

International SEMATECH e-Diagnostics Program

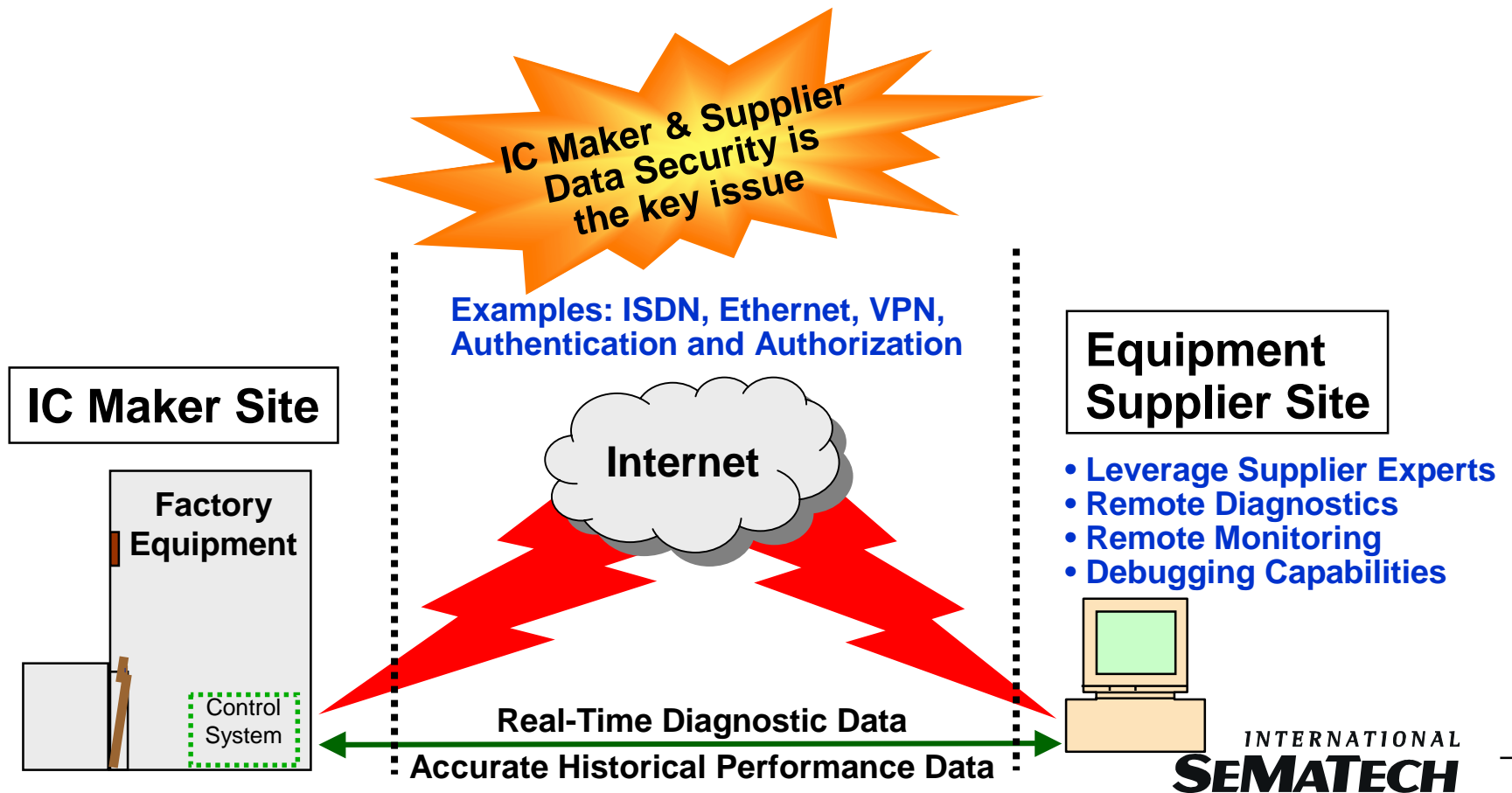
www.sematech.org/public/resources/ediag/index.htm

Harvey Wohlwend, International SEMATECH
harvey.wohlwend@sematech.org, 512.356.7536

December 5, 2000

e-Diagnostics Overview

- Remote monitoring & diagnostics allow supplier experts to rapidly fix factory equipment issues from their sites
- Suppliers need accurate historical performance data from factory equipment to rapidly drive continuous improvement



How do the Teams fit?

Define the scope of e-Diagnostics.

Describe data collection requirements, types of data, properties, and system architecture and data security sensitivity.

Size the network bandwidth requirements.

Define the data set transmitted to or viewed by a supplier under what security given the sensitivity of the data and the urgency of the problem.

Create guidelines, share best practices, drive commercialization of open architecture, Internet based access for suppliers to monitor equipment, provide improved uptime, optimize PMs, and reduce MTTR.

Capability Taxonomy

Data Taxonomy

Network Bandwidth

e-Diagnostics Guidelines

Data Security

Single Wire Interface

Protocol Definition

Define requirements for physical and logical e-Diagnostics connection to the tool, particularly related to existing tool control systems.

Define the protocol requirements for moving data among the tool, fab storage, supplier, and active and passive remote operations.

e-Diagnostics Working Groups

Network Bandwidth Requirements

Leader: Harvey Wohlwend - ISMT

Members: KLA-Tencor, AMAT, Intel

Capability Taxonomy

Leaders: Gary Viviani - Varian and Dave Bloss - Intel)

Members: IBM, AMAT, Nikon, TEL, TI, Schlumberger, Teradyne, Avantcom

Data Taxonomy

Leaders: Ed Kaz - AMAT, Nick Nikolic - KLA-Tencor

Members: IBM, Nikon, TEL, Axcelis, TI

Single Wire Resolution

Leader: Dave Bloss - Intel

Members: IBM, KLA-Tencor, AMAT

Protocol Definition

Leaders: Roger Eastvold - KLA-Tencor and James Martin - Intel

Members: Axcelis, Nikon, IBM, Teradyne, SVGL, Schlumberger, Lam, Avantcom, domain Logix, Infineon

Data Security

Leaders: Piero Fioravanti - Intel and TBD - IBM

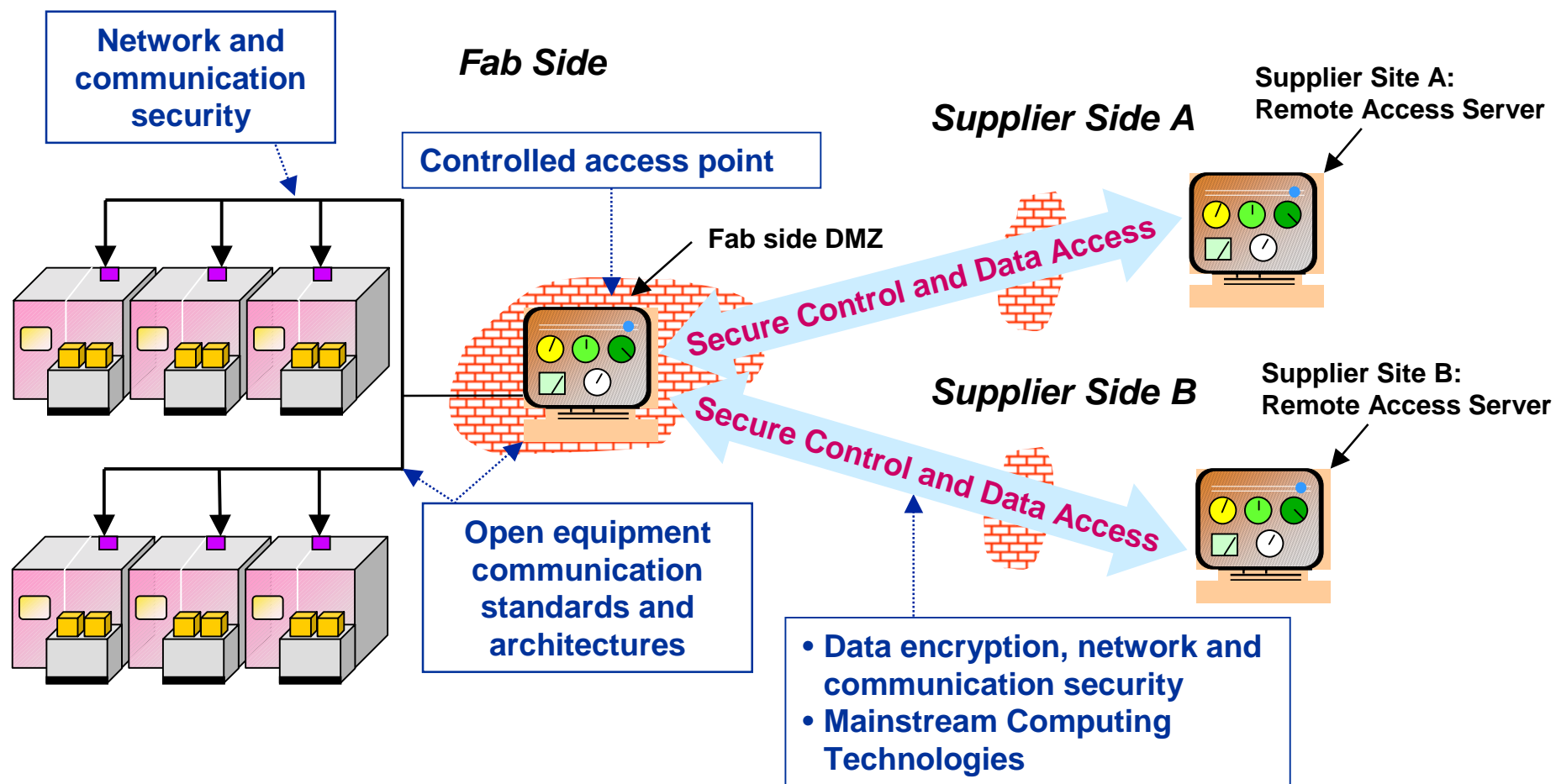
Members: KLA-Tencor, AMAT, Teradyne, Schlumberger, domain Logix

Other Participating Companies

ISMT Member Companies +

Advanced Energy, Adventa, ASML, ASYST Technologies, BOC Edwards, Brooks Automation, Canon, CYMER, DNS, Electroglas, GE, Hitachi, Honeywell, IPC, Kokusai, K&S, Murata, Novellus, PRI, SEMY, SISA, Symphony Systems, Triant

ISMT e-Diagnostic Guidelines



Full guideline document available at:
<http://www.sematech.org/public/resources/ediag/index.htm>

ISMT e-Diagnostic Capability Definitions

Level 3 - Prediction:

___ Predictive Maintenance, Self
Diagnostics, Automated Notification

Level 2 - Analysis:

Automated Reporting and
Advanced Analysis with SPC capability

Level 1 - Collection and Control:

Remote Tool Operation, Remote
Performance Monitoring, Remote Equipment

Level 0 - Access and Remote Collaboration:

Remote connectivity to the tool and remote
collaboration capabilities (text, audio, video)

Full capability definition document available at:

<http://www.semtech.org/public/resources/ediag/index.htm>

e-Diagnostics Security Guidelines V1.1

Purpose/Scope:

Define Information Technology security guidelines to support e-Diagnostics as defined in the International SEMATECH e-Diagnostics Guidelines. All guidelines apply to individual factory tools as well as any intermediate storage or concentration areas. Intellectual property protections, such as recipe content are addressed by the e-Diagnostics team and are beyond the scope of this document.

- System, including security, must be based on non-proprietary networking and computer architecture.
- System must meet or exceed standard Information Technology security practices, as defined in BS 7799 (Draft ISO 17799.)
- Communication must take place over standard communication connections using TCP/IP protocols. Legacy serial connections may be used for low bandwidth tools.
- All remote access must be from only known identifiable sources using techniques such as PKI digital certificates validated by an agreed certificate authority, handheld authenticators, or biometric techniques.

e-Diagnostics Security Guidelines V1.1 (cont.)

- Data transmission and external storage must have the capability to be encrypted using standard publicly available secure methods in compliance with export control restrictions. All Internet and Extranet based remote access and storage must be secure and encrypted. Intranet based remote access and storage is at customer discretion.
- Audit trails, including who, what, and when must be maintained for all data transfers and any remotely initiated changes.
- System must support detailed access control at the data item level for read, write, and remote control functions.
- System must function as part of a single network connection to the tool. It must also be capable of being supported on a separate dedicated network if desired. Security requirements apply to multiple networks if used.
- Data transmission volumes and requirements must be clearly defined for normal and maximum levels.
- Firewall configuration impact must be minimal and clearly defined.

e-Diagnostics Summary

- **e-Diagnostics Guidelines and Security Guidelines are complete, they are the defacto standard**
- **Moving into prototyping, proof of e-Diagnostics concepts**
- **Suppliers and IC makers developing roadmap for standards and implementations, compliance assessments**
- **e-Diagnostics is a successful International SEMATECH member company and supplier collaboration, now expanding globally**

For further information please contact:
Harvey.Wohlwend@sematech.org