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

Randy Torrance
21st May 2008

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

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. Copyrights
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**

- 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

**iPhone Product Teardown - Wireless board**

- CSR 41B14 BlueCore4-ROM
- Infineon 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
- Infineon PMB8876 S-Gold2 baseband processor
**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

**System Analysis - Hardware Reverse Engineering**

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

![Image of embedded components and software tools related to system analysis.](additional_images)
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...

...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

- Extract code...
- Disassemble code...
- Assembler
- '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
Process Analysis – IMX013 Pixel Array – Plan View

SEM images of organic & nitride lenses

Metal 3
Metal 2
Metal 1
Transistors
Substrate Doping
Process Analysis – Cross-Section of Pixel Array

Nitride lens

SCM X-section

Transfer transistor

Transistor Characterization

- Nanoprober can probe transistors to 45-nm node (with great care!)
- Allows us to compare transistor performance against industry published data, competitive product, or previous generations
Functional Analysis – Understand the Architecture

Analog VS Embedded Memory, Standard Logic, I/O

Block Identification

Functional Analysis – Cell Topology and Layout

NAND Cell

6T SRAM

Analog Blocks

IO’s
Circuit RE Flow

- Reports + IC Inside Browser
- Die
- Layers
- Annotate
- Analysis, Verification
- Schematic

Circuit RE Flow

- Depot
- Delayering
- Imaging
- Stitching, Aligning
- Annotation
- Extraction, Analysis
- Schematic Entry
- Netlist
- Simulation
- Verification
- Reports

13
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
- No two chips are alike:
  - Bip, CMOS
  - 0.5um, 45nm
  - LP, HS, options
  - Low-K
  - Copper
  - Gold
  - Mixed metals
  - MEMs
  - Stacked die

Samsung 8-Gb NAND Flash Memory
Delaying

An example:

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

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

Circuit Analysis – Delaying

- 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 3
Atheros AR5110 - Metal 2

Delayering

Atheros AR5110 - Metal 1
Atheros AR5110 - Poly
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
Optical vs. SEM – e.g. TI OMAP1310, 0.13 µm process, transistor layer
- 450 nm optical light just doesn’t cut it anymore

Image Capture

Circuit RE Flow

Depot
Delaying
Imaging
Stitching, Aligning
Annotation
Extraction, Analysis
Schematic Entry
Netlist
Simulation
Verification
Reports
Annotation

The olden days...
**Annotation**

The olden days...

**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
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
Annotation – Polygon Feature Extraction

Edge Detection

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

- 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
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”
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

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
  - 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
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.
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

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
Circuit RE Flow

- Depot
- Delayering
- Imaging
- Stitching, Aligning
- Annotation
- Extraction, Analysis
- Schematic Entry
- Netlist
- Simulation
- Verification
- Reports

Circuit Analysis - Deliverable

- Organized, readable, hierarchical schematics

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

Chipworks IC Inside Browser

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