Protecting Virtual Components:
Balancing Buyers and Sellers Needs

by

Marc Greenberg
Manager, IP Procurement
Motorola Semiconductor Products Sector
Architecture and Systems Platforms
System-on-a-Chip Design Technology

When a design team produces a Virtual Component (VC), also called Intellectual Property (IP), for external sale, their goal is to produce the easiest to use block in the least possible time. Doing so reduces the time-to-market, the end product design cycle time, and the support time. Companies selling VC blocks can derive revenue from the fact that these blocks can be and are well protected from theft or misappropriation. The buyer wants to know that purchasing the IP block will actually decrease (and not increase) design cycle time based on the ease of use. When the buyer purchases a block, that buyer is purchasing a competitive advantage from improved performance (expanded feature set), reduced costs, and/or faster design cycle time.

Lawyers define a VC (or intellectual property) as a creative design technique from which the creator gains value by preventing others from using it. Faced with an environment that increasingly stresses extensive VC reuse as a daily reality for both VC creators and system integrators, a new, more functional definition of a VC would be as follows: A VC is a design which performs a specific function from which we gain value by enabling others to use it.

In the past, operating under the old definition, any producer of a microprocessor guarded it zealously. Under today's changing marketplace most microprocessor companies derive a substantial portion exclusively from licensing their microprocessor. Some companies in the industry today actually derive all of their income from licensing. This article will discuss how best to meet the needs of both buyer and seller while still maintaining adequate protection for the VC.

Legal Protection

Today, a VC is effectively a piece of software with a range of value from nominal to phenomenal. Non-authorized distribution of a VC block such as on a CD or published on the Internet could cause substantial harm to the creator/seller. A huge black market already exists in consumer and business software. Piracy of a valuable VC block could cause the value of a company who holds the rights to that block to plummet.

In one all too easy to imagine scenario, a prospective customer obtains an evaluation copy of the VC block, integrates it into their design, but doesn't pay the licensor. If the block was a hard VC, you could simply look at the device, since by definition, a hard VC

includes a pre-defined layout. Detecting unauthorized use of firm or soft VC is more difficult since, by definition, the layout is performed by the licensee.

Legal protection for the VC consists of copyrights, trade secrets, and/or patents. Once these protections are in place, companies must effectively manage and protect their VC blocks by using non-disclosure agreements, carefully controlling access to the design data, license agreements, and litigation.

Technical Protection

Technical protection is the means by which a seller might prevent or detect unauthorized use of the VC, obfuscation, encryption, digital watermarking, automatic netlist generation and black box techniques, shipping VC as hard macros (where RTL would be functionally more useful for the buyer), and forensic technology investigators. Using obfuscation, the seller removes all notes in the design and replaces all meaningful signal names. This approach seeks to largely disable the design to prevent unauthorized use. It is unlikely that even if an obfuscated block were stolen, that it could be used.

Encryption is a similar, but technically more advanced protection method. Verilog, the principal industry design language, offers encryption algorithms that can only be decrypted by specific Verilog decryption algorithms. Digital watermarking in a VC introduces a certain performance characteristic into the design. This watermark is transparent to the licensee, but provides a ready means to identify the design in the event of unauthorized use.

Hardening techniques including automatic netlist generation, black box techniques, and shipping as hard macros are all means to avoid shipping RTL code, which would be functionally more desirable to the buyer. If a licensor suspects unauthorized use of a VC block, that seller can turn to a forensic technology investigator to identify code to identify the suspected application. Despite any or all of these methods, no amount of protection can prevent a very determined attack on the VC or an employee theft.

Advantages and Disadvantages to Buyer

A major risk for the buyer involves the issue of protection. Whenever the seller is using any technical protection, it puts the buyer in the hands of the vendor for support. In the event that the vendor goes out of business or a buyer's competitor purchases the vendor, the buyer faces a major risk. When technical protection is used, the buyer is totally at the mercy of whoever has the source code.

A hardened VC block can receive patent protection only when the design has been executed in silicon. In the event that the buyer is purchasing use rights under a patent, it means that only licensed users can implement the design and the rights holder (seller) has to defend its value in the event of unauthorized use. The only other advantage to the buyer is that the circuit design is fixed. The buyer will receive support and will be spared the agonies of inexpert modification by buyer's designers.

Advantages, Disadvantages, and Best Approach

The bottom line for the seller of a valuable VC block is that the seller must protect both the revenue stream and the investment in the development of that block. On the downside, the seller must incur increased cost and workload to implement technical protection. If on the other hand, the seller attempts to increase or strengthen legal protections, the result can be protracted negotiations with customers. Protracted negotiations achieve no benefit to either buyer or seller. The more difficult the seller makes the negotiation, the slower the seller realizes the revenue and conversely, the buyer loses potential design cycle benefits, as well.

For the buyer, a protection technology would be acceptable if it does not impede the use or performance of the VC. However, the buyer's risk is increased when the buyer does not have all of the design data available. In the case of a hard-macro, black-box or an encrypted model, the buyer is dependent on the seller to provide a bug-free product. The buyer is also dependent on the seller to support the VC block for as long as the buyer designs the end product and any derivative technologies. If the block is encrypted or black-box, then the buyer needs some established method of extracting the source data in case of emergency. This could be a code or key escrow arrangement, which adds to the complexity of the IP transaction.

One benefit of some forms of technical protection is that the user can't change the internals of the VC block, which in most cases is an advantage. It's a disadvantage when there is something genuinely wrong with the block and the user is unable diagnose or fix it.

The ideal solution is for sellers to confidently embrace their existing copyright, patent, and trade secret rights and be willing to share source code with trusted licensees. The point for sellers is to protect what can legally be protected without creating a problem or distraction from the ongoing flow of business.

* * * END * * *

(Word Count: 1,226)