Nano-probing and EBIC/EBAC

Dr. Navid Asadi

Physical Inspection and AttacKs on ElectronicS (PHIKS)

Presented by: Nitin Varshney

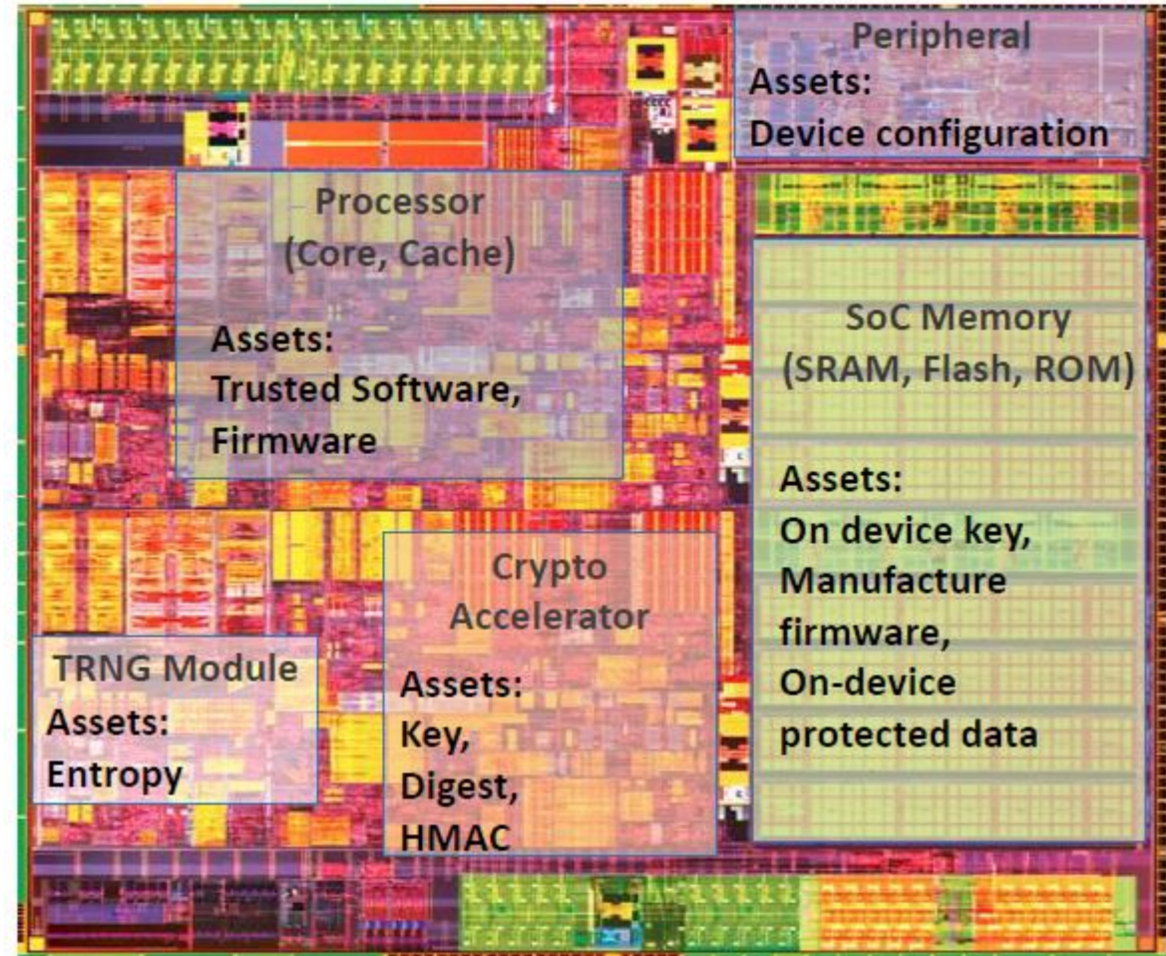
All Rights Reserved

Critical Assets in SoCs

Asset: A resource of value worth protecting from an adversary

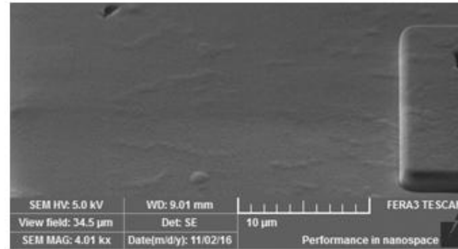
Examples:

- On-device keys (developer/OEM)
- Device configuration /defeaturing
- Manufacturer firmware
- Application software
- On-device sensitive data
- Communication credentials
- Random number or entropy

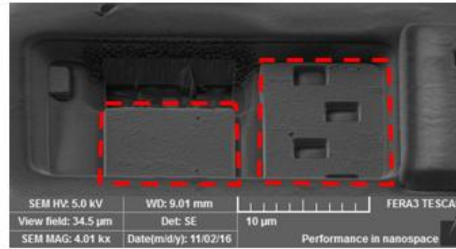


All Rights Reserved

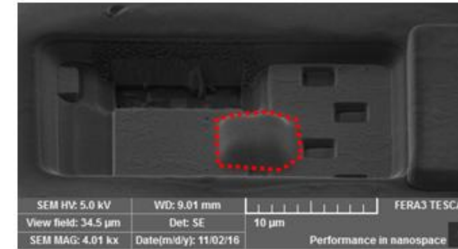
Rise of Invasive attacks



Pre-FIB surface



FIB milling to expose adjacent interconnects



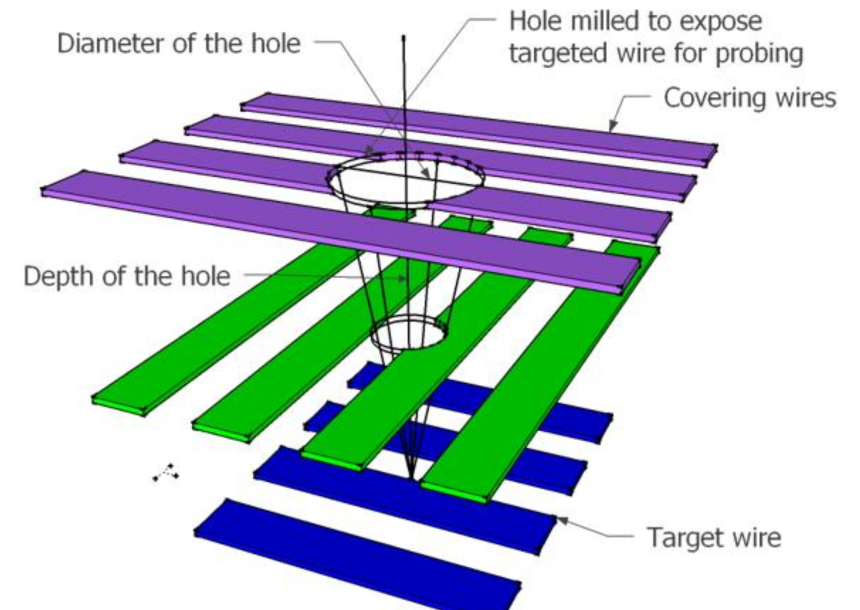
FIB deposition to short adjacent interconnects

Focused Ion Beam (FIB)

- A powerful tool commonly used in the development, manufacturing, and editing of ICs

Micro-probing / editing Attack

- Probing at signal wires to extract security sensitive information
- Front-side attack and back-side attack

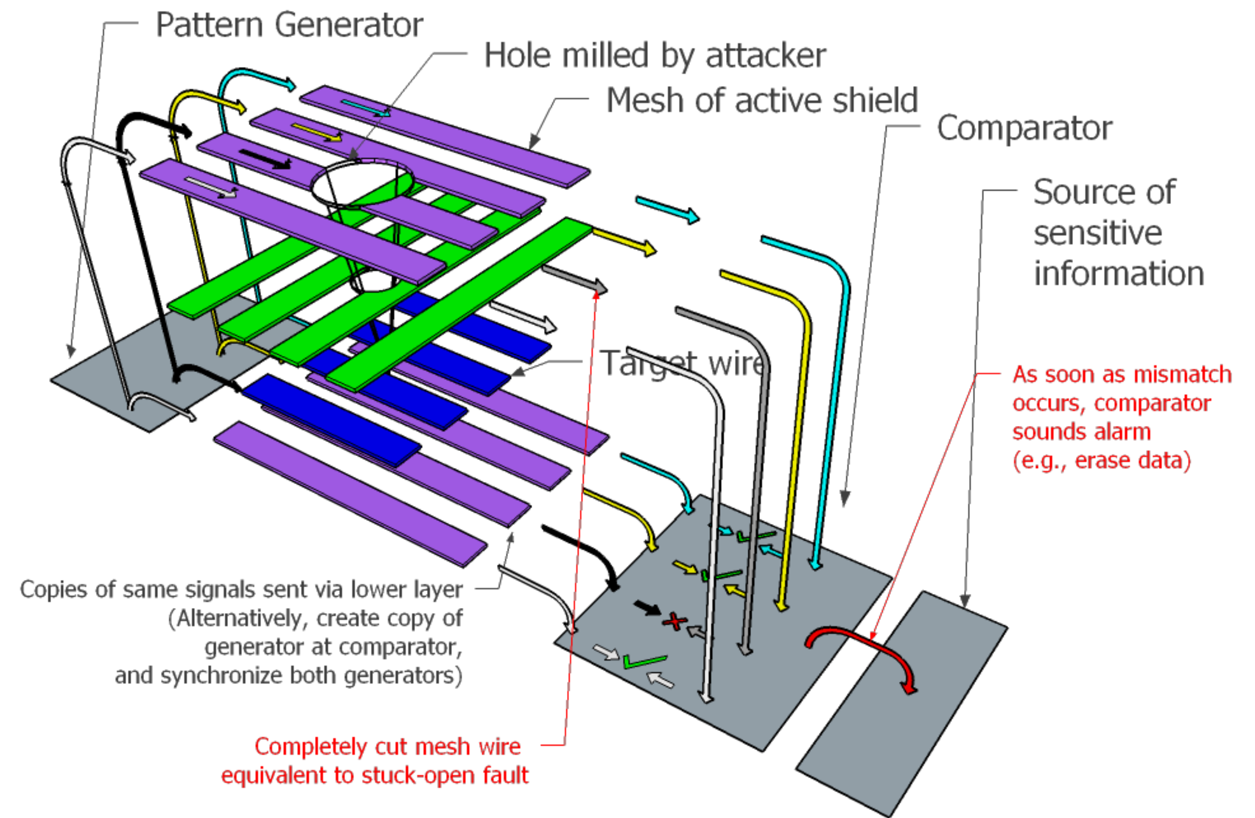


All Rights Reserved

Active Shields

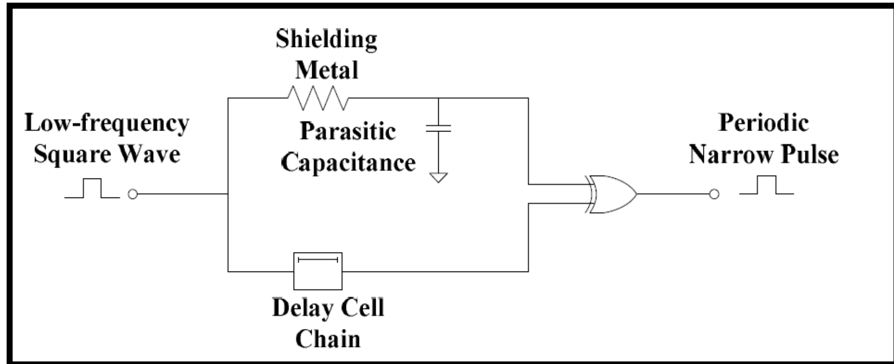
Limitations

- Occupy at least one routing layer, costly.
- Could be easily bypassed by the FIB with high aspect ratio.
- If the shield structure can be reverse engineered, it's vulnerable to reroute attack.
- The shield could be disabled by editing its control circuit.
- Only protects against front-side attacks.



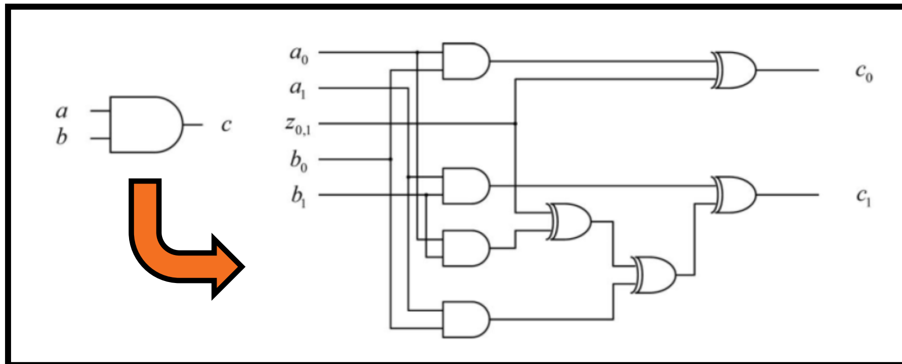
All Rights Reserved

Analog Shields and t-Private Circuits



Limitations

- Unreliable due to process variation especially with feature scaling



Limitations

- Large area overhead ($O(t^2)$)

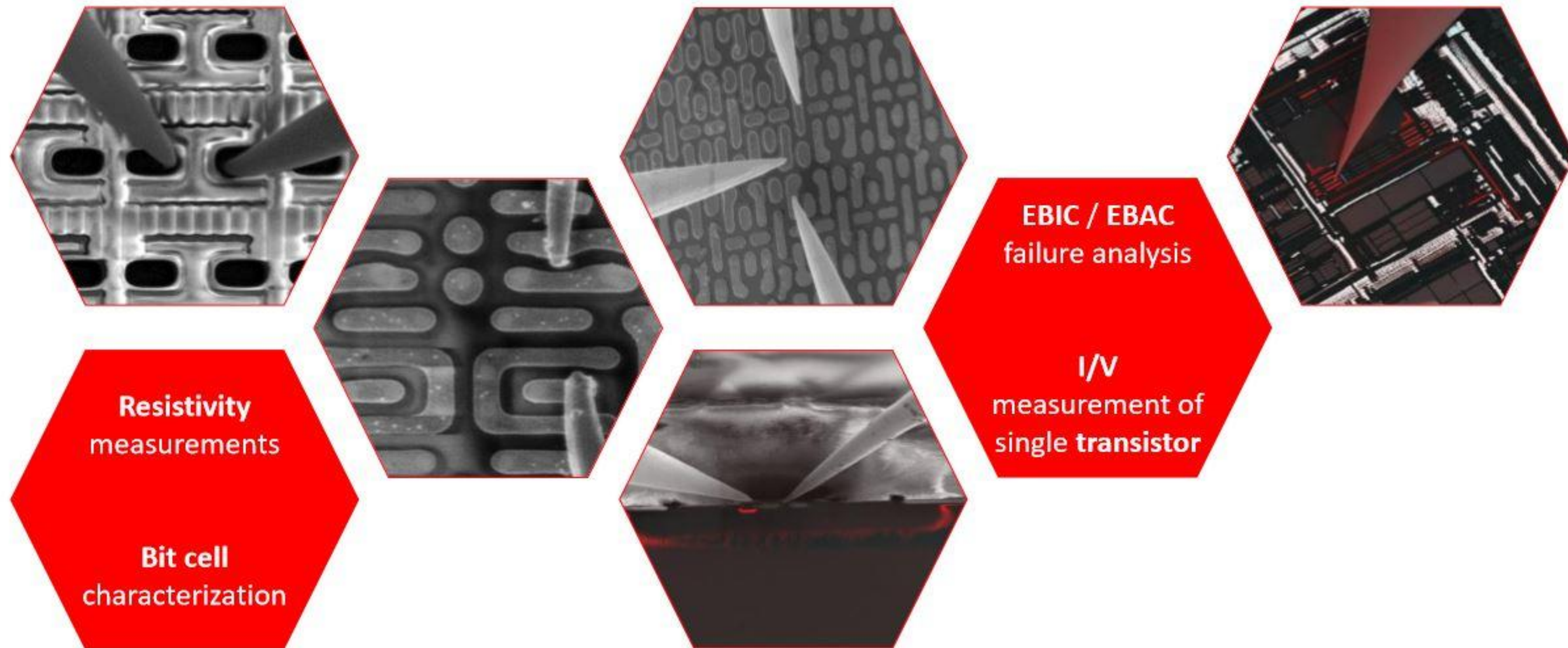
Summary

- Existing countermeasures are limited and/or expensive
- No notion of what is most in need of protection
- No approach can be easily incorporated into conventional design flow

All Rights Reserved

Applications of Electrical Probing in Semiconductors

1. Nanoprobing and Failure Analysis



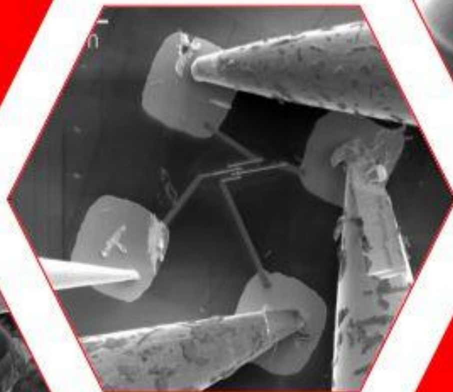
FICS Research

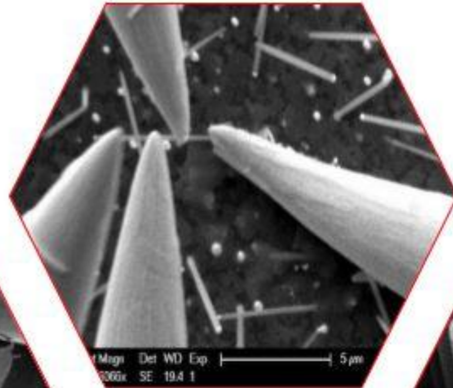
All Rights Reserved

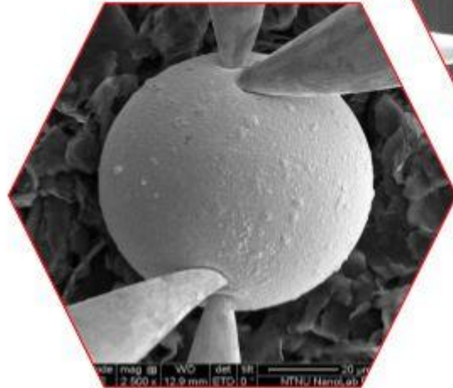
2. Electrical Characterization

4 point probing measurements

Thin film/coating characterization

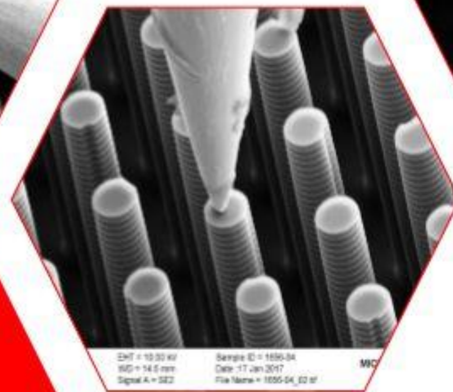


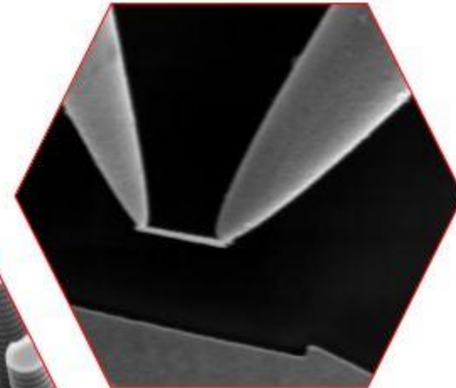




Fragile sample testing

Single structure isolation





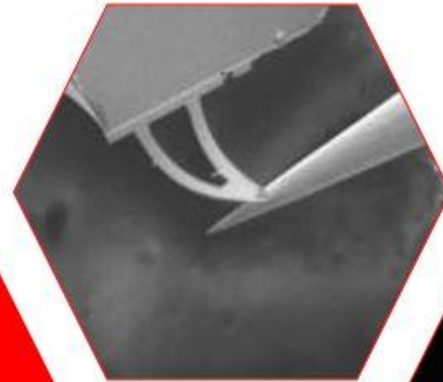
All Rights Reserved

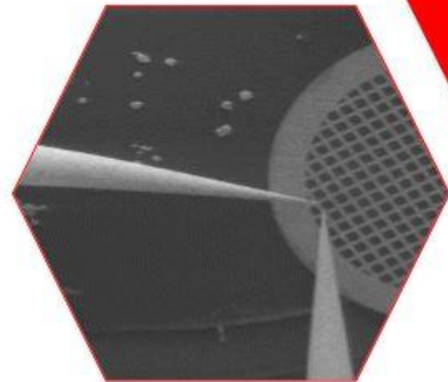
UF UNIVERSITY of FLORIDA

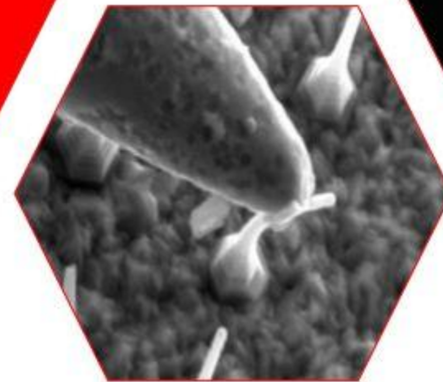
3. Sample Handling and Positioning

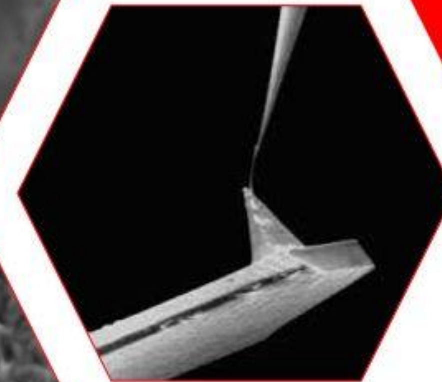
TEM sample preparation

Micro-/Nano manipulation









Nanostructures positioning and assembly

Mechanical testing

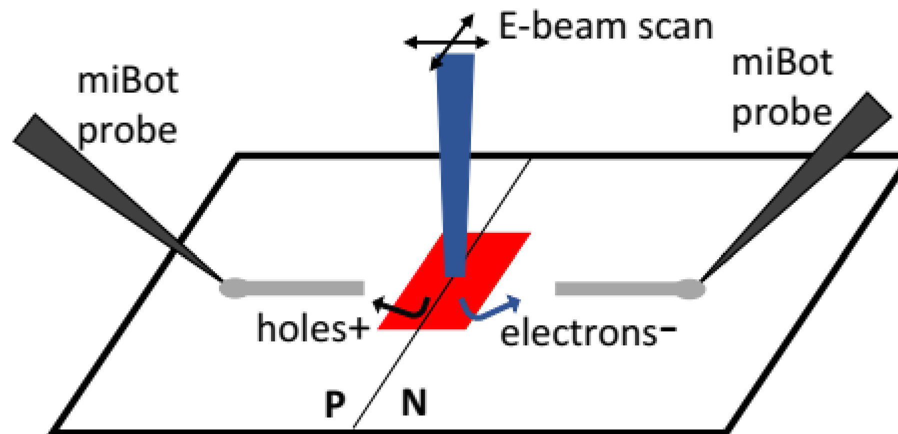
FCS Research

All Rights Reserved

Electron Beam Induced Current

EBIC is a method used for the imaging and characterization of p-n junctions, the recombination strength of defects, and the diffusion length and surface recombination velocity of minority charge carriers in semiconducting materials and devices.

It is most effective when employed alongside EDS or EBSD as part of a wider workflow, for example, nanofabrication in the FIB, or sample preparation for the TEM or atom probe.

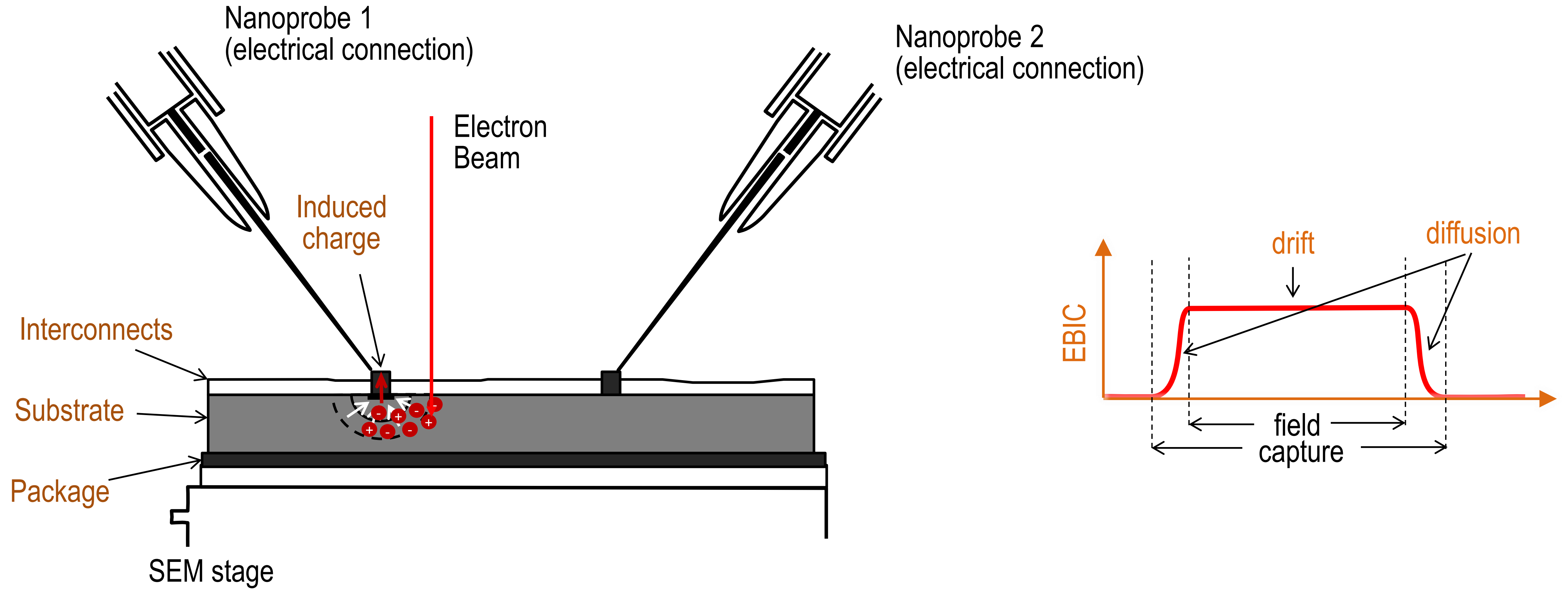


Electron Beam Induced Current

All Rights Reserved

FICS Research

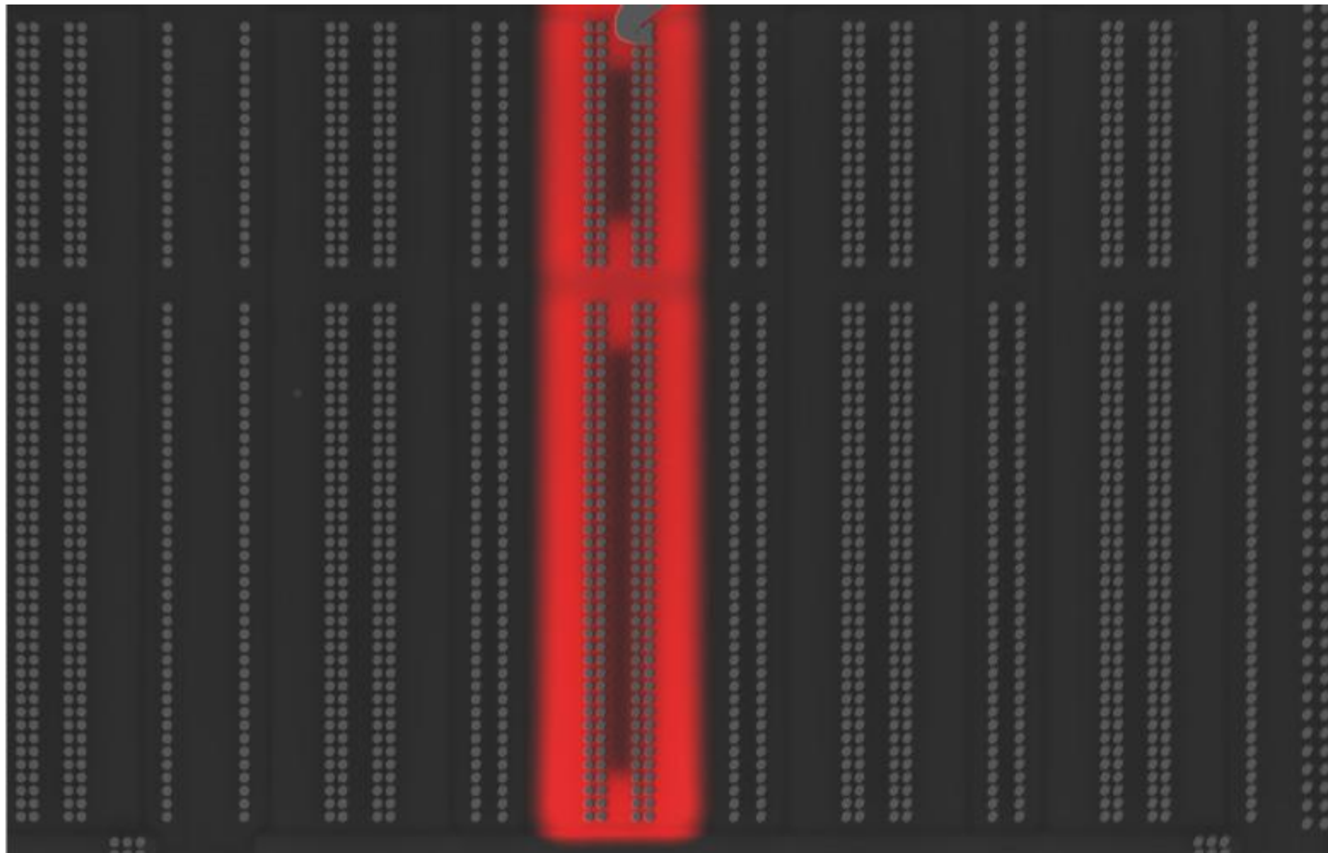
How it Works?



All Rights Reserved

Applications in Hardware Security

Map electric fields with the highest spatial resolution



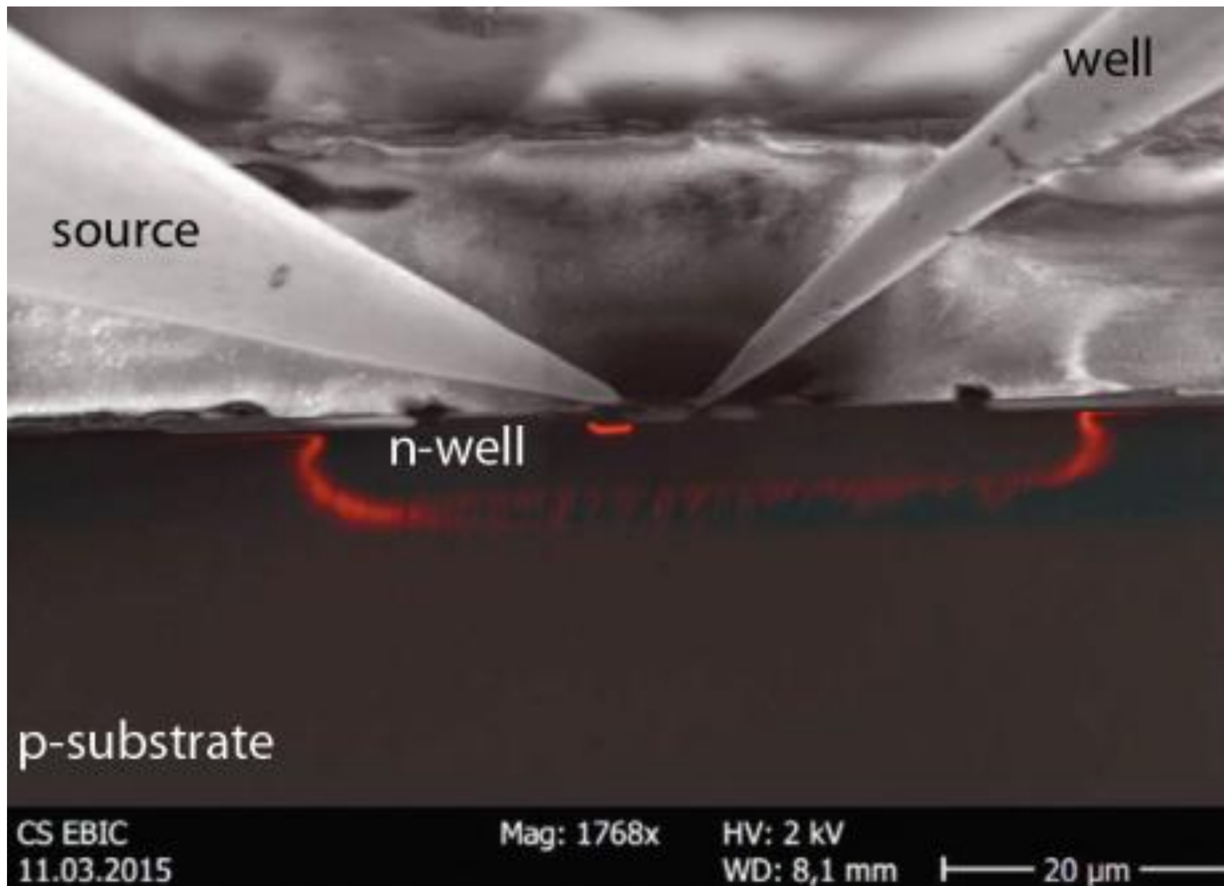
- Visualise internal electric fields from PN junctions or Schottky contacts.
- Validate doping profiles and areas with design, or reverse engineer devices.
- Identify defects with electrical activity and correlate with structure (SE, In-Lens) and composition (EDS, EBSD).

FICS Research

All Rights Reserved

Applications in Hardware Security

Access third dimension with depth profiling.



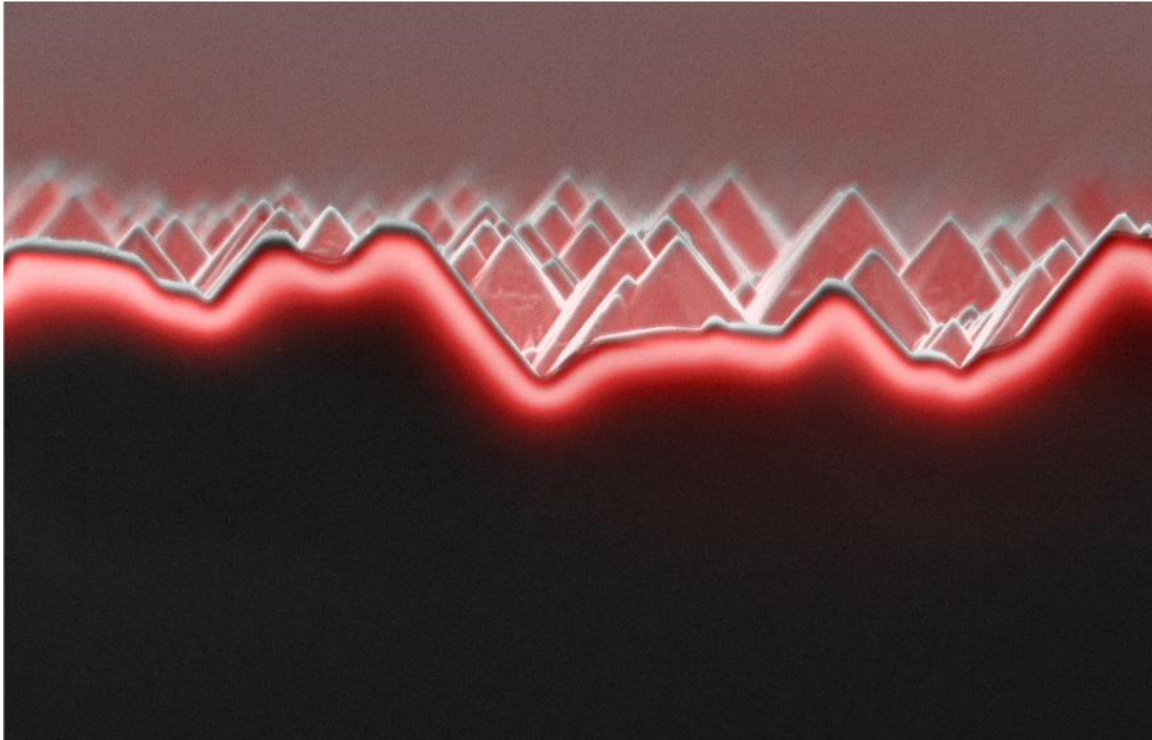
- Manipulate depth of EBIC signal by changing kV in SEM.
- Investigate EBIC images of cross-sections in FIB-SEM.
- Export EBIC depth series for 3D reconstruction.

All Rights Reserved

Applications in Failure Analysis

UNIVERSITY of FLORIDA

Map complex electric fields on 3D structures.



- Characterise relationship between surface topography and electrical activity.
- Determine internal quantum efficiency from measured induced- and beam-currents.
- Distinguish between active and passive defects – at operating conditions.

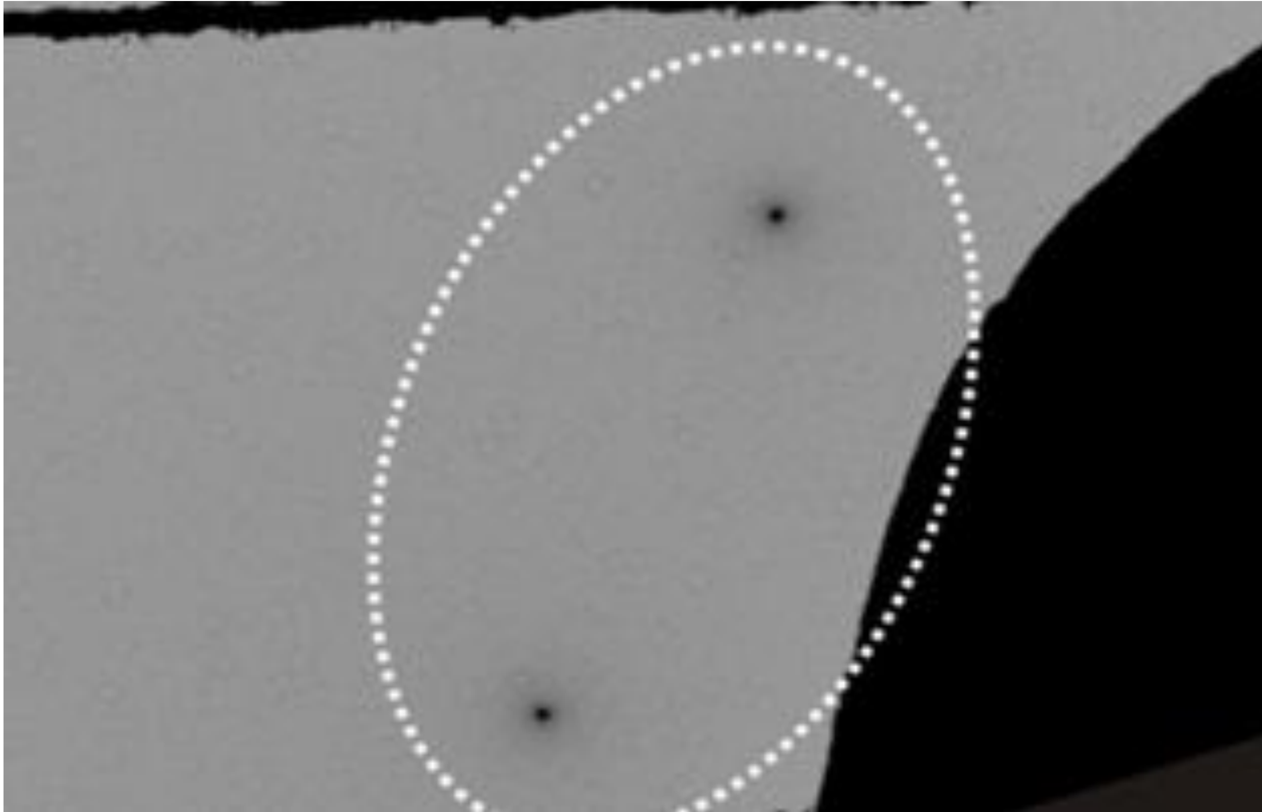
FICS Research

All Rights Reserved

Applications in Failure Analysis

UNIVERSITY of FLORIDA

Enable localisation for TEM or atom probe microscopy.



- Localise defects with sufficient resolution for TEM sample prep.
- Avoid alignment errors by directly imaging defects with EBIC in FIB SEM.
- Use live EBIC imaging to stop milling during sample preparation.

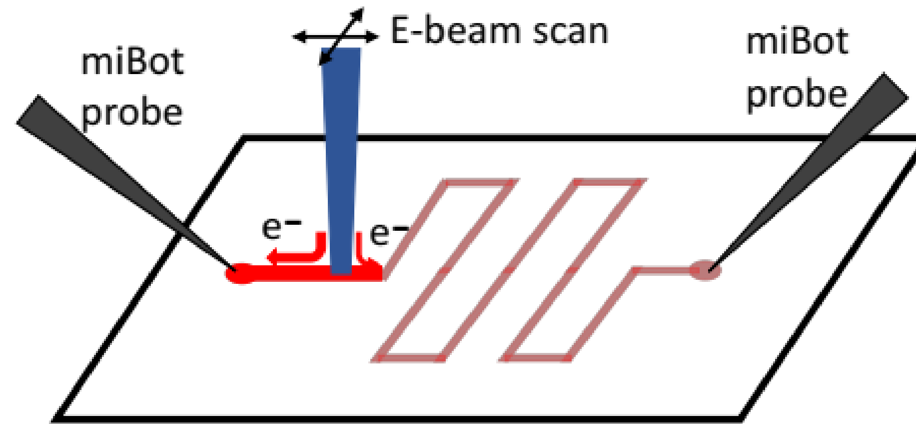
FICS Research

All Rights Reserved

Electron Beam Absorbed Current

EBAC is a method employed for the identification and physical failure analysis of metal defects (opens and shorts), high resistivity areas and layer non-uniformities in CMOS devices. It is primarily used in combination with electrical nanoprobing.

The electron beam of the SEM scans the DUT and injects charges absorbed by metal lines under the surface. A current is then induced and measured by a probe placed with a miBot nanomanipulator at contact level.

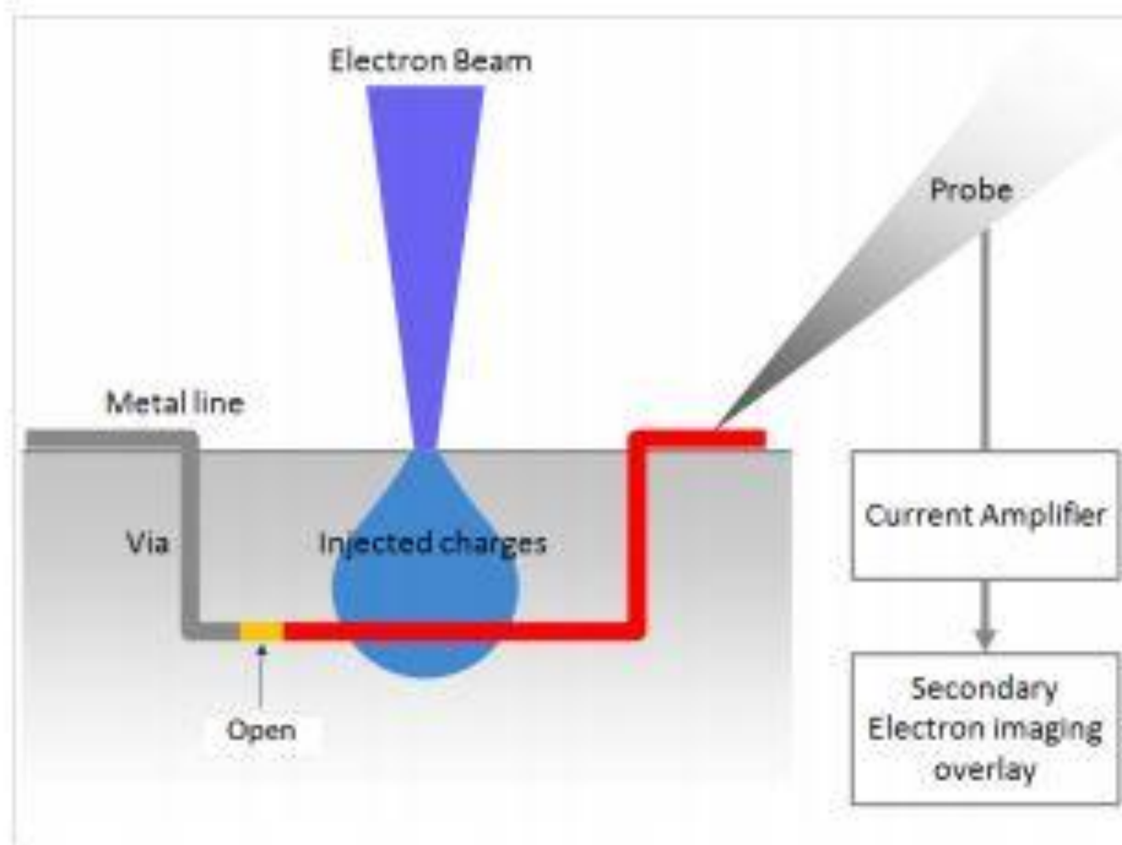


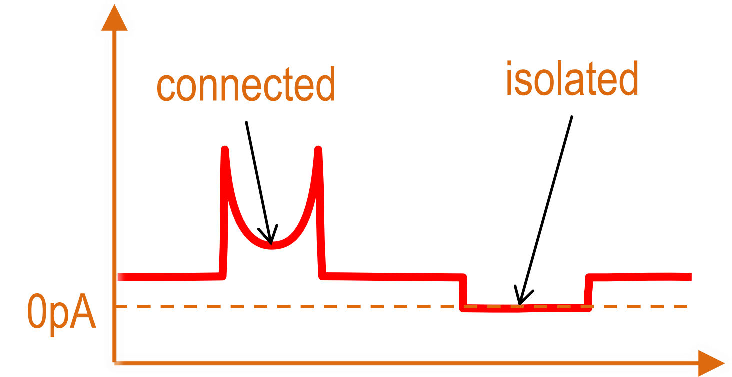
Electron Beam Absorbed Current

FICS Research

All Rights Reserved

How it Works?



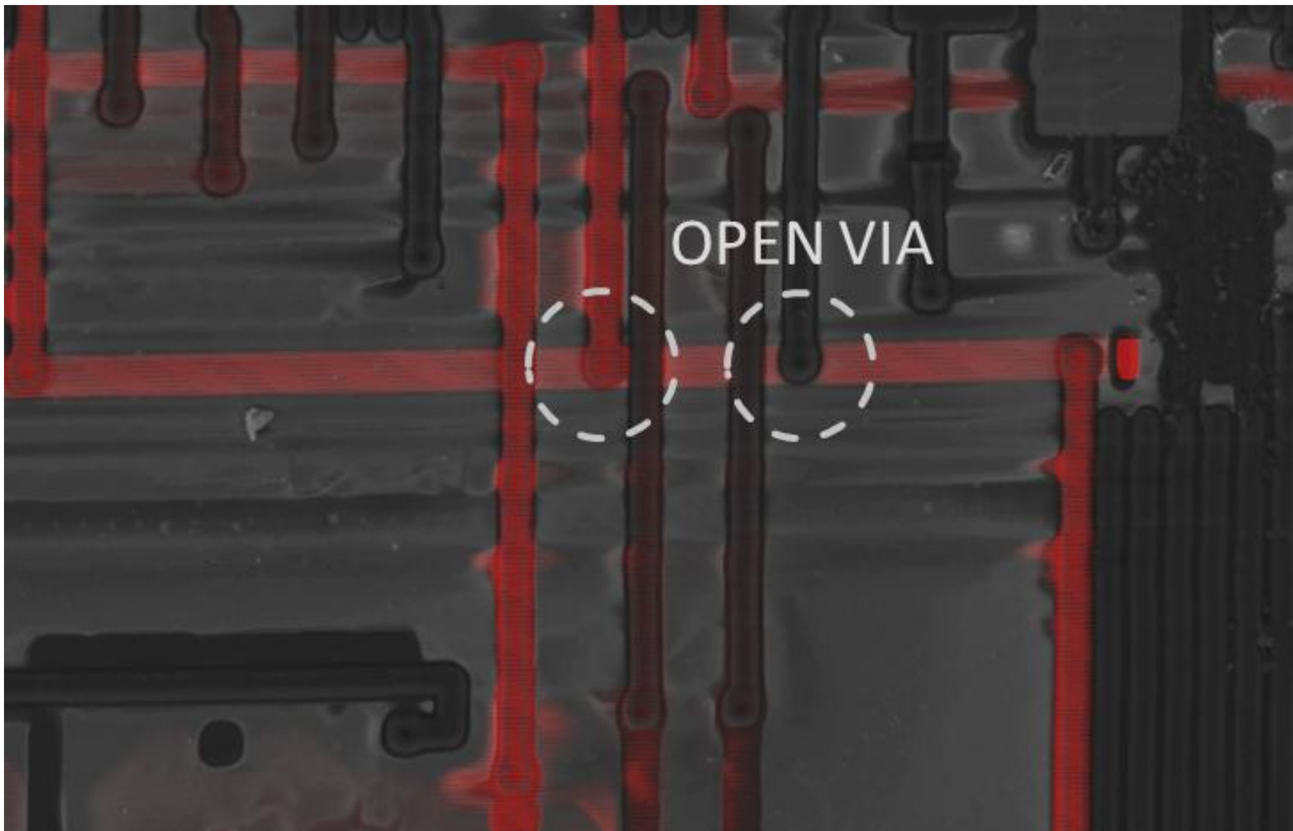


FICS Research

All Rights Reserved

Applications in Hardware Security

Find exact location of any open, resistive or shorting defect.



- Localize cuts caused by cracking, corrosion, electro-migration or particles.
- Identify resistive opens caused by interface contamination at vias.

FICS Research

All Rights Reserved

Applications in Hardware Security

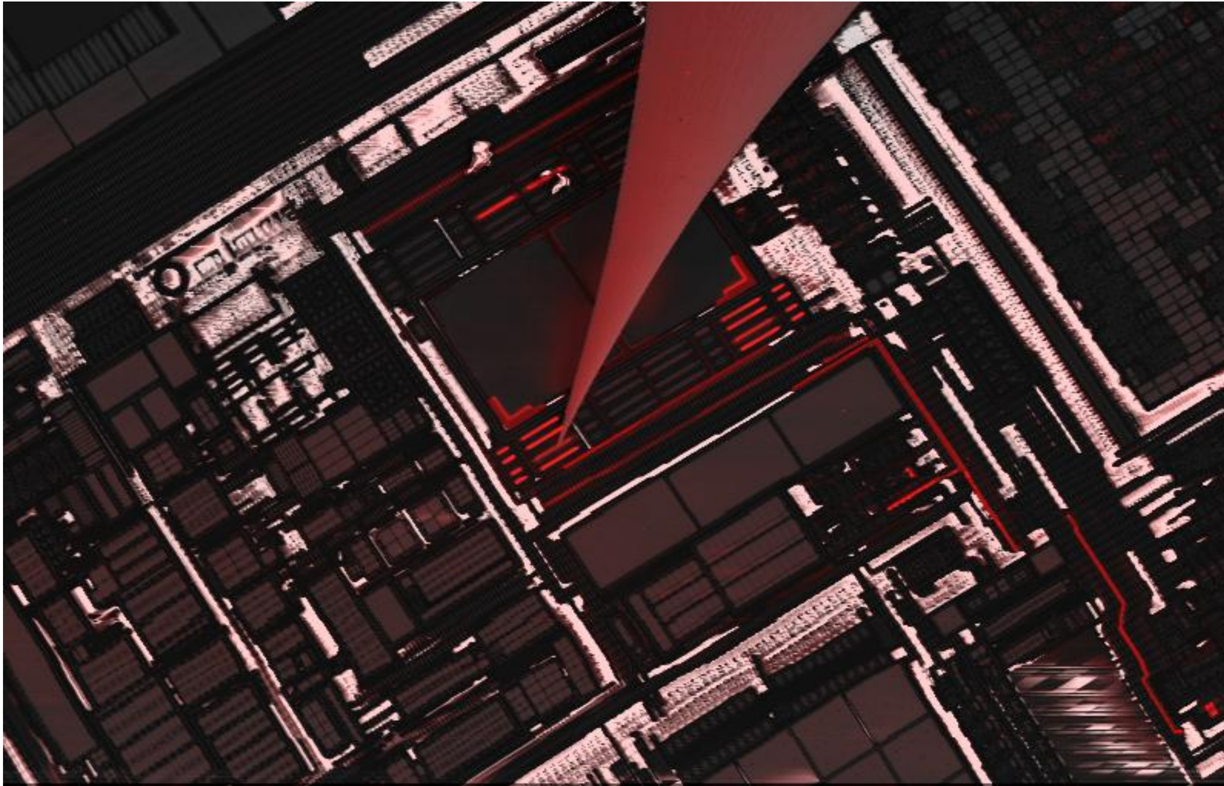
Characterize interconnects with the highest resolution.

- Reveal electrical integrity of nets with sub-micron resolution.
- Diagnose contamination, metal patterning defects, resistive interconnectors.
- Directly isolate defects to exact layer and die location.

All Rights Reserved

Applications in Hardware Security

Access failures invisible in voltage contrast



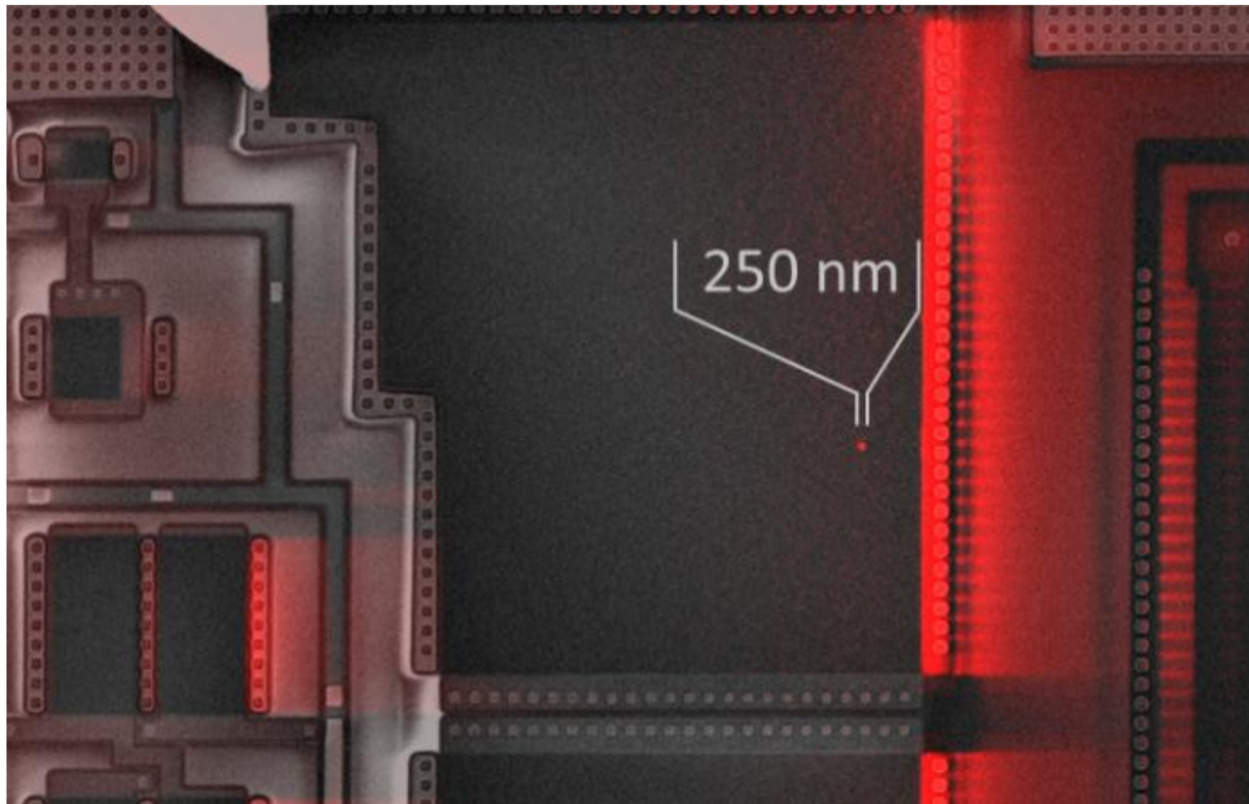
- Find low resistances that allow charge tunnelling through interconnects.
- Investigate structures in contact with the silicon substrate.
- Characterize large metal structures

FICS Research

All Rights Reserved

Applications in Failure Analysis

Localize defects in thin dielectric layers.



- Visualize weaknesses in GOX or COX before breakdown.
- Pinpoint oxide shorts caused by ESD or EOS with sub-micron resolution.
- Preserve the original defect with nW power dissipation during analysis.

All Rights Reserved

Needs in the Semiconductor

UNIVERSITY of FLORIDA

Technologies are shrinking

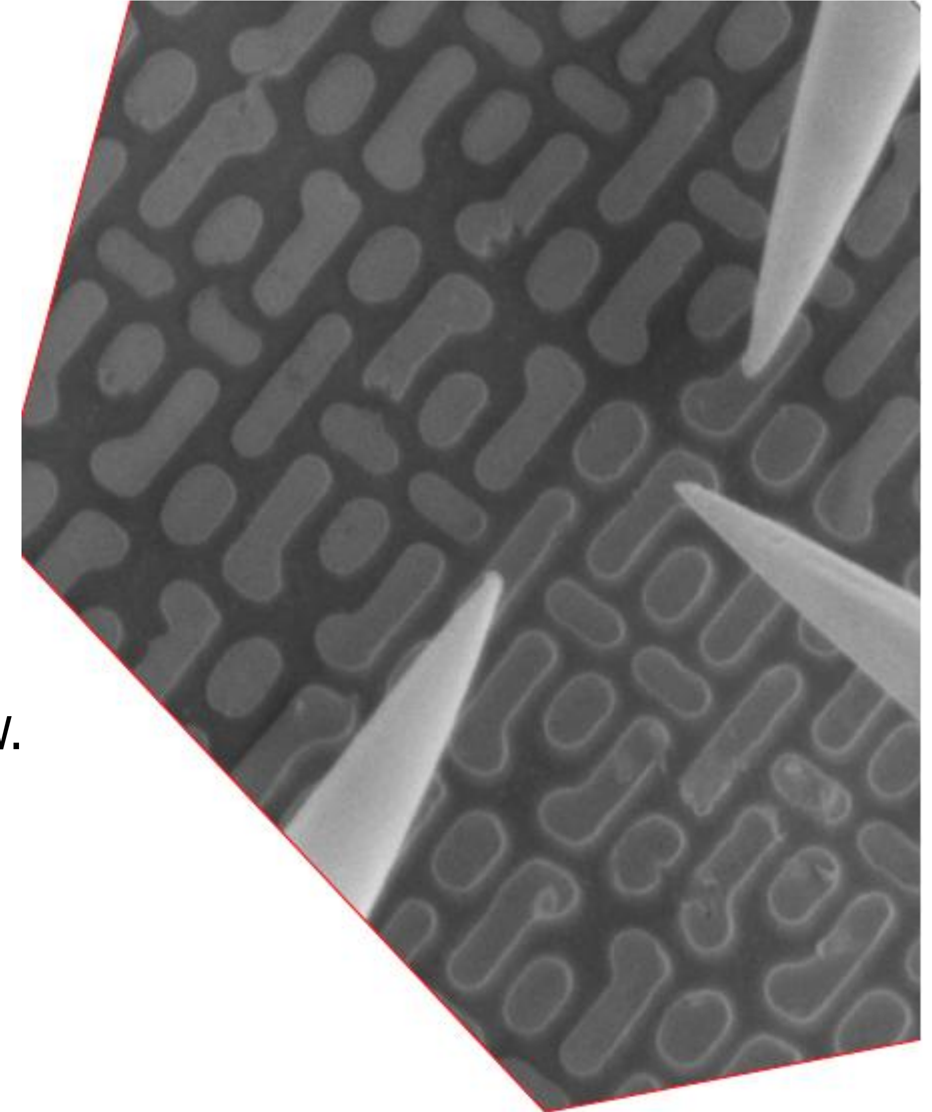
- Nanometer resolution for a precise positioning
- High mechanical stability for steady electrical contacts
- Adapted probes materials and tip radius.

Architectures are becoming complex

- Versatile configuration for a quick adaptation
- Software assistance to guide the operator within the workflow.

Data collection time is limited

- Fast system installation
- Reporting capabilities



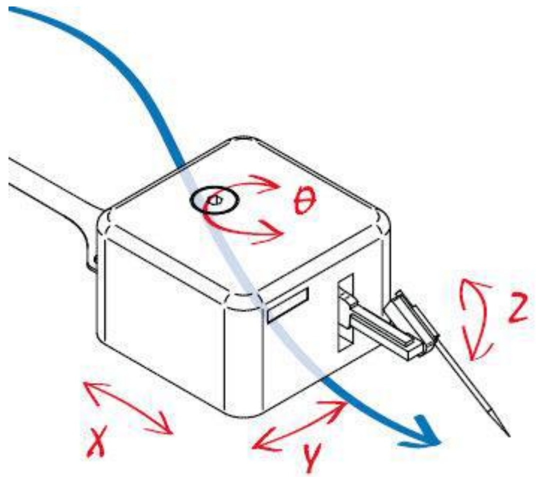
FICS Research

All Rights Reserved

Core technology: a mobile piezo robot

UNIVERSITY of FLORIDA

Axis of movement



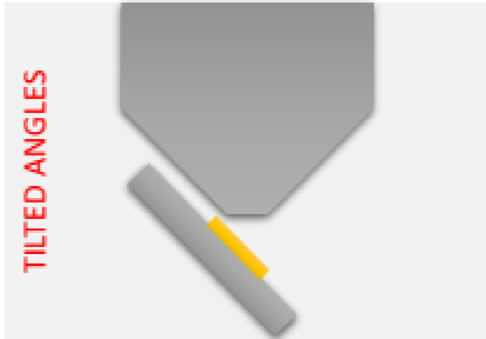
- Micro to nanometer positioning resolutions
- Centimeter range displacements
- High mechanical stability and near-zero drift
- Freely moving on their stage. Maintained on it with a magnet
- XYZ and rotation movements
- High vacuum compatible
- Can be adapted to different sample size and applications

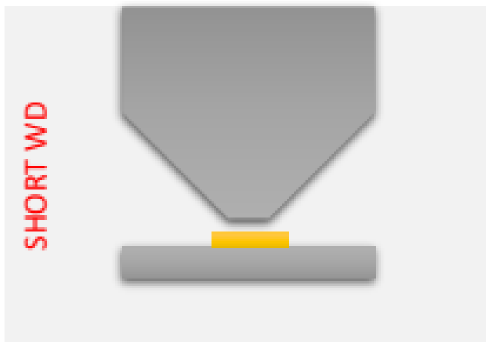
FCS Research

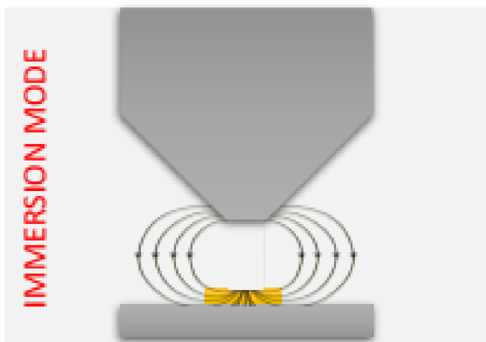
All Rights Reserved

Nanoprobing Platform

UNIVERSITY of FLORIDA







Independent & shielded cabling for excellent signal-to-noise ratio and low-current measurements.

From 1 to 8 independent nanoprobers

Integrated biasing of the sample

Wide range of industry standard probes materials and tip radius

Large and multiple samples with adjustable height for the work at short working distances and low acceleration voltage

Compact and light platforms, compatible with load-lock systems

FICS Research

All Rights Reserved

Basic Operation Voltage Range

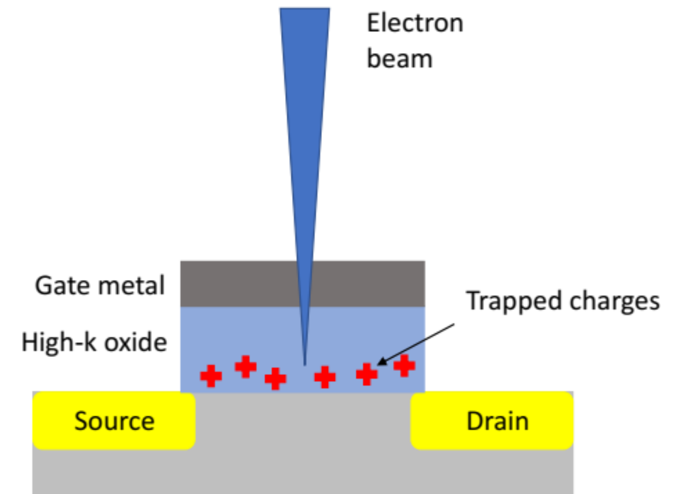
Oxide material sensitive to electron beam:

- Generation of oxide trapped holes.
- Trap generation at the interface.

Results in:

- Shift of the Threshold voltage.
- Increase of leakage current.

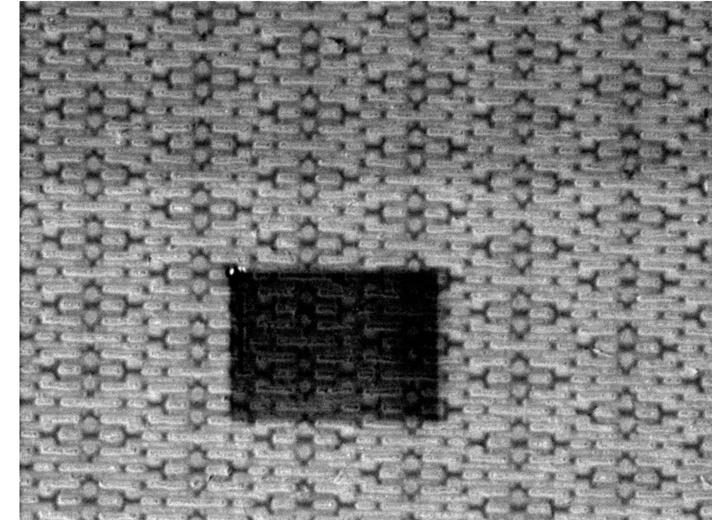
Therefore, it is required to image at low KV to avoid changing transistor characteristics. (typically 500V to 1kV depending on technology).

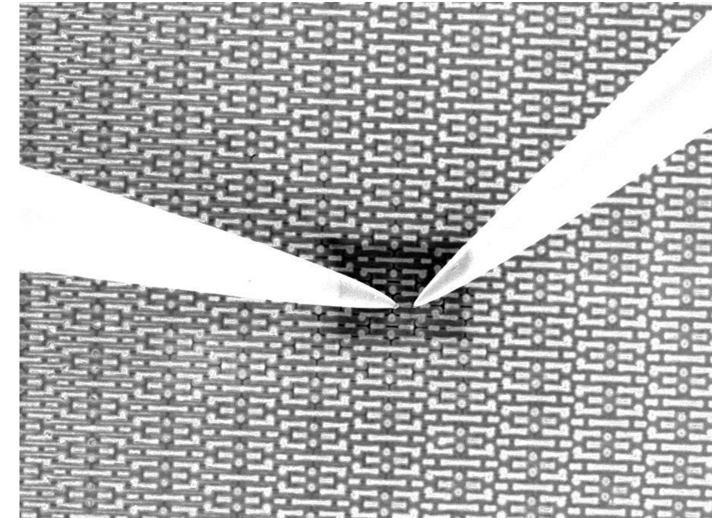


All Rights Reserved

Challenges

UNIVERSITY of FLORIDA





Hydrocarbon contamination

- Inside the chamber
- From outside, when installing new probes, sample, etc.

Contamination has consequences on:

- Imaging quality
- Electrical contact

Suggestions:

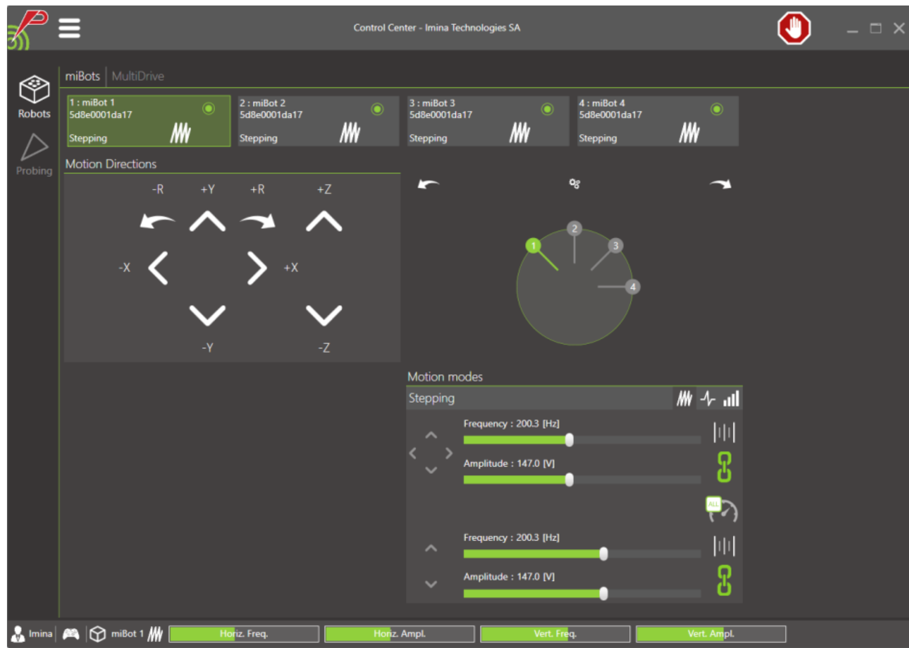
- Store the system in a safe environment.
- Use a plasma cleaner to remove hydrocarbon contamination.

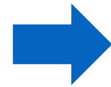
FICS Research

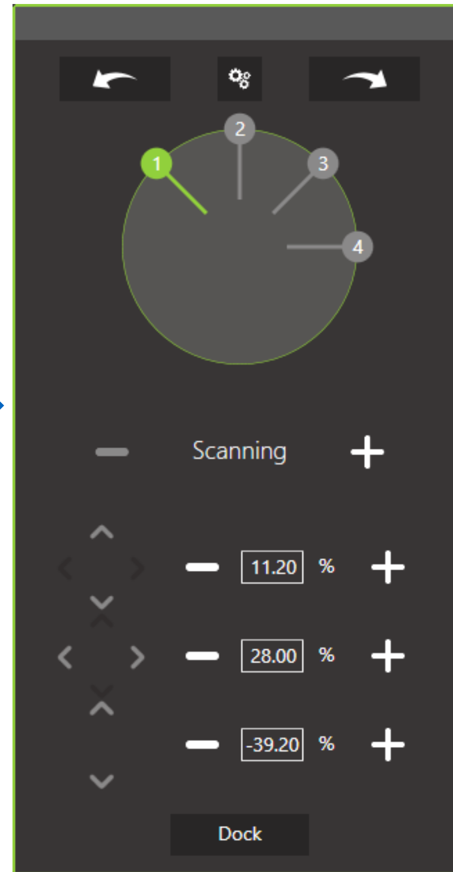
All Rights Reserved

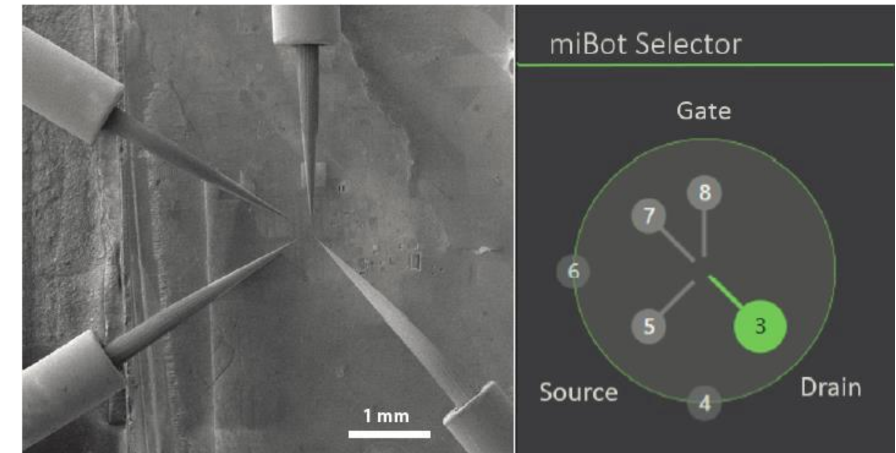
Control Center and Probes Approach

UF UNIVERSITY of FLORIDA







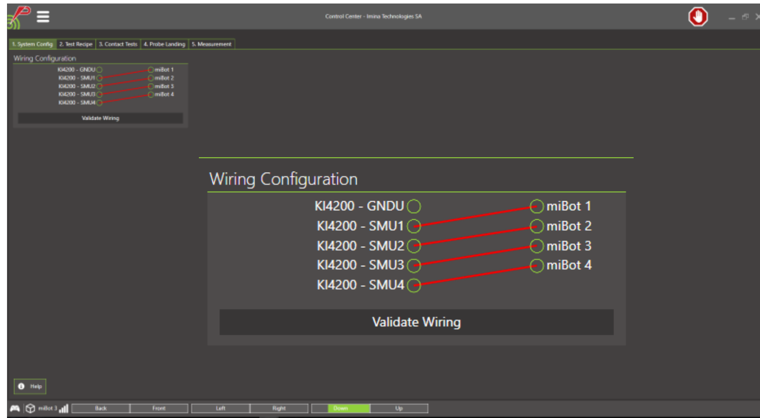


FCS Research

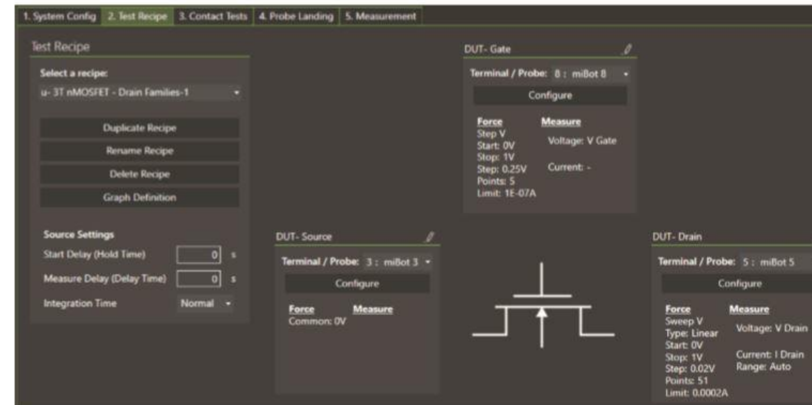
All Rights Reserved

Steps involved in electrical probing

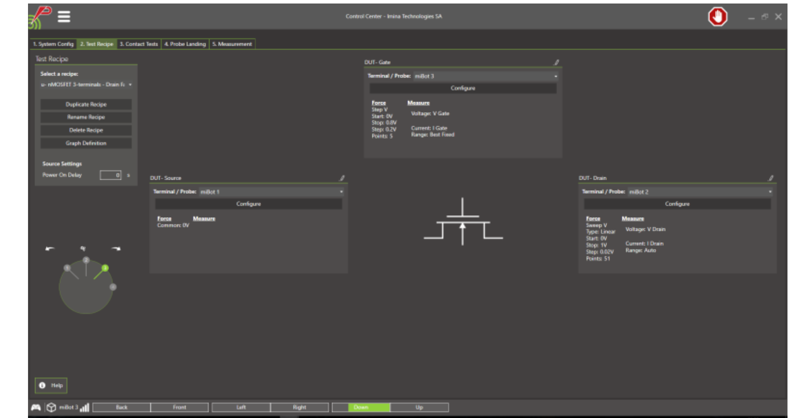
UF UNIVERSITY of FLORIDA



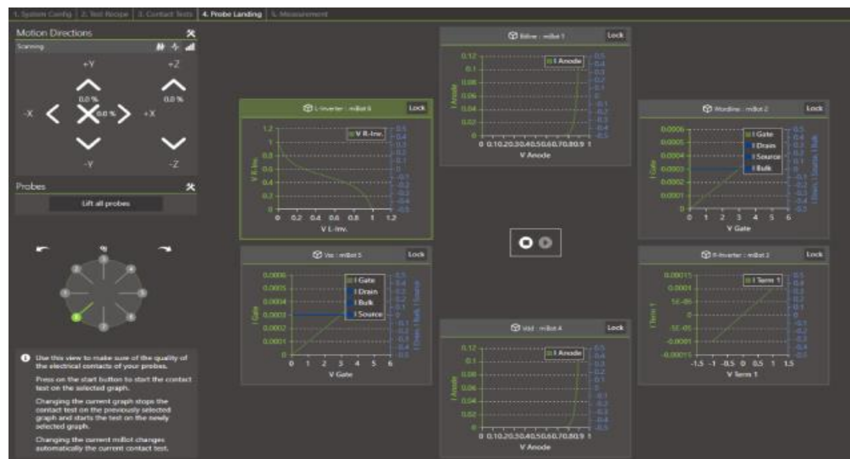
1: System configuration



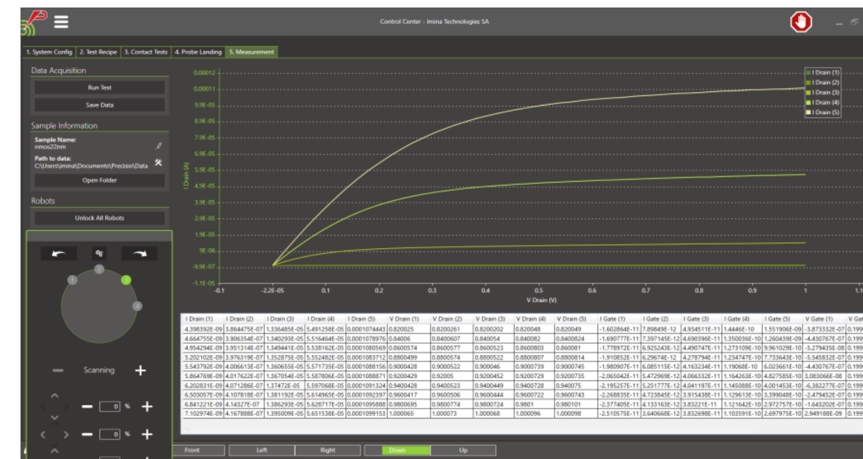
2: Test Recipe



3: Probe Landing



4: Live Contact Testing

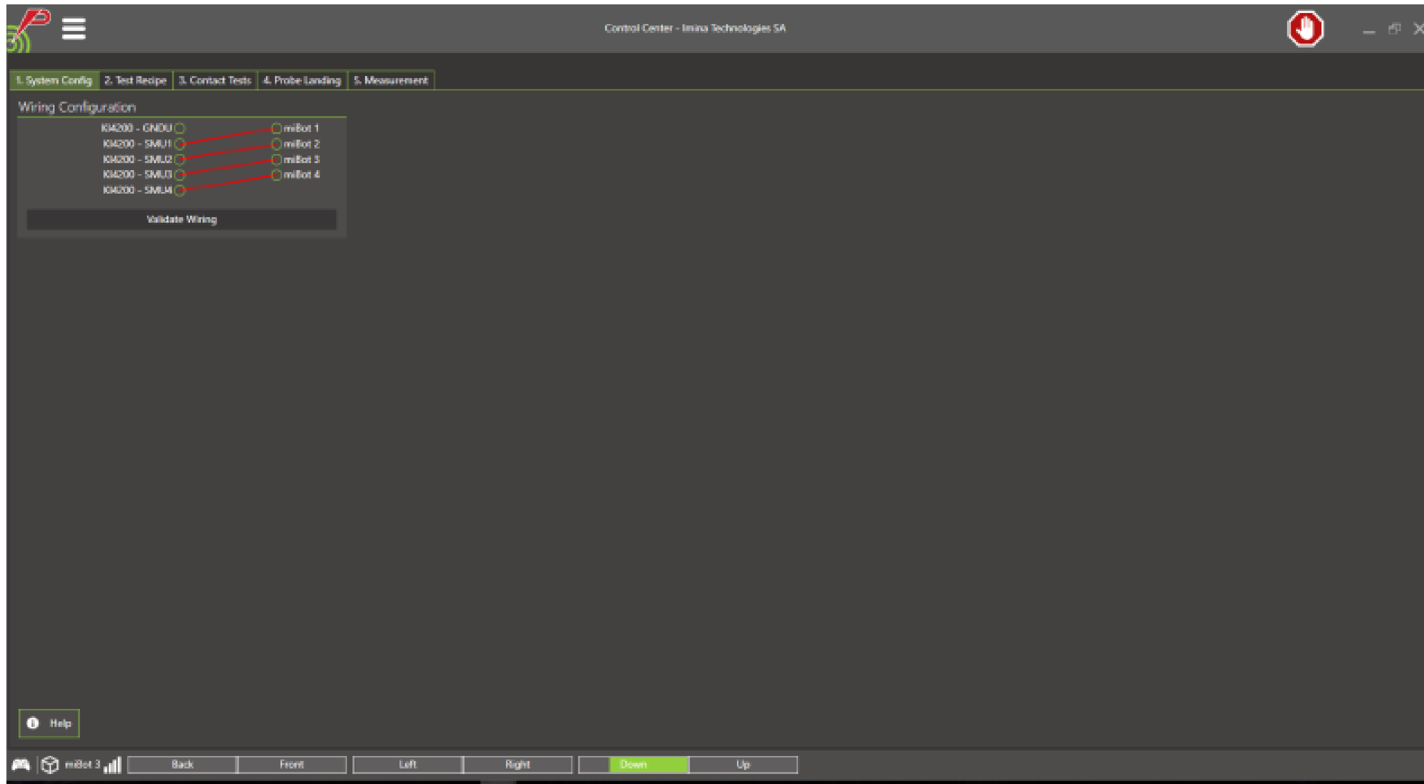


5: Measurement & Report

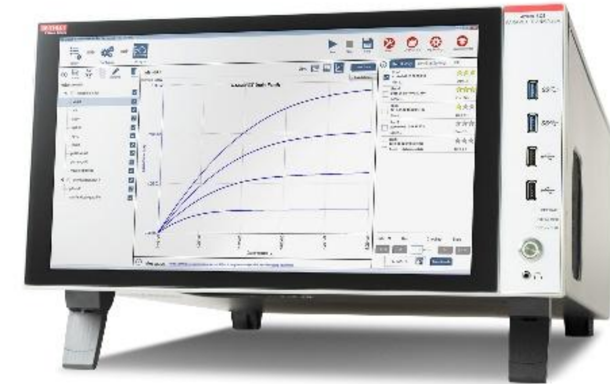
FICS Research

All Rights Reserved

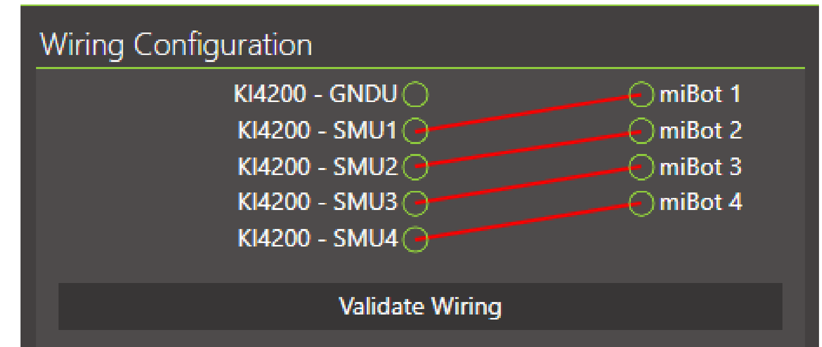
Steps involved in electrical probing



1: System configuration



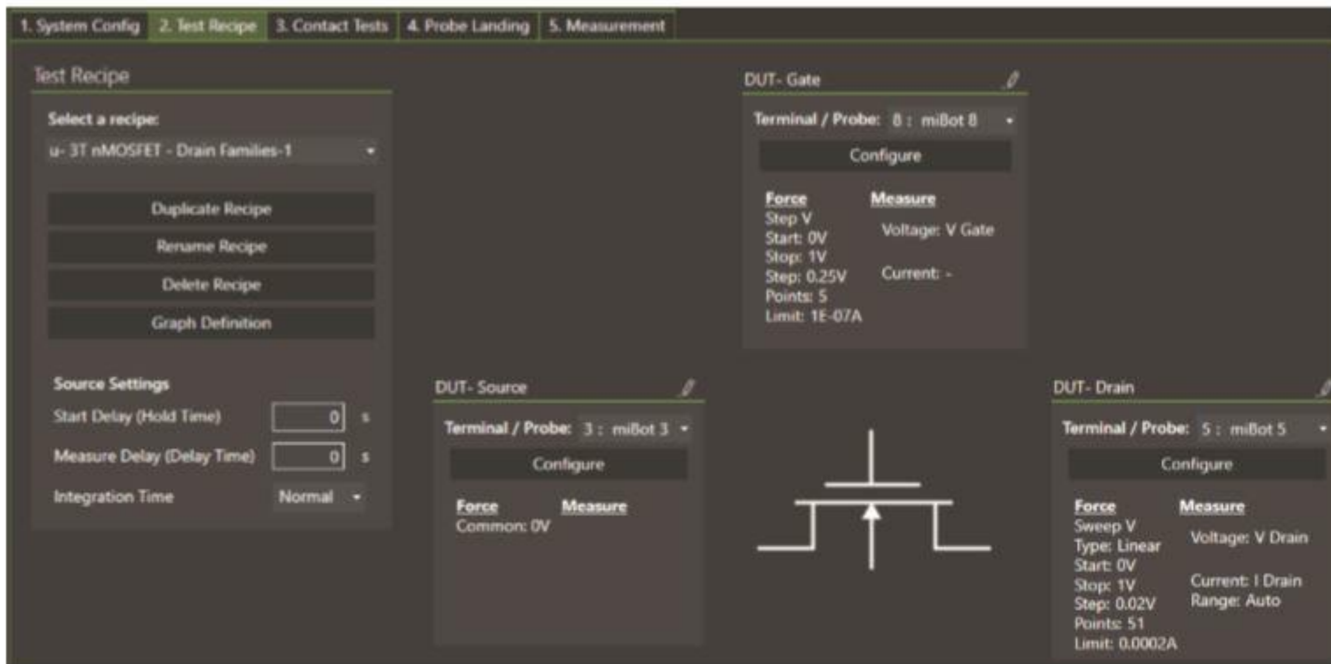
Keithley 4200SA Parameter Analyzer



FICS Research

All Rights Reserved

Steps involved in electrical probing

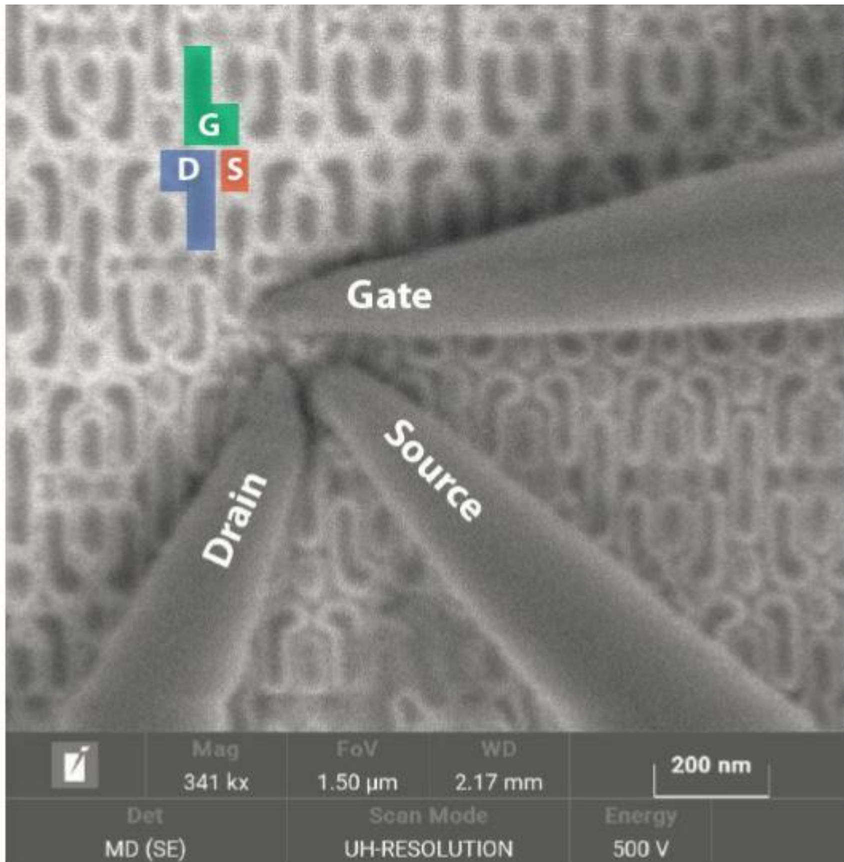


2: Test Recipe

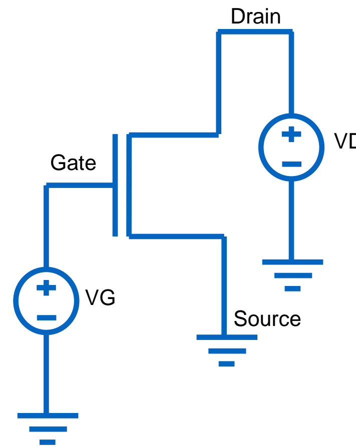
- Predefined test recipes for NMOS and PMOS transistor characterization can be selected.
- Their parameters such as the current compliance, current and voltage range, and number of test points are tuned based on the theoretical properties of the DUT (Device under Test).
- The device used in this case is 3T-nMOSFET.

All Rights Reserved

Steps involved in electrical probing



3: Probe Landing



- The probes tips are then sequentially lowered down in contact with each transistor node.
- Switching from one prober to another and adjusting their speed and positioning step size was intuitively done using the control pad.
- Once all probes had touched down, the beam was deflected away from the test area to avoid affecting electrical measurements.

FICS Research

All Rights Reserved

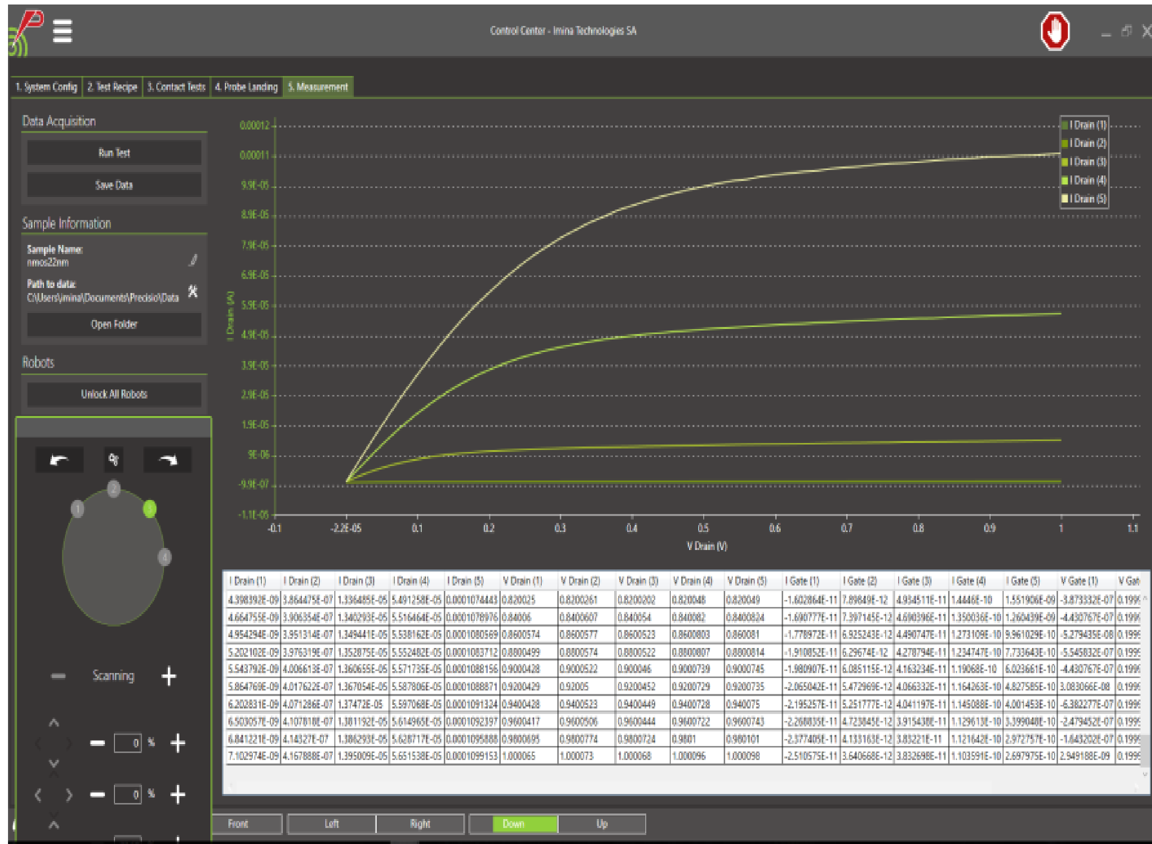
Steps involved in electrical probing

4: Live Contact Testing

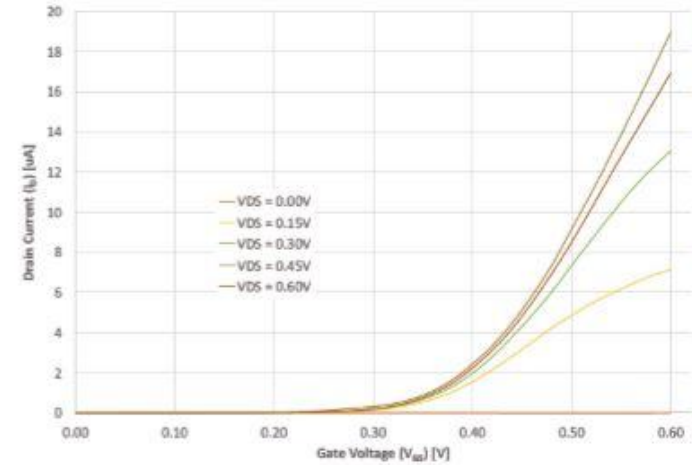
- Precisio™ contact test module was then used to quickly check the quality of electrical contacts by repeating fast measurements.
- When required, probes position was slightly adjusted until measured curves become characteristic of the DUT.

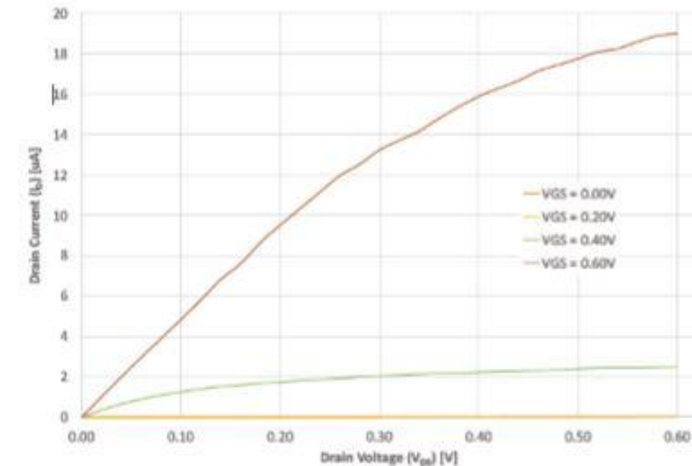
All Rights Reserved

Steps involved in electrical probing



5: Measurement & Report





NMOS transistor characteristics
(Top) Drain current vs Gate-Source voltage sweep
(Bottom) Drain current vs Drain-Source voltage sweep.

All Rights Reserved

Steps involved in electrical probing

5: Measurement & Report

- Before starting the characterization of transistors, leakage current of each channel was measured when probes were not in contact with the DUT. It was lower than 200 fA on all channels.
- The test recipes for this device were configured with a current compliance on ID and IS set to 100 mA. The Drain and Gate voltage sweeps were made in 31 steps of 0.02 V. The Drain and Gate voltage bias were made in 4 steps of 0.20 V.
- The transistors were characterized by measuring the Drain current ID when sweeping Drain-Source voltage VDS at different Gate-Source voltages VGS (ID=f(VDS)) and when sweeping Gate-Source voltage VGS for different Drain-Source voltages VDS (ID=f(VGS)).
- Source current IS and Gate current IG are also measured.

All Rights Reserved