



Semiconductor Equipment Security Guidelines: Intellectual Property Protection

**International SEMATECH Manufacturing Initiative
Technology Transfer #07114888A-ENG**

Advanced Materials Research Center, AMRC, International SEMATECH Manufacturing Initiative, and ISMI are servicemarks of SEMATECH, Inc. **SEMATECH**, the **SEMATECH** logo, **Advanced Technology Development Facility, ATDF**, and the **ATDF** logo are registered servicemarks of SEMATECH, Inc. All other servicemarks and trademarks are the property of their respective owners.

**Semiconductor Equipment Security Guidelines: Intellectual Property
Protection
Technology Transfer #07114888A-ENG
International SEMATECH Manufacturing Initiative
December 19, 2007**

Abstract: This report from the MFGM045M project describes a security framework and guidelines for protecting intellectual property (IP) on equipment in a semiconductor manufacturing environment. Components of the framework define the capabilities of IP protection software. This document should prove useful to both IC maker and original equipment manufacturer personnel.

Keywords: Business Trends, Computer Software, Intellectual Property

Authors: Harvey Wohlwend

Approvals: Harvey Wohlwend, Project Manager
Brad Van Eck, Program Manager
Scott Kramer, Director
Laurie Modrey, Technology Transfer Team Leader

Table of Contents

1	Purpose/Scope	1
	1.1 Intended Audience	1
2	References	2
3	Business-Level Requirements	2
	3.1 IC Maker Process-Level Information Security	2
	3.2 Supplier Equipment-Level Information Security	2
	3.3 Equipment Troubleshooting and Performance Tuning	2
	3.4 IC Maker-Level Collaborations	2
	3.5 IC Maker-to-Foundry Relationship.....	3
	3.6 IC Maker and Supplier Collaborations	3
	3.7 IC Maker (N+1) Process Generation Challenges.....	3
	3.8 Time Value of IP.....	3
	3.9 IP in Different Functional Areas	3
4	IP Protection Capability.....	3
	4.1 Hardware-Connectivity Layer.....	4
	4.1.1 Platform.....	4
	4.1.2 Network File Shares (Inside the Equipment).....	4
	4.1.3 External Boxes	4
	4.1.4 User Credentials.....	4
	4.1.5 Controlling Access to Different Removal Media.....	4
	4.2 Software-Logical Layer	4
	4.2.1 Authentication	5
	4.2.2 Authorization	5
	4.2.3 Access Control	5
	4.2.4 Logging	5
	4.2.5 Identification of IP	5
	4.3 Business Layer	6
5	Constraints.....	7
	5.1 Tool Operation	7
6	Roles and Responsibilities.....	7
	6.1 IC Maker	7
	6.2 Foundry	7
	6.3 OEM.....	8
7	Future Requirements	8
8	Summary.....	8

Acknowledgments

The IP Protection project would like to thank the participating ISMI member company representatives for their openness during the teleconferences and for their cooperation in the development of this document.

1 PURPOSE/SCOPE

This document highlights the complex intellectual property (IP) challenges IC makers and original equipment manufacturers (OEMs) in the semiconductor manufacturing environment. The document presents a security framework that specifies the essential components of information security, which in turn allows the seamless integration of daily manufacturing and support activities with the handling of intellectual property. The components of the framework are capabilities, not product specifications or specific business processes. They can be considered high level requirements to characterize the behavior of IP protection software. The framework provides the following:

- Guidelines based on standard and non-proprietary capabilities
- Guidelines for software design in information security
- Guidelines based on common practices in the semiconductor industry, such as usage of foundries, extensive partnering and collaborations, and concurrent multiple technology nodes
- Information required for integrating IP handling with manufacturing operating procedures
- Emphasis on the key areas of IP protection connected with the semiconductor equipment and process
- Requirements to provide traceability of equipment IP when removed or transferred from the equipment

The IP equipment security framework will NOT

- Highlight areas of IP concern within the semiconductor manufacturing process and equipment technology
- Recommend products, services, or specific design options
- Endorse or advocate security business models
- Apply role-based security to the entire computing environment within the equipment or integrate with existing IC maker corporate security systems
- Use cost estimations in the recommendations
- Include standard business practices (e.g., use of firewalls, integrity of backups, and recovery)
- Recommend deviations from these guidelines based on individual company policies and practice

1.1 Intended Audience

Knowledge of the equipment IP security framework is required for all areas of semiconductor manufacturing, including those in the following roles:

- IC maker process engineers, equipment engineers, and manufacturing operations personnel
- Assembly, test, sort, and supporting areas, including hardware and software

- Supplier local and remote field service engineers
- Supplier and third-party application developers and software architects

2 REFERENCES

- [*E-Diagnostics Guidebook*](#), Technology Transfer #01084153D-ENG.
- [*Semiconductor Equipment Security Guidelines – Virus Protection*](#), Technology Transfer 04104567C-ENG.
- [*SEMI E139, Specification for Recipe and Parameter Management \(RaP\)*](#).
- [*Role-Based Security*](#), NIST.

3 BUSINESS-LEVEL REQUIREMENTS

Business-level requirements are based on current business practices within the semiconductor industry. The following sections outline equipment IP security requirements.

3.1 IC Maker Process-Level Information Security

IC makers make significant investments in semiconductor process technology to get the most performance from the semiconductor products they manufacture and sell. Process-level IP security is crucial to their long-term financial success.

3.2 Supplier Equipment-Level Information Security

Suppliers provide state of the art equipment for the matching process technology that enables the IC makers to manufacture semiconductor products. Supplier IP security is critical to their long-term financial success.

3.3 Equipment Troubleshooting and Performance Tuning

IC makers and suppliers are faced with situations in which critical information is needed to troubleshoot either equipment function or performance. Some troubleshooting examples include equipment downtime, yield, process failures, performance, and equipment/chamber matching. The critical information typically includes IP from IC makers and suppliers such as recipes, run rates, or equipment diagnostic information. The purpose of these IP security guidelines is to provide infrastructure support to make the necessary information available and yet be comfortable that IP is protected.

3.4 IC Maker-Level Collaborations

Due to the mounting costs of semiconductor process technology development, several IC makers are collaborating in limited areas. The challenge they face is how can IP security facilitate IP sharing in specified areas while protecting the other areas. IP information should be classified related to importance and age, such as the related controls (in which period of time a reclassification should happen) and the activities (what activities should take place when the IP classification has been changed).

3.5 IC Maker-to-Foundry Relationship

Different IC makers run different products and processes on the same “shared” equipment. Hence, IP must be separated based on the IC makers’ requirements.

3.6 IC Maker and Supplier Collaborations

Due to the mounting costs of semiconductor process technology and equipment development, IC makers and suppliers are collaborating to develop new equipment to support new process technology. They face challenges similar to those in IC maker collaborations, in that each party wants to share only required information while securing all other IP.

3.7 IC Maker (N+1) Process Generation Challenges

The mounting costs of process equipment present a big cost challenge for new process technology development. The (N+1) process technology developers must use the N process technology equipment while it is producing products from N process technology. The challenge is how IP security can enable both (N+1) and N process engineers to share equipment but yet be able to secure IP from (N+1) and N technologies from each other.

3.8 Time Value of IP

The IP value of semiconductor technology decreases over time. Since IP protection is not free, it would be wasteful to incur a great expense by constructing a highly secure system that ultimately protects worthless information assets. The effort expended to address security threats is balanced against the damage that would result from information exposure or corruption. Protecting older technology (e.g., 180 nm) today the same way as 45 nm technology may not make business sense to all IC makers.

IP protection capability must be selectable by the IC makers.

3.9 IP in Different Functional Areas

Not all areas of semiconductor processing require equal levels of IP protection. For example, wafer handling may not require IP protection at all. However, thin films, diffusion, etch, and lithography may have varying degrees of IP protection issues. The IP protection capability must be sensitive to the different functional areas.

4 IP PROTECTION CAPABILITY

IP protection is aligned with the security architecture described in the *e-Diagnostics Guidebook*, Chapter 7, “Security Architecture.” This alignment includes controlled access to equipment data and supporting computer systems. All access is logged.

The essential elements of the architecture are described below, emphasizing relevance to equipment IP protection. The three components of security are the following:

- Hardware-Connectivity Layer
- Software-Logical Layer
- Business Layer

4.1 Hardware-Connectivity Layer

This layer focuses on the computer-to-computer connectivity between equipment and other systems in and through the IC maker's Intranet. The capabilities of hardware-connectivity relevant to equipment IP security are listed below.

4.1.1 Platform

The platform includes the hardware, operating system, and software products. The operating system must be able to support role-based security through authentication, authorization, and access control.

4.1.2 Network File Shares (Inside the Equipment)

The supplier's tools need to support network segmentation and isolation for the IC manufacturer and supplier's benefit. Suppliers also need to support file- and folder-level user ID, password protection, partitioning, access control, and control of access to proprietary information. Equipment software connects only to authorized applications. These mechanisms also protect internal people from accessing the protected space.

4.1.3 External Boxes

External connections (e.g., data collection/monitoring devices, Interface A, Interface C) are subject to the role-based security requirements.

4.1.4 User Credentials

There can two approaches to user credentials: operating system (OS)-based or application-based. Technically, the two methods are generally equivalent to each other and the choice between the two requires a detailed business and software requirements analysis. Equipment supplier must support at least one of these methods.

4.1.4.1 OS-Based

This approach emphasizes the use of OS-provided security credentials to perform authentication and authorization. OS-based credentials are easier to administer and manage from a corporate IT security vantage point.

4.1.4.2 Application Based

This approach uses credentials that are defined within the context of the application. They are independent of the OS-based user credentials and must be managed separately.

4.1.5 Controlling Access to Different Removal Media

IC makers may turn off and on access to removal media within equipment, depending on business policy.

4.2 Software-Logical Layer

This layer focuses on the dynamic aspects of security typically lying in the realm of software. End users, such as engineers and service technicians, or applications interact with equipment through the software (i.e., the control systems software). The key security capabilities of interest to equipment IP security directly related to role-based security are described below.

4.2.1 Authentication

Each user belongs to at least one group of users; each user is provided unique security credentials that enable individual accountability for IP security. Use of generic accounts is counterproductive to IP protection and is discouraged as it violates role-based security. Ideally, authentication is tied into a company-wide, factory-wide system.

4.2.2 Authorization

Each user group has clear mapping to what they are allowed to do based on manufacturing roles and responsibilities. A basic tenet of role-based security, the “need to know” is enforced. The default setting is limited access; special approval is required to get broader tool access.

4.2.3 Access Control

Each user group has clear and unambiguous file and directory-level access control privileges that support its role.

4.2.4 Logging

The equipment must log all activities (e.g., file creation, file access, file dissemination, external disk/memory connection, etc). This enables appropriate and inappropriate activity to be identified and IP protection policies and procedures to be enforced. When the protection mechanisms are violated, action can be taken. Either an active or passive detection enforcement system is implemented.

4.2.5 Identification of IP

4.2.5.1 File-Based IP

One of the fundamental units of IP is the “file,” which may contain different forms of IP. For example, IP can be in the form of text, binary data, images, or any combination of the three. When IP is placed in a file, access control settings for the file based on the users and or groups provide IP protection. IP-laden files can be placed in directories that can also be protected through access control at the user and or group level.

4.2.5.1.1 Separation of IP

The requirement for separation follows the identification of IP. The separation can be implemented in different files and directories with appropriate access control based on user and group roles. For example, in case of collaborations using a specific piece of equipment, the system must be able to provide controlled access to shared areas while restricting access to IP-protected areas for all users simultaneously.

4.2.5.1.2 Archiving, Restoring, or Purging (ARP)

Files that are not needed but are identified as IP pose a leakage risk if left behind. ARP is recommended to move older IP to another location where version controls are tighter and stricter.

4.2.5.1.3 File and Directory Names

Engineers tend to name files with IP such as recipe information to make it easier to classify and differentiate the files. With IP being handled at the file access control level, two versions of each file with IP should be made: one for the IC maker and the other for the supplier. The system is required to maintain a table of names with proper associations.

4.2.5.2 Other Sources of IP Data

4.2.5.2.1 Database

The information is available in the form of a result of a query. Access control with databases and tables must be done on a user-by-user level. Some database products allow row/column level protection as well.

4.2.5.2.2 Secondary Storage

Secondary media such as USB, CD-ROM, etc. is disabled during tool operation based on business policies (Section 4.3).

4.2.5.2.3 Middleware

The information is the form of the data coming from another program, e.g., interaction with message queues. The middleware product must support delegation with appropriate authentication and authorization controls.

4.3 Business Layer

The business layer focuses on the business aspects of integrating security with the manufacturing operations. The relevant areas for equipment IP protection are as follows:

- Nondisclosure agreements (NDAs) are legally binding contracts between IC makers and suppliers that detail how they must conduct business with each other. Sharing IP is part of the NDA; the technology and process used should be agreed upon and spelled out in the agreement.
- Each stakeholder must identify its IP. This includes analyzing digital assets (e.g., recipes, log files, performance data), determining issues in the end-to-end path, and building a comprehensive (defined levels of data security) set of preventive measures to safeguard the IP.
- Business guidelines for sharing IP include defining circumstances under which an IC maker shares recipes and performance information.
- IC makers provide policies for controlling access to removal media within equipment such as USB memory sticks/disks, CD/DVD, etc. The access will be controlled by the tool owners and could be based on production mode and the role of the support personnel. For example, secondary media may be brought on-line only when the tool software is being upgraded for tool maintenance; even then the media must be virus-scanned. The tool owner must have the capability to disable/enable the use of secondary storage.
- Auditing of IP handling allows each party to review the other party's IP handling procedures.
- Separate backups are maintained for IP protected and non-IP protected information.
- All IP must be purged from the tool at the tool's end of life. This can be done by 32 pass wipes, degaussing, or physically replacing the equipment hard drives. This is particularly relevant with a controlled country.
- When replacing or maintaining hard disks, the tool end-of-life requirements must be enforced.

- The requirements for tool reuse/movement are the same as for tool end of life.
- When manufacturing tools are upgraded, reclaimed, or replaced for any reason, all IP must be cleansed from the hard disks or any other storage. The OEM provides a report to the IC maker that all IP information has been removed from the equipment.
- All storage backups that contain IP data are destroyed using typical IT methods that are compliant with generally accepted practices and international standards for secure disposal or reuse of equipment.
- Security policies are required for managing the transfer or movement of equipment IP external to the equipment, such as the transfer to automation systems and mobile computing devices like personal digital assistants (PDAs). The security policies could specify methods and levels of encryption, handling procedures, auditing, logging, etc.
- Training is required on IP protection for all employees that handle IP and whenever a violation occurs.

5 CONSTRAINTS

Other aspects of equipment design to protect equipment IP are described below.

5.1 Tool Operation

Most equipment have a generic user account to operate the equipment. The generic user account can be used by the IC maker, but it *cannot* be used for equipment IP protection, and role-based security will not be used for operating the tool.

6 ROLES AND RESPONSIBILITIES

IC makers and OEMs have distinct roles in protecting each other's IP. The basis of IP protection is a clear and unambiguous definition of IP and implications of IP loss to the stakeholder. These definitions should be reviewed periodically for importance and the time-value of IP. If there is no value to the information, the IP protection mechanism should be turned off for that information.

6.1 IC Maker

The IC maker, including foundries, is primarily focused on the process aspects of semiconductor technology. The IC maker (asset owner) is responsible for identifying the objects (including, but not limited to, recipes and metrology images) that require IP protection within the process space and the use cases associated with handling IP.

Each IC maker defines the procedures for granting and logging access to resources available through the network. Role access, extension, or termination must be reviewed periodically.

6.2 Foundry

The foundry has a relationship with multiple IC makers. Both the IC maker and the foundry must identify the objects to be protected.

Each foundry defines the procedures for granting and logging access to resources available through the network. Role access, extension, or termination must be reviewed periodically.

6.3 OEM

OEMs are focused on the equipment aspects of semiconductor technology including identifying the objects that require IP protection from an equipment vantage point (asset owner). Additionally, OEMs must incorporate IP protection into the equipment controls software according to IC maker use cases.

Tools must provide capabilities to support operations without storing recipes at the tool. For recipes that require IP protection, no older versions of the recipe must remain on the tool once the recipe is deleted from the tool.

OEM-generated backups must not contain any IC maker IP.

7 FUTURE REQUIREMENTS

Tools must support a factory-wide recipe and parameter system (SEMI E139, RaP). The use of unique ids (UUIDs) for every recipe provides additional IP protection.

Factories must integrate equipment authentication and authorization with either factory-level or IC maker company-level capabilities.

IC makers must align on equipment IP traceability and handling procedures for IP external to the equipment.

8 SUMMARY

IP protection is a joint responsibility between IC makers and OEMs. Protecting IP is critical to the long-term financial success of the semiconductor industry. Intellectual property must be protected from the time the information becomes valuable throughout its entire life cycle.

**International SEMATECH Manufacturing Initiative
Technology Transfer
2706 Montopolis Drive
Austin, TX 78741**

**<http://ismi.sematech.org>
e-mail: info@sematech.org**