Reverse Engineering 101

The How and Why of Reverse Engineering for Technical Teams

Written by: Dick James, Senior Technical Advisor

CHIPWORKS

INSIDE • TECHNOLOGY

About Chipworks

At Chipworks, we find out what's inside technology - specifically, what's inside chips, devices, software, almost anything electronic you can think of. Whether you're involved in patent protection or litigation, researching your latest product design, or just trying to find out what the competition's up to, let Chipworks do the analysis for you. We have the expertise to take apart the product - or the patent - to discover its secrets. An internationally-recognized leader in patent portfolio development and technical competitive analysis, Chipworks is headquartered in Ottawa, Canada, with offices and representation worldwide.

RE Spreads Innovation and Helps Companies Stay Competitive

There are a lot of car buffs in the world. And, when we stop to think about it, we realize that when one auto manufacturer launches a new model, the others will buy some, take them back to the plant, and rip them apart to see what new features and technology are inside them. And then, if the new ideas are sales-worthy, they introduce similar innovations in their own models.

We also assume that the shift in technology from Europe and North America to Asia is the result of Asian industries buying products, taking them apart, and copying them.

These are two general examples of what is more precisely known by its practitioners as "reverse engineering" (RE). Specifically, the reverse engineer takes an existing product, and disassembles it in almost a forensic manner so as to look at the component parts and the technology used in its production.

This practice is in wide use across all industries, not as a form of industrial espionage, but as a legitimate and legal method to ensure that your products can compete with your most innovative and most cost-efficient competitor's products.

RE can cover objects from as large as aircraft down to the smallest microchip. Motivation for RE has varied from the paranoia of the Cold War (remember the U2 spy-plane?), through commercial piracy, to competitive intelligence, and courts of patent law.

Aside from the highly-publicised examples of spy planes and Chinese jets landing in Taiwan, if we look back over the last few decades, the reverse engineer has had a significant influence on the dissemination of technology in the electronics industry. Not the least has been the migration of technology to developing countries and the growth of the electronics industry in Asia – a bit of an apocryphal tale, but undoubtedly true.

After all, if you want to get into a new area of business, the simplest thing to do is to buy the existing product and take it apart to see what's in it. Having done that, you know what parts you have to buy, and what technological challenges you face putting your version together. This is a subset of one of the most basic business rules – know the competition!

Don't underestimate the patent business

Texas Instruments and IBM are now estimated to receive more than $1 billion a year in royalty income.

Although the traditional North American image is of a low-cost Asian competitor copying a western design, the reality is that the leading users of reverse engineering are international and multi-national companies. In the global economy, innovation is no longer reserved for the Western nations.

Applications of RE have now become more openly commercial. It is a recognised part of competitive intelligence and is commonly used to support patent licensing activities – both of which are means to spread technology, but on a more controlled basis.

There is also a need to RE archaic parts that are no longer in production, but still need to be replaced in long-lived equipment such as nuclear reactors, airliners, and ships.

A fact of life these days is that simple tear-downs of products are not good enough any more. Advances in electronics technology, namely the massive integration of billions of

individual devices and masses of functions into single components, have forced reverse engineering to evolve into a specialised niche of the profession.

Who needs Reverse Engineering?

There are two distinct uses of reverse engineering in the semiconductor and micro components industries.

Patent Intelligence

The first application is in the defence of intellectual property (IP). Patent lawyers and patent licensing teams use reverse engineering information to identify devices that infringe on their intellectual property. This can be for the purpose of litigation to protect their well earned market position, or for licensing to generate additional revenue from their IP. Also, if a company is on the receiving end of a patent complaint, RE can also be used as a defensive activity to invalidate a patent by showing prior use.

Competitive Technical Intelligence

In the competitive intelligence field, the technical and product teams that are designing and selling semiconductor devices use the information for multiple reasons:

1) To speed their time-to-market and time-to-profit through reduced costs and faster revenue
2) To reduce the design risk in highly innovative markets by benchmarking best-practices
3) To identify what is real and what is hype around competing products in order to win the sockets on both price and proven features

Design teams are being demanded more-and-more to look outward to ensure that they are fully understanding the customer and fully understanding their competitive landscape. When the CEO demands, 'What do you know about the competition?', you need to be armed with the answers.

Chipworks delivers these answers by delivering timely, high-quality reverse engineering of the tiniest devices. We do this with a combination of state-of-the-art electron microscopy, 1000's of pages of wet lab procedures, proprietary software and tools, and years of design and reverse engineering experience.

RE in the Electronics Industry

At least in the case of semiconductors, RE is protected in the United States by the Semiconductor Protection law, which allows it "…for the purpose of analysis, evaluating or teaching…" Other countries have similar legislation.

The competitive technical intelligence customers are usually within manufacturing companies, performing product development, or doing strategic marketing or bench-marking studies. The patent intelligence clients are usually patent lawyers or intellectual property (IP) groups within manufacturing companies. There are also an increasing number of companies that are purely licensing companies, and only deal in IP.

Reverse engineering of electronics products can broadly take several forms:

- Product tear-downs – identify the product, package, internal boards, and components
- System level analysis – analyse operations, signal paths, and interconnections
- Circuit extraction – delayer to transistor level, then extract interconnections and components to create schematics

•Process analysis – examine the structure and materials to see how it is manufactured, and what it is made of.

Basic Analysis

Product tear-downs are the simplest type of RE in electronics; the device is dissembled, the boards and sub-assemblies photographed, and a description o the components is noted. Chipworks is usually only interested in what is in the device at this level, but there are also companies that use the data to provide a bill of materials and tentative costing for the manufacture. Figure I shows a Panasonic-made NTT FOMA mobile phone partly torn down to expose the smaller LCD display and the camera sub-unit.

Figure 1. NTT FOMA Cellphone

System level analysis can be very complex, depending on what degree of analysis is required. As an example in a patent context, we needed to know exactly how a digital camera worked in order to prove use of invention. We took several cameras apart to get one dismembered but functioning camera, and connected probes between the interfaces and a logic analyzer. Then we carefully studied the device's timing, and by comparing the results with the patent claims, produced evidence that the camera operation used the invention. Figure 2 shows the sequence of events followed to examine the camera's functions.

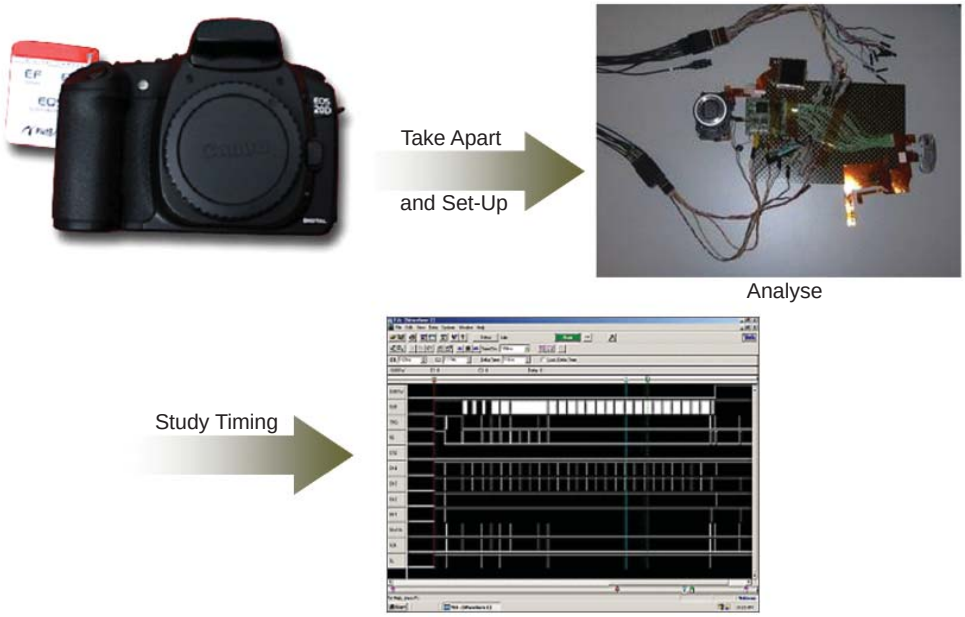


Figure 2. Digital Camera Analysis

Circuit Extraction

Circuit extraction of semiconductor chips has been become progressively more difficult as device dimensions shrink, if not almost impossible.

In the "olden days", we simply used to take lots of photographs of the different layer of a chip, tape them together, and crawl around on the floor marking up the interconnects.

Figure 3. Simpler Days in RE!

Today we have 50-nm transistor gate lengths, way beyond the resolution of optical microscopes, and we use electron microscopes just to see the transistors. This is essentially what has made RE of semiconductor circuitry such a specialized business.

Now we need a dedicated SEM (Scanning Electron Microscope) to image the different layers, and specially developed software to stitch the thousands of images from each layer together with minimal spatial error. At Chipworks we empoy an advanced tool called SEM-ICIS meaning Scanning Electron Microscope with Image Capture and Imaging System. There is no other system quite like it in the world, and only a small handful of less cost-effective options for doing this highly specialized work.

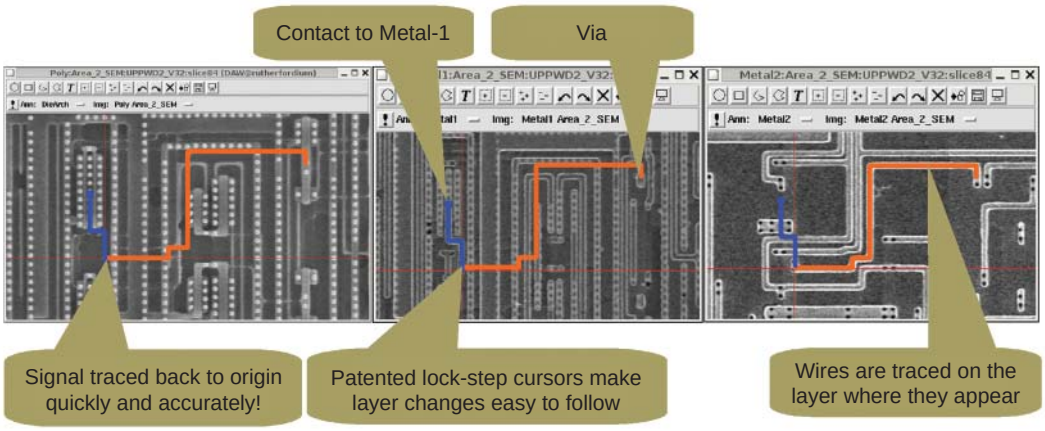


Figure 3. Simpler Days in RE!

Figure 4 shows SEM images from the polysicon transistor layer, and first and second metal levels of a device, with a couple of interconnects marked up for illustration. Full circuit extraction means taking note of all transistors, all contacts/vias between levels, and all interconnects at each level, and then condensing them to a schematic readable by a design engineer. Typically we extract blocks of circuitry at a time, and cross-reference the blocks so that the full schematic is available if required. Not a quick or easy task, but necessary in some circumstances!

In addition to having the advanced microscopy and specialized software to synchronise the multiple layers, doing advanced circuit extraction on todays highly engineered devices requires more specialized path tracing software and a highly trained engineer. The latter is a specialist who has both forward design expertise and reverse engineering expertise.

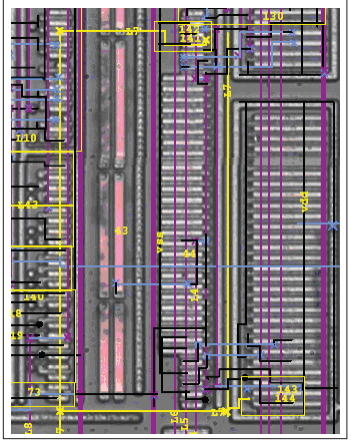
Process Analysis

Process analysis of chips is in some ways more straightforward, since microanalytical tools have been around for some while. Every wafer fab has a range of equipment for process control and failure analysis, and we use the lab-scale equivalent. Using the cellphone example, we were interested in the CMOS image sensor in the camera.

We removed the camera module from the device and took it apart, recording the details until we ended up with the CMOS imager die (Figure 5).

Circuit Surprises

Breaking down a circuit is not always straightforward. Some design clearly demonstrate multiple design loops to handle the lower and higher end functions, and others suggest late bug correction as shown here. Either way, special expertise is needed to make sense of such complicated designs:



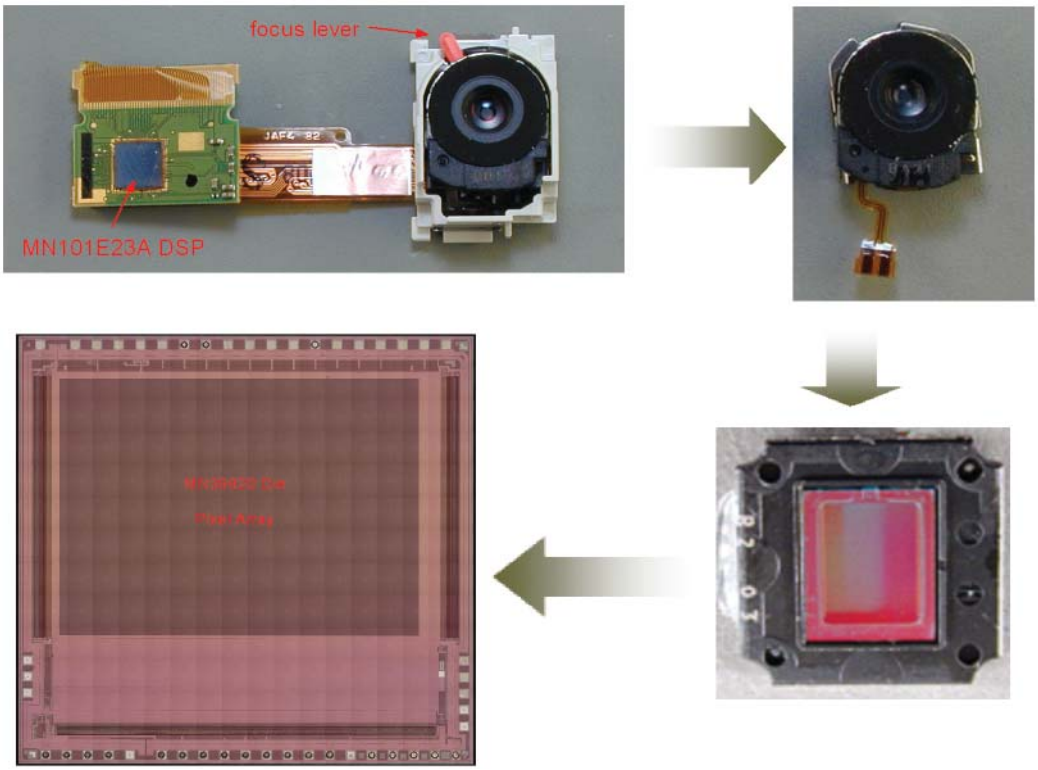


Figure 5. Disassembly of CMOS Image Sensor from Cellphone

Then we begin the actual chip analysis. This part was a fairly leading-edge sensor for the time, with a pixel size of 2.85 x 2.85 µm, so the emphasis was on a detailed examination of the pixel. Figure 6 shows some of the features seen in the pixel area.

A few words of explanation here – TEM (Transmission Electron Microscopy) looks through the sample to give high resolution images of the device structure; and SCM (Scanning Capacitance Microscopy) is a way of seeing the positive and negative doping that makes up the actual working transistors, resistors etc., in the silicon chip.

Mastering Reverse Engineering

Reverse engineering know-how is a combination of historical expertise of devices and forward-thinking expertise on the latest technology. We need to be able to identify why certain design considerations were made, to quickly connect the dots on a complex circuit, to identify the foundry or facility used based on design and chemical composition, to take apart devices that are no longer visible in the optical range, and to have the wherewithal to solve the completely unknown.

Historically, device deconstruction was relatively easy to do and the main challenge was in mapping the large and complex circuits. Today, with ever shrinking feature sizes, and ever increasing complexity in device types and uses, sample preparation is becoming equally as challenging.

Some devices enter and exit the lab in a matter of hours, fully opened-up, delayered and ready for imaging. These days devices combine very thin layers, small circuit path lengths, multiple materials, innovative materials, and unusual functional models (most specifically in Micro-Electrical Mechanical Sensors). Sometimes it is necessary to destroy several devices to get the sample ready to be imaged. In the rare circumstance we have to prepare 20 or more samples to get the information that we need.

Chipworks is able to mitigate this risk and keep the cost down by leveraging our expertise so that when we see a device with unique problems we are able to apply historical processes to make the sample preparation easier.

The Challenges Keep Coming

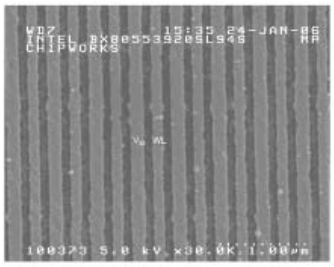
For reverse engineers, life will not get any easier in the electronics business. In semiconductors, the current challenges are the 65-nm node devices beginning to be delivered, and the 45-nm processes being ramped up in development fabs. The consumer electronics business keeps bouncing from killer-app to killer-app, and we have to stay on top of all the new gizmos that keep appearing.

The RE business has to keep evolving to keep up with the changes in electronics and design, and it has become a discipline in itself created by the needs of ever-developing technologies.

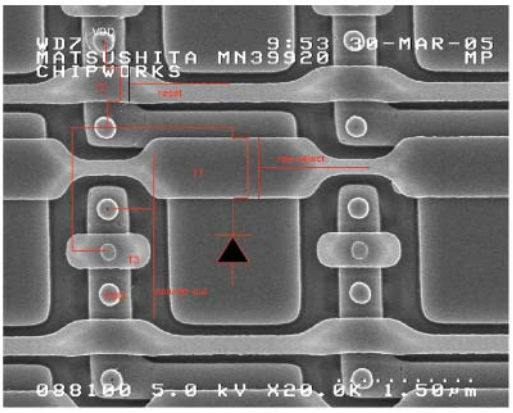
A challenge that manufacturers and designers will need to stay on top of. Chipworks, for example, has noticed that 65-nm devices have come to market much slower than past technology nodes. Evidence is showing that the same will be true of future nodes. This means that the leaders in the industry have probably overcome some difficult design and manufacturing considerations.

Increasing Complexity

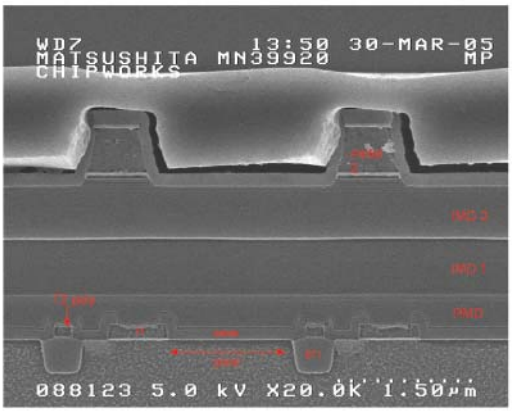
As the node shrinks the previously ignored becomes critical. A simple example is the need to see how your competition is coping with Line Edge Roughness to understand how they were able to design gates according to the limitations of their fabrication capability.



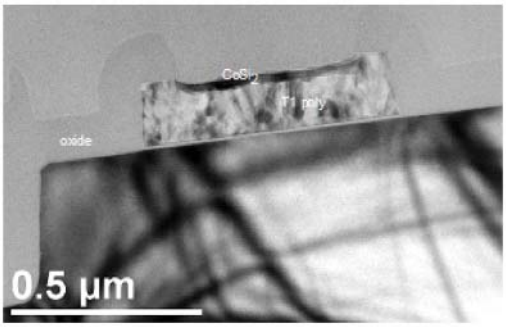
Metal 3 V_{ss} Power Buses and Word Lines



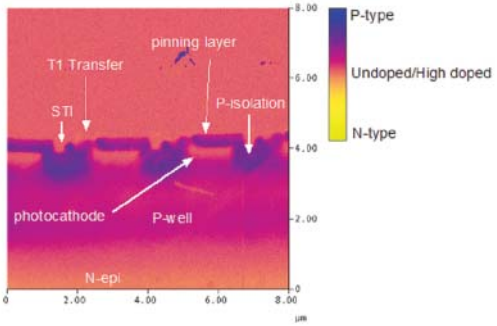
a) Plan-View SEM of Pixel



b) Cross-Sectional SEM



c) Cross-Sectional TEM of Pixel Transfer



d) Cross-Sectional SCM Image of Pixel

Figure 6. Analysis of Pixel structure in CMOS Image Sensor

Chipworks Technical Capabilities

Circuit Analysis

Chipworks advanced laboratory and analytical capabilities reveal the circuit layout at each lithographic layer of a semiconductor device. Full circuit extraction is possible, using Chipworks proprietary software tools. These capabilities allow Chipworks to analyze all types of microelectronic devices including digital/logic, embedded and stand alone memories, analog mixed signal, sensors/MEMs, wireless LAN, CMOS image sensors, DSP's, microprocessors, displays, and discretes. The results are provided in professionally published, well-organized, Circuit Analysis Reports (CAR) providing accurate, annotated schematics.

Transistor Characterization

Electrical transistor characterization is performed to complement a physical analysis of a semiconductor device. Chipworks' experienced lab staff and engineers use our in-house SEM based probe station to produce full DC transistor characterization down at the 65 nm node and beyond. The results are published in our Transistor Characterization Reports (TCR).

Process Analysis

Process analysis gives you detailed information on the fabrication methods used to manufacture a semiconductor device. Advanced analytical instrumentation and sample preparation techniques, combined with our experienced engineering analysts, allow Chipworks to fully reverse engineer the process used to fabricate a semiconductor device. Chipworks has analyzed numerous types of CMOS, bipolar, BiCMOS, GaAs, SiGe, SOI, MEMS and optical processes. The most sophisticated analytical techniques are used to identify the specific aspects of a chip's structure; including feature sizes, material composition, fabrication techniques, and doping levels in the silicon substrate. Chipworks publishes a wide range of process analysis reports, including our flagship Structural Analysis Reports (SAR) and our Process Review Reports (PRR, IPR).

Some Key Technologies Employed

TEM STEM XPS TEM EDS SEM-ICIS TOF SIMS FESEM EELS SCM FTIR SIMS AES Optical Microscope AFM SRP SEM EDS

Contact Chipworks

For any custom reverse engineering, to order some of our reports on the latest device, or to review our library of historical reports please contact Chipworks.

Chipworks
3695 Richmond Rd.
Suite 500
Ottawa, Ontario
K2H 5B7 Canada
T: 1.613.529.0414
F: 1.613.829.0515
www.chipworks.com
info@chipworks.com