



INSIDE TECHNOLOGY

The state-of-the-art in Semiconductor Reverse Engineering at Chipworks

Randy Torrance
9th September 2009

Agenda

- About Us
- The What and Why of Reverse Engineering
- Product Teardowns
- System Analysis
- Process Analysis
- Circuit Analysis
- Putting it all together: A Case Study



Chipworks

- Chipworks is a reverse engineering services company, based in Ottawa, Canada, with offices around the world providing semiconductor companies with:
- Technical Intelligence to engineers and business unit managers to give you a technical view of your competition.
- Patent Intelligence to IP groups and law firms providing technical intellectual property services to support licensing negotiations and patent portfolio development.



Reverse Engineering – What is it?

- In the semiconductor industry, reverse engineering (RE) can be:
 - Product Teardowns – what chips are used
 - System Analysis – how chips are used
 - Circuit Analysis – how chips work
 - Process Analysis – how chips are built, and what are they made of



Reverse Engineering - Is it legal?

Reverse Engineering is protected by the Semiconductor Chip Protection Act:

Title 17. Copy rights

Chapter 9. Protection of Semiconductor Chip Products

906. Limitations on exclusive rights; reverse engineering; first

- (a) Notwithstanding the provisions of section 905, it is not an infringement of the exclusive rights of the owner of a mask for –
- (1) A person to reproduce the mask work solely for the purpose of teaching, analyzing, or evaluating the concepts or techniques embodied in the mask work or the circuitry. Logic flow, or organization used in the mask work; or
 - (2) A person who performs the analysis or evaluation described in paragraph (1) to incorporate the results of such conduct in an original mask work which is made to be distributed



Why Reverse Engineer?

Patent Intelligence:

- To determine if others are infringing your patents
- To find prior art to invalidate others patents

Technical Intelligence:

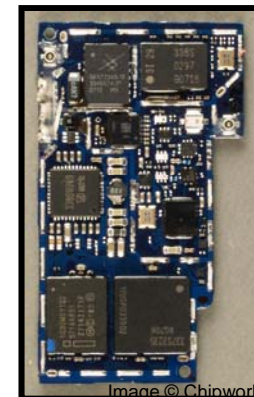
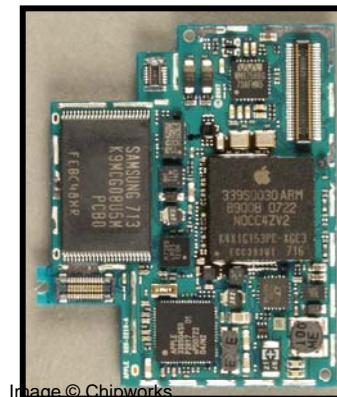
- To benchmark your designs versus your competitors
- To see new and innovative techniques
- To understand best practices

Verification:

- To understand how secure your own chips are

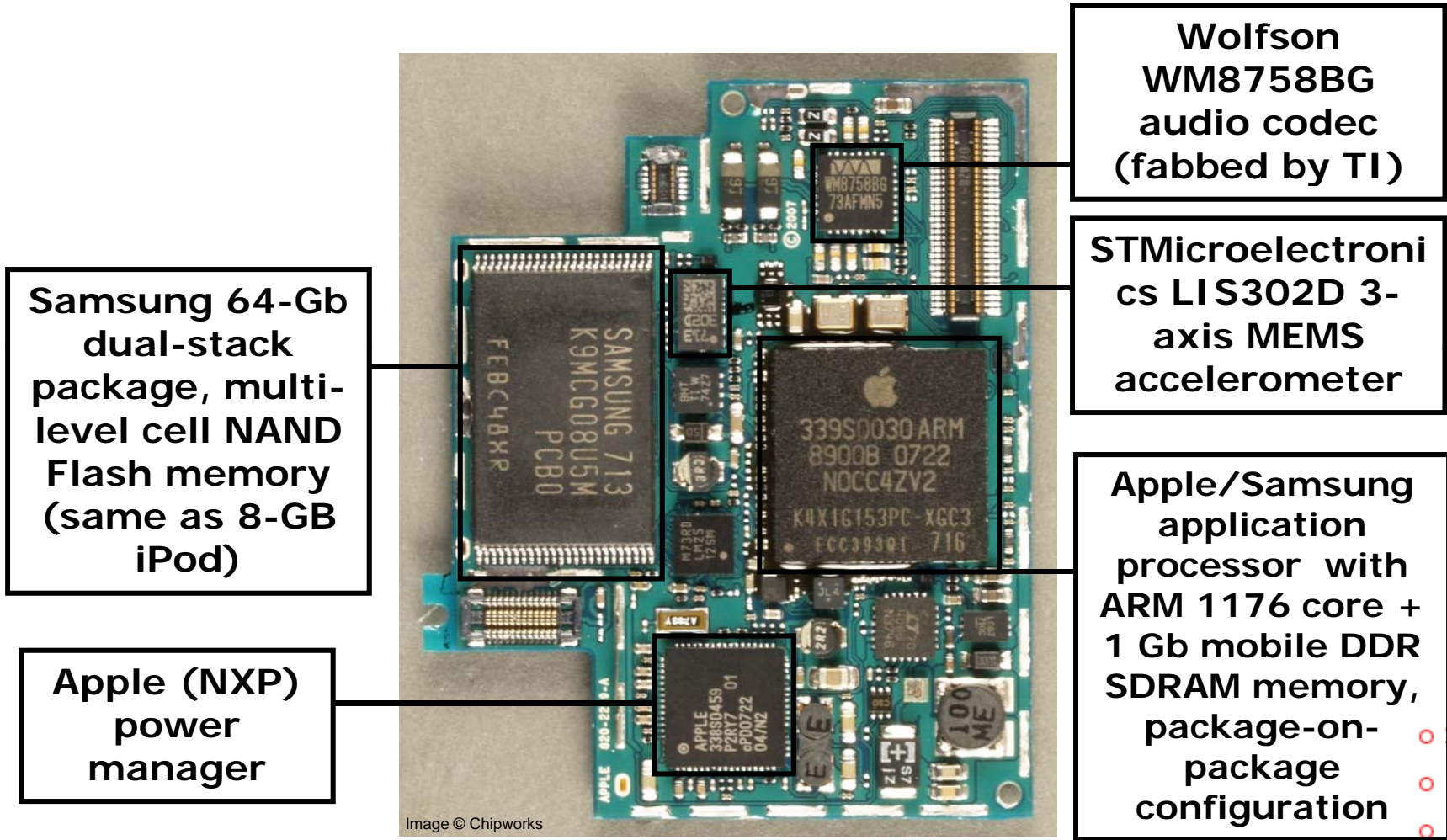
The Start to Reverse Engineering

Product Teardown – example: Apple's iPhone



iPhone Product Teardown - iPod board

INSIDETECHNOLOGY



Samsung 64-Gb dual-stack package, multi-level cell NAND Flash memory (same as 8-GB iPod)

Apple (NXP) power manager

Wolfson WM8758BG audio codec (fabbed by TI)

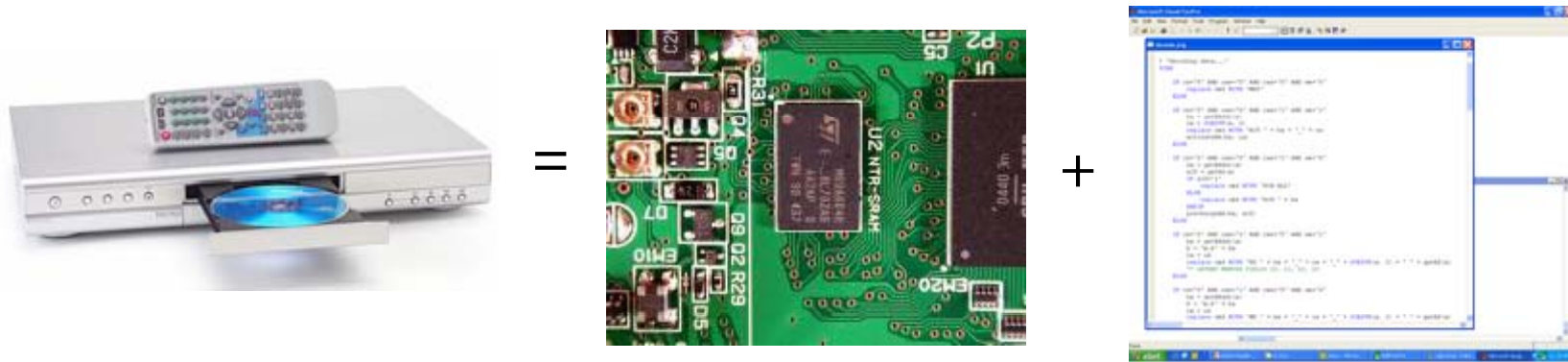
STMicroelectronics LIS302D 3-axis MEMS accelerometer

Apple/Samsung application processor with ARM 1176 core + 1 Gb mobile DDR SDRAM memory, package-on-package configuration

Image © Chipworks



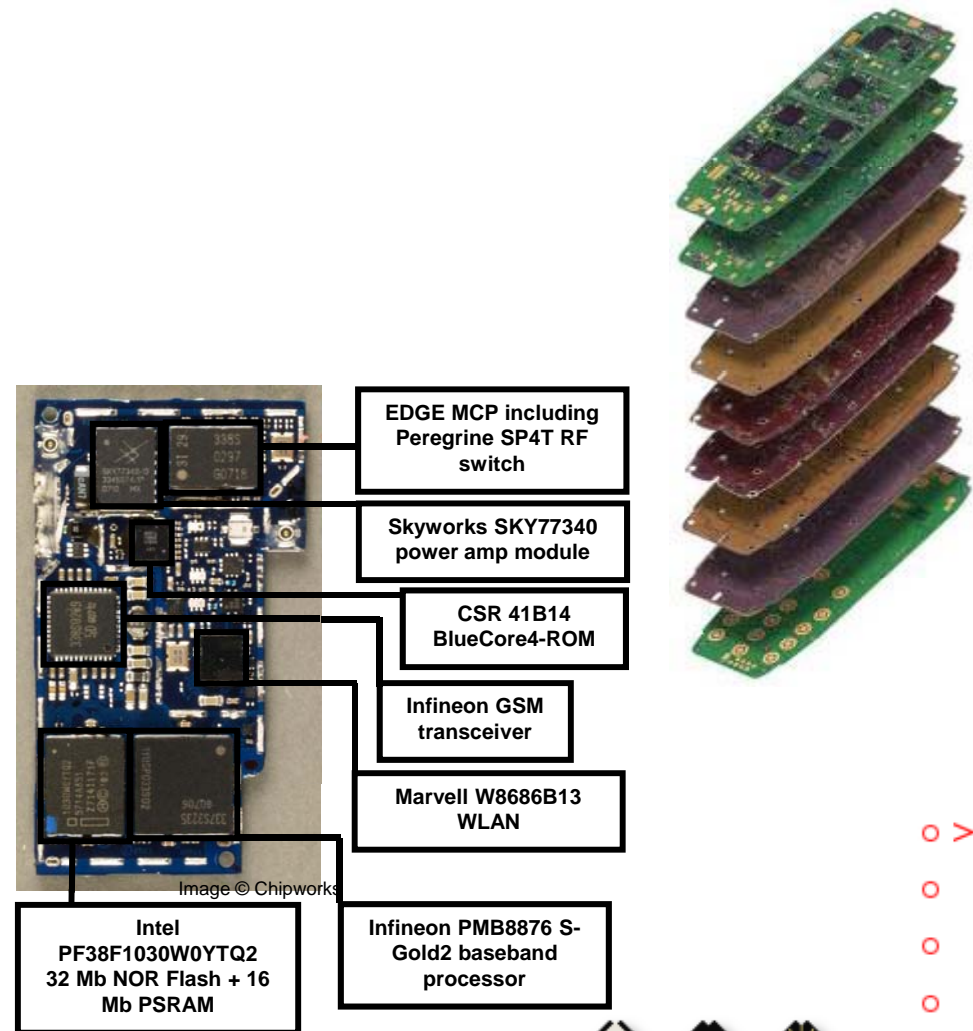
Types of System Analysis



- Hardware analysis:
 - Reverse-engineering at the physical circuit or board level
 - Functional analysis using test stimulus and monitoring outputs and internal signals
- Software analysis:
 - Software reverse engineering involves extraction and reconstruction of embedded code
 - Software functional analysis

System Analysis - Hardware Reverse Engineering

- **Teardown device**
 - Screwdrivers, etc
- **Identify components**
 - Datasheets, web, part number decoders
- **Remove components**
- **Delayer boards**
 - Delayering station
- **Trace connections**
 - ICWorks (our circuit analysis software)
- **Schematic capture**
 - ICWorks, Cadence



System Analysis - Hardware Functional Analysis

For example: Discover how a digital camera works in order to prove use of invention

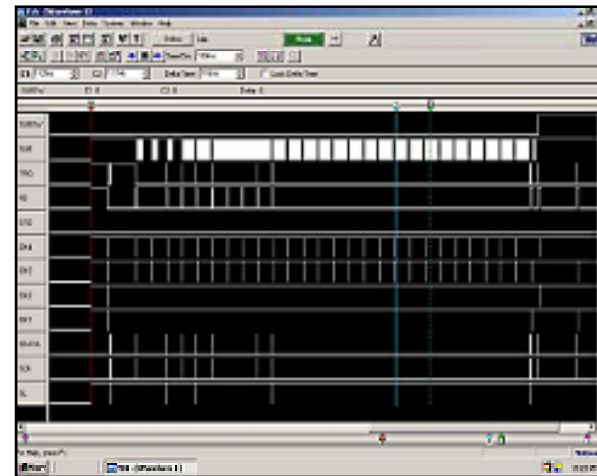
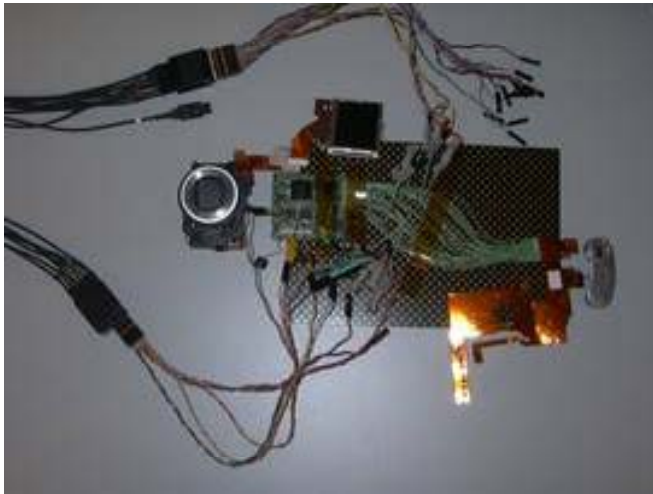


Examine patent...



...disassemble camera to get a dismembered but functioning camera...

System Analysis - Hardware Functional Analysis

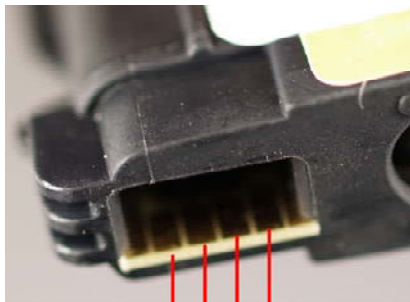


...connect probes
between the interfaces
and a logic analyzer...

...create testbench and test
vectors, test, collect
waveforms, study the
timing...

...and document the evidence

System Analysis - Software Reverse Engineering



SDA
VDD
SCL
VSS



```

00000000 | 68 F0 9F E5 00 00 A0 E3 64 10 9F E5 00 00 81 E5
00000010 | 00 00 E0 E3 5C 10 9F E5 00 00 81 E5 58 10 9F E5
00000020 | 00 00 81 E5 54 00 9F E5 D2 F0 21 E3 00 D0 40 E2
00000030 | 50 F0 21 E3 40 DF 40 E2 13 00 00 EB 00 00 A0 E3
00000040 | 00 10 A0 E3 C0 2D A0 E3 00 00 81 E5 04 10 81 E2
00000050 | 02 00 51 E1 FB FF FF 1A 24 10 9F E5 B0 00 D1 E1
00000060 | 20 20 9F E5 02 00 50 E1 0A 00 00 1A E3 17 00 EA
00000070 | 04 00 00 30 04 00 00 C8 14 F0 FF FF 1C F0 FF FF
00000080 | 00 30 00 00 F8 FF 07 30 AA AA 00 00 00 C0 9F E5
00000090 | 1C FF 2F E1 95 21 00 30 00 C0 9F E5 1C FF 2F E1
000000A0 | 77 1A 00 30 1D 1B 00 30 27 1B 00 30 00 00 00 00
000000B0 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000C0 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    
```

Binary

Disassemble
code...



```

for (nbreg=0; nbreg<2000000; nbreg++){
    asm ( "addl %eax, %edi" );
}

asm(
    "push %ecx \n\t"
    "push %eax \n\t"
    "push %edx \n\t"
    "cli \n\t"
    "mfence \n\t"

    "movl $0x0,%ecx \n\t"
    "movl $0x01080000,%edx \n\t"
    "movl $0x005aa55,%eax \n\t"
    mem_write
    mem_inc
    mem_write
    mem_inc
    mem_write
    mem_inc
    mem_write
    mem_inc
    "movl $0x02080000,%edx \n\t"
    "movl $0x00a55aa,%eax \n\t"
    "movl $0x0,%ecx \n\t"
    mem_write
    
```

Assembler

Extract code...

```

for addr=0 to 255 {
    Start_Condition
    Slave_Address ( 0xBF )
    Wait_for_ACK
    Word_Address ( addr )
    wait_for_ACK
    Read_Data
    Stop_Condition
}

;issue start condition
;send slave address to the EEPROM, LSB=1 for read
;wait for acknowledge
;send word address to the EEPROM
;wait for acknowledge
;read 8-bit data at address addr
;issue stop condition
    
```

'C-like' Code

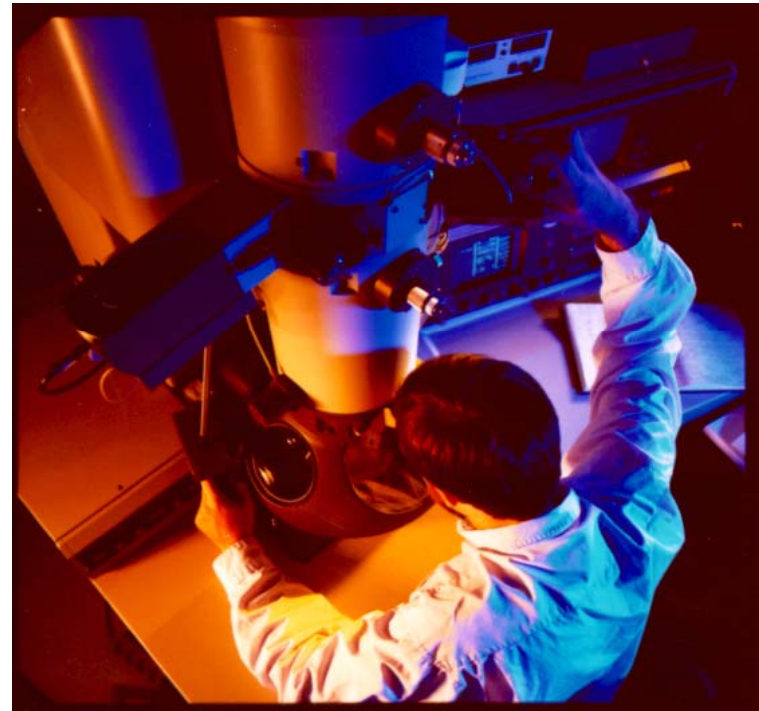


Decompile code...



Process Analysis

- Look at the structure of a chip
- Identify the chemical make-up of the structure
- Estimate the process sequence



The "Rules" of Process RE

- We see what we see!
- We can't see everything we want to see
- Sometimes we don't know what we see!
- Sample preparation isn't perfect – it can create confusing artifacts
- What we see doesn't always agree with corporate marketing hype
- SEM/TEM calibrations are NIST/NPL traceable and +/- 5% accurate

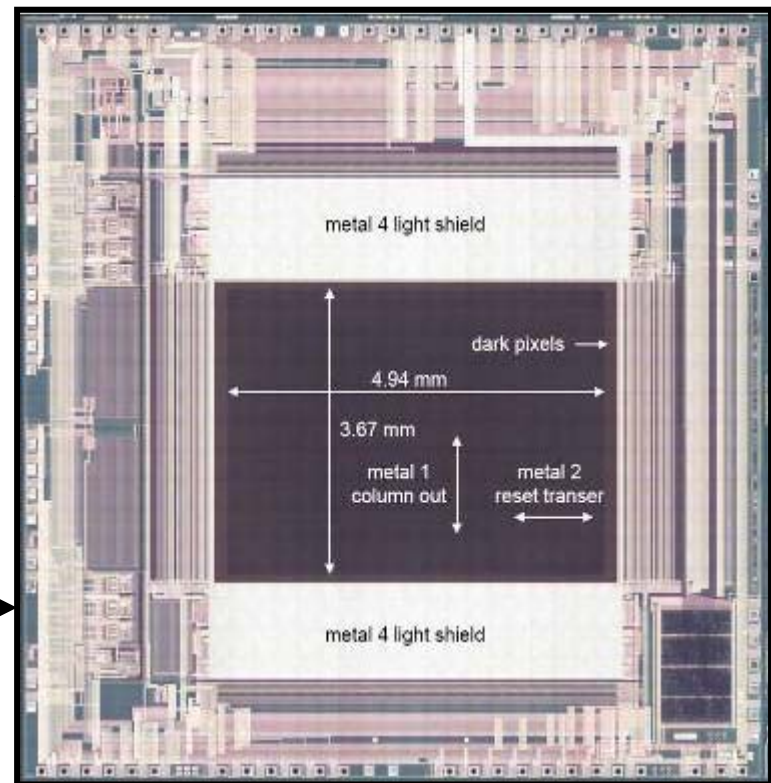
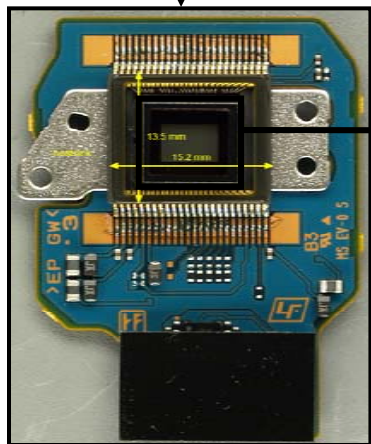


Process Analysis – Sony's Clearvid IMX013 4-Mpixel CMOS Image Sensor

Extracted from Sony DCR-DVD505 Handycam

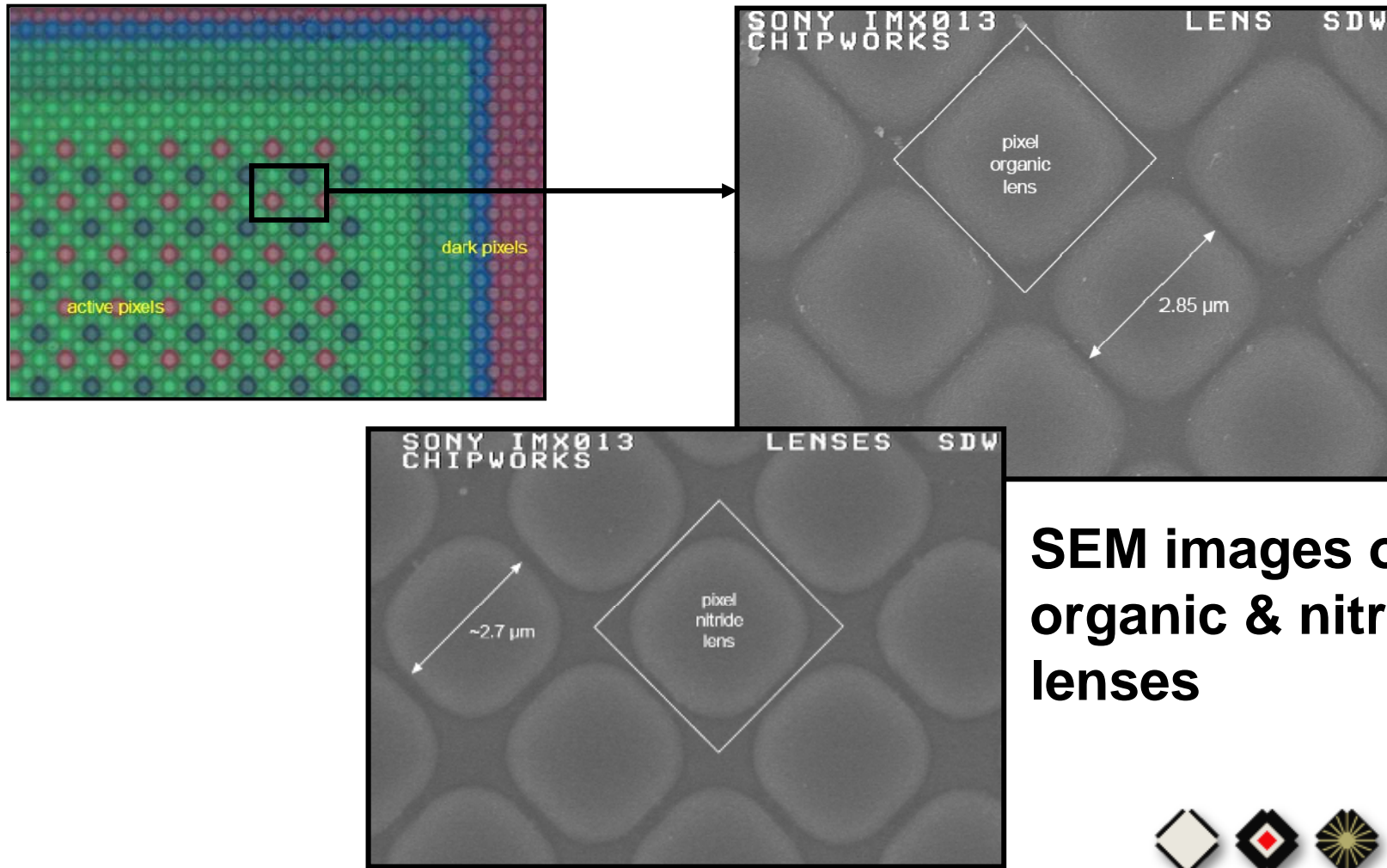


Sensor module



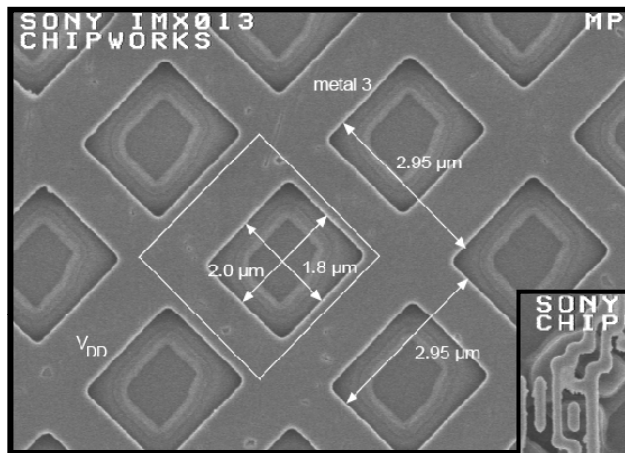
Die photo

Process Analysis – IMX013 Pixel Array – Plan View

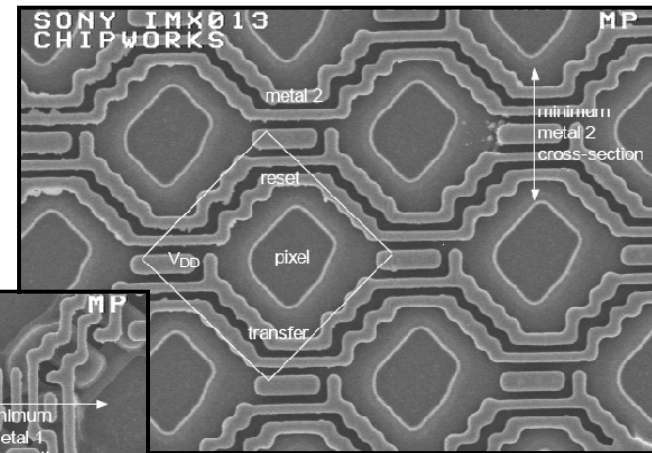


SEM images of organic & nitride lenses

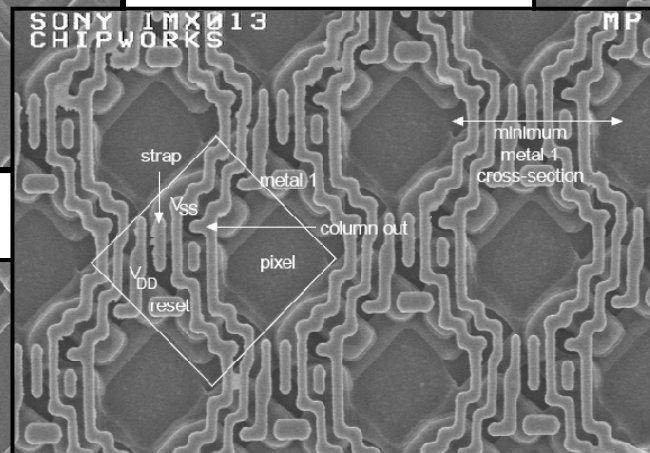
Process Analysis – IMX013 Pixel Array – Plan View



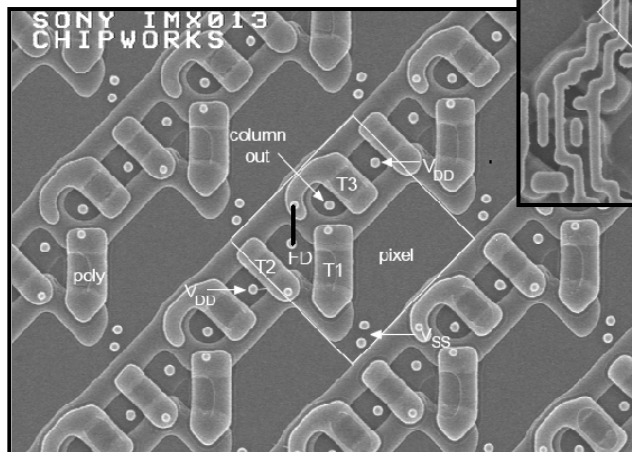
Metal 3



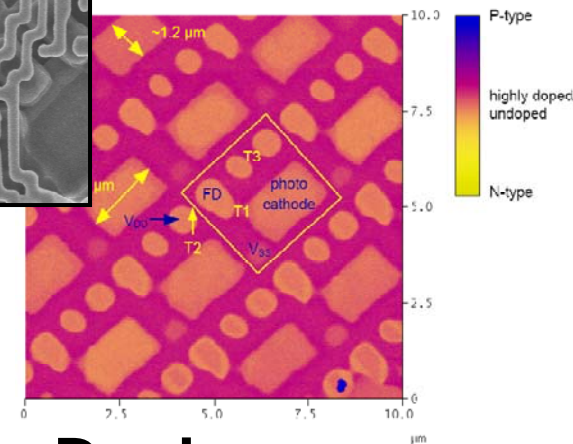
Metal 2



Metal 1



Transistors

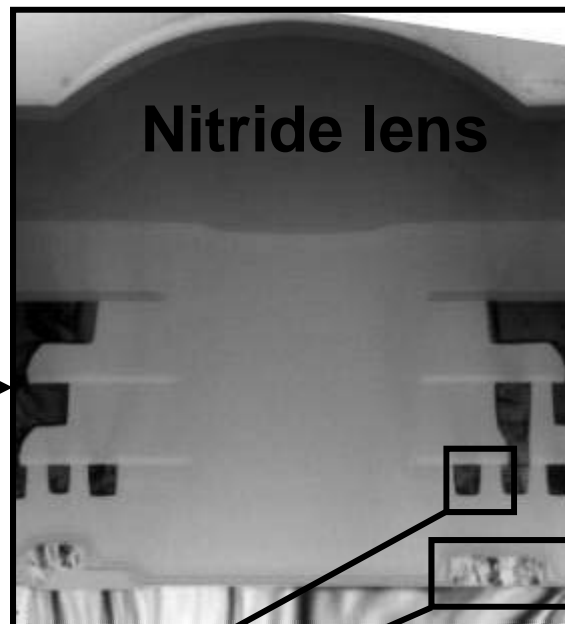
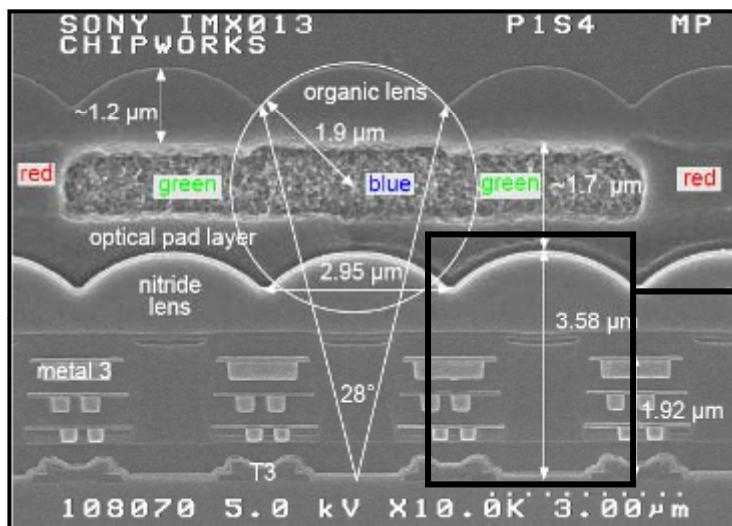


Substrate Doping (SCM)

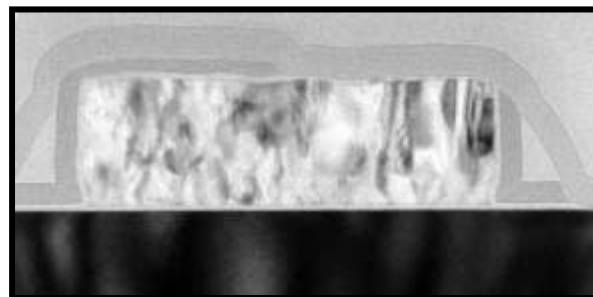
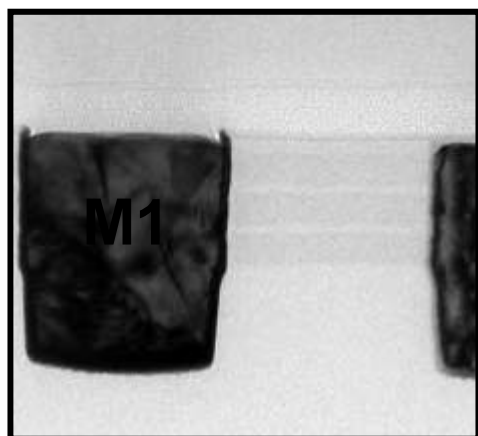
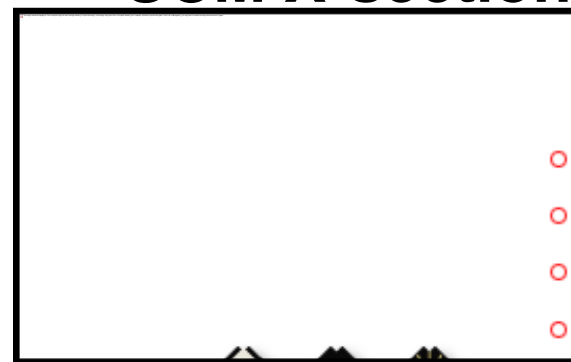


Process Analysis – Cross-Section of Pixel Array

SEM

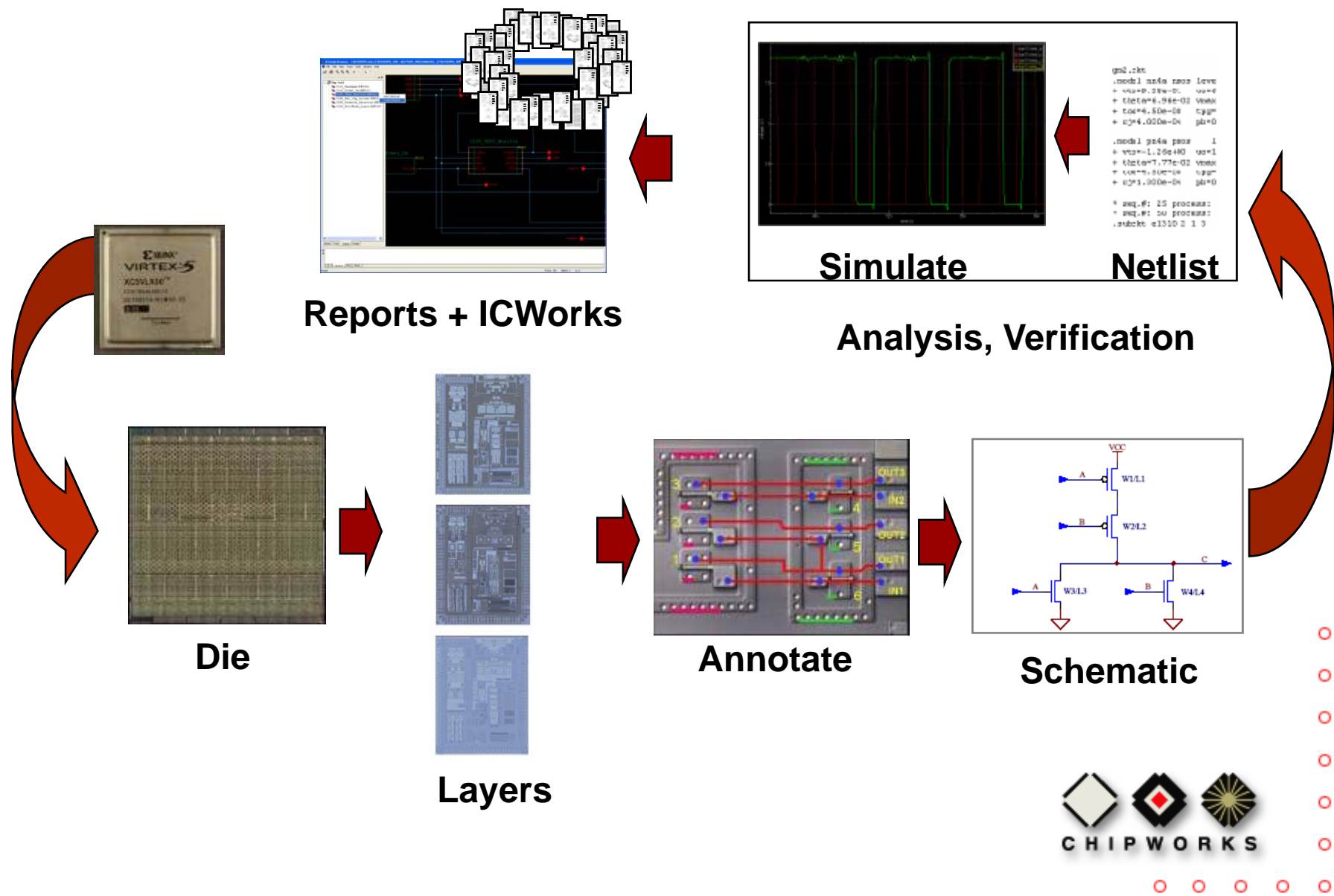


SCM X-section

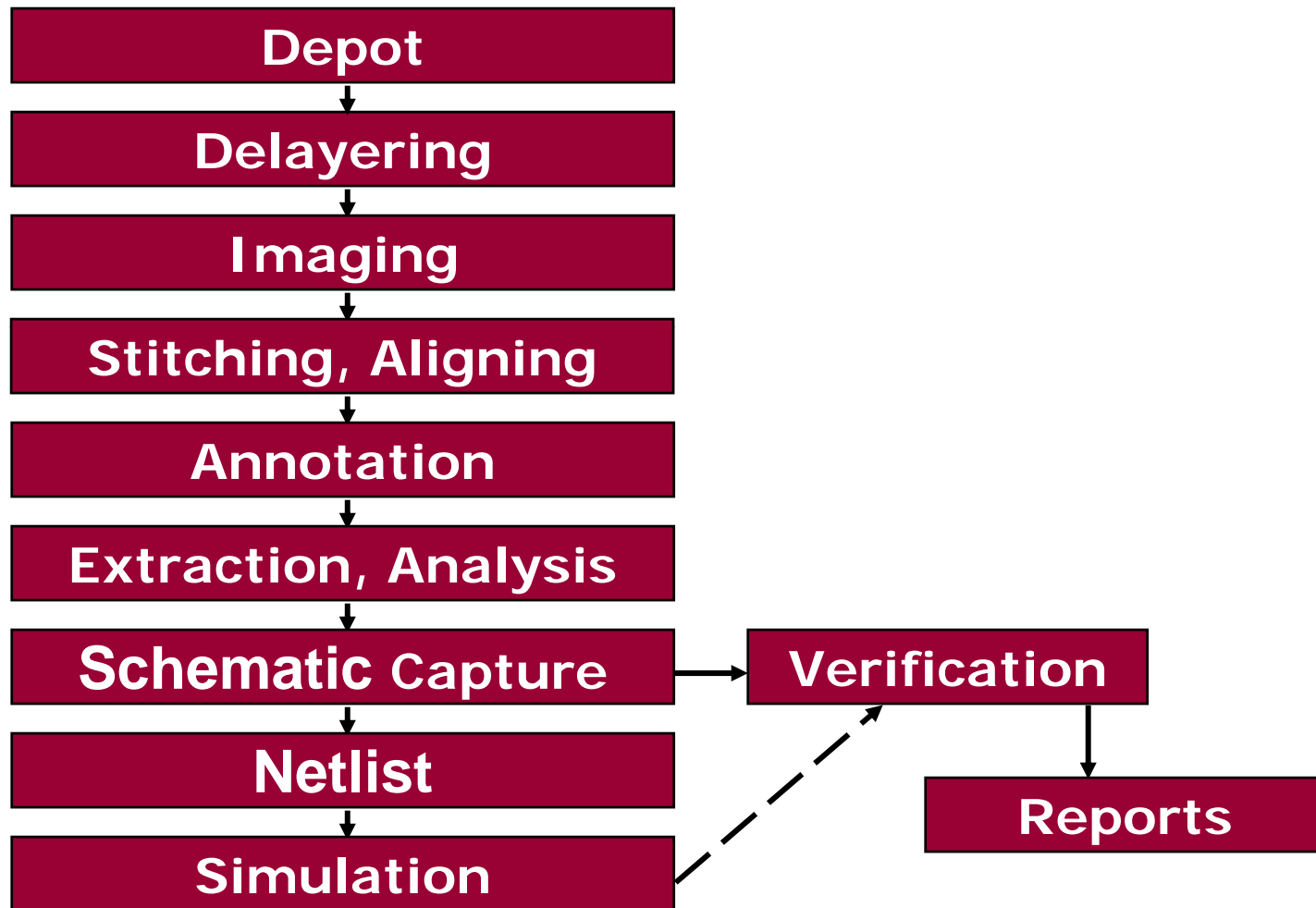


Transistor TEM

Circuit RE Flow



Circuit RE Flow



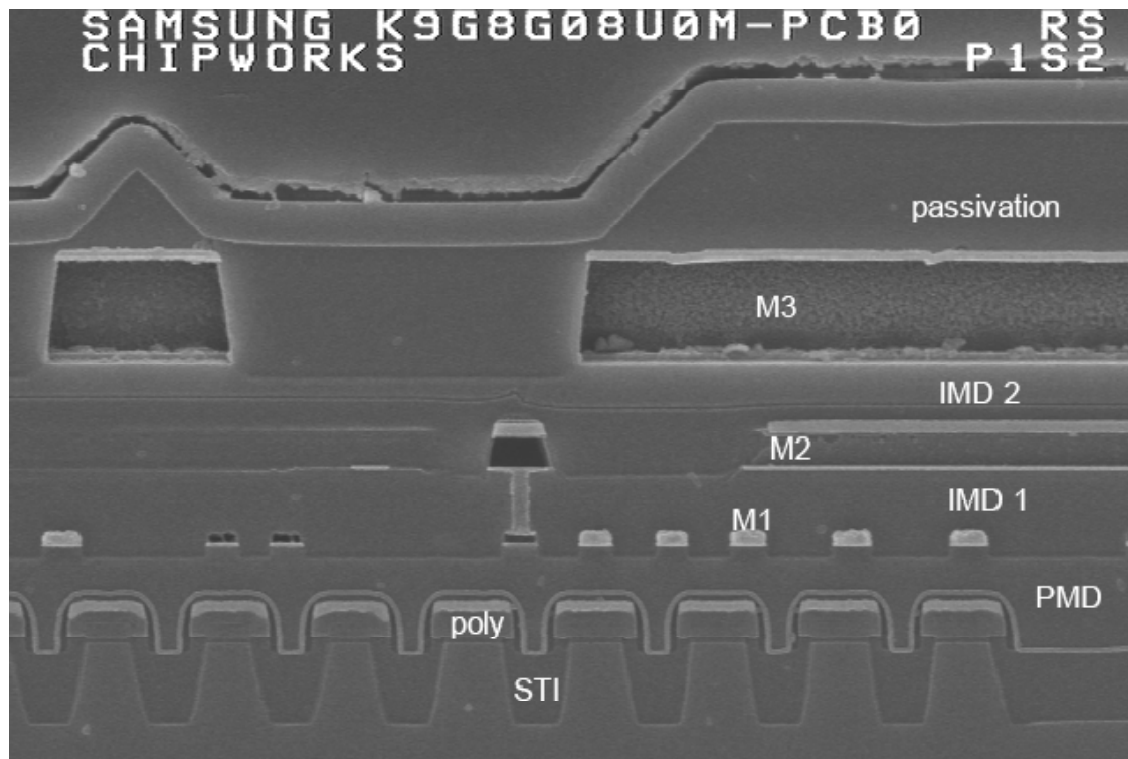
Circuit Analysis – Package Removal

- Remove plastic packaging by placing sample in acid bath
- A variety of acids and temperatures are used depending on package type



Circuit Analysis – Delayering

- Take cross-section SEM photo to identify layers



Samsung 8-Gb NAND Flash Memory

- Recent challenges:
 - 45nm
 - Low-K dielectrics
 - High-K gates
 - Metal gates
 - Copper
 - Gold
 - Mixed metals
 - MEMs
 - Stacked die

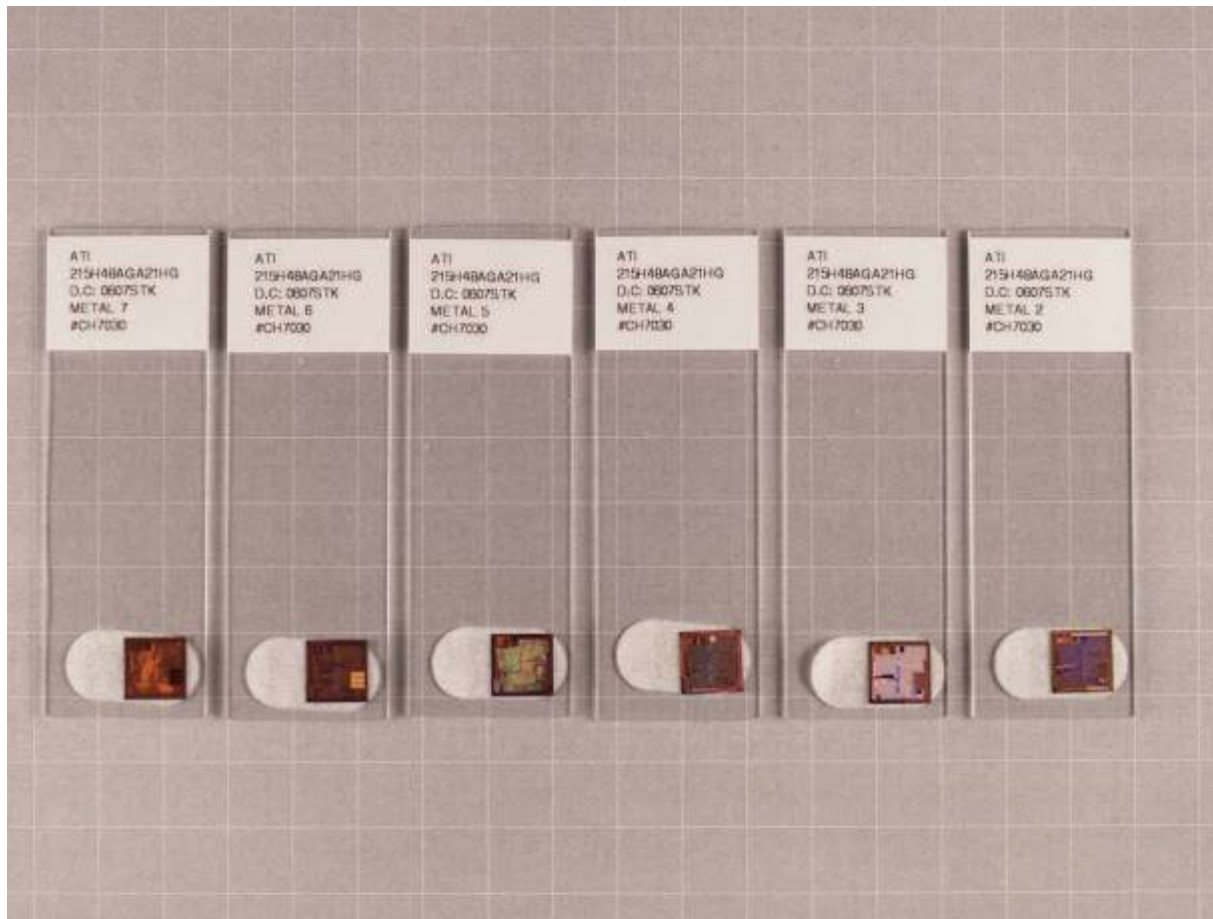
Circuit Analysis – Delayering

- Chose a technique and recipe, or develop a new one
- Remove layers one by one, typically via:
 - Reactive Ion Etching (RIE)
 - Inductively Coupled Plasma (ICP)
 - Micro-polishing

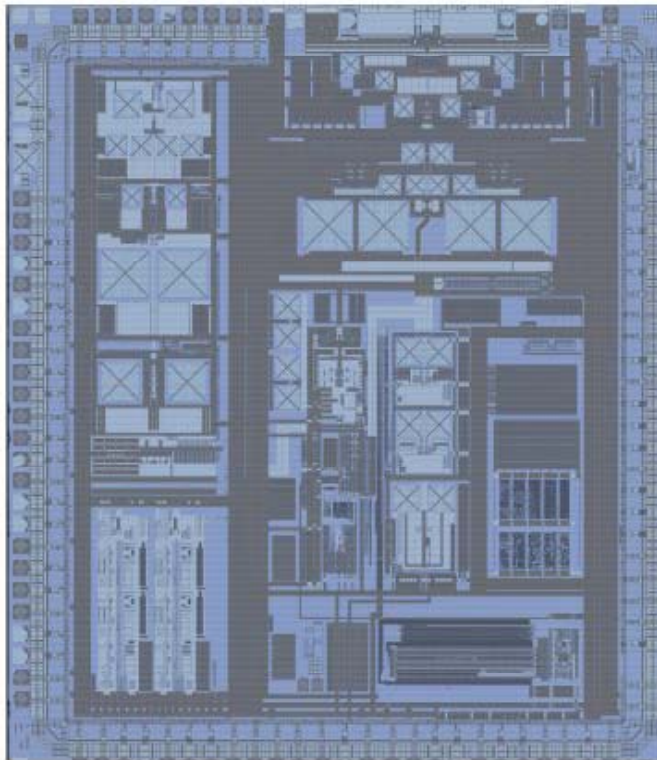


Delayering

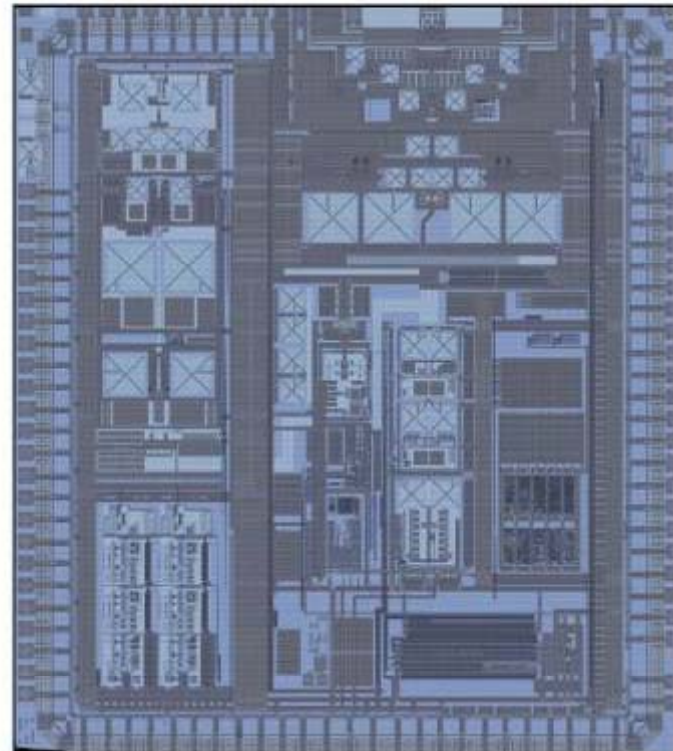
- A sample is prepared for each metal interconnect layer, polysilicon layer and substrate diffusions.
 - e.g. for 6 metal layer device, need to prepare 8 samples



Delayering



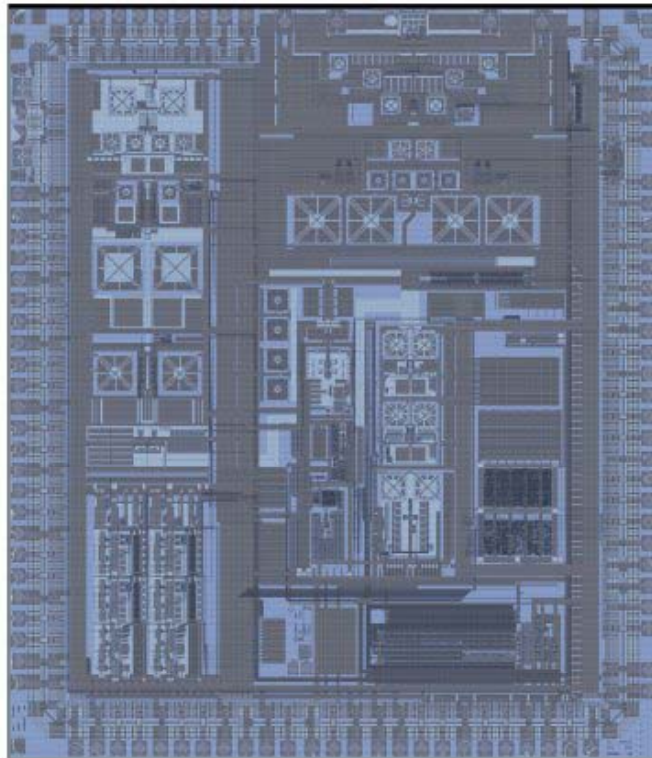
Atheros AR5110 - Metal 5



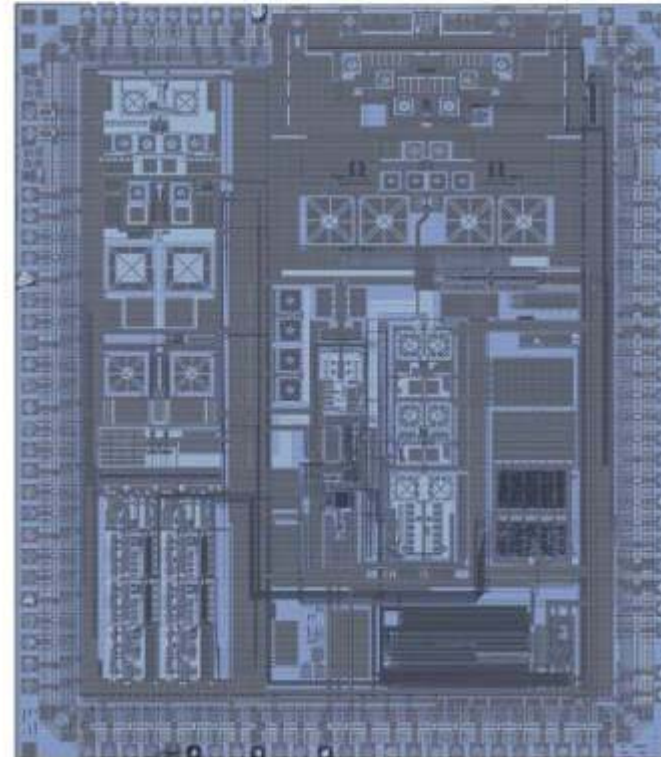
Atheros AR5110 - Metal 4



Delayering

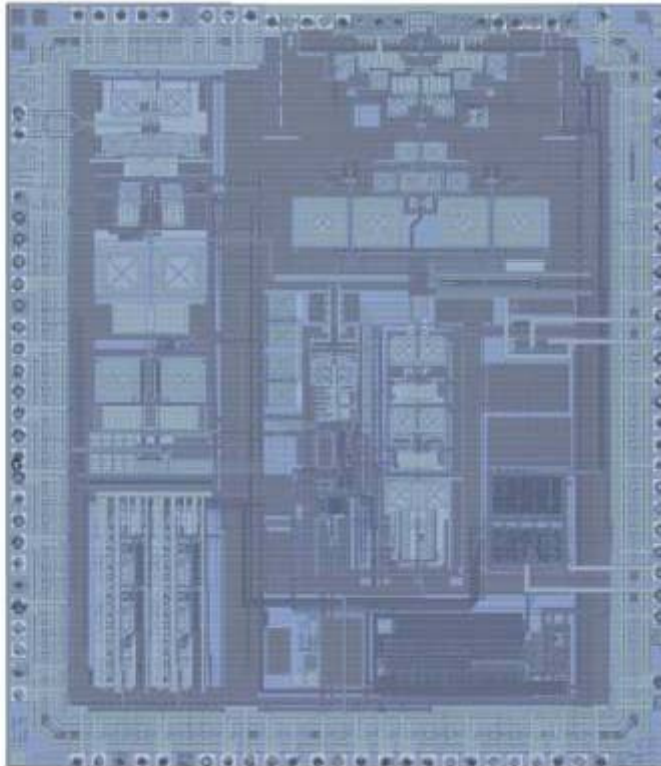


Atheros AR5110 - Metal 3

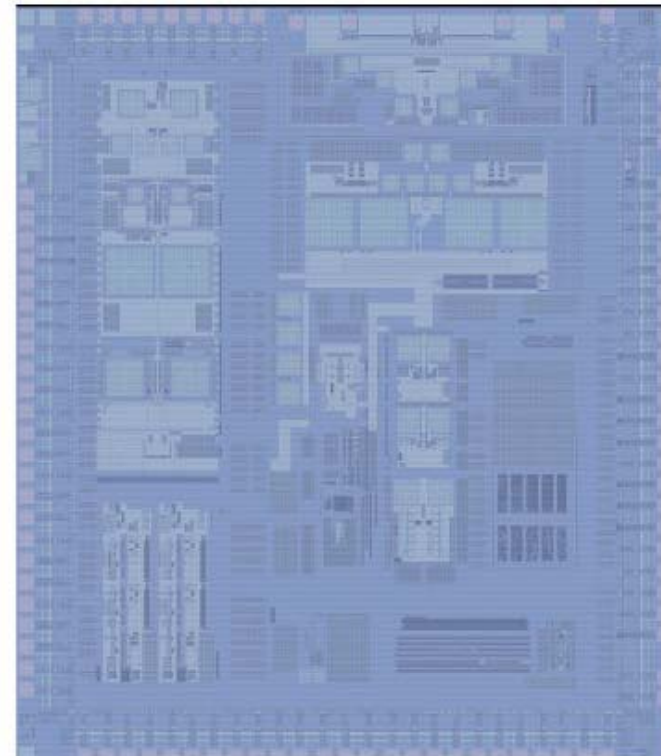


Atheros AR5110 - Metal 2

Delayering



Atheros AR5110 - Metal 1



Atheros AR5110 - Poly



Circuit RE Flow

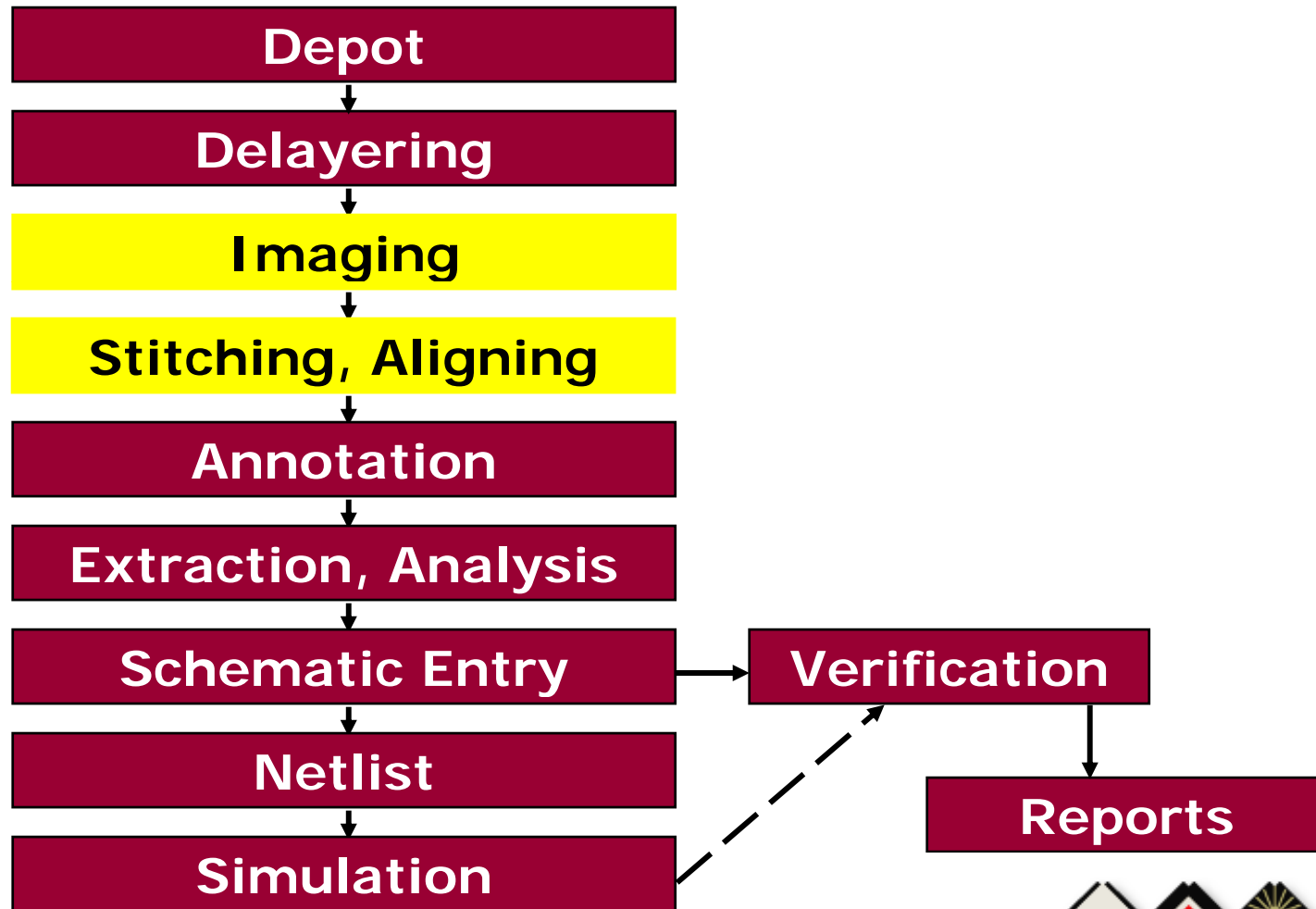


Image Capture

- Capture high magnification images using microscope (SEM and optical), automated stage and digital camera
- Use software to stitch all the images together, and for inter-layer registration

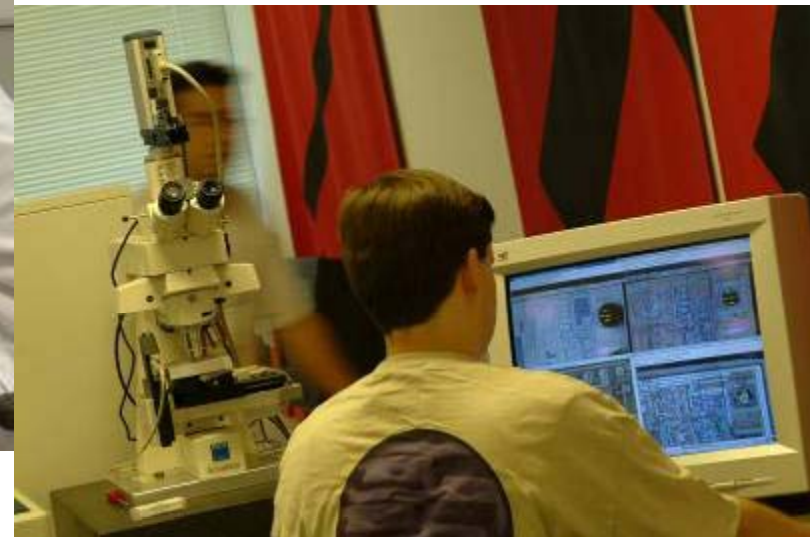
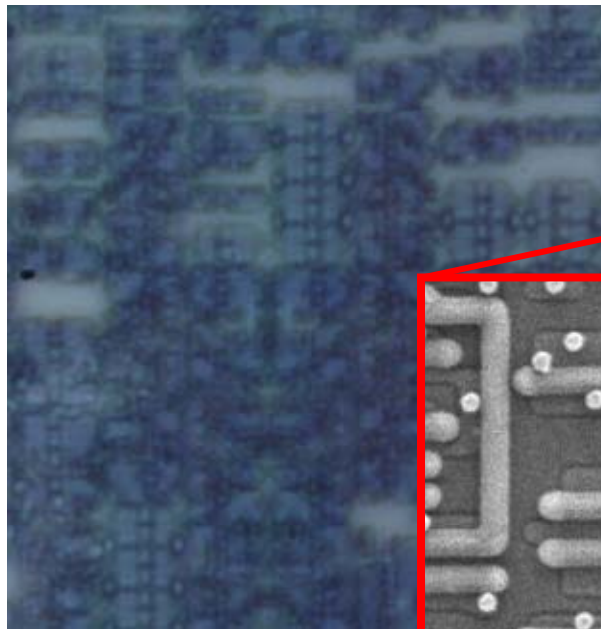


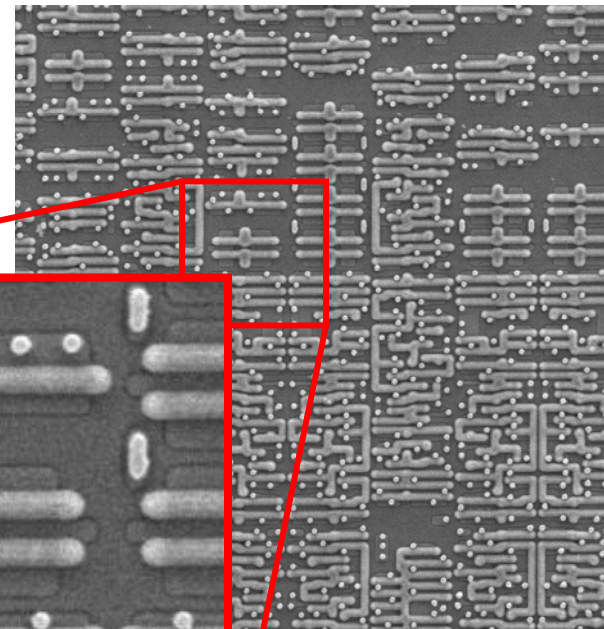
Image Capture

Optical vs. SEM – e.g TI OMAP1310, 0.13 μm process, transistor layer

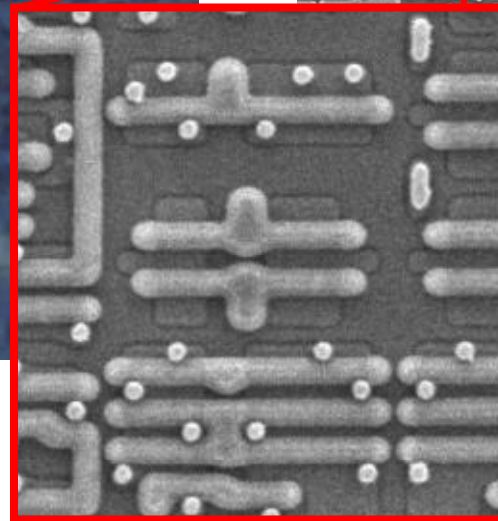
- 450nm optical light just doesn't cut it anymore



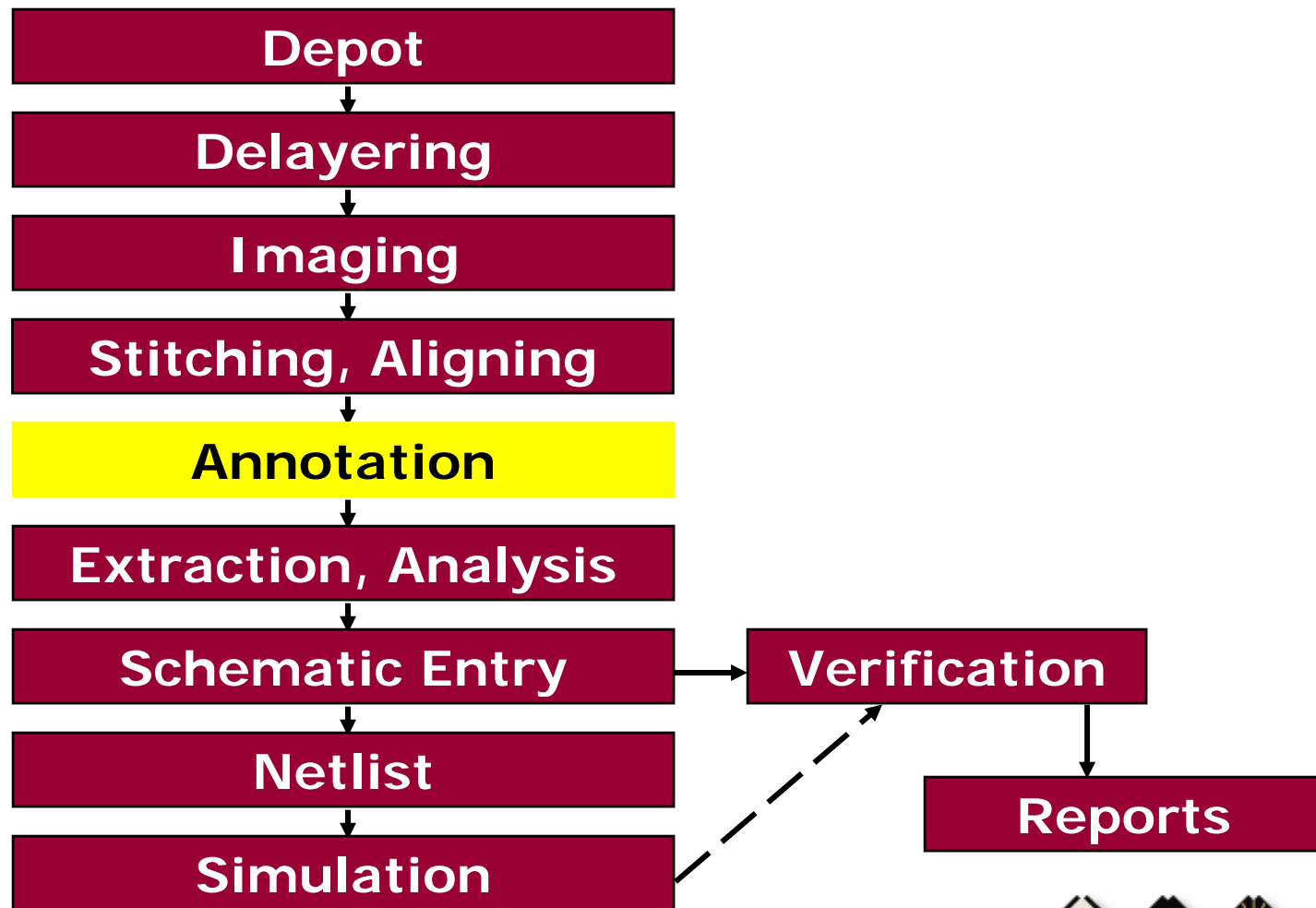
Optical



SEM



Circuit RE Flow

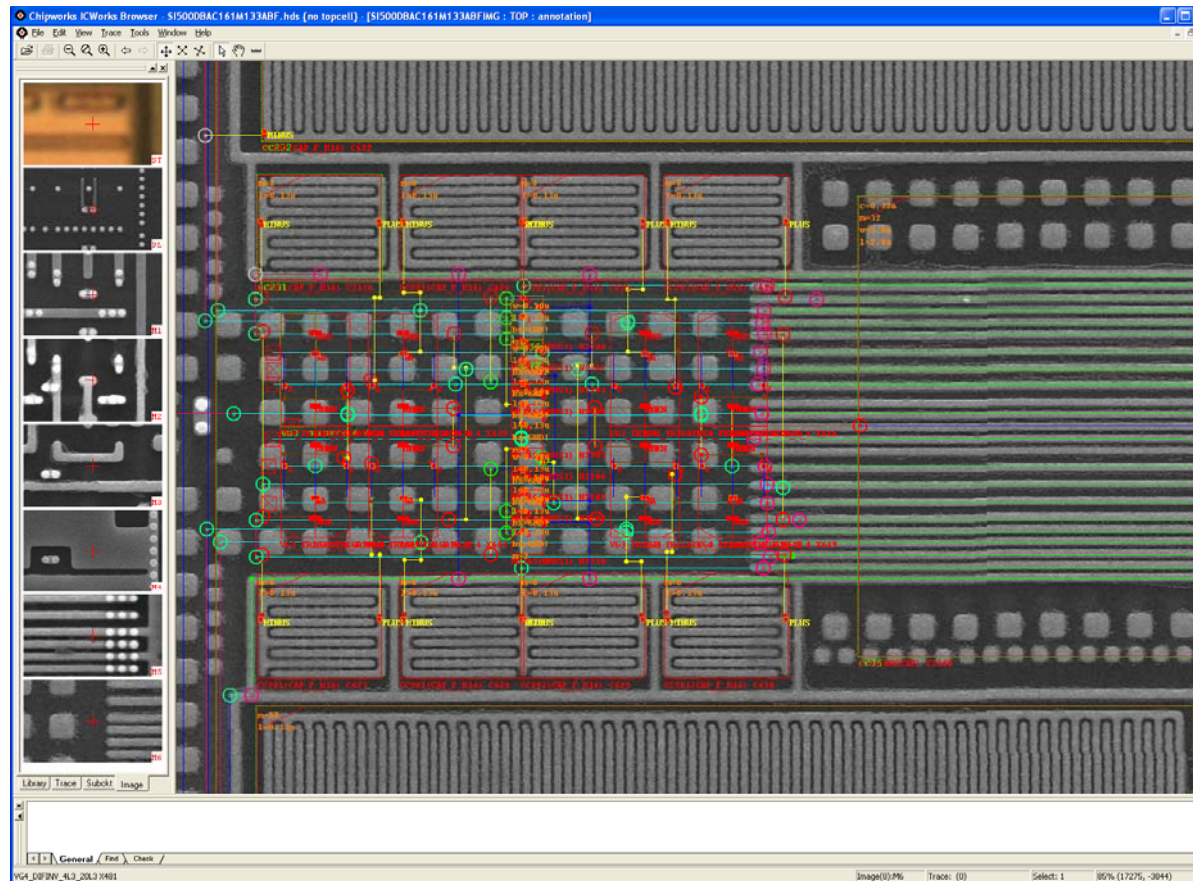


Annotation

The old days...

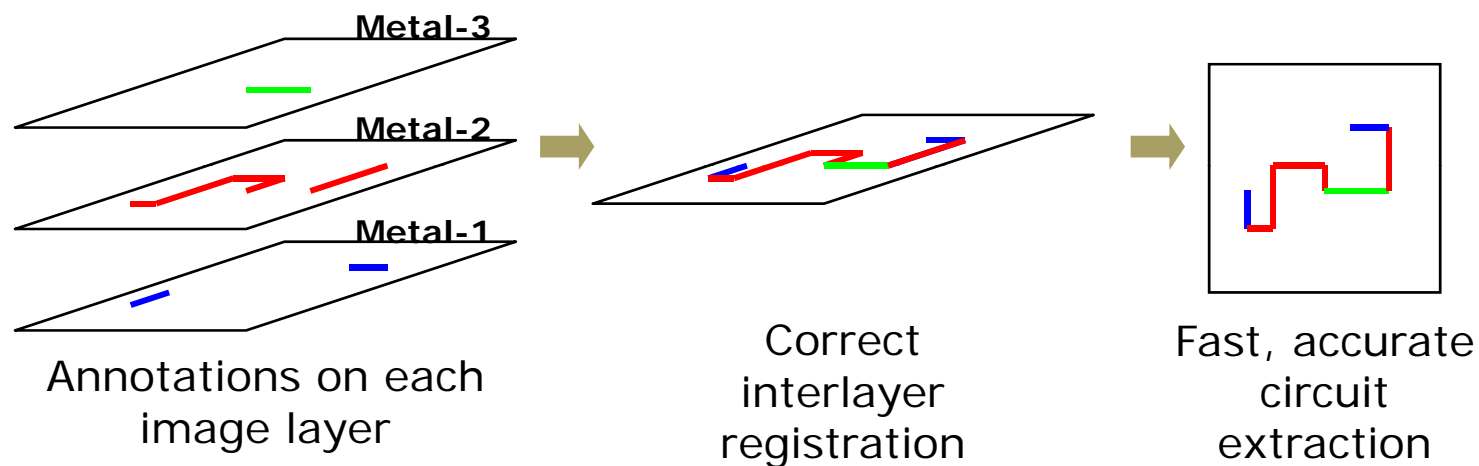


Annotation



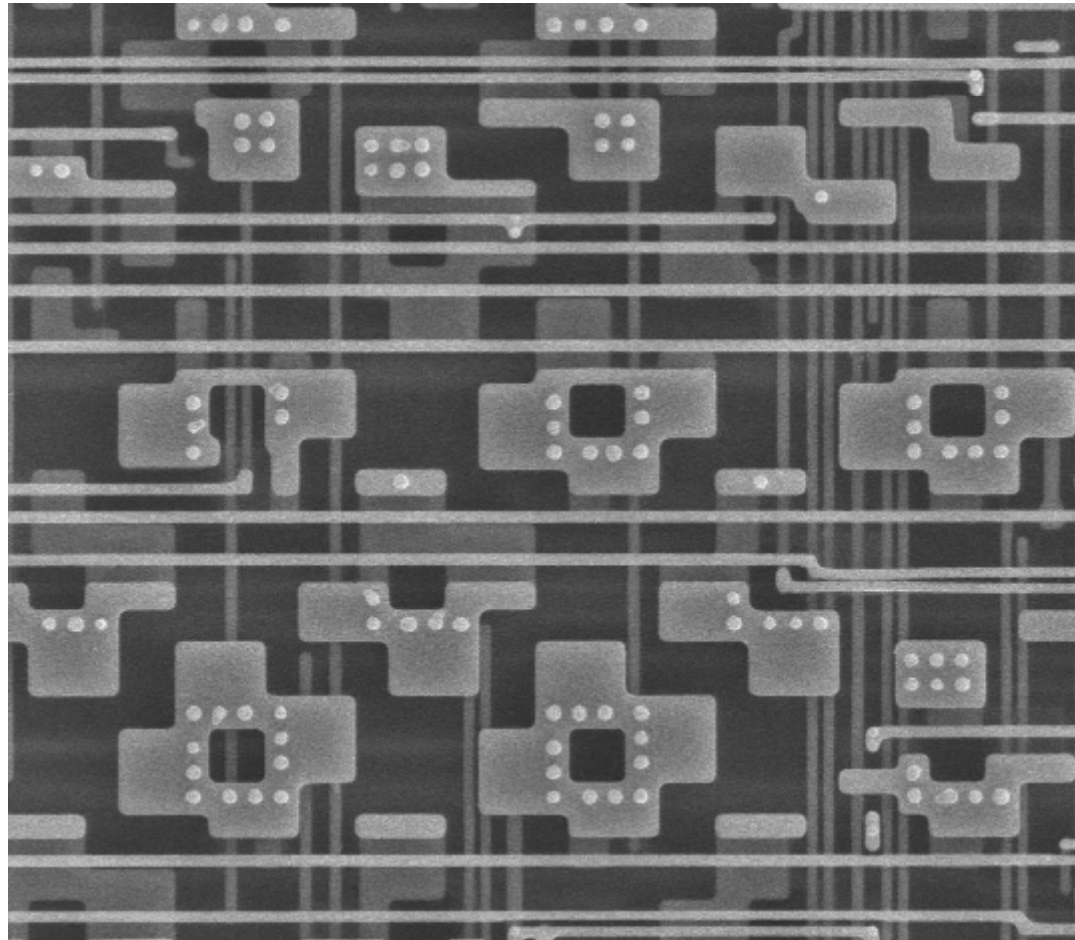
- Wires are traced on the layer where they appear
- Layers are all aligned and any can be visible
- All layers can be shown at side

Annotation



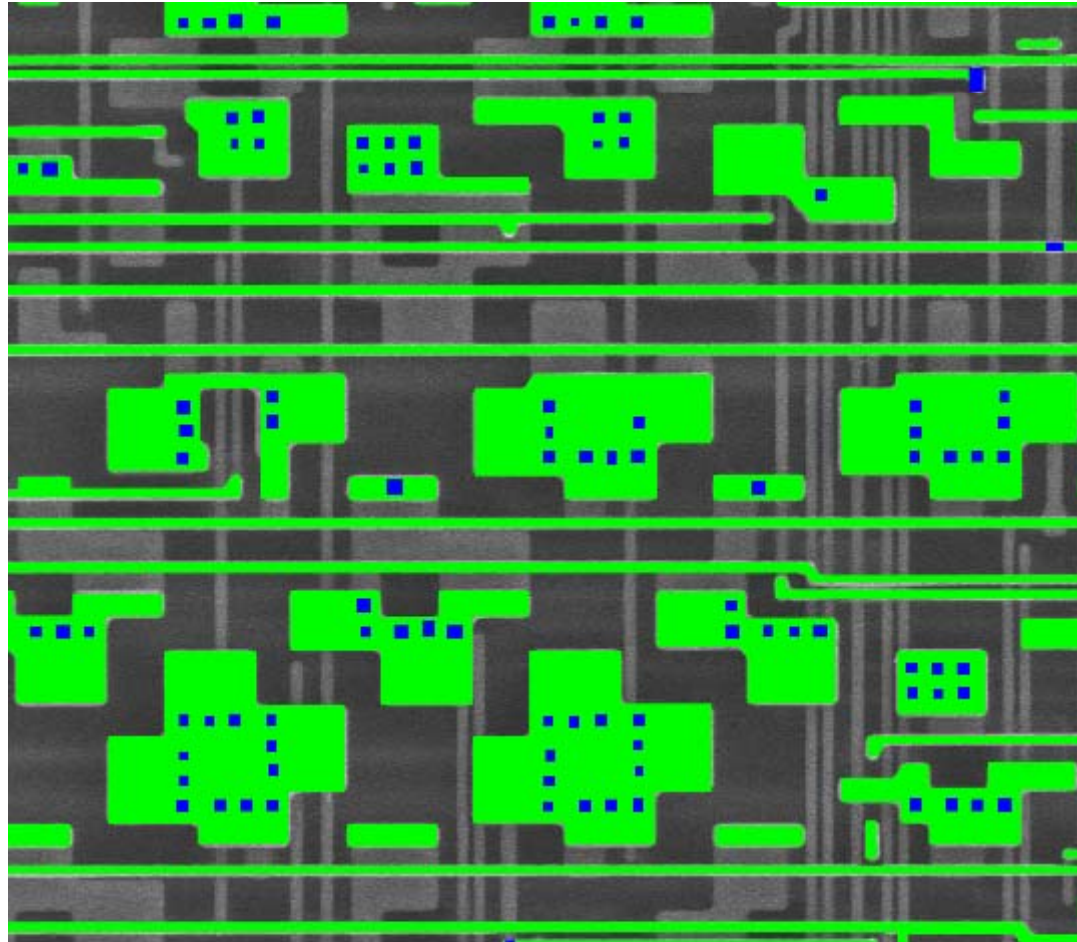
Annotation – Polygon Feature Extraction

Raw M4 layer image



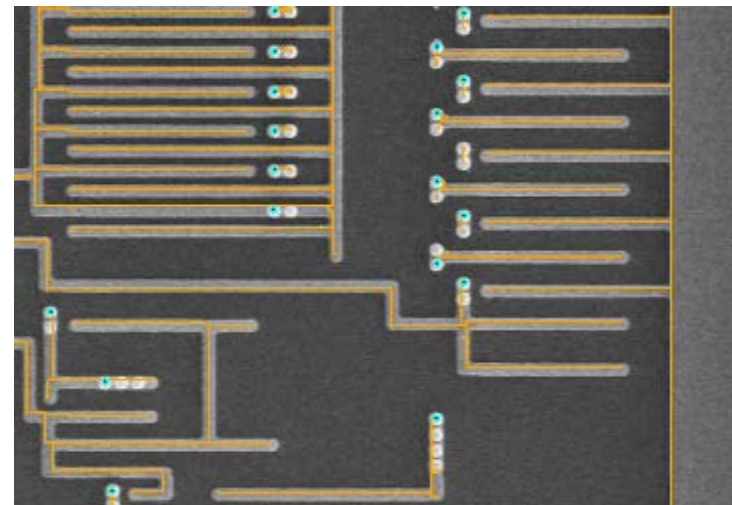
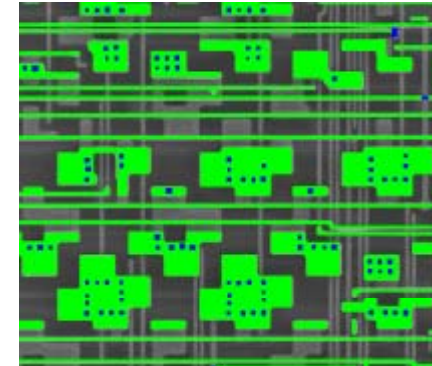
Annotation – Polygon Feature Extraction

Fill in polygons based on heuristics (size, brightness, color, etc.)



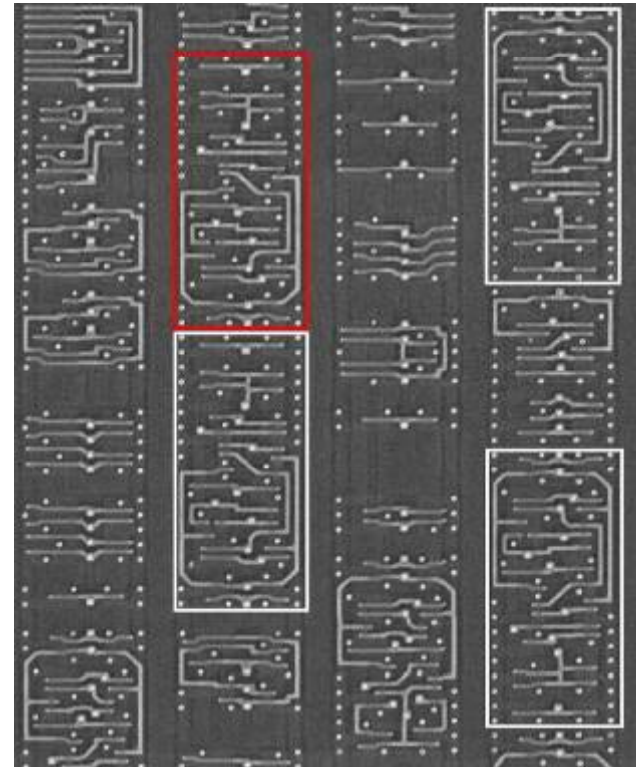
Circuit Analysis – Polygon Feature Extraction

- Rule-based DRCs can improve accuracy
 - E.g. small breaks in wires, floating or missing contacts
- Can move to centerline wires and point contacts
- Feature extraction challenges:
 - Visibility of other layers
 - Brightness variability
 - Sample prep artifacts



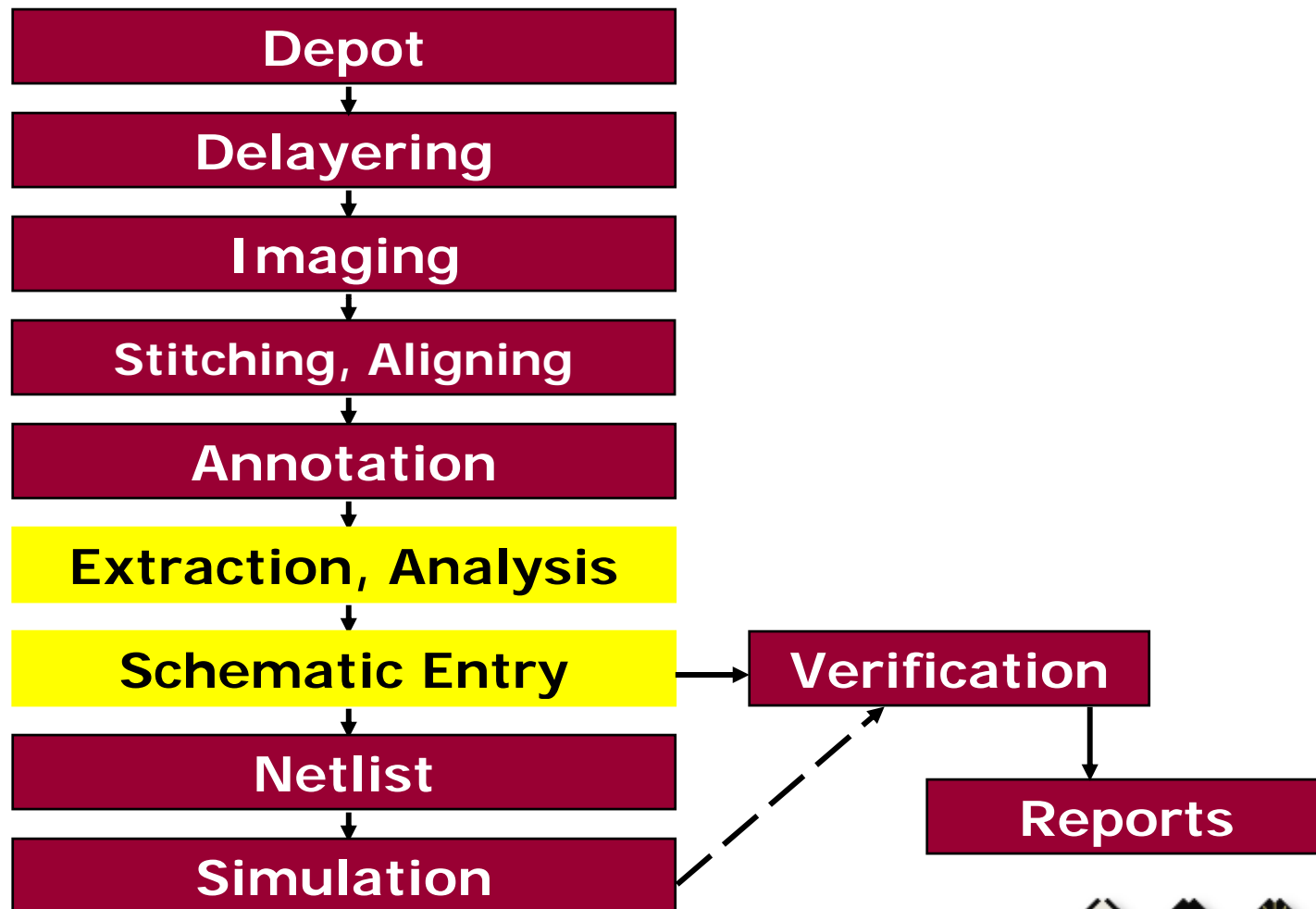
Annotation – Ever More Automation

- Further automation is possible after the feature recognition:
 - After wires are annotated vias can often be placed automatically
 - Once a device is defined, identical instances of this device can be searched for and found using pattern matching image recognition
 - This is especially useful for digital logic

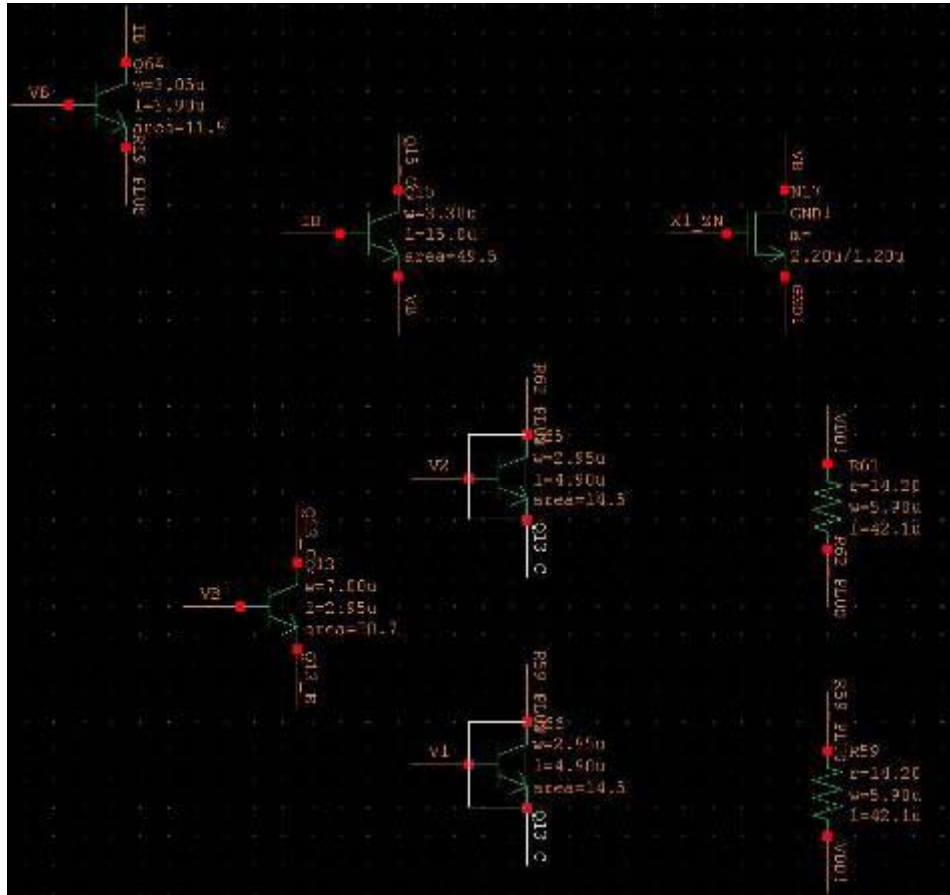


Standard cell recognition

Circuit RE Flow



Schematic Readback

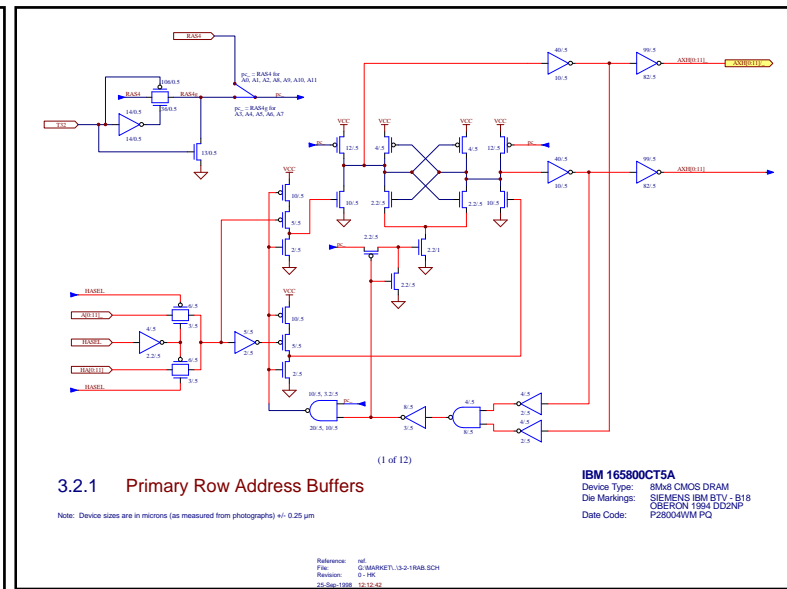
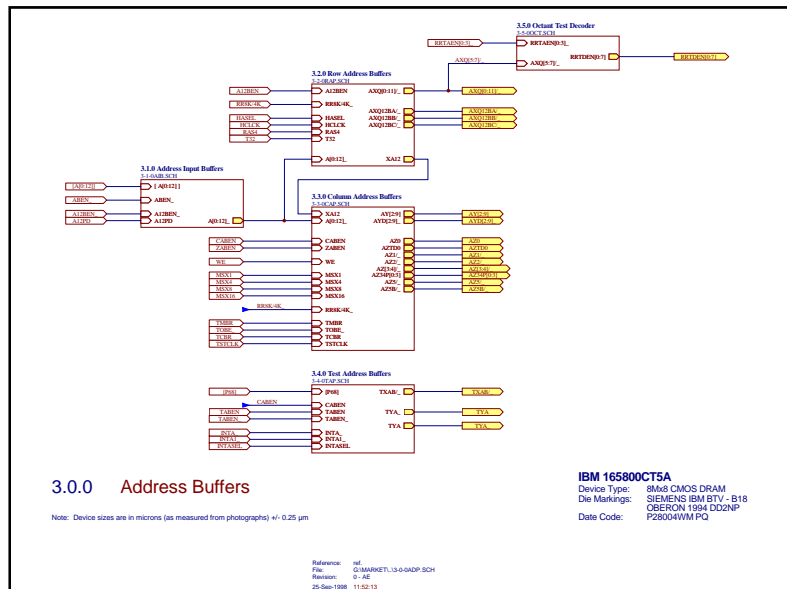


Auto-extracted devices placed on schematic in same relative positions as the layout

However, this arrangement of transistors or gates does not convey a great deal of information, so...

Analysis

- The analysis phase:
 - arranging the transistors and gates
 - organizing a readable, hierarchical schematic set
 - understanding the function and reason behind the design



Analysis

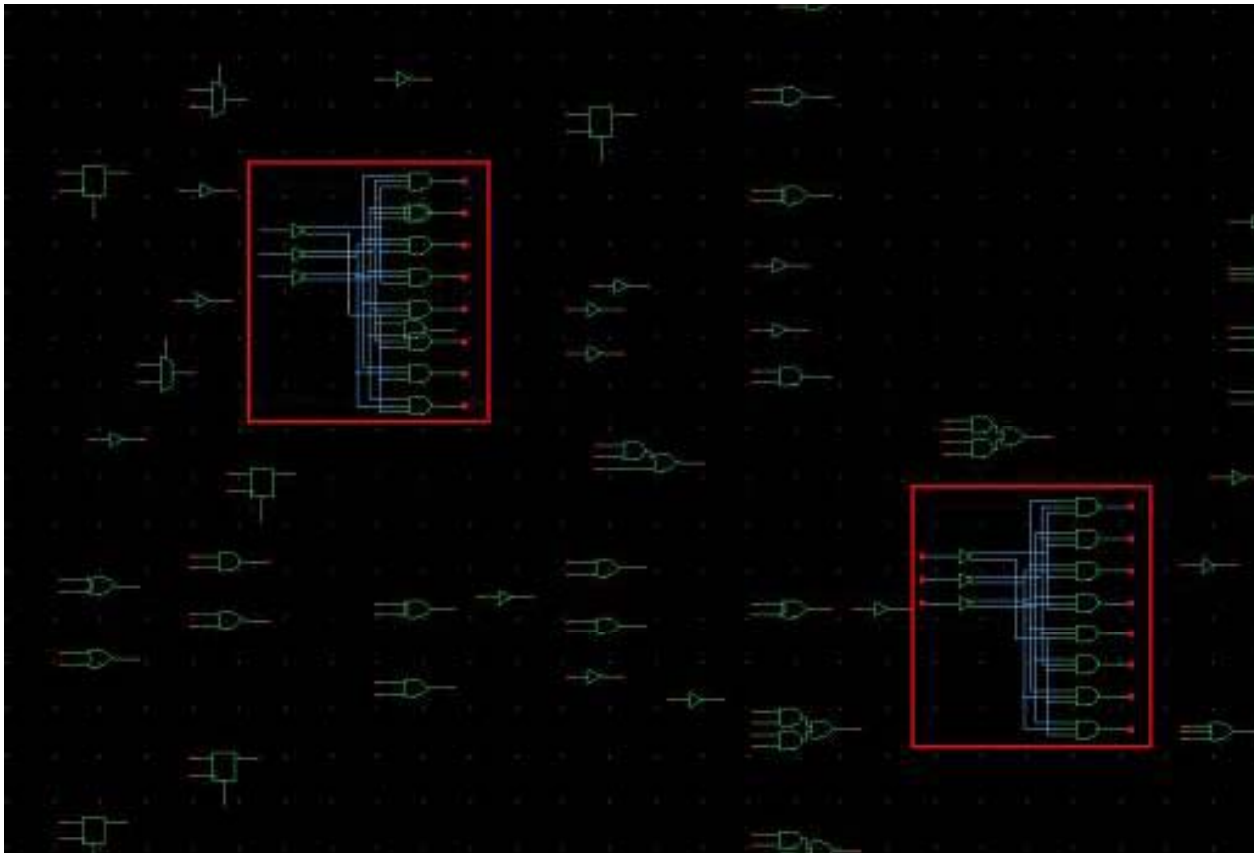
▪ Tools

- Schematic organization can be done using the usual design schematic editors (e.g. Cadence Composer)
- However, these tools tend to be optimized for forward design rather than reverse engineering
- ICWorks Arranger is optimized for schematic organization from layout
 - Simple structures such as diff pairs and current mirrors can be found automatically
 - Subcircuits are easily grouped, created, and linked hierarchically
 - Subcircuit input devices can all be gathered with one keystroke
 - Identical subcircuits can be located and organized automatically



Analysis

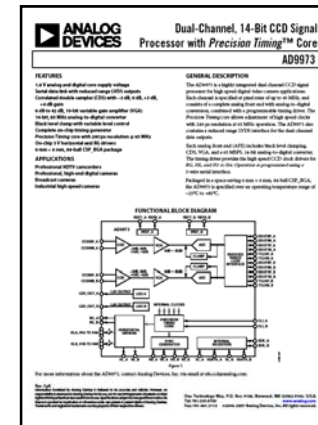
- One instance defined manually, others matched and organized automatically



Example sub-circuit search and organization

Analysis

- **Other inputs**
 - Public information and datasheets can help with schematic organization
 - Technical papers and patents hold interesting clues
 - Floorplan and layout information can be very valuable
 - For analog circuits the layout often follows a logical progression
 - For digital... not so much
 - An experienced RE analyst is invaluable

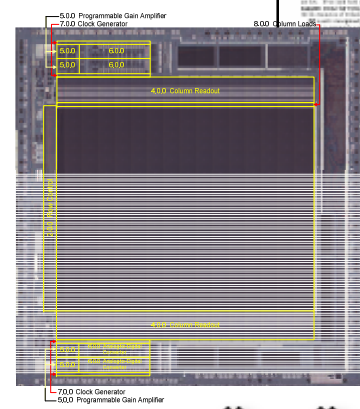


Engineering in the Semiconductor Industry

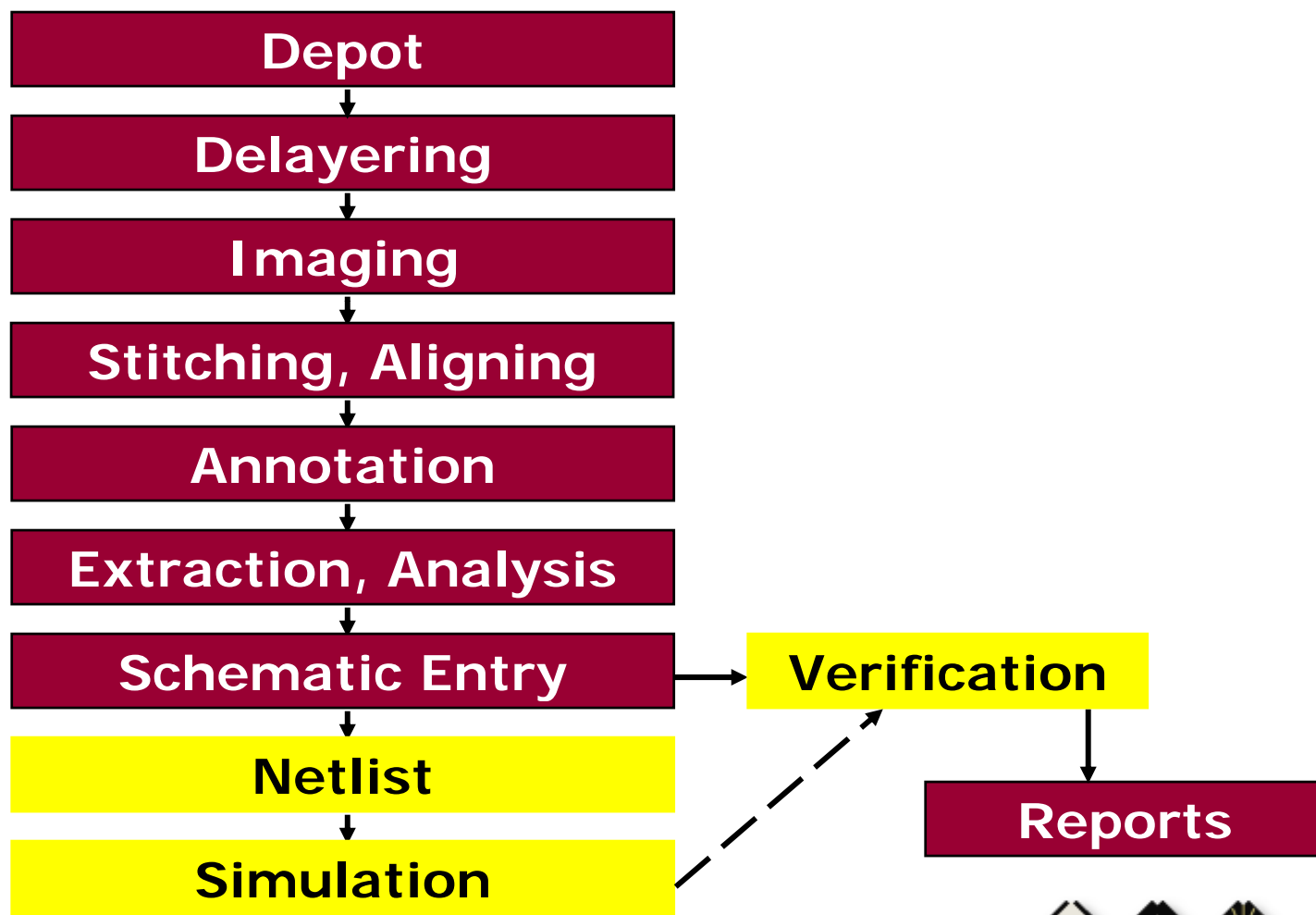
...the semiconductor industry is facing a number of challenges...

...the industry is facing a number of challenges...

...the industry is facing a number of challenges...



Circuit RE Flow

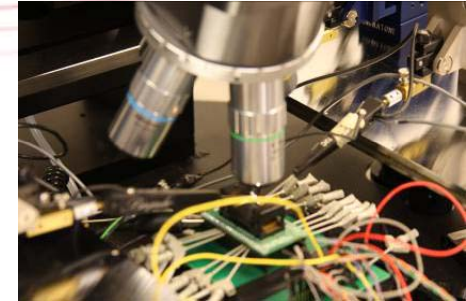


Verification

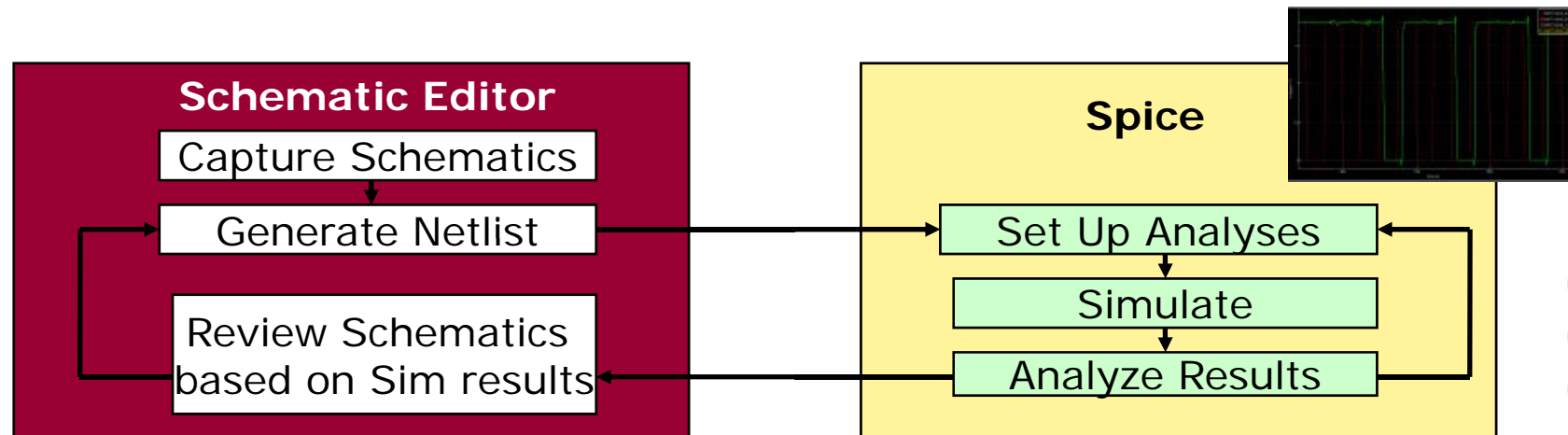
- As with forward design, the first pass schematic is not always 100% correct
- However, in contrast to forward design, 100% correct is often not essential:
 - Clients are usually most interested in circuit structure
 - Device sizes only need to be approximate
 - Even if simulation is desired, we rarely have process models for competitive chips, and hence accurate device sizes are not critical
- Of course, device sizes can only be as accurate as measured from actual devices:
 - As measured on silicon, not mask sizes or layout database sizes
 - The process on any particular device could be anywhere between best and worst case



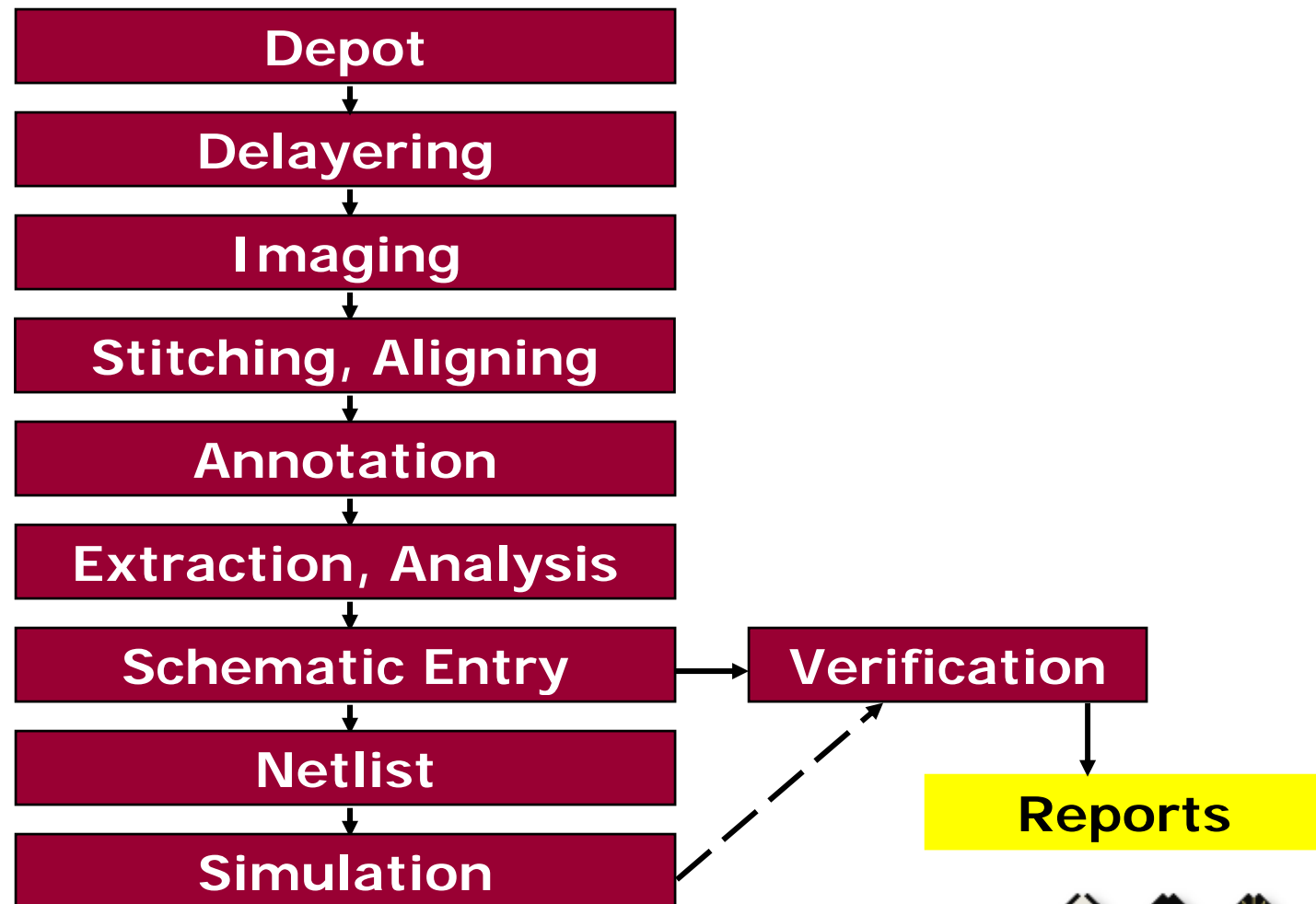
Verification



- Multiple techniques are available:
 - Redundant annotation
 - DRCs: floating wires and contacts, floating gates, shorted outputs...
 - Greater use of automated extraction tools
 - Our schematic editor flags errors whenever the connectivity is broken (connectivity derived from annotated images)
 - Simulation (either digital or analog)
 - Microprobing
 - And, of course, experienced analysts who can quickly see when a circuit makes sense, and when it doesn't

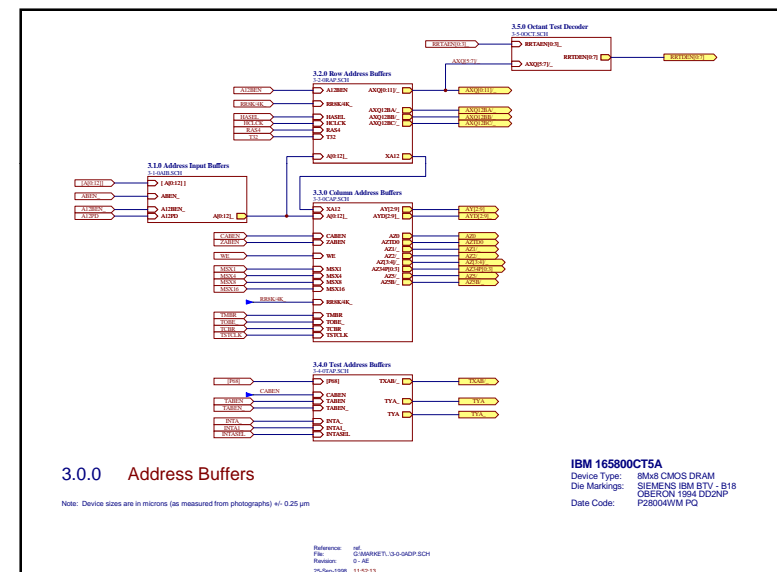
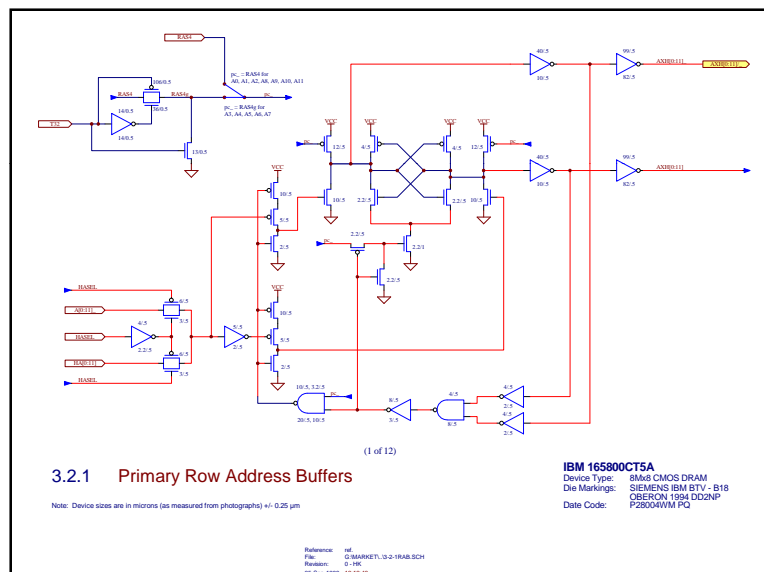


Circuit RE Flow



Circuit Analysis - Deliverable

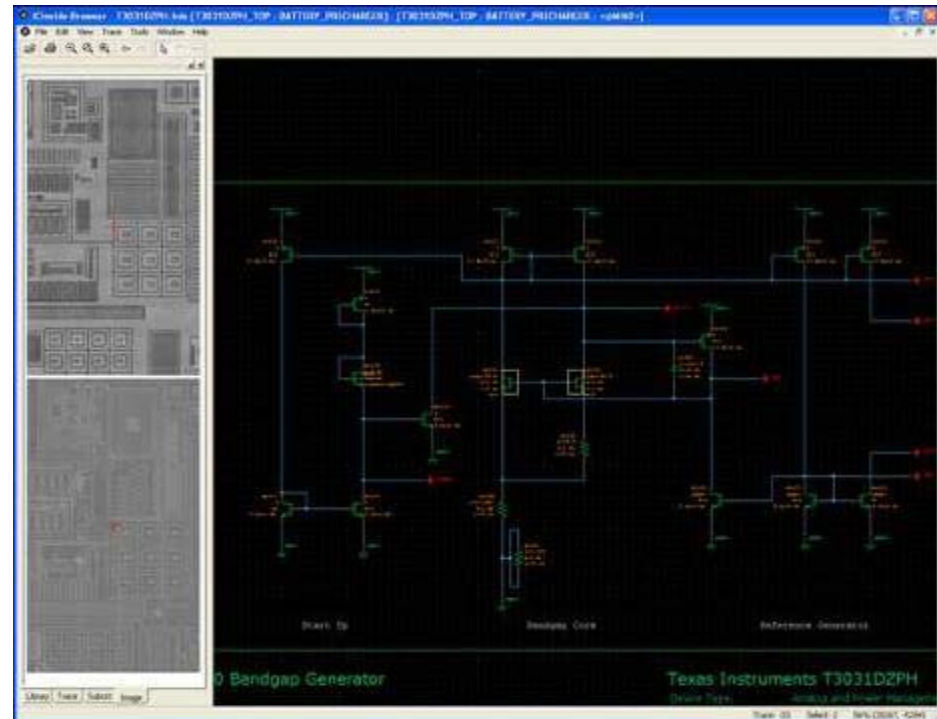
- Organized, readable, hierarchical schematics



- Optional Outputs: Netlists, simulated waveforms, micro-probed waveforms, block diagrams, timing diagrams, circuit equations

Chipworks ICWorks Browser

Interactive software application to view both schematics and images, and to pan, zoom, trace and bi-directionally cross-probe between the two.

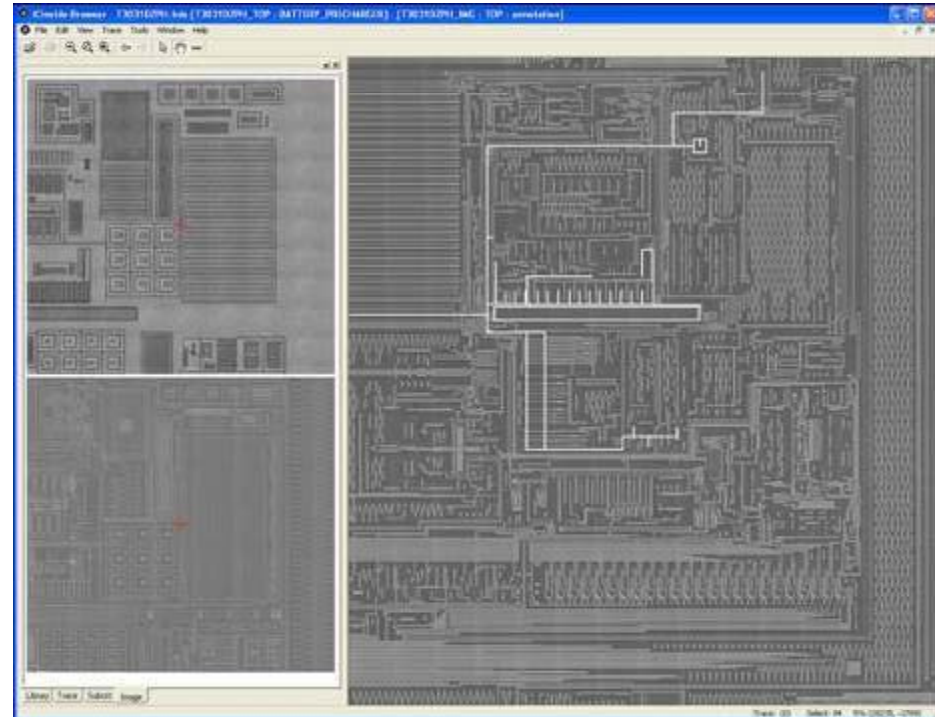


ICWorks Browser



Chipworks ICWorks Browser

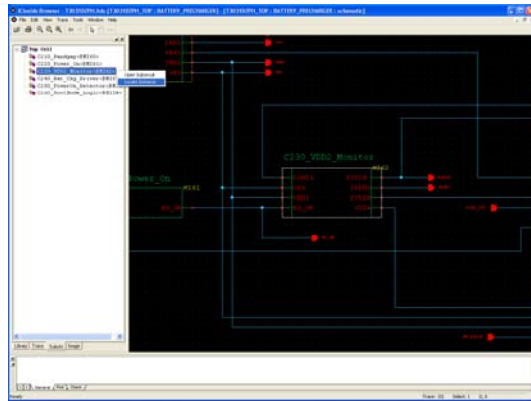
Highlight and easily trace one or more circuit paths throughout the device's layers (example shown – power routing)



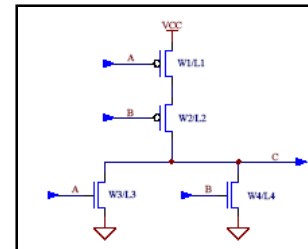
ICWorks Browser



Powerful Export Capability



ICWorks Browser



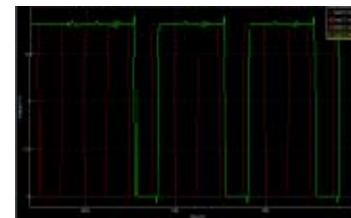
Schematic Editors (EDIF200)

```
model p1to nmos level 1
+ vto=0.25e-01 uo=1
+ theta=1.96e-02 vma=
+ tau=4.70e-07 rps=
+ cj=9.000e-06 pb=0

model p2to pmos level 1
+ vto=-1.25e-01 uo=1
+ theta=7.77e-02 vma=
+ tau=4.70e-07 rps=
+ cj=1.300e-06 pb=0

* seq.#: 25 processes
* seq.#: 50 processes
* date: 03/10/2013
```

Netlist



Simulate

ICWorks Browser



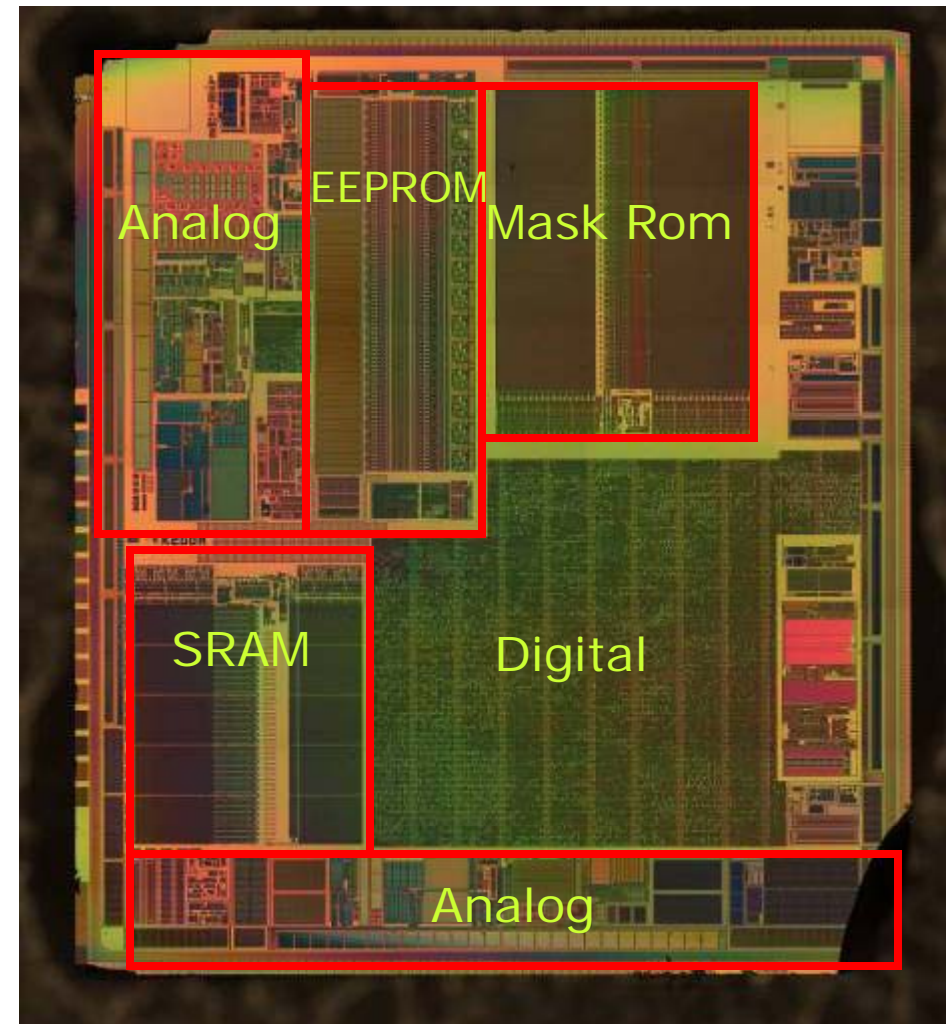
Mixed Functional/Physical Chip Analysis

- Combine functional testing, physical extraction, and simulation to understand chip
- Result is not schematics, but specific understanding of a chip, such as a portion of a datasheet or functional specification
- Powerful method of understanding complex chips and SOCs using many RE techniques together to complement each other
- Can be useful for chips with hardware security and encryption also



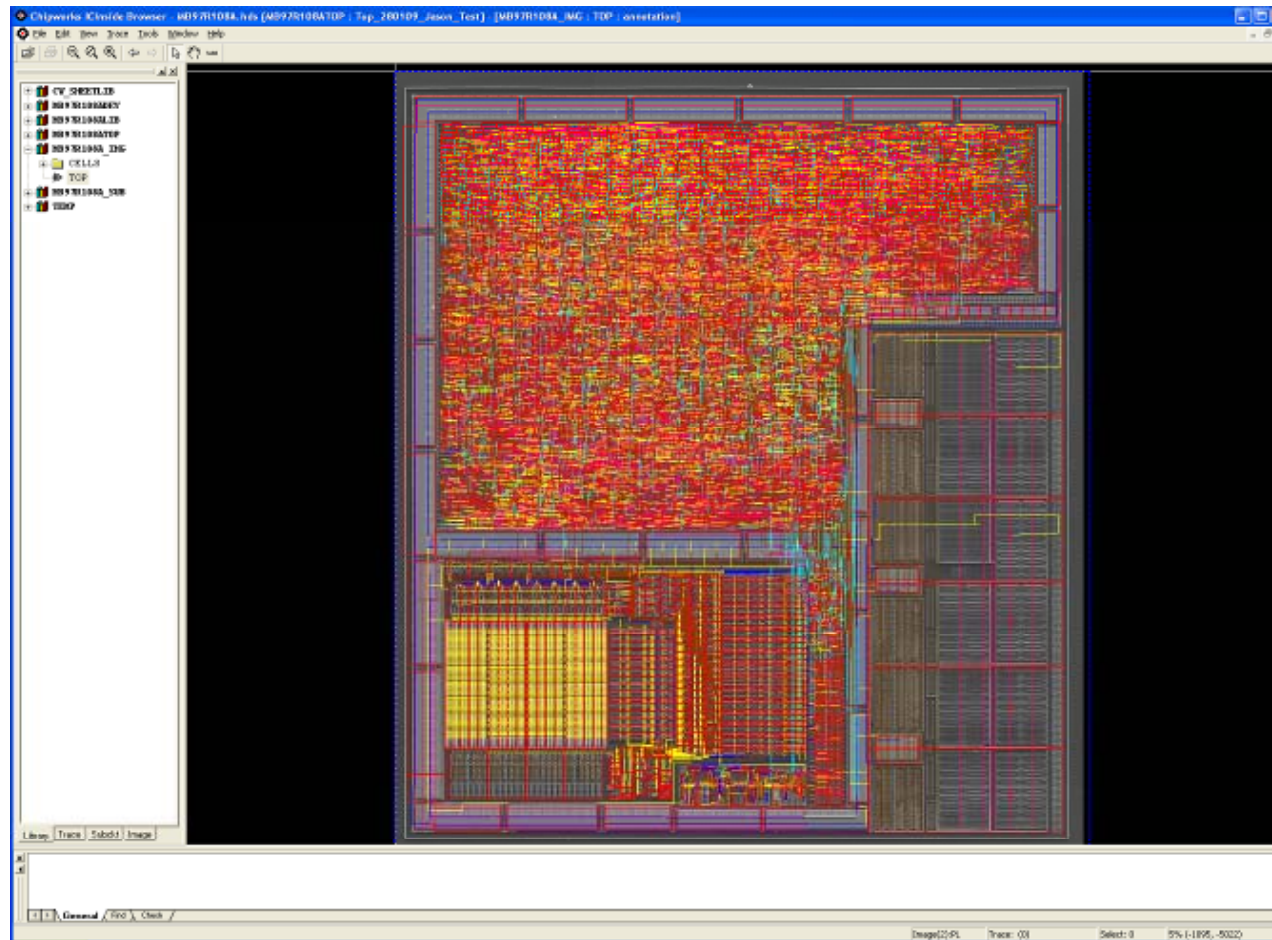
Case Study

- Goal: to understand a mixed analog digital ASIC with embedded SRAM, ROM and EEPROM, and a hardware encryption algorithm running on-chip
- Interface to chip was an unknown encrypted protocol
- Many techniques need to be utilized
- Step one: Depot, delayer, image, stitch, and align.



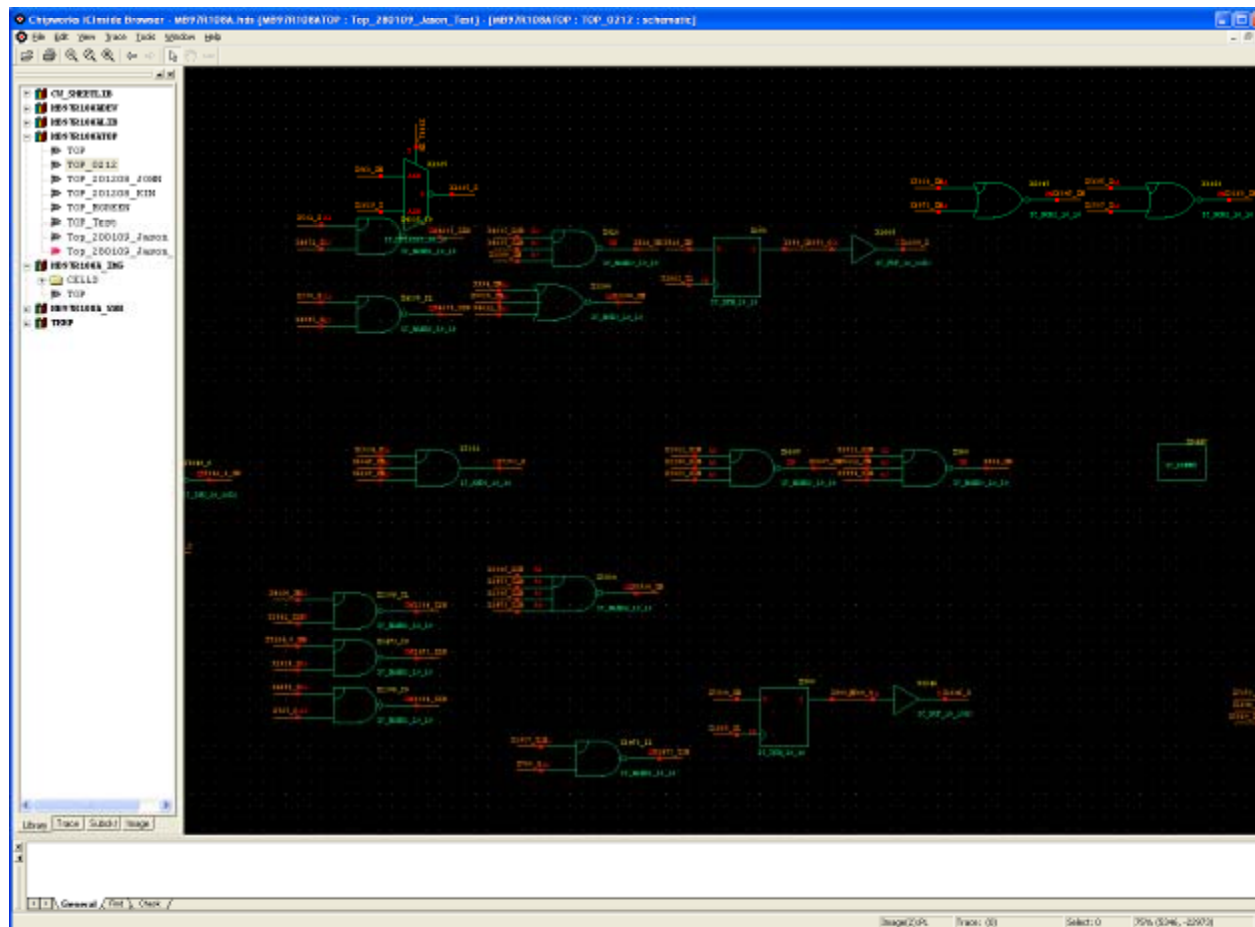
Case Study

- Annotate, Design rule checks



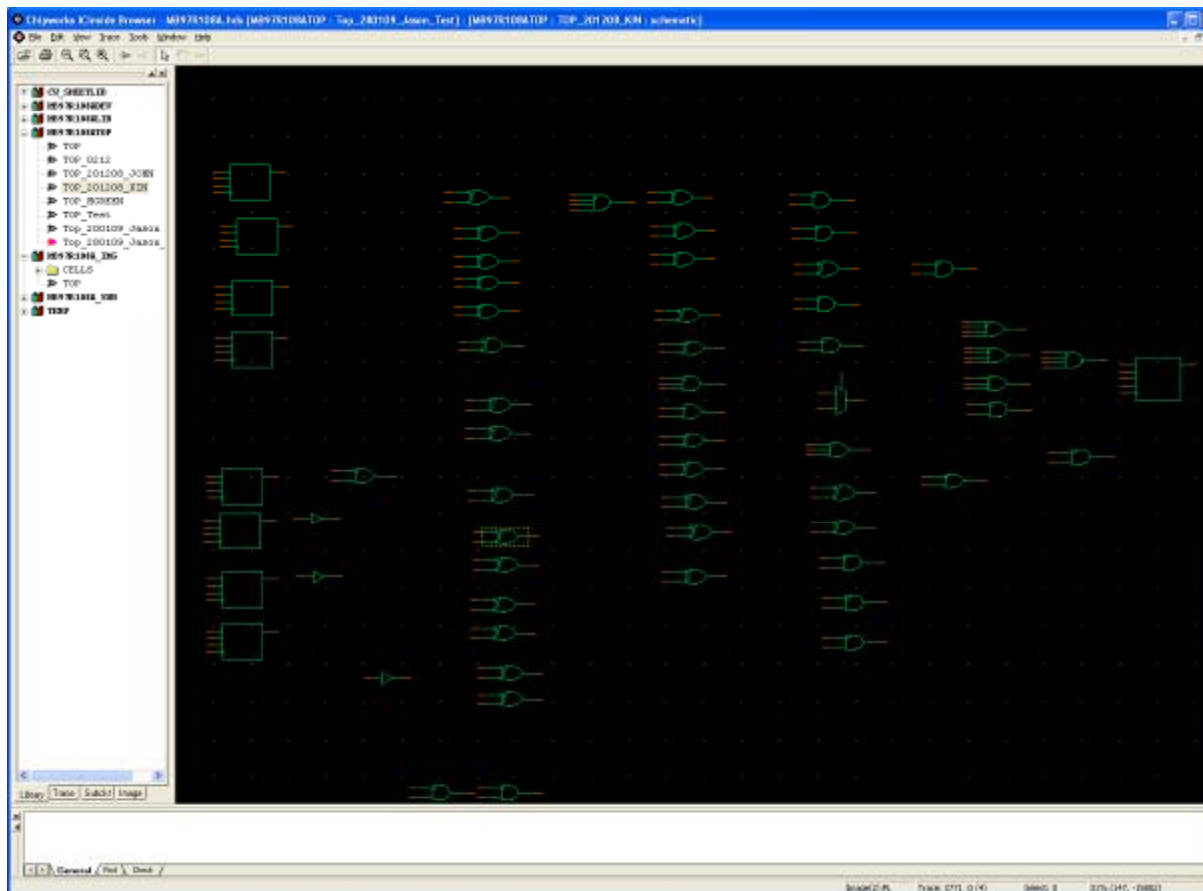
Case Study

- Export to flat un-organized schematic and netlist



Case Study

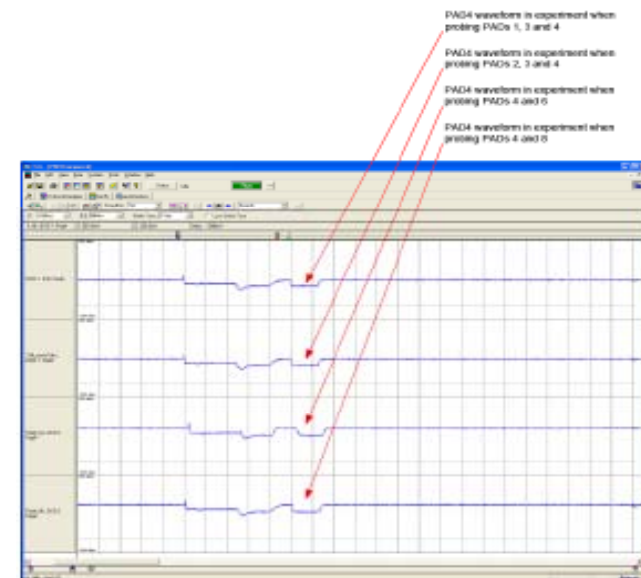
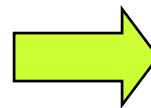
- Do limited schematic organization, often to find specific functions
 - In this case we found a 56-bit register, very interesting...
- Usually the analog logic is more fully organized than digital



Case Study

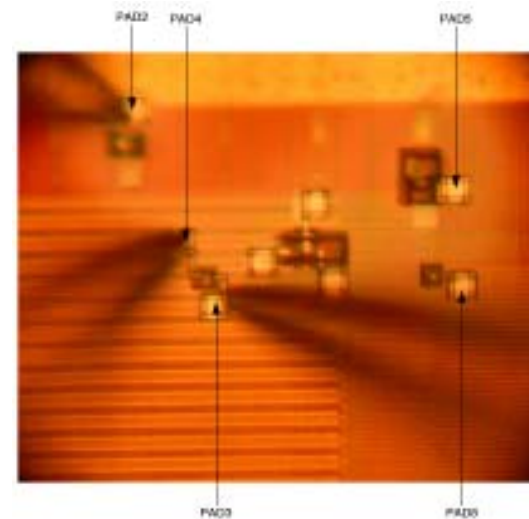
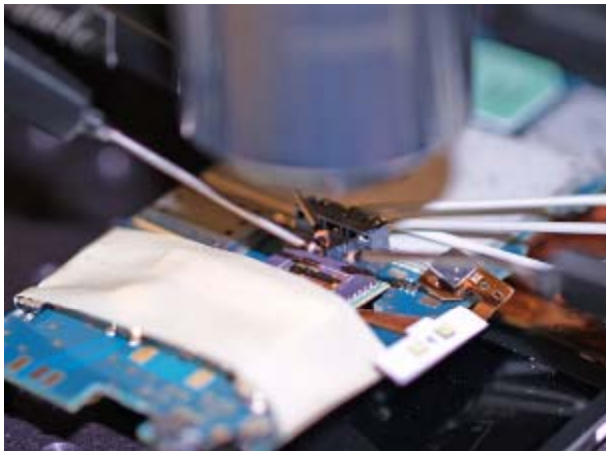
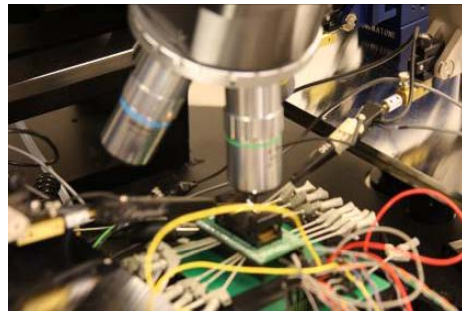
- Run top level test cases captured from system to verify and debug the netlist
- In this case we found the netlist simulated fine, and the outputs of the netlist simulation matched the actual chip outputs up to a point
- At that point nothing matched, likely the chip started encrypting its responses
- The matching outputs up to that point indicated that our netlist was at least fairly accurate

```
// File      : Dig_Top_TB.v
// Generated : Tue Jan 20 11:39:10 2009
// From      :
// c:\Dig_Top\TestBench\Dig_Top_TB_settings.txt
// By       : tb_verilog.pl ver. ver 1.2s
//
//-----
//
// Description :
//
//-----
`timescale 1ns / 1ps
module Dig_Top_tb;
//Internal signals declarations:
wire X24_Z;
wire X37_Z;
wire X41_Z;
wire X100_Z;
```



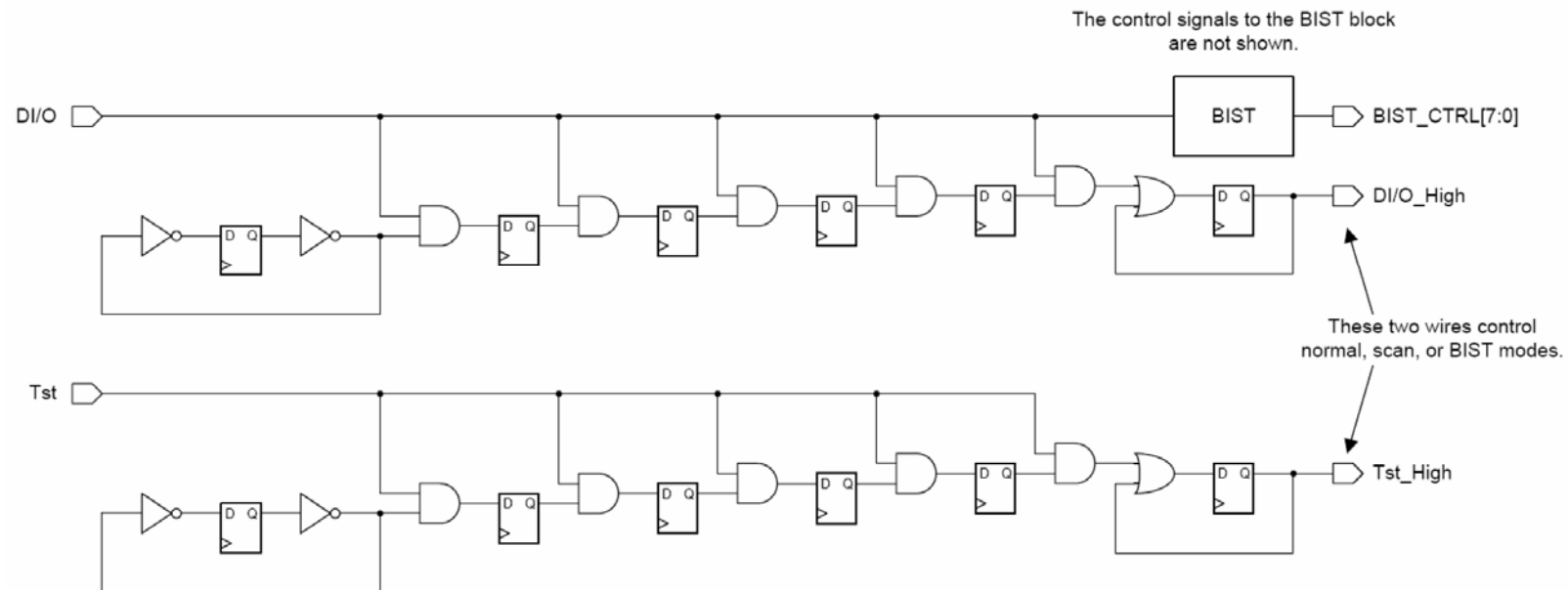
Case Study

- There are many possible methods for reading on-chip EEPROMs
 - Sometimes test modes can be discovered to read these
 - Other times microprobing can help
 - Chip microsurgery using focused ion beam (FIB) is also possible



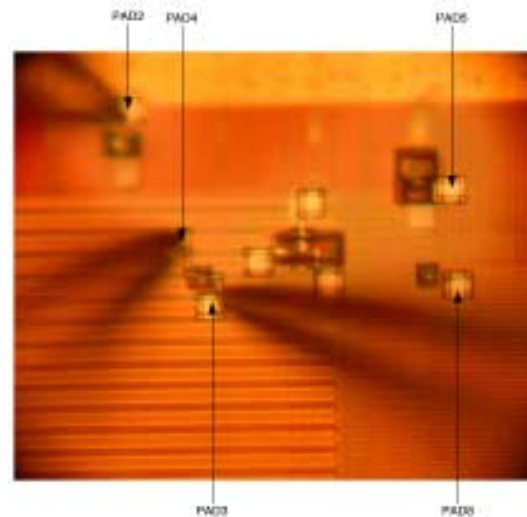
Case Study

- Step 1: what modes exist:
 - In this case our circuit analysis revealed 3 modes on this chip: normal, scan, and built in self test (BIST)



Case Study

- We considered using a test mode to read the EEPROM, however
 - BIST only returned a PASS or FAIL, no data
 - Scan did not run through the EEPROM data, but did allow access to most registers
- Another option: load data and control using scan, then switch to normal mode to read memory, then switch back to scan to read out memory
 - However, the only way to switch modes was to power down, erasing the state just set
- Solution: FIB microsurgery to enable switching modes while powered



Case Study

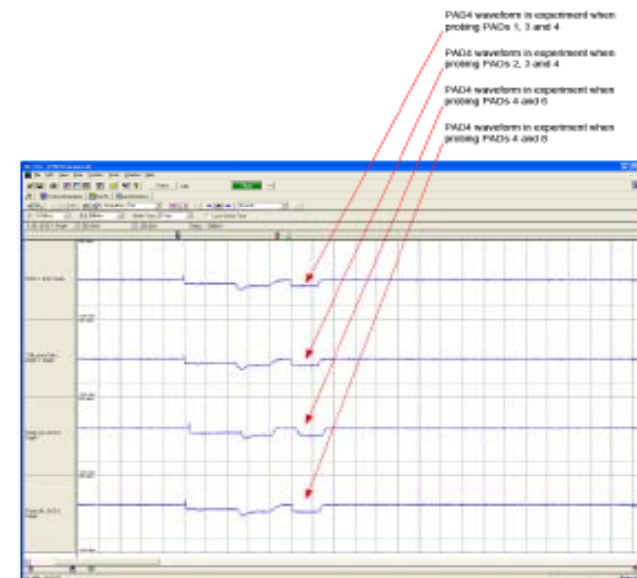
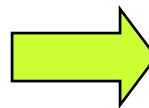
- We then took a few chips and:
 - Jet-etched the package off, leaving the chip operational
 - Removed the top layer of glass
 - Cut some on-chip wires, and added others
- Through analysis of the extracted schematics of the EEPROM access circuits and digital logic, determine the state required to read the EEPROM
- Using our altered chips, load in this state through the scan path, switch to normal mode to read EEPROM, and switch back to scan to read it out.
- Success: the EEPROM was read
- Next this memory data is added to our model of the chip



Case Study


- Now we could run top level test cases captured from system using our extracted keys: success, the outputs of simulation matched the captured system data
- Now we can also create new test cases if desired
- The full netlist means that all nodes in the chip are observable!

```
// File      : Dig_Top_TB.v
// Generated : Tue Jan 20 11:39:10 2009
// From      :
// c:\Dig_Top\TestBench\Dig_Top_TB_settings.txt
// By       : tb_verilog.pl ver. ver 1.2s
//
//-----
//
// Description :
//
//-----
`timescale 1ns / 1ps
module Dig_Top_tb;
//Internal signals declarations:
wire X24_Z;
wire X37_Z;
wire X41_Z;
wire X100_Z;
```



Case Study

- Results of sims can be used to understand functions
- And datasheet type information can be collected



TEXAS
INSTRUMENTS
www.ti.com

bq27010, bq27210

8 AUGUST 2008 – APRIL 2009, REVISED JANUARY 2007

APPLICATION INFORMATION

Control and MODE Registers (CTRL/MODE) — Address 0x000x01

The device control register is used by the host system to request special operations by the bqJUNIOR. The highest priority command set in the MODE register is performed when the host writes data 0xA9, 0x58, or 0xC5 as indicated to the control register. The CTRL register and MODE bits 5, 4, 3, 1, and 0 are cleared when the command is accepted. The host must set the appropriate command bit in MODE before sending the command key to CTRL.

Mode Register (MODE) — Address 0x01

	BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
COMMAND KEY = 0xA9	GPEN	GPSTAT	WRTNAC	DONE	PRST	INIT	FRST	SHIP ⁽¹⁾
COMMAND KEY = 0x58	GPEN	GPSTAT	CEO	CIO	WNACCI	INIT	VRTCVC	WRTLMD
COMMAND KEY = 0xC5	GPEN	GPSTAT	LROCF	LROCFV	LROCFM	INIT	LROCFG	LROCFM

(1) bq27010 only

GPEN GPEN sets the state of the GPIO pin. A 1 configures the GPIO pin as input, while a 0 configures the GPIO pin as an open-drain output. This bit is initialized to the value of bit 7 of the 8x01G register in the EEPROM. The user should keep this bit set or cleared as desired when other bits in this register are written.

GPSTAT GPSTAT sets the state of the open drain output of the GPIO pin (GPEN = 0). A 1 turns off the open drain output, while a 0 turns the output on. This bit is set to 1 on POR. When the GPIO pin is an input (GPEN=1), this bit returns the logic state of the GPIO pin. The user should keep this bit set or cleared as desired when other bits in this register are written.

WRTNAC WRTNAC is used to transfer data from the AR registers to NAC. Other registers are updated as appropriate. This command is useful during the pack manufacture and test to initialize the gauge to match the estimated battery capacity.

DONE DONE is used to write NAC equal to LMD. Useful if the host uses a charge termination method that does not allow the monitor to detect the taper current. The host system could use this command when the charging is complete to force update of internal registers to a full battery condition.

PRST Partial reset. This command requests a reset of all RAM registers except NAC, LMD, and the CI bit in FLAGS. This command is intended for manufacturing use.

INIT The INIT status bit is set to 1 by the bqJUNIOR if there is a full reset or if data corruption is detected in the internal memory containing EEPROM coefficients. Either of these events will cause the bqJUNIOR to update internal memory values. If NAC, LMD, CVCT, or EEPROM-initialized coefficients need to be modified from their original values, the host should first update the values and then clear the INIT bit. The INIT bit is not cleared by the bqJUNIOR.

FRST Full reset. This command bit requests a full reset. A full reset reinitializes all RAM registers, including the NAC, LMD, and FLAGS registers. This command is intended for manufacturing use.

SHIP This command bit requests that the device (bq27010 only) should be put in ship mode. See the Power Mode section for a description of the ship mode. This command is intended for manufacturing use.

CEO This command bit requests that the external offset value is measured. Care should be taken to insure that no charge or discharge current flows during the time this measurement is made. The external offset value is the total offset of the DSOC plus any external PCB effects. The result can be read in 0x256. The result is a signed number with an LSB value of 1.225 μ V. The command takes approximately 5.5 seconds to make the measurement. This command is intended for manufacturing use. The CIO offset value may be subtracted from the CEO offset value to determine the external board offset. This value can be programmed into PKCF[0:2] in the EEPROM for automatic compensation of this external offset value.

CIO This command bit requests that the internal offset value is measured. The internal offset value is

Submit Documentation Feedback

13

Summary

- I have reviewed the reverse engineering of electronic systems, circuits, and component structures.
- RE of semiconductors requires state-of-the-art, leading-edge equipment.
- There are many different techniques used to understand chips.
- It is possible to extract operational and manufacturing information as well as system, circuit, and process.
- Chipworks uses all these methods to gain an understanding of how chips work.



Acknowledgement

I would like to thank Chipworks' laboratory staff and analysts, who actually do all the hard work of analyzing these complex devices. They do a great job!

