e-Manufacturing Security Framework
NIST ATP Project
March 18, 2003

Larry Barto
AMD
Larry.Barto@amd.com
Agenda

- History
- Project Scope
- Obstacles
- Proposed Solution
- Standards
- Project Plan
**Background**

- **History**
  - NIST ATP is a rigorously competitive cost-sharing program designed to assist U.S. industry pursue high-risk research & development with high-payoff potential for the U.S.
  - AMD and several other organizations submitted a NIST ATP Proposal in the 2001 competition entitled:
    - “e-Manufacturing security framework to improve semiconductor productivity”
  - Team won a 3-year NIST ATP award totaling about $10 million
    - U.S. Government funds 49.99 %, participants fund 50.01 %
  - **Progress**
    - Project started in November 2001
    - Completed Phase I (Security Framework) in January 2003
  - The project currently has 3 Joint Venture Partners

[Images and logos for NIST, AMD, Ocean Sensor, and ILS Technologies]
Partner Expertise

- **Fab and factory systems expertise**
  - Project administrator
  - Application and security requirements
  - Pilot site

- **Wireless e-Diagnostics™ Applications**
  - Advanced Wireless Sensor Systems
  - Vibration, ESD, pressure, temperature, etc.
  - Condition-based maintenance

- **e-Diagnostics and Automation Applications**
  - eCentre™ product
  - 3rd party e-Diagnostics software provider for the semiconductor industry
  - Contract with IBM to deploy eCentre for tools in the new 300mm factory in East Fishkill
Project Goals and Objectives

• Objective
  – Enable collaborative manufacturing for mutual benefit while protecting intellectual property

• Goals
  – Develop a security framework for collaborative manufacturing that allows dynamic, fine-grained security controls over the data of both the tool supplier and IC manufacturer
  – Develop a number of collaborative manufacturing applications, integrate them with the security framework and pilot them in a fab to demonstrate the feasibility and measure benefits

• Project Phases
  – Phase I – Security Framework
  – Phase II – Secure e-Diagnostics
  – Phase III – Secure e-Manufacturing
Why Collaborative Manufacturing?

- Wafer fabrication plants can significantly increase productivity of manufacturing tools by
  - Increasing tool up time
  - Decreasing non-product wafer
- Meaningful gains require collaboration among tool suppliers and chipmakers to resolve problems
- Electronic interaction offers the most cost effective and quickest means to collaborate
- This collaboration is just the start, other gains may be found through:
  - Condition-based Maintenance
  - Advanced Process and Equipment Control
  - Fault Detection
  - Spare parts management
  - Interfaces to Supply Chain Management
Obstacles

- **Business Model – Top business concern**
  - How do chip makers and suppliers make a return?
  - Who pays for the capability?
- **Security**
  - Concerns about the security of tool and the intellectual property it contains (in the form of recipes, process data, and embedded logic) have impeded the exploitation of electronic collaboration
  - This was expressed as the most serious technical concern at:
    - ISMT e-Diagnostics face-to-face supplier break-out: Sep 2000
    - Interviews at ITRS and SEMICON West
    - SEMI Software Symposium: Nov 2002
The Security Problem

- **Security** is the Achilles heel for Chipmakers and tool supplier collaboration, due to concerns over:
  - Intellectual Property
  - Tool Control
  - Recipes
  - Safety

- **Sharing** of some sensor and process data, and even recipe development information in some cases, must occur for collaboration to work

- **International SEMATECH** has outlined security requirements in their e-Diagnostics Guidelines
  - Firewalls
  - Security Levels
  - VPN
  - IPSec
What’s Different?

- **Security Framework**
  - Other efforts are addressing *connection* security
    - Establishing a secure pipe between the remote site and the fab tool
    - Controlling basic access, i.e., user authentication
  - Our project addresses *content* security
    - What specific data items can be accessed?
    - What commands can be issued?
    - Under what conditions?
      - May depend on dynamic factory state (tool, MES, etc.)
      - May depend on other active users
      - May depend on aggregation of data items
    - How should the data be transformed?
      - Hiding, categories, ranges, selective sampling, etc.
    - What additional types of encryption are required?
Innovative Solution

- We are developing an **open security framework** that will enable
  - Remote diagnostics of tool by chip makers and suppliers, to decrease the mean time to repair
  - Condition-based maintenance to increase tool up time and factory efficiency
  - Spare parts management through and across the supply chain, to improve response time and decrease parts inventories
  - Factory-level automated process control across multiple tool types from different vendors, to allow the factory to integrate support from competing suppliers without compromising intellectual property.
  - Confidence that the intellectual property of all parties remains secure
Open Security Framework

• What is an *open security framework*?
  − External interfaces are published and become standards
  − Anyone can develop and market a Security Framework that complies with the interface standards
  − Anyone can develop and market collaborative applications that integrate with any standards-compliant Security Framework

• Our project is developing the first implementation of the Security Framework: Flexible Security Wrapper
  − Leverages existing standards (XML, SOAP, etc.)
  − Attuned to emerging standards
    • Use where possible
    • Influence changes where experience/analysis shows a need
FSW Interfaces

- Developing standards
- Potential developing standards
- Emerging SEMI standards

Client

FSW

Tool / Sensor

SOAP HTTPS

SOAP HTTP

XML

Virtual Factory

MES
 Relevant Emerging SEMI Standards

- **3507 – Equipment Client Authentication and Authorization**
  - Abstract model of authenticated communication and ACL (Access Control List) management

- **3509 – Data Collection Management**
  - Abstract model of Data Collection Plans, DCP management interface and state models, and DCP reporting formats

- **3510 – Equipment Self Description**
  - Abstract model of equipment metadata describing units, types, equipment structure, state models and events, alarms/exceptions

- **PR8-0303 (3563) – Proposed Standard for Equipment Data Acquisition**
  - A restricted “interim” means for the industry to begin prototyping and early development of essential EDA concepts using the targeted technology

- **3522A Common Equipment Model (CEM)**
  - Documents the model of physical equipment structure

- **Guidelines for XML Usage Within SEMI**

The Security Framework intends to use the above standards to communicate with the tool and will influence them as required.
Client-FSW Interface

- **Client-initiated functions**
  - Initialize
  - Login
  - Logout
  - Get Data Model
  - Get Data (equipment constants, status variables, alarm state, recipes, etc.)
  - Add Event Listener (event report, enable/disable alarm, set trace)
  - Remove Event Listener
  - FTP
  - Remote Tool Operation (RTO)

- **Tool-initiated functions**
  - Initialize
  - Asynchronous Notify (event reports, alarm reports, trace data)
FSW Interface to Virtual Factory

- **Virtual Factory**
  - Façade from which dynamic factory state information is obtained
  - Updates in real-time from MES and other relevant sources

- **FSW-initiated functions**
  - Initialize
  - Get Attribute Names
  - Get Attribute Value
  - Subscribe to Attribute
  - Unsubscribe to Attribute

- **Virtual Factory-initiated functions**
  - Attribute Value Changed
Phase I – Security Framework

• **Tasks**
  - Investigate Security Requirements
  - Define Security Reference Model
  - Develop Flexible Security Wrapper (FSW)
  - Develop Prototyping Environment
  - Solicit and incorporate industry feedback

• **Status – Phase I is completed**
  - The first implementation of the FSW has been developed and tested in a simulated factory environment
  - The approach appears to be feasible
  - Initial performance testing is encouraging
  - Additional refinements will occur in Phases II and III as the FSW is integrated with representative applications
Phase I Technical Learning

• Throughput
  – The prototype system was distributed over seven 7 PC’s, each performing at AMD Athlon 1800 level or better
  – Implemented an FSW Thread Pool servicing separate queues for incoming/outgoing requests/responses to improve system performance
  – Achieved a sustained message rate of 20 messages/sec for two users (small messages < 1 KB)

• SOAP / HTTP
  – Desired a SOAP API layer that allowed SOAP communication without requiring a stand-alone web server
  – The library had to be small enough to distribute easily and have a license that allowed it's use without fee
  – The library eventually used was GLUE (www.themindelectric.com), which is free for use in the standard version. The professional version requires a license and fees. Six other SOAP libraries were evaluated.
Phase II – Secure e-Diagnostics

- Develop security policy configuration tools
  - Develop GUI to define security rules
  - Develop or purchase rules engine to evaluate security rules

- Define e-Diagnostics requirements and evaluation criteria
  - Select tool type for a fab pilot
    - Identify several tool types that would provide benefit to the fab
    - Determine which tool suppliers are interested
    - Find the best match between tool supplier and fab interests
  - Identify potential sensor application with tool or separate pilot
  - Collect application/security requirements from fab and supplier
  - Determine evaluation criteria (availability, mean time to repair, etc.)
  - Establish baseline metrics for evaluation criteria
    - Important to measure the benefits
Phase II – Secure eDiagnostics

- Develop e-Diagnostics application
  - Incorporate requirements from fab and tool supplier
  - Integrate with Flexible Security Wrapper

- Run pilot demonstration in fab
  - Develop tool connect software changes to enable e-Diagnostics in parallel with control thru SECS/GEM port
  - Install project software at fab site and tool supplier
  - Install sensor (external to tool or separate location)
  - Run pilot with tool supplier during September/October 2003
  - Collect metrics and determine benefits

- Verify security of Flexible Security Wrapper
  - Use contractors with security expertise to evaluate security
  - Evaluate architecture of Flexible Security Wrapper
  - Test vulnerability of system in prototype lab at ILS Technologies

- Status – Phase II underway since January 2003
Phase II Milestones

- Security Policy Configuration Tools
  - Practical enough for operational deployment
  - Flexible enough to implement required security policies
    - Includes handling rules with dynamic dependencies
- e-Diagnostics Application
  - Provides required functionality
  - Provides benefits according to evaluation criteria
    - Metrics from fab pilot compared with baseline metrics
- Secure Flexible Security Wrapper
  - Withstands attack by outside consultants in prototype lab
  - Performs with e-Diagnostics application during pilot
Phase III – Secure e-Manufacturing

- Tasks
  - Evaluate productivity opportunities and existing applications
  - Develop and test predictive maintenance application
  - Develop and test embedded sensor application (i.e., ESD detection)
  - Convert APC application
Summary

• Conclusions
  – It appears feasible to develop an open security framework to allow collaborative manufacturing while protecting intellectual property
  – The open security framework can provide fine-grained control of data/commands, dependent on dynamic factory conditions, with acceptable performance

• Tool Suppliers
  – We’re looking for volunteers for pilot projects

• Questions?

Contact Information:
Larry Barto
512-602-4845
Larry.Barto@amd.com