



CHIPWORKS

INSIDETECHNOLOGY

## The state-of-the-art in Semiconductor Reverse Engineering (RE101)

Randy Torrance  
21<sup>st</sup> May 2008

INSIDETECHNOLOGY

### Agenda

- About Us
- The What and Why of Reverse Engineering
- Product Teardowns
- System Analysis
- Process Analysis
- Circuit Analysis
- Schematic/Image viewing in **ICInside** Browser



CHIPWORKS

www.chipworks.com

## 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
  - Process Analysis – how chips are built, and what are they made of
  - Circuit Analysis – how chips work



## 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?

To provide competitive technical intelligence (Or patent infringement intelligence.) Technical intelligence is uniquely fact-based and helps answer questions that fit neatly into the goals of several stakeholder groups.



## Why Use Reverse Engineering to Reduce Design Cost?

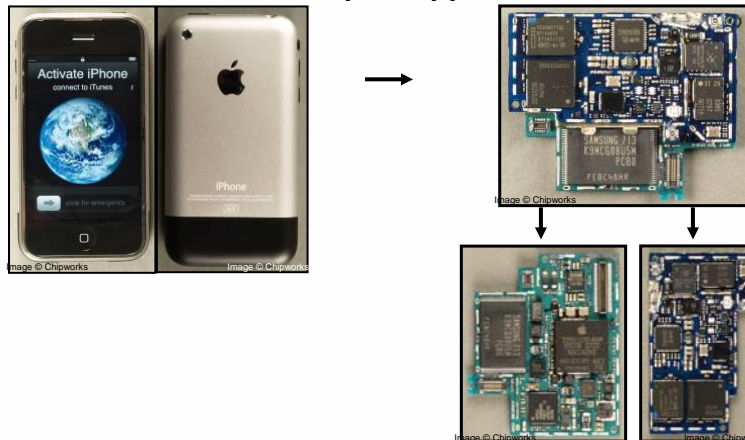
- Average design costs are now ~\$4M with a 12% CAGR in the last 5 years
- Number of new designs decreased from just over 6000 to just under 5000 in the same time period.
- Reverse engineering ensures that you meet or exceed your competitors devices and not just the specification
- Reverse engineering is used successfully with 95% of the big semiconductor companies counted among Chipworks customers

Source: VLSI Research



## The Start to Reverse Engineering

### Product Teardown – example: Apple's iPhone



## iPhone Product Teardown - iPod board

INSIDETECHNOLOGY

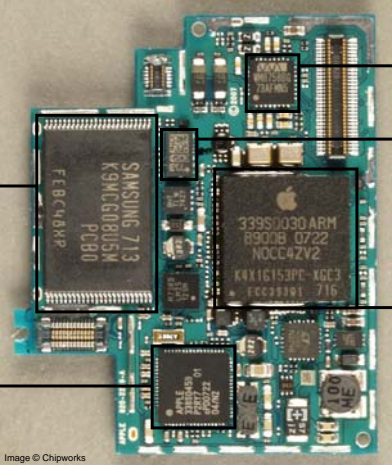


Image © Chipworks

**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**



www.chipworks.com

## iPhone Product Teardown - Wireless board

INSIDETECHNOLOGY

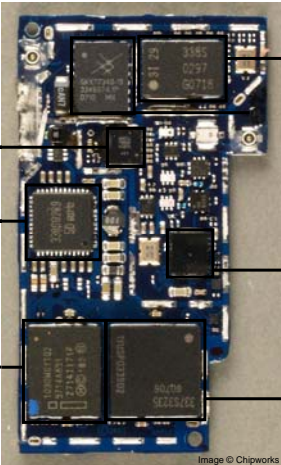


Image © Chipworks

**CSR 41B14 BlueCore4-ROM**

**Infinion GSM transceiver(?)**

**Intel PF38F1030W0YTQ2 32 Mb NOR Flash + 16 Mb PSRAM**

**EDGE MCP including Peregrine SP4T RF switch**

**Skyworks SKY77340 power amplifier module**

**Marvell W8686B13 WLAN**

**Infinion PMB8876 S-Gold2 baseband processor**



www.chipworks.com

## Types of System Analysis



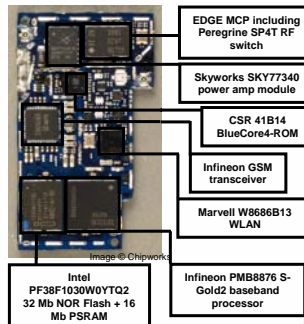
- **Hardware analysis:**
  - Reverse-engineering at the circuit or board level
  - Functional analysis using test stimulus and monitoring outputs and internal signals
- **Software analysis:**
  - Software reverse engineering involves extraction and reconstruction of embedded code
  - Software functional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



www.chipworks.com

## System Analysis - Hardware Reverse Engineering

- **Teardown device**
  - Screwdrivers, etc
- **Identify components**
  - Datasheets, web, internal part numbering maps
- **Remove components**
- **Delayer boards**
  - Delayering station
- **Trace connections**
  - IC Inside (our circuit analysis software)
- **Draw schematics**
  - IC Inside, Cadence Composer



INSIDETECHNOLOGY



www.chipworks.com

## System Analysis - Hardware Functional Analysis

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



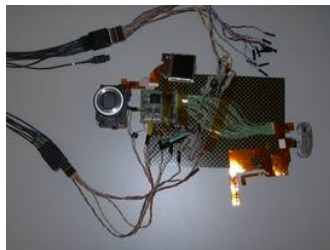
Examine patent...



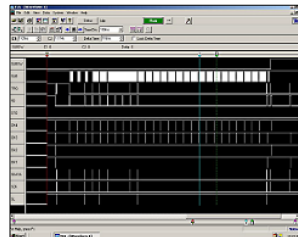
...disassemble camera to get a dismembered but functioning camera...



## 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



```

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 02 F0 21 E3 00 00 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 20 A0 E3 00 00 81 E5 04 10 81 E2
00000050 02 00 51 E1 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 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
000000B0 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
    
```

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...

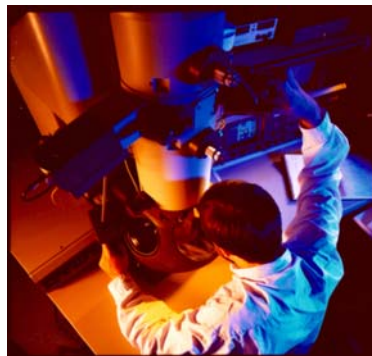


CHIPWORKS

www.chipworks.com

## Process Analysis

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



CHIPWORKS

www.chipworks.com



## 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

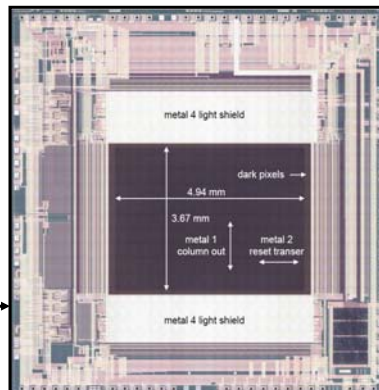
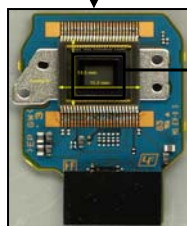


## Process Analysis – Sony's Clearvid IMX013 4-Mpixel CMOS Image Sensor

Extracted from Sony DCR-DVD505 Handycam

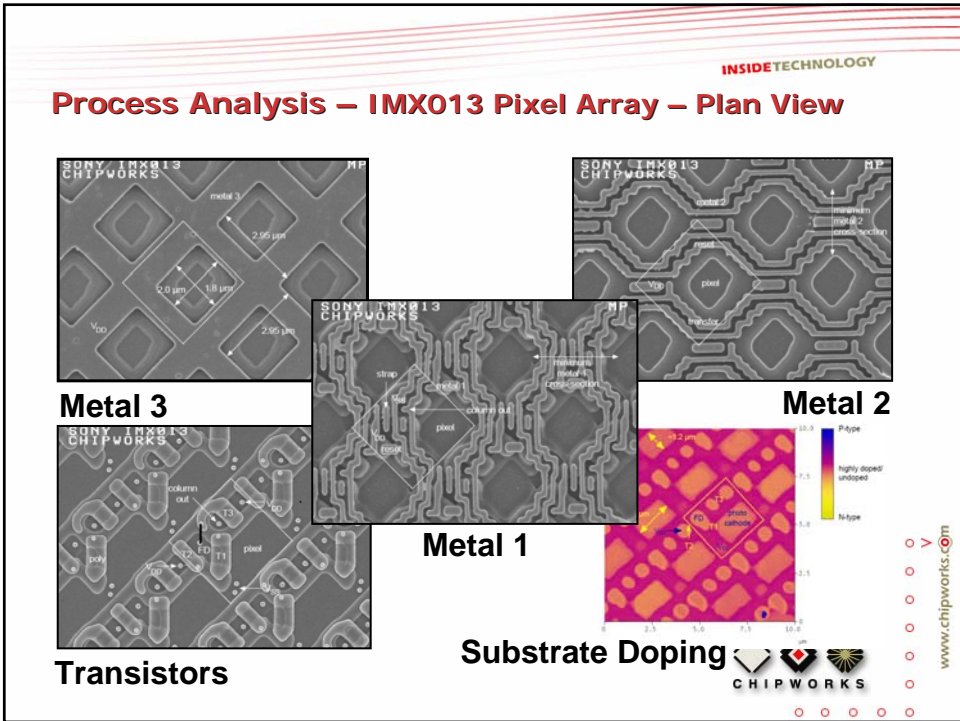
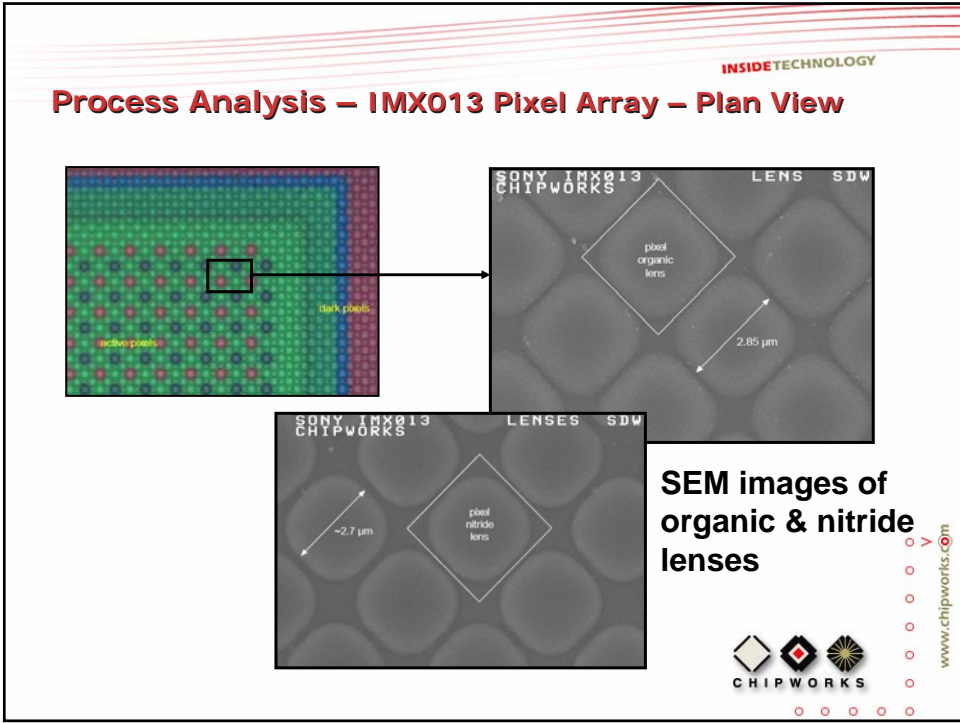


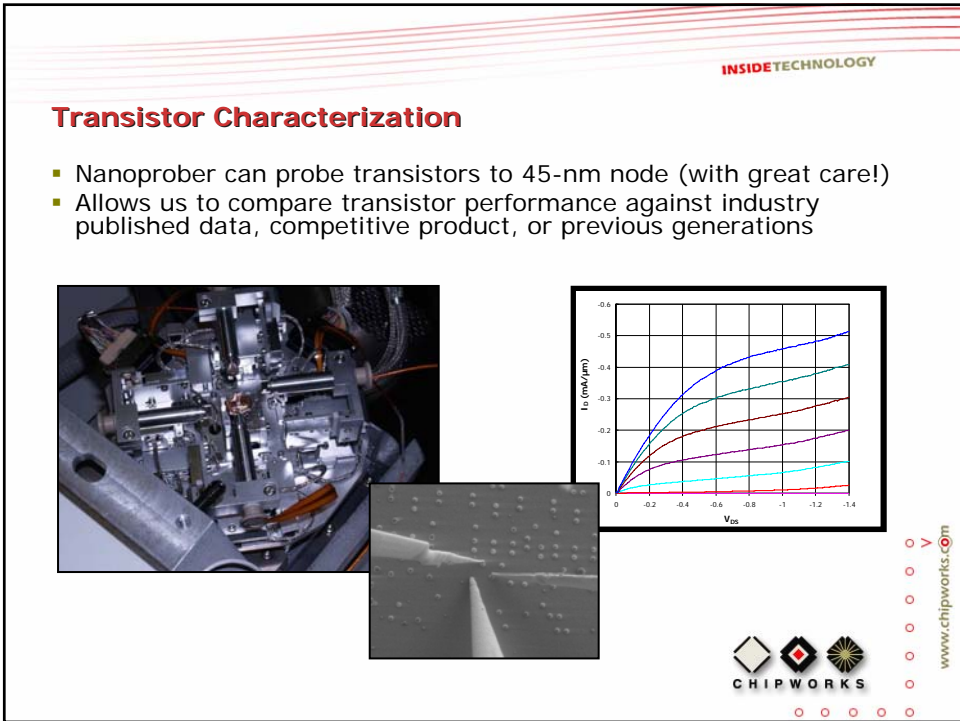
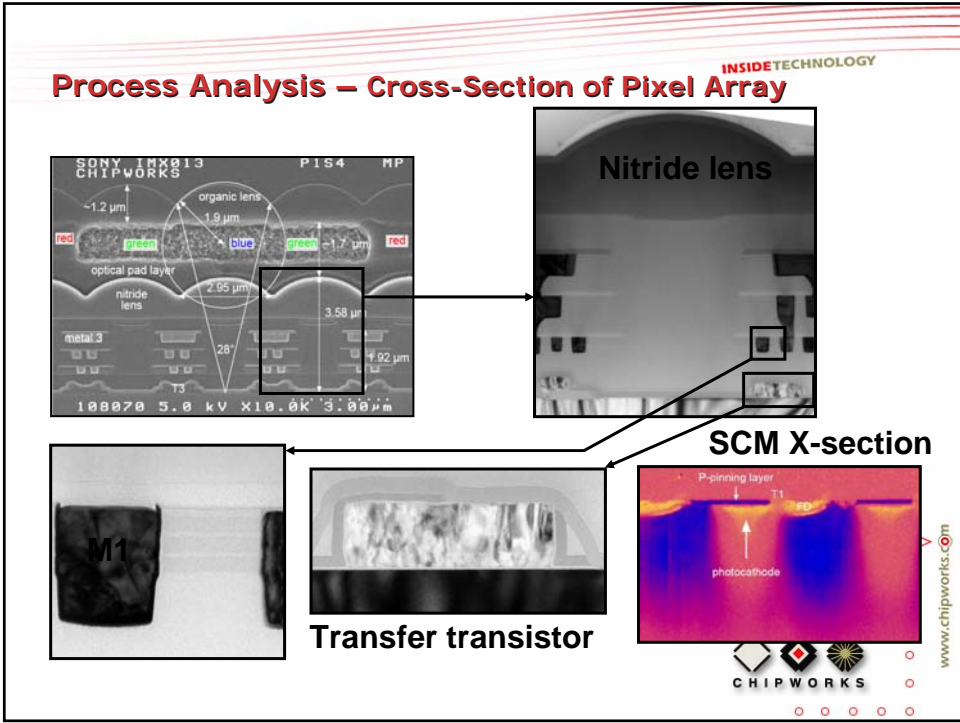
Sensor module



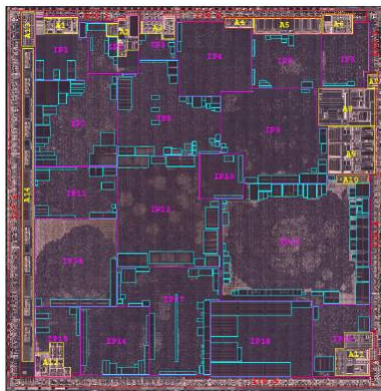
Die photo



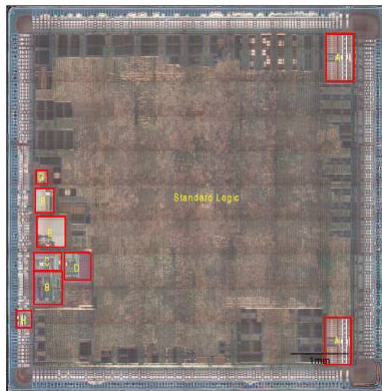




## Functional Analysis – Understand the Architecture



Analog VS Embedded Memory, Standard Logic, I/O



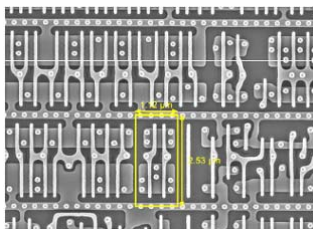
Block Identification



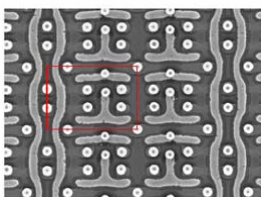
www.chipworks.com



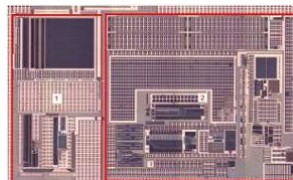
## Functional Analysis – Cell Topology and Layout



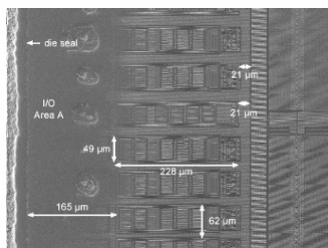
NAND Cell



6T SRAM



Analog Blocks

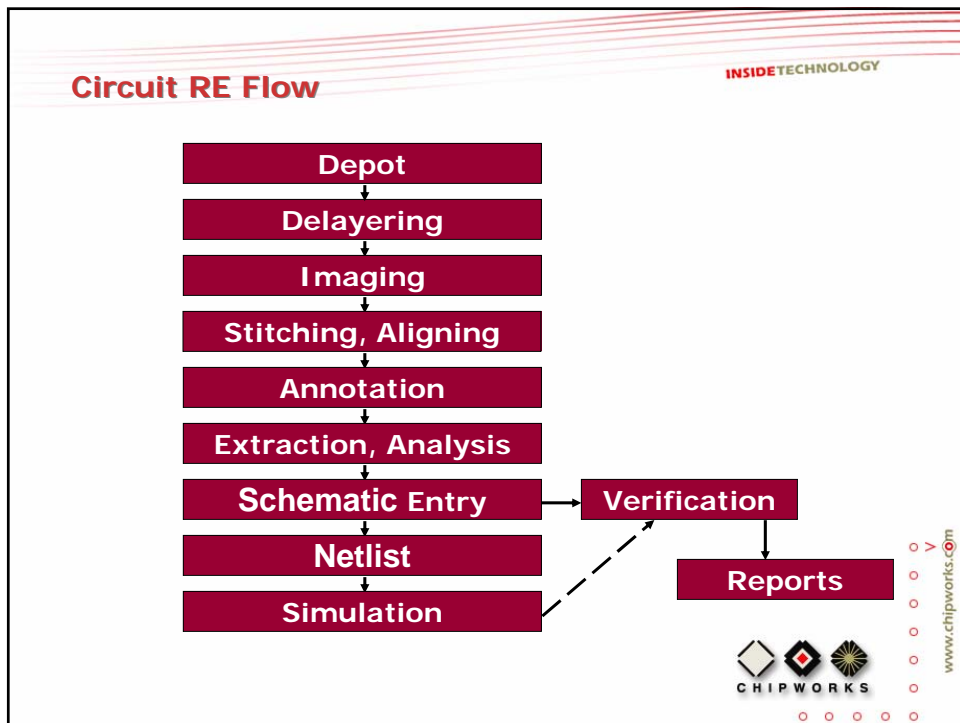
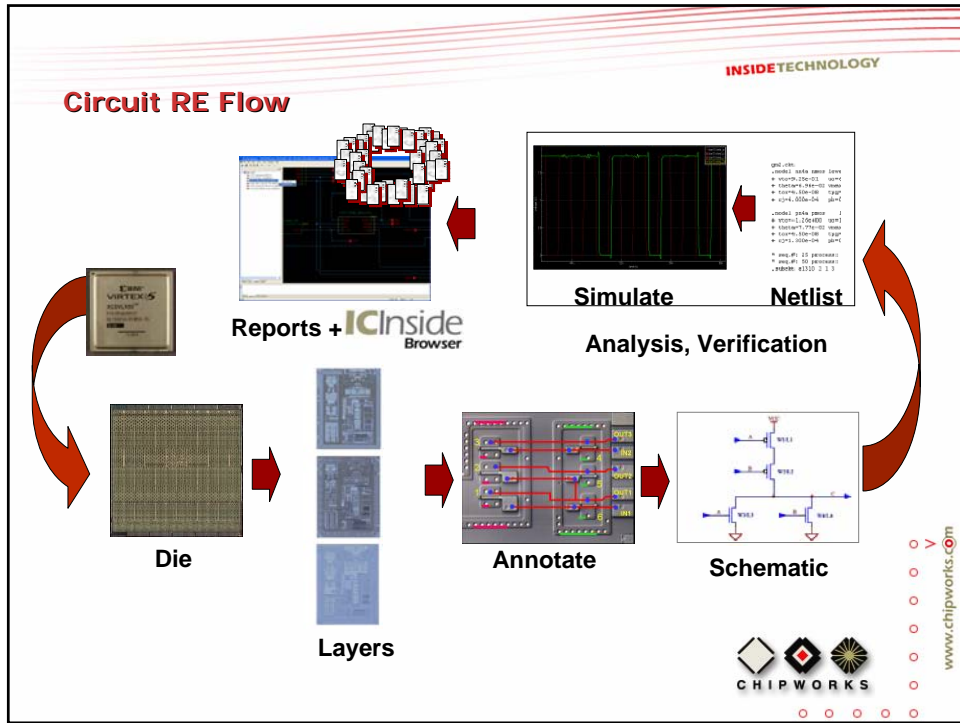


IO's



www.chipworks.com





## 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

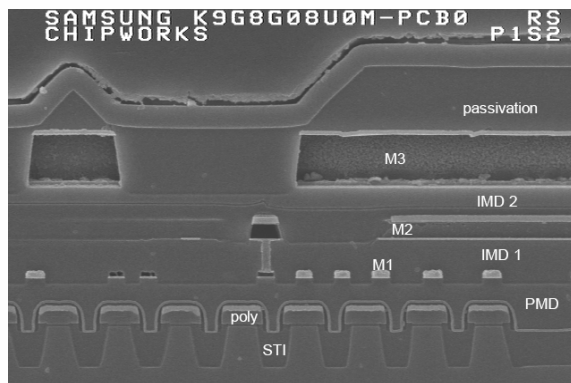


www.chipworks.com



## Circuit Analysis – Delayering

- Take cross-section SEM photo to identify layers



Samsung 8-Gb NAND Flash Memory

- No two chips are alike:
  - Bip, CMOS
  - 0.5um, 45nm
  - LP, HS, options
  - Low-K
  - Copper
  - Gold
  - Mixed metals
  - MEMs
  - Stacked die

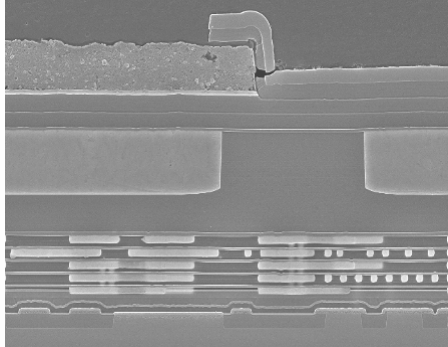


www.chipworks.com



## Delayering

An example:



SEM cross-section of 65-nm TI baseband processor for Nokia

- Metals: Al, Cu, TiN, TaN
- Metal thickness: 0.15 $\mu$ m to 1.4 $\mu$ m
- Dielectrics: silicon nitride, oxynitride, oxide, SiOC, SiONC, and PSG
- Dielectric thicknesses: 47nm to 2.6 $\mu$ m



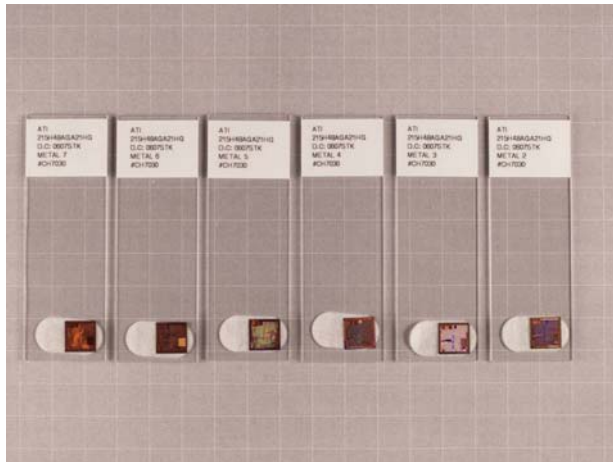
## Circuit Analysis – Delayering

- 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)
  - Polishing



## Delayering

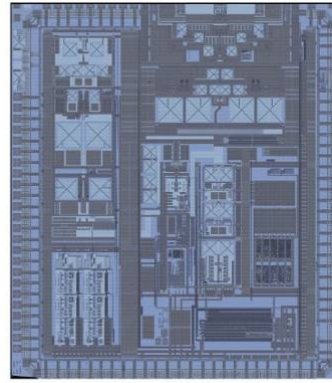
- A sample is prepared for each metal interconnect layer, polysilicon layer and substrate diffusions.
  - e.g. for 4 metal layer device, need to prepare 6 samples



## Delayering



Atheros AR5110 - Metal 5

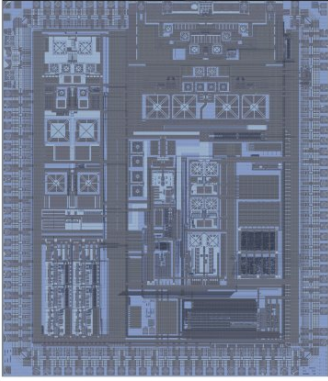


Atheros AR5110 - Metal 4

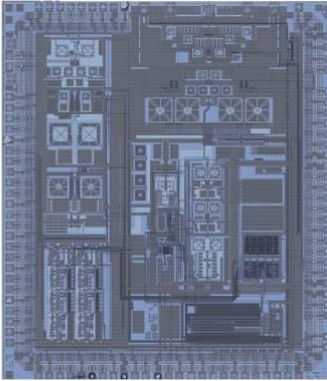


**INSIDETECHNOLOGY**


**Delaying**



Atheros AR5110 - Metal 3



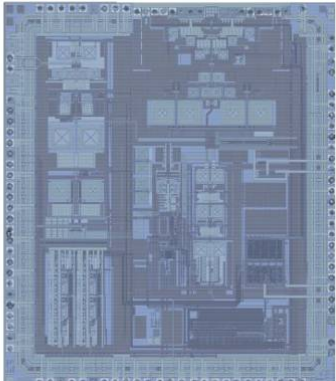
Atheros AR5110 - Metal 2



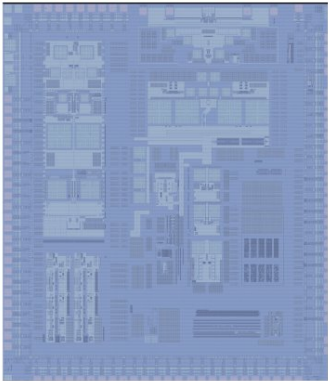
www.chipworks.com

**INSIDETECHNOLOGY**


**Delaying**



Atheros AR5110 - Metal 1

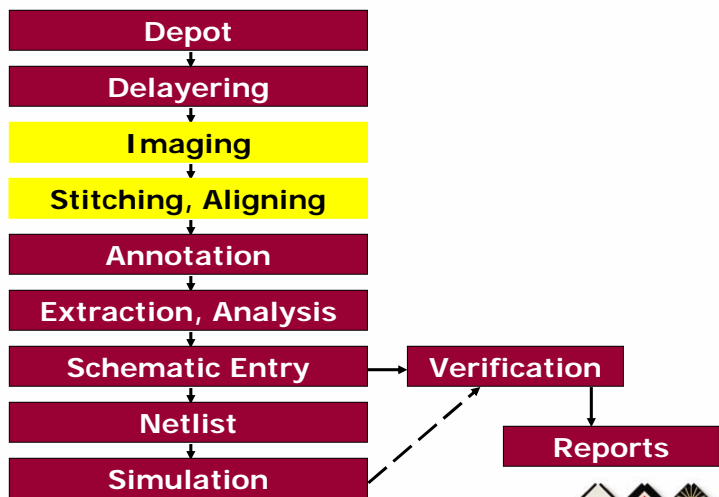


Atheros AR5110 - Poly



www.chipworks.com

## Circuit RE Flow



## Image Capture

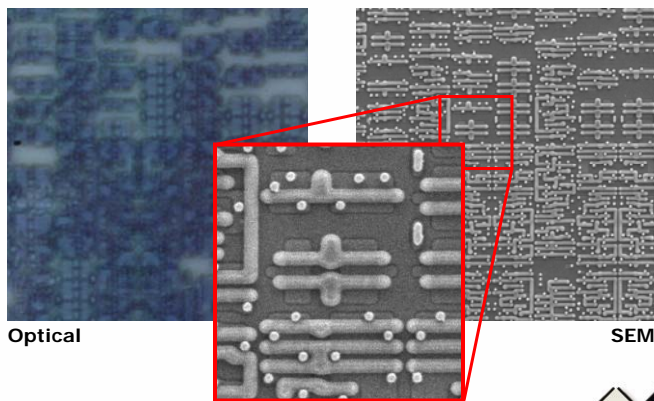
- Capture high magnification images using microscope (SEM and optical), automated stage and digital camera
- Use software to stitch all the images together, and for inter-layer registration



### Image Capture

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

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



Optical

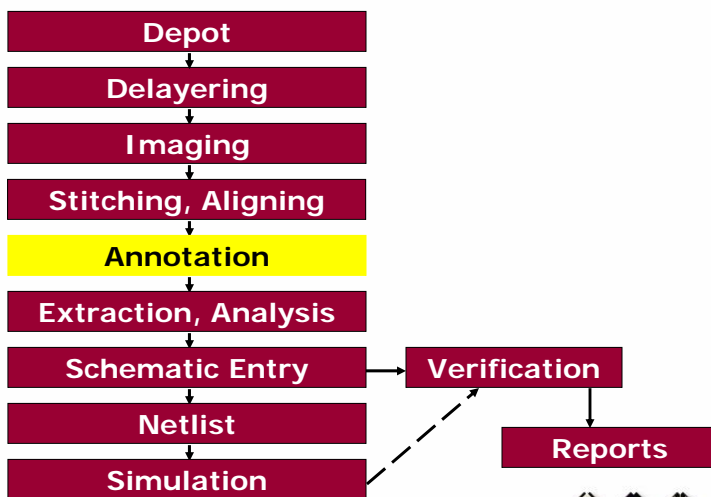
SEM



www.chipworks.com



### Circuit RE Flow



www.chipworks.com



### Annotation

The olden days...



### Annotation

The olden days...



## Annotation

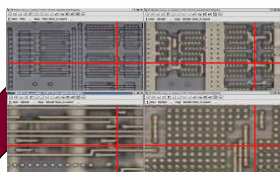
The olden days...



www.chipworks.com

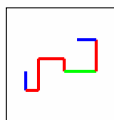
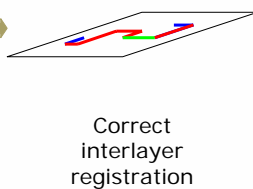
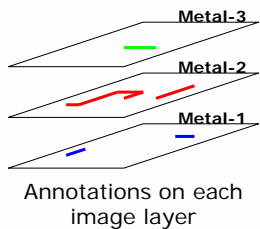


## Annotation



### Software Automation

- Wires are traced on the layer where they appear
- Annotations are visible in any/all views
- Lock-step cursors make layer changes easy to follow



Fast, accurate circuit extraction

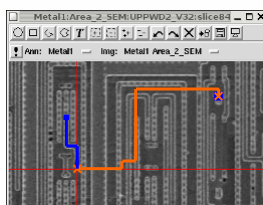
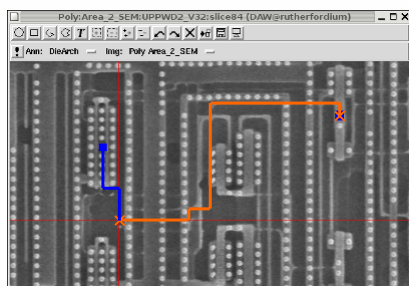


www.chipworks.com



## Annotation

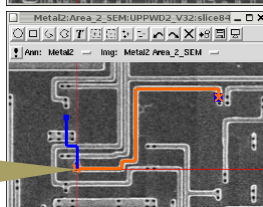
Synchronized multi-layer display and annotation:



Wires are traced on the layer where they appear

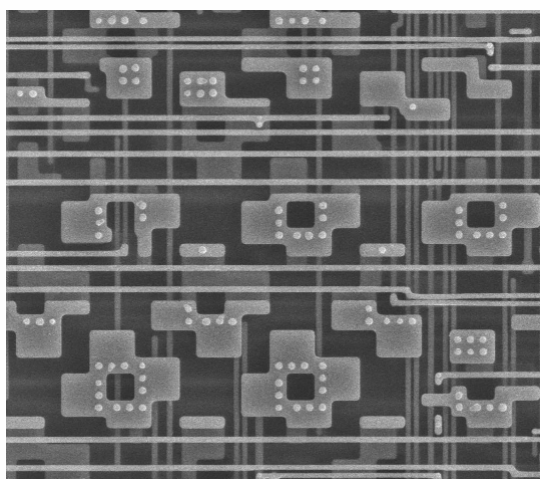
Annotations visible in any/all views

Patented lock-step cursors make layer changes easy to follow



## Annotation – Polygon Feature Extraction

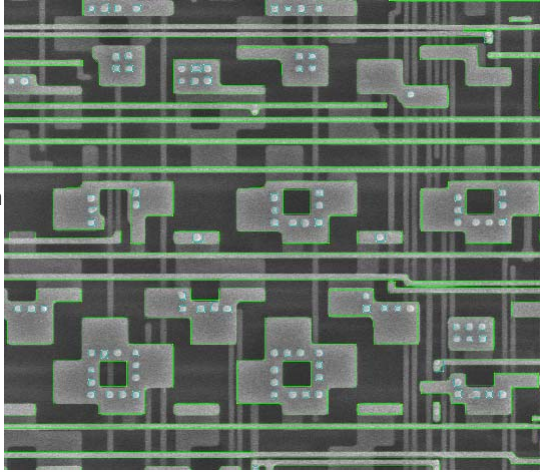
Raw M4 layer image



INSIDETECHNOLOGY

## Annotation – Polygon Feature Extraction

Edge Detection



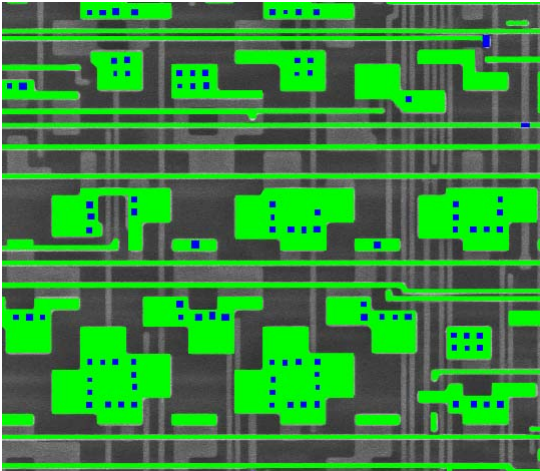
www.chipworks.com

CHIPWORKS

INSIDETECHNOLOGY

## Annotation – Polygon Feature Extraction

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

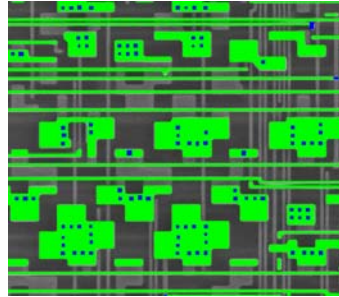


www.chipworks.com

CHIPWORKS

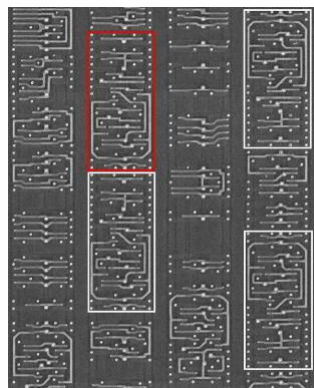
## Circuit Analysis – Polygon Feature Extraction

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



## Annotation – Ever More Automation

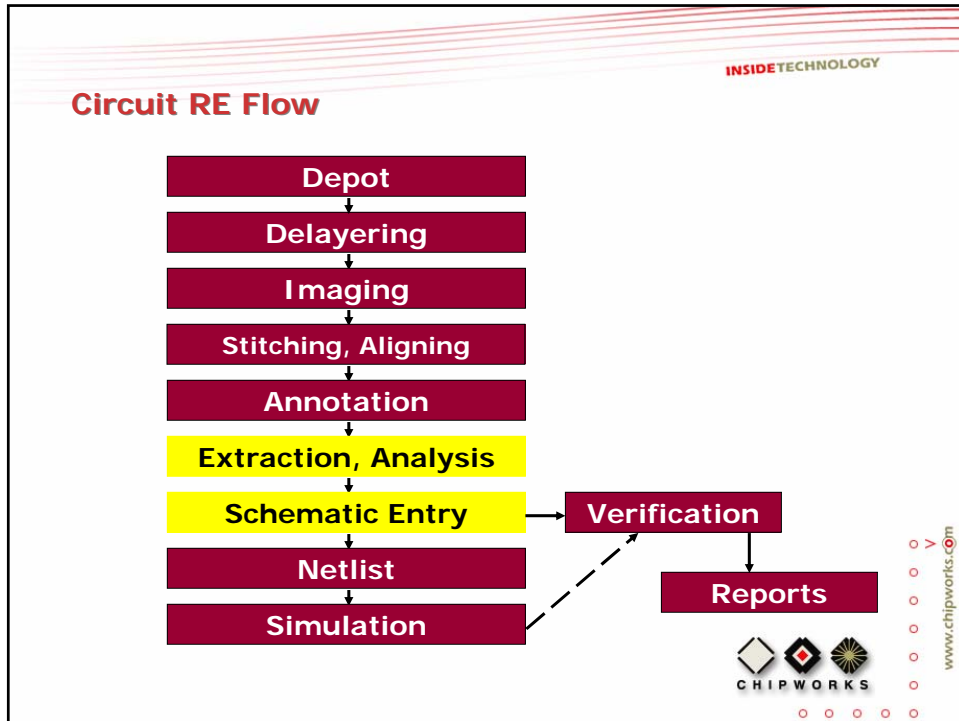
- Further automation is possible after the feature recognition:
  - After wires are annotated vias can often be placed automatically
  - Once a device is defined, identical instances of this device can be searched for and found using pattern matching image recognition
    - This is especially useful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



Standard cell recognition







INSIDETECHNOLOGY

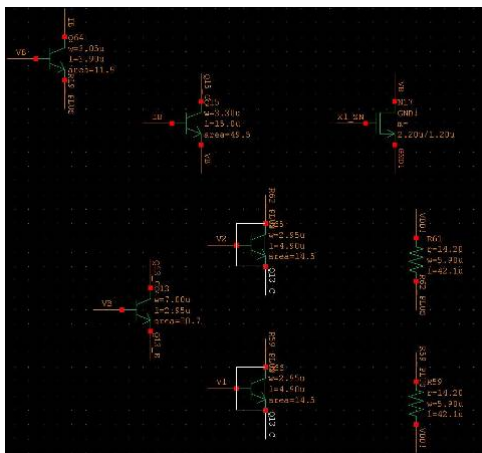
## Schematic Readback

- Two methods are available for moving from annotated images to schematics or netlist:
  - Manual extraction
    - Used by experienced analysts for sub-circuits where the schematic is quickly visible from the images
    - Can be a very efficient method of simultaneous circuit extraction and analysis, since the schematic can be organized as it is drawn.
  - Automated extraction
    - Very useful for large blocks of circuitry, and is especially valuable for digital blocks.
    - Devices are placed in schematic in the same locations they occupy in the layout
    - Becoming the norm, since it creates a schematic “correct by design”

www.chipworks.com

CHIPWORKS

## Schematic Readback



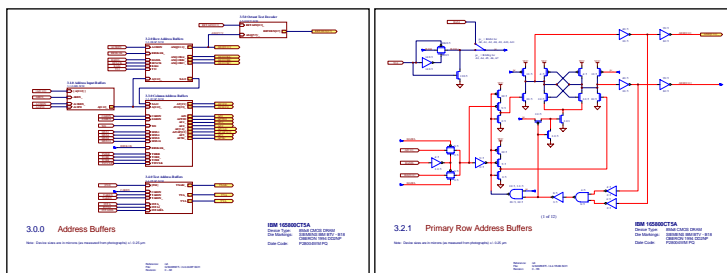
- Auto-extracted devices placed relative to layout positions
- A random arrangement of transistors or gates does not convey a great deal of information



www.chipworks.com

## Analysis

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



www.chipworks.com

## Analysis

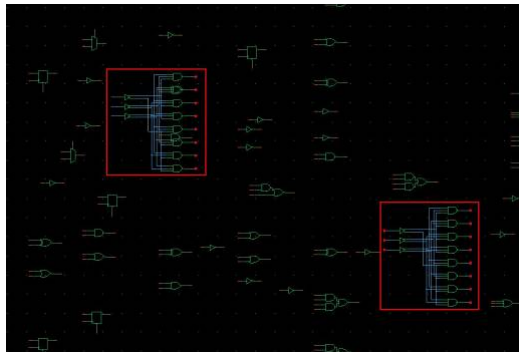
### Tools

- 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
- A specialized RE schematic editor 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

- Auto-extracted devices placed as per the layout to give a flat, unorganized schematic
- One instance of a sub-circuit defined manually, others matched and organized automatically
- Can place in sub-cells



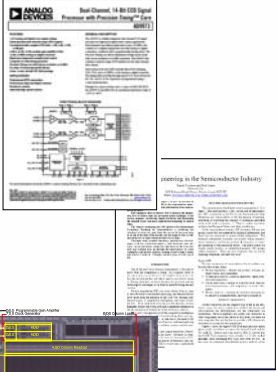
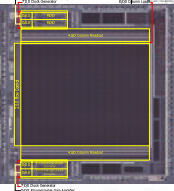
Example sub-circuit search and organization




**INSIDETECHNOLOGY**

## Analysis

- **Re-creating meaning**
  - Public information and datasheets can help with schematic organization
  - Technical papers from journals and conferences hold interesting clues
    - IEEE Explore
  - 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.

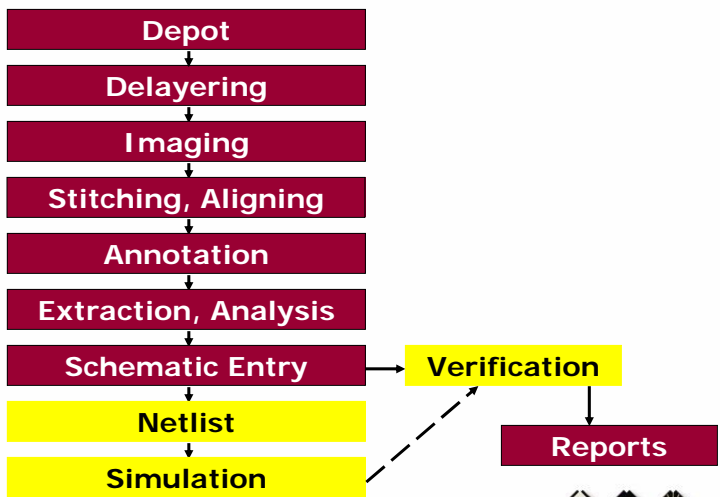



www.chipworks.com



**INSIDETECHNOLOGY**


## Circuit RE Flow



```

graph TD
    Depot[Depot] --> Delaying[Delaying]
    Delaying --> Imaging[Imaging]
    Imaging --> Stitching[Stitching, Aligning]
    Stitching --> Annotation[Annotation]
    Annotation --> Extraction[Extraction, Analysis]
    Extraction --> Schematic[Schematic Entry]
    Schematic --> Netlist[Netlist]
    Netlist --> Simulation[Simulation]
    Schematic --> Verification[Verification]
    Simulation -.-> Verification
    Verification --> Reports[Reports]
  
```

www.chipworks.com



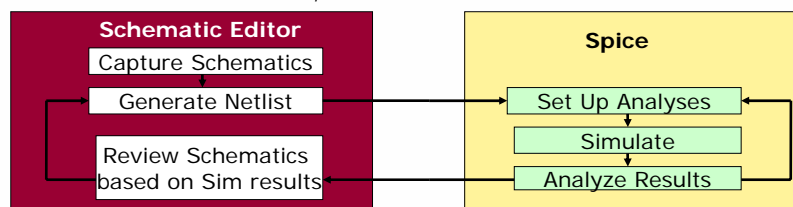
## Verification

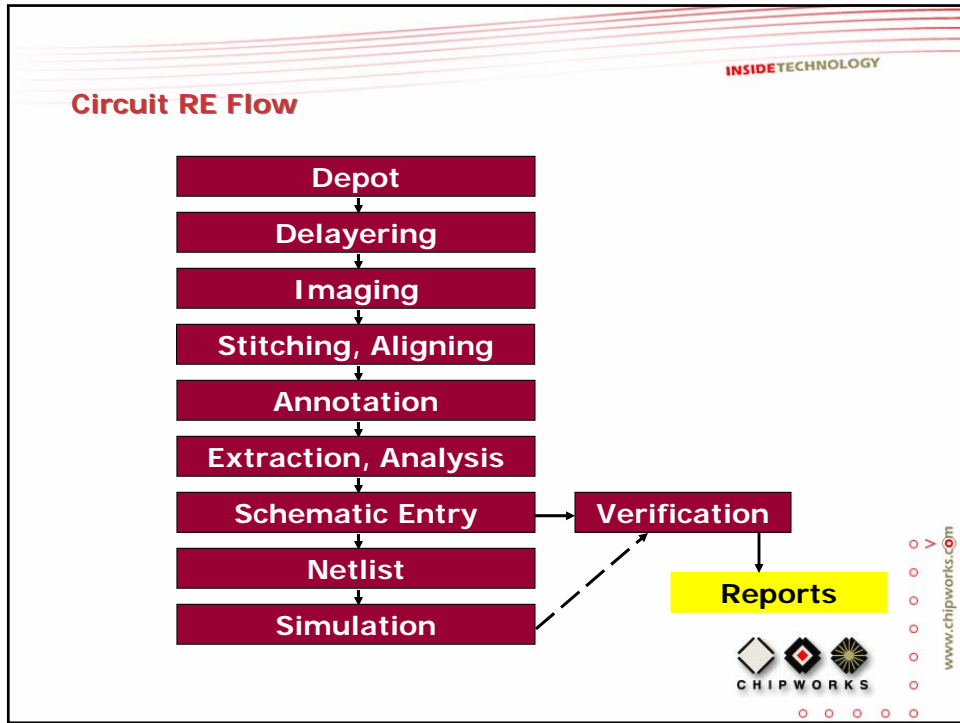
- As with forward design, the first pass schematic is not always 100% correct
- However, in contrast to forward design, 100% correct is normally less essential:
  - Clients are usually most interested in circuit structure
  - Device sizes only need to be approximate
    - Even if simulation is desired, we rarely have process models for competitive chips, and hence accurate device sizes are not critical
- Of course, device sizes can only be 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, netlist compare
  - 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





INSIDETECHNOLOGY

## Circuit Analysis - Deliverable

- Organized, readable, hierarchical schematics

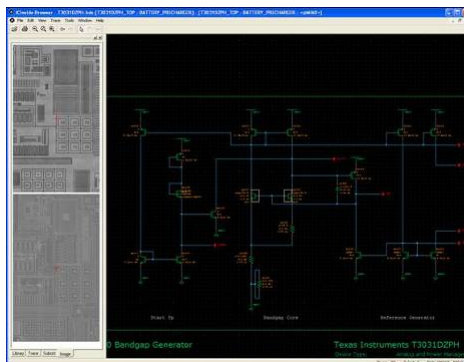
- Optional Outputs: Netlists, simulated waveforms, micro-probed waveforms, block diagrams, timing diagrams, circuit equations

www.chipworks.com

CHIPWORKS

### Chipworks IC Inside Browser

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



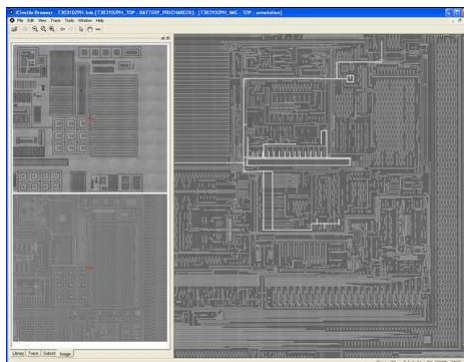
**IC**Inside  
Browser



www.chipworks.com

### Chipworks IC Inside Browser

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



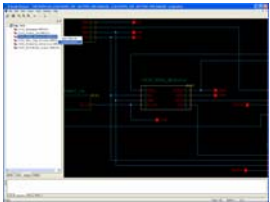

**IC**Inside  
Browser

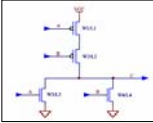


www.chipworks.com

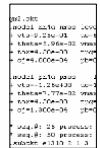
**INSIDETECHNOLOGY**

## Powerful Export Capability

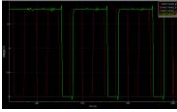





**Schematic Editors  
(EDIF200)**





**Netlist**



**Simulate**

**ICInside  
Browser**






www.chipworks.com

**INSIDETECHNOLOGY**

## 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.
- It is possible to extract operational and manufacturing information as well as system, circuit, and process.
- This provides intelligence for product/process development, marketing, and bench-marking.
- It can also be correlated with patents and other IP to show evidence of IP usage.



www.chipworks.com



## 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!



**If I have seen further it is only by  
standing on the shoulders of giants.**

***-Isaac Newton***

**Chipworks can help you meet your  
competitive intelligence needs**

