



Intellectual property (IP) comes in many shapes and forms – patented inventions, copyrighted material, trademarks to reinforce brand identity, proprietary designs that determine product appearance, trade secrets or company specific ‘know how’.

The term can refer specifically to internally developed design blocks or cores licensed from an IP vendor to form part of a system on chip (SoC) design. Under the umbrella of intellectual assets, IP might represent one part of a combination of tools and prior knowledge necessary to engineer a new product.

Shorter time to market requirements and the huge number of transistors available nowadays ensure that no matter what the design environment – system or SoC – a level of design reuse is likely to be taking place. Any successful reuse based model relies upon cooperation and trust between engineers, as knowledge of intimate design

IP is a valuable asset in today's knowledge economy.

So how can you protect it?

By **Vanessa Knivett**.

details such as the RTL HDL source code has to be shared. Meanwhile, with design, test and manufacturing environments now seldom centralised, IP needs to be shared across borders, making it difficult for those charged with protecting it to monitor where it is and who has access to it.

Whatever the form of IP at your disposal, the ability to quantify, qualify and protect it makes good sense. Just as an externally sourced design has a price tag, so internally developed IP needs a value and the appropriate security.

Notes Christian Heidarson, Gartner's lead analyst for IP: “For a company that operates in emerging markets, the most significant threat to its intellectual capital is that of IP diffusion, not IP misuse. IP diffusion happens when key employees leave for another company, taking with them valuable knowledge and customer relationships. This can be entirely legal, as long as the employees don't bring

# Mine, all mine!





with them any proprietary designs.” Ensuring the appropriate non compete and non disclosure agreements in employment contracts is a start.

Precious IP is likely to be supplied in a more usable form to a contract manufacturer. The migration of contract manufacturing to lower cost economies may have fiscal advantages, but an unproven supply chain can expose IP to misuse. Confirms Heidarson: “Using design and manufacturing services exposes a company’s IP to third parties that are often based in countries with weaker legal systems than US and European companies will be used to.”

Though there are many reputable contract manufacturers in lower cost regions, IP theft there is believed to be rife. Notes Heidarson, who is based in China: “The

market. Heidarson advises: “The most powerful and most common strategy for protecting IP is only dealing with companies that you trust. This is because technological solutions for protecting IP make the IP less flexible in the design process and can be overcome by a party determined to do so.”

For IP theft is just as likely beyond the manufacturing stage, through cloning, whereby a competitor copies a product, or through reverse engineering to steal the actual design. The latter is more common with analogue technologies, which tend to make use of more mature processes. The problem with this type of IP misuse is that it serves to devalue the original technology, as none of the subsequent products will reflect the cost of the engineering effort that went into the original.

### Anti theft strategies

Popular strategies to deter IP thieves include making products difficult to copy using techniques such as encryption, compartmentalising production so different parts of a product are made by different companies, and ensuring that key technologies are kept in countries with robust legal systems.

Most recently developed IP theft deterrents are being implemented within the SoC community. Many of these techniques are based on rendering certain design elements as unique and thus easier to detect when they are misused, for example through tagging and tracking mechanisms, the use of digital signatures or digital fingerprinting, digital watermarking or noise fingerprinting. The reality is that, for IP core vendors, it’s customers who can perpetrate IP misuse by using cores incorrectly.

Ironically, for companies keen to detect where their silicon IP is being used, it may mean adopting the skills of the IP pirate. Dr Tom Kean, managing director of Algotronix, explains why tracking silicon IP is so difficult. “If it is in a custom chip, the only practical technique is to etch open the package and look for it using a microscope. Even this technique is difficult for soft IP, which is processed by synthesis or automatic place and route tools. If the IP

is on an fpga, then it is theoretically possible to use watermarking on the bitstream to detect IP. However, this technique is defeated if the person misusing the IP encrypts the bitstream.”

Algotronix is one company developing solutions to simplify IP tagging and detection, having developed a circuit technique for tagging complete fpga or ic designs or IP cores. The tags have been designed to be small and low power, so that multiple tags can be realistically be on a single chip, with a sensor placed on the package to detect the tags. The technology will be launched at the forthcoming Design Automation Conference in June.

### Open sesame?

With so much IP changing hands, it may not always be practical to defend every IP transgression – indeed, it may be advantageous to be more open with IP.

Recounts Bill Seymour, head of Nokia’s Intellectual Rights department: “In certain cases, you want to create a bigger market – you will want to make sure that everybody has access to the technology.” In this case, essential IP is submitted to a standards committee and the developer agrees to abide by fair, reasonable and non discriminatory pricing when licensing the technology to other parties – including direct competitors.

Licensing revenues are just one way of obtaining value from IP, as a developer taking this route may also be able to negotiate cross licensing deals that provide access to other essential patents. The Open Source model is of course the ultimate extension of a freer approach to IPR, whereby a company forsakes its licensing rights in return for community R&D.

Inevitably, IP protection requires a multipronged approach. However, a balanced IPR strategy and open collaboration are now viewed as complimentary. Talking at a recent event about Nokia’s ambition to be ‘the best internet platform’, Seymour affirmed that, whilst it would still protect its technologies: “Open collaboration and open standards ... continue to be something that you hear from us. It was the key to success in gsm; it is the key to success in internet.”



“IP diffusion happens when key employees (take) with them valuable knowledge and customer relationships.”

Christian Heidarson, **Gartner**

legal framework is solid and modelled on British IP law. Enforcement is the problem, as courts still lack experience and the responsibilities of officials remain murky.”

One source of IP theft is overbuilding, where an unmonitored manufacturer builds more product than ordered and then sells them on the local black