
e-Diagnostics Measurement & Assessment

Chris Stambaugh - Schlumberger

stambaugh@san-jose.tt.slb.com, 408. 586.4902

July 20, 2001

INTERNATIONAL
SEMATECH

07/16/2001 3:18 PM j:\stndpres\template\IntST.ppt - 1

Measurement & Assessment Team Goals

- **Define the process and mechanisms by which IC Makers and Vendors can assess guideline compliance of e-Diagnostics solutions**
- **Keep the compliance metrics or scorecards as succinct and straight forward as practical**

Team Participation

- **Measurement & Assessment Team included representatives from:**
 - SEMATECH
 - Schlumberger
 - KLA (Brooks Automation)
 - Applied Materials
 - AMD
 - Agilent
- **Also inputs from:**
 - Teradyne
 - Intel
 - DomainLogix
 - AgileTCP

M&A Sub-team Initial Work & Results

- **Expected Results**

- Assessment metrics will be based on previous work
 - e-Diagnostics Capability definitions & Use Case scenarios
- Pass/Fail scorecards to assess tangible parts of e-Diagnostics solutions with conformance requirements
 - Factory Tool and e-Diagnostics Server(s)
 - Security aspects of solutions
- Provide specific guidance to IC Maker/Vendor pairs as they plan for and implement specific solutions
 - IC Maker and Supplier Readiness Scorecards
- Start with Level 0 and work your way up!

M&A Sub-team Initial Work & Results

- **Results:**

- Main focus to date has been on Level 0
- Level 0 Tool-Server draft checklist complete
- IC Maker and Supplier Readiness draft complete
 - Identified individual and “shared ownership” areas
- Initial Security checklist based on e-Diagnostics Security Architecture Guidelines
- Decision on audit method
 - Self-audit with the expectation that a complete evaluation of a specific implementation of an e-Diagnostics solution (i.e., for an IC Maker/Supplier pair), will require a fresh review of each companies audit results

M&A Sub-team Initial Work & Results

• Level 0 Tool-Server checklist

**Subset of
Tool-Server
Scorecard**

e-Diagnostics Compliance Scorecard Tool-Server Feature Layer--Level 0

RED = Mandatory
YELLOW = Optional
TS = Factory Tool and e-Diagnostics Server

		Feature	Tool	Server	Description of Feature
Collaboration	TS-CO0.4	Real-time application sharing	YELLOW	YELLOW	Ability to share applications within the collaboration session. Does not include remote tool control applications covered in Capability Level 1.
	TS-CO0.3	Chat Capability	RED	RED	Text Chat sessions among all participants
	TS-CO0.2	Real-time shared file viewing, including still images.	RED	RED	All participants can view files simultaneously (still images generated on-tool can be viewed by all participants).
	TS-CO0.1	T120 based	RED	RED	Collaboration software must be implemented using the standard T.120 conferencing protocol suite
File Transfer	TS-FT0.2	Two step file transfer (Fully auditable)	RED	RED	File transfer is done in two steps, tool-server-user. There is no direct access to the tool. Every transfer is recorded. What was transferred and who did it.
	TS-FT0.1	Dynamically authorize files for transfer	RED	RED	The ability to request and grant permission to transfer files not on the pre authorized list
Admin	TS-AD0.2	Capability discrimination by user	RED	RED	The ability to grant users with different capabilities or privileges based on roles. Implies the necessary ability to set up, modify and delete, user and group accounts or privileges.
	TS-AD0.1	Complete Audit Trail of user history within e-Diagnostics environment	RED	RED	A record of users logging in/out of the e-Diagnostics environment as well as actions performed.
Security	TS-SE0.3	Adheres to advanced connectivity and security compliance checklist	YELLOW	YELLOW	If there is an advanced or recommended section of the security checklist then compliance would be recorded here
	TS-SE0.2	Adheres to minimum connectivity and security compliance checklist	RED	RED	Complies with the mandatory sections of the checklist from the security team
	TS-SE0.1	External access to e-Diagnostics system through central aggregation point	RED	RED	Connectivity to tools from outside the IC maker's firewall is through a central aggregation point.

M&A Sub-team Initial Work & Results

- Level 0 Tool-Server checklist

e-Diagnostics Compliance Scorecard			
Tool-Server Feature Layer--Level 0			
<p>RED= Mandatory</p> <p>YELLOW= Optional</p> <p>TS= Factory Tool and e-Diagnostics Server</p>			
Feature	Tool	Server	Description of Feature

Admin Section

TS-AD0.2	Capability discrimination by user			The ability to grant users with different capabilities or privileges based on roles. Implies the necessary ability to set up, modify and delete, user and group accounts or privileges.
TS-AD0.1	Complete Audit Trail of user history within e-Diagnostics environment			A record of users logging in/out of the e-Diagnostics environment as well as actions performed.

M&A Sub-team Initial Work & Results

- **IC Maker and Supplier Readiness Scorecards**

- For each specific e-Diagnostics implementation, the Supplier and IC Maker should reassess their state of compliance
- Categories for Readiness scorecards include:
 - Support Policies
 - Network Admin
 - Training
 - Safety Procedures
 - System Admin Procedures
 - IT Infrastructure
- Scorecard items either Mandatory or Optional, and they have either Supplier, IC Maker, or shared ownership

E-Diagnostics Compliance Scorecard			
IC Maker Readiness Feature Layer (rev 0.7)			
RED	= Mandatory		
YELLOW	= Optional		
Sand	= Shared IC Maker/Supplier Responsibility		
	SHR = Readiness feature that has "shared" responsibility		
	ICR = Readiness feature that has IC Maker responsibility		
		IC Mfg Readiness	Feature Description
Feature			

M&A Sub-team Initial Work & Results

- IC Maker and Supplier Readiness Scorecards

E-Diagnostics Compliance Scorecard				
IC Maker Readiness Feature Layer (rev 0.7)				
	RED	= Mandatory		
	YELLOW	= Optional		
	Sand	= Shared IC Maker/Supplier Responsibility		
	SHR	= Readiness feature that has "shared" responsibility		
	ICR	= Readiness feature that has IC Maker responsibility		
		Feature	IC Mfg Readiness	Feature Description
Support Policies	SHR-SU.7	Defined e-diagnostics system support availability (e.g. When will the system have engineering support staff)	YELLOW	
	SHR-SU.6	Defined e-Diagnostics Server and related hardware	YELLOW	
	ICR-SU.5	Defined User Authentication procedures	RED	
	SHR-SU.4	Defined Encryption requirements and Methodology for data files, software, voice, video transmission	RED	
	SHR-SU.3	Defined data that will be allowed in-out the Factory (file	RED	
	SHR-SU.2	Defined protocols/ports (inbound/outbound) for access	RED	
	SHR-SU.1	Defined mechanism to ensure supplier specific data (IP) is protected from unauthorized access	RED	
Safety Procedures	SHR-SA.3	inherent tool safety mechanisms	RED	
	SHR-SA.2	Defined safety procedures in place (to prevent tool in e-diagnostics session from being put into service)	RED	Procedures for entry and exit from an E-Diagnostics session must be clearly defined
	SHR-SA.1	interference with E-Diagnostics session/remote control safety training generated from the IC makers side	RED	
System Administration Procedures	ICR-SY.4	Configure a new tool to be accessed via e-Diagnostics	RED	
	ICR-SY.3	Add new suppliers users to authentication mechanism	RED	
	ICR-SY.2	Configure user entitlements (e.g. pre-authorization for passive requests including file transfer, remote session, telnet, etc.)	RED	
	SHR-SY.1	Routine scheduled maintenance procedures	RED	

Subset of IC Maker Readiness Scorecard

M&A Sub-team Initial Work & Results

- IC Maker and Supplier Readiness Scorecards

Examples

Safety

SHR-SA.3	E-Diagnostics system cannot circumvent or alter the inherent tool safety mechanisms	
SHR-SA.2	Defined safety procedures in place (to prevent tool in e-diagnostics session from being put into service)	

Training

SUR-TR.2	Define support procedures (who will respond to an e-diagnostics session request, escalation procedure) generated from the Supplier side	
SHR-TR.1	Data/confidential information handling procedures generated from the Supplier side	

M&A Sub-team Initial Work & Results

- **Security Scorecard categories include:**

- Business Layer
- Logical Layer
- Hardware Connectivity Layer
- e-Diagnostics Environment

Subset of Security Scorecard

e-Diagnostics Compliance Scorecard

Security Checklist (rev 0.7)

RED = Mandatory
YELLOW = Optional

		Feature		Description of Feature
Business Layer	SEC-BUS.3	Security Responsibility	RED	IC Maker and Supplier have determined and documented security responsibilities and policies, that clearly identify the physical resources and controls required by the e-Diagnostics system. This includes tasks such as remote support, collaborative engineering, installation, qualification and administration of the e-Diagnostics system.
	SEC-LOG.2	The e-Diagnostics system itself is intentionally protected	RED	Security controls are utilized to protect against unauthorized access, modification, substitution, delay, insertion or deletion to data, cryptographic keys, applications and systems.
Logical Layer	SEC-LOG.1	e-Diagnostics system is restricted to authorized personal	RED	Only those IC Maker and Vendor individuals who are properly authenticated and authorized to function within the e-Diagnostics environment (as per the e-Diagnostics Capability and Use Case sections of the Guidebook) will have access to the e-Diagnostics environment
	SEC-HW.2	Isolated e-Diagnostics network	RED	Vendors and IC Makers must provide physical and logical protection (such as Firewall technology) to ensure that the part of the e-Diagnostics environment within their control, is separate and isolated from the rest of their company networks and resources.
Hardware Connectivity Layer				

What's Next

- **Aug '01 Finalize Level 0**
- **Oct '01 Define Level 1 Tool-Server Scorecard**
 - Make modifications to Readiness and Security Scorecards as appropriate
- **Q4 '01 Initial drafts for Level 2 and Level 3**