



Maintaining your competitive edge

Pierrette Breton of Global Intellectual Strategies discusses reverse engineering and its impact on trade secrets

Picture: 3DProf / Shutterstock

Understanding your competitor and what they offer, at what quality and at what price, simply makes good business sense. A petrol station owner verifies his geographically closest competitor's prices and adjusts his prices accordingly. This type of knowledge is commonly referred to as competitive intelligence and is used by businesses to maintain a competitive edge.

So how does one gain competitive intelligence? It can be as simple as looking next door to see a price advertised and as complex as reverse engineering a product to understand what provides quality, and uniqueness to the product. For example, one may be interested in a new anti-wrinkle face cream formula, or a new mobile phone antenna design, or how to manufacture a multi-chip integrated circuit package. Each one of these examples requires a different analysis during the reverse engineering process.

So, what is reverse engineering and how is it different from usual product design or forward engineering? As a product is being designed or forward engineered, the product is conceptually planned then synthesised,

prototyped, and tested. At this stage, design flaws are identified and corrected. The design may be adjusted, re-synthesised and tested, and finally manufactured. Reverse engineering follows this path, but in reverse. It is the art of taking something apart to determine how it works or how it was made or manufactured. Figure 1 shows this process.

Acquire product and teardown into subparts

A product, a mobile phone for example, is acquired and taken apart in a process commonly referred to as a teardown¹. In some instances this can be a time consuming and painstaking task. Each step of the teardown process is recorded through meticulous imaging so as to preserve the information on how elements are assembled or interconnected. Many teardown examples can be found on the internet, with some popular examples from www.ifixit.com and www.isuppli.com.

However, a teardown will only get you so far. The feature or improvement that gives your competitor a competitive edge may be found within a sub-part of the product, making it important to further teardown that sub-part.

For an example, see figure 2 of a "teardown of an IC". The image shows the disassembly of a multi-chip package and reveals the microelectromechanical systems (MEMS) and integrated circuit (Logic ICs) within.

Analysis of the feature

The next step is to analyse the feature of interest using one or a combination of the following methodologies:

- Identification of materials used;
- Extraction of quantitative information of the materials used;
- Imaging of the product in various plane views, such as top, bottom, side and cross-sectional views;
- Extraction of the electrical circuit;
- Testing of electrical signals;
- Analysis of video or audio content; and
- Extraction of software functions.

Figure 2: The disassembly of a multi-chip package revealing the microelectromechanical systems and integrated circuit within

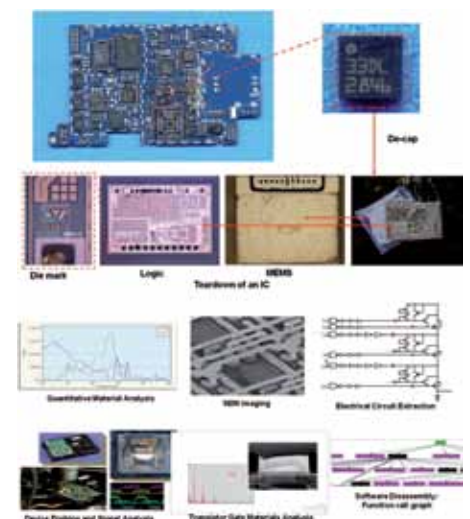
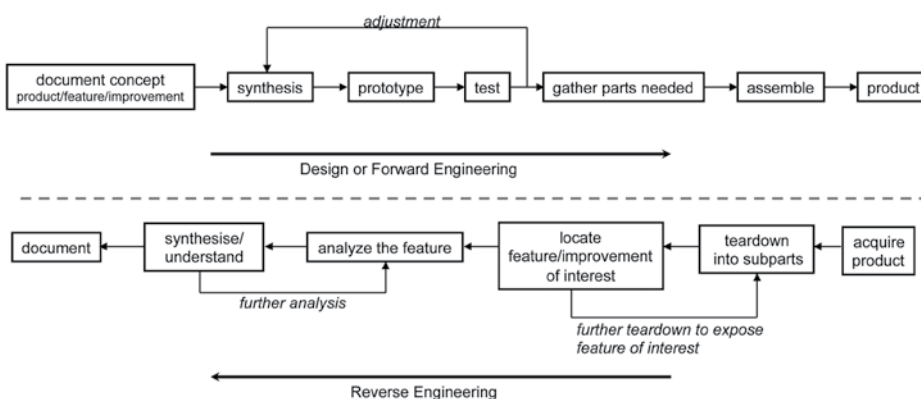


Figure 1: The product engineering process



Synthesise/understand/ document

Once the analysis process is completed, the results are reviewed by an expert knowledgeable in the technology. Conclusions are reached and the feature is documented. The goal may be to:

- Identify the materials used and their relative concentrations;
- Identify the recipe;
- Identify the manufacturing steps;
- Provide a bill of materials and material costs;
- Understand the electrical circuit timing and operation;
- Understand compliance to a standard;
- Understand the software functions and timing of the functions.

Trade secrets

While gathering competitive intelligence, a competitor will come to know what you may prefer to keep as a trade secret. Therefore, is information obtained through reverse engineering theft of trade secrets?

The Economic Espionage Act of 1996 ("EEA") criminalised the theft or misappropriation of trade secrets, but clearly states that companies and individuals have the right to discover the information underlying a trade secret through their own research and hard work. It further states that a person may legally discover the information underlying a trade secret by reverse engineering². (See EAA 18 USC §1831-1839 sections IVC 1 and 2.) Further, in *ConFold Pac Inc v Polaris Indus* 433 F 3d 952, 959 (US Court of Appeals for the Seventh Circuit 2006) the court concluded that, "It is perfectly lawful to 'steal' a firm's trade secret by reverse engineering." (Circuit Judge Posner)³.

So, how does reverse engineering impact your trade secrets? If you can manufacture it, it can be reverse engineered – at least in theory. For example, according to Intel, "making microprocessors is a complex, demanding process involving more than 300 steps"⁴. To identify the 300 manufacturing steps required to fabricate such a microprocessor will require understanding the number of layers used, likely hundreds, the composition and quantification of the materials for each layer and the thickness of each layer. Some of the manufacturing steps will be deduced, as a necessary step to achieve a result, but cannot be substantiated as any material at that step has been removed or consumed during the manufacturing process. It will be impossible to provide, with any precision, temperatures at which process steps are completed and even

the most knowledgeable expert will arrive at a manufacturing process that only resembles the actual process used.

However, if your trade secret is in the material used in the fabrication of the gate of a transistor⁵, the information is more easily obtained at a reasonable cost and may be obtained within a week. There are a number of labs throughout the world which are capable of such an analysis.

"What one must consider is that it may not be advantageous to invest heavily in a reverse engineering effort – as it can take time and be costly."

Can you protect your trade secrets in light of the abundance of reverse engineering services? What one must consider is that it may not be advantageous to invest heavily in a reverse engineering effort – as it can take time and be costly. Examples of reverse engineering projects range in price from US\$1,000 to over US\$1,000,000 and can take one week to one year after a product is acquired. In many cases your competitor is better off investing in intense R&D, recognising that by the time the answer is obtained you have moved on to other improvements and continue to have the leading edge.

How best to protect your trade secrets from reverse engineering?

Find out the cost and time to reverse engineer the feature you want to protect. Weigh the time and financial investment that your competitor must make with your company's goals and directions. If you deem that you are at risk you may want to consider anti-tamper solutions for both your software and hardware. Anti-tamper solutions include enclosures that sense tampering and "zero out" critical data automatically. Also available are tamper-resistant coatings that cause permanent silicon damage during a physical tamper in an integrated circuit⁶.

Gathering competitive intelligence is an important part of doing business and reverse engineering is one of the tools used for this purpose. Your trade secrets can be at risk depending on the investment required to uncover your trade secrets. Such risks can be

mitigated by devising a patenting strategy that minimises your dependence on trade secrets. More specifically, as an alternative to protecting your knowledge or intellectual property through trade secrets which can usually be uncovered, patenting provides you with another form of protection for your intellectual property.

Footnotes

1. The product is disassembled, photographed and the components are inventoried.
2. United States Department of Justice Computer Crime & Intellectual Property Section, Theft of Commercial Trade Secrets – 18 USC § 1831-1839 <http://www.cybercrime.gov/ipmanual/04ipma.html>
3. United States Department of Justice Computer Crime & Intellectual Property Section, Theft of Commercial Trade Secrets – 18 USC § 1831-1839 <http://www.cybercrime.gov/ipmanual/04ipma.html> . Reverse Engineering is legal if the product is legitimately obtained.
4. <http://www.intel.com/pressroom/kits/chipmaking/background/background.htm>
5. See "transistor gate materials analysis" in figure 2. This image shows a transistor in cross-sectional view and identifies titanium and silicon as materials used in the manufacture.
6. <http://www.altera.com/literature/wvp/wvp-01066-anti-tamper-capabilities-fpga.pdf> and http://www.gore.com/en_xx/products/electronic/anti-tamper/anti-tamper-respondent.html.

Author



Pierrette Breton has over 21 years experience as an intellectual property expert, specialising in semiconductor reverse engineering. In 2000, Ms Breton founded Global Intellectual Strategies. She has been deposed on numerous occasions in support of patent litigations and has testified at trial as an expert witness within the semiconductor discipline. Pierrette Breton is a registered patent agent.