

e-Diagnostics/e-Manufacturing requirements and successes at AMD

Stephan Gramlich
April 20, 2004

- **e-Diagnostic strategy**

- Results in individual projects
 - e-Diagnostic / e-Manufacturing Security Framework (NIST ATP Project)
-

1. AMD wants a single universal e-Diagnostics approach that can support all OEMs.

We don't want a different proprietary solution from each OEM, each requesting their own server installed at AMD.

2. Security is of paramount concern. AMD must be able to protect its IP and control access to the tools.

3. We prefer the e-Diagnostics solution be provided by an independent 3rd party rather than one of the OEM's. With this approach we can ensure the e-Diagnostics solution provides AMD with security controls we can trust.

4. The business issues surrounding e-Diagnostics still need to be resolved:
 - (a) who is going to pay for it and how ?
 - (b) what are the quantifiable benefits to each party (OEM & chipmaker) ?

-
- e-Diagnostic strategy

- **Results in individual projects**

- e-Diagnostic / e-Manufacturing Security Framework (NIST ATP Project)
-

Results in individual e-Diagnostic / e-Manufacturing projects



- Inspection tools and production tools from several OEMs connected via VPN and by using SecurID
 - ~ 25% of all issues can be solved by using remote diagnostics
- On-site data collection server for tools from several OEMs
 - Supports central onsite monitoring
- Implementation of SAP Plant Maintenance to manage PM & CM activities incl. automated parts ordering and tracking process

-
- e-Diagnostic strategy
 - Results in individual projects

- **e-Diagnostic / e-Manufacturing Security Framework (NIST ATP Project)**



- Team has a 3-year NIST ATP award totaling about \$ 10 million
 - Project title: “eManufacturing security framework to improve semiconductor productivity”
 - U.S. Government funds 49.99 %, participants fund 50.01 %
 - Project started in November 2001
- The project currently has 3 Joint Venture Partners
 - **AMD**
 - Project Administrator
 - Provides fab requirements & pilot site
 - **ILS Technology**
 - e-Diagnostics and Automation Applications (eCentre)
 - **Oceana Sensor Technologies**
 - Wireless e-Diagnostics Applications
 - Advanced Wireless Sensor Systems

- **Objective**

- Enable collaborative manufacturing for mutual benefit while protecting intellectual property

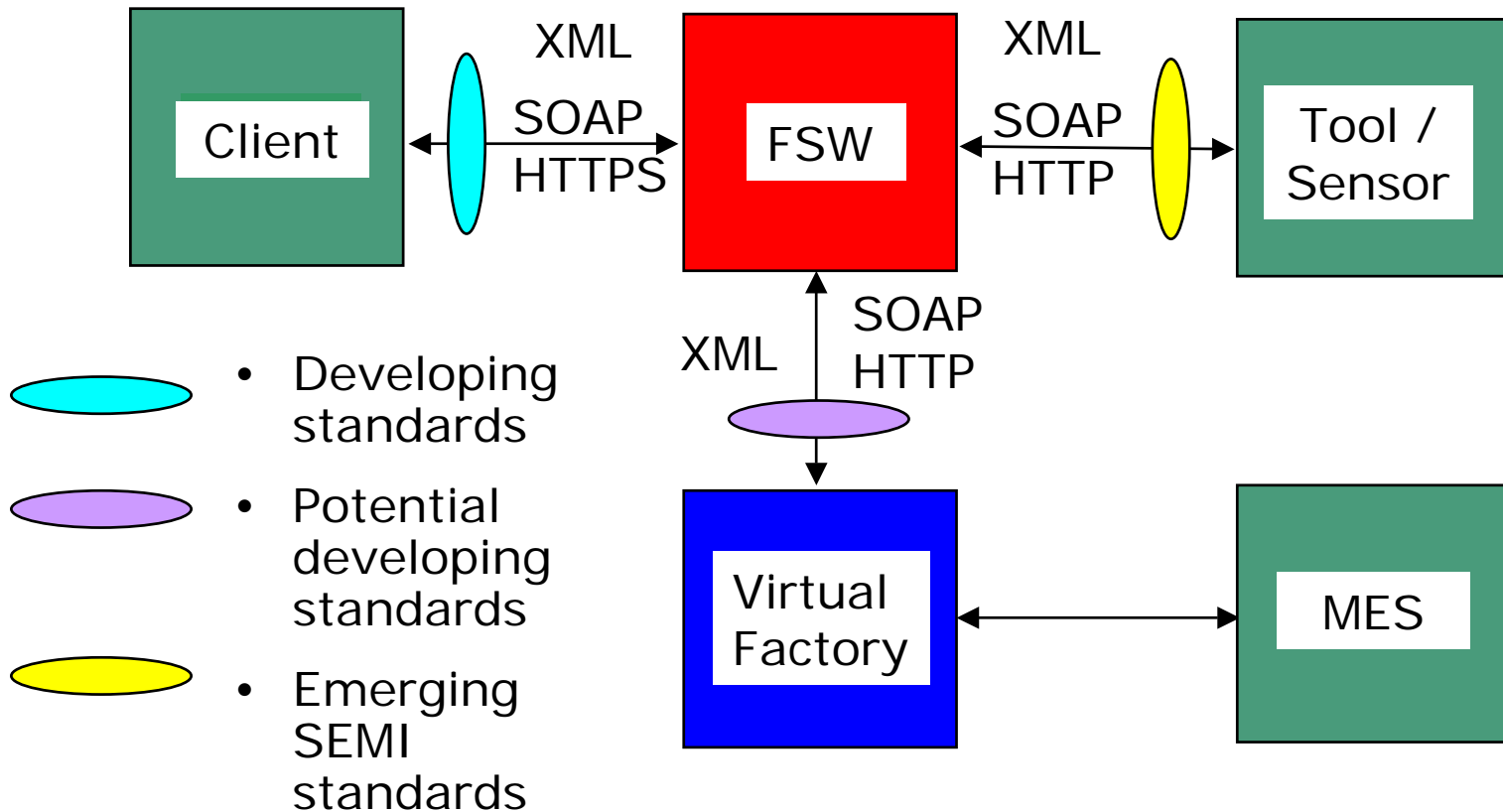
- **Goals**

- Develop an *open security framework* for collaborative manufacturing that allows dynamic, fine-grained security controls

- Wafer fabrication plants can significantly increase productivity of manufacturing tools by
 - Increasing tool up time
 - Decreasing non-product wafers
- OEM's can increase productivity by
 - Reducing travel costs
 - Providing specialized expertise quickly, efficiently
- Meaningful gains require collaboration among tool suppliers and chipmakers to resolve problems
 - Electronic interaction offers the most cost effective and quickest means to collaborate
- Security is a major concern in electronic collaboration
 - Intellectual Property, Tool Control, Recipes, Safety

- 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 Security Framework 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 security is required as data is moved within the fab ?

- 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.)
 - Uses emerging SEMI standards (Interface A) where possible
 - Ballot 3509, E125, E120, E121, E132
 - Influence changes to standards where experience/analysis shows a need



- **Status – Phase I is completed (January 2003)**

- ✓ The first implementation of the FSW has been developed and tested in a simulated factory environment
- ✓ The approach is feasible
- ✓ Performance is encouraging
- ✓ Additional refinements planned in Phases II and III as the FSW is integrated with representative applications

- **Status – Phase II is nearing completion (April 2004)**
 - ✓ Developed a GUI to graphically define security rules
 - ✓ AMD and Semitool developed e-Diagnostic requirements & evaluation criteria for a pilot
 - ✓ NIST team developed an e-Diagnostic application based on ILS' eCentre and integrated it with the Flexible Security Wrapper
 - ❖ Pilot in progress at AMD's Submicron Development Center with Semitool Plater and ACMS chemical management system
 - ❖ Feedback from outside security experts currently being incorporated into the FSW based on the results of simulated attacks in the prototype environment

• Preliminary Results

- The e-Diagnostics capability is useful for troubleshooting problems that required specialized expertise such as software issues
- Useful for applying patches and performing tricky software upgrades with the assistance of remote experts
- AMD tool owners find the Remote Tool Operation capability (front panel access from office/home) useful for performing their daily duties

• **Tasks**

- Evaluate productivity opportunities and applications
- Develop and test equipment control applications
 - Alternative e-Diagnostic architectures
- Develop and test FIPS 140 security application
 - Federal Information Processing Standard for sensitive information
- Develop and test process control applications
 - Integration of FSW security with fab process control systems as well as industrial process control in non-SEMI industries

• **Status - Phase III is in progress**

- ✓ Completed evaluation of current challenges and opportunities and developed an updated list of applications
- ❖ Requirements analysis and design underway for several applications that will be integrated with the FSW

- The commercial release of eCentre currently supports file transfer (FTP) and Remote Tool Operation (RTO) very robustly. These features have been available commercially for some time.
- eCentre 2.1 contains the first commercial release of the data collection plan (DCP) management functions and is capable of communicating with a Flexible Security Wrapper (FSW).
- The FSW is not yet commercially available

• Conclusions

- It is 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
- e-Diagnostics provides benefits to both chipmakers and OEM's

• Tool Suppliers

- We're looking for additional OEM's for pilot projects

• Questions ?

Contact Information:
Stephan Gramlich
+49/0351 277-3200
Stephan.Gramlich@amd.com

IBM is a registered trademark of International Business Machines Corporation.

© 2004 Advanced Micro Devices, Inc. All rights reserved.

AMD, the AMD Arrow logo, AMD K6, AMD Duron, AMD Athlon, AMD Opteron, the AMD64 logo, and combinations thereof, are trademarks of Advanced Micro Devices, Inc in the U.S. and/or other jurisdictions. Other product and company names used in this presentation are for identification purposes only and may be trademarks of their respective companies.