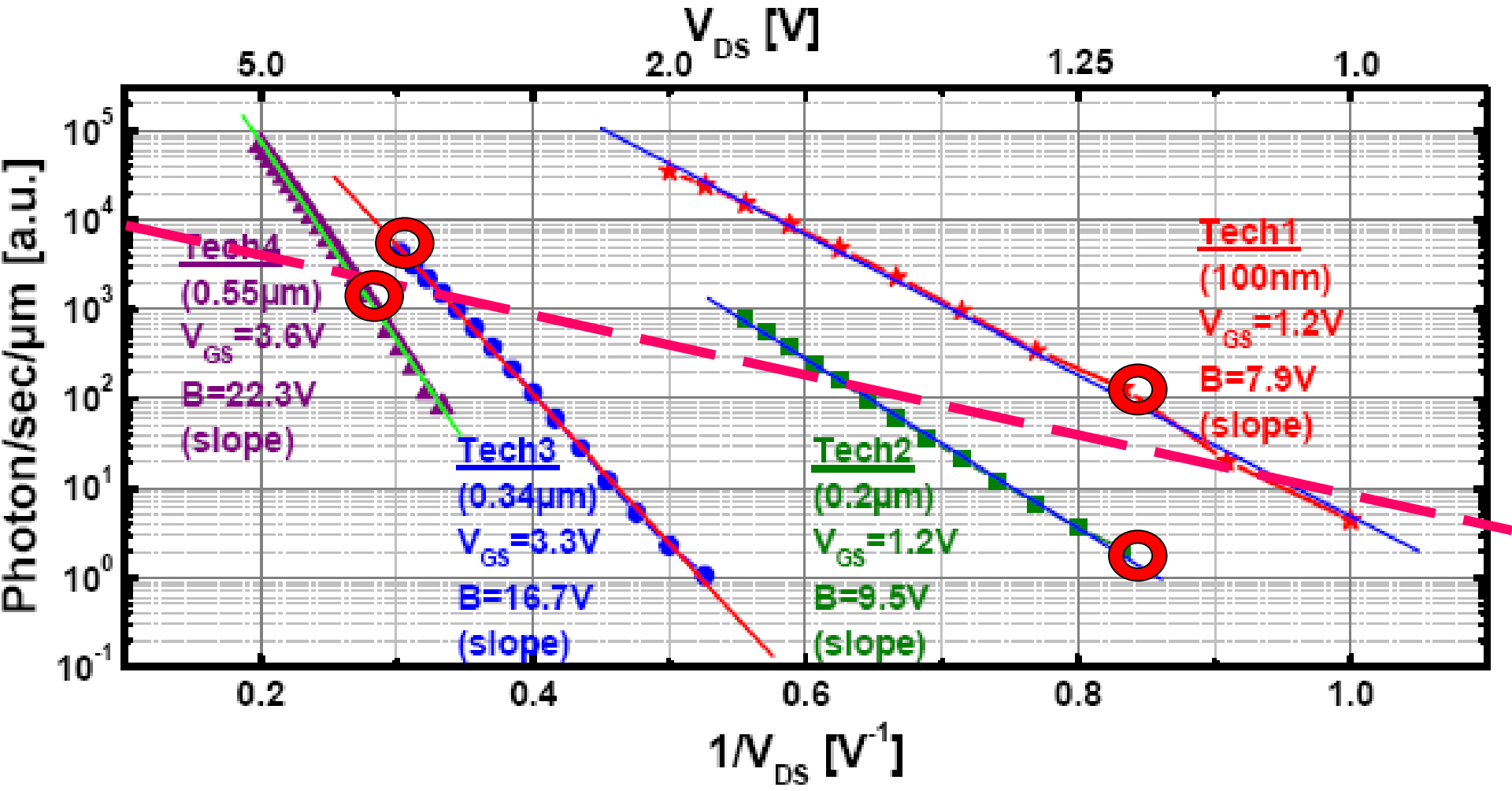
Watching the Chip at Work



courtesy Richard Ross / IBM

...unthinkable with frontside detection

Scaling of CMOS technologies
Challenges for photon emission microscopy

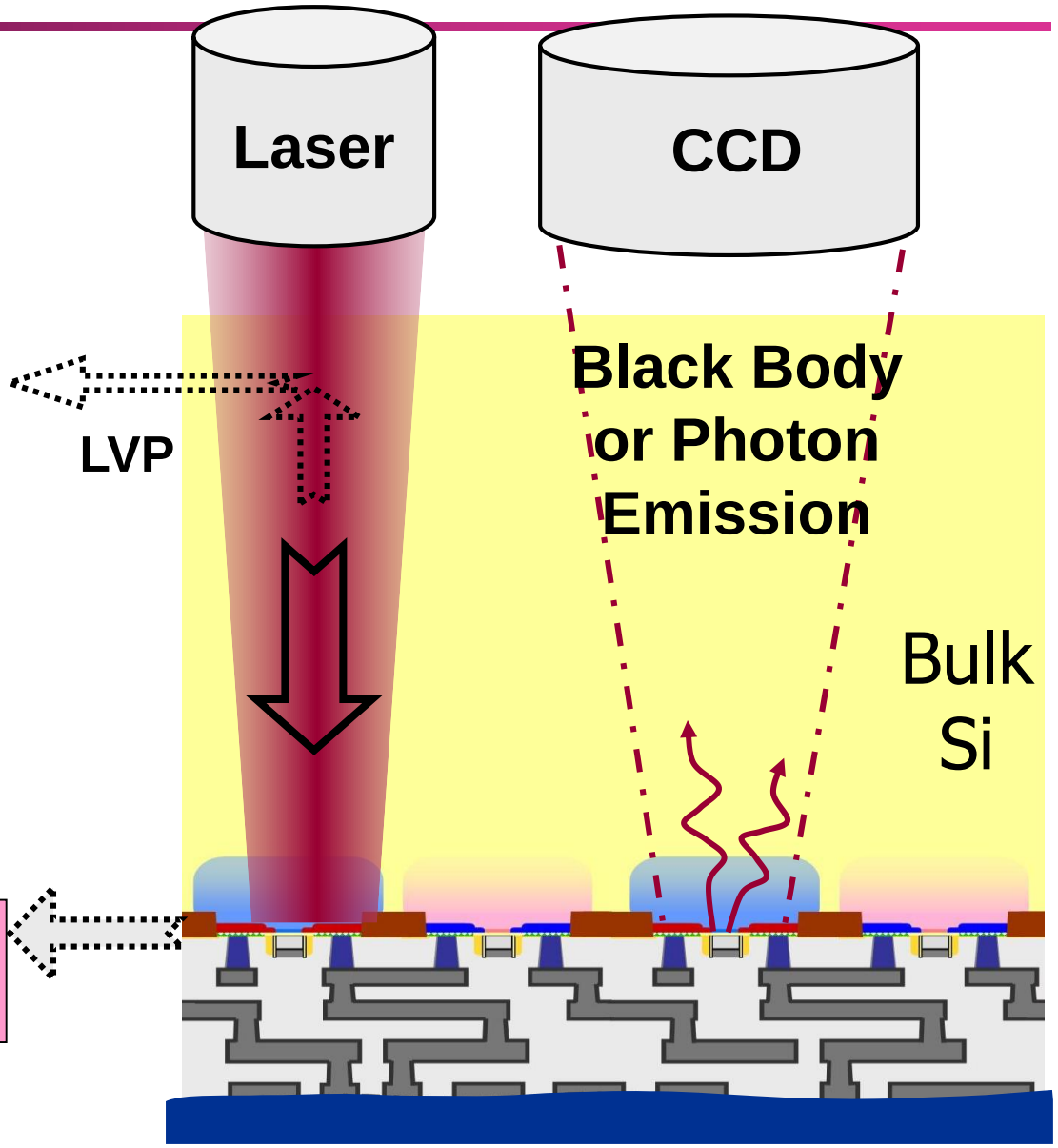


Modified by CB after: "Hot-carrier photoemission in scaled CMOS technologies: A challenge for emission based testing and diagnostics", Alberto Tosi, Franco Stellari, Andrea Pigozzi, Giulio Marchesi, Franco Zappa, IEEE IRPS 2006

Optical Backside Circuit Analysis

- Time Res. Photon Emission: Rise and Fall Events of Pattern
- Laser Voltage Probing: Quantitative Voltage Waveform
- Laser Stimulated Delay Variation: Tester Pass / Fail Decision

Laser Stimulated Electrical Signal



Photoelectric Laser Stimulation (PLS)

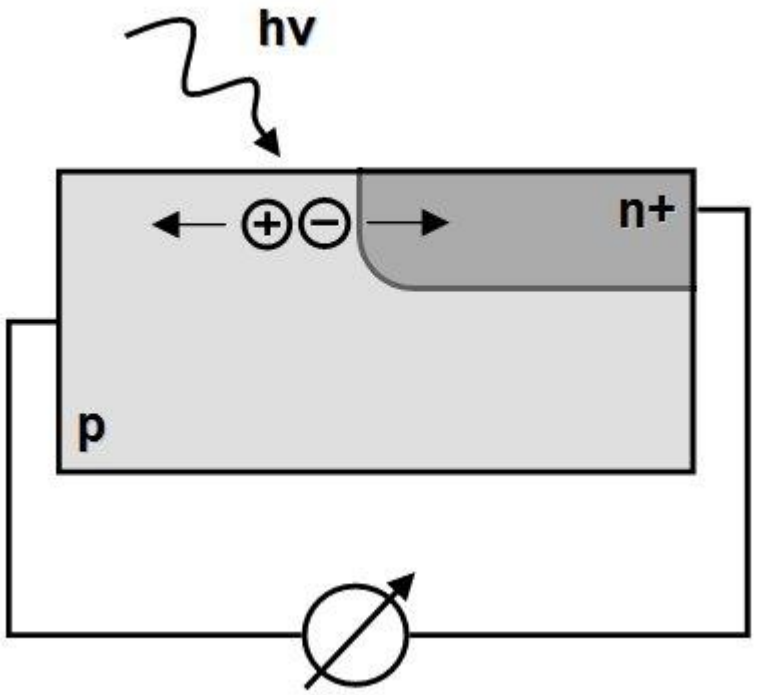
Optical Beam Induced Current (OBIC)

Key Issues:

- **Scanned Laser Beam**
- **Penetration Depth = f (Wave Length)**
- **Sensitive to Any El. Field w/Terminals**

Application:

- **Test Structures**
- **Input / Output Structures**
- **Latch up**

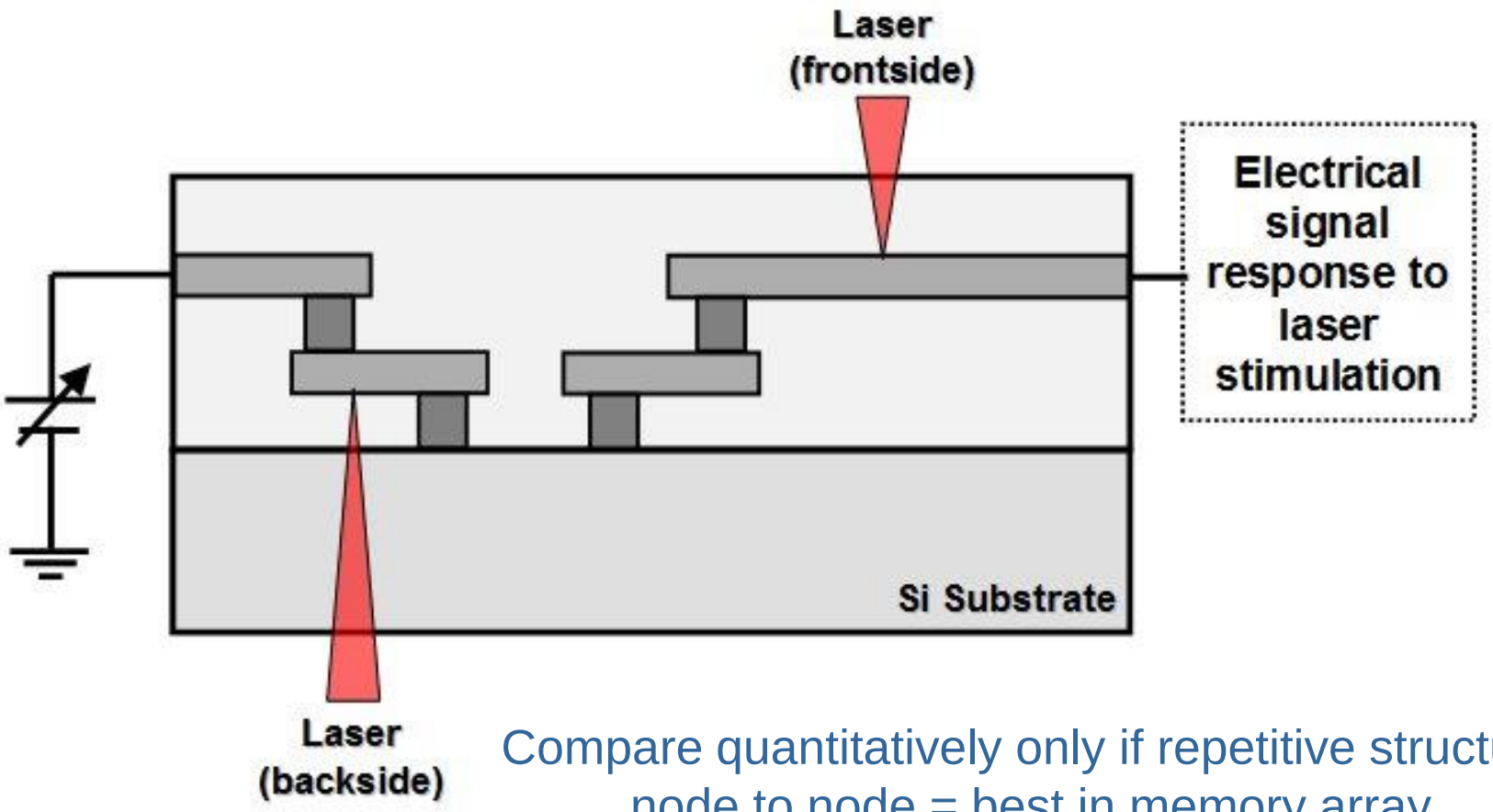


28

Thermal Laser Stimulation (TLS): OBIRCH / TIVA

OBIRCH = Optical Beam Induced Resistance Change

TIVA = Thermally Induced Voltage Alteration

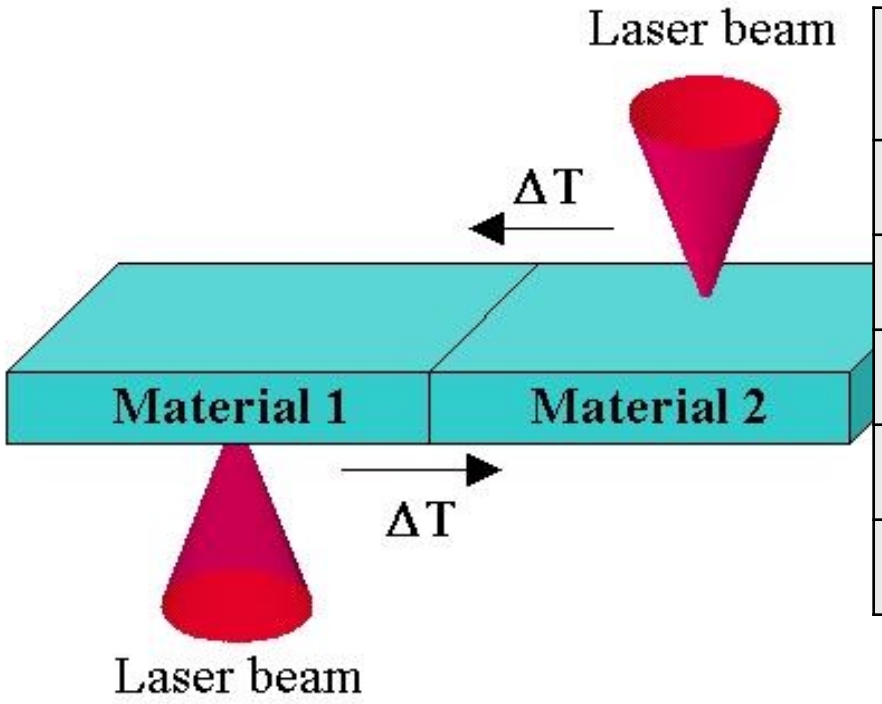


Compare quantitatively only if repetitive structure

node to node = best in memory array

29

Thermal Laser Stimulation (TLS): Thermoelectric (Seebeck) Effect



Material or junction	S [μV/K]
Al	-3.5
Cu	6.5
W	3.6
Al / n+ Si	287
Al / p+ Si	-202

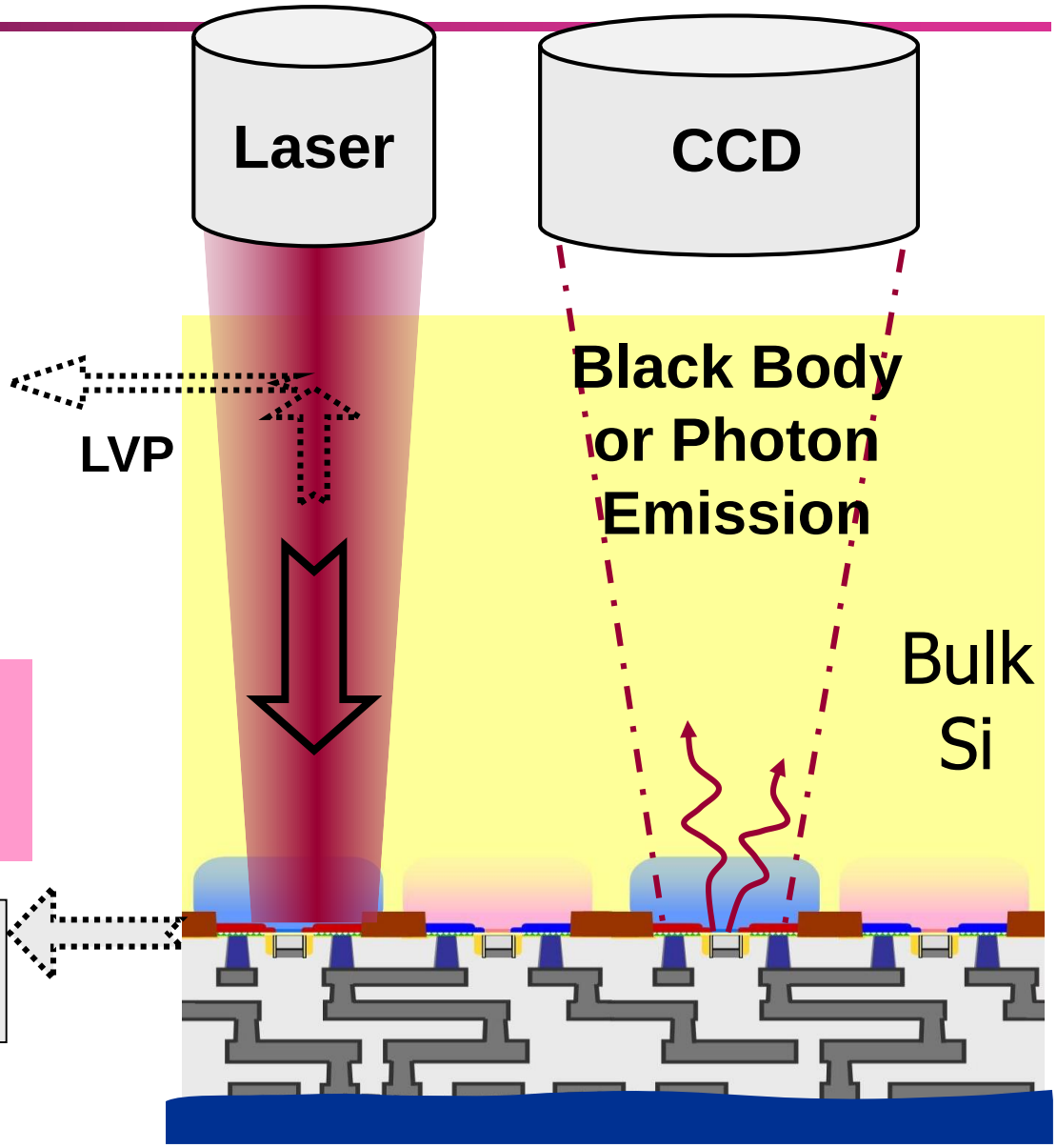
$$\Delta V = (S_1 - S_2)\,\Delta T = S_{12}\,\Delta T$$

30

Optical Backside Circuit Analysis

- Time Res. Photon Emission: Rise and Fall Events of Pattern
- Laser Voltage Probing: Quantitative Voltage Waveform
- Laser Stimulated Delay Variation: Tester Pass / Fail Decision

Laser Stimulated Electrical Signal

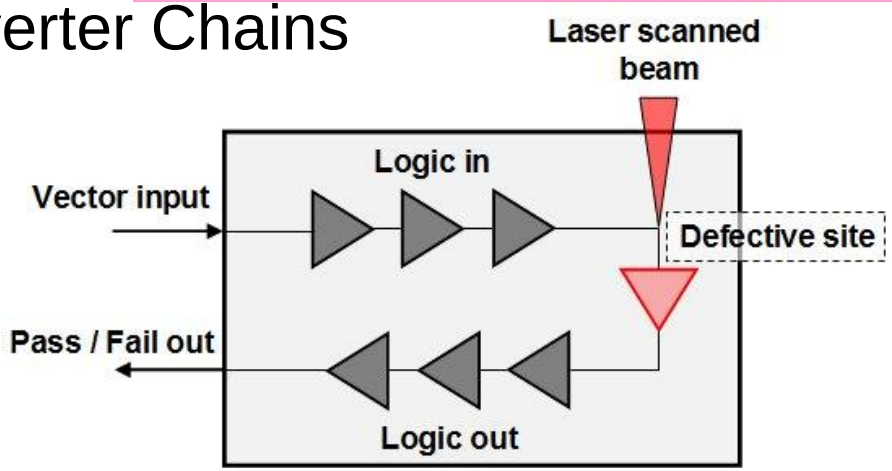


Laser Stimulated Delay Variation, Fault Injection: LADA, SDL

LADA = Laser Assisted Device Alteration by photocurrents

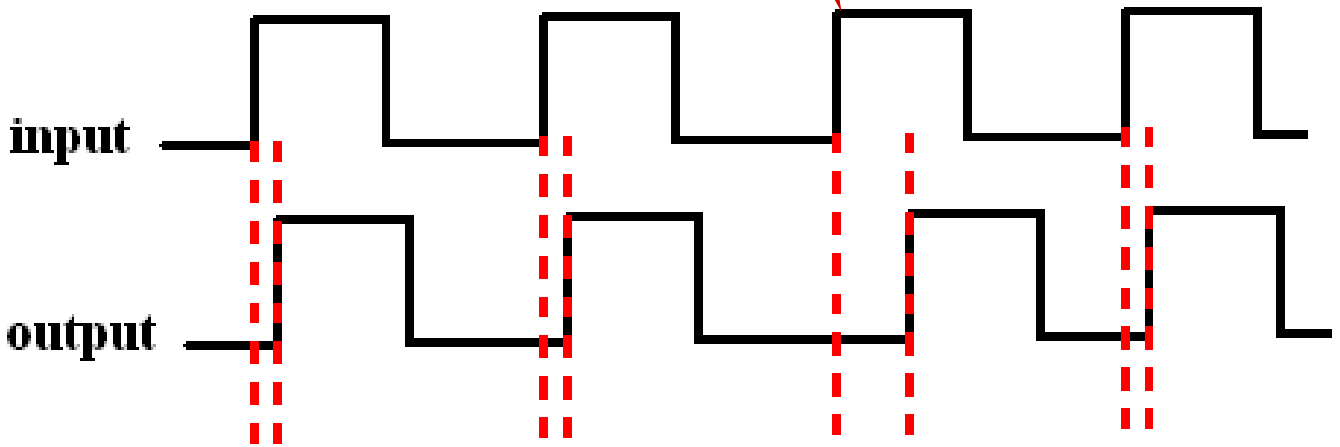
SDL = Soft defect Localization by Thermal Stimulation

Inverter Chains



timing analysis !!

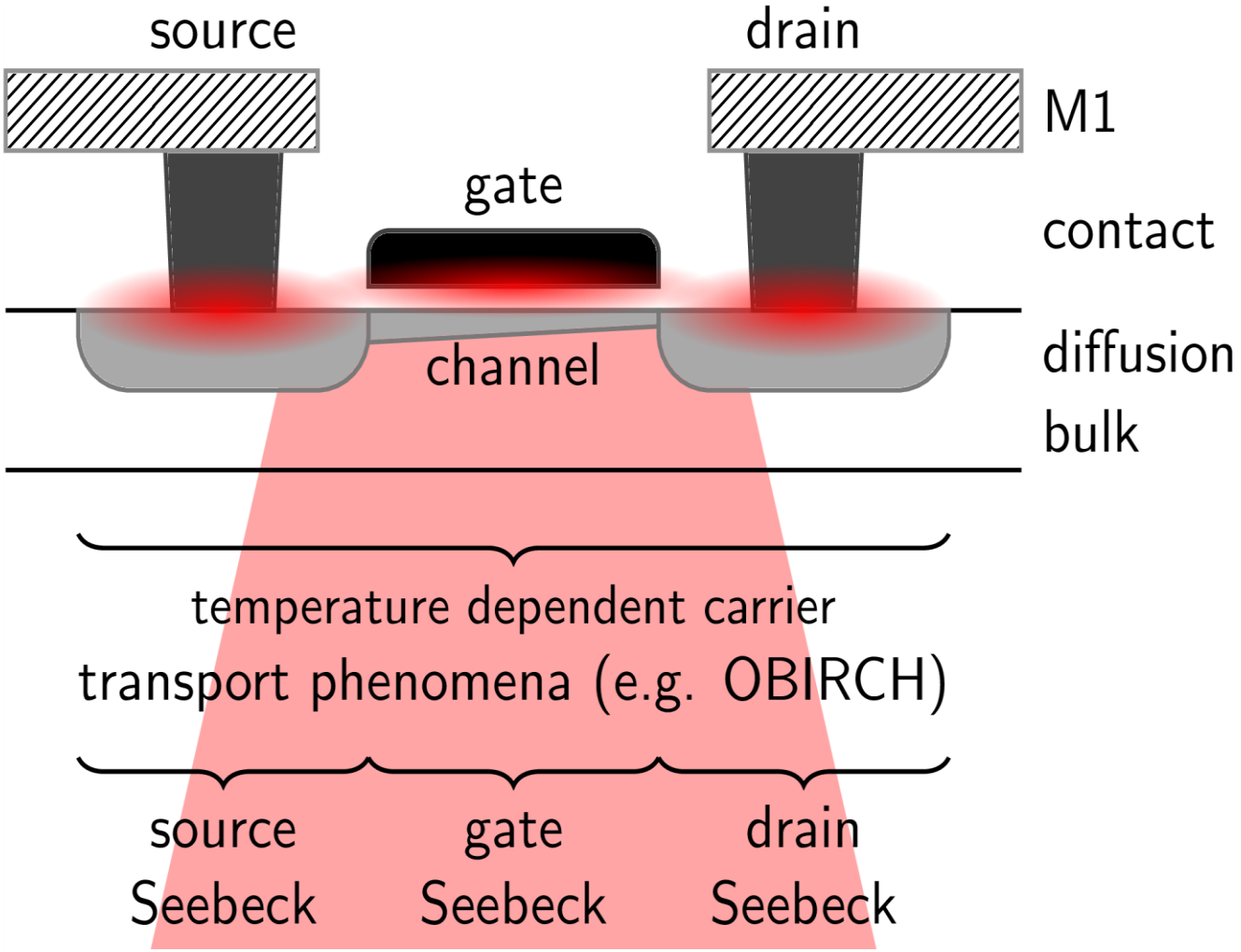
Laser Stimulation



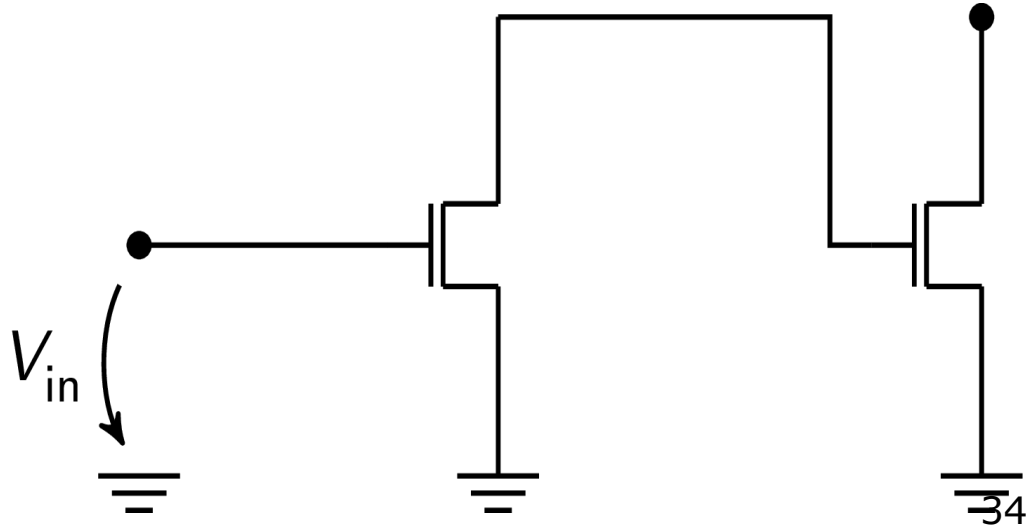
Fault Injection !!

Delay Variation ~ 10 - 50ps

Thermoelectric Stimulation of FET

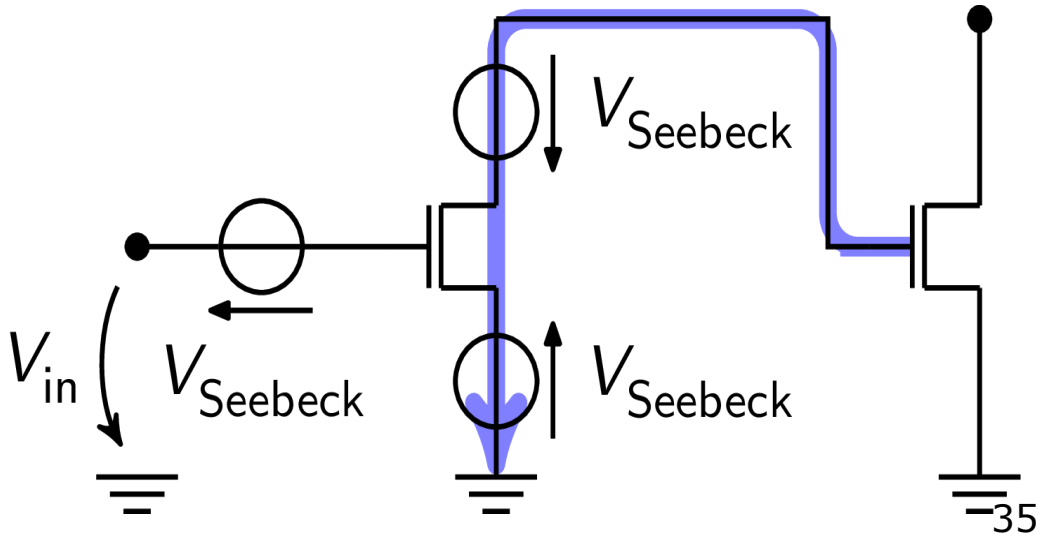


Thermoelectric Stimulation of SRAM Flip Flop

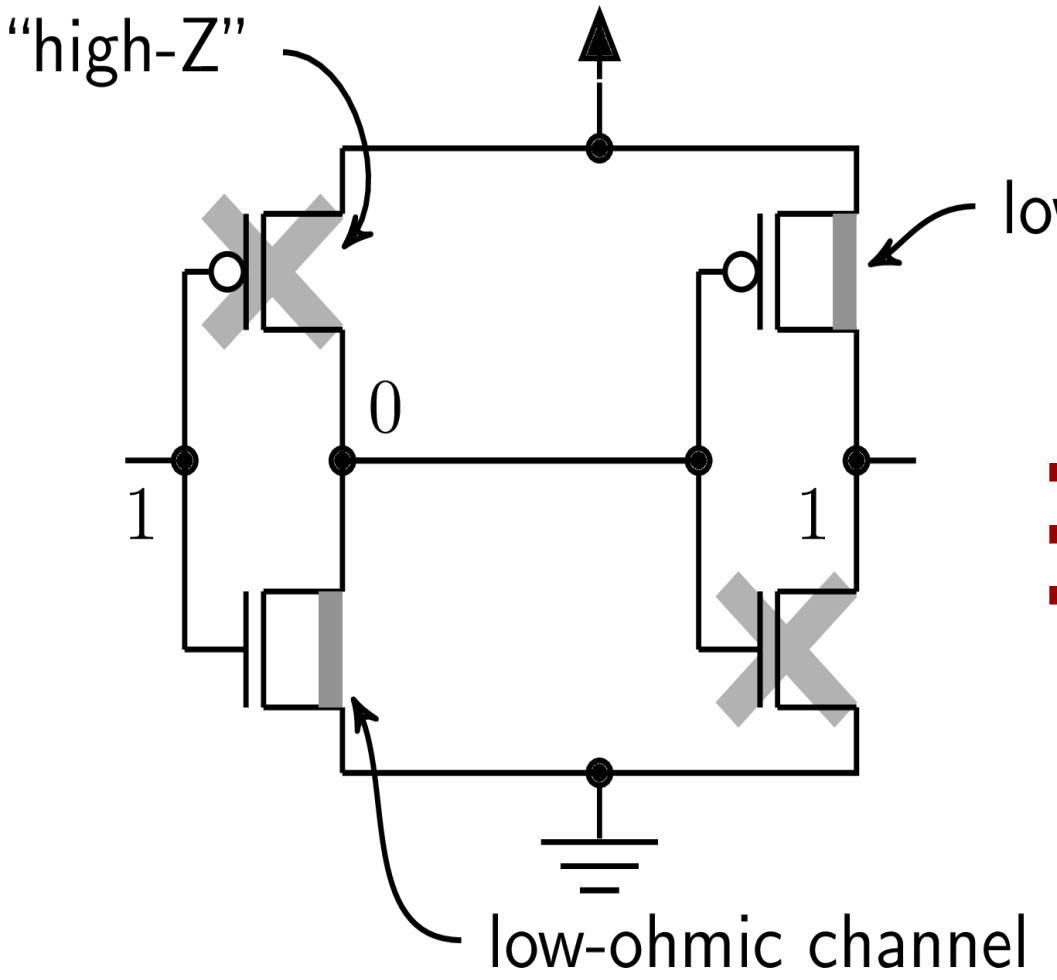


Thermoelectric Stimulation of SRAM Flip Flop

- Seebeck at Gate adds up to input voltage
- Seebeck at Drain adds to output voltage
  Seebeck at Source reduces output voltage
- Source Seebeck increases input voltage and increases bulk potential (nmos)
- Bulk Seebeck increases bulk potential (nmos, probably on multiple transistors simultaneously)

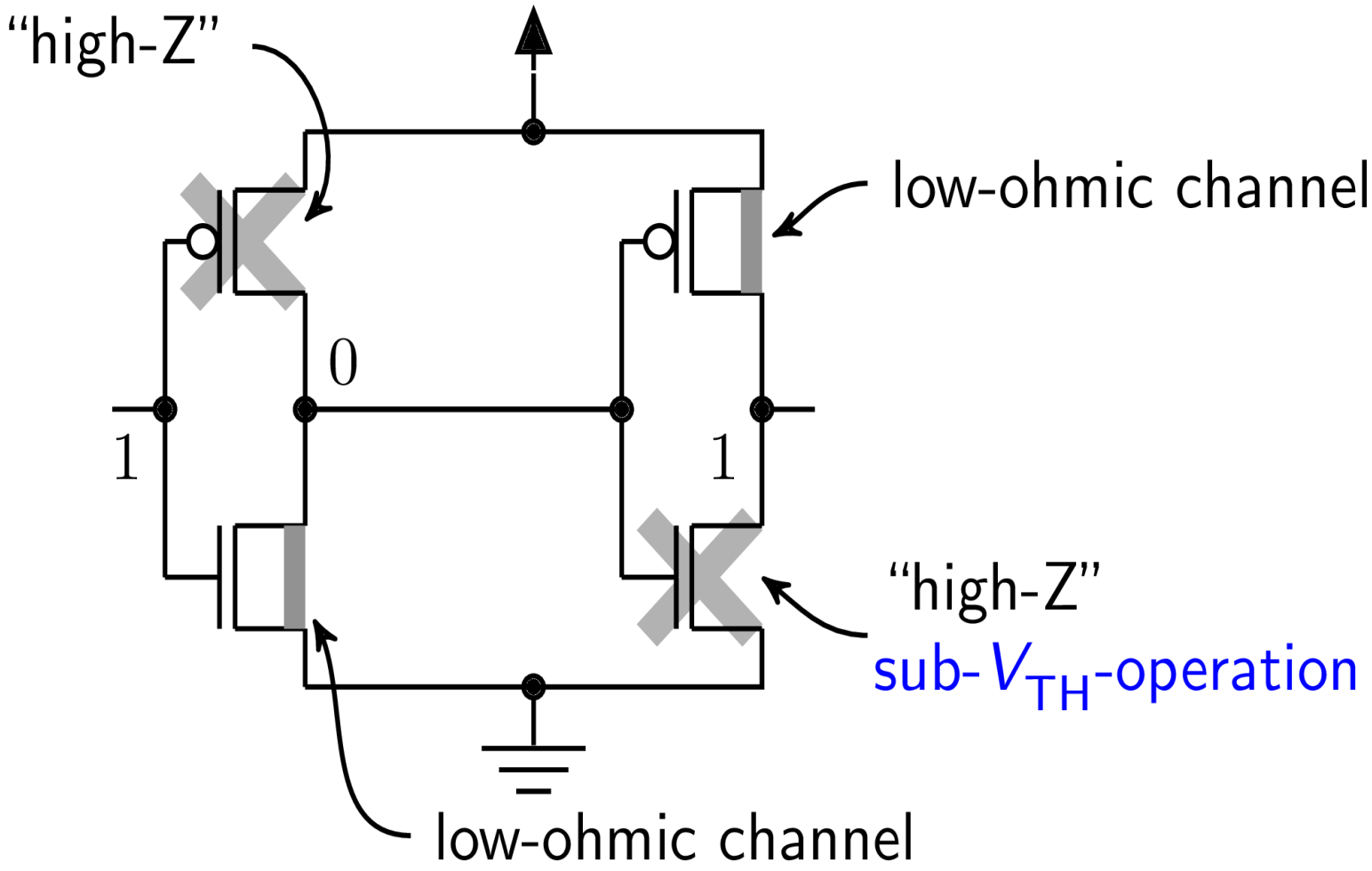


Thermoelectric Stimulation of SRAM Flip Flop

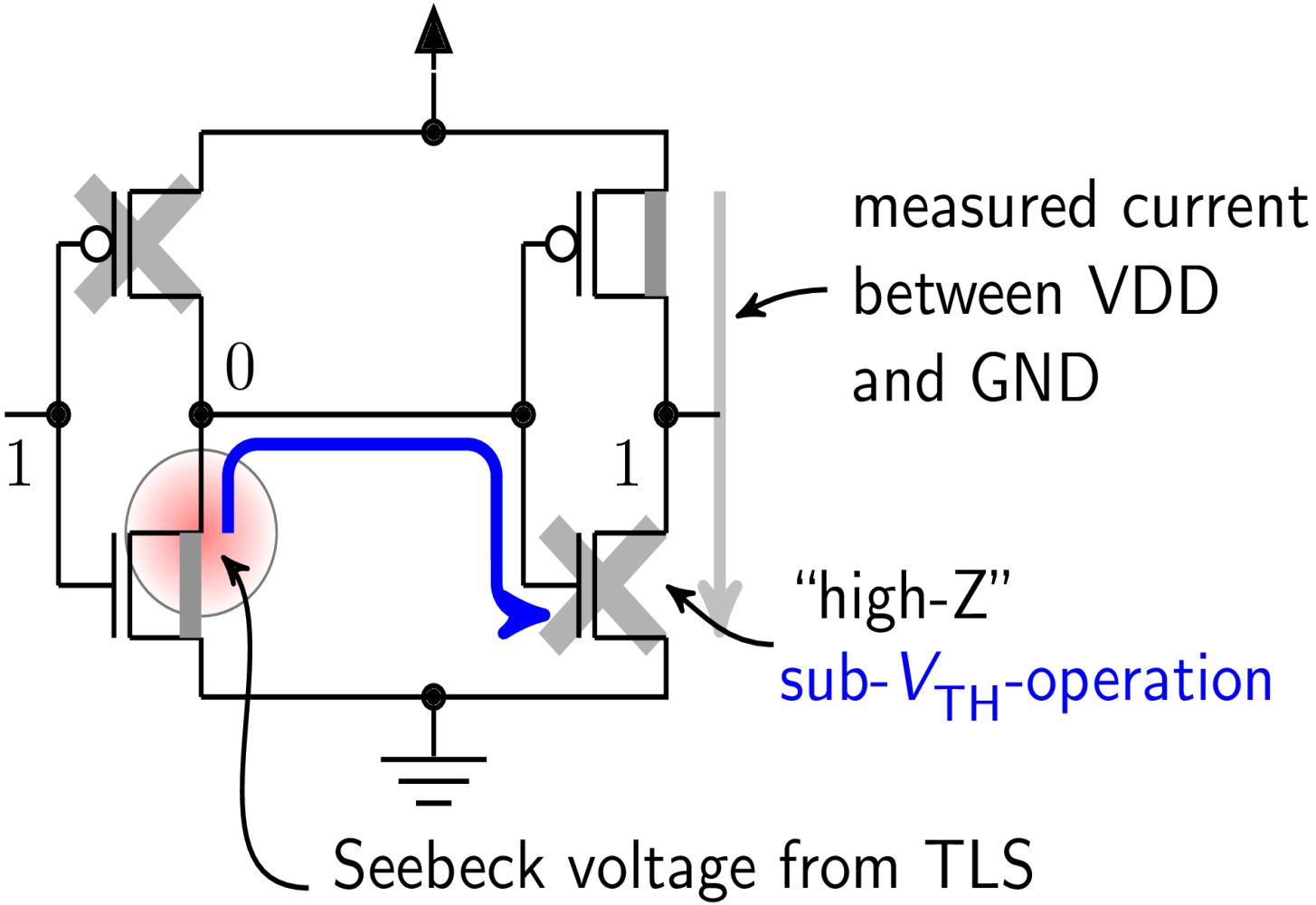


- Logic “1“ at input & output
- High Impedance / off:
- left PFET, right NFET

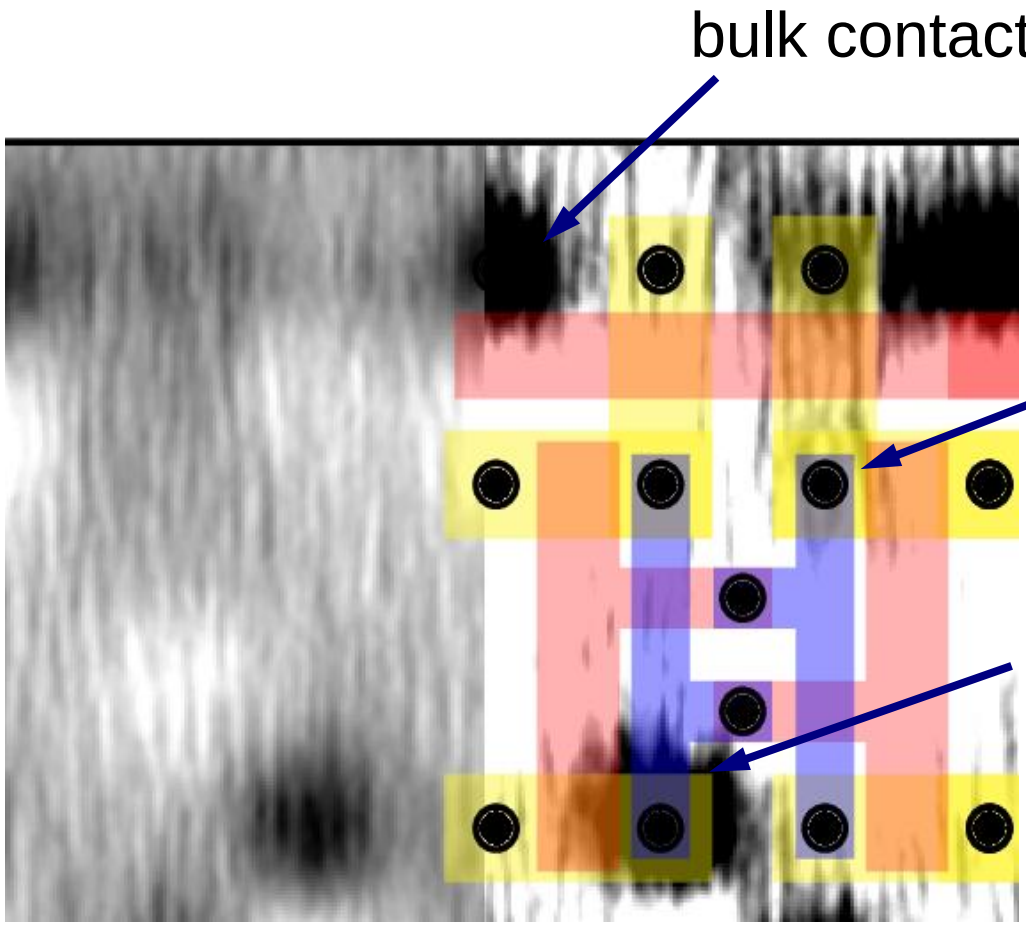
Thermoelectric Stimulation of SRAM Flip Flop



Thermoelectric Stimulation of SRAM Flip Flop

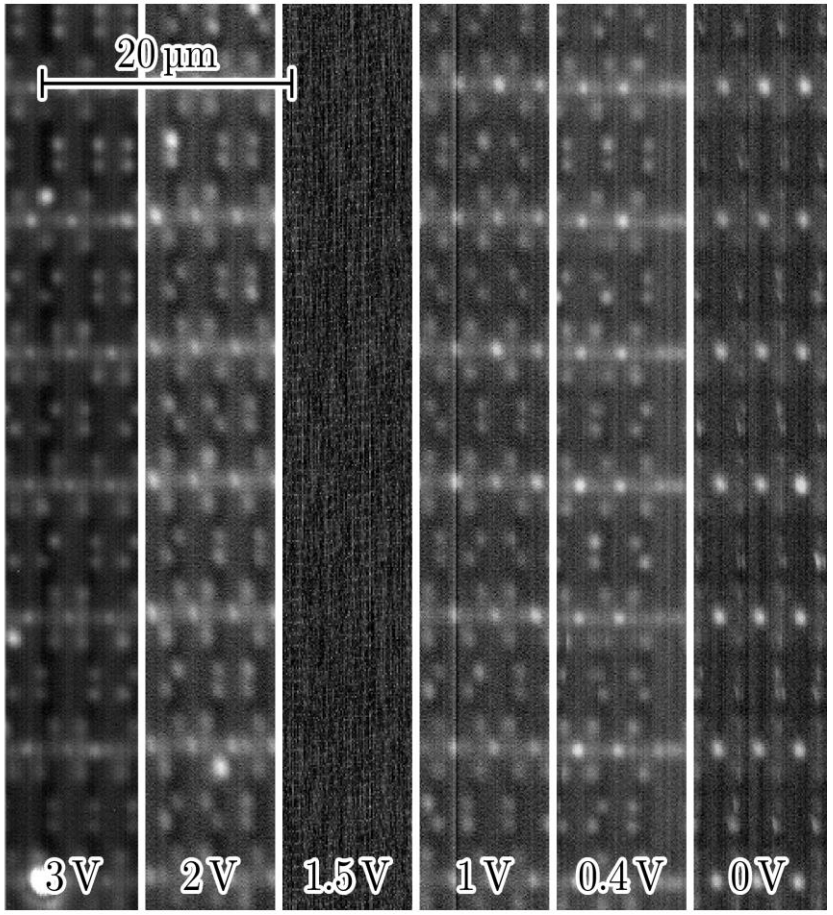


Contactless Read out of Logic SRAM State



Contactless Read out of Logic SRAM State / No Clock

- Simple Structure in Digital Circuits
- Repeated Layout is 100% regular
- Result Shows Irregular Pattern only for Powered Circuit
- Pattern is Data Dependent



1.5V: Logic running, non-static current consumption distorts measurement

In A Nutshell

- Contactless signal tracking mandatory in IC development & FA
- Contactless signal tracking = Physical Interaction
- Today physical interaction needs to access chip through backside = optical techniques play major role
- Backside access allows to compare signal quantitatively = new level of precision in signal reconstruction
- When debug and FA can access each electronic information in IC, these techniques are an enormous risk for IC security attacks

Outline

Why contactless Fault Isolation in ICs

Technology Node and CFI Evolution

The Benefits of CFI Backside Approach

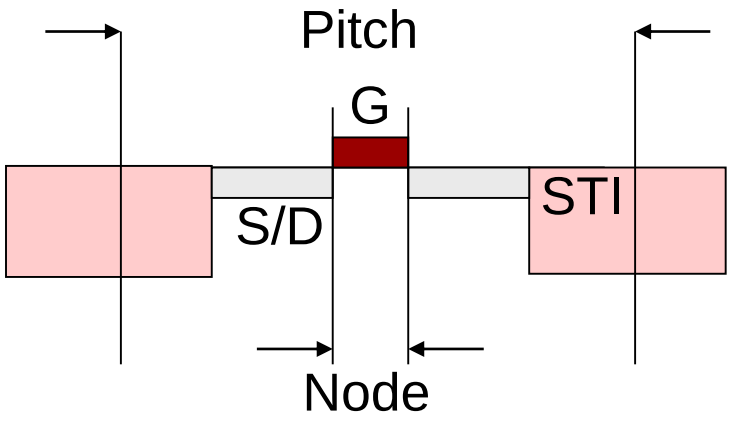
Relevant CFI Techniques and Attack Risks

IoT Roadmap: Nanoscale FinFET & Low Power

CFI will prevail and the Attack Risk with it

Backside Protection

CFI Resolution Required for Nanoscale Technologies



CFI requires to resolve pitch

Pitch ca 3.5-8x min. feature size

ITRS 2.0 2018:

Tech Node	Pitch	Year
45nm	160nm	2007
32nm	112nm	2010
22nm	90nm	2012
14nm	70nm	2014
10nm	64nm	2017
7nm	50nm	2018
5nm	40nm	2020
3nm	32nm	2024

CFI Resolution

$R = 0.61\lambda/NA \quad NA = n \times \sin\alpha$

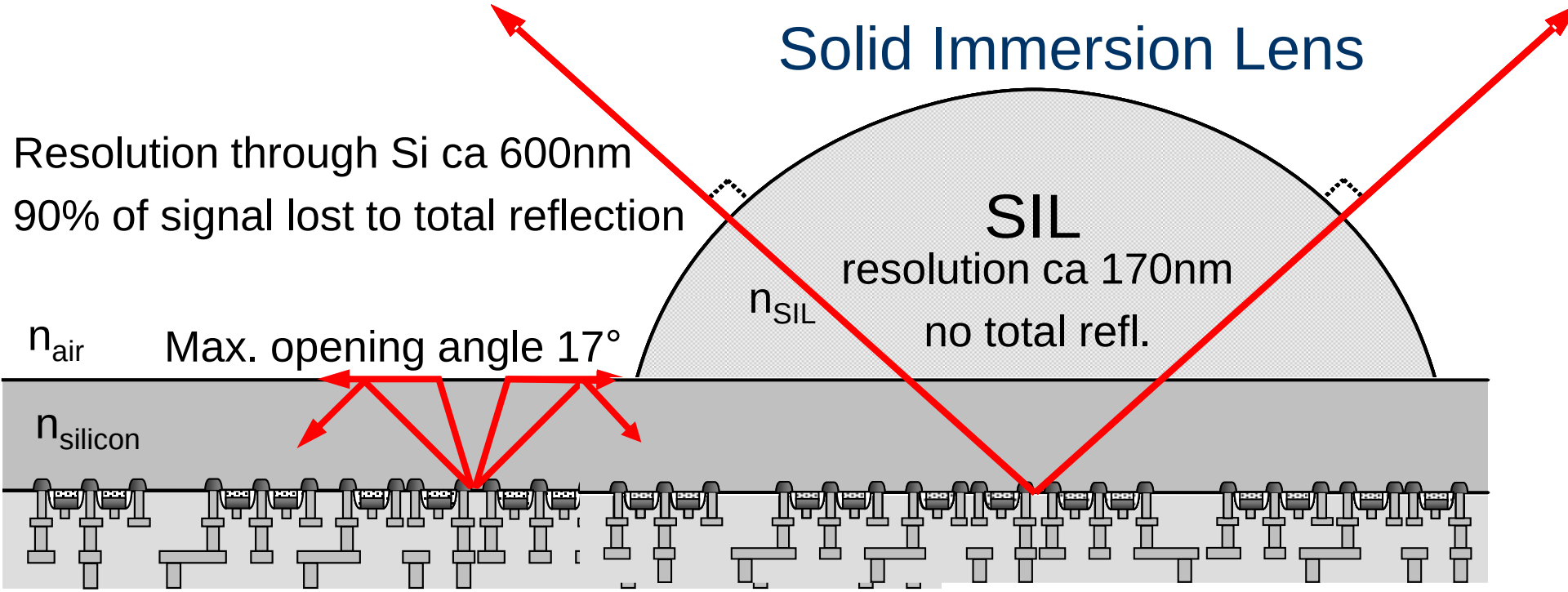
λ: Light wavelength (NIR: ≈ 1µm) NA: Numerical aperture

n: Index of refraction (Air = 1, Si = 3.5) sinα: Aperture of Objective (<1)

Solid Immersion Lens

Resolution through Si ca 600nm

90% of signal lost to total reflection



SIL increases resolution… !! and signal intensity !!

But: There is some tolerance…

Discussion of required resolution by Intel @ ISTFA 2015

NIR is good for…

	Technology node				
	32nm	22nm	14nm	10nm	7nm
Lens NA	1.4 (LIO)	2.6 (SIL)	3.0 (SIL)	3.3 (SIL)	TBD
Optical resolution @ λ = 1500 nm	654 nm	352 nm	305 nm	277 nm	TBD – new solution needed
@ λ = 1064 nm	464 nm	250 nm	216 nm	197 nm	TBD
Contacted gate pitch	112.5 nm [2]	90 nm [3]	70 nm [1]	~64 nm [4]	~50 nm [4]
FI capability	Fair	Very good	Good	Fair	TBD
F (1500)=	5.81	3.91	4.36	4.32	5.54
F(1064)=	4.12	2.77	3.08	3.07	3.94

Diffraction-limited resolution δ:

$$\delta = \frac{0.61\lambda}{NA}$$

Correlation factor F = Resol. / Pitch

Table from v. Haartman et al, Proc. 41st ISTFA 2015, Nov. 1-5, Portland OR, pp 47-51

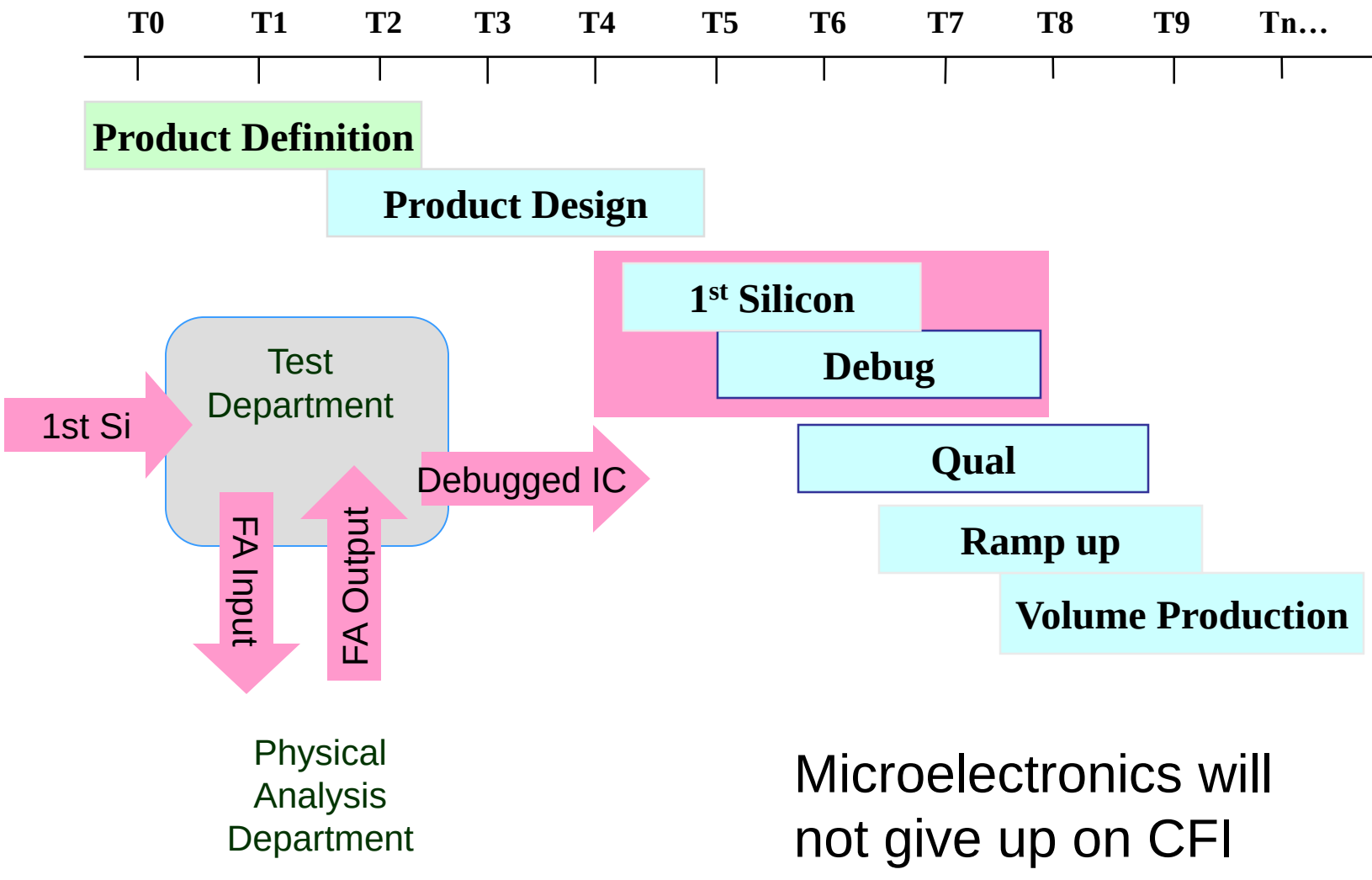
What can we expect?

- IoT Technology roadmap hard to predict
- Nominal shrink will use higher device density through 3D
- Drastic VDD drop

ITRS 2.0 Report 2018 (Dimension [nm])				
Tech Node	Pitch	Year	Voltage	Structure
45	160	2007	1V	Planar
32	112	2010	0.9V	Planar / PD SOI
22	90	2012	0.85V	Planar / FD SOI
14	70	2014	0.85V	FinFET / FD SOI
10	48	2017	0.8V	FinFET / FD SOI
7	42	2018	0.7V	FinFET / LGAA
5	32	2020	0.7V	FinFET / L(V)GAA
3	24	2024	0.6V	VGAA /M3D

ITRS - International Technology Roadmap for Semiconductors edition 2015 [Online]. Available: http://cpmt.ieee.org/itrs-2-0-2015-edition.html

Reminder: Role of CFI in IC Development Process



Microelectronics will not give up on CFI

Ref – Steve Maher

CFI Trends to Match IoT Requirements

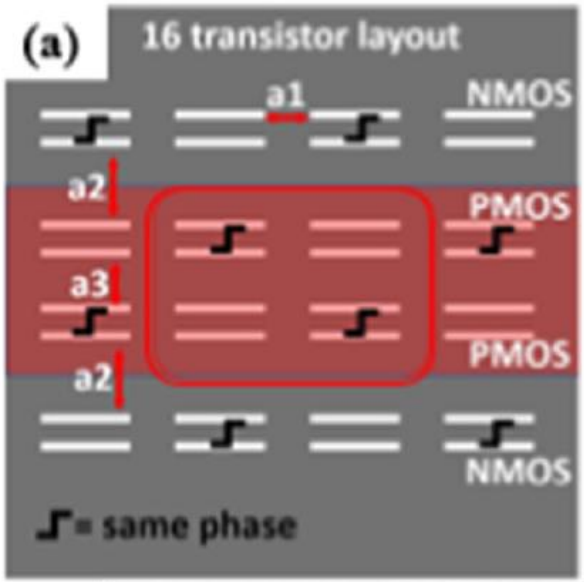
IoT challenge: Cloud for manufacturing: high data rate

→ Low power, further miniaturization, 3D

– where does the research go?

- Low power:
  - LVP ok
  - Photon Emission?
- Image Resolution:
  - LVP: Shorter Wavelength?
  - Return to E Beam?
- Alternatives / Complimentary?
  - Simulation of signal mix?
  - 3D?

Nanoscale: Challenge to NIR - CFI



14nm RESOLUTION PREDICTION

Fin pitch	48nm
Gate pitch	78nm
Fin width	14nm
Gate width	14nm

$R = 0.61\ \lambda/NA$

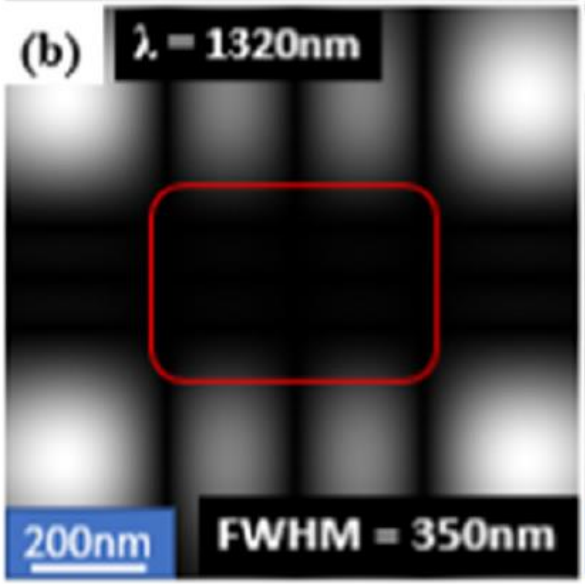
$NA = n \times \sin\alpha$

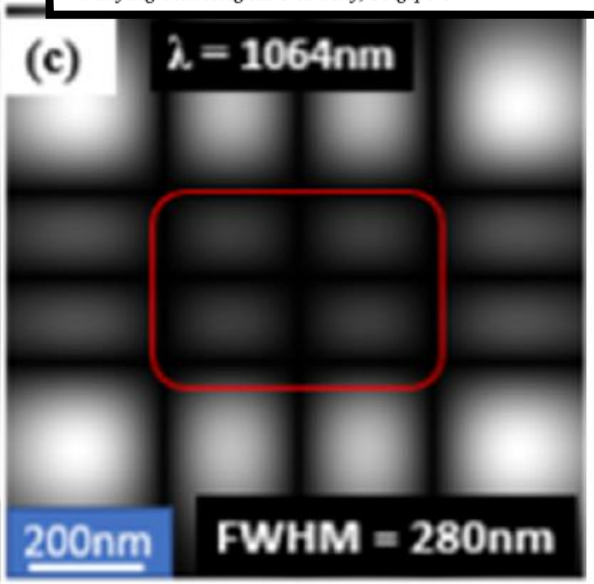
Understanding spatial resolution of laser voltage imaging

V.K. Ravikumar[a,b,*], G. Lim[b,c], J.M. Chin[b], K.L. Pey[a], J.K.W. Yang[a]

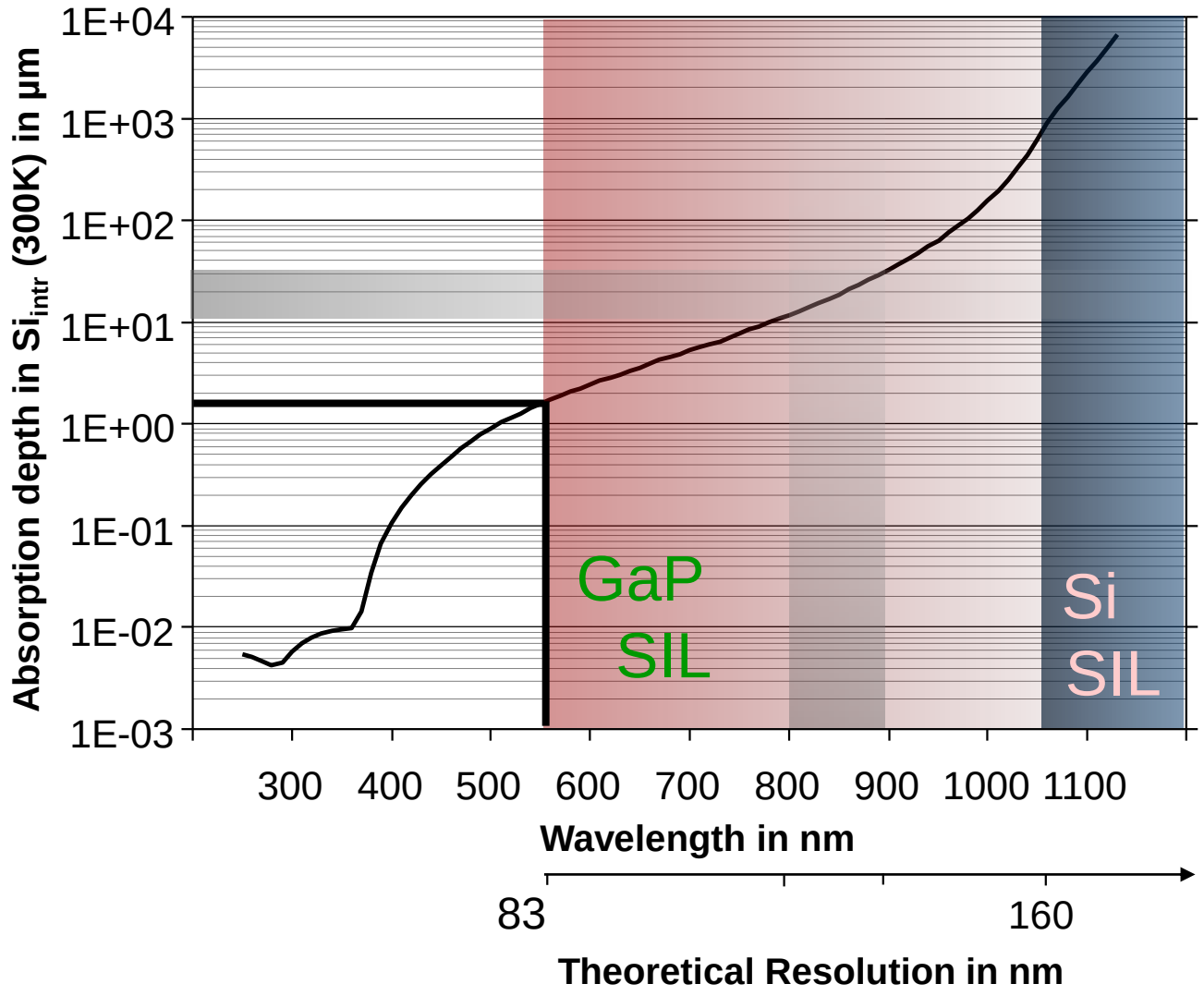
[a] Singapore University of Technology and Design, Singapore
[b] Advanced Micro Devices Singapore Pte Ltd, Singapore
[c] Nanyang Technological University, Singapore

ESREF 2018

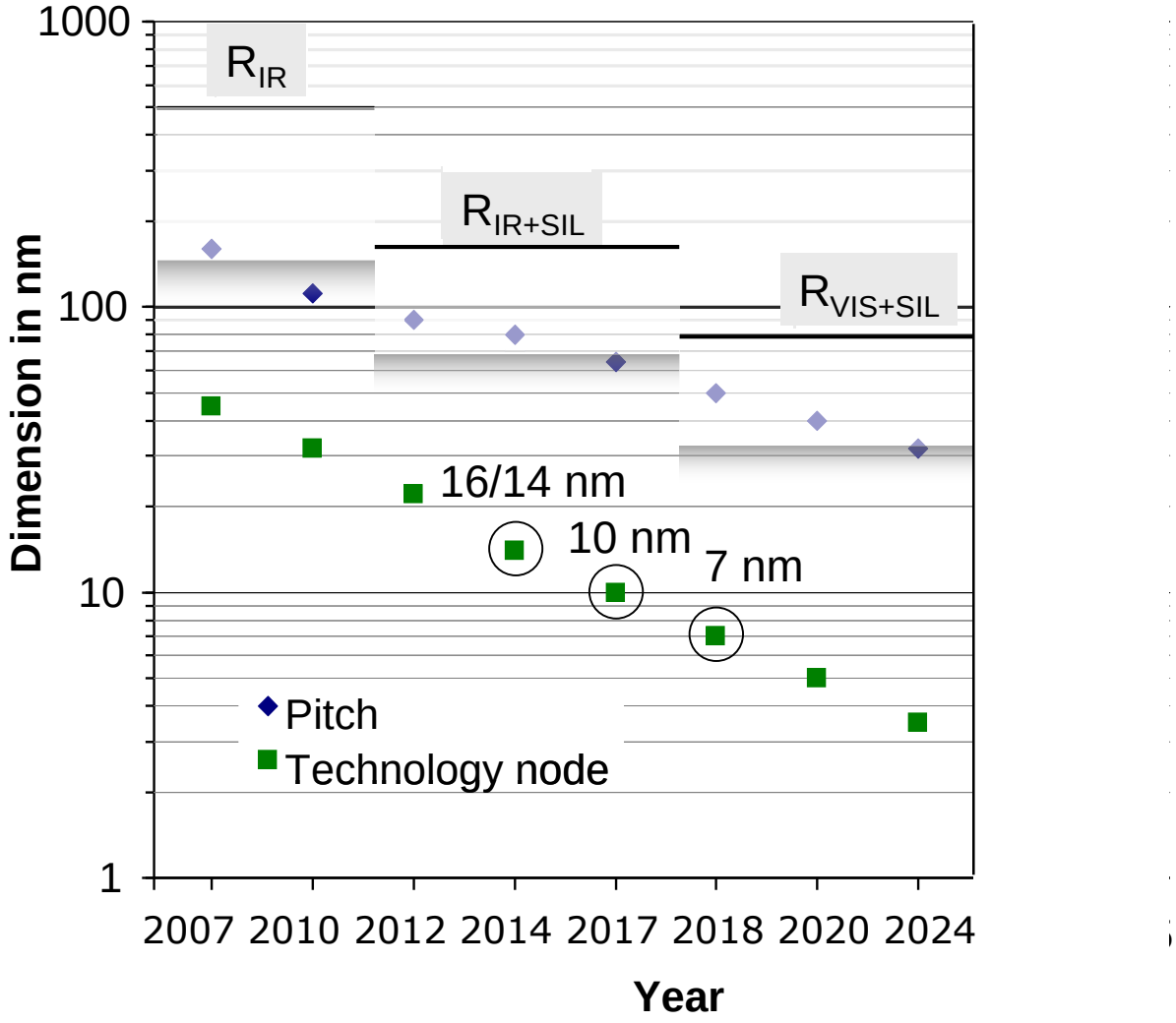




Moderately Shorter Wavelength – GaP SIL



CFI is ok for 10 more years of Moore‘s Law – through chip backside with 1-3 µm Si thickness



Resolution is based on wavelength and numerical aperture

Resolution necessary for CFI ≠ pitch
~200 nm resolution is “good” for 14 nm node

Shorter Wavelength: Bulk Absorption / Sample Thickness

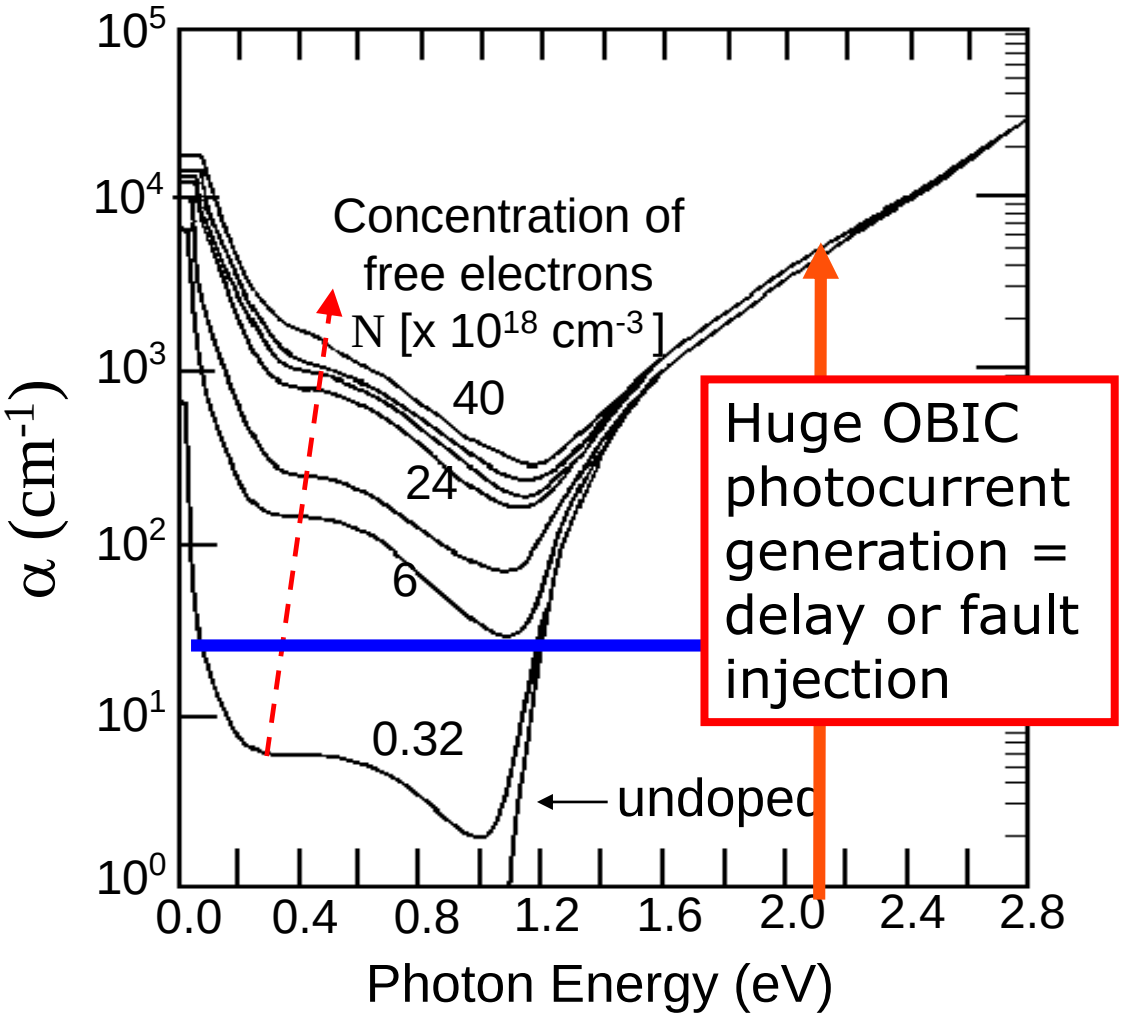
Sufficient transmission through Si good for die thickness of

1µm

10µm

100µm

500µm



Soref et al., IEEE J. of Quant. Elec., Vol. QE-23, No.1, January 1987

Backside E Beam Probing on Ultra Thin Si

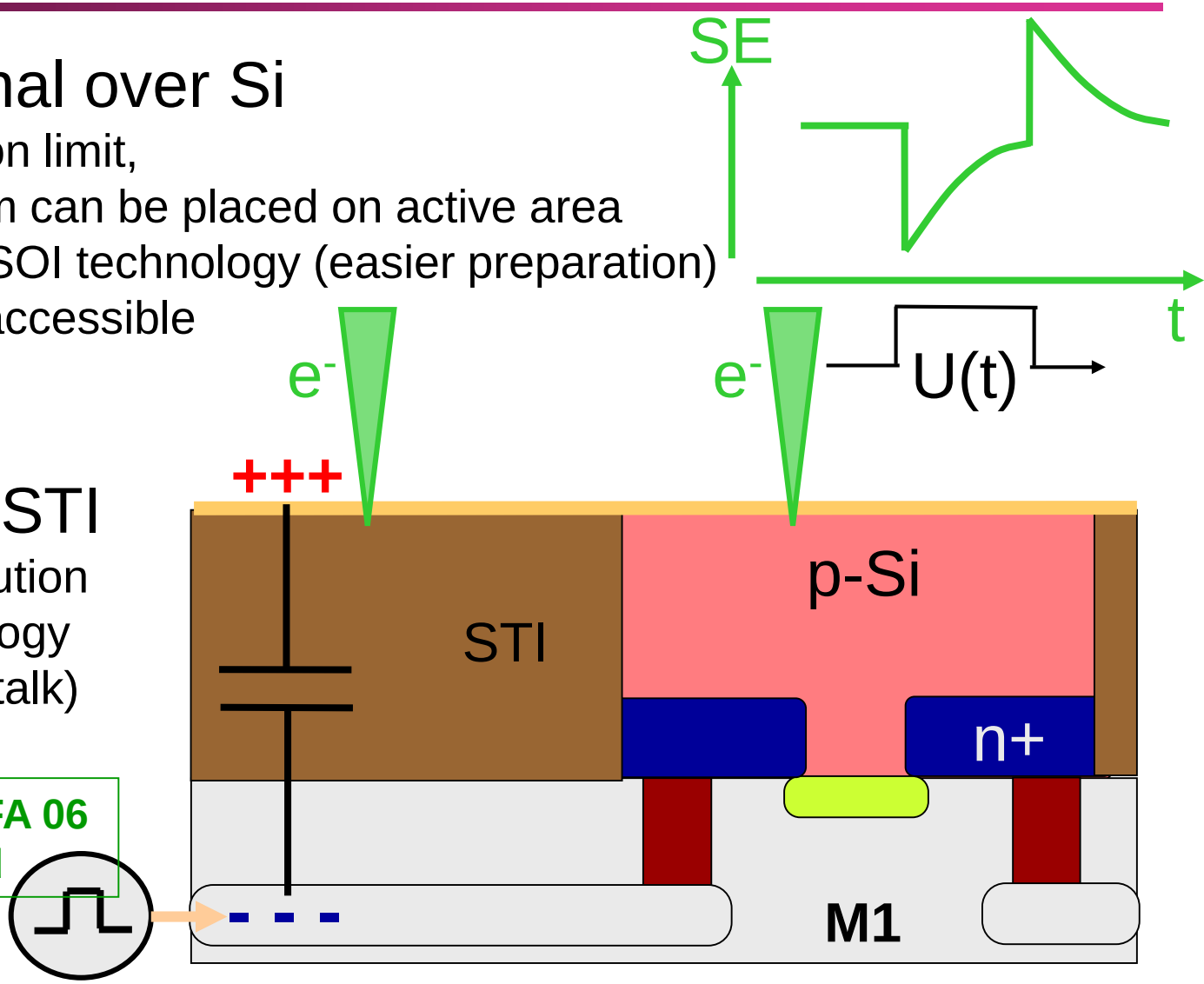
Active FET signal over Si

- hardly any resolution limit,
  as long as the beam can be placed on active area
- very promising for SOI technology (easier preparation)
- every circuit node accessible

M1 signal over STI

probably facing resolution limit for latest technology (Z-distance / pitch, x-talk)

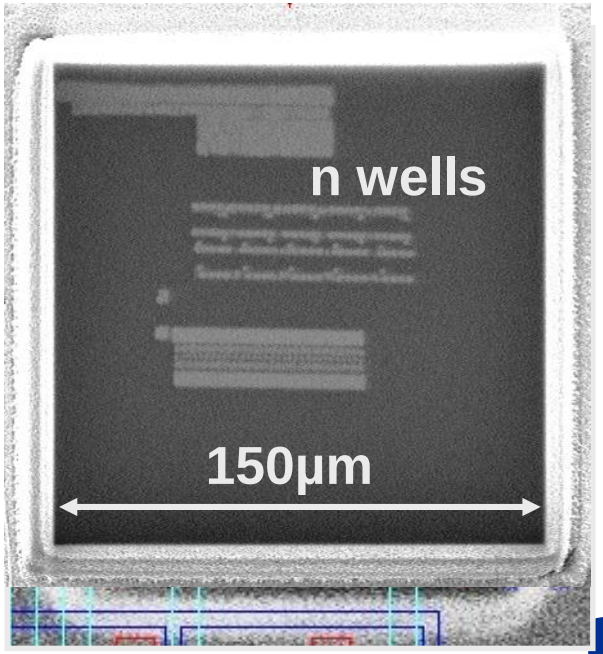
TUB Research @ ISTFA 06
Best Paper Award

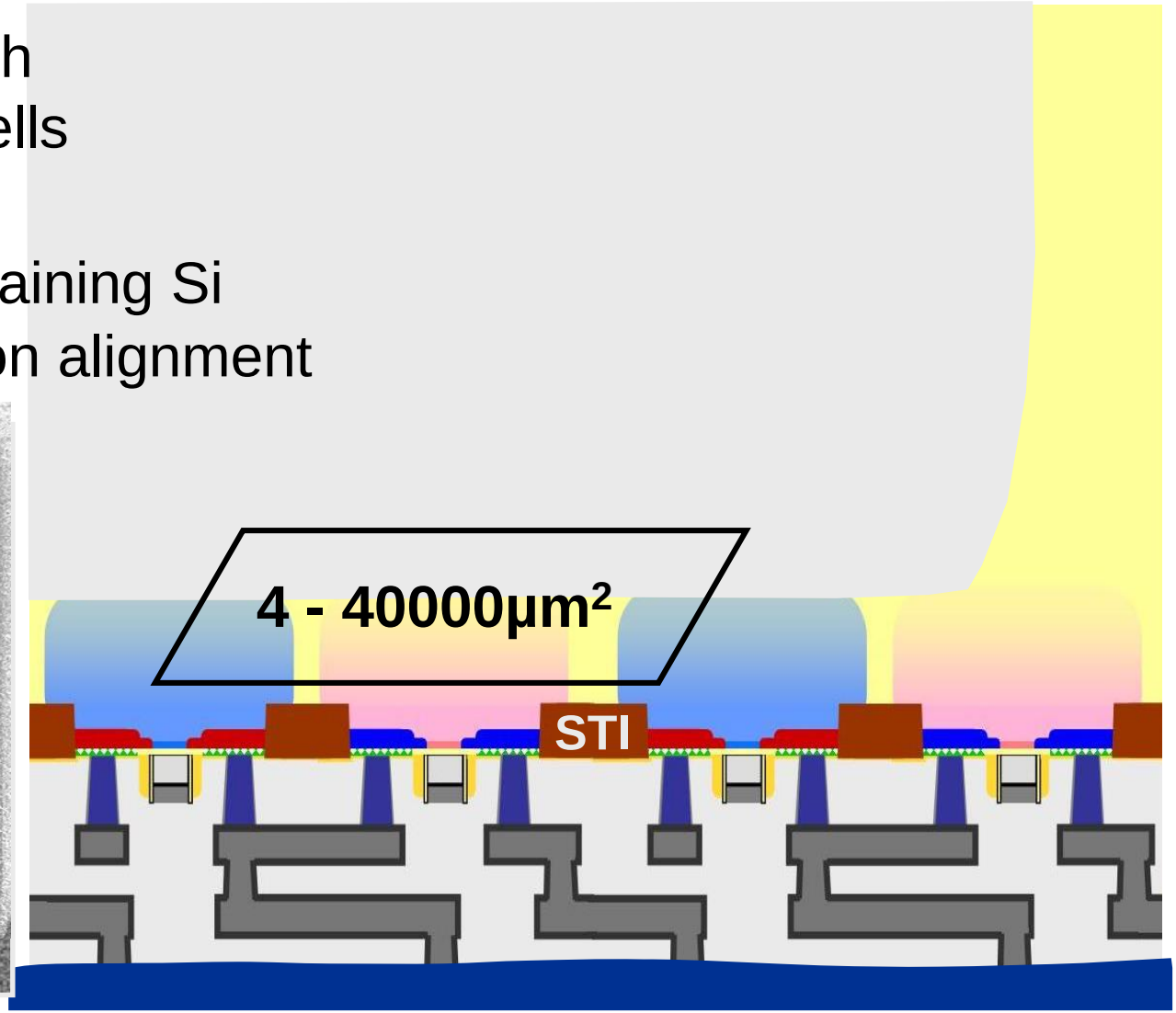


FIB Backside Circuit Edit Procedure

- mechanical thinning
- localized FIB trench
  - stopping on n-wells
  - stopping on STI

    < 400nm remaining Si
- local high precision alignment





Circuit Edit on Ultra thin Silicon

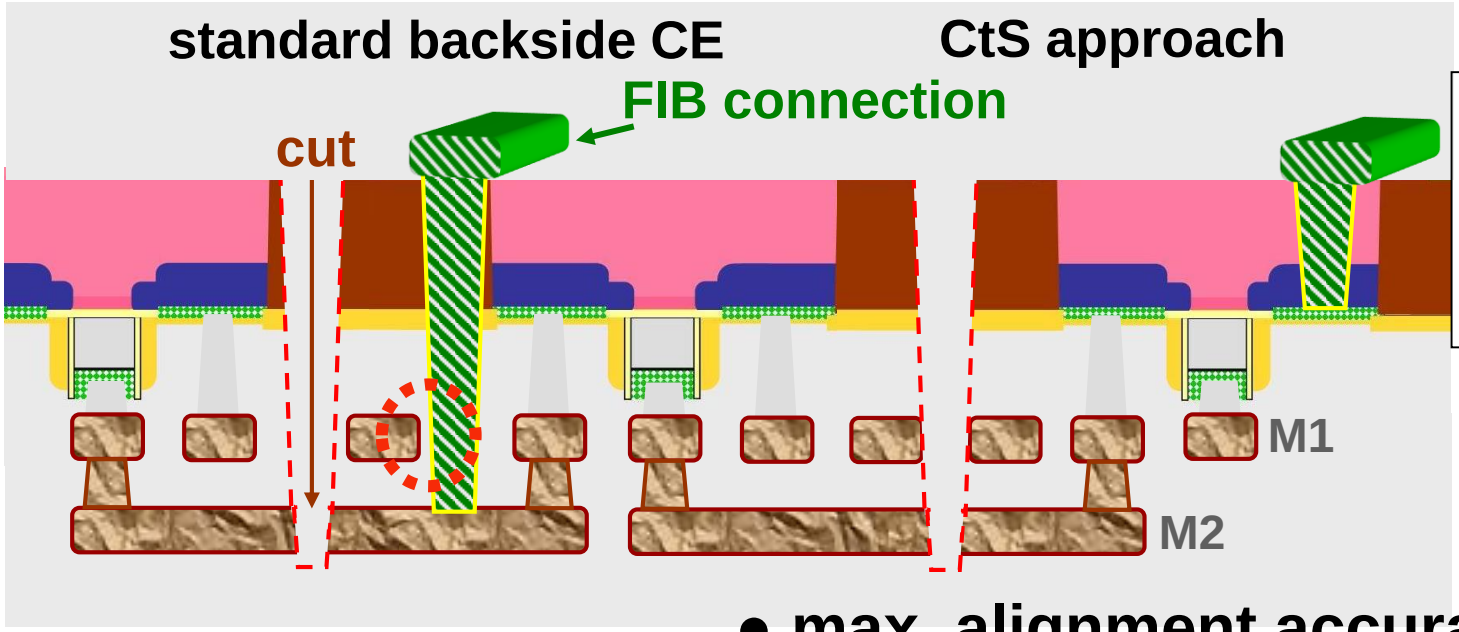
Contact to Silicide:

- reduced aspect ratio
- low ohmic contacts
- access to any node on Chip
- only "cut" on metal
- CE on device level

Successfully applied for:

CE, direct probing & device characterization (backside AFP)

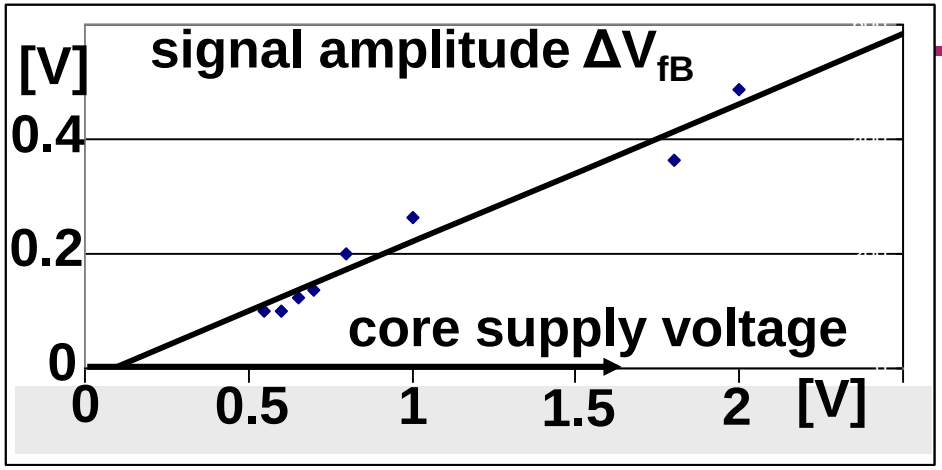
Thinning closer trims device performance to desired logic state



FIB "wrinting" of keys

- **max. alignment accuracy (<20nm)**

E Beam Probing / Signal Scaling



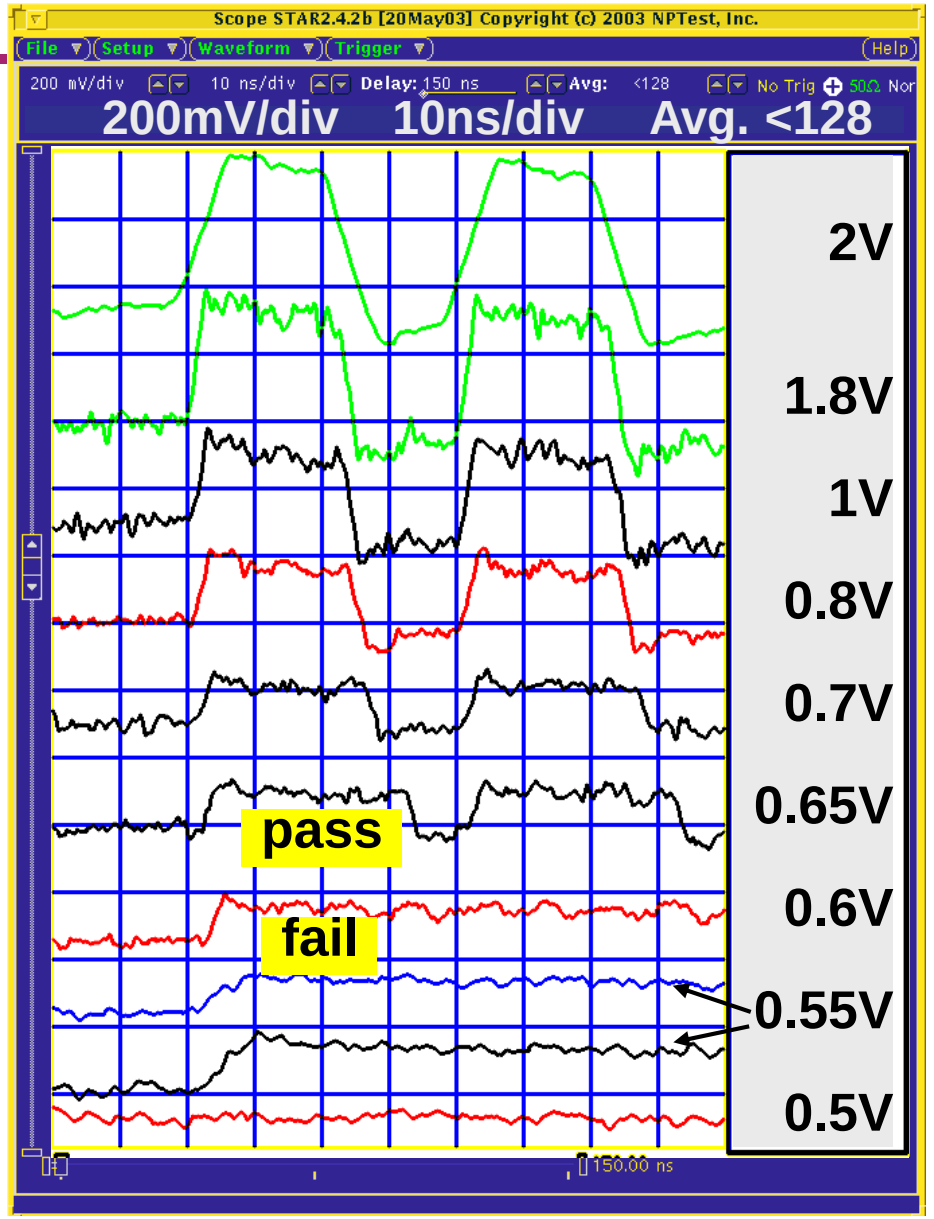
- linear V_{dd} scaling

- but: For waveform of 10GHz:

Minimum 3 electrons per 10^{-10} s

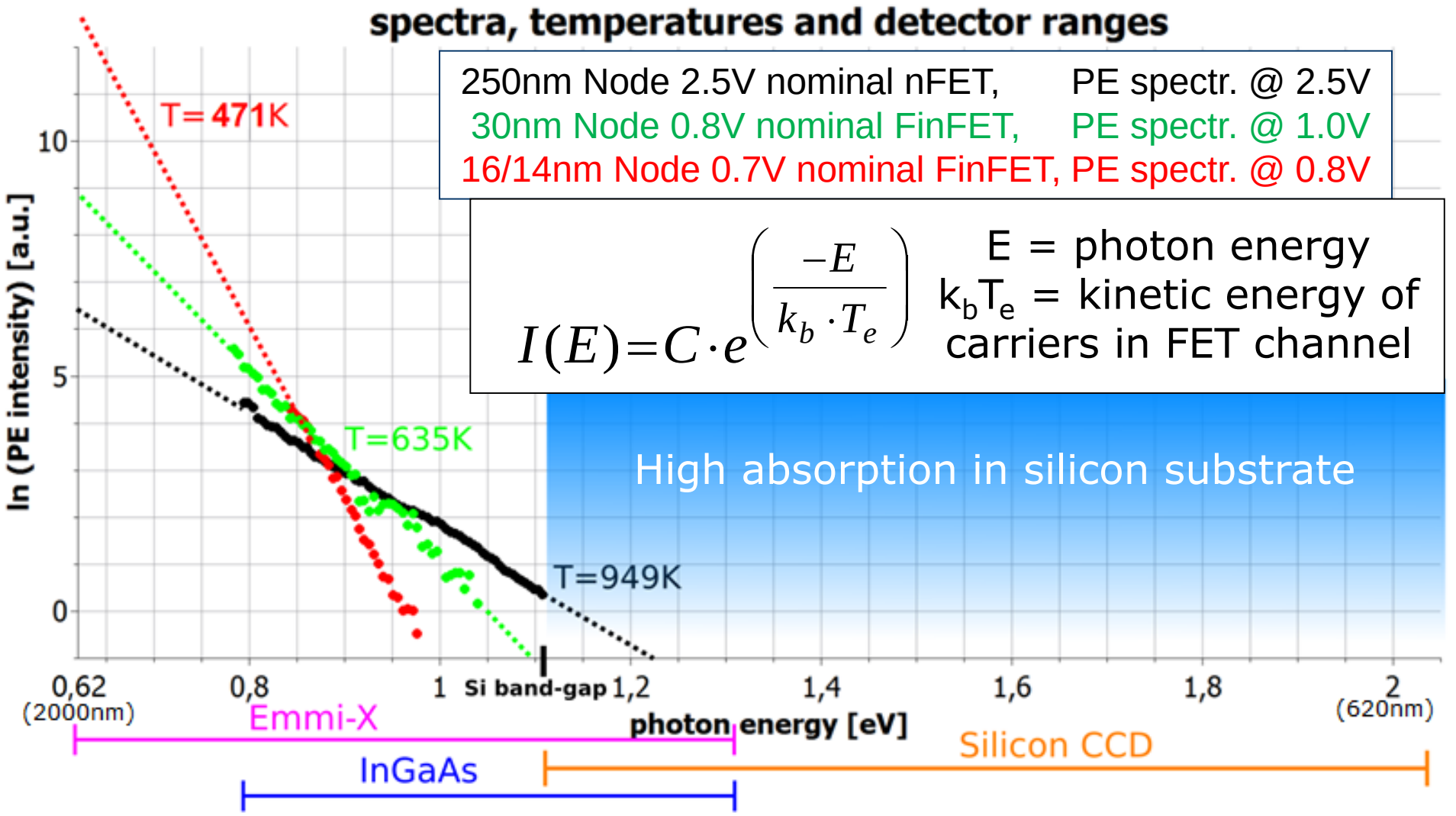
→ E Beam current > 5µA

SEMs: max 100nA



TUB Research @ IEEE IPFA 07
Best Paper Award

Photon Emission and Low Power Technologies

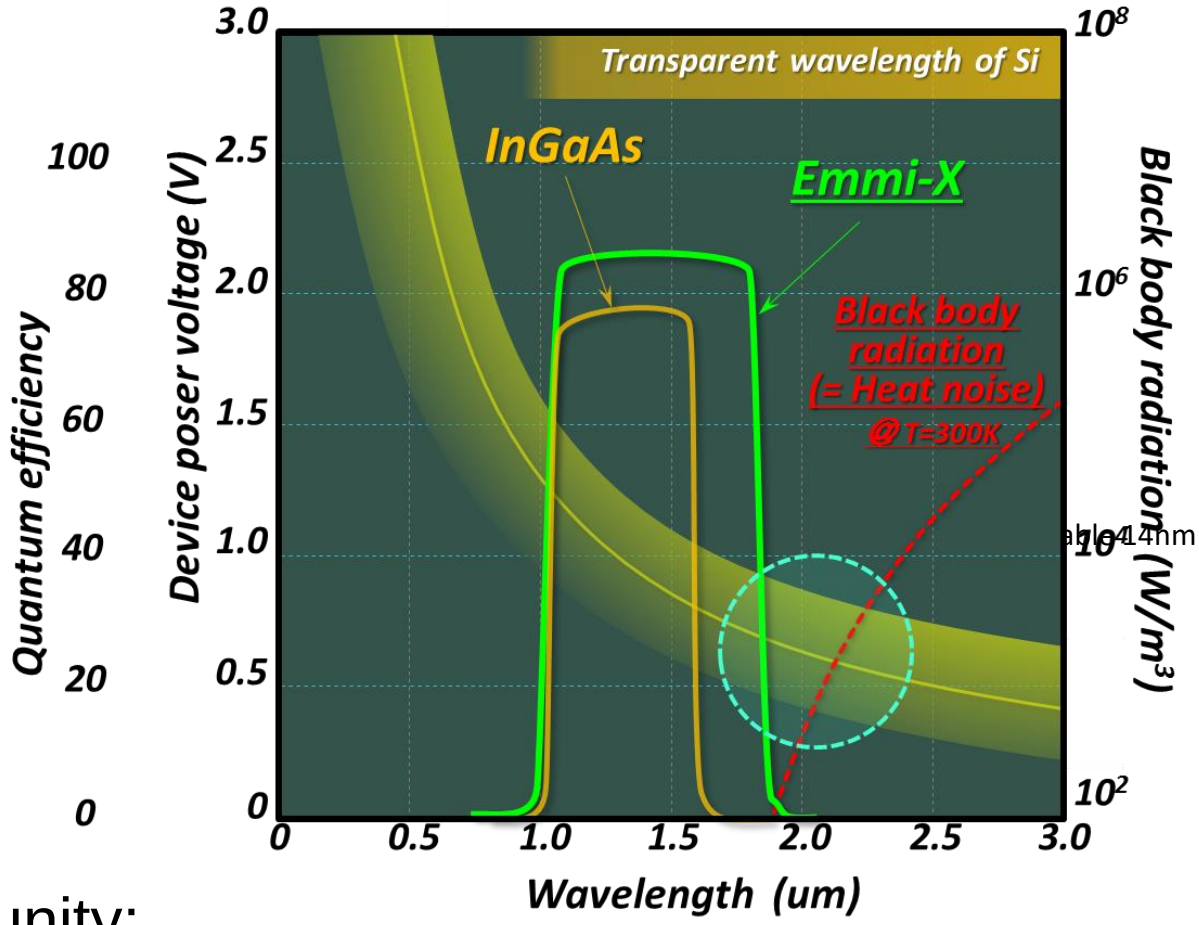


Expanded Detector Sensitivity into IR for Low Power

High sensitivity for low voltage device: < 0.5V verified

Low noise by selectable optimized filters

High resolution 1000 x 1000 pixels



Source: Hamamatsu Emmi-X Camera

New detector opportunity: Superconducting Single Photon Detector SSPD, also dynamic

New CFI Techniques for IoT Requirements

- Low power:
  - LVP ok
  - Photon Emission may work but resolution probematic; only complimentary technique
- Image Resolution:
  - LVP: Shorter wavelength good for resolution but Thin sample + Delay Induction / Fault Injection ?
  - E Beam: Perfect resolution but dynamic probing limited to < GHz + electron induced degradation?
- Alternatives / Complimentary?
  - Simulation of signal mix detected in field of view of NIR based CFI techniques?

Maybe new CFI techniques too complex…

- Then a simulation of the expected signal mix might be a solution….

Pattern search automation for combinational logic analysis (CLA)

Ravikumar Venkat Krishnan[1,2], Seah Yi Xuan[1], Lim Gabriel[1], Tan Abel[1], Lua Winson[1], Gopinath Ranganathan[1], Phoa Angeline[1], Chua Choon Meng[3]

1. Advanced Micro Devices, Singapore; 2.Singapore University of Technology and Design, Singapore; 3. SEMICAPS, Singapore

Correspondence email: Venkat-krishnan.ravikumar@amd.com

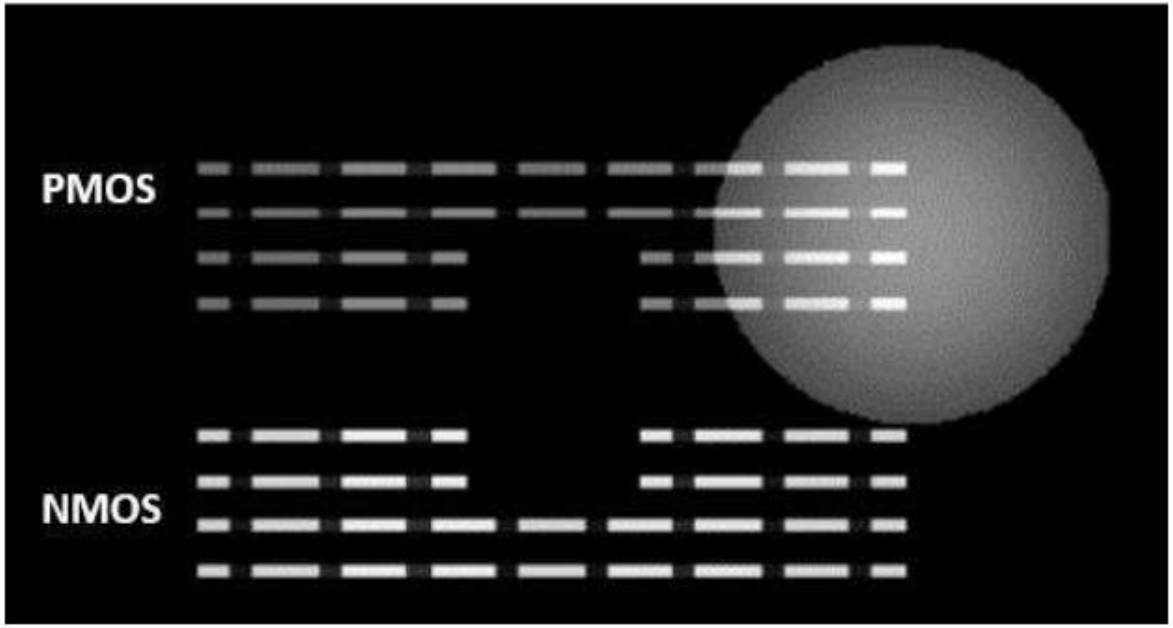


***Figure 6**: Simulation of the XNOR and the optic probe parked on the PMOS output Z net. The white rectangles are positions of the fin polygons, and the gate polygons are not visible. The white circle is the position of the laser.*

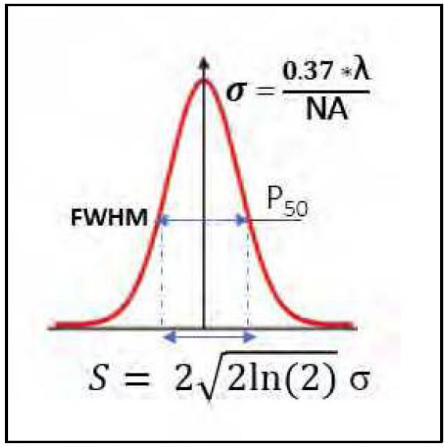


***Figure 1:** Simplified model of the optic probe profile relating the probe diameter to the NA and wavelength*

ISTFA™ 2018: Conference Proceedings from the 44th International Symposium for Testing and Failure Analysis October 28–November 1, 2018, Phoenix, Arizona, USA

Simulated vs. Measured Laser Probing Signal

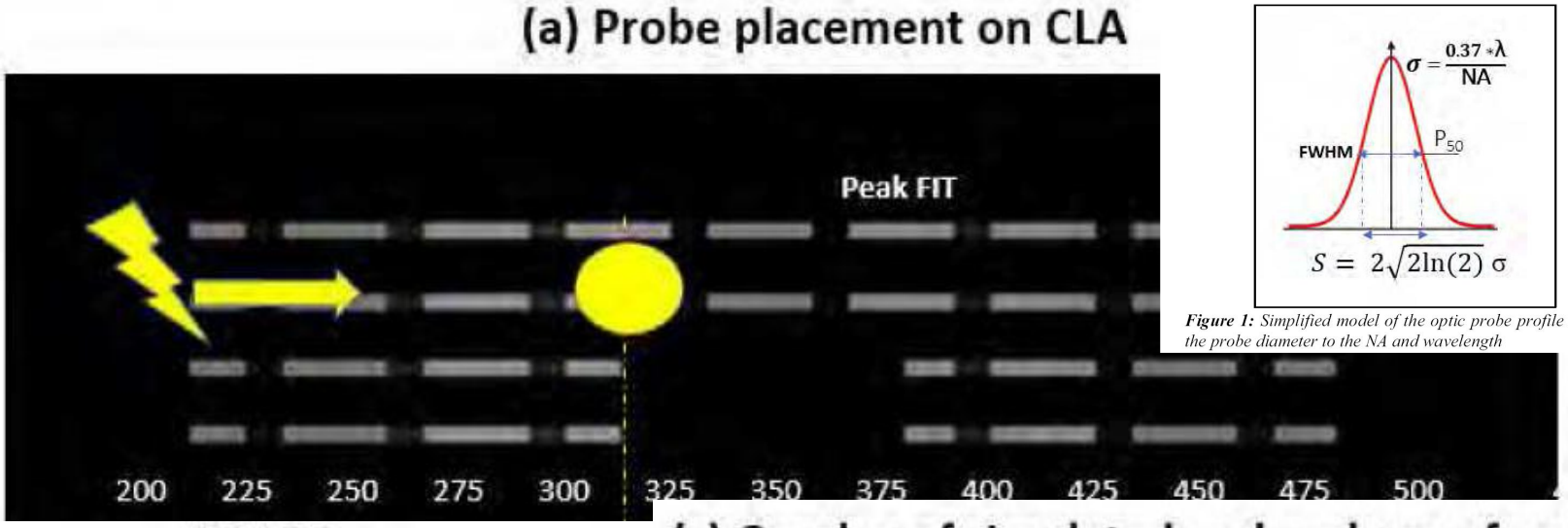
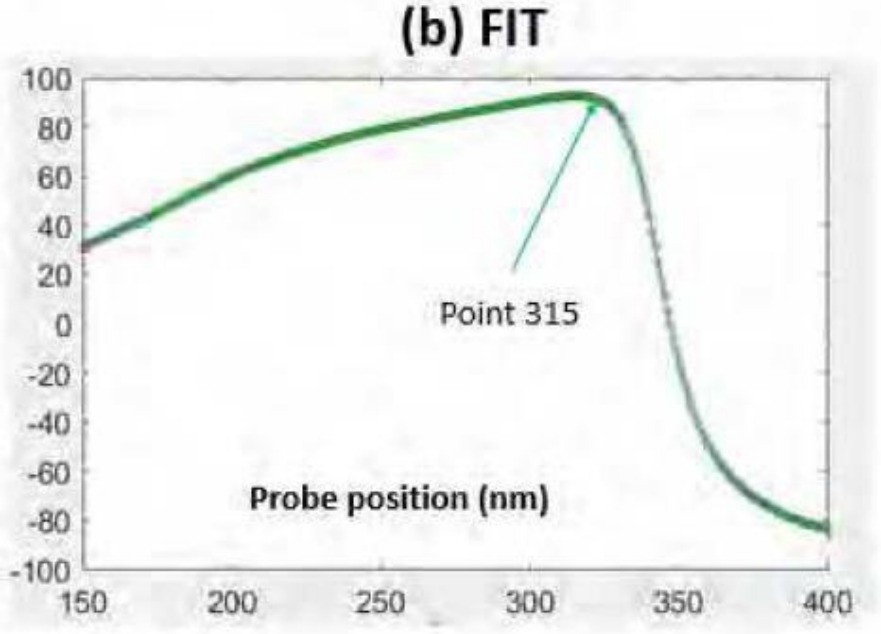
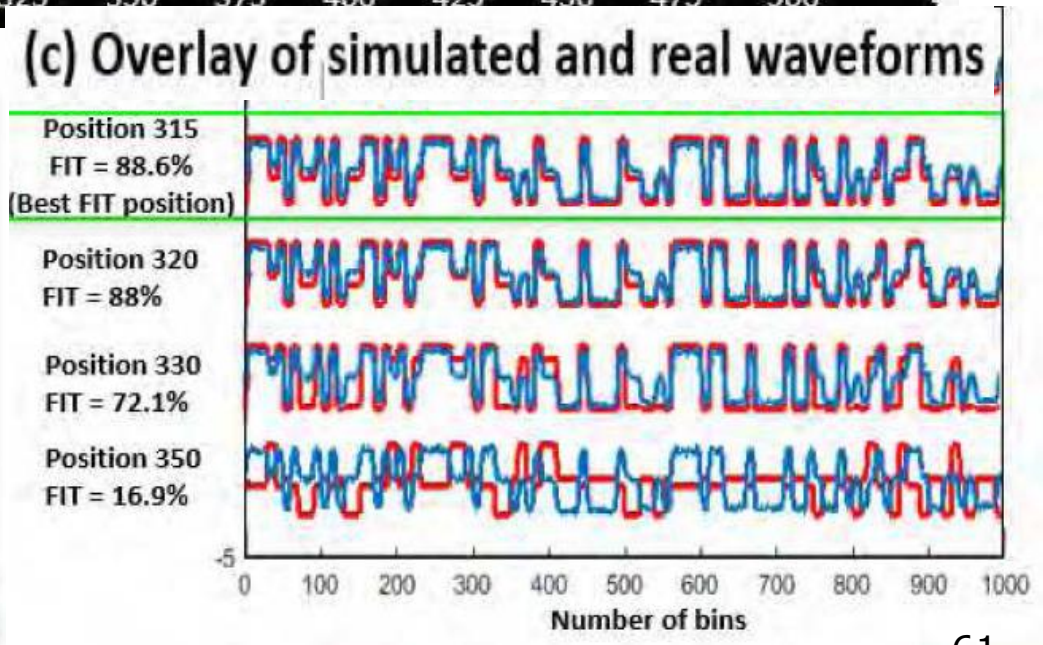
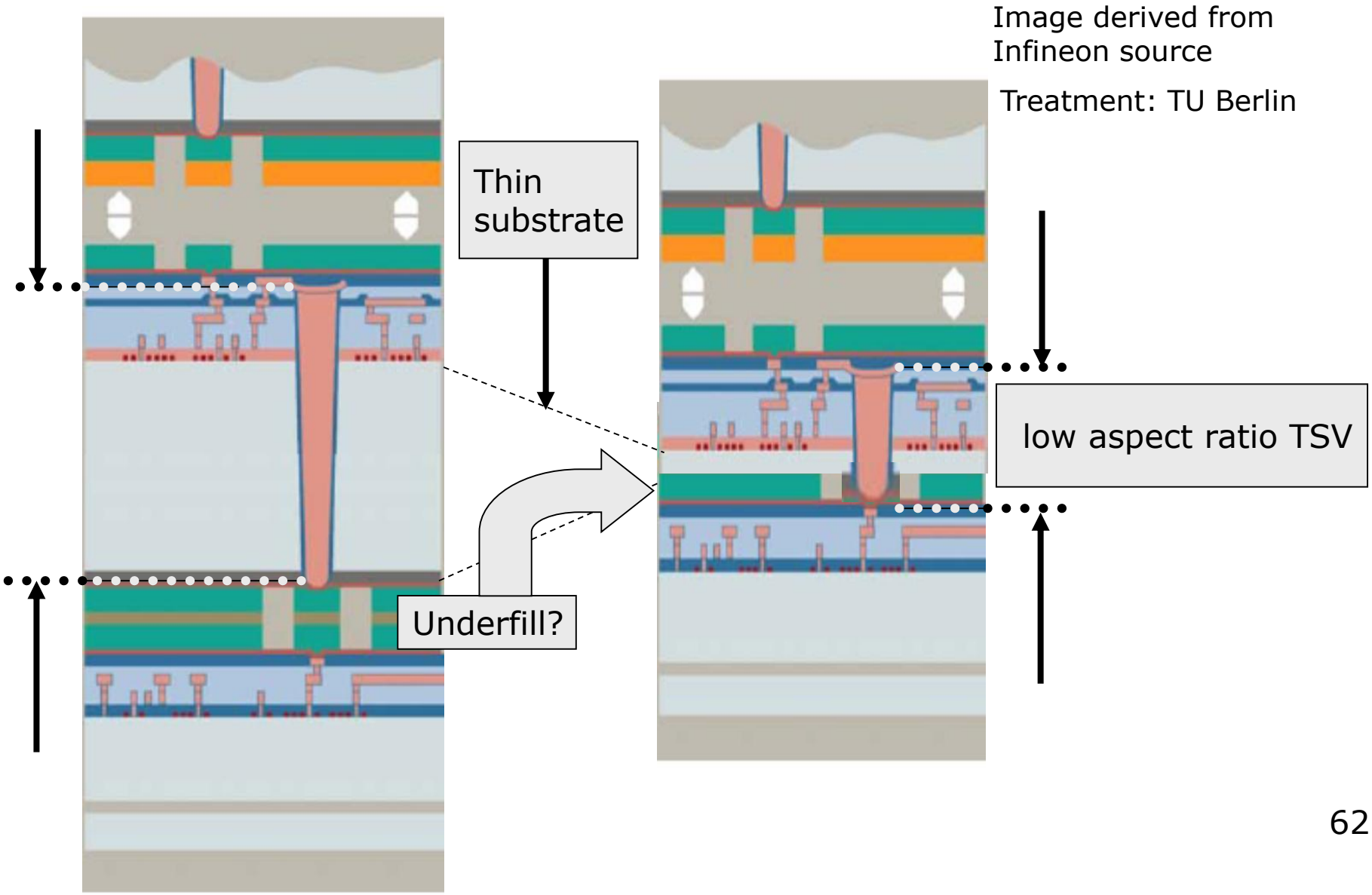


Figure 1: *Simplified model of the optic probe profile relating the probe diameter to the NA and wavelength*





3D Integration and SoC for IoT



CFI Readiness for SoC / Package Level

- Dimensions in 3D SoC / Packages will come closer to chip level technologies:
- Optical CFI techniques will conquer 3D as well
- Underfill / Interposer: Lock in Thermography dynamic
- Time domain reflectormetry THz

- Global interconnects will go photonic:
- Laser based CFI techniques may be used to modulate photonic signals

- Programmable BIST:
- May cover much of future debug / FA needs

63

In A Nutshell

- Contactless signal tracking mandatory in IC development & FA
- Contactless signal tracking = Physical Interaction
- Today physical interaction needs to access through chip backside = optical techniques play major role
- Backside access allows to compare signal quantitatively = new level of precision in signal reconstruction
- When debug and FA can access each electronic information in IC, these techniques are an enormous risk for IC security attacks
- Challenge: Nanoscale Miniaturization
- The demand for contactless signal tracking in IC development will provide solutions throughout all coming technologies for debug and FA that will support the security attackers as well
- Progess to new technologies will not protect from CFI attack risk - but only a valid backside protection strategy

Outline

Why contactless Fault Isolation in ICs

Contactless = Physical Interaction

Technology Node and CFI Evolution

The Benefits of CFI Backside Approach

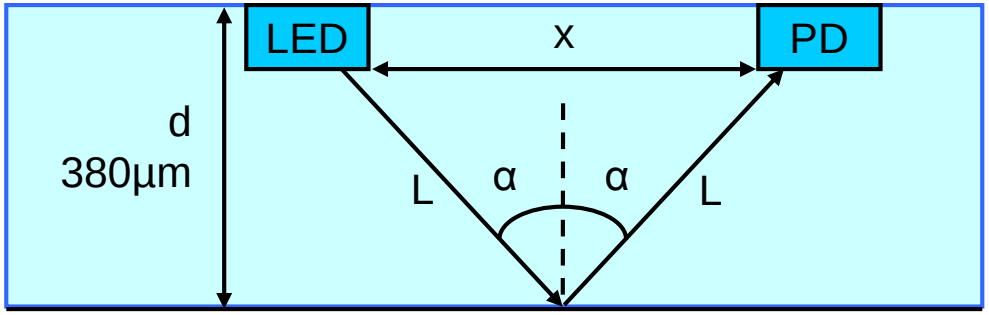
Relevant CFI Techniques and Attack Risks

IoT Roadmap: Nanoscale FinFET & Low Power

CFI will prevail and the Attack Risk with it

Backside Protection Concepts

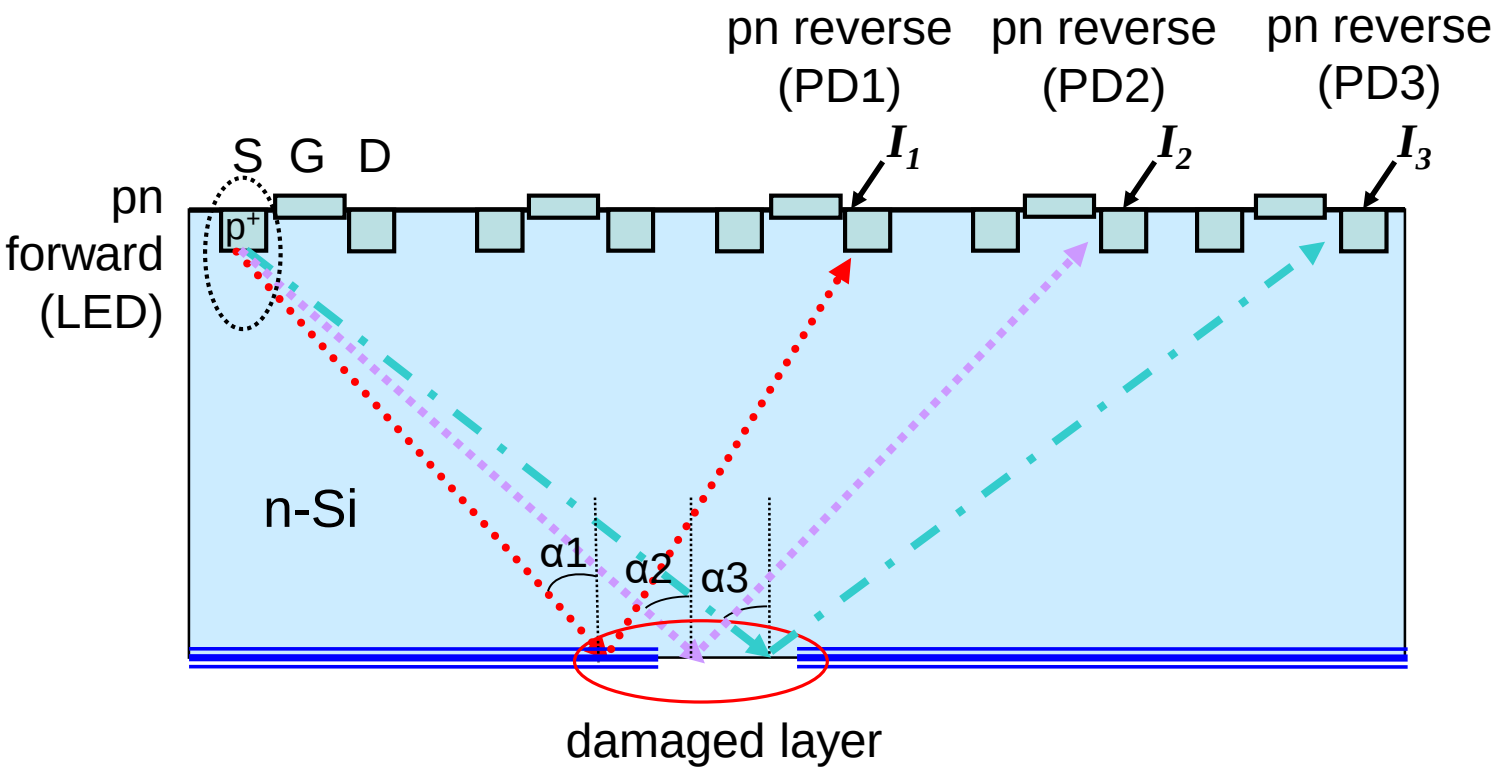
Backside Protection (NXP patent)



Detector	x (µm)	L (µm)	α (°)
PD1	360	420	25,2
PD2	780	544	45,7
PD3	1097	667	55,2
PD4	1766	884	64,5

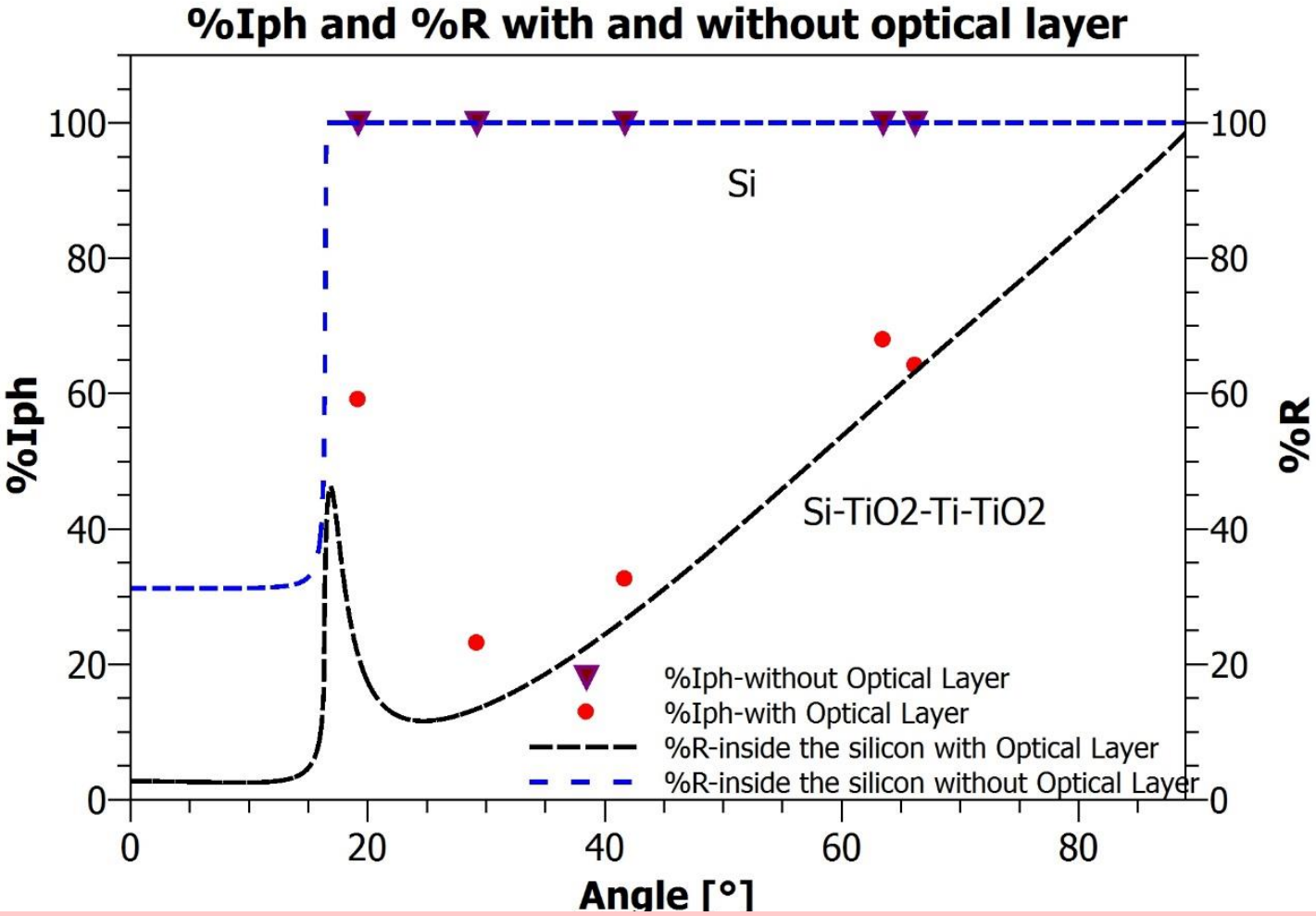
Cross section of the chip with locations of light source (LED) and detectors (PD). X is the lateral distance between LED and PD, d is the thickness of silicon and α is the angle of incidence.

Backside Protection (TU Berlin add on)



Cross section of chip protected by optically active layer and attack detection technique

Optically Active Layer for Backside Protection



Better light souces needed?

(laser souces originally for optical interconnect?)

Conclusion

Contactless Fault Isolation is essential in IC circuit development

Contactless = Physical Interaction (today: NIR optics)

IC Technology requires Backside Access: Beneficial to CFI

– and the Attacker !

IoT Roadmap: Nanoscale FinFET & Low Power

CFI will prevail: EOP Visible light sources, PE in > 0.5V

Backside E Beam Probing / FIB

CFI Attack Risk will not fade away with Nanoscale !

Backside Protection Mandatory in Future

A wizard is never late…nor is he early

He arrives precisely when he means to.

[The Lord of the Rings]

In A Nutshell

- Contactless signal tracking mandatory in IC development & FA
- Contactless signal tracking = Physical Interaction
- Today physical interaction needs to access through chip backside = optical techniques play major role
- Backside access allows to compare signal quantitatively = new level of precision in signal reconstruction
- When debug and FA can access each electronic information in IC, these techniques are an enormous risk for IC security attacks
- Challenge: Nanoscale Miniaturization
- The demand for contactless signal tracking in IC development will provide solutions throughout all coming technologies for debug and FA that will support the security attackers as well
- Progess to new technologies will not protect from CFI attack risk - but only a valid backside protection strategy