FREUD Methods

FIB Invasive Attacks and Countermeasures

Valery Ray
vray@partbeamsystech.com

USE-IT 2007, Toulouse France
Functional Reverse Engineering of Undocumented Devices (TM)

Extraction of functionality and data without full reverse-engineering of manufacturing process
Outline

- Workflow of FIB process
- Signal extraction and injection, RC issues
- Limitations of existing FIB technology
- Countermeasures to FIB methods
Workflow of “FIB invasion”

- Layout capture and location of nodes
- Navigation and positioning
- Bypassing protective shields, if needed
- Making contacts and extracting data
Layout Capture and Node Location

Alignment Reference

Data Nodes
FIB Navigation to Nodes

- Must be done by coordinates – shield prevents direct navigation with optics;

- Have to use sacrificial device for locating nodes, two devices for small-linewidth shielded ICs;

- Two steps of localization – coarse and precise;
Coarse Navigation on Sacrificial Device (s)

- Stage coordinate conversion OM to FIB
- Laser mark in OM – find mark in FIB
- Scan bitmap, stitch, locate nodes, convert bitmap to FIB stage coordinates
References and Nodes in FIB

Use alignment references for navigation and deprocess nodes to capture position.
Navigation with Local Alignment

- Accuracy of FIB stage is limited – how to navigate on small-linewidth devices?
- Shield is preventing optical navigation
- Use reference points for coordinate navigation
- Use protective shield as your local reference!
Electrically Bypassing Shield

- Bypass protective shield locally
  - Works on analog and digital shields
  - One or two lines may need bypassing per contact
  - Takes 30 to 120 min. of FIB time per contact

- Bypass entire shield
  - Best for analog shields
  - Takes 30 to 120 min. of FIB time per device
  - Requires follow up by non-FIB techniques
Shield Disabling

- Disable shield control circuitry
  - Requires detailed analysis of layout
  - Simulate “OK” shield on input of circuitry
  - Simulate “OK” output (no interrupts, alarms, etc…)

- Disable “NOK” actions
  - Requires detailed analysis of layout
  - Cut output of charge pump – disable flash erase!
  - Cut “security interrupt” nodes
Making Contacts and Pads

Create HAR vias to connect to the nodes and deposit contact pads for probing.

Clean overspray of metal depo.
Data Extraction

- Connect contact pads to data acquisition equipment by microprobing
- Ensure proper buffering of the connection lines – internal nodes can’t drive 100pF cable
- Use ultra-low capacitance buffers for glitch recovery
Signal injection

- Injection of impulses into data bus can alter execution of embedded code

- Basic application: disrupt end of loop command during ATR – data memory could be extracted

- Suitable buffers are not available from OEMs – design and build your own!
Limitations of existing FIB technology

- Accuracy of navigation
  - Targeting multiple nodes on <150nm devices without local reference is unreliable

- Aspect ratio of contacts
  - Detection of endpoint on contacts deeper than 20:1 depth/width is very difficult

- Linewidth (technology node) limitations
  - Making deep contacts smaller than 150 nm is a high art and done very slow
Countermeasures against FIB

- FIB attacks are high-cost effort and can be made uneconomical:
  - Planarize devices and use small linewidth
  - Thick copper metal shield difficult to cut
  - Use Liquid Crystal Polymer passivation
  - Use leakage-sensitive analog shields and double shield layers
Summary

- FREUD by FIB methods can’t be prevented, but can be made uneconomical

- Basic countermeasures are relatively inexpensive in manufacturing – planarize devices, use thick copper plate in addition to active shield

- Advanced countermeasures become viable as cost of IC manufacturing is reduced: active double-shielding, Liquid Crystal Polymer passivation
www.partbeamsystech.com