

e-Diagnostics Working Group Meeting

Breakout Group Results

September 20, 2000

Single Wire Resolution

Team Objective

Define a guideline for the number of logical and physical connections between a production tool and the factory network

Team Membership

Single Wire Resolution	Dave Bloss (Intel)	Reza Bonabi (KLA-T) Dave Busing (KLA-T) Jim Chalmers (KLA-T) Ray Bunkofske (IBM) Bob Wiggins (IBM) Juan Bocanegra (AMAT) Shay Assaf (AMAT) Margaret Pratt (ISMT) Neil Frank (AMAT) Frank Kaplan (AMAT)
------------------------	--------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Any Other Members??

Single Wire Process

- **Single wire definition process**
 - Review network bandwidth study results - **DONE**
 - Review data taxonomy results - **DONE**
 - Review capability taxonomy results - **DONE**
 - Review security guidelines - **DONE**
 - analyze options - **IN PROGRESS**
 - recommend guideline - **IN PROGRESS**

Single Wire Guideline

- **e-Diagnostic connection and traditional SECS/GEM connection must be logically separated**
- **Equipment must support single or dual network connections**
 - allows for cost savings if low e-Diagnostic capabilities are required/desired.
 - allows legacy tools to be retrofit with auxiliary CPU's to enable e-diagnostics
- **Arbitration of control must exist on the tool to deal with control requests from e-Diagnostics and the SECS/GEM connection**
 - ensure safety, contention and deadlock issues are handled
 - impact on production throughput of e-Diagnostic requests must be predictable and configurable
 - configuration must exist for the types of control the e-Diagnostics connection can have on the tool

Single Wire Guideline Graphic

O.K.

Tool



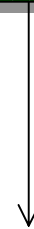
SECS/GEM



e-Diagnostics
Protocol

O.K.

Tool



SECS/GEM &
e-Diagnostics Protocol

Single Wire Considerations

- All e-diagnostics communications (request and reply) go through e-diagnostics port - OK
- Only e-diagnostics messages are accepted on the e-diagnostics port - OK
- The tool must be smart enough to ensure proper wafer processing, no compromises are allowed because of other requests including e-diagnostics - OK
- Temporary Impacts to throughput due to e-Diagnostics may be desired and acceptable (configurable) - OK
- Requests which would push the bandwidth (CPU or network) over the limit are rejected (return code -1 or some such) to avoid problems. - OK
 - **would be dealt with at the application level. [it could also be dealt with at the tool if the tool is smart enough RJB]**
 - **needs to be configurable, temporary impacts are sometimes acceptable**

Single Wire Considerations

- All e-diagnostics functions to be configured by the customer - OK
- Customer performs all authorizations - OK
 - **some authorization will be required locally at the tool.**
- Need a way of coding in business practices (I.e. no log file transfer during recipe download or vice-versa) - OK
 - **Some sort of e-diagnostics state model**

Implementation Notes

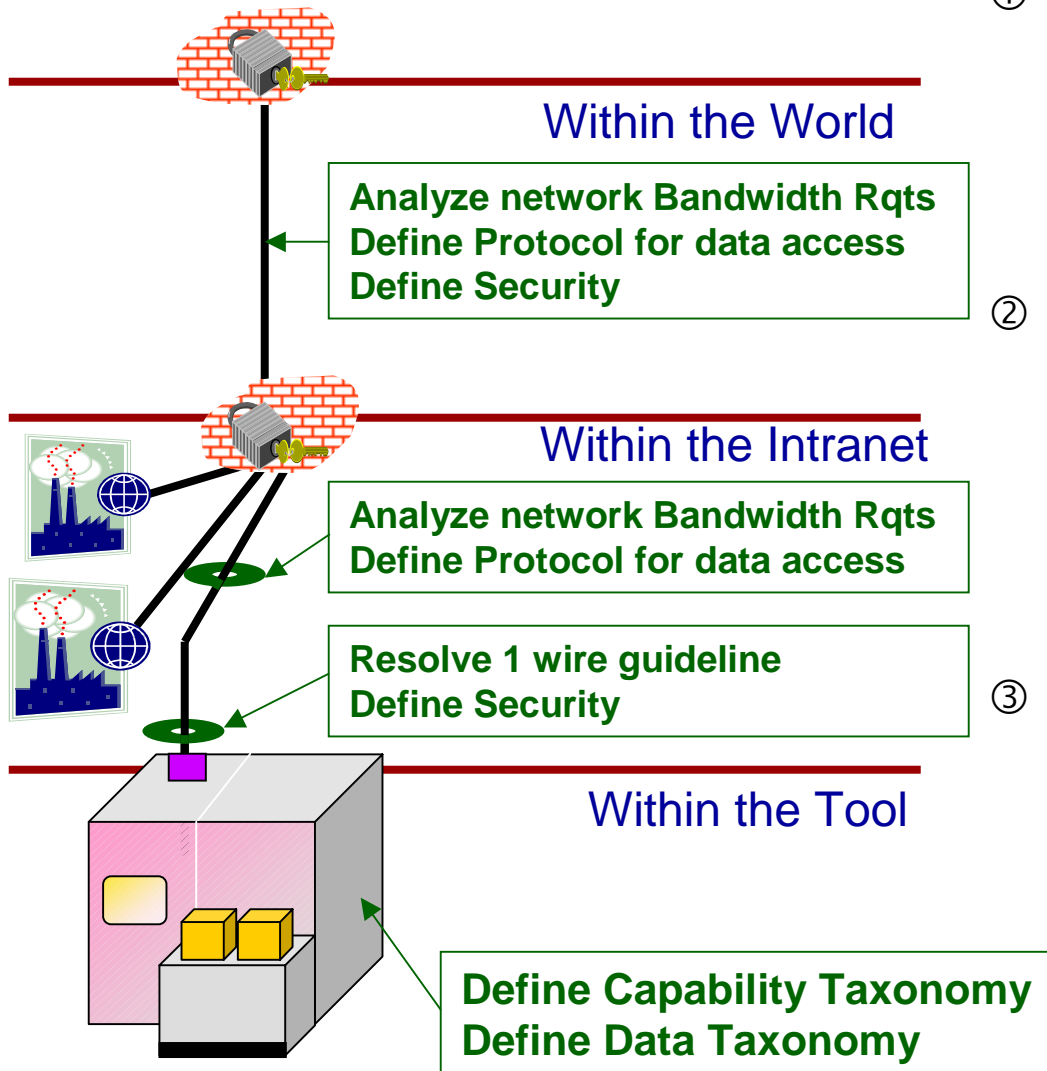
- Possibly implement a "gateway" application to prevent overloading the tool [or network].
 - **This would require checking with other software components of the fab to know how close to the edge the various components are.**

Single Wire Next Steps

- **Gather input from the WG** **TODAY**
- **Publish results to the sub-team** **9/21**
- **Complete discussions and wrap guideline in a document** **10/4**
- **Discuss guideline with Japanese** **10/5**

Reference

e-Diagnostics Capability Definition



① Reduce MTTR

- Basic remote access to tool data
- Equipment experts can review and analyze 'raw data' from anywhere in the world

② Proactive Monitoring

- Monitor leading indicators / summary data
- Some external system or people analyze the data and predict future tool behavior

③ Predictive / Preventative Maintenance

- Automatic identification of pending failures by the process tool
- Automatic action of tool to fix the issue
 - e.g. order spare part, call service representative, etc.

Alternative Architectures

Definitions

- **Remote control: (1) remote ability in e-diagnostics to ask tool to perform any action that affects the state of the hardware (2) tool configuration; (3) download software program**
- **Relationship to “remote access”**
- **Change to “remote operation” to avoid confusion with SECS/GEM term**
- **Application - ??**
- **“real time” -**

e-Diagnostics Server

- one per tool? per supplier? per fab?
- where does data reduction occur?
- where does data summarization occur? per tool, tool type, per supplier, across supplier
- one portal (URL) into fab?
- remote operations communications may be “proprietary” to supplier? data security concerns? may need arbitration
- who provides this “server”? potential conflict of interest, liability

e-Diagnostics Server

- **could be just something that sends and receives data between fab and supplier**
- **integration with outside-the-tool data**
 - APC, MES, metrology,
- **consensus on two logical connections**
- **what about sharing data between 2 tools?**

Tool Administrator

- **hang logically an administrator on tool or hang it on n tools - looks like part of the tool to the factory**
- **does not replace “e-diag server”, is part of the tool, not part of e-diagnostics architecture**

More issues

- **e-Diagnostics process requires data from outside the tool**
- **include supplier e-Diagnostics apps inside the fab**
- **someone outside both fab and supplier sites that needs access to data - network and data security issue - need to login either to supplier site or user site. VPN vs Web.**
- **local vs remote access control**

“Clearing House”

- provides simplicity of implementation
- security and clearing house function
- filters still have to be in fab
- why store data there?
- different certification methods supported
- communications gateway
- requirement for single security gate
- extra cost to supplier?
- should be invisible to e-Diagnostics functions - is it?

EFEM data and Transport data

- **who is responsible for getting EFEM data to EFEM supplier? does EFEM supplier have to “parse it out of someone else’s data”, which brings up security data**
 - for 300mm OEM is responsible
 - for 200mm may be “direct” (via fab)
- **OEM is responsible for integrated subsystems - 3rd party may be needed to help diagnose**
- **transport diagnostics may be specific to a tool, may involve material info**

Options

- **outsource e-Diagnostics server**
- **put apps on tool or outside**
- **clearing house is optional**

Action Items

Scenario team should draw up 3-4 architectural scenarios / use cases and fit it against other working groups.

Protocol Definition

e-Diagnostic Data Production

Agreed to move forward on the assumption that e-Diagnostic data collection is not to be produced for mission-critical manufacturing consumption

Remote Operation

- **Distinguish between tool computer access for the purpose of running programs, etc. which do not directly affect tool behavior AND tool control (loading/executing recipes, etc.)**
- **What protocol considerations are there for the two scenarios above? Suppliers would like to be able to have this sort of access potentially without fab personnel present (fab has already locked down what is accessible in this manner)**
- **New use case identified**

Data Security

Data Security Team

Leader: Piero Fioravanti Intel

Claude Baudoin	Schlumberger	Olivier Louveau	STM
Tim Johnson	GE	Gerry McMahon	Teradyne
Richard Beaver	Adventa Control	Neil Frank	AMAT
Carl Fiorletta	Adventa Control	Kirby Hess	AMAT
Arthur Luk	Canon	Michael Borman	AMD
Glen Ingebrigtsen	HP	Reza Bonabi	KLA-Tencor
Michael Sigman	ISMT	Roger Eastvold	KLA-Tencor
Michael Locy	KLA-Tencor	Peter Gaboury	STM
Sean Mcnamera	Nikon	Juan Bocanegra	AMAT
Scott Smith	Nikon		

Charter

Given what data will be available to be shared, determine how to adequately and realistically protect the data and associated intellectual property exchanged as a result of e-diagnostics, while enabling the gains of e-diagnostics for both suppliers and manufacturers.

In Scope

- Classification of Data Security
- Classification of authorization levels and escalation procedures for higher-level access
- Security associated with granting activities i.e., remote control, s/w update...
- Data disposal

Out of Scope

- Data transmission and other items covered by IT Security Guidelines
- Data retention times
- Data definition
- Method and location of access (IT Security)

Deliverables

- Classification matrices (push out for feedback)
- Cost of loss (risk assessment)
- Examples
- Authorization Levels
- Disposal
- Time to authorize
- Duration of authorization
- Encryption level
- Use (repair, development, engineering, etc)
- Definitions and assumptions
- Definitions of events and associated security levels
- Statement of expectations
- POR (timeline including other subgroups Phased approach in the fab, in the world)

Next Steps

- Validation
- Set up a weekly meeting
- Proceed with deliverables (developed by this group)
- Submit to the rest of the group
- Identify the audience for an RFI on the matrices
- Distribute and disposition the responses