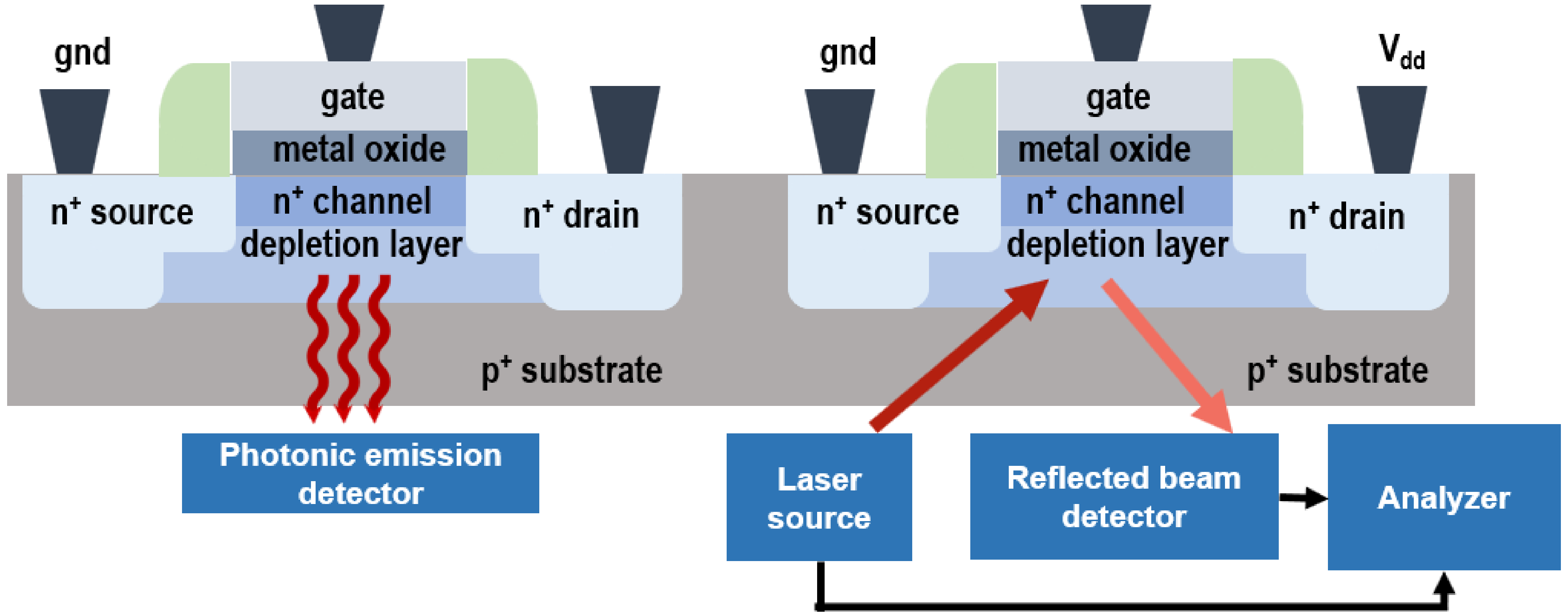
Optical Analysis of Integrated Circuits

Presented by: Mir Tanjidur Rahman
Dr. Navid Asadi

Physical Inspection and AttacKs on ElectronicS (PHIKS)

Optical Attacks/Inspection

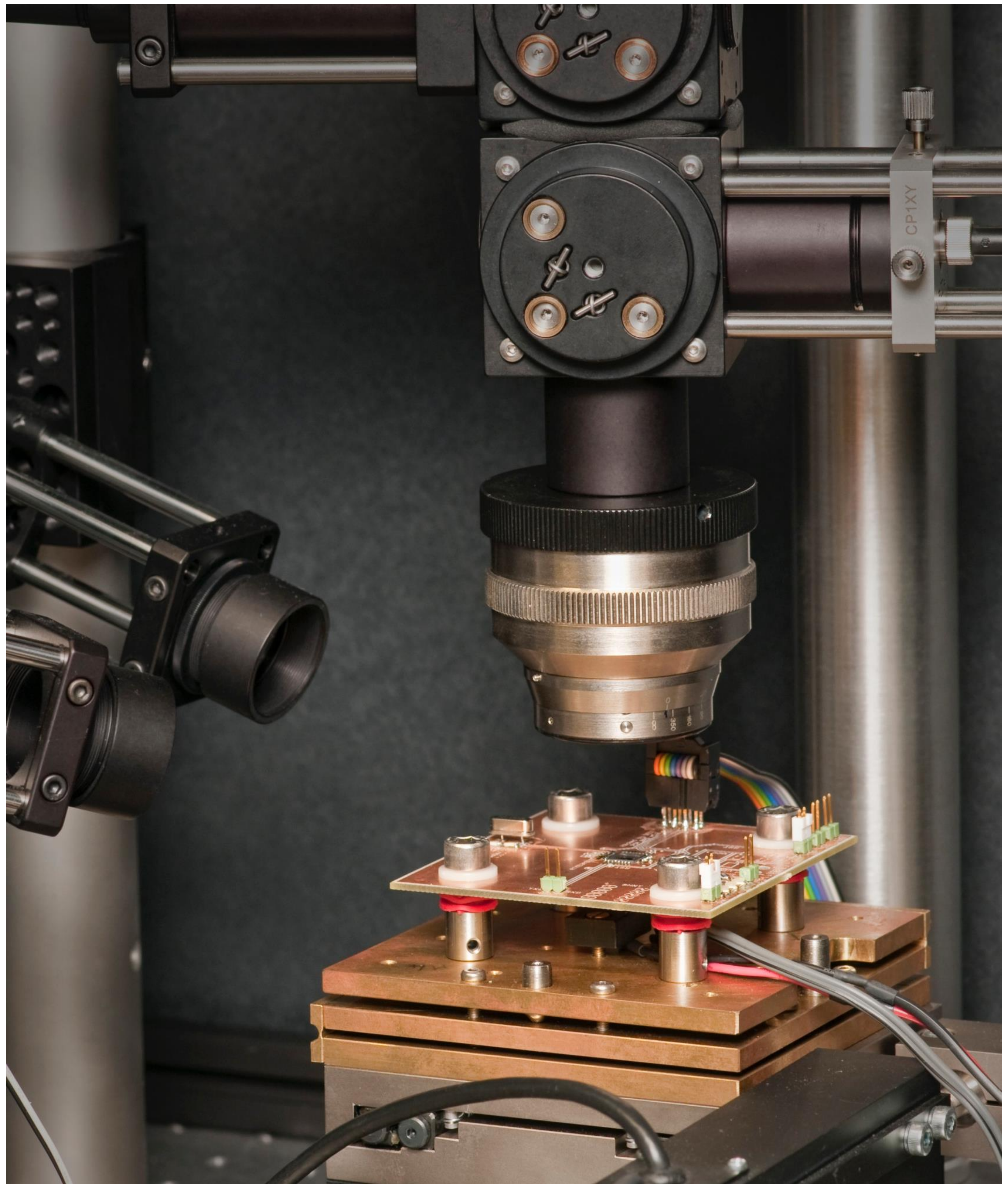
- Silicon is transparent to near infrared photons



- **Optical Inspection/Analysis**
  - **Photon Emission Analysis**
    - **Picosecond Circuit Analysis (PICA)**
  - **Laser Stimulation**
    - **Photoelectric Laser Stimulation ($\lambda<1.1\mu m$)**
      - **Laser Fault Injection**
    - **Thermal Laser Stimulation ($\lambda>1.1\mu m$)**
      - **Seebeck Effect Imaging (SEI)**
      - **Soft Defect Localization (SDL)**
      - **Resistive Interconnect Localization (RIL)**
      - **Optical Beam Induced Resistivity Change (OBIRCH)**
      - **Thermally Induce Voltage Alteration (TIVA)**
  - **Electro-optical Analysis**
    - **Electro-optical Frequency Mapping (EOFM) / Laser -Voltage Imaging (LVI)**
    - **Electro-optical Probing(EOP) / Laser Voltage Probing(LVP)**

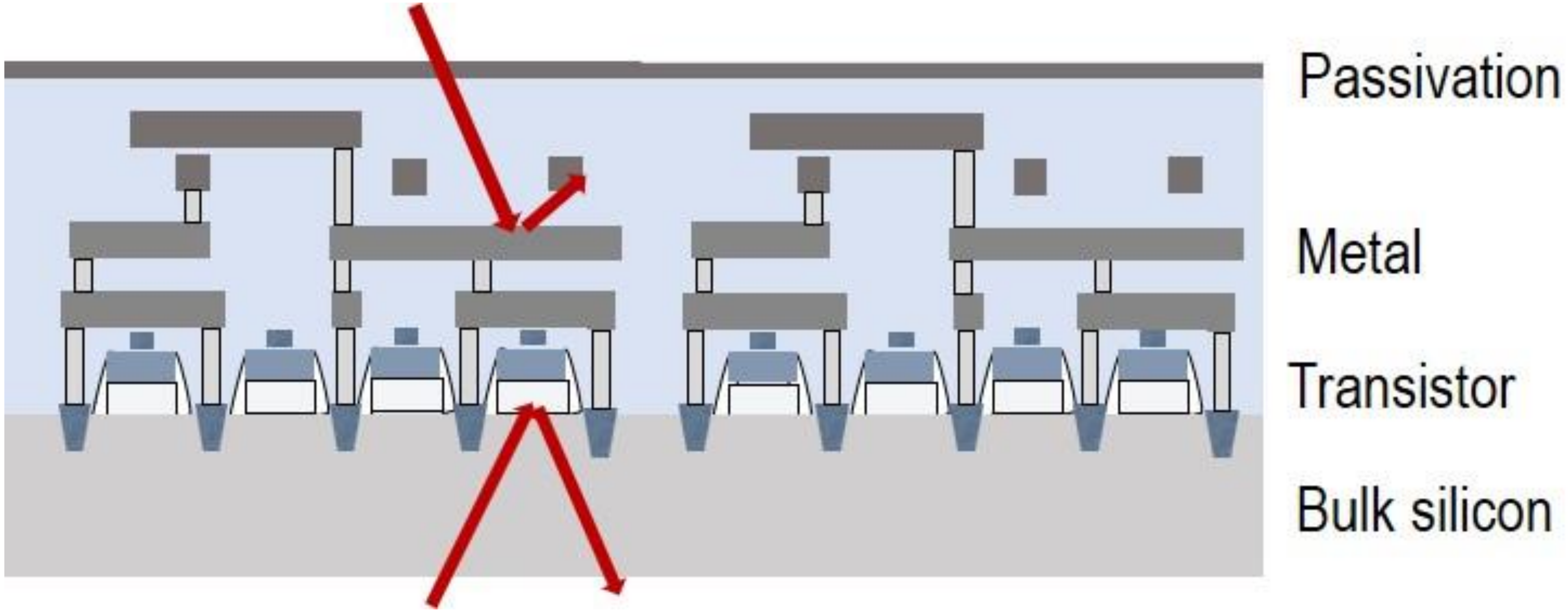
Semi-Invasive Optical Analysis

- Access to the surface of the chip without creating contacts with internal wires
- Optical interactions with transistors using known Failure Analysis (FA) tools
- Normally does not damage the system
- May or may not leave tamper evidence



IC Backside vs. IC Frontside

Frontside: Multiple interconnect layers obstruct the optical path to transistor devices

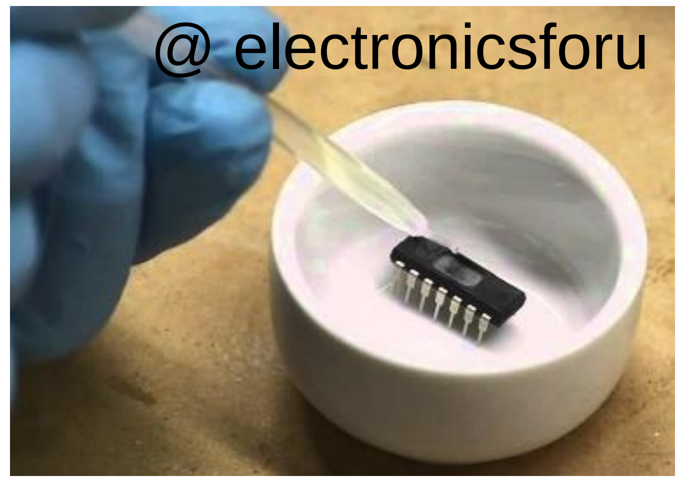


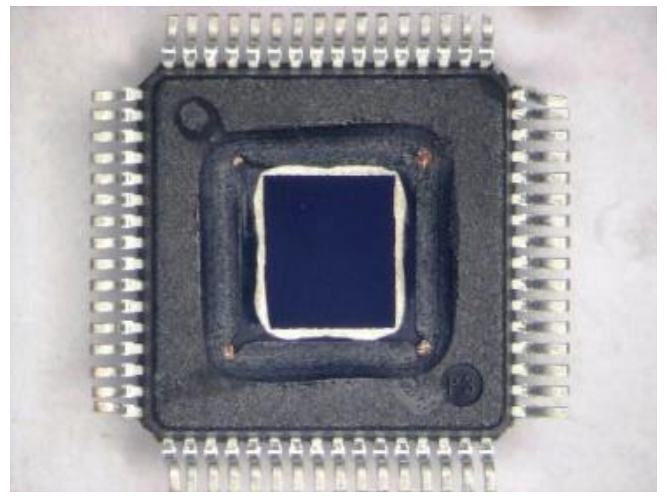
Backside: Active devices are directly accessible

Sample Preparation Step

optical inspection method and packaging style define sample prep steps

Chip backside exposing → **Polishing up to 10-30 um thickness** → **Backside coating (optional)**


@ electronicsforu



Non-flip chip → **Depacakging**
- Acid etching
- Polishing

→ **Die Backside Thinning***

Non-flip Chip→ accessible after depackaging and die backside polishing


@ PAINE 2019

Flip Chip on PCB

↓

Remove Heat Sink
- Hotplate
- knief

↓

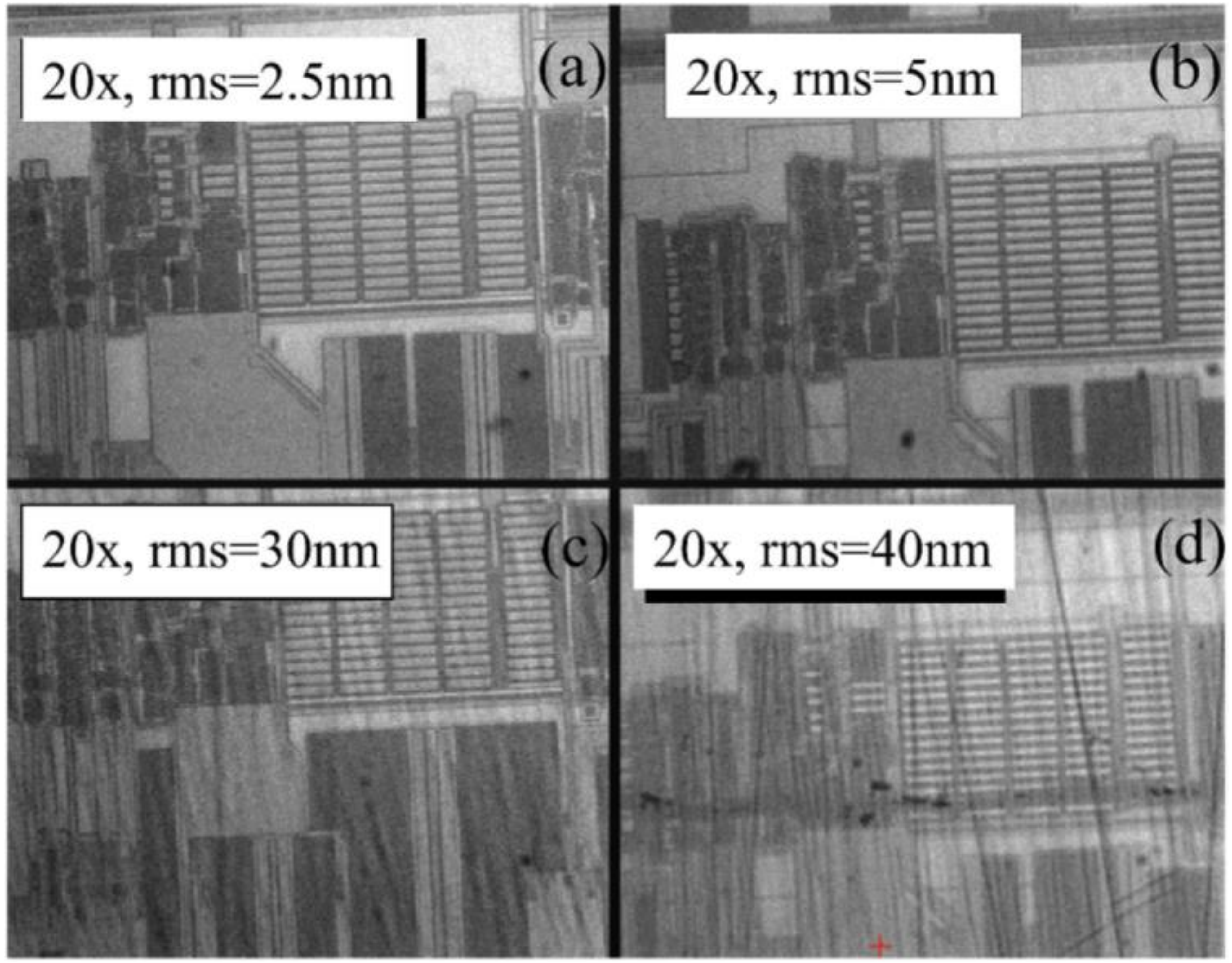
Die Backside Thinning*
- Selective polishing

Flip Chip→ bare die allows direct optical inspection of SoC implementation

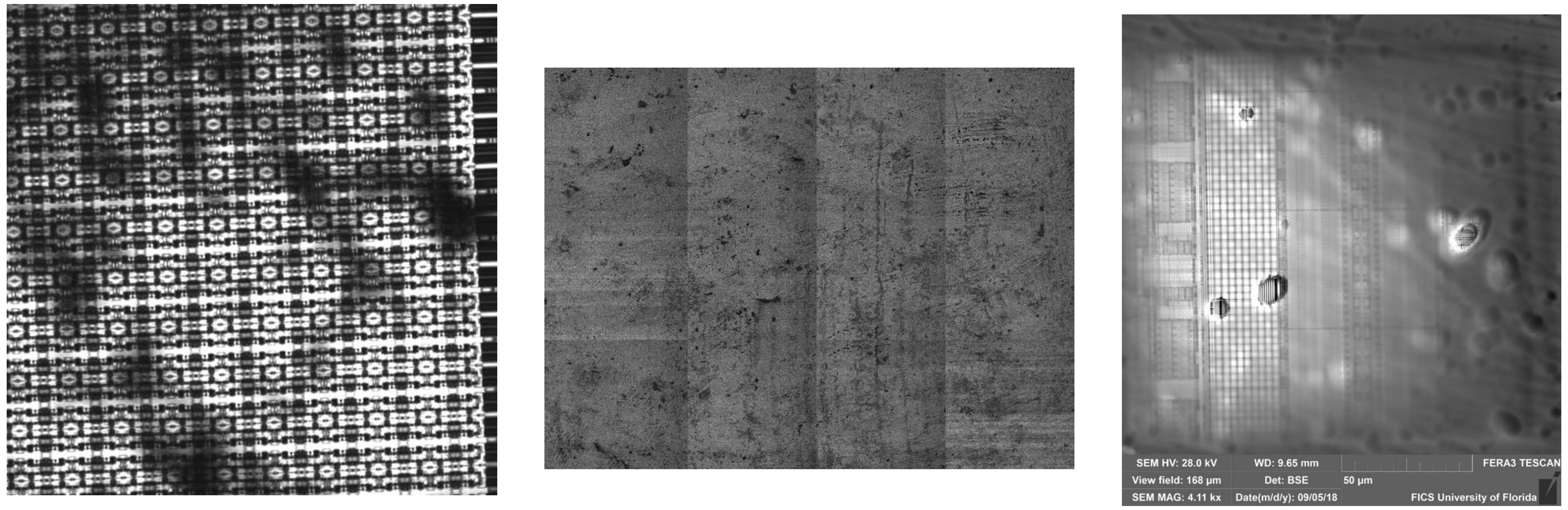
*Depends on microscope, lens capability and attack approach

Sample Preparation Challenges

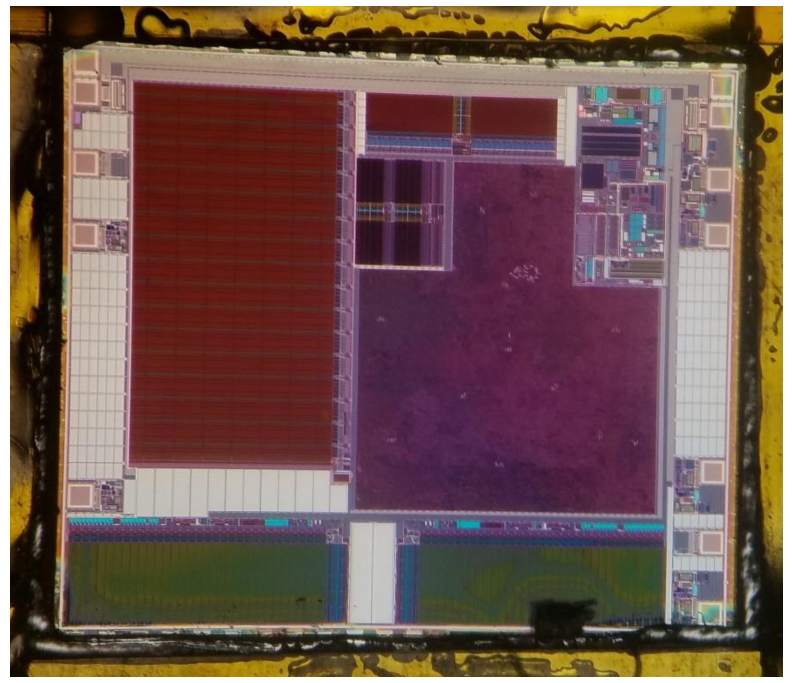
Smoothness of surface defines the quality of the imaging



Polishing aftermath: Surface roughness



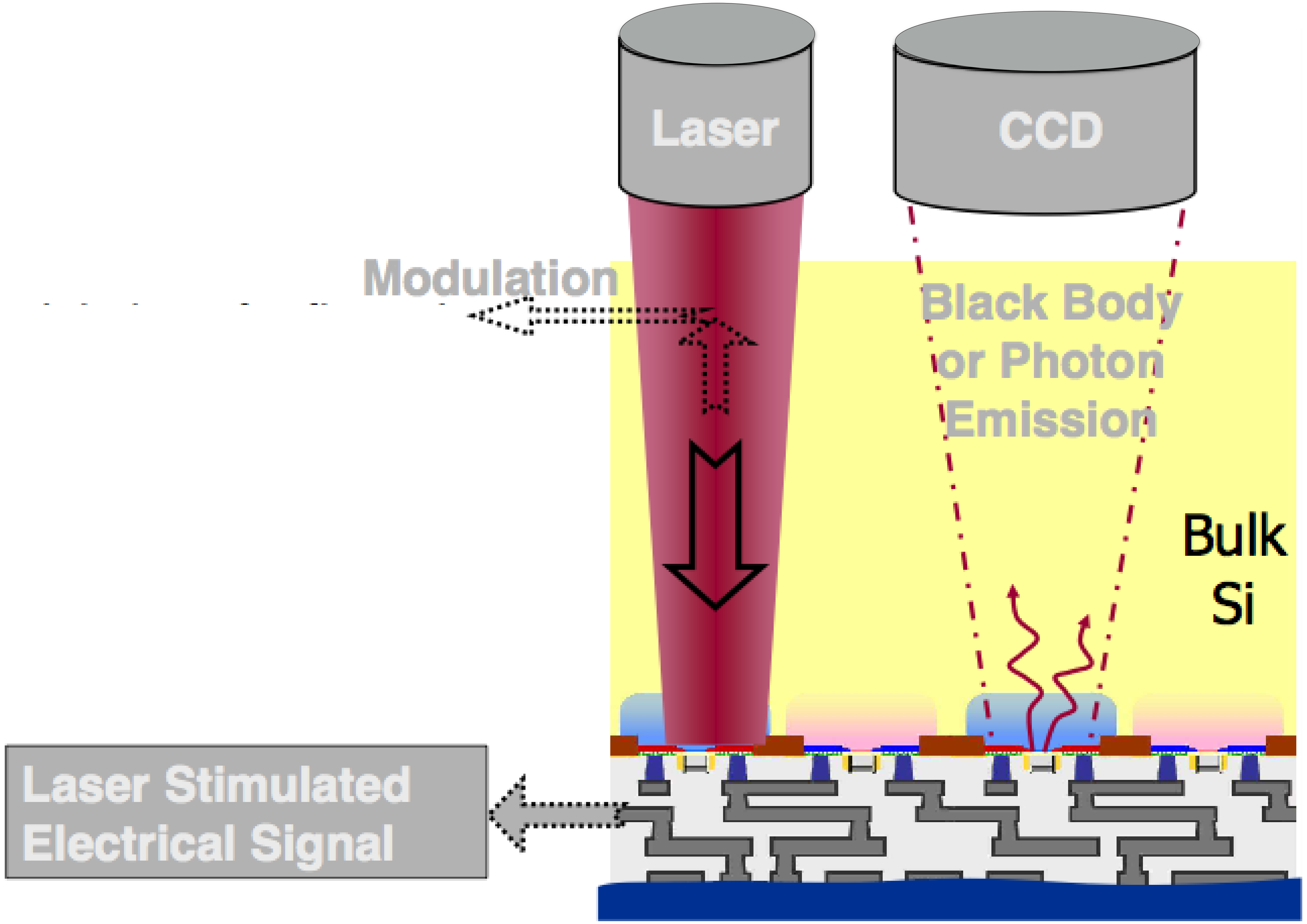
Polishing aftermath: Residue on surface



Plasma etch: Chip mostly dead/ impossible for chip connected to board

Optical Backside Analysis

- **Photon Emission**
- **Laser Stimulation/Fault Injection**
- **Optical Contactless Probing**



All Rights Reserved

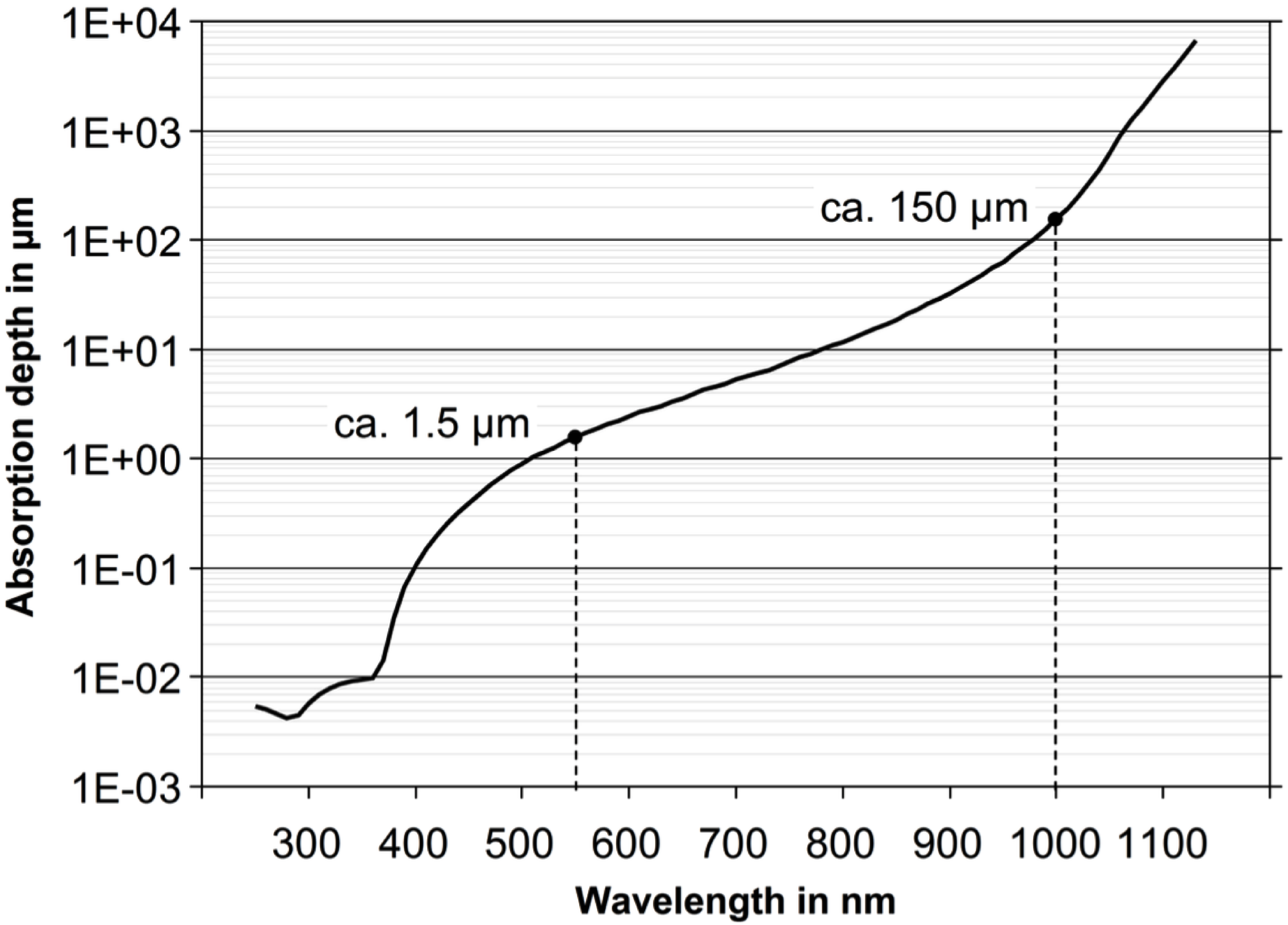
Equipement Examples

HAMAMATSU PHEMOS

SEMICAPS LTP 3000

Optical Resolution
And
Laser Spot Size

Absorption depth of silicon at 300K



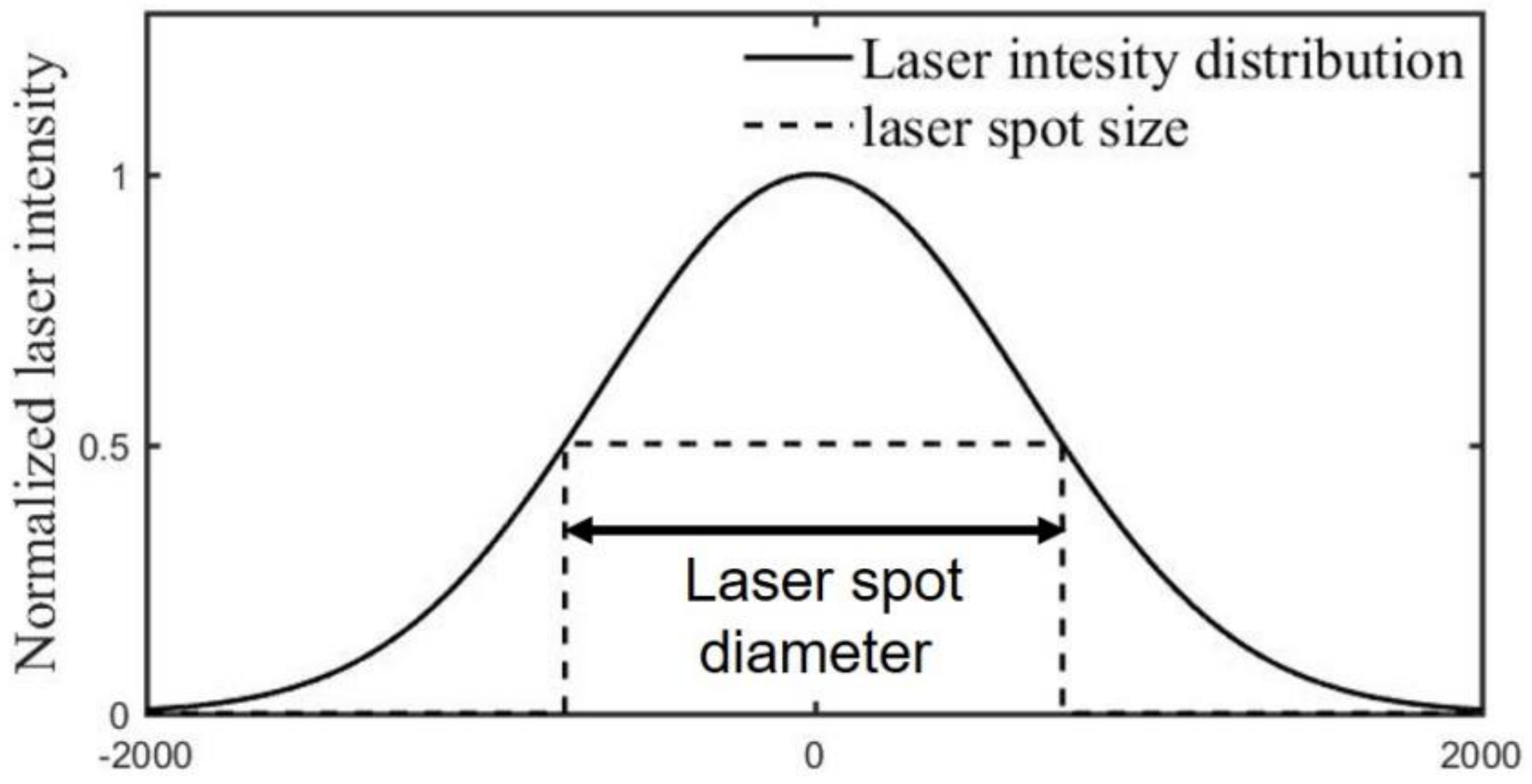
Near Infra Red (λ≈1µm+) ideal for backside access

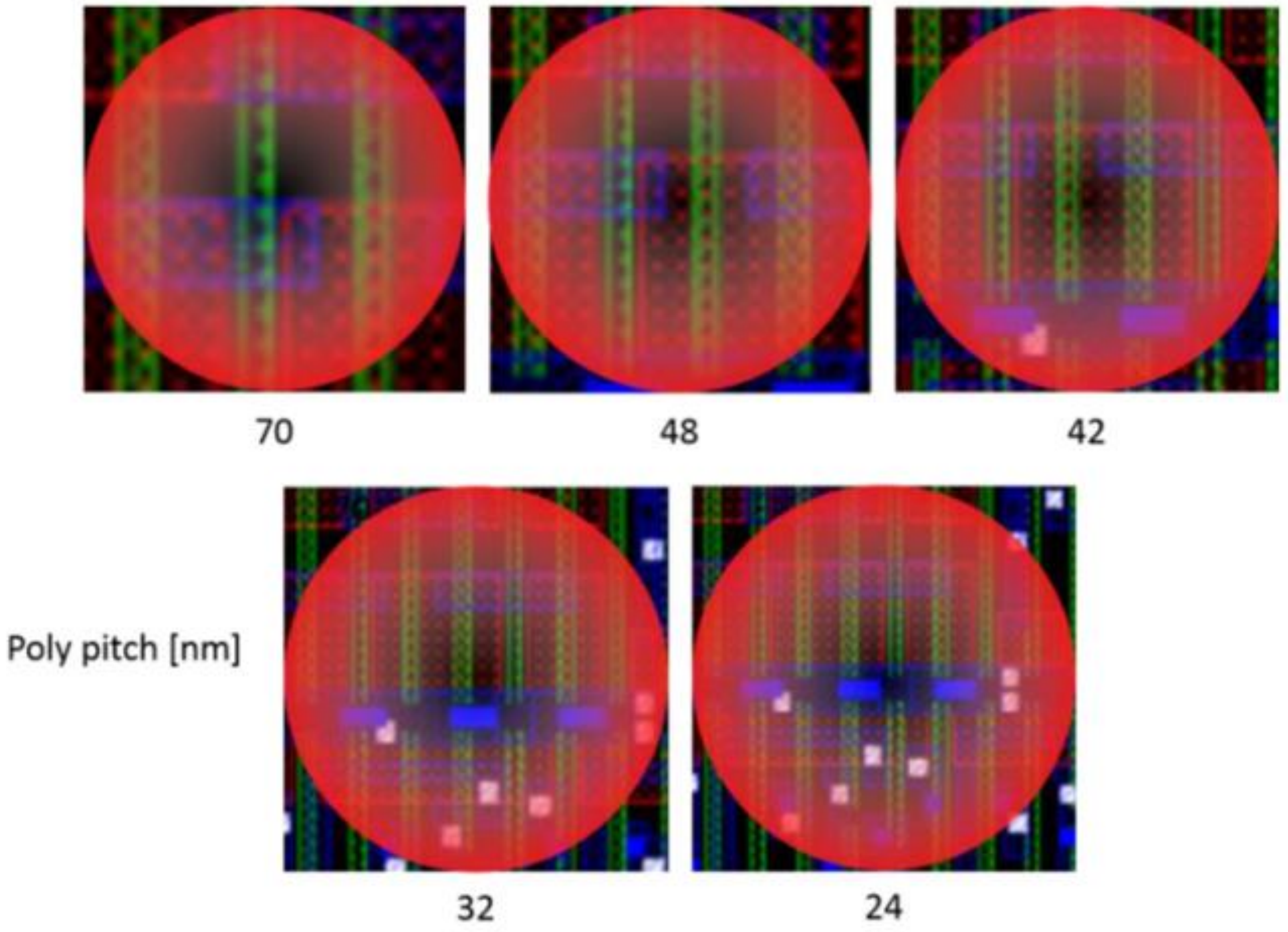
***R* ≈ *λ / (2 NA), NA:* Numerical Aperture (in air < 1)**

With λ≈1µm, *R* is at best around 500nm

Source: Boit, C., et al. "From IC debug to hardware security risk: The power of backside access and optical interaction." *Physical and Failure Analysis of Integrated Circuits (IPFA), 2016 IEEE 23rd International Symposium on the*. IEEE, 2016.

LASER SPOT SIZE



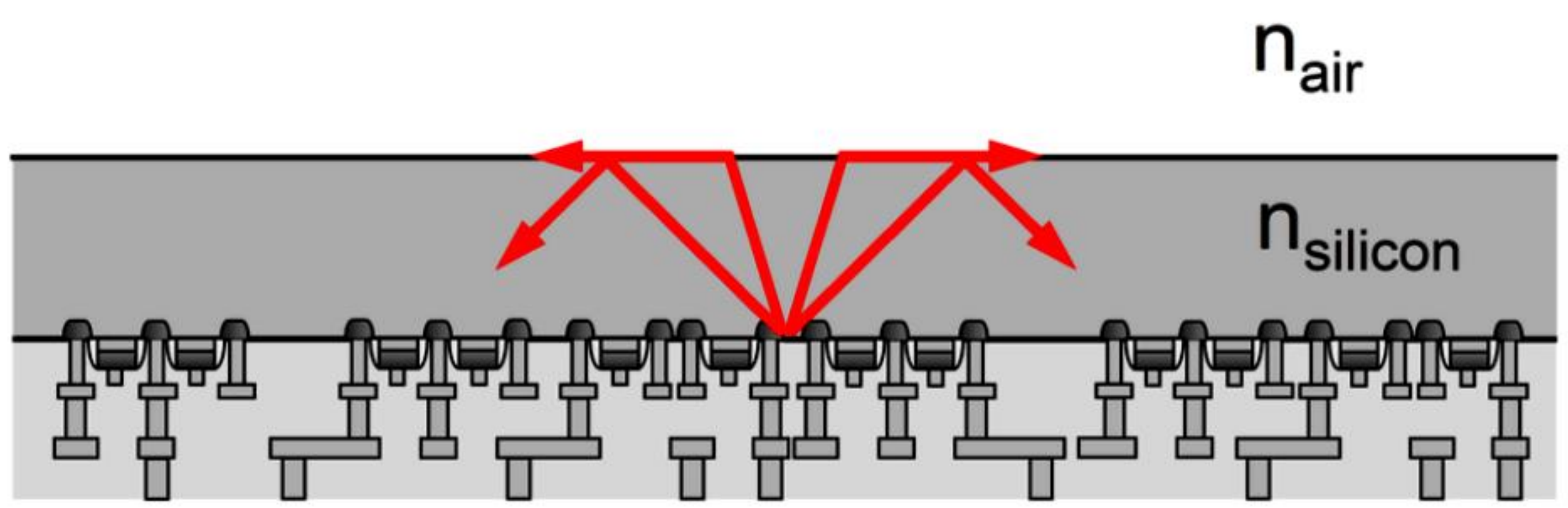


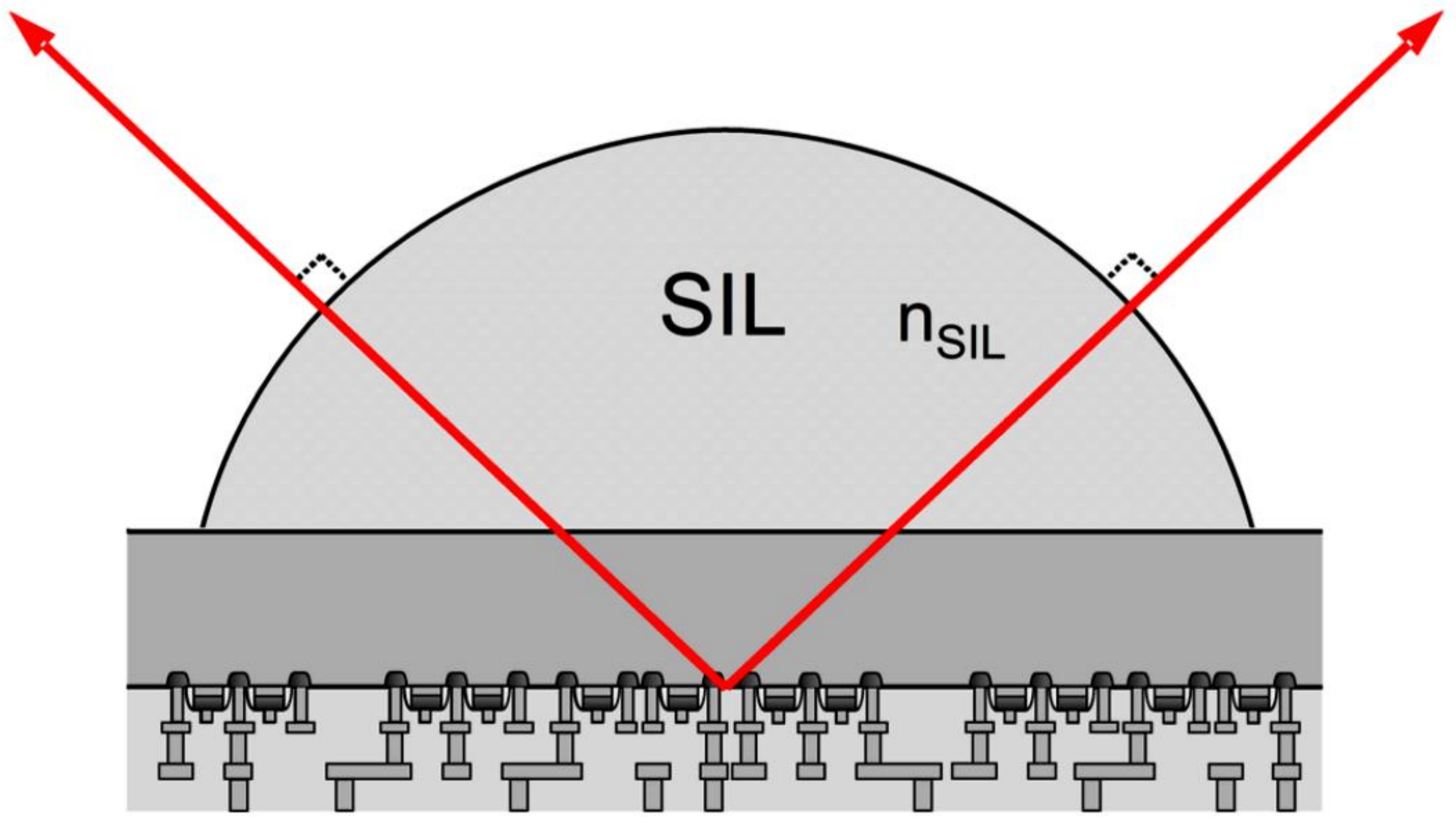
- **For any confocal microscope, spot diameter, D = 1.22λ / NA**
- **Follows Gaussian distribution**
- **Spot size is defined at full width at half maximum of intensity**
- **Defines the sharpness of the edges, effect of laser stimulation on neighbor cells**

lens	Numerical Aperture (NA)	Optical Resolution (nm)		Laser Spot Size (nm)	
		λ = 1300 nm	λ = 1064 nm	λ = 1300 nm	λ = 1064 nm
20x	0.40	1625	1330	2803	2295
50x	0.76/1	855/650	700/532	1476/1121	1208/918

Solid Immersion Lens (SIL)

- A Introducing immersion, namely a spherical solid immersion lens (SIL) on back surface. Optical Resolution, $R \approx \lambda / (2n\,NA)$
- NA is increased by the index of refraction n_{SIL}. For silicon and $\lambda = 1$ µm, n is 3.5, resulting in a maximum R of around 150 nm.

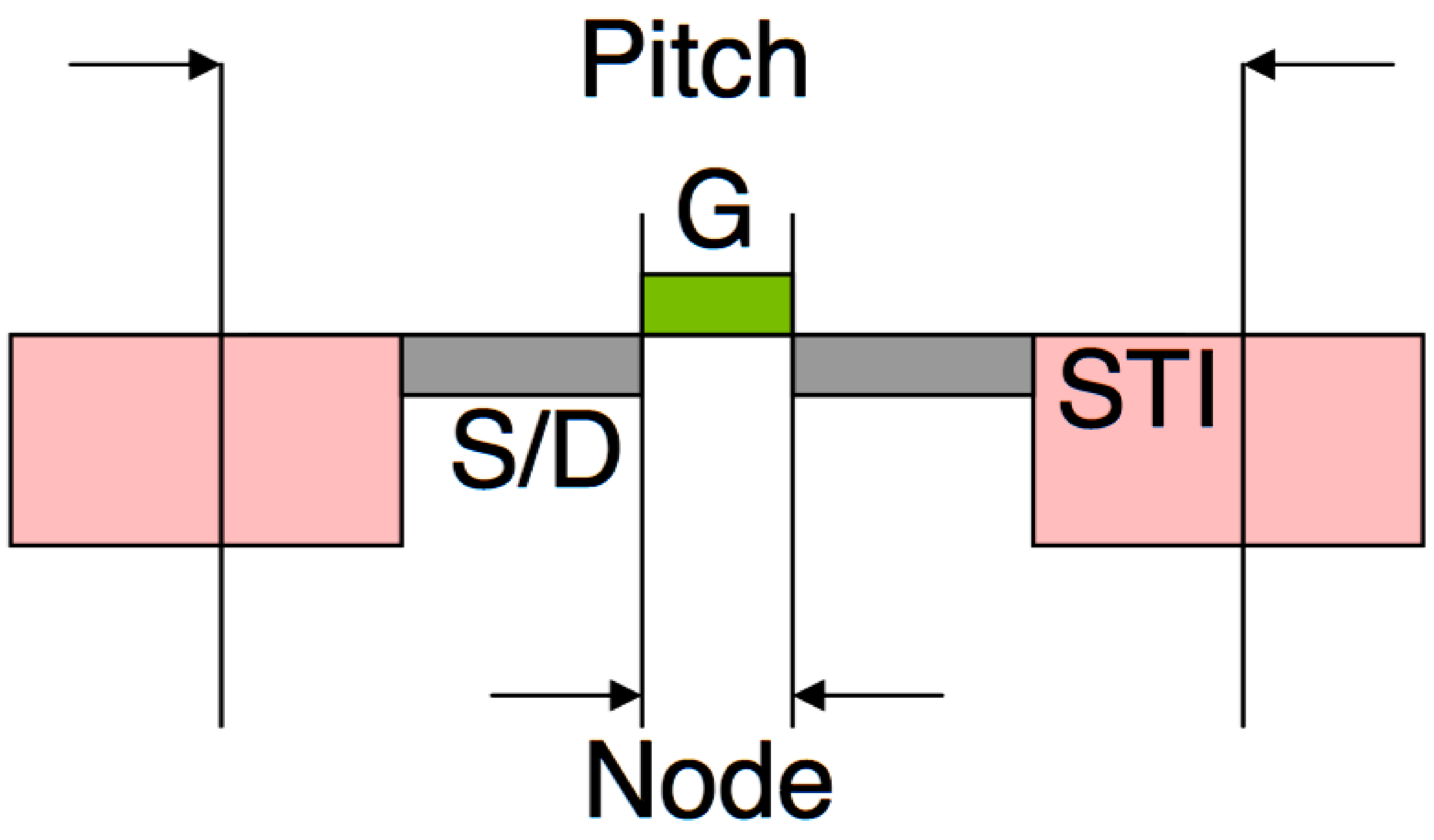




What is the required Resolution?

- NIR + Si SIL resolution ca 100-120nm
- D&D requires to resolve pitch
- Pitch ca 3.5-8x min. feature size
- NIR good for > 20nm node technologies

➢ But: there is some tolerance



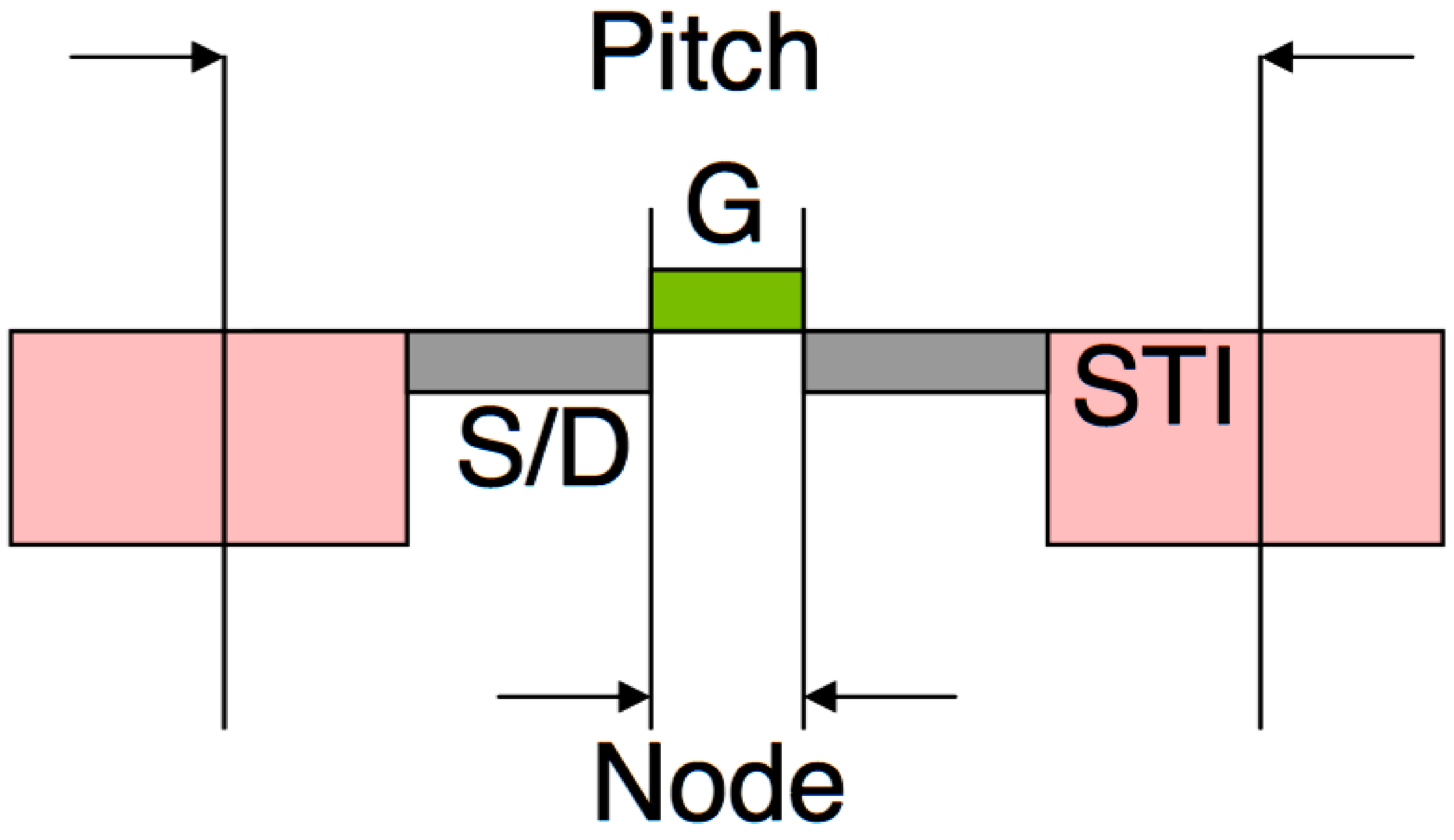
ITRS:

Tech Node	Pitch	Year
45nm	160nm	2007
32nm	112nm	2009
22nm	90nm	2011
14nm	70nm	2013

What is the required Resolution?

- NIR + Si SIL resolution ca 100-120nm
- D&D requires to resolve pitch
- Pitch ca 3.5-8x min. feature size
- NIR good for > 20nm node technologies

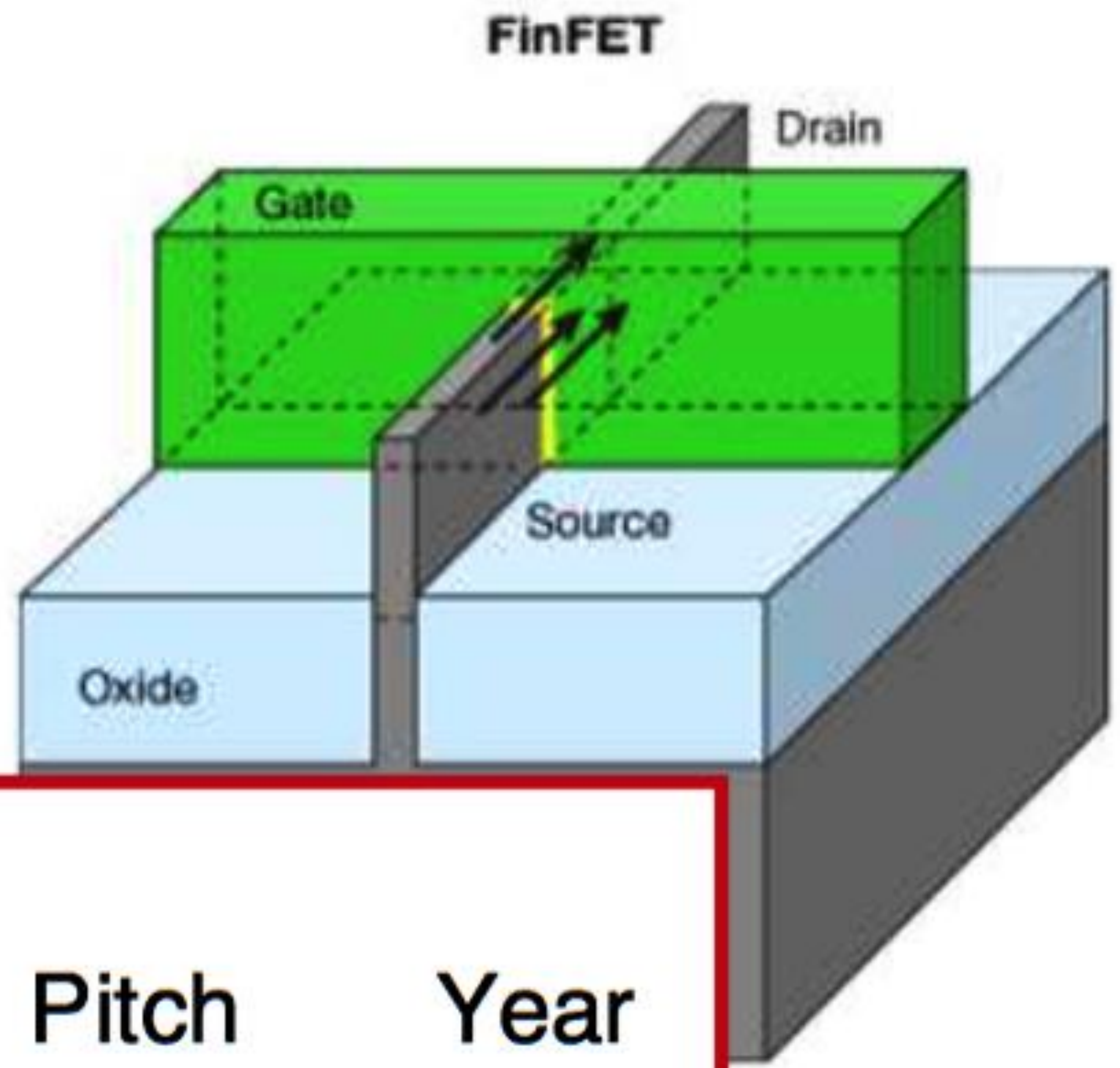
➢But: there is some tolerance



ITRS:

Tech Node	Pitch	Year
45nm	160nm	2007
32nm	112nm	2009
22nm	90nm	2011
14nm	70nm	2013

What is the required Resolution in FinFET age?



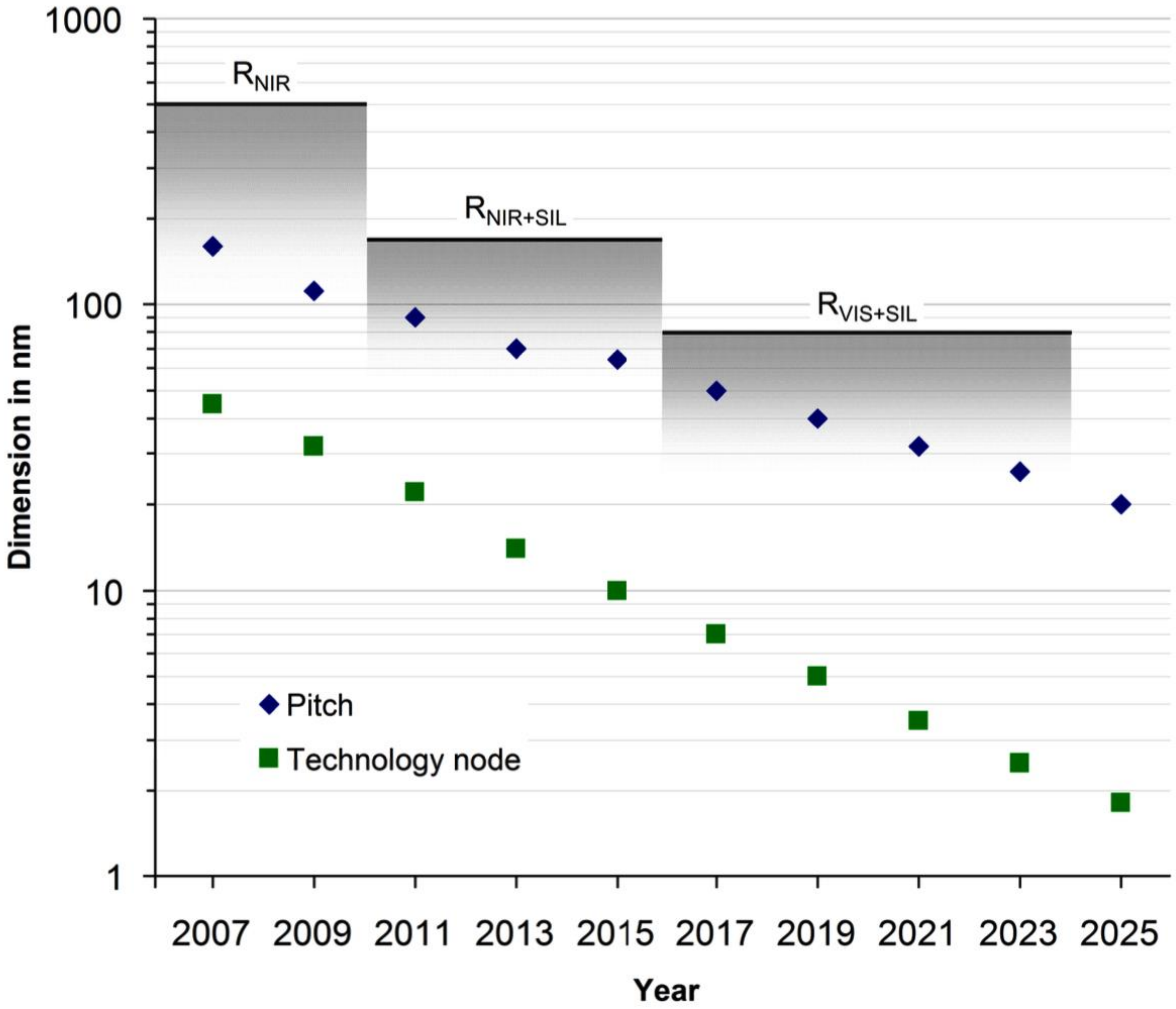
- NIR + Si SIL resolution ca 100-120nm
- D & D requires to resolve pitch
- Good for > 20nm node tech
- For FinFETs, min 2x improvement necessary

ITRS 2013:

Tech Node	Pitch	Year
16nm	80nm	2013
10nm	64nm	2015
7nm	50nm	2017
5nm	40nm	2019
3.5nm	32nm	2021
2.5nm	26nm	2023
1.8nm	20nm	2025

Image: https://www.synopsys.com/Company/Publications/DWTB/PublishingImages/dwtb-finfet-jan2013-fig2.JPG

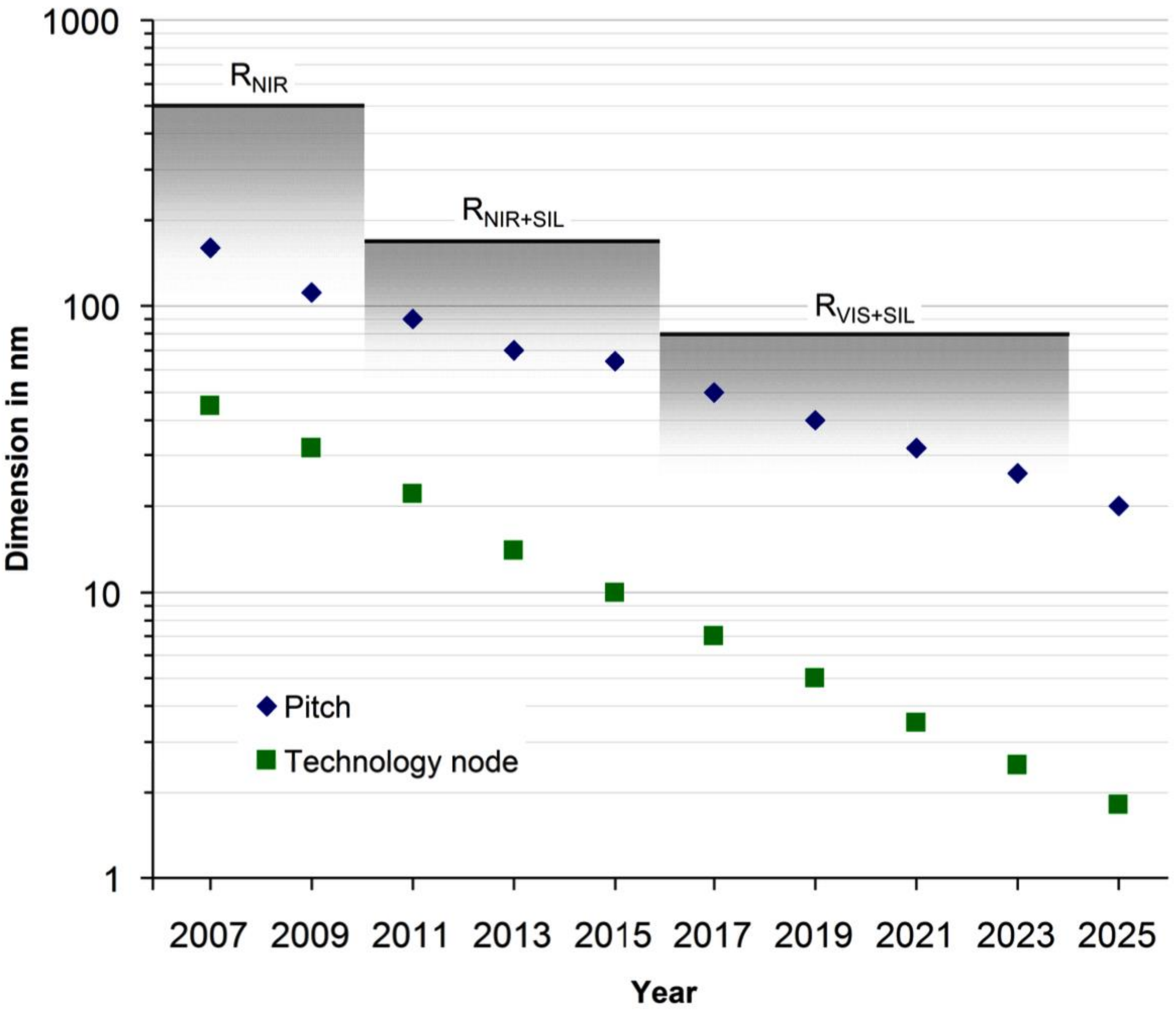
Pitch vs. Node Technology

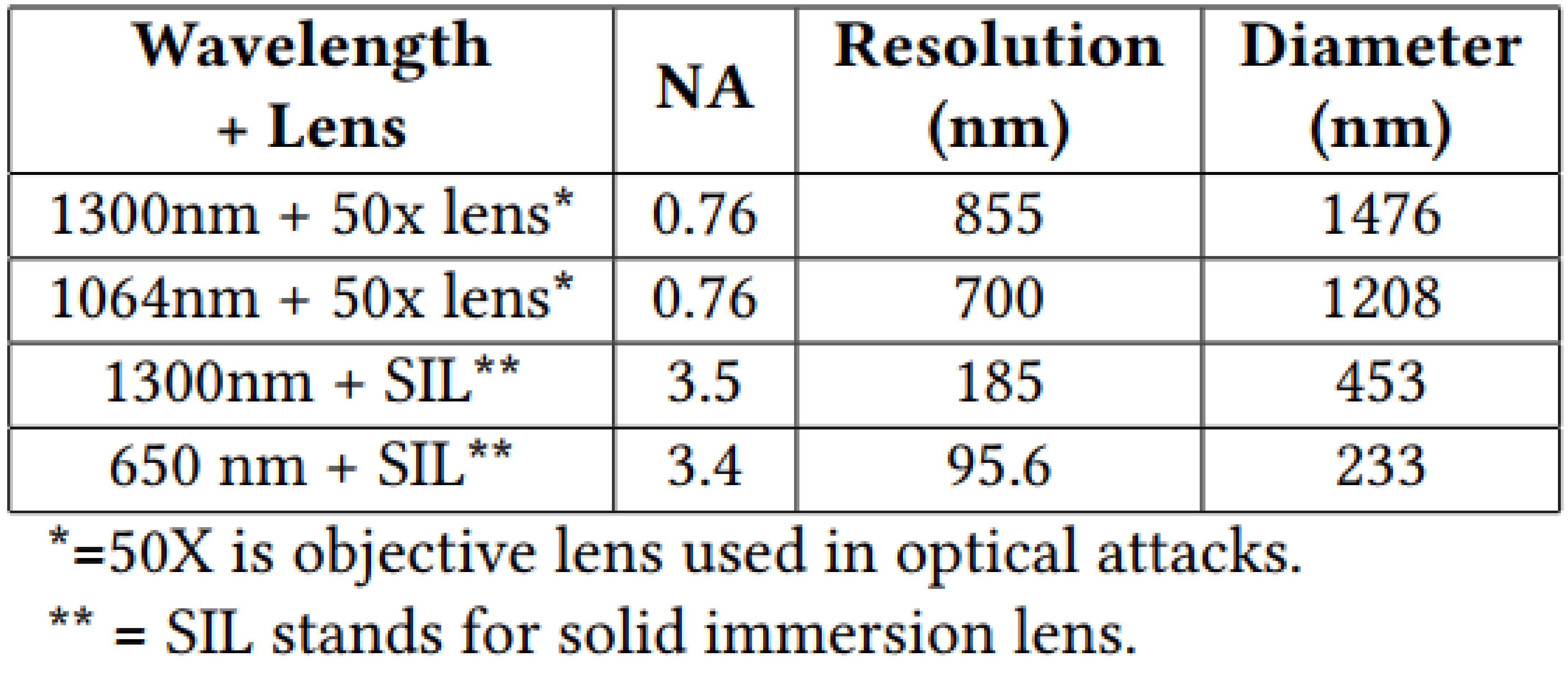


- **The only solution is the reduction of λ, *R ≈ λ / (2 NA)***
- **Lasers ~ 650nm available**
- **But the silicon has to be polished to 10 µm to be transparent for visible light**
- **Currently not available on many optical equipment**

Source: Boit, C., et al. "From IC debug to hardware security risk: The power of backside access and optical interaction." *Physical and Failure Analysis of Integrated Circuits (IPFA), 2016 IEEE 23rd International Symposium on the*. IEEE, 2016.

Pitch vs. Node Technology: Comparison for SIL

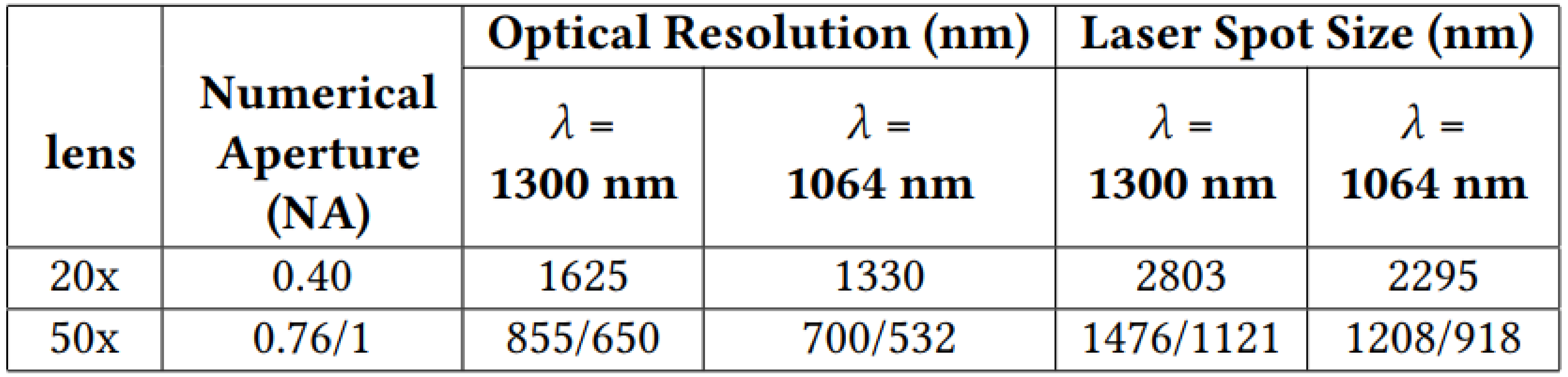




Wavelength + Lens	NA	Resolution (nm)	Diameter (nm)
1300nm + 50x lens*	0.76	855	1476
1064nm + 50x lens*	0.76	700	1208
1300nm + SIL**	3.5	185	453
650 nm + SIL**	3.4	95.6	233

*=50X is objective lens used in optical attacks.

** = SIL stands for solid immersion lens.

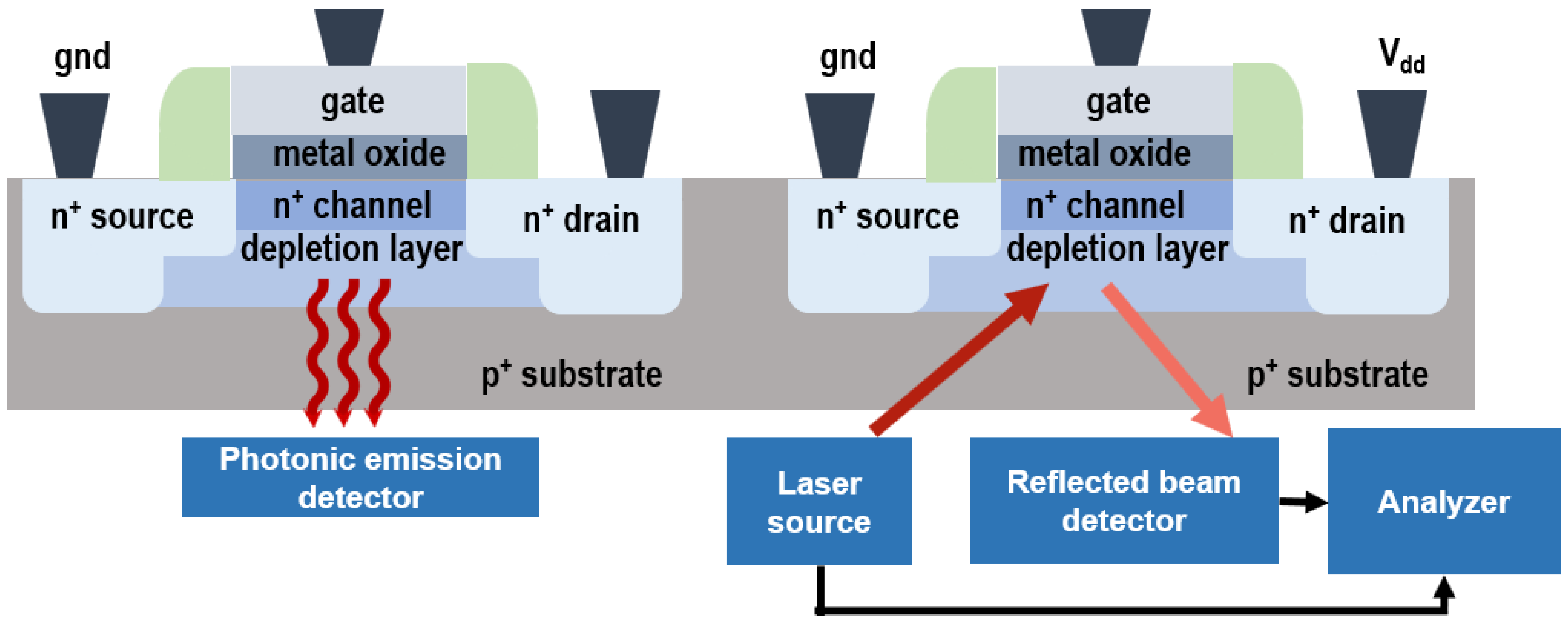


lens	Numerical Aperture (NA)	Optical Resolution (nm)		Laser Spot Size (nm)	
		λ = 1300 nm	λ = 1064 nm	λ = 1300 nm	λ = 1064 nm
20x	0.40	1625	1330	2803	2295
50x	0.76/1	855/650	700/532	1476/1121	1208/918

Optical Inspection/Attack

Optical Attacks/Inspection Taxonomy

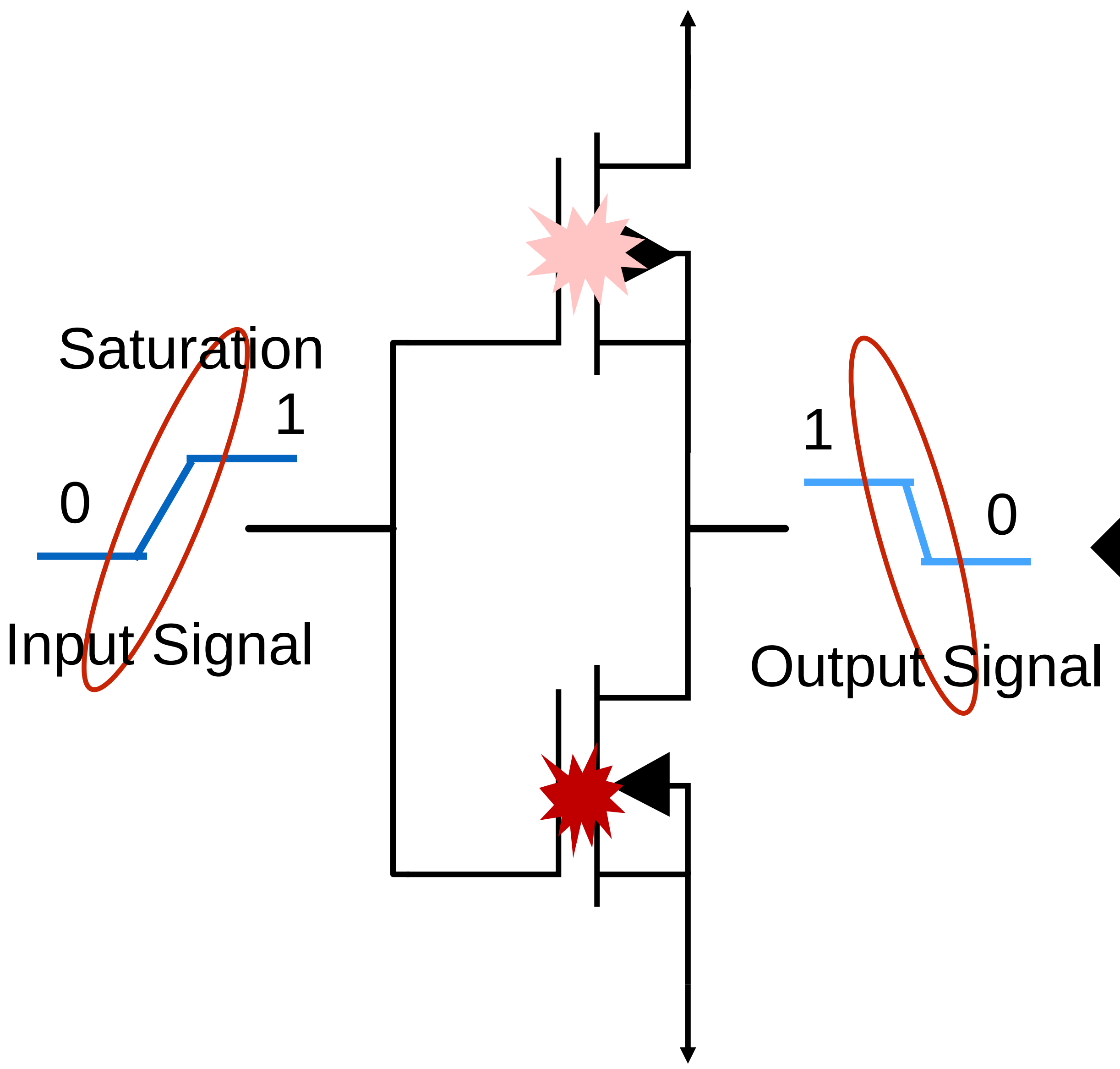
- The taxonomy is defined by the active and passive inspection method.



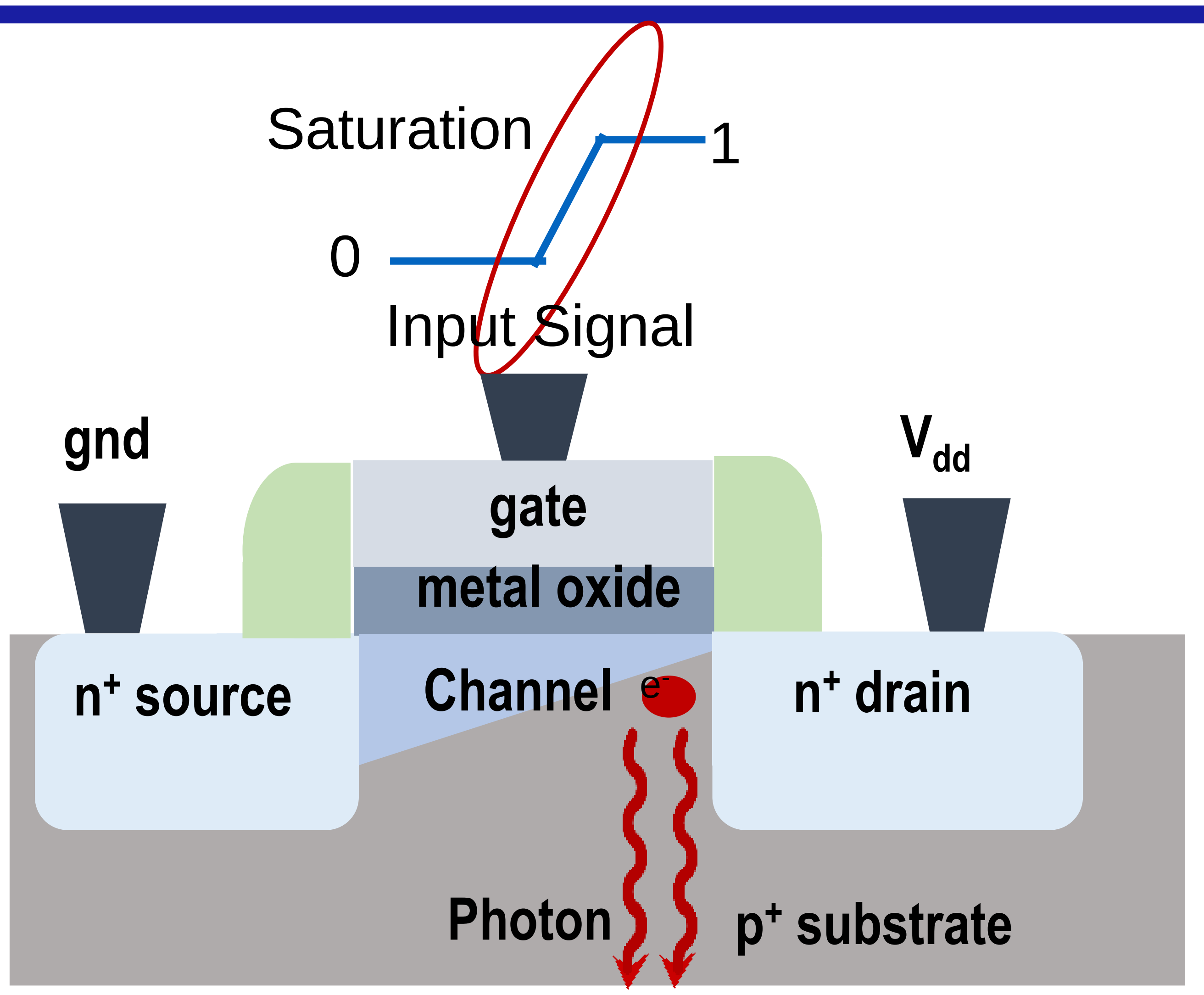
Optical Inspection/Analysis
- **Photon Emission Analysis**
  - **Picosecond Circuit Analysis (PICA)**
- **Laser Stimulation**
  - **Photoelectric Laser Stimulation (λ<1.1μm)**
    - **Laser Fault Injection**
  - **Thermal Laser Stimulation (λ>1.1μm)**
    - **Seebeck Effect Imaging (SEI)**
    - **Soft Defect Localization (SDL)**
    - **Resistive Interconnect Localization (RIL)**
    - **Optical Beam Induced Resistivity Change (OBIRCH)**
    - **Thermally Induce Voltage Alteration (TIVA)**
- **Electro-optical Analysis**
  - **Electro-optical Frequency Mapping (EOFM) / Laser -Voltage Imaging (LVI)**
  - **Electro-optical Probing(EOP) / Laser Voltage Probing(LVP)**

Photon Emission Analysis

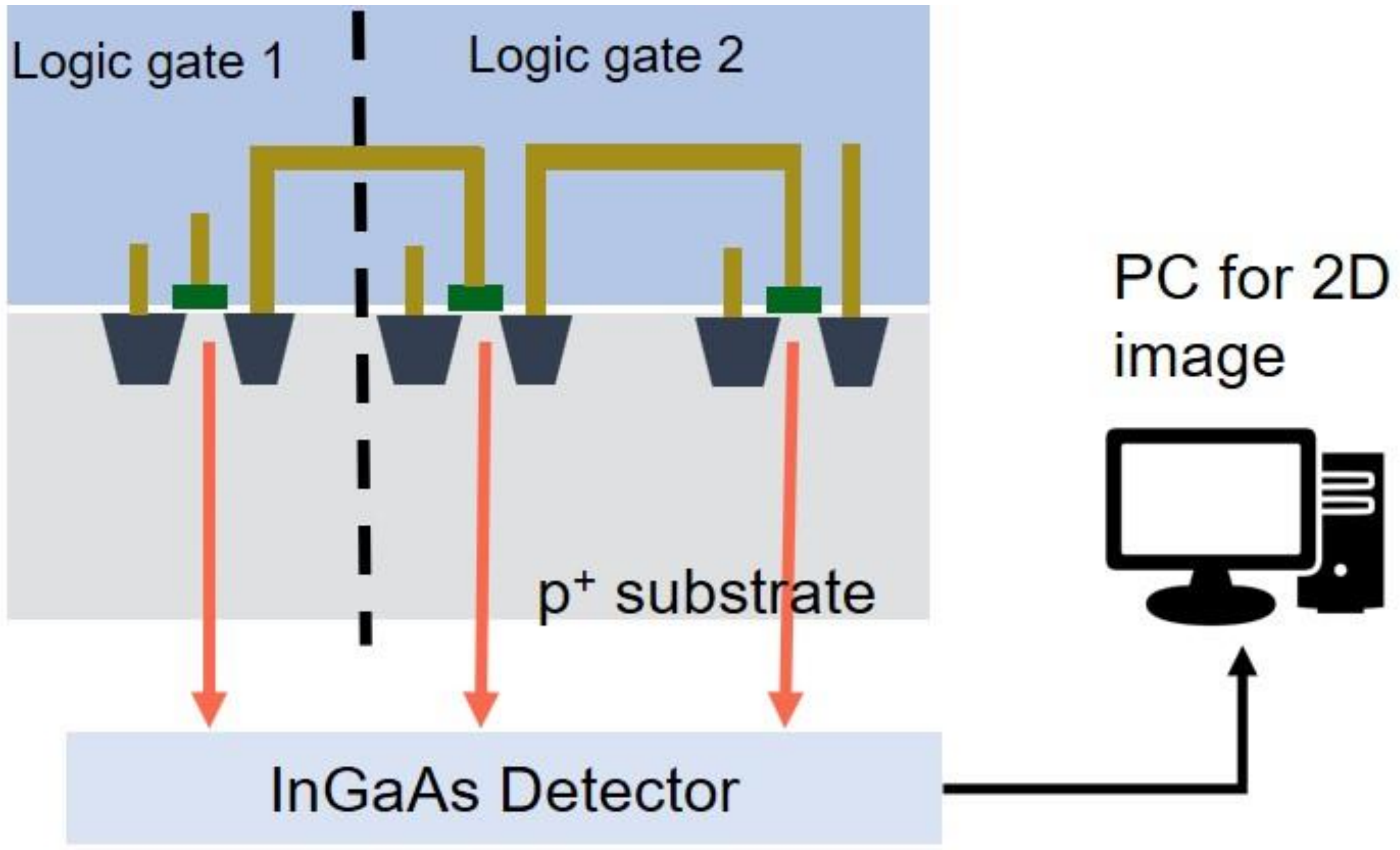
Photon Emission Analysis (PEA)



Circuit level (Inverter)
activity in the chip



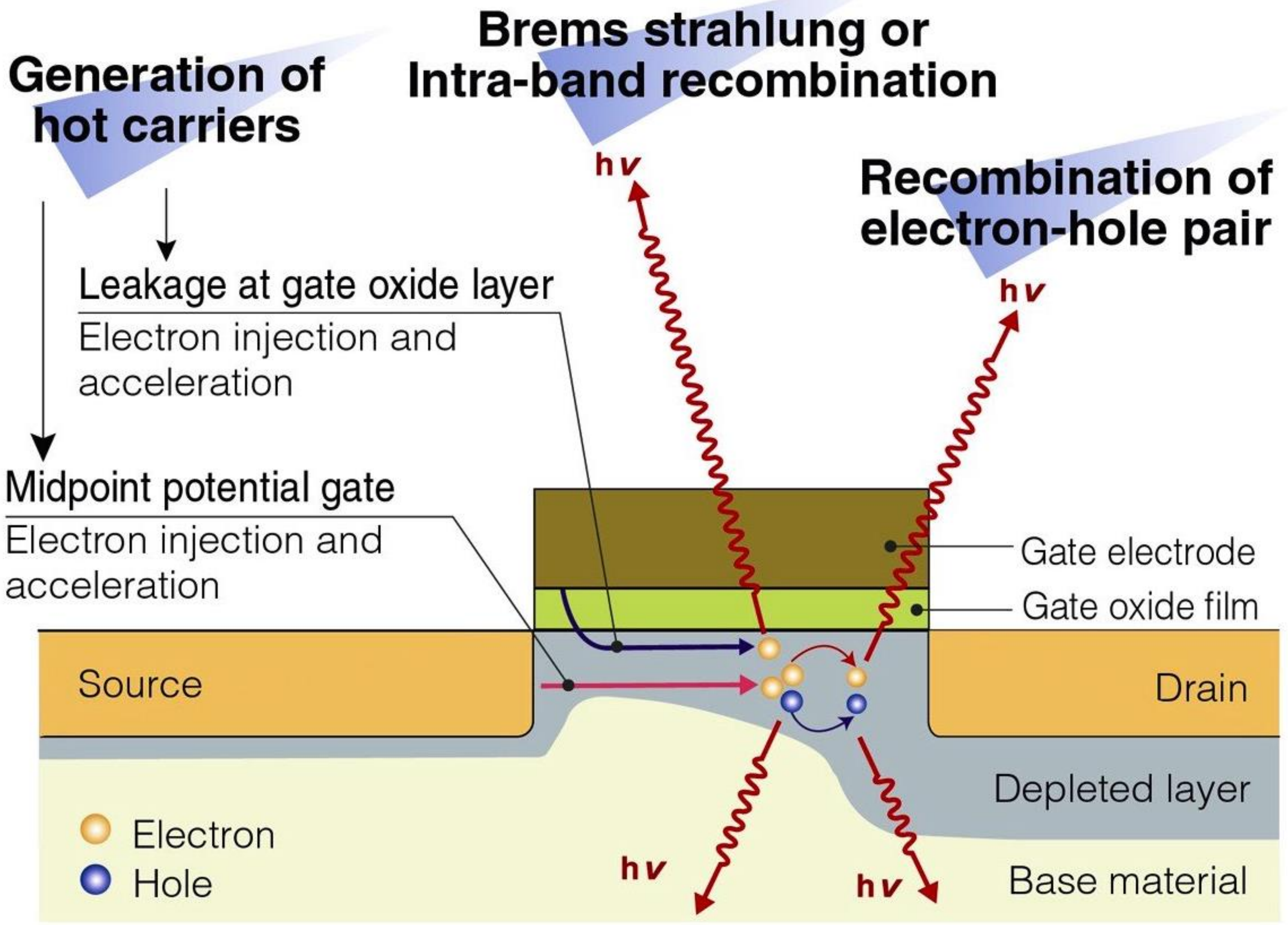
Device level (N-MOSFET)
activity in the SoC

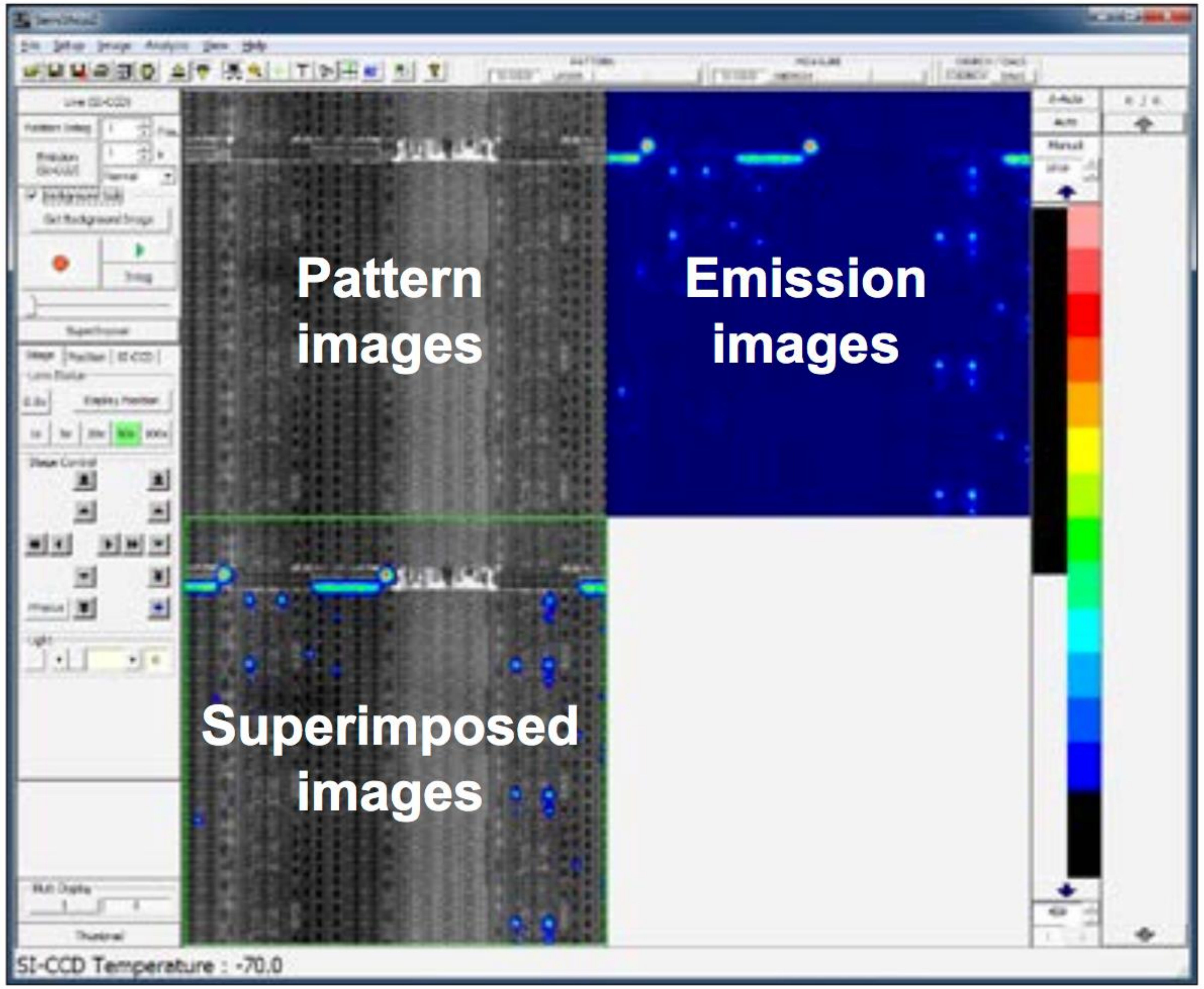


The 2D image generation

- Photons with higher kinetic energy emits photons
- Photons from N-MOSFET >> photons from P-MOSFET
- 2-D mapping image of photons captured by InGaAs detector generated

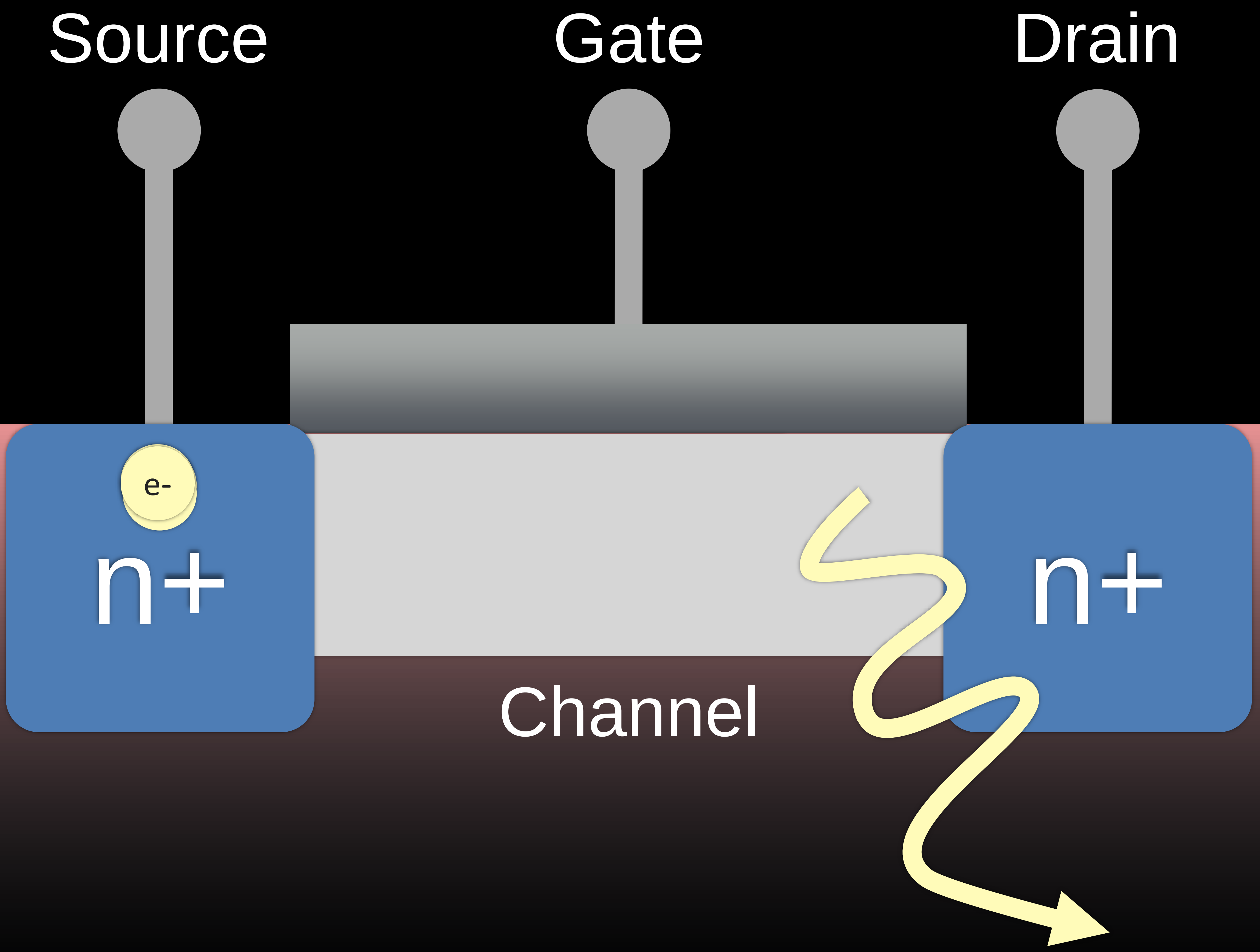
Mechanism of Photon Emission





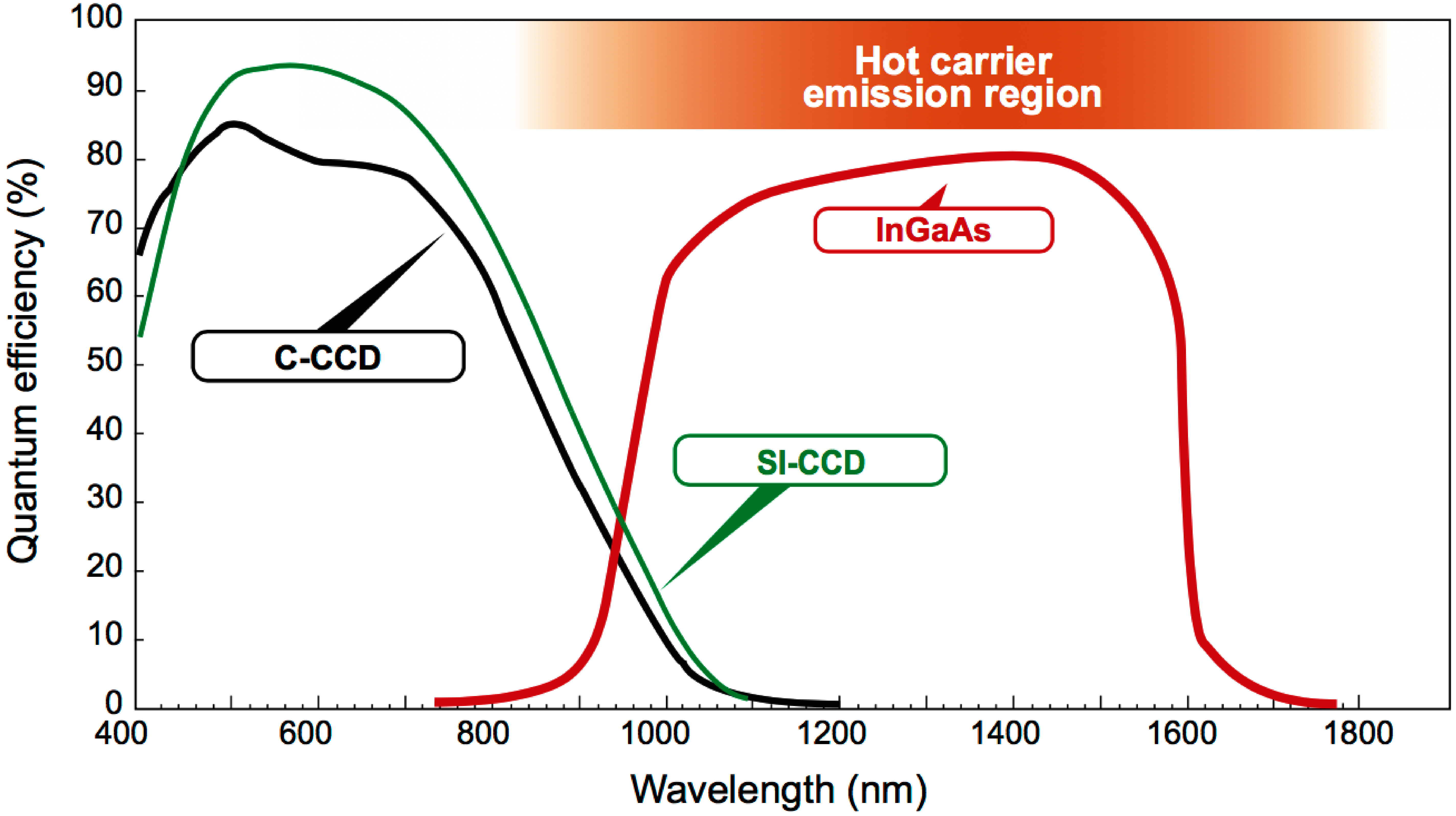
SI-CCD Temperature : -70.0

Bremsstrahlung (Braking Radiation)



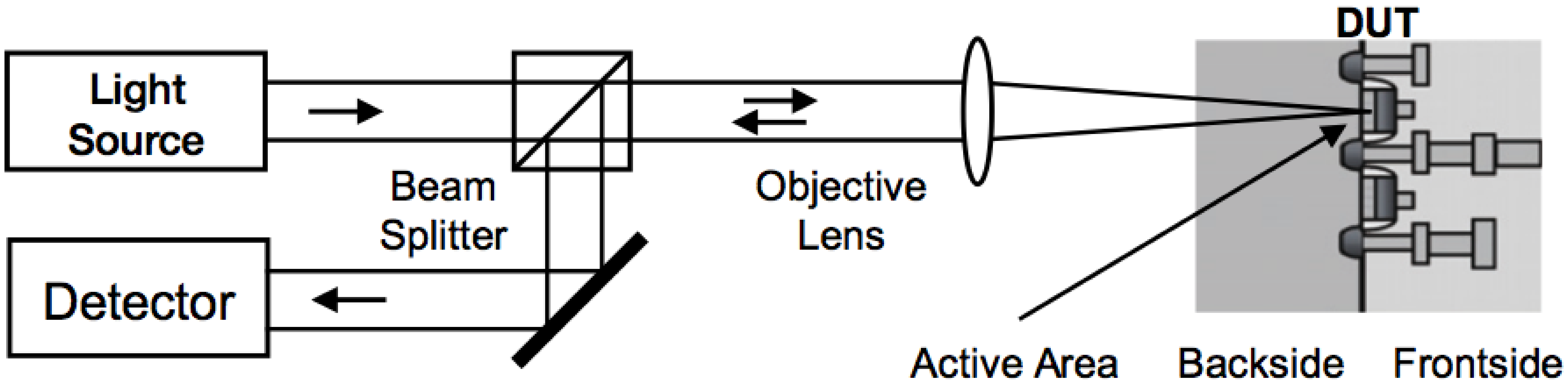
A comparative Chart of Wavelength Sensitivity Ranges

- Due to ultra-miniaturization, semiconductor devices now have lower operating voltages
- The light intensity emitted from transistors becomes weak (E α V) and also cause light emissions to occur at longer wavelengths (E α 1/λ).
- To detect such weak light emissions, a detector with high sensitivity in the near-infrared range longer than 900 nm is required.



Optical Contactless Probing

Optical Contactless Probing



- **Changes in the absorption coefficient and the refractive index of device in active area by electrical field and current.**

- **Electro-Optical Probing (EOP)** or **Laser Voltage Probing (LVP):** Optical beam intensity altered by voltage/current —> probing of electrical signals on the node

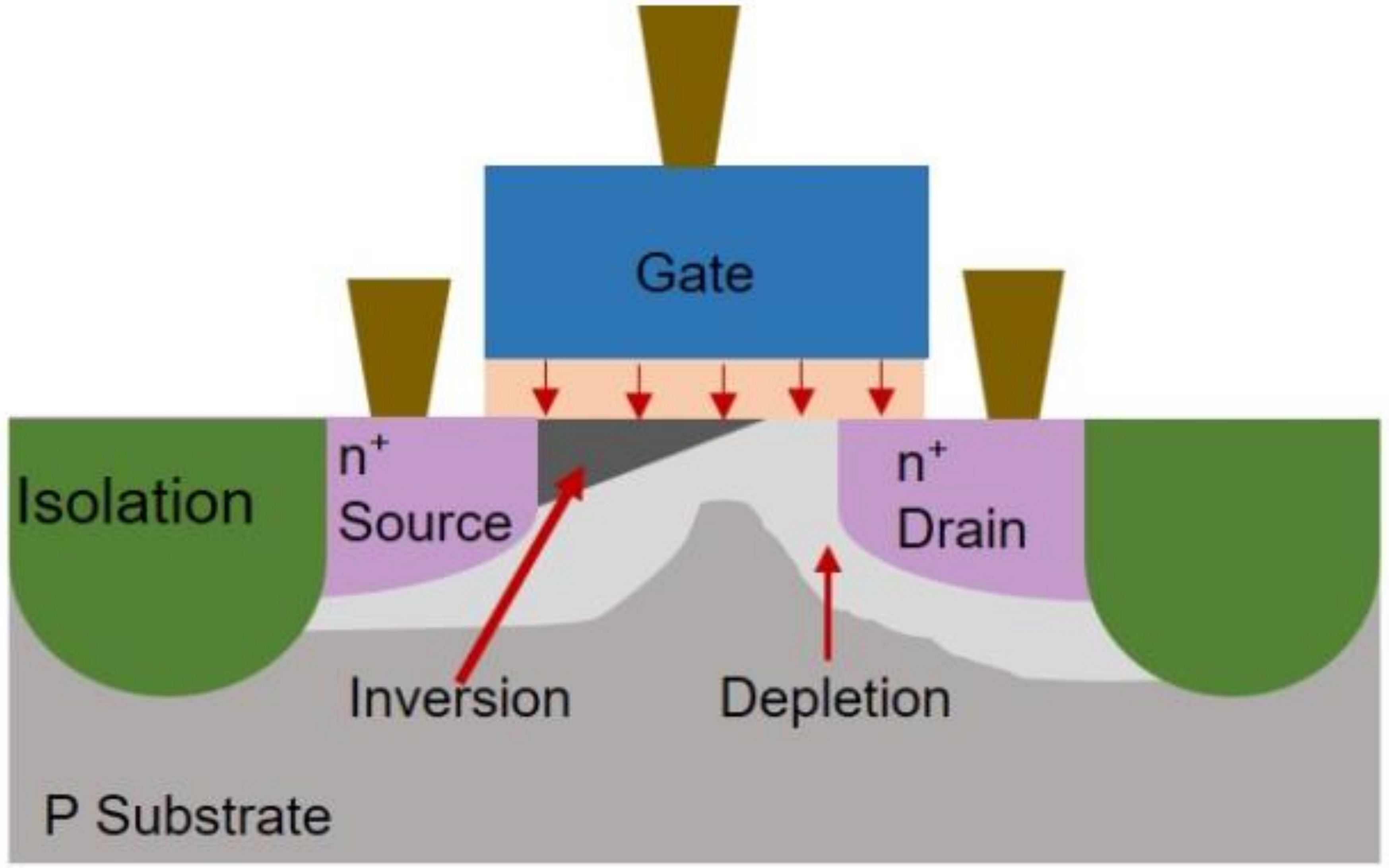
- **Electro-Optical Frequency Mapping (EOFM)** or **Laser Voltage Imaging (LVI):** Feeding the reflected signal to a detector with a narrow band frequency filter while scanning the laser—> detecting node switching with this frequency

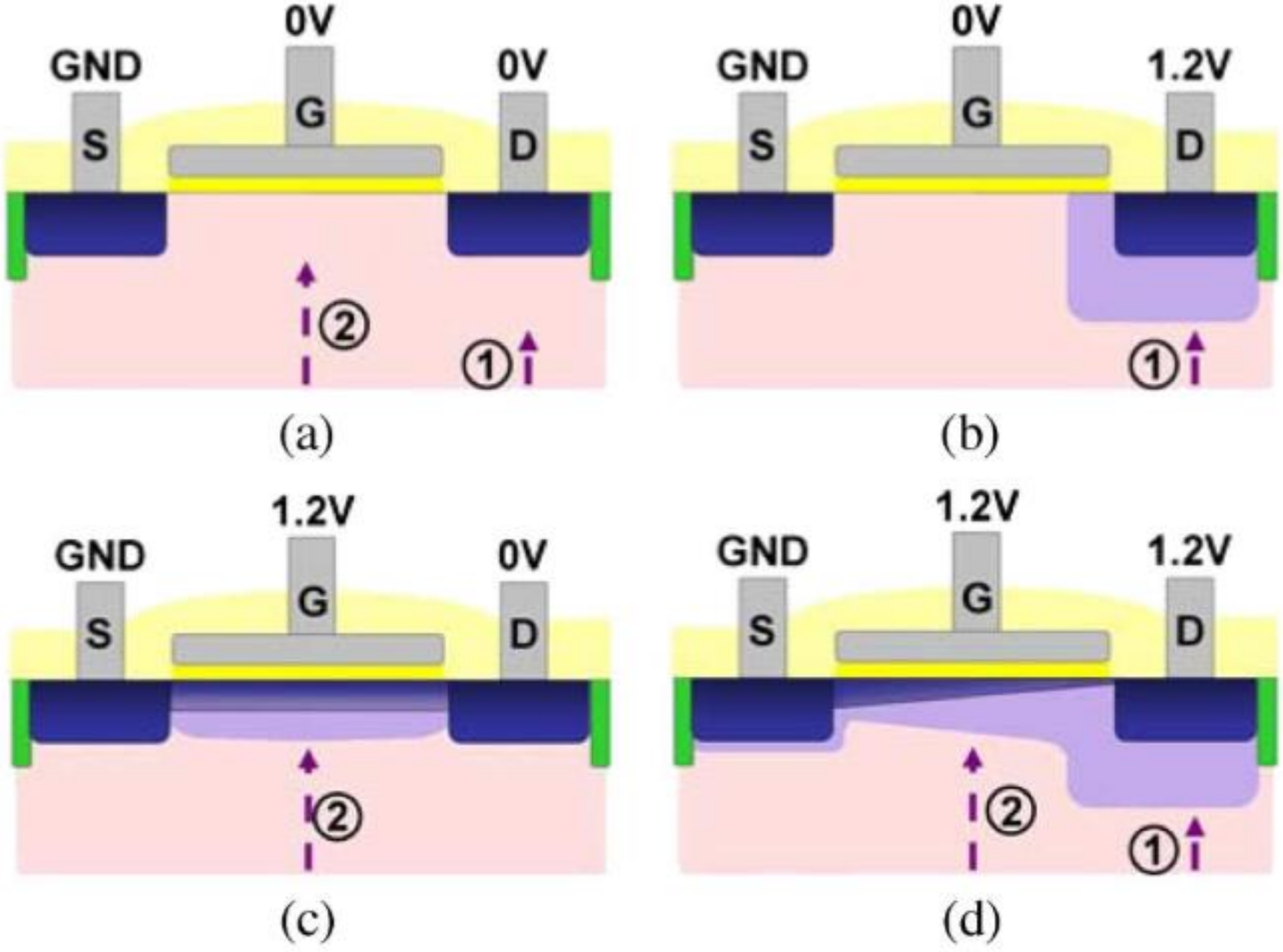
Optical Contactless Probing

- **Changes in the absorption coefficient and the refractive index of device in active area by electrical field and free carrier density.**

$$\Delta n = \frac{\lambda^2 q^2}{8\pi^2 c_0{}^2 \epsilon_0 n_0}\left[\frac{\Delta N_e}{m_e} + \frac{\Delta N_n}{m_h}\right]$$

$$\Delta \alpha = \frac{\lambda^2 q^3}{4\pi^2 c_0{}^3 \epsilon_0 n_0}\left[\frac{\Delta N_e}{m_e \mu_e} + \frac{\Delta N_n}{m_h \mu_h}\right]$$

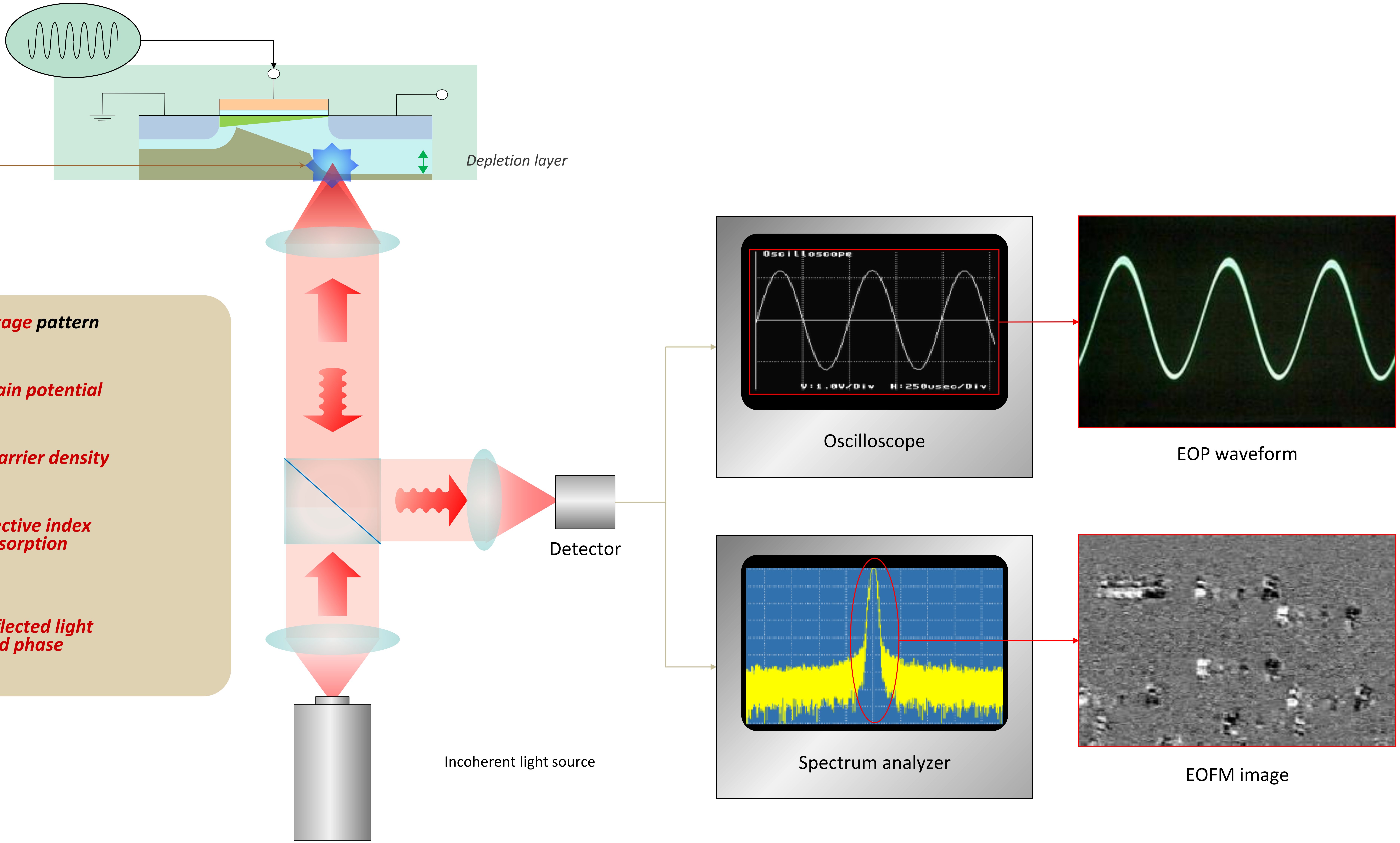




(a) (b)

(c) (d)

Mechanism of EOP/EOFM Analysis



Supply gate voltage pattern

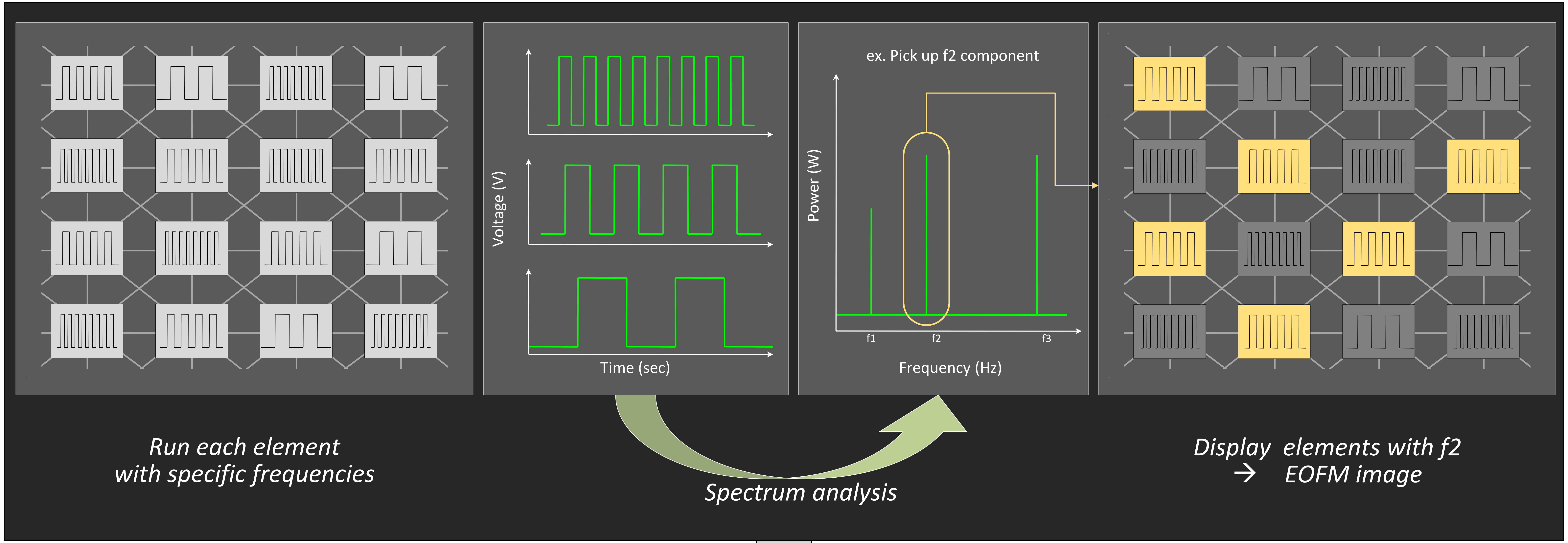
Oscillation of drain potential

Perturbation of carrier density

Change of reflective index and light absorption

Variation of reflected light strength and phase

EOFM Image Acquiring and Application



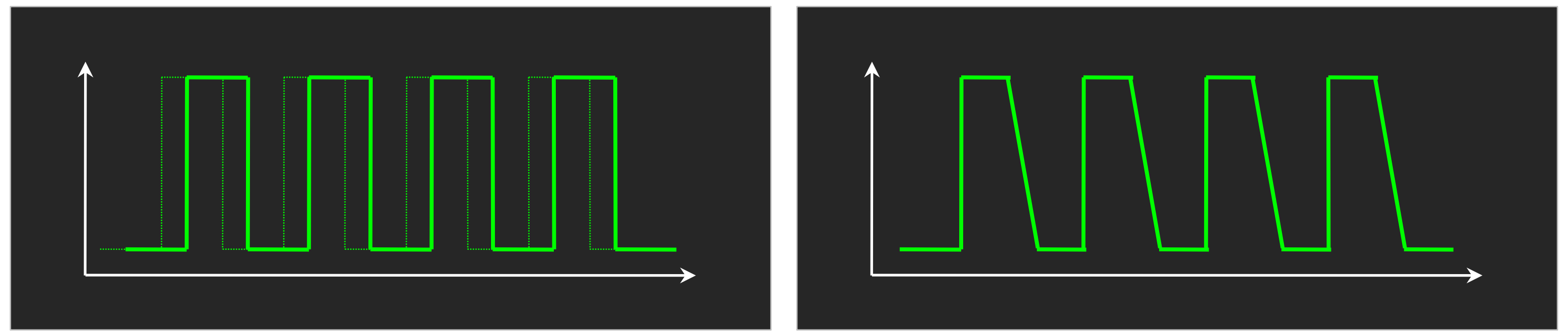
Run each element
with specific frequencies

Spectrum analysis

Display elements with f2
→ EOFM image

Adjust conditions to get the clearest EOFM image

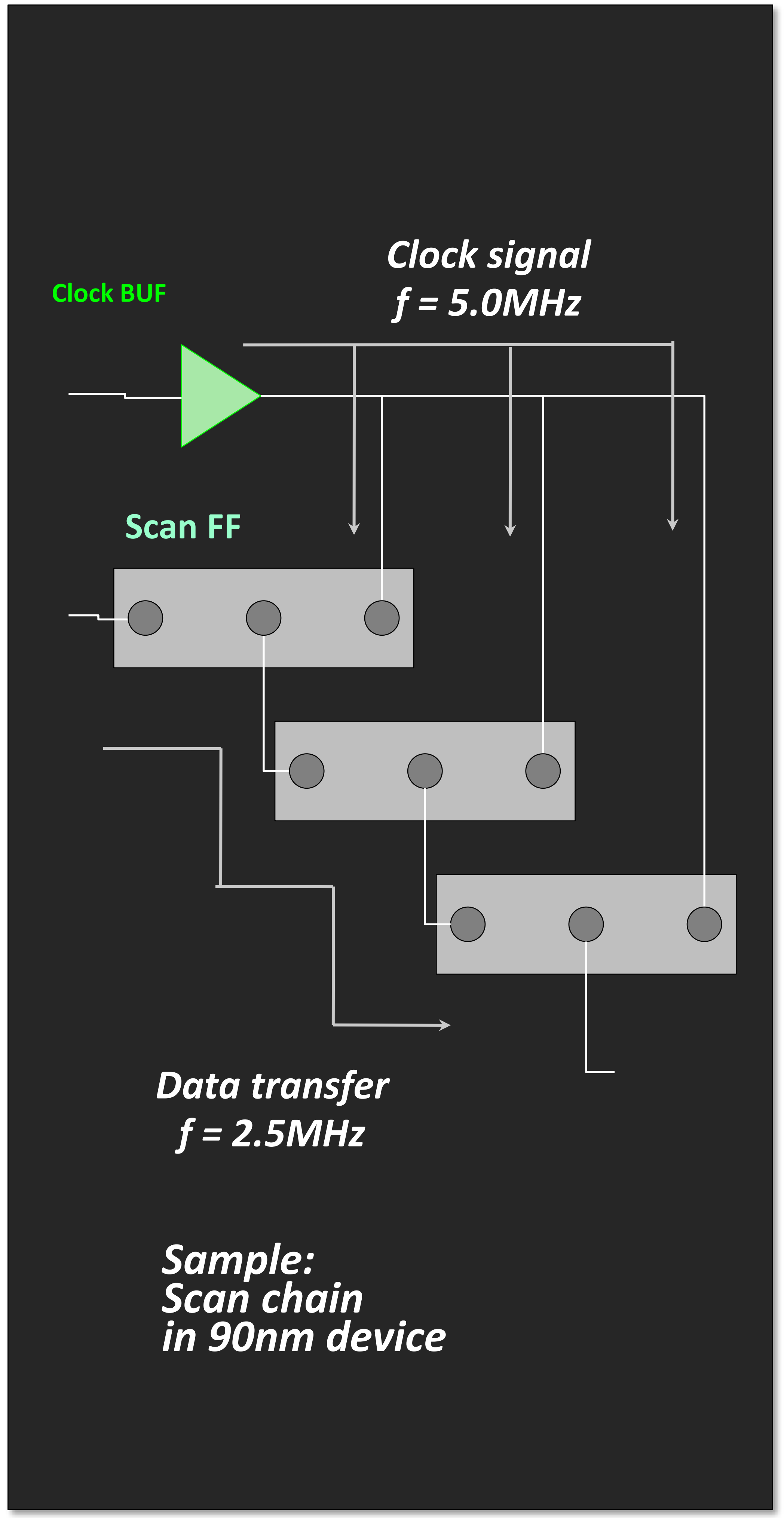
Acquire waveform at the suspicious points in the EOFM image



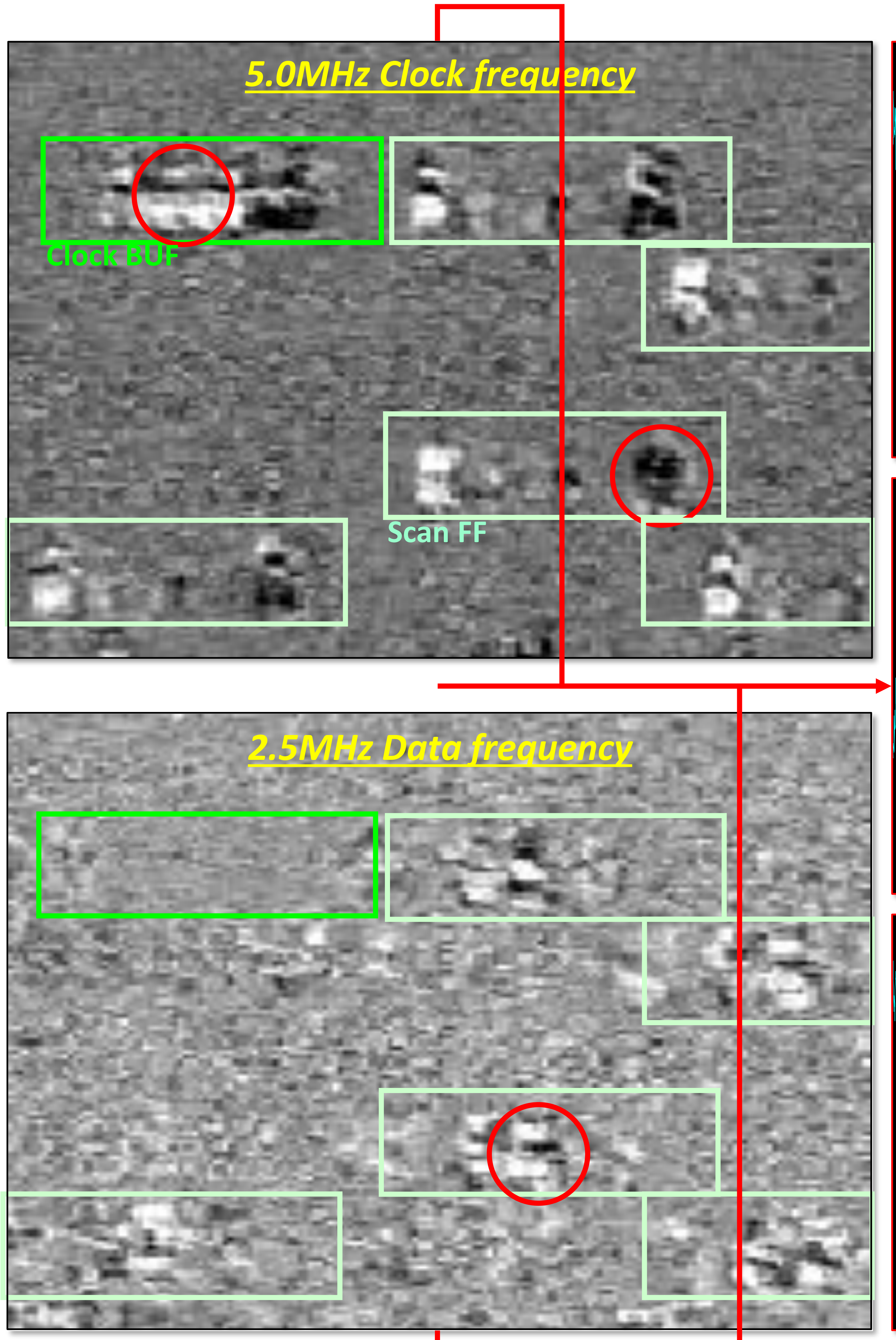
ex. Delayed or dull waveform

Elements with specific frequency observation and EOP analysis

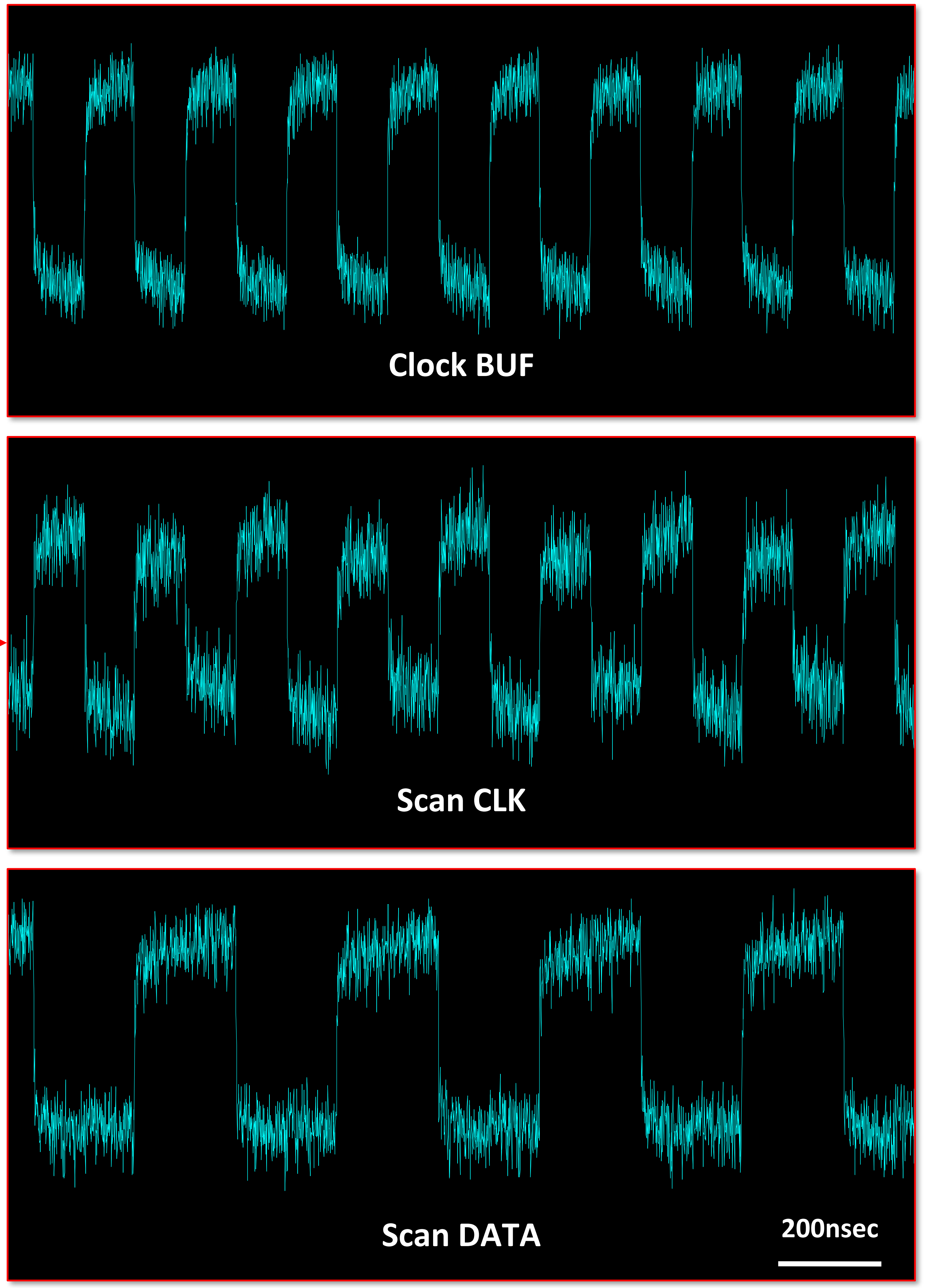
Scan Flipflop Operation Check by EOFM/EOP



Experiment setting



EOFM image



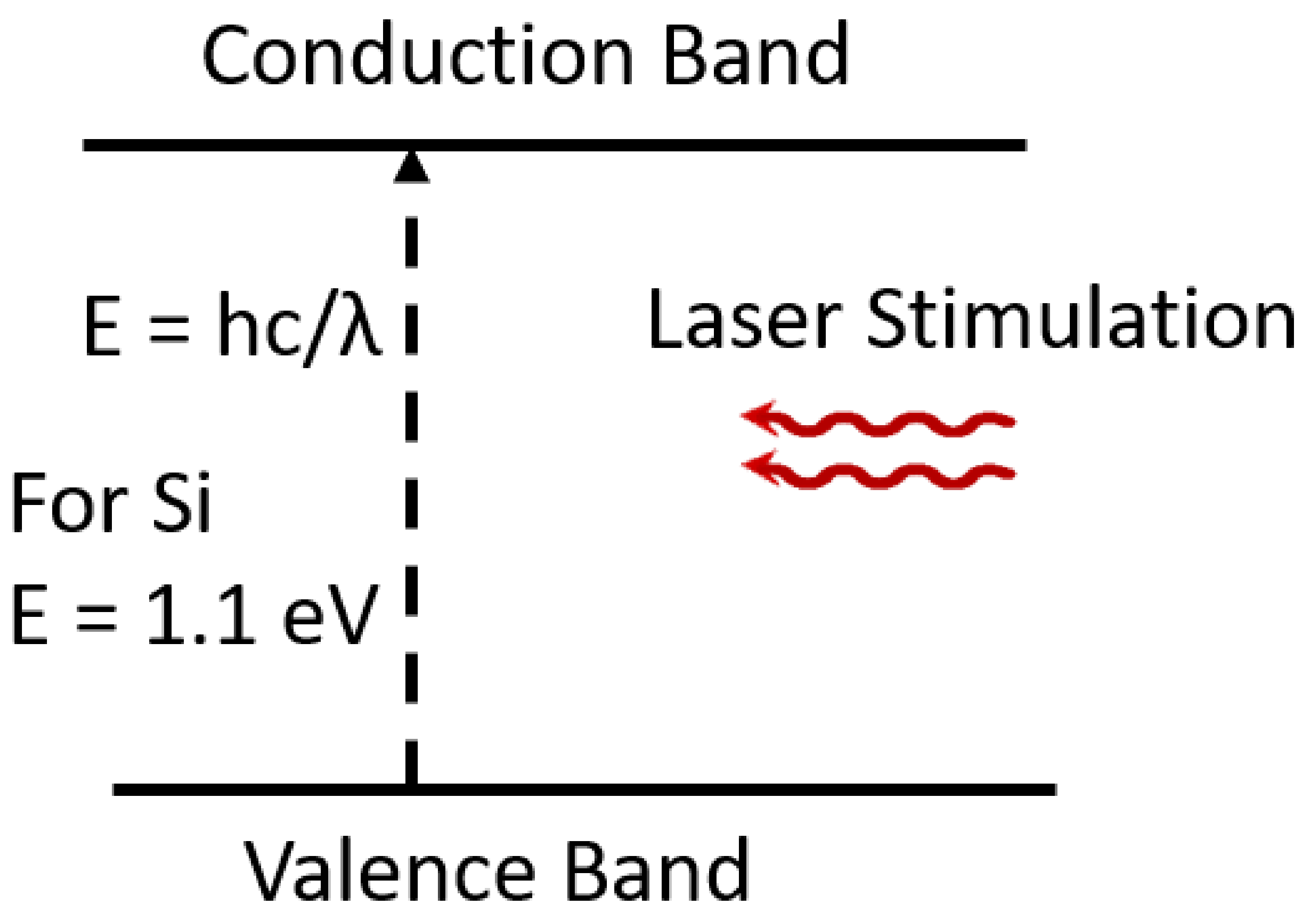
EOP waveform

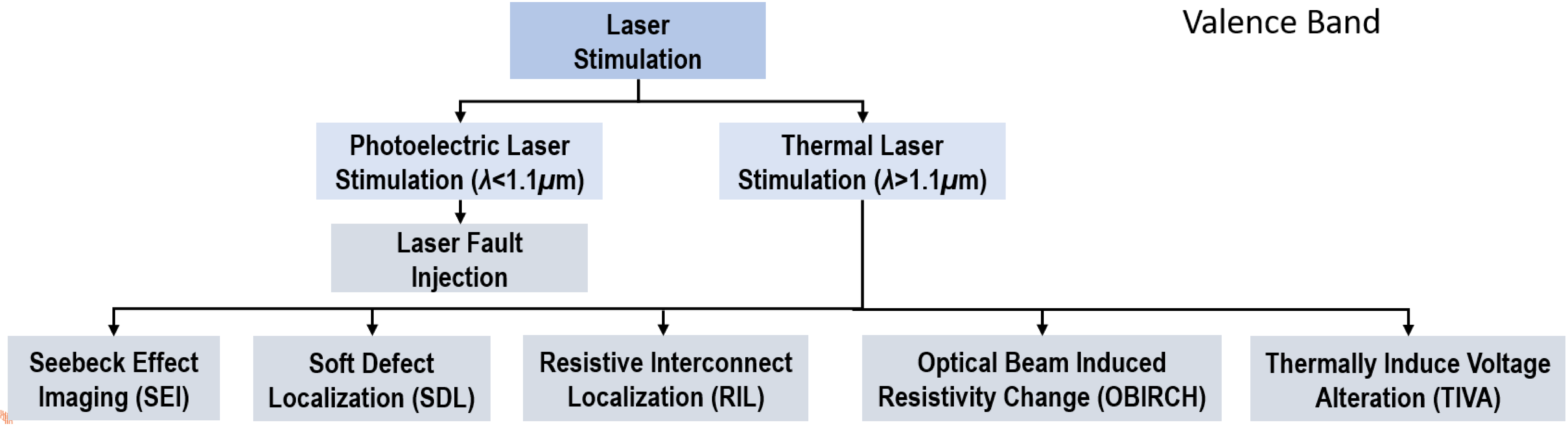
Confirming analysis site in EOFM image and acquiring EOP waveform

Laser Stimulation / Optical Beam Induced Resistance Change (OBIRCH)

Laser Stimulation Analysis

- Laser with different wavelength induce photoelectric or thermal effect in the chip
- Depending on the wavelength of laser optical attack method changes





Laser Stimulation

Photoelectric Laser Stimulation ($\lambda<1.1\mu m$)

Thermal Laser Stimulation ($\lambda>1.1\mu m$)

Laser Fault Injection

Seebeck Effect Imaging (SEI)

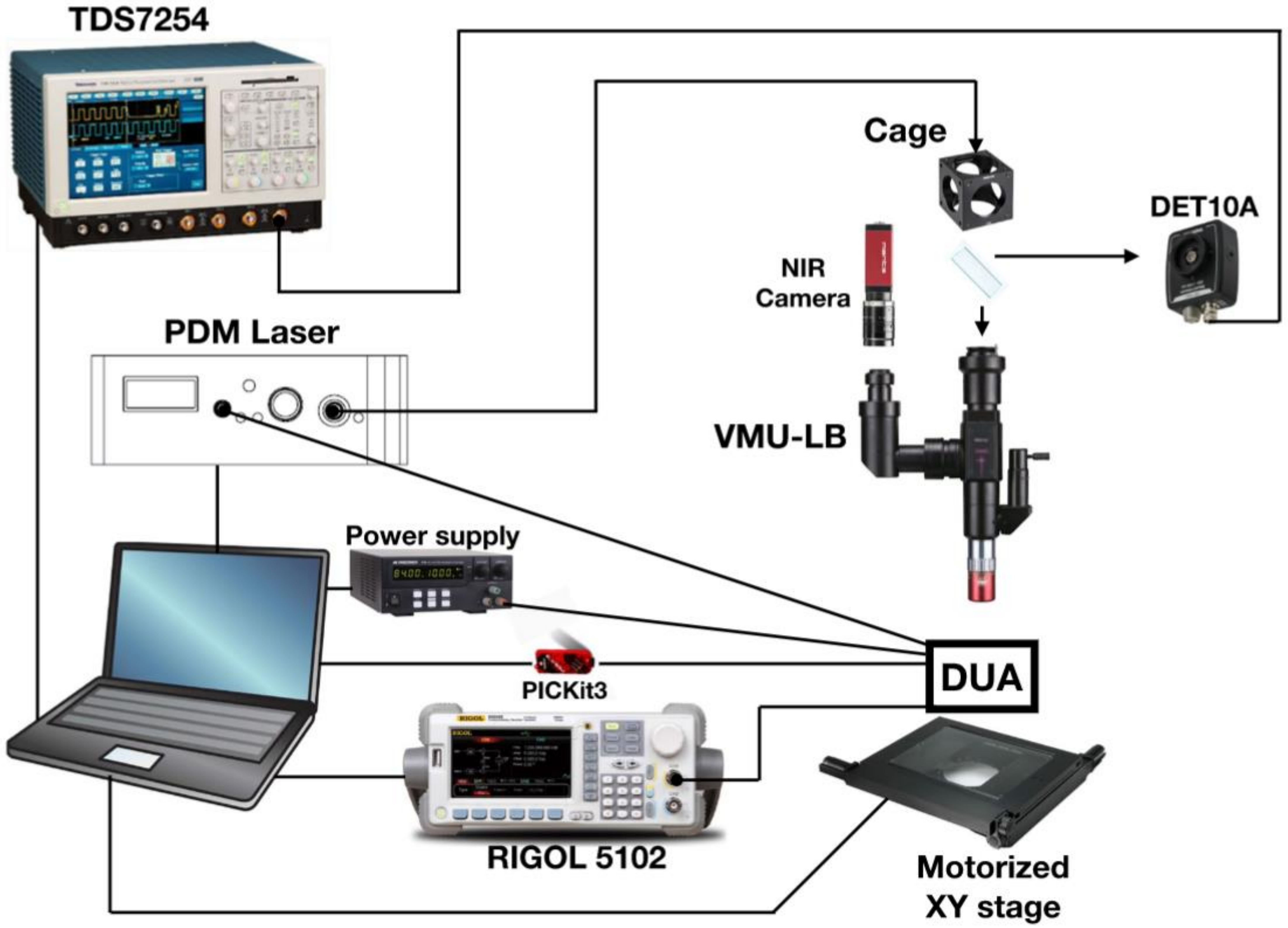
Soft Defect Localization (SDL)

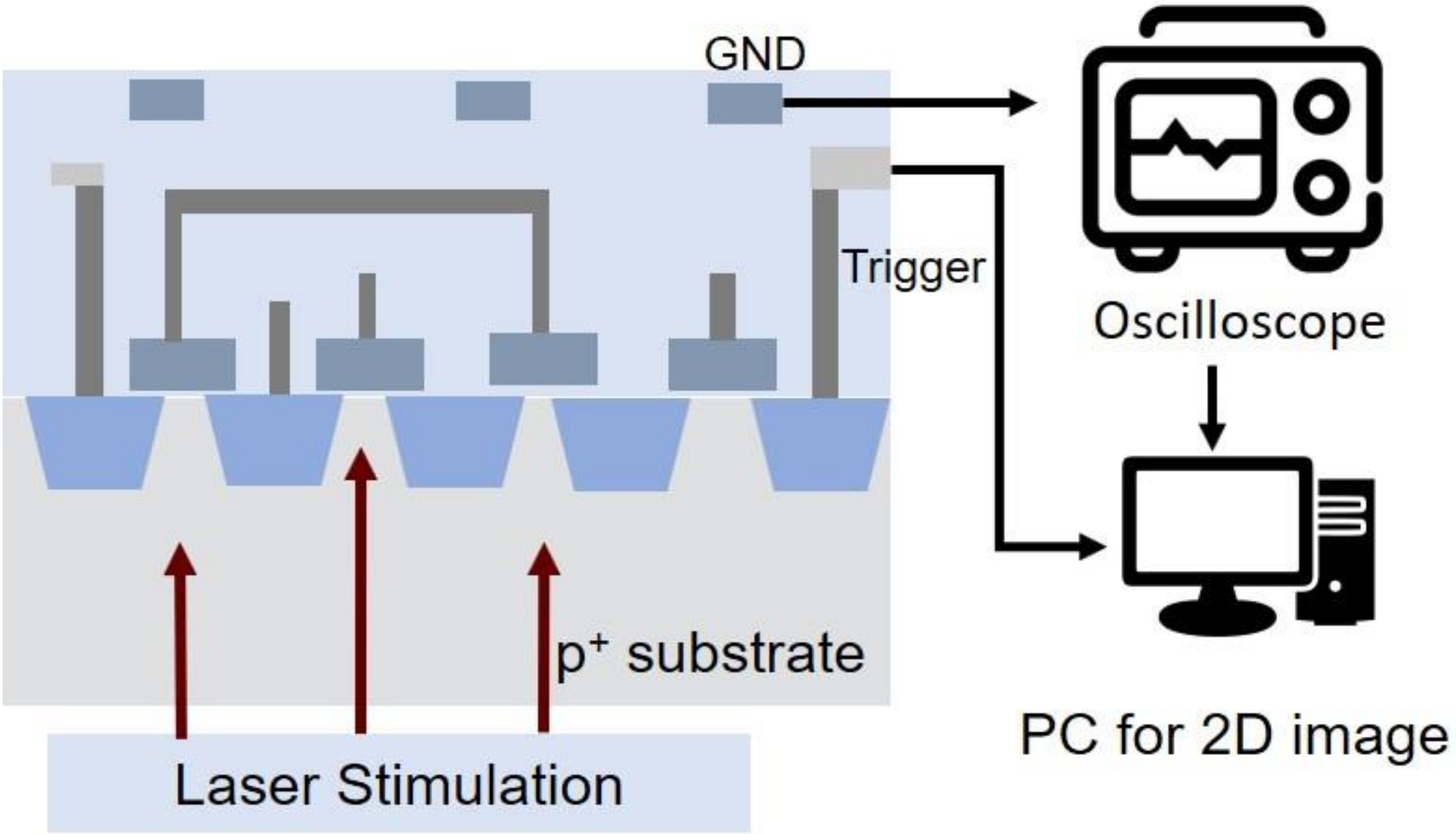
Resistive Interconnect Localization (RIL)

Optical Beam Induced Resistivity Change (OBIRCH)

Thermally Induce Voltage Alteration (TIVA)

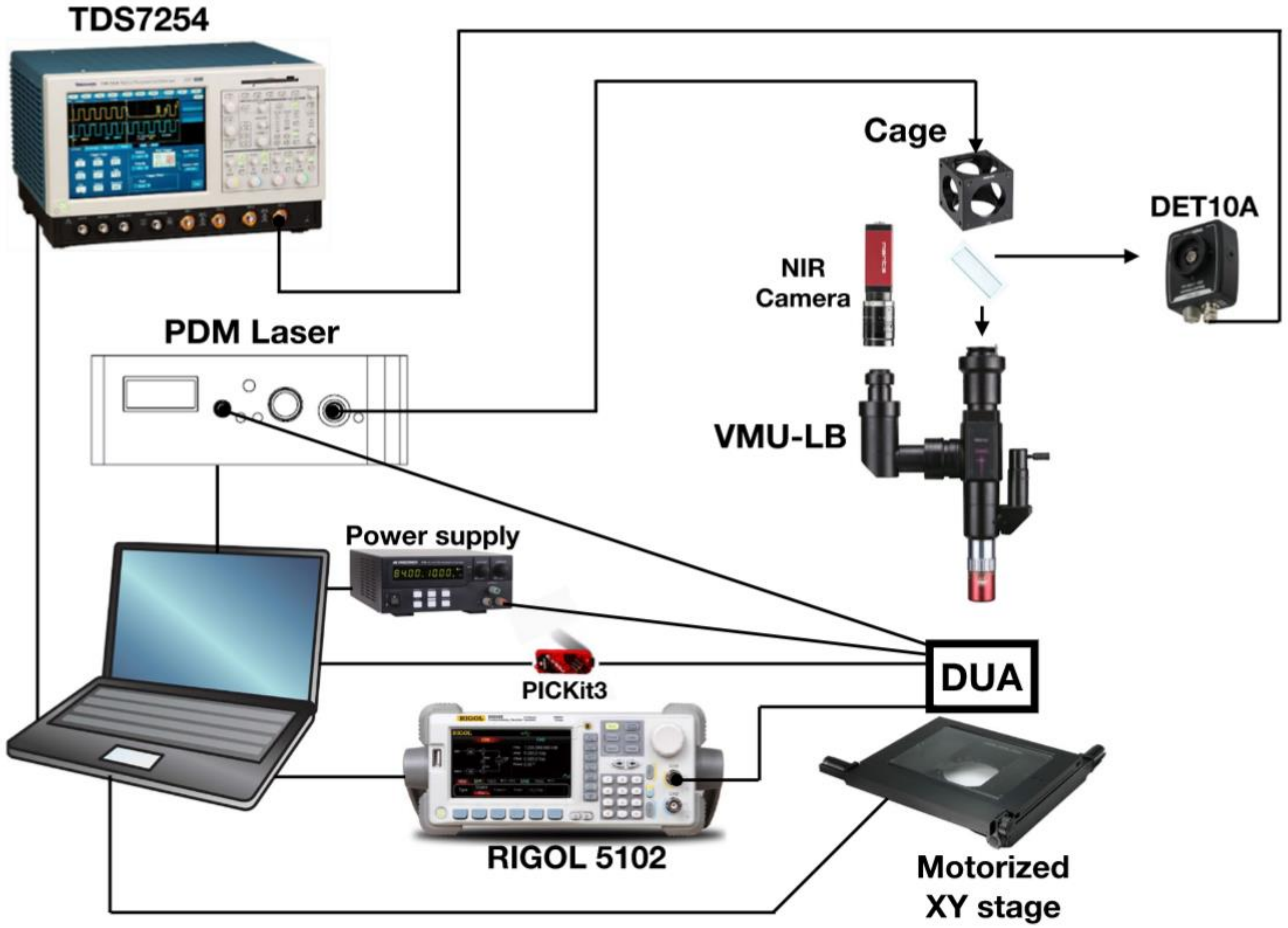
Laser Fault Injection





- $\lambda < 1.1\ \mu$m used for laser stimulation
- Used for changing the state of transistor in the circuit

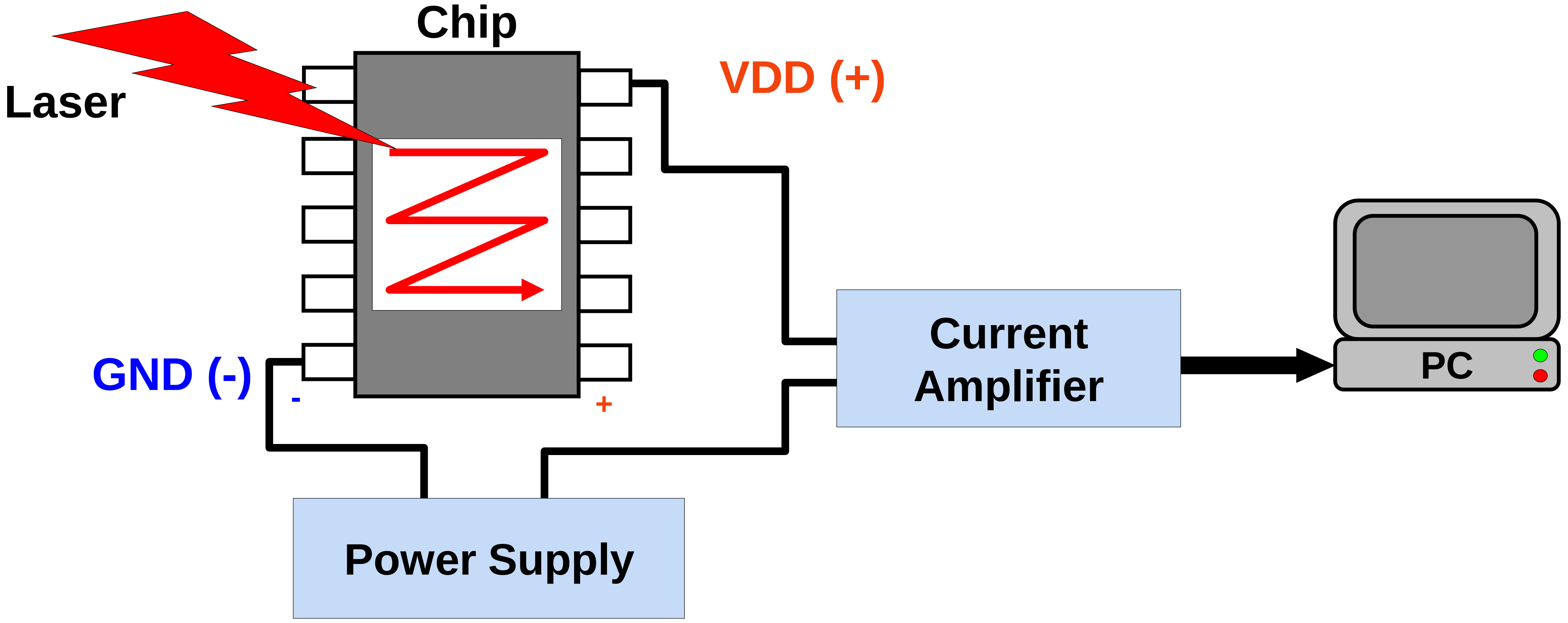
Laser Fault Injection



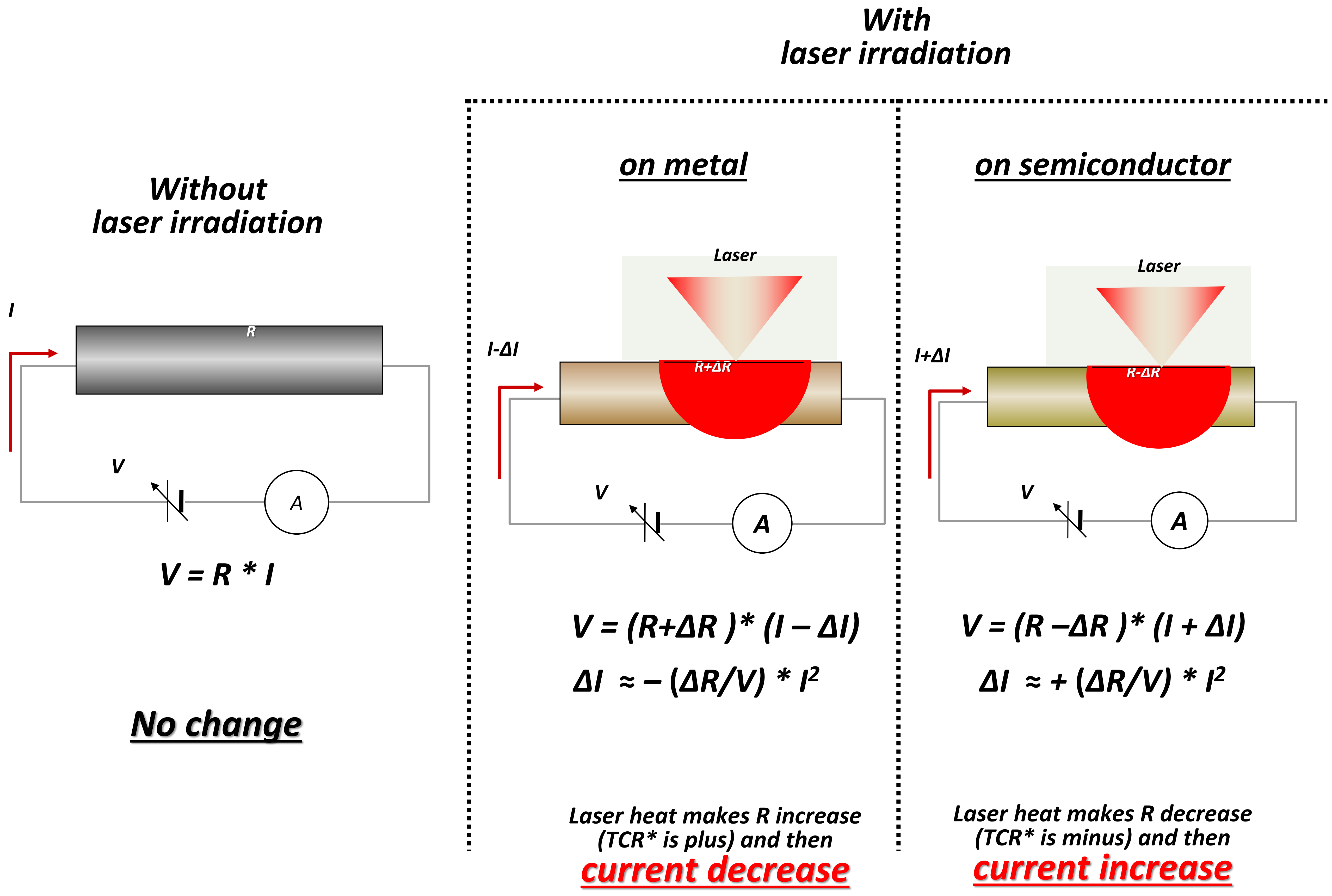
```
Freq(C3)      608.0MHz   Low signal amplitude   Period(C3)   1.645ns   Low signal amplitude
Freq(C2)      19.96MHz   Low signal amplitude   Period(C2)   50.1ns    Low signal amplitude
Pos Wid(C4)*  200.5ns    Low signal amplitude   High(C4)     35.0mV
Low(C4)       1000.0µV
                                                M 80.0ns 5.0GS/s     IT 80.0ps/pt
Ch3     50.0mV  Ω          Ch4     50.0mV  Ω    A  Ch4  ⁄  10.0mV
```

- *λ* < *1.1* *µ*m used for laser stimulation
- Used for changing the state of transistor in the circuit

Laser Change by Laser Irradiation



- The chip is scanned with a laser beam with either thermal or photoeletric interaction (TLS/PLS)
- The current changes in response to the stimulation due to resistance change and Seebeck effect.



Without laser irradiation

$V = R * I$

No change

on metal

$V = (R+\Delta R)*(I-\Delta I)$

$\Delta I \approx -(\Delta R/V)*I^2$

Laser heat makes R increase (TCR is plus) and then* ***current decrease***

on semiconductor

$V = (R-\Delta R)*(I+\Delta I)$

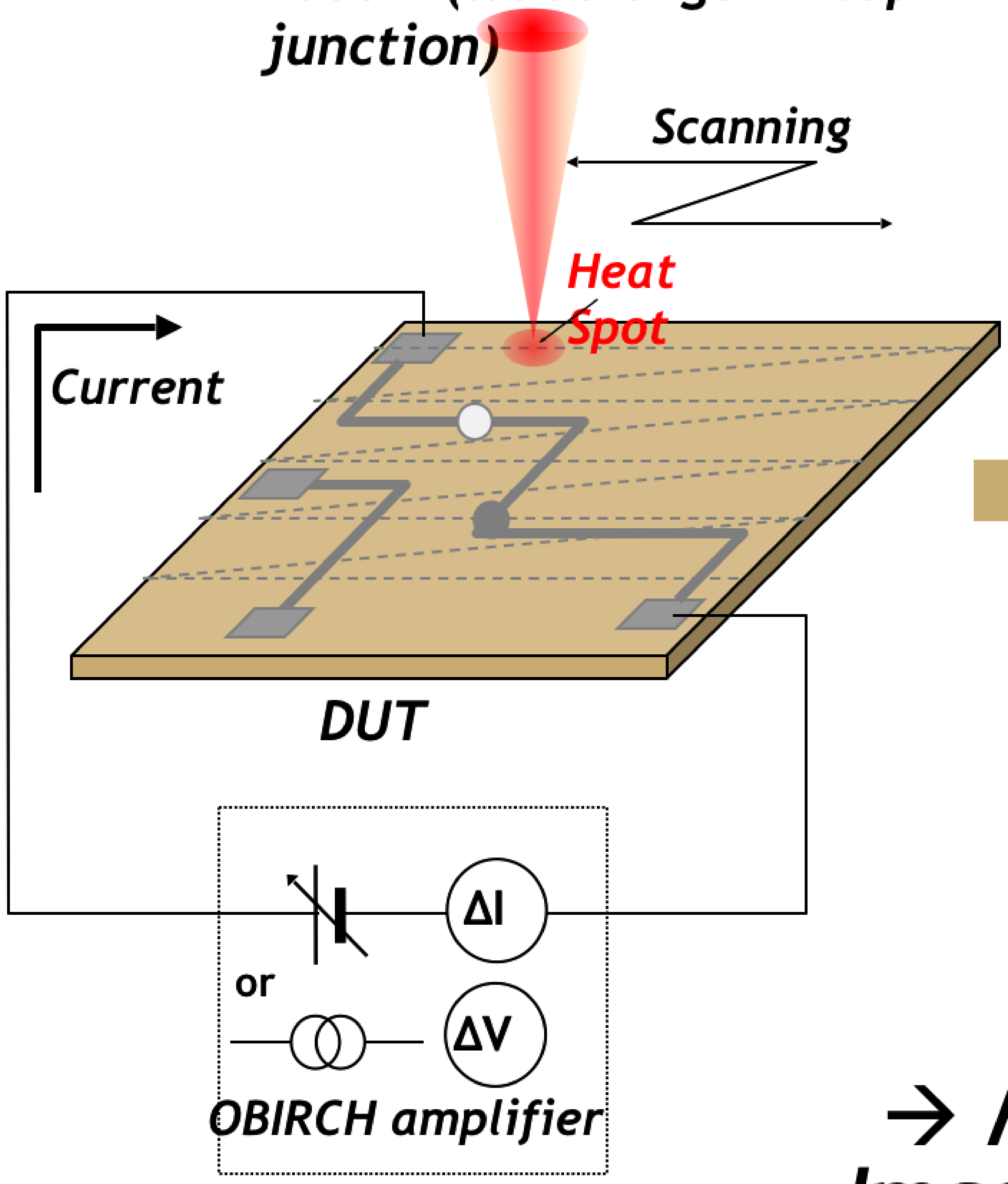
$\Delta I \approx +(\Delta R/V)*I^2$

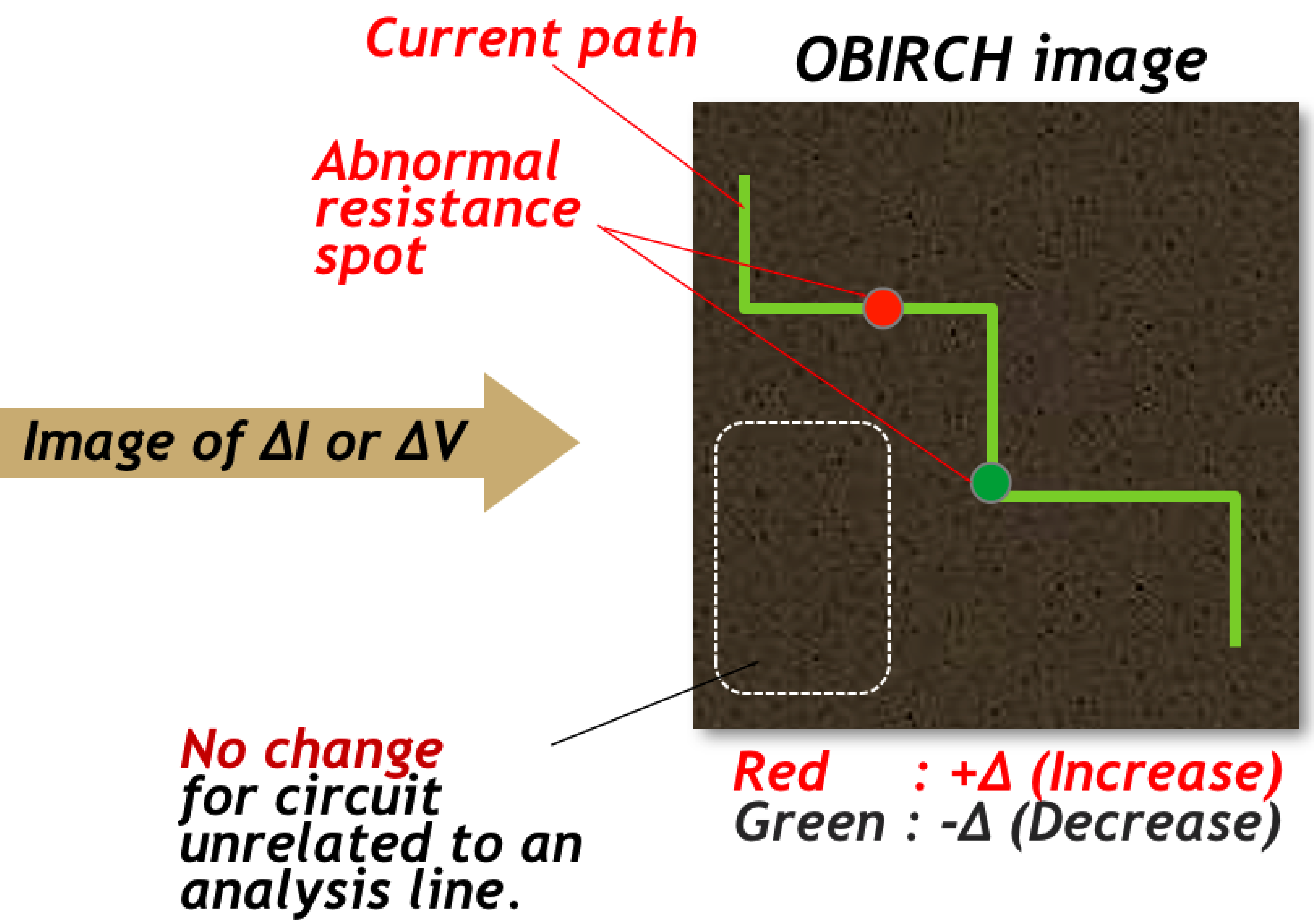
Laser heat makes R decrease (TCR is minus) and then* ***current increase***

**TCR = Temperature Coefficient of Resistance*

Mechanism of OBIRCH Analysis

Laser (wavelength 1.3μm← generate no electron-hole pair at p-n junction)





Applying electrical bias
→ Monitoring current or voltage
Imaging change of the current or the voltage