VSI Alliance™
White Paper

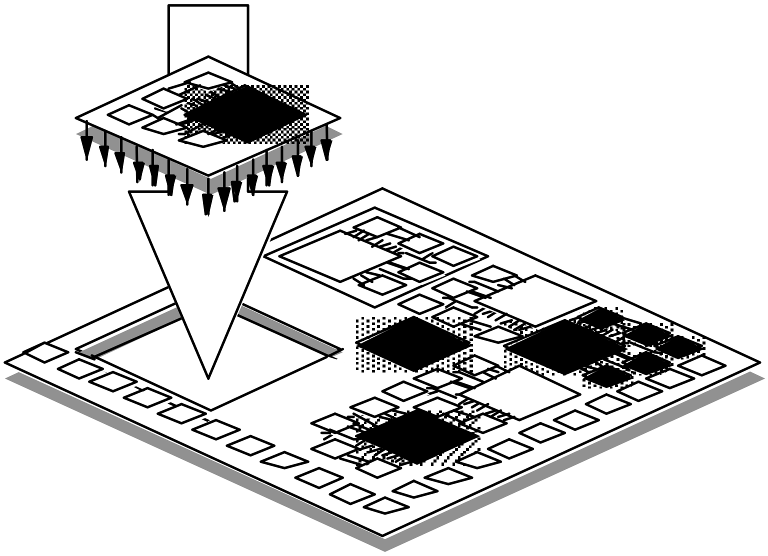
Intellectual Property Protection: Schemes, Alternatives and Discussion

Version 1.1
(IPPWP1 1.1)

Issued by the
Intellectual Property Protection
Development Working Group

Released August, 2000

Revision 08Jan01



NOT LEGAL ADVICE
The discussions of the law in this document are not intended to be legal advice. This document is not to be used as a legal reference. Readers should refer to their own legal counsel for answers to questions concerning the law.

Copyright Notice

Please send comments/questions to:

IP Protection Development Working Group (DWG), VSIA

Ian R. Mackintosh
Chair
3054 Three Springs Road, San Jose, CA 95140
408-406-3152, i.mackintosh@att.net

Raymond Burkley
Vice-Chair
Burkley Associates, P. O. Box 496, Cupertino, CA 95015
408-735-1540, rburkley@netgate.net

VSI Alliance
115495 Los Gatos Blvd, Suite 3, Los Gatos, CA 95032
408-356-8800, info

Intellectual Property Protection Development Working Group

Members of the Development Working Group:

ARM
ECSI
Mentor Graphics
Oki Electric Industry
Philips Semiconductor
VCX
Cadence Design Systems
Fujitsu
Netlogic Microsystems
Palmchip
UMC
Xilinx

Individual Members:

Patrick Beauvillard
Miodrag Potkonjak
Raymond Burkley (Vice-Chair)
Ken Hodor

Active Contributors

Simon Watt	ARM
Richard Terrill	Cadence Design Systems
Mark Bales	Cadence Design Systems
Adam Morawiec	ECSI
Minesh Shah	Fujitsu Ltd.
Takeshi Fuse	Fujitsu Ltd.
Ken Hodor	Individual Member
Ian Mackintosh (Chairman)	Mentor Graphics
Tom Wong	Metis Associates
Al Kwok	NetLogic Microsystems
Tadashi Hiruta	Oki Electric Industry
Jauher Zaidi	PalmChip
Robin Bhagat	PalmChip
Miodrag Potkonjak	Individual Member
Patrick Beauvillard	Individual Member
Raymond Burkley (Vice-Chair)	Individual Member
Benson Lee	UMC
James Burnham	Xilinx
Larry Rosenberg	VSIA-TC Chair

Technical Editor/Author:

Ian Mackintosh

Revision History

Revision 0.1- Yatin Trivedi created initial version 4/30/98.
Revision 0.1.1- Ken Hodor, Mark Bales and Yatin Trivedi made additions 5/2/98
Revision 0.2- Contribution by Ken Hodor, Tom VandenBerge, Raymond Burkley, Minesh Shah, 5/21/98
Revision 0.3- Re-write and additions by Ian Mackintosh 10/31/99 (see Acknowledgements)
Revision 0.4- Ian Mackintosh made edits per DWG recommendations, 01/12/00
Version 0.4 – Editorial Staff formatted cover/headers/footers/updated DWG Membership Page –15Feb00
Version 0.4 – Editorial Staff copy edited and added disclaimer to cover–24Feb00
Version 1.0 – Editorial Staff formatted for Board Review –5Jul00
Version 1.0 – Editorial Staff formatted for Final Release, updated Mackintosh contact info, added legal notice page –28Aug00
Version 1.1 – Editorial Staff corrected formats in footnotes, headers, title page, revision history, table of contents and contributors page – 08Jan00

Acknowledgements

Grateful thanks are provided to the numerous current and past IP Protection DWG members who contributed such diligence and thought in making the publication of this White Paper possible, especially Tom VandenBerge and Ken Hodor. A special acknowledgment is afforded to Raymond Burkley.

Table of Contents

VSIA IP PROTECTION DWG

By late 1999, VSI Alliance^{TM} (VSIA) had established eight Development Working Groups (DWG's) each strongly supporting the VSIA vision:

"To dramatically accelerate system chip development by specifying open standards that facilitate the mix and match of virtual components (VCs) from multiple sources."

The Intellectual Property Protection (IPP) DWG was created in 1997 to address the issue of protection of virtual components (VCs). The goals of this DWG were to:

- Enable IP Providers to protect their VCs against unauthorized use
- Protect all types of Design Data used to produce and deliver VCs
- Detect use of VCs
- Trace use of VCs

SCOPE

Various solutions exist for protection of virtual components (VCs), but not all are equally applicable to each type of VC. Trade-offs exist between the value (perceived or real) of the VC, difficulty of implementation of the protection scheme, and the resulting usability of the protected VC by both the integrator and the end user. This paper briefly discusses and introduces known technologies and mechanisms that support the broad spectrum of VC types, sources of VCs, and business requirements for VC users and providers.

The scope of this paper is to identify open, interoperable, standards-based solutions (or guidelines and information where standards are not practical) for VC protection which balance the level of security with customer usability of VCs, while fostering design reuse from creation through to the effective use of VCs. In this context, "VC" includes products, technology and software that may be protected through patents, copyrights or trade secrets. The trade-offs discussed can be used in selecting appropriate protection mechanisms for hard, firm and soft VCs.

The broad target audience for this paper includes VC providers, VC users (system designers or integrators), EDA vendors, and semiconductor vendors who utilize virtual components in standard product FPGA, CPLD, ASIC, or SoC market segments. Various protection, detection, and tracking mechanisms that can be employed with VCs and that are licensable to another party are discussed. This paper is concerned with protection of VCs and not with protection of design programs (EDA tools) used in processing them through a design flow.

INTRODUCTION

The general infringement of all types of intellectual property (IP) in the United States has become a major problem. At the 1998 annual RSA Conference, it was estimated that the cost of IP infringement approaches $1 billion per day. This problem has received so much attention that the FBI launched Operation Counter Copy to address it. Today, the FBI estimates that 80 percent of all infringements of electronic designs can be traced to sources from within the company that developed the IP. The other 20 percent occur at external points of vulnerability, caused by the ease with which end-products can be reverse engineered, copied or simply stolen.

In the area of electronic design, there are an estimated 100 reverse engineering shops in the US; approximately 70 percent of these are funded by government(s), and many of the techniques developed are leaked, or even published, to the industry. The American Society for Industrial Secrets estimates that in the US alone, trade secret theft is in excess of $2 billion per month.

Although the protection of VCs is rapidly becoming a major concern within the VC and Electronics Industry as a whole, the overall awareness of the issue remains low. As the electronics industry shifts to a design-for-reuse methodology, virtual component trading is expanding, and the potential for infringement (intentional or unintentional) is growing in proportion. Unfortunately, awareness of the liabilities may only be achieved in the aftermath of a highly visible, industry scare.

How, then, can virtual components be protected? Unfortunately, potential infringers have the upper hand today, with so few IP protection programs in place. In truth, it is almost impossible to guarantee protection of a VC in all of its uses, data forms, and exposures during use. However, it is realistic to define and apply adequate mechanisms and precautions such that the costs for infringers exceeds the value of success and the cost of the protection afforded to VC owners is consistent with the risk and value of loss.

An early example of an IP Protection scheme was to have EDA tools create and operate on an encrypted form of the source code of a virtual component. However, encryption supported by EDA tools has inherent flaws (see the section on Protection Mechanisms):

- EDA tool vendors do not license encryption algorithms to others.
- The author of the VC must trust and rely upon the EDA vendor’s security, since the EDA vendor retains decryption capability.
- All EDA tools have back-door access to the encrypted data in order to determine if problems encountered are due to a bug in the tool or the VC.

It is essential that practical solutions support both customer use and supplier distribution models in the form of recommended guidelines, practices, standards and implementation plans.

OVERVIEW: Security Schemes

There are three approaches to the problem of securing a VC. Using the *deterrent* approach, the VC owner may deter the infringer from contemplating the theft of the VC by using proper legal means. With the *protection* approach, the owner tries to prevent unauthorized use of the VC. And, using the *detection* approach, the owner detects and traces both legal and illegal use of the VC, so that a proper course of action can be taken.

Deterrents provide external communication of legal protection in an attempt to deter an illegal act from occurring. They do not provide any physical protection. Types of deterrents available include:

- Patents
- Copyrights
- Trade Secrets
- Contracts and Lawsuits

Protection involves taking active steps to try to prevent the unauthorized uses of VC's from occurring. Protection mechanisms include such tangibles as:

- Licensing Agreements
- Encryption

Detection involves the ability to determine that an unauthorized use has occurred and then, tracing the source of the theft. Detection and traceability methods that are becoming available include:

- Foundry IP Tracking or Tagging (see VSIA's, Virtual Component Identification: Physical Tagging Standard)
- Digital Signatures, such as, Digital Fingerprinting and Digital Watermarking
- Noise Fingerprinting

Ideally, a trace would be created every time a VC is used in any form during design, implementation or fabrication. Information would be logged and carried along with other data including tool use, user identification, time, date, etc. For designers (users of VC's), assembly of multiple VCs requires that auditing be made hierarchical. Such an ideal system would uncover theft and provide notification back to the VC Provider.

Security Schemes appropriate for a VC are determined by the specific application point of the VC during its life-cycle. A VC evolves through phases of development, licensing, use, and sales of an end product; and, discovery of an infringed property can occur anywhere in that evolution process. At specific points of this life-cycle, different security schemes will need to be implemented. An example of these schemes and the life-cycle phase of a VC is shown below.

Example Security Schemes Applicable During VC Life-Cycle

	Development	**Licensing**	**VC Integration**	**Manufacture**	**End Component Use**	**End Application**	**Infringement Discovery**
DETERRENTS							
Patents	X		X				
Copyrights	X		X				
Trade Secrets	X		X				
Contracts		X					
Lawsuits							X
PROTECTION							
Licensing Agreement		X			X	X	
Encryption	X						
DETECTION							
Tracking				X			X
Tagging	X		X				X
Digital Fingerprinting	X		X				X
Digital Watermarking	X		X				X
Noise Fingerprinting	X		X				X

DETERRENTS

Traditional deterrent protection mechanisms are patents, copyrights, trademarks and trade secrets. The primary goal of patents and copyrights is to encourage commercialization and give exclusive rights to the originator for a specific period of time. These methods provide varying degrees of protection, especially in the international community.

A developer needs to understand the regulations and principles behind the methods of providing protection to VC designs, both for the protection of the developers own designs and for the protection of other developer's virtual components. A detailed search and analysis of patents, copyrights and trademarks should be conducted prior to initiating any VC developments, to establish any potential infringements of other intellectual property rights, and to aid in determining the worth of the developer's proposed VC design.

Patents

It is important to note that patents are only recognized in the specific country where the patent was filed. Typically, a US patent costs $10K-$30K (including prosecution and lifetime maintenance fees) and is applicable (active) for up to 20 years. An international patent costs approximately $50K-$100K (including prosecution, translations and annual annuities over the life of the patent) with varying duration of protection.

A patent also requires extensive documentation. The author must prove novelty and utility and give complete directions for implementing the invention. Once a patent is issued, it is fully disclosed to the public. If an international application for patent protection in other countries under their laws is not submitted, these patents will be protected only in the country of application.

Copyrights

Copyrights were originally designed to protect literature, music and dramatic works. They only prohibit copying expressions of an idea, not the idea itself (as a patent does). Therefore, it is easier to get a copyright than a patent. Copyrights have a much longer period of protection (50 years beyond the life of the author), and they are recognized internationally. However, international laws make them difficult to enforce. With respect to semiconductor designs, copyrights have only limited use. They are generally applied only to the die or masks to prevent exact copies.

Trade Secrets

A trade secret law has a broader scope of coverage than patents and copyrights. However, the author must take deliberate steps to protect and secure the information in order to be covered by trade secret laws. The author must also derive economic benefit from the secret information. Typically, trade secrets are created and owned by companies, rather than individuals. Trade secrets are kept by the originator to maintain exclusive rights. A prime example is the recipe for Coca-Cola. It is not only a trade secret, but no one person knows the whole recipe.

To receive protection under trade secret laws, a company must restrict access to information being held as a trade secret. If the information must leave the premises, intent must be shown to protect and control the data. In regard to contracts with other companies, trade secrets must be described in detail, the rights being granted must be well-defined, and the information must be declared to be held as a trade secret. Access to trade secret information must be carefully and consistently documented. As noted previously, the major hole in security is from within companies. So, it is imperative that the employees sign employment contracts stipulating the company policy on trade secrets. If the information becomes public, trade secret law cannot be used as protection.

Governing Law

It is also very important to understand the nature and scope of the jurisdiction that provides the various types of protection, since laws are made and adjudicated by different government organizations. The following chart is used to illustrate the diversity between governing bodies and is not to be interpreted as a comprehensive summary of the worldwide laws that govern the protection of Intellectual Property.

GOVERNMENT	COPYRIGHT	TRADEMARK	PATENT	TRADE SECRET
US-Federal	Yes/50-100 Years	Yes/Permanent	Yes/17-20 Years	No-Guidelines
US-State	No	Yes (Varies)	No	No-Guidelines
Foreign	Yes/No	Yes/Some	Yes/Some	No

It should be noted that Intellectual Property rights in all cases except those involving trade secrets are affirmative rights, which means that the burden is upon the owner to initiate action against the infringer in cases of alleged infringement of a patent, copyright or trademark. On the other hand, trade secrets are often treated in the same manner as tangible property rights, which means that the authorities may take action against the accused party under criminal law, if the owner reports a theft or loss. The burden of pursuing affirmative rights rests with the owner of the Intellectual Property.

PROTECTION MECHANISMS

For highly proprietary VCs of great value, loss of control of EDA design data could result in large financial losses. So, it is important to protect these VCs with a high degree of security, such as that provided by encryption. At the same time, it is prudent to provide customers with a means of evaluating potential VC purchases, prior to the actual purchase.

Encryption

Encryption provides a means of giving potential customers access to an executable version of a VC without specific access to the source code. This mechanism allows recipients to try the VC, integrate it, and process through the various EDA tools in the flow towards silicon manufacturing without specifically disclosing the structure of the VC to the customer.

The problem is that not all EDA tool vendors provide tools supporting encryption; encryption is often proprietary, and there exists built-in "back-doors" to EDA tools that could permit a user to gain access to the unencrypted source code. As more EDA vendors establish their VC protection philosophy and strategy, the power of encryption could become more available and viable in supporting VCs, despite problems of customer willingness to pay for such capabilities.

Not all encryption schemes are optimal and any scheme employed should pass minimum tests of usability. For example, the public domain Pretty Good Protection (PGP) encryption scheme has been considered as a low-cost, open method to protect the distribution and exchange of VCs. However, there is currently insufficient infrastructure and control over the use of keys, which diminishes the value and potential in this application.

Hardware Protection

A powerful means of directly protecting EDA design data of a VC is simply not to release the design data, except in more indirect forms:

a) in the form of GDS II tapes (under foundry control) to make masks for the complete chip, or
b) in the form of a programmable device such as an FPGA (see section on Silicon Security), for use in a hardware or emulation platform.

Neither of these forms permits access to complete design views, and both of these methods increase the level of difficulty in gaining access to source information defining the VC.

Chemical Protection

Passivation technology was developed to protect the actual silicon die from the reverse engineering process. Much of this work was carried out by the military and involves the creation of inert passivation applied to the silicon as part of the normal manufacturing process. The passivation acts in its usual, protective fashion unless its surface is scratched and exposed to the atmosphere. When this happens, the passivation becomes reactive and damages the exposed silicon, preventing reverse engineering.

DETECTION SCHEMES

Various mechanisms exist to allow the identification of ownership of a VC. These schemes afford differing levels of security; some are deeply and undetectably buried in a design and others are openly displayed, easy to observe, and used as a simple means of tracing a VC. The most well-known schemes are described below.

Tagging and Tracking

Tagging and tracking are simply attaching tags or labels to VCs for tracing these elements (generally in the manufacturing phase) and enabling honest people to keep appropriate records and conduct their business efficiently and safely.

An example of such a scheme is the VSIA's, IPP DWG sponsored "Virtual Component Identification: Physical Tagging Standard", available to both VSIA members and non-members. This technique simply creates a GDSII label for any VCs grouped on an IC design. This label (or "tag") contains information on title, ownership, origination date, number of occurrences, etc. and permits an entity, such as a silicon foundry, to record uses, recognize ownership and administrate events and royalty payments.

Alternative tagging technologies are emerging, such as that from SIIDTECH (Portland, Oregon), which permits the unique and repeatable creation of digital ID's for individual silicon die. This patented technology offers a drop-in GDSII cell for the silicon die that features single pad readout of a non-volatile signature ID. It is technology for the physical silicon level of abstraction, equally useful to both foundries wishing to record unique identifiers for individual wafers, or to markets demanding individual identification and tracking of silicon die.

It is likely that in the future, infrastructure will emerge whereby an independent body will carry records of IP ownership, labeling, tagging and even digital signatures. Such an enterprise would be similar to that already existing in the music industry, where royalties for the use of music are collected and distributed to both users and owners of that music, who are due royalties.

Digital Signatures

A VC has a digital signature or fingerprint, which is a characteristic of the VC that acts as a virtually unique and exclusive identifier. More accurately, a digital signature is a finite, possibly hierarchical sequence of symbols drawn from a finite alphabet.

The fingerprint is generally the indigenous characteristic of a VC, whereas a signature can be the representation of that fingerprint, whether it is indigenous, or artificially inserted in the VC for purposes of identification or tracking.

Digital Fingerprinting

Digital fingerprinting is sometimes called passive watermarking. Here the recording and extraction of the unique digital signature utilizes inherent, pre-existing characteristics or attributes of a VC. The signature is a representation of the unique features and overall structure of the VC. Essentially, the mechanism is like a lossy compression scheme, where a complex and possibly hierarchical VC is characterized into a single digital signature.

The benefits of the scheme include avoidance of tampering with or changing of the VC, the use of standard design flows, and speed of implementation without performance hits. Fingerprints do NOT lend themselves to reverse engineering of the VC and are very suitable to be collected in databases (a la FBI fingerprinting). Such unique identifiers could find application as keys in encryption schemes.

Limitations include the fact that a fingerprint does not carry with it such useful information as the owner, VC name, etc. and so has some weakness relative to a simple tagging mechanism. A simple revision of a VC establishes a new fingerprint.

It is possible to record the digital fingerprint of a VC at most levels of abstraction in the design hierarchy. The VSIA IPP DWG plans to publish further work on digital fingerprinting during the year 2000.

Digital Watermarking

Digital watermarking is an indirect protection scheme in that it provides a deterrent to infringers by offering the ability to demonstrate ownership of a VC to its originator. The process of active watermarking consists of the implantation of a digital signature into a VC at a particular level of design abstraction, while utilizing the intrinsic features and structure of that level.

Watermarking is a hot area for research both within industrial and academic circles. Promising recent work suggests that efficient tools and methods are emerging to make the cost of both implementation and detection of watermarks economically feasible in the not-too-distant future.

Hierarchical watermarking is a scheme that targets more than one abstraction level for the same VC. Watermarks have been demonstrated at the highest level of algorithmic abstraction and propagated down to the physical level. An example might be the encoding of a digital pattern of "1's" and "0's" in the pass band of a complex filter, that can be observed (for example) in the frequency spectrum of that filter in the physical domain. A further example would be the encoding of an extractable pattern in a piece of logic that utilizes unused state transitions to implement the watermark; undetectable to all but those most intimately familiar with the VC.

The key challenges in this area are to develop tools and methods that are extremely difficult to defeat, have low cost/performance penalties, do not impede the native operation of the system, and are intuitively acceptable as proof of ownership in a court of law.

Additionally useful characteristics of watermarks include their holographic nature. It is possible to employ a watermark (a digital signature) broadly across a whole design, within single or multiple VC's, or even inside small functional areas. This practice means that small or even large portions of a design cannot be copied without the risk of traceable watermarks remaining undisturbed and verifiable within their new and illegal application.

Noise Fingerprinting

Noise fingerprinting is another passive scheme for identifying digital circuits. Here the switching activity within a circuit causes a unique noise signature into the silicon substrate, with a resultant spectrum for the signature being determined by process variations, input sequences, and circuit implementation specifics.

Particular input stimuli can be generated for a VC or design and the resultant noise characteristics are observed through substrate pads, pick-ups, or supply lines. These fairly exotic concepts can be implemented without requiring many of the expensive forensic technologies often customary when checking for unauthorized use of VCs and whole designs within fabricated chips.

SILICON SECURITY

The following discussions review some of the most popular forms of silicon implementation for VCs. It is generally possible to reverse engineer and extract intellectual property from each type of silicon technology – the issue is the degree of difficulty for each type.

Extracting a whole VC from silicon can be more difficult than reverse engineering the entire functionality of the silicon die. This is because a VC realized in silicon can be physically merged with other functions or, (for example) be just an embedded part of a larger bit-stream. So, reverse engineering an entire silicon die or function is one thing, but it requires different and more VC-specific knowledge to extract a particular VC. The following are some silicon technologies explained in more detail to illustrate how this applies:

Programmable SRAM Devices.

Many designs today are utilizing programmable logic to speed their time to market. Programmable devices based on SRAM are volatile; meaning the configuration data is lost each time the device loses power (whether intentionally or because of power interruption.) SRAM-based devices typically store the configuration information in an external location, such as a serial PROM or microprocessor code space, which is downloaded each time the device is powered-up.

There are two techniques used to copy SRAM-based programmable designs: either duplicate the PROM, or duplicate the configuration bit-stream and program the other devices. Either approach can be accomplished quickly and easily. While this technique would allow the illegal copies of a complete SRAM FPGA, a specific IP implemented in the design is not compromised. Extracting Intellectual Property requires an additional and more sophisticated technique. Not only is the capture of the download configuration information needed, but so is the internal logic structure of the SRAM-based FPGA itself, to determine the function performed as a result of the programming. Since most SRAM-based programmable logic has a regular structure, this can be determined for a given architecture, with appropriate investment in reverse engineering. Internal logic structures are proprietary and are unpublished, and while it may be cost effective to reverse engineer a 3000 – 5000 gate design, it is a daunting task to extract Intellectual Property from a flat netlist of 1-2 million gates. An engineering team might often be better off creating their own block diagrams and developing their own VC implementation.

Hard-Mask ICs

It is popularly believed that the most difficult programmable device to reverse engineer is a hard mask IC. However, due to the need for failure analysis tools, the industry has developed many sophisticated techniques to reverse engineer a hard mask IC. One technique is to selectively strip off one layer at a time, photographing the layers as they are exposed. These photographs are then overlayed, and the interconnect and transistors are extracted from the design. (See the section on, Chemical Protection, which would prevent this approach from being taken.)

An experiment was performed utilizing this technique, which showed that it took two weeks to reverse engineer and capture an entire 386 processor. This experiment showed that if a complete chip is reverse engineered, a copy can be made. A more difficult task is to extract individual VCs so that they can be independently used in a different design. So, while hard mask integrated circuits are more secure than SRAM or flash-based technologies, extraction and use of a particular VC netlist comprised of 10K's to millions of gates, (when logical functions may be physically merged), may require comparable expertise to creating the VC from scratch.

Antifuse Programmable Devices

Once programmed, an antifuse is inherently non-volatile, which allows the device to retain its configuration indefinitely without external means-batteries, PROM or microprocessor code space. Antifuses do not have any residual electric or magnetic fields to detect, nor is there anything visual that can be seen from the top or bottom of the die to determine the programmable state of the antifuse device locations.

The only successful attempts at locating programmed antifuses has been using a Transmission Electron Microscope (TEM). This is a destructive sample technique that costs approximately $1,000 for a single TEM sample, today. With approximately 500,000 antifuse sites on a typical antifuse part, it would cost at least $500 million to capture a complete design. Furthermore, to capture the design, 20,000 programmed antifuses would have to be identified exactly to copy or reverse engineer a single sub-10K gate design. A limitation of antifuse technology is the relatively low gate count of 50-100K gates. Even though there are no known efficient techniques to reverse engineer antifuse technology, some antifuse providers have already provided the ability to incrementally change FPGA die areas in such a way as to permit the insertion of digital signatures or keys on a chip-by-chip basis.

So, be aware that when a native implementation technology (such as SRAM, hard-mask, antifuse, flash, etc.) is selected, there is an inherent ease/difficulty in extracting both the entire design and also in extracting a specific portion of that design (such as a single VC).

CLOSING DISCUSSION

It is up to each developer, owner or licensee of virtual components to determine the type and amount of protection that will be employed for each VC in their possession. The party needs to have an assessment made of the actual and strategic value of each VC design in order to determine the type of protection or control dictated for the VC. How important is the design (VC) to the company and what is the cost of the potential loss of control of the VC? The owner needs to understand the regulations and principles of the methods providing protection to VC designs. Where will the user of the VC integrate, fabricate and sell the chips that are generated using the developer's VC?

It is important to understand the nature and type of protection that should be afforded to the VC, since legal organizations that operate under different governments may be called upon to adjudicate the improper use of the VC. Therefore, very significant factors in the licensing of virtual components are not only a complete understanding of their use and application, but also the development of a high-level of mutual trust with the licensee.

Based on a careful assessment of the above, the owner of VCs must then decide which forms of protection and care provide the best security and level of risk for releasing the VC to a third (and fourth, etc.) party, given the value of the sale/trade. The tradeoffs used in making this type of decision are often unique and may be specific to each developer, user, and also to each virtual component developed and licensed.

Owners should generate a matrix for each virtual component that documents and analyses the following categories of exposure, in order to assess the type of protection that is appropriate for each element of a virtual component.

The chart below shows an example of how one might evaluate, and afford protection to, a given virtual component. The value statement is that of the particular element of the virtual component to the owner. There are no fixed rules that can be used in making this type of assessment, because considerations are all relative to the owner's business, their personal and technical judgements, and the projected effect upon current and future revenue and profit potential for the company. It is likely that over time, some of the actions relative to the considerations will change and so, any matrix such as this will need to be updated and maintained.

Example VC Protection Scheme Summary

Item	Protection	Patent	Protection Type	Item Value	Protection Cost
System Evaluation Model	No	No	LA	$	$
Test Bench	No	No	LA	$	$
Behavioral Model	No	No	LA or DF	$	$
Bus Model	Yes	No	LA or DF	$	$
Schematic Diagram	Yes	Possible	LA	$	$
RTL Source	Yes	Possible	LA,E,DW	$	$
Physical Netlist	Yes	Possible	F	$	$
GDS II Tape	Yes	Possible	LA,E,DW	$	$

Total Sum Cost of Protection Schemes = $
Company Value of VC = $

LA= Legal Agreement
DF= Digital Fingerprint
E= Encryption
DW= Digital Watermark
F= Antifuse FPGA

In addition to the decision on the investment of protection schemes for a given VC, such judgements should be preceded by understanding such issues, as:

a) Where will these various levels of abstraction reside?
b) Who will and should have access to this data?
c) How will the environment be secured?
d) How will data in transit be protected?
e) How are tools manipulating the data secured?

Not every company can practically afford to guard against all potential liabilities and implement exhaustive protection schemes. However, it is prudent that every company should understand the scope of its liabilities and be proactive in the selection of their intellectual property protection schemes.

In a closing observation, one would consider it imprudent, for example, if the head of a household did not carry insurance for the home, an event of death, or loss of the family car. Why then would responsible executives and managers not protect their investors by thoughtfully securing the intellectual property of their company?

GLOSSARY

Antifuse	A technology used in FPGA's for realizing logic functions by the programming of low-resistance (antifuse) connectors.
ASIC	Application Specific Integrated Circuit
CPLD	Complex Programmable Logic Device
DWG	Development Working Group (such as, VSIA's IPP DWG)
EDA	Electronic Design Automation
Forensics	The process of detection or validation of ownership - generally those expensive analysis methods performed on silicon realizations of VC's or components.
Foundry	A contract manufacturer of silicon wafers; normally not possessing or selling semiconductor products of its own.
FPGA	Field Programmable Gate Array
GDS II	The physical database used for building masks employed in the silicon wafer manufacturing process, Graphical Design Stream, II.
Hard-Mask IC	A predefined semiconductor realization of digital and/or analogue circuitry. The function is fixed unless containing programmable elements.
ID	Identification (label or) Designator.
IP(P)	Intellectual Property (Protection)
Passivation	A normally inert coating applied to protect silicon die during the manufacturing and assembly processes.
PROM	Programmable Read Only Memory; a semiconductor memory, which is both readable and programmable.
Reverse Engineering	The action of recreating higher level original design information from available materials, i.e., recreating VC schematics from a silicon die by reconstructing transistor connectivity off the bare silicon images.
RTL	Register Transfer Language. A high level and simplifying method of efficiently representing digital logic functions.
SRAM	Static Random Access Memory; a semiconductor memory type. Non-volatile, able to read/write data.
VC	Virtual Component
VSIA	VSI Alliance

BIBLIOGRAPHY

1. FBI Site, re: Piracy/Trade Secrets
   http://www.fbi.gov/majcases/copy/copy.htm#ex2

2. Bruce Schneir, "Applied Cryptography, etc.," John Wiley & Sons, ISBN 0471117099.

3. Irene Fernandez and Dennis Fernandez, "Building Legally Sound Intellectual Property Portfolio," p. 42, Silicon Strategies, June 1998

4. SIIDTECH, Portland, Oregon. Founder Steve Sapiro (USA) 503-357-8239

5. Digital Signature and Certificates-Entrust Technologies, Inc.
   http://www.entrust.com

6. E. Charbon and I. Torunoglu, "Intellectual Property Protection via Hierarchical Watermarking," in International Workshop on IP Based Synthesis and System Design, 12/98

7. R. Gharpurey, E. Charbon, R. G. Meyer and A. L. Sangiovanni-Vincentelli, "Substrate Noise: Analysis and Optimization for (IC) Design," Kluwer Academic Publishing, Boston, MA, appears 1Q2000