



**International SEMATECH
e-Diagnostics Guidebook**

(Working Document, version 0.7)

Table of Contents

1	INTRODUCTION.....	6
1.1	SCOPE AND LIMITATIONS	6
1.2	DOCUMENT OVERVIEW	6
1.3	DEFINITIONS.....	6
2	E-DIAGNOSTICS GUIDELINES V1.0.....	7
2.1	PURPOSE/SCOPE:	7
2.2	E-DIAGNOSTICS DEFINITION:	7
2.3	SAFETY AND SECURITY:	8
2.4	ARCHITECTURE:	8
2.5	COLLABORATION:	8
3	E-DIAGNOSTICS SECURITY GUIDELINES V1.1	8
3.1	PURPOSE AND SCOPE.....	8
3.2	SECURITY GUIDELINES.....	9
4	CAPABILITY TAXONOMY.....	9
4.1	GENERAL CAPABILITY REQUIREMENTS.....	9
4.2	LEVEL 0 – ACCESS AND REMOTE COLLABORATION: REMOTE CONNECTIVITY TO THE TOOL AND REMOTE COLLABORATION CAPABILITIES.....	10
4.2.1	<i>Remote Connectivity</i>	10
4.2.2	<i>Remote Collaboration</i>	10
4.3	LEVEL 1 – COLLECTION AND CONTROL: REMOTE PERFORMANCE MONITORING AND TOOL OPERATION.....	11
4.3.1	<i>Remote Equipment Configuration</i>	11
4.3.2	<i>Remote Equipment Operation</i>	11
4.3.3	<i>Monitor Equipment Performance in Real Time</i>	12
4.3.4	<i>Data Storage</i>	12
4.3.5	<i>Data Collection</i>	12
4.4	LEVEL 2 - ANALYSIS: AUTOMATED REPORTING AND ADVANCED ANALYSIS WITH SPC CAPABILITY 13	
4.4.1	<i>Automated Data Reporting and Analysis</i>	13
4.4.2	<i>Data Compression</i>	13
4.5	LEVEL 3 - PREDICTION: PREDICTIVE MAINTENANCE, SELF DIAGNOSTICS, AND AUTOMATED NOTIFICATION.....	14
4.5.1	<i>Predictive/Proactive Equipment Self-diagnosis</i>	14
4.5.2	<i>Decision Logic</i>	14
4.5.3	<i>Notification</i>	14
5	DATA TAXONOMY	15
5.1	GENERAL DATA REQUIREMENTS.....	15
5.1.1	<i>Preserving Tool Performance</i>	15
5.1.2	<i>General Architectural Considerations for Tool Data</i>	15
5.1.3	<i>General Data Formats</i>	15
5.1.4	<i>Auxiliary Tool Data</i>	16
5.1.5	<i>MES Data</i>	16
5.1.6	<i>Data Accuracy and Precision</i>	16
5.1.7	<i>Data and Tracking Capability Classifications</i>	16
5.1.7.1	Data Persistence Classes.....	16
5.1.7.2	Parametric Tracking Capability.....	17
5.2	EVENT DATA	17
5.2.1	<i>Non-Exception Events</i>	18
5.2.2	<i>Exception Events</i>	18

5.2.3	<i>Closed-loop Positive Performance</i>	18
5.3	RECIPE PERFORMANCE DATA.....	19
5.3.1	<i>Performance for Metrology and Inspection Equipment</i>	19
5.3.2	<i>Recipe Performance for Process Equipment</i>	19
5.4	TOOL HEALTH MONITORING DATA.....	19
5.4.1	<i>Diagnostics Types</i>	20
5.4.2	<i>Diagnostics Results Types</i>	20
5.4.3	<i>Wafer or Reticle-based Diagnostics</i>	20
5.4.4	<i>Other Tool Health Data</i>	20
5.4.5	<i>Diagnostics Periodicity</i>	21
5.5	OPERATIONAL PERFORMANCE DATA.....	21
5.5.1	<i>Operational Performance Metrics</i>	21
5.6	SYSTEM BASELINE DATA.....	22
5.6.1	<i>Software</i>	22
5.6.2	<i>Equipment constants</i>	22
5.6.3	<i>Recipe Revision Control</i>	22
5.6.4	<i>Static test and sensor results (BKM Results)</i>	22
5.6.5	<i>Benchmark Data</i>	22
5.6.6	<i>Design Specifications</i>	23
5.7	TOOL USAGE DATA.....	23
5.7.1	<i>Tool Usage Data Categories</i>	23
6	DATA SECURITY	24
6.1	DATA SECURITY ASSUMPTIONS.....	24
6.2	DATA CLASSIFICATION.....	24
6.3	CLASSIFICATION MATRICES.....	25
7	PROTOCOL DEFINITION	26
7.1	SCOPE AND LIMITATIONS.....	26
7.2	CAPABILITY LEVEL 0.....	27
7.2.1	<i>Use Case: View/Download Equipment Files</i>	27
7.2.1.1	Transport Protocol Considerations.....	27
7.2.1.1.1	Assumptions & Constraints.....	27
7.2.1.1.2	Options.....	27
7.2.1.1.2.1	FTP.....	27
7.2.1.1.2.2	FTP over SSL.....	27
7.2.1.1.2.3	HTTP over SSL.....	27
7.2.1.1.2.4	Third Party Application Software.....	27
7.2.1.1.3	Pro/Con.....	27
7.2.1.1.3.1	FTP.....	28
7.2.1.1.3.2	FTP over SSL.....	28
7.2.1.1.3.3	HTTP over SSL.....	28
7.2.1.1.3.4	Third Party Application Software.....	28
7.2.1.1.4	Recommendation.....	28
7.2.1.1.5	Open Issues.....	28
7.2.2	<i>Use Case: Remote Collaboration</i>	28
7.2.2.1	Transport Protocol Considerations.....	29
7.2.2.1.1	Assumptions & Constraints.....	29
7.2.2.1.2	Options.....	30
7.2.2.1.3	Pro/Con.....	30
7.2.2.1.3.1	Third party software.....	30
7.2.2.1.3.2	Custom developed software.....	30
7.2.2.1.4	Recommendation.....	30
7.2.2.1.5	Open Issues.....	30
7.3	CAPABILITY LEVEL 1.....	30
7.3.1	<i>Use Cases: Monitor Remote Equipment Operation</i>	30
7.3.1.1	Transport Protocol Considerations.....	30
7.3.1.1.1	Assumptions & Constraints.....	30

7.3.1.1.2	Options	31
7.3.1.1.3	Pro/Con.....	31
7.3.1.1.4	Recommendation	31
7.3.1.1.5	Open Issues.....	31
7.3.2	<i>Use Case: Replicate Tool Data from Store to Supplier</i>	31
7.3.2.1	Transport Protocol Considerations	31
7.3.2.1.1	Assumptions & Constraints	31
7.3.2.1.2	Options	32
7.3.2.1.3	Pro/Con.....	32
7.3.2.1.3.1	DB Links	32
7.3.2.1.3.1.1	Cons.....	32
7.3.2.1.3.1.2	Pros.....	32
7.3.2.1.3.2	HTTP	32
7.3.2.1.3.2.1	Cons.....	32
7.3.2.1.3.2.2	Pros.....	32
7.3.2.1.3.3	CORBA/RMI	32
7.3.2.1.3.3.1	Cons.....	32
7.3.2.1.3.3.2	Pros.....	33
7.3.2.2	Recommendation.....	33
7.3.2.3	Open Issues	33
7.3.3	<i>Use Case: Report Equipment Data</i>	33
7.3.3.1	Transport Protocol Considerations	33
7.3.3.1.1	Assumptions & Constraints	33
7.3.3.1.2	Options	33
7.3.3.1.3	Pro/Con.....	33
7.3.3.1.3.1	HTTP	34
7.3.3.1.3.2	Middleware	34
7.3.3.1.3.3	MQSeries	34
7.3.3.1.3.4	Tibco	35
7.3.3.1.3.5	CORBA products	35
7.3.3.1.3.6	Java RMI, JMS.....	35
7.3.3.1.3.7	COM+	36
7.3.3.1.4	Recommendation.....	36
7.3.4	<i>Use Cases: View Remote Equipment Configuration, Change Remote Equipment Configuration</i>	37
7.3.4.1	Transport Protocol Considerations	37
7.3.4.1.1	Assumptions & Constraints	37
7.3.4.1.2	Options	38
7.3.4.1.3	Pro/Con.....	38
7.3.4.1.4	Recommendation	38
7.4	CAPABILITY LEVELS 2-3.....	38
8	NETWORK BANDWIDTH REQUIREMENTS	39
8.1	ASSUMPTIONS	39
8.2	DATA POINTS	40
8.3	SCENARIOS	40
8.3.1	<i>Worst Case Scenario</i>	40
8.3.2	<i>Connectivity Case Scenario</i>	40
8.3.3	<i>Typical Case Scenario</i>	41
8.4	SUMMARY	41
8.5	NETWORK ANALYSIS.....	42
8.5.1	<i>Data Throughput Analysis</i>	42
8.5.2	<i>Data Latency Analysis</i>	43
8.6	CONCLUSIONS	44
9	SINGLE WIRE GUIDELINE.....	45
9.1	SINGLE WIRE CONSIDERATIONS.....	45
9.2	CONCLUSION	45
9.3	SINGLE WIRE IMPLEMENTATION NOTES.....	46

A	APPENDIX A - USE CASES	47
9.4	CAPABILITY LEVEL 0 USE CASES.....	47
9.5	CAPABILITY LEVEL 1 USE CASES.....	55
9.6	CAPABILITY LEVEL 2 USE CASES.....	60
9.7	CAPABILITY LEVEL 3 USE CASES.....	62
B	APPENDIX B - NETWORK ANALYSIS FORMULAE AND COMPUTATION	64

1 Introduction

This document is intended to provide guidelines for the selection of communication and data representation technologies for the implementation of an e-Diagnostics system.

1.1 Scope and Limitations

The goal of this document is to define e-Diagnostics capabilities that will positively impact both the effectiveness of the support offering and ultimately improve Overall Equipment Efficiency of factory operations.

It is the intent that the e-Diagnostics vision not be constrained by current practical challenges or limitations, e.g., network bandwidth. The intent is that the capabilities suggested in this document be implemented with the best methods possible today and evolve as new capabilities become available..

Further, this document is not to supersede existing computer network LAN/WAN services. The purpose is to provide requirements that result in minimally essential loads on existing structures.

1.2 Document Overview

This document is organized around identified usage scenarios (Use Cases) for each capability level defined by the **e-Diagnostics Capability Taxonomy**. At the time of this writing, those capabilities are as follows:

- Level 0 – Access: Collaborative trouble shooting with basic remote connectivity
- Level 1 – Collection and Control: Remote performance monitoring and Tool Operation
- Level 2 – Analysis: Automated reporting and Advanced Analysis
- Level 3 – Prediction: Predictive maintenance, self-diagnostics, and automated notification
- Level 4 – Cross-Tool Correlation
 - Each capability level involves one or more Use Cases, and each Use Case may have implications for transport protocols or data representation. There is a section for each unique protocol consideration and the Use Cases which drive its requirements are listed in the section title.

1.3 Definitions

This section defines what specific terms and acronyms mean in this document.

AEC	Advanced Equipment Control
APC	Advanced Process Control
BKM	Best Known Method
CIP	Continuous Improvement Plan

Company	Entity that utilizes Supplier equipment
CORBA	Common Object Request Broker Architecture
TCP/IP	Transmission Control Protocol/Internet Protocol
DTD	Data Type Definition
EPT	Equipment Performance Tracking
FDC	Fault Detection Classification
FTP	File Transmission Protocol
HSMS	High Speed Messaging System
HTTP	Hyper Text Transfer Protocol
JMS	Java Messaging Service
JVM	Java Virtual Machine
MES	Manufacturing Execution System
MTBI	Mean Time Between Interrupt
MTOL	Mean Time Off Line
MTTA	Mean Time To Assist
MTTR	Mean Time To Repair
OEE	Overall Equipment Efficiency
RbR	Run-by-Run (same as RtR)
RMI	Remote Method Invocation
RtR	Run-to-Run (same as RbR)
SSL	Secure Sockets Layer
Supplier	Equipment provider, or its agent, to Company
SPC	Statistical Process Control
VoIP	Voice over IP

2 e-Diagnostics Guidelines V1.0

These high level requirements provide guidance for e-Diagnostics implementations. They are the first deliverable from the e-Diagnostics user community.

2.1 Purpose/Scope:

The fundamental purpose of e-Diagnostics is to increase the availability of production and facilities equipment, reduce mean time to repair, and provide significant reduction in field service resources/costs. This capability must be available for 200mm and 300mm fab equipment, Probe/Assembly/Test equipment, and key Facilities equipment.

2.2 e-Diagnostics definition:

Capability to enable an authorized equipment supplier's field service person to access any key production or facilities equipment from outside the IC maker's facility/factory via network or modem connection. Access includes ability to remotely monitor, diagnose problems or faults, and configure/control the equipment in order to bring it into full productive state rapidly, within security, safety, and configuration management guidelines.

The **e-Diagnostics solution** consists of equipment and auxiliary hardware and software applications.

2.3 Safety and Security:

- Safety is imperative. Potential solutions must address worker, product, and equipment safety. An operational interlock is required to ensure safety.
- Data security is paramount. Potential solutions must address network, communications, data encryption, and other relevant issues. Only authorized personnel may be able to access the view-based, relevant data to perform diagnosis.
- Remote data and control access must be selectively provided. Therefore, the e-Diagnostics system must have built-in capability that determines when to allow specific remote functions to be executed based on specific states or condition of the equipment.

2.4 Architecture:

- The solutions must support remote accessibility of equipment diagnostic data from outside the IC maker's firewalls. Two-way communications between these two locations is needed to support interactive problem solving.
- The solutions must permit sharing of key diagnostics and monitoring data between multiple factory and supplier sites on an as-needed basis to enable remote detection of issues and proactive trouble-shooting.
- The solutions must enable predictive maintenance, including notification when equipment will need service or repair.
- e-Diagnostics solutions must be implemented using an open architecture based on mainstream computer technologies, non-proprietary standards, and data models.

2.5 Collaboration:

- The solutions must provide the same equipment monitoring/diagnostics data at the local and remote sites. Identical representations and user interfaces at both sites are highly desired.
- The solutions must enable run-time data collection, storage, and retrieval. The e-Diagnostics system must enable analysis of this data and decision support capability.
- The solutions must allow audio-visual collaboration such as video teleconferencing or video over Internet Protocol to enable remote experts to view/diagnose equipment and sub-assembly problems in real-time and to communicate with factory personnel.

3 e-Diagnostics Security Guidelines V1.1

Security is paramount to the success of e-Diagnostics. These Security Guidelines were defined in collaboration with the International SEMATECH Semiconductor Manufacturers Information Technology Security Council. This council is made up of security officers from the various member companies..

3.1 Purpose and 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.

3.2 Security Guidelines

1. System, including security, must be based on non-proprietary networking and computer architecture.
2. System must meet or exceed standard Information Technology security practices, as defined in BS 7799 (Draft ISO 17799.)
3. Communication must take place over standard communication connections using TCP/IP protocols. Legacy serial connections may be used for low bandwidth tools.
4. 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.
5. 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.
6. Audit trails, including who, what, and when must be maintained for all data transfers and any remotely initiated changes.
7. System must support detailed access control at the data item level for read, write, and remote control functions.
8. 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.
9. Data transmission volumes and requirements must be clearly defined for normal and maximum levels.
10. Firewall configuration impact must be minimal and clearly defined.

4 Capability Taxonomy

4.1 General Capability Requirements

Capabilities are described by 5 levels (0-4). Each level is intended to build on the previous level, each bringing increased capability. Equipment that is defined by a Supplier to be "Level 3 Capable" necessarily has Level 0-2 capabilities as well.

The level numbers increase according to a blend of many factors: the sequence of support tasks that might be performed; the ease of implementing the necessary Fab infrastructure and tool designs required to execute the diagnostic and repair tasks; and, decreasing human assistance and increasing automation expected with each level.

e-Diagnostics Capabilities Summary

Level 0 – Access and Remote Collaboration: Remote Connectivity to the tool and Remote Collaboration capabilities.	Level 3 - Prediction: Predictive Maintenance, Self Diagnostics, and Automated Notification.
Level 1 – Collection and Control: Remote Tool Operation, Remote Performance Monitoring, Data Collection and Storage.	Level 4 - To be determined?
Level 2 – Analysis: Automated Reporting and Advanced Analysis with SPC Capability	

4.2 Level 0 – Access and Remote Collaboration: Remote connectivity to the tool and remote collaboration capabilities.

This level requires two fundamental capabilities:

1. Remote connectivity to the tool within the IC Company's environment. This requires all of the connectivity and security challenges be satisfied.
2. Practical tools implemented in a way which allows effective remote collaboration sessions between the tool in the Company environment and remote experts.

Key Ideas:

- Remote Connectivity
 - Fab Network/Topology/Requirements
 - LAN/WAN Management
 - Access Controls Remote Collaboration

4.2.1 Remote Connectivity

Connectivity to the tools from outside the IC Company's firewall shall be through a central aggregation point to allow for security administration, compatibility with Fab network topology/security requirements, and scalability.

Company Personnel security measures must be established and in place to prevent Company Employees from transmitting confidential information to Suppliers.

The e-Diagnostics system shall provide active management of concurrent tool connections, LAN utilization, and WAN (remote connection) bandwidth.

Access to data shall be limited to customer-approved data on a per user basis. Remote access shall be limited to approved functions, applications, and/or protocols on a per user basis.

4.2.2 Remote Collaboration

The e-Diagnostics system shall be capable of real-time 2-way document/text, image sharing between remote locations. Video and VoIP might be included, pending network bandwidth. Standard tools such as telephone-based voice contact, electronic file sharing, and ethernet-based videoconference and collaboration systems may be used.

BENEFITS: Reduce support cost, Reduce MTTR, Predictive maintenance, CIP data collection

STANDARDS: Action required for ISMT to specify security standards required for real-time collaboration data access through Company and Supplier corporate firewalls.

Action required for ISMT to adopt standard protocols for data collaboration.

4.3 Level 1 – Collection and Control: Remote performance monitoring and Tool Operation.

Key Ideas:

- Remote Equipment Configuration
- Remote Operation of Equipment
- Remote Performance Monitoring in Real Time
- Data Storage
- Data Collection

4.3.1 Remote Equipment Configuration

This capability includes the ability to remotely logon to a tool or tool environment to analyze and, if authorized, to modify software aspects of the tool. The remote support must be able to manually setup, update, or upgrade tool-specific software or software that is common to a group of tools from a single Supplier. This capability must include tracking any permanent changes made via the remote connection.

BENEFITS: Reduce Support Costs, Reduce MTTR, Preventative Maintenance

STANDARDS: No new standards.
Should adhere to file transfer and connectivity/security standards agreed to by the overall e-Diagnostics forum.

4.3.2 Remote Equipment Operation

Level 1 of e-Diagnostics requires that a person be able to operate the tool remotely in order to diagnose specific tool health issues. This functionality includes the ability to remotely view and actuate user interface functions as if standing at the tool. This includes the ability to remotely access, load, download, execute, and analyze results from tool diagnostics, calibrations, recipe, and user programs. Note: It does not, by default, grant the authority to download recipes themselves.

Access authorization shall be granted by appropriate and responsible personnel at the tool for each remote connection. The Company will decide and control who has this authorization capability. The tool must be locked in an Off-line state during remote operation, precluding the ability to attempt Host-control.

The remote operation capability must not be able to bypass any of the safety protections inherent in the tool or its operation.

BENEFITS: Reduce Support Costs, Reduce MTTR, Prevent Future Problems
STANDARDS: Potentially a new standard around remote operation and safety.

4.3.3 Monitor Equipment Performance in Real Time

The tool shall support real-time equipment availability tracking (SEMI EPT Standard).

- Tool shall make data, as defined in Data Taxonomy Guidelines, available to a data server and Host in some type of "event messages" form to support above metrics
- Tool shall use uniform standard formats as defined by the e-Diagnostic's protocol definition sub-team.

BENEFITS: Reduce Support Costs, Reduce MTTR
STANDARDS: Use uniform standard formats (like XML) and standard transport protocols (like MSMQ, HTTP).

4.3.4 Data Storage

Equipment e-Diagnostics data shall be stored in a database at the IC Company site for future analysis and reporting. The database must be accessible from a remote Supplier location. Data must be transmitted and stored during Host control or Off-line states.

Tools shall be capable of performing System Performance Measurement or overall (e.g., daily) QA health checks and storing resultant data for on-site and remote diagnostic purposes.

BENEFITS: Predictive maintenance, CIP data collection
STANDARDS: Time stamps must be closely synchronized with the host in order to facilitate correlation with other events.
Standards community will need to develop universal XML definitions for tool parameters.
TCP/IP.

4.3.5 Data Collection

Supplier shall be able to collect tool data in near real-time via a standard protocol using an Ethernet connection. Remote data collection must be possible while tool is under Host control or Off-line.

BENEFITS: Reduce support cost, Reduce MTTR, Predictive maintenance, CIP data collection

STANDARDS: Action required for ISMT to specify non-proprietary protocol definition for the remote connection.

4.4 Level 2 - Analysis: Automated Reporting and Advanced Analysis with SPC Capability

Key Ideas:

- Automated data reporting and analysis for SPC
- Data Compression

4.4.1 Automated Data Reporting and Analysis

The e-Diagnostics system must have the ability to automatically produce reports that provide sufficient detail in order to understand the operational state and parametric performance history of the equipment on a per wafer, per lot, or periodic basis. The reports should be resident at the IC maker's site.

The e-Diagnostics system shall provide several types of statistical analysis capabilities. On-tool data pre-processing shall be provided for extraction of salient information associated with larger data sets like trace data. Off-tool analysis shall be provided for statistical comparisons of numerical data representations. Pattern recognition capabilities shall be provided on large data sets. Typical features might be expressed as P-P, RMS, Standard Deviation, Mean, Average, Peak, Rise Time, Frequency, etc.

BENEFITS: Reduce support cost, Reduce MTTR, Predictive maintenance, CIP data collection

STANDARDS: Use standard statistical processing functions and data normalization capabilities.

4.4.2 Data Compression

Although this capability is not a requirement, data compression will most likely be necessary as data sets for e-Diagnostics grow significantly.

Compression can be accomplished by statistical techniques, where the associated statistics represent the "compressed" data, or via modern file compression algorithms, such as PKZIP. In the case of file compression, associated means for conveniently "unpacking" information also have to be provided. Evaluating statistical information and automatically uncompressing data for further analysis or decisions are Level 3 capabilities.

This capability will be tightly coupled to the data analysis capabilities.

BENEFITS: Reduce support cost, Reduce MTTR, Predictive maintenance, CIP data collection

STANDARDS: Use standard statistical processing functions and data normalization capabilities and data packing/unpacking techniques

4.5 Level 3 - Prediction: Predictive Maintenance, Self Diagnostics, and Automated Notification.

Key Ideas:

- Predictive/Proactive Equipment Self-diagnosis
- Decision Logic
- Notification

4.5.1 Predictive/Proactive Equipment Self-diagnosis

At level 3, e-Diagnostics capable tools must be capable of self-diagnosing. This implies that tools know what diagnostics or health checks can be executed as well as when it is safe and appropriate to do so.

By combining the capabilities of on-board diagnostic routines initiated by the tool itself, decision logic, and automated notification, the e-Diagnostics system will be able to make proactive decisions regarding maintenance and repair considerations.

BENEFITS: Reduce support cost, Reduce MTTR, Automated Predictive maintenance, CIP data collection

STANDARDS: Self-initiated diagnostic routines must lock the tool in an Off-Line state.

4.5.2 Decision Logic

The e-Diagnostics system shall provide the ability to apply logic or rules to the output from data analysis or data from the database to make simple decisions and initiate secondary actions.

BENEFITS: Reduce support cost, Reduce MTTR, Predictive maintenance, CIP data collection

STANDARDS: N/A

4.5.3 Notification

Based on established decision logic, the e-Diagnostics system shall provide notification of failures, excursions, or negative trends to Supplier and Company.

Although not a required capability, possible tie-in to the FAB MES system should be considered if beneficial and practical in the future.

BENEFITS: Reduce support cost, Reduce MTTR, Predictive maintenance
STANDARDS: Standard capabilities for paging, emailing, and interface to suppliers.
Customer Relationship Management (CRM) systems.
Automated notification must conform to established security guidelines.

5 Data Taxonomy

This section defines the data structure boundary, but does not impose requirements on specific data acquisition or FDC methods.

5.1 General Data Requirements

5.1.1 Preserving Tool Performance

Data collection shall not inhibit tool performance. If tool performance and data collection are co-dependent on the same CPU resources, those resources must be managed in a manner that preserves tool performance. Preservation of data is a secondary concern.

5.1.2 General Architectural Considerations for Tool Data

The principal equipment system shall implement a two-stage filtering architecture on data collection. At the first stage, filtering will be configurable to determine what data is captured and stored on-tool, e.g., in flat-file logs. At the second stage, filtering will be configurable to determine what data is exported off-tool as a subset of the data that is “storable” on-tool. This requirement does not specify how long data should be stored on-tool or off-tool, e.g., in some cases, data may not actually be stored on-tool for any duration. However, there must still be a means for temporarily storing any data on-tool for purposes of testing data integrity.

5.1.3 General Data Formats

Data formats on-tool and off-tool shall have the following properties:

- Data must be accessible across multiple computing platforms and operating systems.
- Data must be generally “extractable” such that individual items or fields within a larger data structure can be universally parsed and manipulated.
- Data structures must be universally interpretable either by standard data type definition (DTD) or data self-description.
- Definition of data structures must be flexible to alter particular data structures and extensible to add new data structures.
- Data formats must be open and non-proprietary such that middleware and software for managing data is universally available.

Note: The data taxonomy group recommends existing SECS-II message formats and new XML formats as candidates for consideration by the protocols group.

5.1.4 Auxiliary Tool Data

Overall system architecture shall support a means for combining principal tool data with auxiliary tool data for e-Diagnostics analyses. This requirement does not specify whether data is merged on-tool or off-tool. A means shall exist for obtaining data from tool auxiliary systems, e.g., AEC/APC add-on boxes, etc. As an example, if a “feed-forward” system has been implemented, but is currently not functioning, e-Diagnostics data capability shall exist for diagnosing this system.

5.1.5 MES Data

Overall system architecture shall support a means for combining principal tool data with data from the Manufacturing Execution System (MES) for e-Diagnostics applications that require both sets of data. This requirement does not specify whether data is merged on-tool or in the MES system. Useful MES data items *may* include:

- Material ID (carrier ID, lot number, and wafer ID)
- Current process recipe
- Process Sequence
- Lot size
- Product family
- Layer or stage
- MES's view of tool and module states
- PM history, schedule
- Component lifetimes

The MES data required for any particular e-Diagnostics use case may be conditional. To the extent that it is necessary, a means shall be provided for dynamically authorizing access to MES data such that agreeable data security is upheld.

5.1.6 Data Accuracy and Precision

- Data structures shall incorporate the data, the units, and the precision of the data. Reporting data with 10 significant figures that is only accurate to three is misleading.
- Time stamps for event data shall accurately reflect the event at collection time and not additional delays imposed by data processing and transmission.
- Specific triggers for events shall be well documented and traceable.
- Merging tool data with off-tool data (i.e., MES) requires that the tool's clock and the factory's or middle-ware's clock be synchronized.

5.1.7 Data and Tracking Capability Classifications

5.1.7.1 Data Persistence Classes

The following classes are used to quickly characterize equipment data availability against a specific list of customer requests. If certain data items do not have the desired class on a particular equipment, a change in class may be negotiated (e.g., a customer may require certain types of Class 3 data re-implemented as Class 2 or Class 1 data.

Class 1 Data (“Stock Data”) is available all the time from every tool, standardized data structures are used to transmit the data and remain constant. Fundamental data, all equipment suppliers agree that this data will always exist. (pressures, temperatures, RF parameters for all RF sub-systems, etc.). Available Class 1 Data does not change based on software release.

Class 2 Data (“Custom Data”) may come and go depending upon hardware and software configuration. Standardized formats are used but will vary. Configuration sensitive information (turbo/cryo pump parameters, auxiliary sensors, etc.) Data that is dependent on how the hardware or software is configured. Available Class 2 Data may change based on software release.

Class 3 Data (“Servicer Data”) may or may not be available using standard query techniques, may be shipped as a binary structure inaccessible to the user. Very low-level component data that may only make sense to the component supplier or servicer. Available Class 3 Data may be independent of tool software releases.

5.1.7.2 Parametric Tracking Capability

A standard classification shall exist for the purpose of communicating parametric data collection capability compliance. This classification will include a premium class, e.g., Class A, capability wherein the following criteria are suggested:

Parametric Data Collection Class	On-Tool Logging Capability	Off-Tool Send Capability
Class A	TBD—Capability greater than or equal to off-tool send capability.	<ul style="list-style-type: none"> • Ability to monitor any parameter known to the tool • Available sample rates of at least 10-50 Hz. • Ability to track at least 50 parameters per process chamber

5.2 Event Data

Events are instantaneous occurrences or changes in equipment state or status. There is no duration associated with any individual event. Collectable events are useful for generating snapshot type reports of the equipment at the time of the events. These reports may contain a custom configurable set of information. Any single collectable event activated for reporting may have one or more different reports associated with the event where multiple reports are allowed to contain overlapping information.

5.2.1 Non-Exception Events

These events are associated with normal functioning of the tool. They can be used for tracking cycles and time-based equipment performance. They are also useful in “recreating a crime scene” and subsequent playback during a post-mortem review of an equipment problem. A minimum list of required events include:

- Start and complete of the following: control job, carrier processing, wafer or reticle processing.
- Change of tool state (e.g., ARAMS or tool’s view of E10) and/or tool operating mode (supplier specific).
- Start and complete of equipment and module tasks (e.g., wafer load, pump-down, transport, chamber or station process, etc.). Note: specific terminology and definitions under development by SEMI task force on Equipment Performance Tracking (EPT).

5.2.2 Exception Events

These events represent the occurrences of unplanned or abnormal behavior. These events can be used to flag or notify appropriate personnel of equipment difficulties. These events are also useful for tracing root causes of equipment difficulty in post-mortem analyses.

Exception events shall follow a standard behavior (according to existing SEMI standards or new e-Diagnostics Guidelines) and shall include the following event sub-types:

- **Error**—an instantaneous exception event whose consequences are not persistent after the event.
- **Alarm Set**—an instantaneous exception event whose consequences are persistent after the event.
- **Warnings**—an indicator notification event that of itself does not represent a noteworthy exception but may act as a predictor of one.
- **Response**—a response event to a prior exception event that marks an action or resolution of that exception. These events may include abort start and complete, alarm clears, requests for assistance start and clear, auto-recovery actions invoked start and complete, automatically detectable repair actions start and complete.

5.2.3 Closed-loop Positive Performance

Exception events present a difficulty in defining coverage in that 100% of all possible failure modes is generally unknowable, or at least impractical, to monitor. To supplement exception coverage, accurate closed-loop measurements of “positive” performance are necessary. The absence of “positive” performance is a likely indicator of undetected exceptions.

- Overall Equipment Efficiency (OEE) and its component metrics, operational efficiency, rate efficiency, quality efficiency, etc.

- Count of wafers out, including effective wafers, assignable scrap and rework, and non-assignable scrap and rework.
- Theoretical production time per unit by recipe (THT)

5.3 Recipe Performance Data

On completion of each recipe, the tool shall send an event indicating “recipe success” to the best extent that is known at that time. In this context, there is at least one recipe per wafer per tool visit, and possibly multiple recipes per wafer. Determining “success” or “failure” is dependent on equipment type as follows.

5.3.1 Performance for Metrology and Inspection Equipment

Performance for metrology and inspection equipment indicates the success with which desired metrology results are accurately obtained. The following descriptive criteria apply:

- Success—if a metrology recipe obtains complete and accurate results according to the recipe specification.
- Marginal Success—if results are only partially complete but accurate, the recipe *may* be marginally successful.
- Failure—if the results are incomplete and inaccurate, the recipe is a failure. Failure also includes scrap, rework, and yield loss issues assignable to the tool (although these are less likely for metrology and inspection equipment).

5.3.2 Recipe Performance for Process Equipment

Measurement of recipe success or failure for process equipment is complicated by the availability of metrology and inspection data results. Definitive recipe evaluation cannot be confined to individual process tools and must be derived from a larger cross-tool, process-specific review. At the time of recipe completion, the following criteria may be applied to the tool’s best knowledge:

- Success—recipe execution was completed with probable indication that the recipe objective was fulfilled. No errors or incidents occurred that might indicate that the recipe objective was not fulfilled.
- Marginal Success—recipe execution was completed but warnings (recoverable errors) or incidents occurred indicating doubt that the recipe objective was completely fulfilled; this should include “recoverable” cases where additional processing and/or rework may be required.
- Failure—(1) recipe execution did not reach completion and cannot be resumed, or (2) errors and/or incidents occurred, indicating with certainty that the recipe objective was not obtained. Failure also includes scrap, rework, and yield loss issues assignable to the tool.

5.4 Tool Health Monitoring Data

Data associated with periodic health checks (i.e., daily monitor, periodic maintenance (PM), system test)

5.4.1 Diagnostics Types

- System Test—End-to-end system test on material comparable to production units, e.g., monitor wafers.
- Subsystems Test
- Field Replaceable Units (FRUs)/Component Test

5.4.2 Diagnostics Results Types

Complex diagnostics may be composed of one or more of the following result types:

- **Pass/Fail Criteria:**
 - Header: Test ID
 - Content: Pass/Fail
- **Parametric:** Values whose performance are neither documented nor characterized. Control limits are optional and specify expected behavior but do not imply failure of a diagnostic test.
 - Header: Parameter ID, units, parametric control limits, data validity limits
 - Content: Current value
- **Specification Status:** Values whose performance are more formally documented or characterized. Control limits are required. Current value outside of the control limits implies a failure of the diagnostic test.
 - Headers: Test ID, units, specification control limits, data validity limits
 - Content: current value, pass/fail
- **Vector Types:** A vector type is data in which individual data points have the same units.
 - Header: same as any of the above three types
 - Content: vector of current values

It is desired to create standard formats for these elemental result types such that a standard dictionary may be developed for interpreting a complex collection of these types.

5.4.3 Wafer or Reticle-based Diagnostics

The Test ID includes a coordinate on a wafer or reticle. The same types of results as in section Diagnostics Results Types apply.

5.4.4 Other Tool Health Data

- **Reference Data:** Used to qualify the success of a diagnostic test may not reside on a tool. For example, this data may reside on metrology review stations/servers and the MES.

- **Tool Service/Maintenance Data:** This data will most likely not reside on the tool. Examples include:
 - Part lifetimes
 - Time since last PM
 - Time since consumable change

5.4.5 Diagnostics Periodicity

For any periodic procedure, a subset of all available diagnostics on the tool may be assigned to that procedure. It may be possible to dynamically change these assignments to improve diagnostic effectiveness. The following are sample types of periodic diagnostics or periodic procedures:

Periodicity	Test ID	Hourly	Shift	Daily	Weekly	Monthly	Quarterly	Bi-yearly	Yearly
System	S1	X							
	S2				X				X
	...		X			X			
Subsystem	SI							X	
	SS1			X					
	SS2			X					
	...					X			
FRU/Component	SSm			X					
	C1			X			X		
	C2					X			
	...						X		
	Cn			X					

5.5 Operational Performance Data

Operational Performance Data are measures of tool performance that are functions of dynamic data. Performance measures may be relative or absolute and must involve some type of comparison, filtering, or analysis. For any piece of operational performance data, that data may be a function of raw data and other measures. Operational Data may be used in the following Use Cases:

- Triage top-level causes of productivity loss and potential for improvement
- Monitor long range improvement or effectiveness of a longer-term maintenance policy
- Support decisions on tool management (dedication of resources, tool evaluations)

5.5.1 Operational Performance Metrics

The e-Diagnostics system is required to support the following operational performance metrics:

- Error Occurrence Frequency (Error Pareto)
- Recipe Usage Frequency
- MTBF, MTTR, and MTOL
- Combined E10/E79 Stack Chart
- Component Metrics of E79 OEE (Availability Efficiency, Operational Efficiency, Rate Efficiency, and Quality Efficiency)

5.6 System Baseline Data

System Baseline Data provides a necessary basis of comparison for all other e-Diagnostics data. This includes data about the tool and the environment that must be available for proper context evaluation of other data.

5.6.1 Software

- Versions of all software components used in the system.
- Shall include such things as the software for: supervisor, process modules, and sub-assemblies. Configuration files for tool mechanical configuration including the module information including options with model numbers and serial numbers for all major components. A system of configuration management shall support traceability down to individual part drawings.
- The last revision date and time should be recorded and an event should be sent related to any revision. A method for evaluating the file against a standard file should be provided for consistent fab wide control.

5.6.2 Equipment constants

- Electromechanical control parameters such as PID values
- Process control limits
- Calibration constants and offset constants for control and sensor assemblies

5.6.3 Recipe Revision Control

- Local revision tracking. An event shall be sent if a local revision is made.

5.6.4 Static test and sensor results (BKM Results)

- The results of non-revenue process tests. Examples are: leak rate tests, flow check tests, pressure tests, vacuum tests and power levels
- Environmental data such as barometric pressure, ambient temperature, and humidity—raw data.

5.6.5 Benchmark Data

Performance benchmarks by tool type including Theoretical Process Time Per Unit by Recipe required for E79 OEE. Because this data involves multiple instances of each tool type, these standard times are likely to be derived and stored off-tool.

5.6.6 Design Specifications

Supplier-specified performance and operational limitations on the equipment, as designed.

5.7 Tool Usage Data

Tool Usage Data is dynamic data about how the tool and its resources are being applied. This data is uncharacterized (neither “good” nor “bad”) and simply represents the status of the tool and/or what the tool is doing moment-to-moment. Tool Usage Data may be used in the following Use Cases:

- Correlate to failures during a review process
- Support control policies (PM scheduling, consumables and parts replacements, etc.)
- Measure tool lifetime or overall wear (like odometer of car)

5.7.1 Tool Usage Data Categories

Tool Usage Data is required in each of the following two categories, as listed:

1. Status Data
 - Current User ID
 - Current Recipe
 - Current Mode (Auto vs. manual, supplier specific)
2. Accumulators
 - Event Counters - Wafer count, job count, etc.
 - “Integrators”/Continuous Accumulators - RF hours

6 Data Security

This sub-working group is developing a set of guidelines specific to data security for e-Diagnostics. Eventually these guidelines shall be translated to specifications so that a developer can use and incorporate into e-Diagnostics solutions. .

6.1 Data Security Assumptions

The Data Security assumptions are:

- By default, no tool data shall be labeled as unclassified or "public" information. Tool data, by default should be classified as level 2 or 3.
- Data shall maintain its classification label no matter where the data resides (in the factory, at the supplier site, in a field service engineer's notebook computer, etc.).

6.2 Data Classification

All e-Diagnostics data is classified for security. The range of classification is as follows (from lowest to highest):

0. Unrestricted/Public: There may be instances of data that have little to no proprietary value (i.e., power quality) that can be collected and useful in different situations (i.e., data presented at public conferences, etc.). We should also consider the possibility where data may be declassified (given age or relevance) but may still be useful for statistical analysis. Classified data could also be "scrubbed" or "sanitized" in such a way that all proprietary data could be removed thus making the data generic but valuable nevertheless. Procedures and processes would define how data is declassified or labeled as "unrestricted." Tool data that has not gone through a process of classification would not default to this level. Data defaults to level 2 or level 3.
1. Confidential/Restricted: where data had a larger audience than Secret/Confidential, but access was limited to the specific scope that the data was associated with. This shall be typically covered by standard, legal agreements.
2. Secret/Confidential: where data was not as restricted as Top Secret/Private but generally the audience was a bit larger. This classification shall be limited by organization and subjected to specific dissemination rules where explicit permission is required for dissemination outside designated organizations.
3. Top Secret/Private: where data was limited to a specific audience and/or dissemination or movement of this data was severely limited. This data classification would restrict the data to a specified list of individuals and require a "sign-off" procedure. In the e-Diagnostics context, this may require certificate authority or actual physical action at the tool where data can be released.

There may be a valid business case for sharing data with a different supplier in the e-Diagnostics effort.

- Data from one tool may impact the performance of another tool or a component in that toolset.
- Data from a different tool may be needed to successfully complete an e-Diagnostics solution.
- Utilizing data from another tool may be beneficial in the effort of preventative maintenance.

The classification matrix may be modified to take this into consideration. This concept shall be covered in the legal agreements signed by IC manufacturer and equipment supplier.

Classification also needs to take into account the boundaries where the data exists. For example:

1. Data restricted to IC manufacturer only.
2. Data restricted to IC manufacturer and equipment supplier from within the factory environment.
3. Data restricted to IC manufacturer and equipment supplier outside of the factory environment.
4. Data can be shared between different equipment suppliers outside of the factory environment.

Group decided that this should be a "property" of the data classification listed above and included in the overall classification matrix.

6.3 Classification Matrices

Classification matrices, including matrix properties, will be developed for the following properties:

- Risk assessment (Cost of loss)
- Examples
- Authorization Levels
- Time to authorize
- Duration of authorization
- Disposal
- Encryption level
- Use (repair, development, engineering, etc.)

Risk Assessment

Classification	Description	Audience	Distribution	Risk Assessment
Level 3	Top Secret or Private Data	Restricted to a specific audience	Limited to the specified audience. Release of the information may require specific "sign-off" procedure.	Outside entity can replicate or significantly accelerate development of a competing product. Sufficient research and development invested thus making the data very valuable. Damage would be irreversible if released to a competing entity.

Level 2	Secret or Confidential Data	Larger audience than Level 3 but limited by organization	Explicit permission needed and required prior to release.	Outside entity can gauge or assess a measurable quality of a product. This may include a certain specification whereby an outside entity could possibly gain a tactical advantage. Damage will occur in the short term and could include adverse public relations or a potential manufacturing advantage (i.e., improved quality, release to market, etc.)
Level 1	Restricted	Larger audience than Level 2 but limited to the specific scope of the associated data.	Limited to those individuals with need to know type access. Distribution limited to the standard and typical legal agreements (NDA, etc.)	The data has limited value by itself. If aggregated with a collection of other similar or related data the value has a greater impact. Damage is similar to Level 2 except it would take place in the long term and require some effort to accumulate and aggregate the data.
Level 0	Unrestricted or Public	Anyone in the public arena	Can be shared without any limitation or reservation.	None

Classification matrices for the other properties are under development.

7 Protocol Definition

7.1 Scope and Limitations

This section defines the essential attributes required of communication software or protocols which shall be addressed when implementing each of the e-Diagnostics system capabilities.

Where possible, recommendations of communications protocols or software best suited to meeting capability needs for e-Diagnostics are provided. Where possible, recommendation of data representation technologies best suited to meeting capability needs for e-Diagnostics are also provided.

The ability to define appropriate communications protocols and data representation technologies is limited by the degree to which system capability and architecture has been defined. At the time of this writing, e-Diagnostics capability and architecture definition are work in progress. As these aspects of the system evolve, protocol and data representation recommendations may also change.

7.2 Capability Level 0

7.2.1 Use Case: View/Download Equipment Files

See Appendix A for Use Case tables.

7.2.1.1 Transport Protocol Considerations

7.2.1.1.1 Assumptions & Constraints

1. File viewing/transfer system shall support multiple data formats (ASCII, binary, etc.)
2. File viewing/transfer system shall be implement-able on multiple hardware platforms (PC, workstations, etc.)
3. File viewing/transfer system shall be implement-able on multiple operating systems (NT, VxWorks, RMX, PSOS, HPUX, Solaris, VMS, etc.)
4. File viewing/transfer system shall integrate with the e-Diagnostics access control system – no additional login or authentication activity should be required
5. File viewing/transfer system shall be implemented on TCP/IP
6. File transfer shall be auditable from a single location
7. Different architectural models shall be accommodated (direct file access to the tool & access to files on a server)

7.2.1.1.2 Options

7.2.1.1.2.1 FTP

FTP [RFC-0959] is a common protocol intended for enabling efficient bi-directional file and data transfer between peers. FTP utilizes the Telnet protocol for control communication and a TCP connection is used for data and file transmission.

7.2.1.1.2.2 FTP over SSL

FTP can optionally be made secure by transporting over a Secure Socket Layer, similar to HTTPS. Support for SSL can be easily implemented within the FTP protocol and can be made to revert back to conventional (non-secure) mode if the server on the tool does not support it.

7.2.1.1.2.3 HTTP over SSL

HTTP [RFC-2616] is a generic stateless request/reply protocol in broad usage throughout the internet. SSL is a secure, reliable, communication protocol which enables encrypted communication between peers. The specification is available from Netscape at the time of this writing at: <http://home.netscape.com/eng/ssl3/draft302.txt>.

7.2.1.1.2.4 Third Party Application Software

Commercial packages such as pcAnywhere and Support Now provide file-transfer capabilities. Such products may use proprietary file transfer algorithms.

7.2.1.1.3 Pro/Con

7.2.1.1.3.1 *FTP*

- + Simple
- + Widely used
- Not secure

7.2.1.1.3.2 *FTP over SSL*

- + Easy to implement
- + Secure
- + Can fall back to traditional (non-secure) FTP
- Implementation dependent

7.2.1.1.3.3 *HTTP over SSL*

- + Simple
- + Widely used
- Not as efficient as FTP
- Requires a web server on the tool

7.2.1.1.3.4 *Third Party Application Software*

- + May provide secure and efficient file transfer (possibly as part of a larger package).
- Licensing costs may be high
- Application software requirements on the tool may be resource hungry.

7.2.1.1.4 Recommendation

Capability Level 0 file transfer shall use, at a minimum, TCP/IP with an FTP demon to enable remote file transfer. It is strongly advised that data encryption and compression be implemented in transfer application. One way this may be accomplished seamlessly is by transporting over SSL.

This recommendation only specifies a minimum level of functionality and does not preclude the use of more sophisticated methods of file transfer.

7.2.1.1.5 Open Issues

- How was administration and access control considered? How was it contrasted with HTTP over SSL?
 - Administration and access control are features of or requirements for other elements of the e-Diagnostics system. Since they are not a function of the file transfer protocol, they were not considered in this work.
 - However, it may be required that a person at the tool be given notification of an impending file transfer or a request for such, and that he must grant permission for the operation to continue successfully. Otherwise the file transfer operation fails or is cancelled.

7.2.2 Use Case: Remote Collaboration

See Appendix A for Use Case tables.

7.2.2.1 Transport Protocol Considerations

7.2.2.1.1 Assumptions & Constraints

1. Collaboration system software shall support the following minimum capabilities:
 - 1.1. Shared file viewing (all participants can view files simultaneously)
 - 1.2. Still image capture and sharing
2. Collaboration system software shall also support the following additional capabilities:
 - 2.1. File transfer among participants (shall support auditing)
 - 2.2. Video transmission
 - 2.3. Voice transmission
 - 2.4. Text/Chat/Instant Messaging
3. Collaboration system software shall run on the TCP protocol.
4. Collaboration system shall be based on an industry standard protocol set (example T.120) or should be platform-independent (i.e., web-enabled).
5. All conference parties shall be authorized/authenticated users of the system.
 - 5.1. Known user to the system.
6. Collaboration session may be initiated inbound or outbound. Adequate security must be provided to prevent security breaches on inbound ports (example: denial-of-service attacks). **Recommend Data Security working group address this issue.**
7. The collaboration system is restricted to the tool, and networked resources required to run the tool, and no access to any other resource off the tool.
8. Any video component of the collaboration system shall accommodate selecting on/off states to permit repositioning of the viewing device to allow suppliers to see selected view of equipment.
9. The collaboration system need not provide any particular capability for filtering sensitive data – text/data/document sharing is strictly at the discretion of the manufacturer and supplier.
10. The collaboration system may include file transfer at the discretion of the remote service provider and the local tool owner. Ultimate storage location for transferred files must be explicitly specified by recipient.
11. The collaboration system can support one-to-one or one-to-many participants.
12. The collaboration system shall be compatible with data encryption mechanism.
13. Collaboration sessions shall support the ability to produce an audit trail through a secure logging mechanism.
14. The collaboration system shall be capable of functioning through standard proxy services (e.g., http proxy services).

7.2.2.1.2 Options

- Third party conferencing software
- Custom developed conferencing software

7.2.2.1.3 Pro/Con

7.2.2.1.3.1 *Third party software*

- + Several products available
- + Web-based software

- Business viability of vendors may be volatile

7.2.2.1.3.2 *Custom developed software*

- + Software can be designed to fully integrate with e-Diagnostics system

- Not a value-added development investment for most equipment supplier companies

7.2.2.1.4 Recommendation

It is recommended that Third Party Applications be selected to implement these capabilities. Any such product must address each of the constraints described above – any variations or deviations are to be negotiated and agreed-upon between manufacturer and supplier. Where specific equipment h/w platforms are not supported, it may be necessary to host software on a system other than the primary equipment control hardware.

7.2.2.1.5 Open Issues

- See Information Security section for details on who can initiate a collaboration session.

7.3 Capability Level 1

7.3.1 Use Cases: Monitor Remote Equipment Operation

Remote service provider is granted authorization to view data at Tool Owner's store. See Appendix A for Use Case tables.

7.3.1.1 Transport Protocol Considerations

7.3.1.1.1 Assumptions & Constraints

1. Data from tool owner's store to remote service provider workstation shall be encrypted.
2. The protocol used for reviewing performance history shall be efficient. Reviewing data would be cumbersome if there were long delays.
3. The protocol shall be platform independent since remote service providers may have different platforms for their workstations.

4. It is assumed that the data at the tool owner's store will be represented in some kind of graph or table format; therefore, graphing capabilities shall be supported in the protocol.

7.3.1.1.2 Options

- HTTP (secure)
 - Assumption that web server will be installed at tool owner's store
 - Can support most widely used web browsers (examples are Internet Explorer and Netscape).

7.3.1.1.3 Pro/Con

- HTTP is a well known, platform independent, means of viewing data over the network.
- HTTP can be secure with HTTPS and supports encryption (digital certificates).
- Remote users can run on any platform which supports a browser.
- Ports associated with web browsing are generally open on most firewalls.

7.3.1.1.4 Recommendation

- Use HTTPS with thin client.

7.3.1.1.5 Open Issues

How much detail do we want to include in the requirements?

7.3.2 Use Case: Replicate Tool Data from Store to Supplier

Data from Tool Owner's store is periodically replicated at Supplier's store. See Appendix A for Use Case tables.

7.3.2.1 Transport Protocol Considerations

7.3.2.1.1 Assumptions & Constraints

1. Data should have guaranteed delivery. If the network goes down, or a connection is lost, the data shall be resent. If the supplier's store only received a portion of the data sent, it may lead to incorrect conclusions.
2. All data from tool owner's store to supplier's store shall be encrypted.
3. Transport mechanism should be platform independent since the tool's store and supplier's store are not known.
4. The ability to configure time periods for replication should exist.
5. Protocol must be able to go through a firewall since there will probably be a firewall between the tool's store and supplier's store.

7.3.2.1.2 Options

- a. DB Links
 - Database links can be established between tool store and supplier store.
- b. Secure HTTP
 - i. Data from tool's store can be packaged and sent to supplier's store via HTTP.
 - ii. Data shall be transported using XML
- c. Corba
 - i. Data from tool's store can be packaged and sent to supplier's store via CORBA.
- d. Use a protocol supplied by Database vendor.
 - i. Need to research existing protocols.

7.3.2.1.3 Pro/Con

7.3.2.1.3.1 DB Links

7.3.2.1.3.1.1 Cons

- Shall have database access rights to create links
- Firewalls shall be opened for link which is not generally done.

7.3.2.1.3.1.2 Pros

- Efficient way to transport data
- Platform independent
- Encryption may exist
 - Oracle allows for encryption – need to check other Databases

7.3.2.1.3.2 HTTP

7.3.2.1.3.2.1 Cons

- Need to specially package data which could add a lot of overhead.
- There is no guaranteed delivery service.

7.3.2.1.3.2.2 Pros

- HTTP does allow for platform independence.
- It is possible to have encrypted communication using SSL.

7.3.2.1.3.3 CORBA/RMI

7.3.2.1.3.3.1 Cons

- Licensing costs for CORBA are high.

- CORBA has a complex configuration which would make it difficult to work with.

7.3.2.1.3.3.2 Pros

- CORBA can run on multiple platforms.
- CORBA has different features depending on what vendor you use. It would be necessary to specify a vendor to ensure that all platforms could be supported with no issues.

7.3.2.2 Recommendation

To be provided.

7.3.2.3 Open Issues

Investigation into protocols supported by database vendors shall still be done.

7.3.3 Use Case: Report Equipment Data

See Appendix A for Use Case tables.

7.3.3.1 Transport Protocol Considerations

7.3.3.1.1 Assumptions & Constraints

1. Data collected by e-Diagnostics is not required to be produced for consumption by IC manufacturing systems for any purpose other than equipment diagnostics and troubleshooting (there is only one consumer of e-Diagnostics data: the e-Diagnostics system)
2. Data only need move off-tool in minute-or-greater intervals
3. System shall guarantee delivery to off-tool storage
4. System shall be implementable on a variety of platforms (SPARC/HP/x86 UNIX variants, NT, W2K, VMS, DOS, etc.)
5. System shall support data encryption
6. Since all communication is behind firewall, no special security considerations beyond encryption need impact protocol selection

7.3.3.1.2 Options

1. HTTP-based messaging
2. Middleware
 - 2.1. MQSeries
 - 2.2. Corba ORBs (Visigenic, Ionix, etc.)
 - 2.3. TIB/Rendezvous
 - 2.4. Java RMI/JMS
 - 2.5. COM+

7.3.3.1.3 Pro/Con

7.3.3.1.3.1 HTTP

- + Freely available on all platforms.
- + W3C XML Protocol Working Group formed for defining an XML-based protocol mapped onto HTTP – will produce XML RPC on HTTP semantics as a standard.
- + Encrypted communication possible over SSL or S-HTTP.
- + Services offered by tool can be made accessible via web server on tool.

- No HTTP-based RPC standard exists. Internet standards development takes time: W3C XML Protocol Working Group formed in September, 2000, and is projecting a recommendation in September, 2001, followed by WG disbandment in April, 2002. Conformant implementations to follow sometime thereafter.
- W3C will not treat transaction management, security context, or anything other than message exchange semantics as in-scope. These elements will continue to remain platform/application-specific even after a W3C recommendation.
- No guaranteed delivery service: developers select or implement this technology on either side of each HTTP request.
- Services offered by tool require http server on tool.
- Performance of HTTP text-based protocols is very likely going to be orders of magnitude slower than binary wire protocols.

7.3.3.1.3.2 Middleware

- + Many middleware vendors provide a range of delivery services, including guaranteed delivery.
- + Many middleware vendors provide sophisticated failure detection and diagnostic logging for troubleshooting.
- + May support pub/sub model, if required.
- + Purchased, not built.

- Licensing arrangements & costs (supplier and manufacturer).
- Product version management (supplier rev cycles must be synchronized and validated with in-fab systems, and potentially with other suppliers' revs).
- Universal platform support may not be available.
- Service availability may not be consistent across platforms.
- Language support may be spotty or non-existent (e.g., Java systems).

7.3.3.1.3.3 MQSeries

- + Guaranteed delivery of asynchronous messages
- + Point-to-point message queue & publish/subscribe models
- + Transaction support
- + Message priority support
- + High performance
- + Multiple platforms including NT, MVS, various Unix flavors, and VMS
- + Multiple language support
- + Highly configurable
- + Support for JMS

- Licensing costs
- Large footprint/overhead
- Site administrative overhead

- Proprietary messaging protocol

7.3.3.1.3.4 *Tibco*

- + Provides guaranteed delivery messaging service.
 - + Flexible, anonymous message categorization.
 - + Field-level data encryption.
 - + Routing control for cross-network communication & self-diagnostic messaging.
 - + Multicast support.
 - + High performance.
 - + Supports point-to-point & publish/subscribe communication models.
 - + Supports LAN & WAN messaging.
 - + Provides a CORBA 2.0 ORB implementation with basic services.
- Proprietary event messaging protocol, data packaging, and programming model.
 - High licensing costs.
 - Train or hire TIB network administrators.
 - Product versions not always backward compatible at the source level.
 - Product versions not always 100% interoperable with previous revisions, factories and vendors need to synchronize upgrade cycles.

7.3.3.1.3.5 *CORBA products*

- + Guaranteed delivery of asynchronous messages
 - + Multiple platforms supported
 - + Publish/subscribe model
 - + Multicast support
 - + Both push & pull event models (Corba Event Service)
- Licensing costs
 - No support for point-to-point message queues
 - Administrative overhead
 - Vendor specific features/specification (e.g., OrbixTalk)

7.3.3.1.3.6 *Java RMI, JMS*

- + Guaranteed delivery of asynchronous messages
 - + Point-to-point message queue & publish/subscribe models
 - + Transaction support
 - + JVM platform (i.e., supports multiple OS platforms)
 - + Corba and EJB compatible
 - + Several commercial implementations available (e.g., SonicMQ)
 - + 3rd-party support for ActiveX/COM
- No multicast support
 - No built-in security model
 - No integrated load balancing/message traffic administration
 - JVM platform (Java language only)
 - Reference implementation not available until J2EE 1.3 release
 - Licensing cost for 3rd-party implementations

7.3.3.1.3.7 COM+

- + Point-to-point message queue
- + Integrated with OS (bundled with NT/2000)
- + Integrated security model
- + Transaction support
- + Message priority support
- + Very high performance
- + Integrated load balancing/message traffic administration
- + 3rd-party support available for non-NT platforms (Unix, VMS, MVS, etc.)
- + 3rd-party support for seamless connectivity to MQSeries

- Integrated with OS (vendor specific)
- Licensing costs for 3rd-party multi-platform support

7.3.3.1.4 Recommendation

Of all options available, only HTTP messaging, CORBA, and Java RMI/JMS are spec-based communications infrastructures, allowing supplier and manufacturer development investments to potentially survive individual product or vendor company lifetimes, or adverse changes in licensing arrangements. This flexibility requires that software implementations do not take advantage of extensions to the standards employed.

HTTP messaging falls short of essential features (quality of service, no available application-to-application communication standard), and early testing of messaging with current proprietary implementations show performance that is 2-3 orders of magnitude slower than binary protocols. While these are early results, they indicate that HTTP-based messaging may not be the best selection for LAN communication in a high volume factory.

Java RMI/JMS provides all essential features required for this capability; however integration with non-Java software systems is problematic, and the JVM is typically a significant consumer of computer system resources. As one of the conditions for a successful e-Diagnostics system is that its implementation does not adversely affect equipment operation, JVM resource consumption on the tool is a significant concern.

Therefore, the recommendation is that off-tool data movement occurs via a CORBA infrastructure, with an initial recommendation for the support of the services below:

CORBA 2.3

- IIOP
- Required language mappings
- Naming Service
- Notification Service
- Security Service

7.3.4 Use Cases: View Remote Equipment Configuration, Change Remote Equipment Configuration

7.3.4.1 Transport Protocol Considerations

7.3.4.1.1 Assumptions & Constraints

1. Remote Operations must run on the TCP protocol.
2. Remote operation shall be based on an industry standard protocol set (example T.120) or should be platform-independent (i.e. web-enabled). This is important to support Level 4 capabilities.
3. Remote operation may be based on a remote procedure call mechanism.
4. Remote operations that change the tool shall be performed when the tool is not in a manufacturing state (for example GEM OFFLINE).
5. Remote operations that view tool status (i.e. "read-only") can be run any time.
6. For remote operations, the control system shall provide an accurate status of the operational condition of the machine.
7. When a tool is under remote operation, a local operator shall be present at the tool.
8. Remote operator shall be the authorized user of the system.
 - 8.1. Qualified for a given level of operation.
 - 8.2. Known user to the system.
9. Local operator initiates the request for service (the case).
10. Software remote operation session may be initiated inbound or outbound. Adequate security shall be provided to prevent security breaches on inbound ports (example: denial-of-service attacks).
11. The local operator grants permission.
12. The local operator has the ability to take control of the session, or terminate the session, at any time.
13. Remote operation is restricted to the tool, and networked resources required to run the tool, and no access to any other resource off the tool.
14. Single sign on capability to related tools.
15. Remote operation can be restricted to approved data only.
16. Remote operation includes the ability to load files when approved by the local operator.
17. Remote control can support one-to-one or one-to-many participants.

18. Remote operation is compatible with data encryption mechanism.
19. Remote operation sessions shall support the ability to have an audit trail through a secure logging mechanism.
20. Remote operation and/or e-diagnostic system shall support recording of revision history into the change log.
21. Remote Operation can work through standard proxy services (example: http proxy services).

7.3.4.1.2 Options

- T.120 (protocol set)
- H.323 (video-conferencing)
- HTTP-S
- Proprietary algorithms

7.3.4.1.3 Pro/Con

Collaboration and Remote Operation:

Protocol	Pro	Con
T.120 and H.323	Open standard	Not broad usage
HTTP-S	Open standard, Broad Usage, secure	Remote operation packages using this protocol are not widely available.
Proprietary algorithms	May satisfy most functional requirements depending on each package.	Proprietary, typically only available on NT

7.3.4.1.4 Recommendation

No specific protocol can be recommended for all applications at the current time. T.120 is a published standard but applications based on this standard are not widely available. Proprietary algorithms cannot be recommended because they are vendor specific.

The recommendation that can be made at this time is that any solution shall satisfy the functional requirements specified in Assumptions and Constraints.

7.4 Capability Levels 2-3

Much of the capability specified at these levels affects application design, but does not directly call for investigations of software communication options. A noticeable exception is the notification capability described at Level 3.

At the time of this writing, analysis and definition of these capabilities have not been produced to a level of detail necessary for undertaking a recommendation for implementation technologies. As this definition evolves, additional analysis and recommendations will be made where appropriate.

8 Network Bandwidth Requirements

This section is the output of the Network Requirements working group of the International SEMATECH e-Diagnostics team. The content is intended as guidance for the other e-Diagnostics groups and to answer the question: "Do we have enough network bandwidth to support the e-Diagnostics capabilities being defined?"

Considerable interaction with the other working groups provided insight into the overall network requirements design guidelines and constraints.

8.1 Assumptions

Some basic numeric assumptions for bandwidth are:

- RS232 rate = 115.2Kbits per second
- TCP/IP and HSMS rate = 1 gigabit per second per pipe, typically used for network backbones and high end servers
- T1 rate = 1.5 Mbits per second
- T3 rate = (up to) 45 Mbits per second

The team characterized current IC manufacturer's fabs with the following assumptions:

- Live data is needed in near real-time, not hard real-time
- 400 tools per fab, each capable of producing e-Diagnostics data
- Each tool variable must be available for e-Diagnostics
- Burst rate: 5000 variables per tool, each variable can be output once per second, and is 48 bits (6 bytes) long, including formatting (non-ASCII)
- Tracking rate: Volume needed for equipment tracking is 1% of data needed during Unscheduled Downtime, excursions
- Metrology tool data is 10% of a process tool e-Diagnostics data

The Network Requirements team is also making the following general assumptions:

- Each higher level in the Capabilities team 4 level model requires all lower levels
- Large file transfers are network intensive as well. Small to medium sized files transfers are not network intensive.
- Level 1 time frame is based on a **<1 minute sample>**
- Level 2 is based on **<10-15 minute samples>**
- Remote command execution is not network intensive
- There are 86,400 seconds per day

The e-Diagnostics data is assumed to be both a flow and at certain times a file transfer. The volume of data initially captured will be the largest and then as we implement Internet transfer to the suppliers that data will be a subset of the initial captured data. It is also expected that additional e-Diagnostics learning will refine and reduce the amount of data needed.

8.2 Data Points

The team identified the following data points to provide a context for understanding current network capabilities and experiences.

- MC1 = 1 kilobyte / tool / second or 8 Kbits / tool / second
- Varian (6/29) = 1/2 gigabyte / tool / day or 46.3 Kbits / tool / second
- TP2 = 10 Mbytes / tool / day or 0.93 Kbits / tool / second
- Full defect wafer map = 160 Mbits /second
- Pre-1998 class PC = 10 Mbits / second transfer rate, typically used for desktops
- New PC with Ethernet card = 100 Mbits / second transfer rate, typically used for servers and high end workstations

8.3 Scenarios

The team used the collective experiences and assumptions documented above to characterize three different possibilities. This was done to provide a context for the various network bandwidth requirements

8.3.1 Worst Case Scenario

The worst case scenario is characterized by 400 tools in a fab each with 5,000 variables each data transmission taking 6 bytes. So that would be a burst rate of:

- 5000 variables * 48 bits * 400 tools
- = 96,000,000 (96M) bits per second of data transmission for each fab

8.3.2 Connectivity Case Scenario

Normal system design provides for a maximum of 10% of tools communicating at the same time to the network. Assuming 400 tools in a fab then 40 tools would be connected to the network at any one time. If these tools are outputting 100 variables 5 times per second the rate would be:

- 40 times 100 variables times 5 transfers per second times 48 bits for each transfer
- = 960,000 bits per second for this fab

8.3.3 Typical Case Scenario

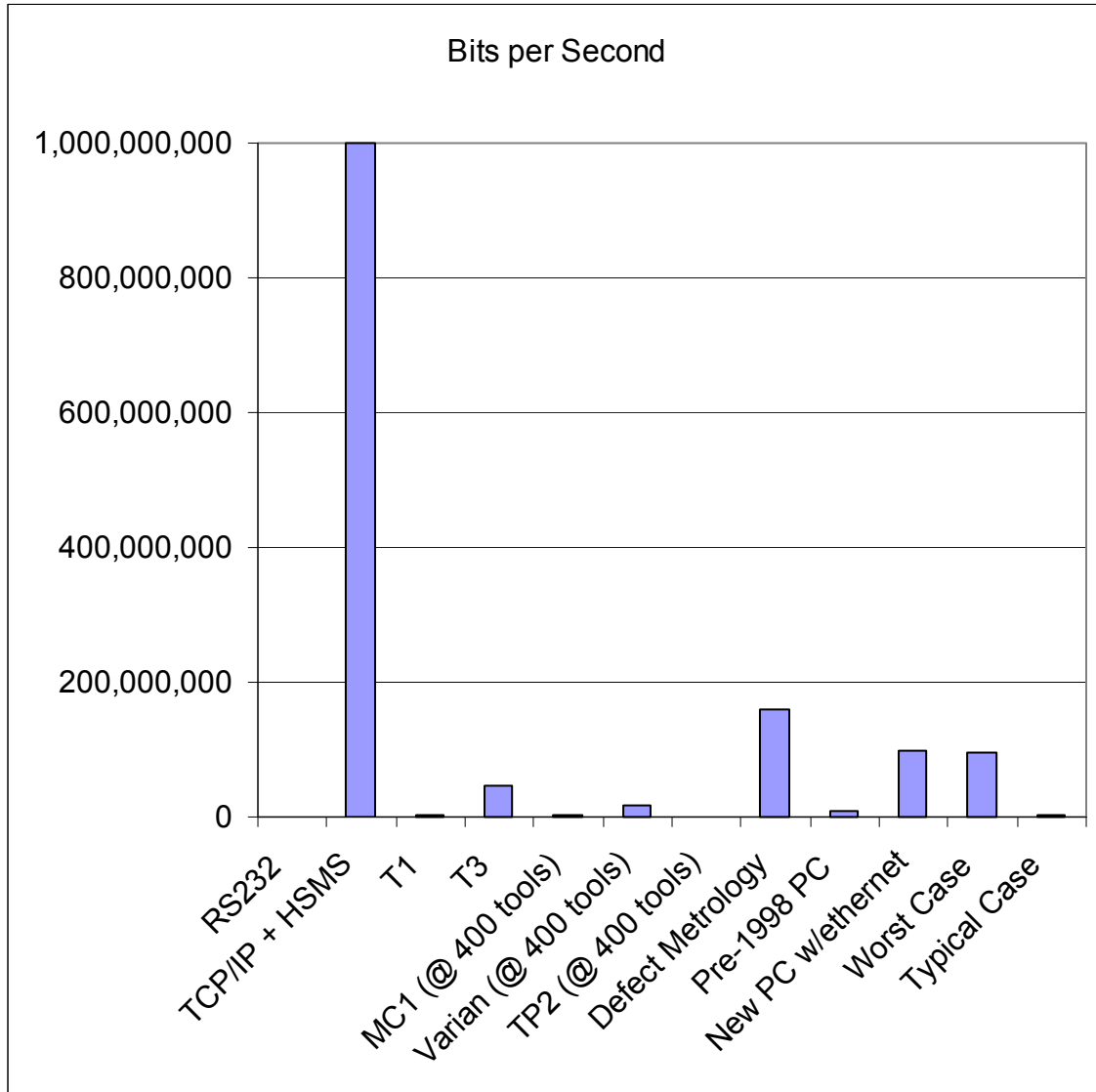
The typical case scenarios is characterized by 10 tools transmitting data at the burst rate of 5000 variables per second and the other 390 fab tools transmitting data at a monitoring rate of 50 variables per second. So that would be a monitoring rate of:

- 10 tools during Unscheduled Downtime,
- 390 tools tracking (1%, 50 variables / second)
- $(5,000 \text{ variables} * 48 \text{ bits} * 10 \text{ tools}) + (50 \text{ variables} * 48 \text{ bits} * 390 \text{ tools})$
- = 3,336,000 (3.3M) bits per second of data transmission for a typical fab

8.4 Summary

This spreadsheet graphically captures the various rates and scenarios discussed above.

Figure 1: e-Diagnostics Network Bandwidth Example Scenarios



8.5 Network Analysis

This section further focuses on the network theoretical capabilities and some actual experiences.

8.5.1 Data Throughput Analysis

Ethernet technology allows for the common packet sizes among commonly used LAN technologies. We assume the following characteristics:

- This analysis assumes a worst case 10 Mbytes tool and network backbone connection and a 20% network utilization rate. Rates at individual sites may be different.
- Switching technology is cost-effective compared to old concentrator technology.
- This analysis is done for real time (live) data collection.

The output from this data throughput analysis is provided in the following two tables:

- Table 1: Theoretical Ethernet-based performance analysis of 400 tools
- Table 2: Actual Ethernet-based performance of each tool

For the details of the formulas used to generate the table entries please see Appendix A. The Cisco data is available at www.cisco.com.

Table 1: Theoretical Analysis of 400 Ethernet-based tools

% Util of Ethernet (Thruput)	Packet rate at burst rate (1530 bytes)	Packet rate for 40 con. tools at burst rate	Packet rate for 80 con. Tools at burst rate	Packet rate for 400 con. Tools at burst rate	Packet rate for Cisco Cat 5000 Switch	Packet rate for Cisco Cat 5500 Switch
20 (2 mbps)	164	6,560	13,120	65,600	1-3 Mpps	1-25 Mpps
40 (4 mbps)	328	13,120	65,600	131,200	1-3 Mpps	1-25 Mpps

Table 2: Actual Analysis of 400 Ethernet-based Tools

Data size per transfer (bytes)	Packet rate at burst rate (1530 bytes) at 2 mbps	Number of packets to be transferred at burst rate	Estimated time for transfer (ms)
32,100	164	21	130
64,200	328	42	260

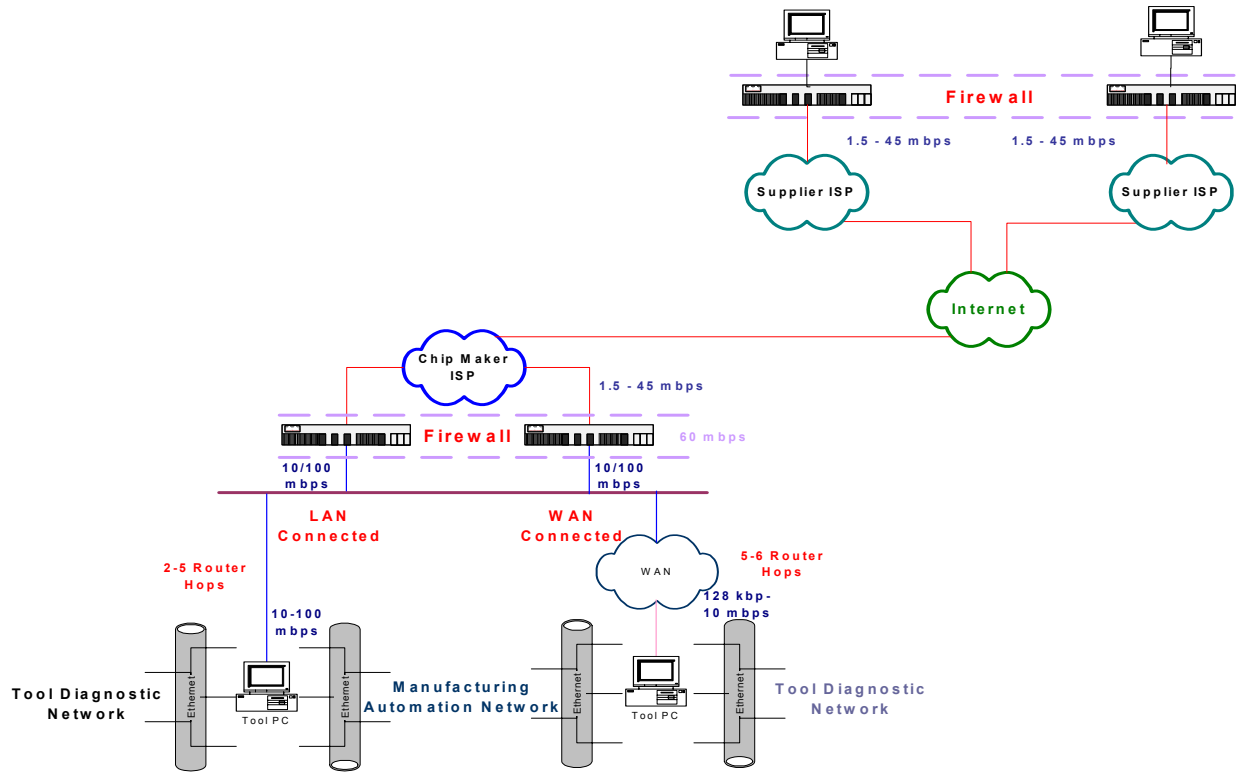
8.5.2 Data Latency Analysis

The following observations are made relative to data latency:

- A large number of router hops is expected from tool to supplier support center.
- We should expect between 1-6 hops within the customer (fab) environment with some paths being all LAN based and other having at least one WAN link.
- Internet performance and availability typically are more unreliable than Intranet.
- State of art in Firewall throughput is about 60 mbps
- We should expect high latency when traversing through WAN links and the Internet.
- e-Diagnostics applications and products must have larger timeouts (2-3 minutes) and retries (5 or higher)

Figure 2, high level e-Diagnostics Network Topology, is offered as an example of a configuration.

Figure 2: e-Diagnostics Network Topology



8.6 Conclusions

The following conclusions are derived from this network bandwidth analysis.

- Given the data requirements of e-Diagnostics, RS232 is inadequate.
- Internal fab networks supporting TCP/IP with HSMS will be sufficient to support e-Diagnostics.
- External networks are potentially (likely) to be an issue. Each point in the configuration should be review locally. It is possible that a dedicated T3 may be needed to support e-Diagnostics capabilities.
- As currently defined level 0 in the 5 level capability model is the most network intensive operation requiring the largest delta in network bandwidth. This is primarily due to the video requirement at level 0.

- Data storage and length of retention is a major issue. It is calculated that data at the typical level would require 6,415.2 gigabytes of storage (without compression) for 6 months of captured data.

This analysis did not include any data encryption calculations.

9 Single Wire Guideline

This section defines a guideline for the number of logical and physical connections between a production tool and the factory network.

9.1 Single Wire Considerations

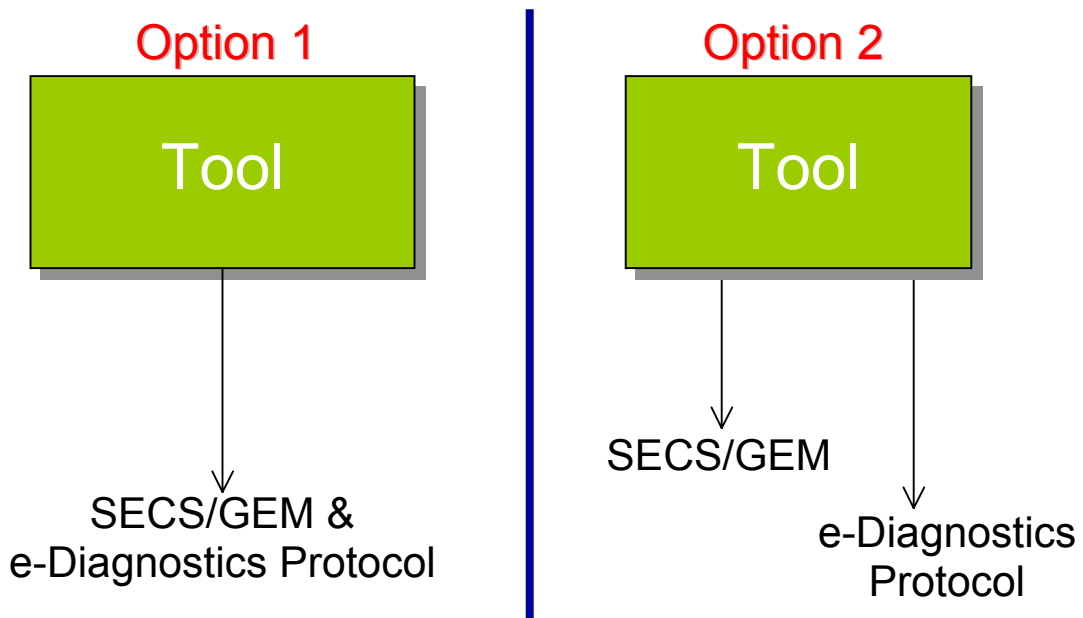
- All e-Diagnostics communications (request and reply) go through e-Diagnostics port
- Only e-Diagnostics messages are accepted on the e-Diagnostics port
- The tool must be smart enough to ensure proper wafer processing. No compromises to equipment performance are allowed because of other requests including e-Diagnostics
- Temporary Impacts to throughput due to e-Diagnostics may be desired and acceptable (configurable)
- Requests which would push the bandwidth (CPU or network) over the limit are rejected (return code -1 or some such) to avoid problems.
 - 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
- All e-Diagnostics functions to be configured by the customer (IC manufacturer).
- Customer performs all authorizations
- 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)
 - Some sort of e-Diagnostics state model may be necessary.

9.2 Conclusion

- e-Diagnostics connection and traditional SECS/GEM connection shall be logically separated.
- Equipment shall support single or dual network connections:
 - This allows for cost savings if low e-Diagnostics capabilities are required/desired.
 - This 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 and:
 - ensure safety, contention, and deadlock issues are handled,
 - impact on production throughput of e-Diagnostics requests must be predictable and configurable,
 - configuration must exist for the types of control the e-Diagnostics connection can have on the tool.

Figure 3: **Single Wire Guideline Graphic**



9.3 Single Wire Implementation Notes

The e-Diagnostics solution may 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.

A Appendix A - Use Cases

9.4 Capability Level 0 Use Cases

This section contains e-Diagnostics use case descriptions for capability level 0.

Use Case Name:	Authorize New Supplier Personnel
Actor(s):	Specific Supplier personnel for which e-Diagnostic authorization is being requested.
Preconditions:	<ol style="list-style-type: none"> 1. Personnel has been authorized at Supplier business to utilize e-diagnostic system at Company site(s). 2. Company and Supplier have established the physical/logical connection capabilities and are satisfied that they meet security requirements. 3. Any appropriate Business Rules are in place between Company and Supplier regarding each others use of the e-Diagnostics system.
Postconditions (success): ¹	Actor has a verifiable and unique identity known to the system, and has access to the e-Diagnostic system
Postconditions (failure): ²	N/A
Trigger:	Supplier identifies a need for the actor to have access to e-Diagnostic capabilities for the Company.

Main Success Scenario:	Step	Action
	1	Known, trusted representative from Supplier business requests system access on behalf of the actor
	2	Supplier representative provides appropriate information for the actor as well as requested privileges (e.g.): <ul style="list-style-type: none"> • Name • Contact information • Regions, sites, equipment types for which access is required
	3	System assigns unique identifier and access privileges to actor
	4	System stores actors description and associates with unique identifier
	5	System provides unique identifier to actor

Extensions: ³	Step Altered	Condition	Action or Other Use Case

¹ What is true about the world after this use case successfully completes

² What is true about the world if this use case fails for any reason

³ List of ways the Main Success Scenario might be altered based on conditions

Use Case Name:	Revoke Authorization of Supplier Personnel
Actor(s):	Specific Supplier personnel for which the e-Diagnostic authorization revocation is being requested.
Preconditions:	Authorization to perform e-Diagnostic functions needs to be revoked for the actor.
Postconditions (success): ⁴	Actor no longer has access to e-Diagnostic capabilities for a specific Company.
Postconditions (failure): ⁵	N/A
Trigger:	Either the Supplier or the Company decides that the actors access to e-Diagnostic capabilities must be revoked.

Main Success Scenario:	Step	Action
	1	Known, trusted representative from either the Supplier or the Company decides that the actors e-Diagnostic access must be revoked.
	2	Notification of the revocation for the actor is documented and sent to the appropriate personnel of both the Supplier and the Company (established Business Rule) Note: Notification must include reason for revoking privileges.
	3	System revokes the actors authorization.
	4	System logs the action into the appropriate audit file.

Extensions: ⁶	Step Altered	Condition	Action or Other Use Case
	2	Need for change in Access privileges, rather than actual revocation.	The same process would be followed, however instead of revoking access, a change in access privilege would be implemented. Again, the reason should be documented and the same notification process should happen.

⁴ What is true about the world after this use case successfully completes

⁵ What is true about the world if this use case fails for any reason

⁶ List of ways the Main Success Scenario might be altered based on conditions

Use Case Name:	Establish Remote Connection
-----------------------	------------------------------------

Actor(s):	Local Tool User, Remote User
Preconditions:	1. Use Case: "Authorize New Supplier Personnel" has been successfully executed.
Postconditions (success):	1. A properly authenticated connection between a Remote User and the local tool or e-Diagnostic Server is established which facilitates e-diagnostic activities. 2. The appropriate information is logged into the audit file.
Postconditions (failure):	1. A connection between Remote User(s) and either the local tool or the e-Diagnostic Server is not established. 2. The appropriate information is logged into the audit file.
Trigger:	1. A Company representative, authorized to initiate a Remote Connection, has requested that a connection be established. Or 2. A Remote User has decided to establish an e-Diagnostic Remote Connection which has been pre-authorized by the Company (for example; a connection into a Supplier's e-Diagnostics Server to view files for which access has also been pre-authorized).

Main Success Scenario:	Step	Action
	1	Actor initiates request for Remote Connection
	2	e-Diagnostic system challenges personnel for unique identifier
	3	Actor provides identifier to e-Diagnostic system
	4	e-Diagnostic system validates actors unique identifier and grants access according to actors privileges within the e-Diagnostic system
	5	Remote Connection is successfully achieved
	6	The activity is logged in the audit file (including requestor identity, session start time, etc.)

Extensions:	Step Altered	Condition	Action or Other Use Case
	3	Actor cancels request or does not provide identifier	System denies access
	4	Identifier validation fails	System denies access

Variations:	Step	List of variations

Non-functional requirements:	
Frequency:	
Open Issues:	

Use Case Name:	Terminate Remote Connection
-----------------------	------------------------------------

Actor(s):	Local Tool User, Remote User
Preconditions:	1. Use Case: "Establish Remote Connection" has been successfully executed.
Postconditions (success):	1. An established Remote Connection will be properly terminated. 2. The appropriate information is logged into the audit file.
Postconditions (failure):	N/A
Trigger:	1. A Local Tool User decides that they want to terminate a Remote Connection. 2. A Remote User ends their work and terminates the Remote Connection.

Main Success Scenario:	Step	Action
	1	One of the Actors decides that the Remote Connection should be terminated.
	2	The actor requests the e-Diagnostics system to terminate the Remote Connection.
	3	The system terminates the Remote Connection (potentially after validating the users intent).
	4	Activity is logged in the audit file

Extensions:	Step Altered	Condition	Action or Other Use Case
	2	Potential time-out feature	The e-diagnostic system could potentially have a time-out capability which would automatically terminate a Remote Connection after a predetermined period of time has elapsed.

Variations:	Step	List of variations

Non-functional requirements:	
Frequency:	
Open Issues:	

Use Case Name:	Remote Collaboration
-----------------------	-----------------------------

Actor(s):	Local Tool User, Remote User(s)
Preconditions:	Use Case: "Establish Remote Connection" has been successfully executed.
Postconditions (success):	<ol style="list-style-type: none"> 1. A real time (minimally) 2-way collaboration session is established between the actors. 2. Through this real-time connection the actors jointly evaluate tool performance while sharing and examining the same information/files.
Postconditions (failure):	A remote collaboration session can not be established in which the same information/files can be shared by both Local and Remote users.
Trigger:	The Local Tool User decides to establish a Remote Collaboration session with a Remote User. The Local Tool User is a Company employee who has proper authorization to initiate a Remote Collaboration Session.

Main Success Scenario:	Step	Action
	1	The Local Tool User initiates the Remote Collaboration Session.
	2	Properly authenticated Remote User(s) joins the collaboration session
	3	The actors collaborate in real time: sharing information, tool data, appropriate files, to achieve the objective of the session.
	4	The e-Diagnostics system logs any file transfers into the audit file.
	5	The Local Tool User is able to see any activities that are performed by the Remote User(s).
	6	The session ends either by the Local Tool User intentionally closing the session or the Remote User logging off of the session.

Extensions:	Step Altered	Condition	Action or Other Use Case

Variations:	Step	List of variations
	3	If the remote collaboration sessions include analysis of very large or detailed files, part of the collaboration can be completed off line, and over a period of hours, days or weeks. In Some cases this is desirable.
	3	Use of separate voice interconnects (telephone) is likely, and not discussed here.

Non-functional	NOTE: Collaboration requires one or both of the following,
----------------	--

requirements:	depending on the e-Diagnostics interface design. <ol style="list-style-type: none"> 1. Detailed Tool Performance and Operational Information in the form of a transferable file that can be reviewed simultaneously at different locations. 2. Ability of the tool interface to support multiple users, simultaneously, so that each collaborator can see the same thing at the same time.
Frequency:	
Open Issues:	

Use Case Name:	View/Download Equipment Files
-----------------------	--------------------------------------

Actor(s):	Remote User
Preconditions:	<ol style="list-style-type: none"> 1. Use Case: "Establish Remote Connection" has been successfully executed. 2. In this case the assumption is that there are Equipment files which the Company has pre authorized access by the Supplier, and it does not require that access be granted in real time. 3. A further assumption is that act of accessing the files does not impact the state of the Supplier Equipment. For example this action includes viewing or downloading, but not modification as is possible in e-Diagnostics Level 1 Capability.
Postconditions (success):	The actor is able to view and/or download Equipment files based on their defined privileges within the e-Diagnostic system.
Postconditions (failure):	The actor is not able to view of download Equipment files.
Trigger:	The actor decides to review Equipment files which are within their privilege level in the e-Diagnostic system.

Main Success Scenario:	Step	Action
	1	The actor locates and accesses the file(s) which has been pre authorized and is in accordance with their privileges within the e-Diagnostics system.
	2	If files are downloaded, the activity is captured within the audit file.
	3	The actor finishes their work and executes the "Terminate Remote Connection" use case.

Extensions:	Step Altered	Condition	Action or Other Use Case

Variations:	Step	List of variations

Non-functional requirements:	
Frequency:	
Open Issues:	

¹ What is true about the world after this use case successfully completes
² What is true about the world if this use case fails for any reason
³ List of ways the Main Success Scenario might be altered based on conditions
⁴ List of possible variations that don't affect the flow of the Main Success Scenario

9.5 Capability Level 1 Use Cases

This section contains e-Diagnostics use case descriptions for capability level 1.

Use Case Name:	View Remote Equipment Configuration and State
-----------------------	--

Actor(s):	Tool Owner, Remote Service Providers, Tool Manufacturer
Preconditions:	Level 0 Connectivity Remote Service Providers' Authorization Level meets or exceeds security level to view tool state/configuration.
Postconditions (success):	Remote Service Providers is able to view equipment state, data, and behavior.
Postconditions (failure):	Remote Service Providers is not able to view equipment state, data, and behavior.
Trigger:	Remote Service Providers selects the "View Current Configuration" option from Use Case "Work and Existing Issue" or "Open a New Issue" or "Work a Related Issue".

Main Success Scenario:	Step	Action
	1	Local Tool Owner initiates a request for remote service.
	2	Remote Service Providers and Local Tool Owner establish connection.
	3	Remote Service Providers and/or Local Tool Owner view current configuration.
	4	Remote Service Providers or Local Tool Owner terminate the connection.

Extensions:	Step Altered	Condition	Action or Other Use Case

Variations:	Step	List of variations
	1	Remote Service Providers initiates request for remote service connection.
	2	Remote Service Providers establishes connection independently.
	3	Remote Service Providers views current configuration independently.

Non-functional requirements:	Note: this capability is NON-INVASIVE.
Frequency:	As needed.
Open Issues:	Tool Must Create a Log of Remote Sessions

Use Case Name:	Change Remote Equipment Configuration /Operation
-----------------------	---

Actor(s):	Tool Owner, Remote Service Providers, Tool Manufacturer
Preconditions:	Level 0 Connectivity Remote Service Providers' Authorization Level meets or exceeds security level to perform requested action. Tool is NOT in Production state.
Postconditions (success):	Remote Service Providers are able to perform actions that affect equipment state, data, and behavior. Remote Service Providers and Local Tool Owner are able to view the new configuration. Configuration change(s) are logged. Tool should be able to be brought back into manufacturing state successfully.
Postconditions (failure):	Remote Service Providers are not able to perform actions that affect equipment state, data, and behavior. Or, Remote Service Providers and Local Tool Owner are not able to view the new configuration. Or, . Configuration change(s) are NOT logged. Tool not able to be brought back into Manufacturing state successfully.
Trigger:	Remote Service Provider selects the "Change Current Configuration" option from Use Case "Work and Existing Issue" or "Open a New Issue" or "Work a Related Issue".

Main Success Scenario:	Step	Action
	1	Local Tool Owner initiates a request for remote service.
	2	Remote Service Providers and Local Tool Owner establish connection.
	3	Remote Service Providers or Local Tool Owner change current configuration and/or executes specific action(s) changing tool state.
	4	Remote Service Providers, Local Tool Owner, or Tool update change log.
	5	Remote Service Providers and Local Tool Owner view new configuration and/or results of executed action(s).
	6	Remote Service Providers or Local Tool Owner terminate the connection

Extensions:	Step Altered	Condition	Action or Other Use Case

Variations:	Step	List of variations
	1	Remote Service Providers initiates request for remote service connection.
	2	Remote Service Providers establishes connection independently.
	3	Remote Service Providers views current configuration independently.

Non-functional	Note: this capability is INVASIVE.
----------------	------------------------------------

requirements:	
Frequency:	As needed.
Open Issues:	Tool Must Create a Log of Remote Sessions (Level 0 Requirement?)

Use Case Name:	Monitor Remote Equipment Operation in Real Time
-----------------------	--

Actor(s):	Tool, Tool User, Remote Service Providers, Tool Manufacturer
Preconditions:	Level 0 Connectivity Remote Service Providers' Authorization Level meets or exceeds security level to view tool state/configuration.
Postconditions (success):	Ability to Monitor Tool Performance as if on Site (In Situ)
Postconditions (failure):	Inability to determine performance characteristics or Monitor Tool Performance
Trigger:	Isolate a Problem or Issue or else for Routine Monitoring or Else Training

Main Success Scenario:	Step	Action
	1	Local Tool Owner initiates a request for remote service.
	2	Remote Service Providers and Local Tool Owner establish connection.
	3	Remote Service Providers and/or Local Tool Owner view .Log Files and/or In Situ (real-time) data.
	4	Remote Service Providers or Local Tool Owner terminate the connection.

Extensions:	Step Altered	Condition	Action or Other Use Case

Variations:	Step	List of variations

Non-functional requirements:	
Frequency:	As Needed, Continuous, and/or configurable intervals
Open Issues:	Tool Must Create a Log of Remote Sessions (Level 0 requirement)

Use Case Name:	Data Storage
-----------------------	---------------------

Actor(s):	Tool, Tool User, Remote Service Providers, Tool Manufacturer
Preconditions:	Level 0 Connectivity
Postconditions (success):	Record all States and Available Signals of the Tool
Postconditions (failure):	Less than Complete Ability to determine what happened on the tool
Trigger:	Routine Operation for Potential Audit or else Problem Resolution

Main Success Scenario:	Step	Action
	1	Tool is Put in the state of data storage (alternative is don't store data).
	2	Data are acquired and utilized for off-line processing and evaluation
	3	
	4	

Extensions:	Step Altered	Condition	Action or Other Use Case

Variations:	Step	List of variations
	1	One or multiple notifications for the same trigger event.

Non-functional requirements:	Note: Data Storage should be minimally invasive and provide for off line post-processing.
Frequency:	Continuous and/or configurable intervals
Open Issues:	Data Latency, Archive Duration

9.6 Capability Level 2 Use Cases

This section contains e-Diagnostics use case descriptions for capability level 2.

Use Case Name:	Automated Data Reporting and Analysis
-----------------------	--

Actor(s):	Equipment User, Equipment Manufacturer
Preconditions:	Level 1 Functionality
Postconditions (success):	Automated Reports are Provided to Actors
Postconditions (failure):	Raw Data are the only source of information on tool performance
Trigger:	Routine Operations

Main Success Scenario:	Step	Action
	1	Generate "Report and Analysis" State is specified
	2	Electronic Automated Reports are created without user intervention.
	3	
	4	

Extensions:	Step Altered	Condition	Action or Other Use Case

Variations:	Step	List of variations

Non-functional requirements:	
Frequency:	Routine Operations
Open Issues:	

Use Case Name:	Data Compression
-----------------------	-------------------------

Actor(s):	Equipment User, Equipment Supplier
Preconditions:	Level 1 Functionality
Postconditions (success):	Information is Retrieved from the Tool in a Format that is Significantly Compressed, as compared with the Pertinent Raw Data from which it is derived.
Postconditions (failure):	Inability to compress raw data
Trigger:	Routine Operations

Main Success Scenario:	Step	Action
	1	Condense the raw data associated with equipment operation into a "smaller space."
	2	User statistical methods or data compression or both
	3	Manipulate condensed form of information in order to make decisions or else resolve problems.
	4	

Extensions:	Step Altered	Condition	Action or Other Use Case

Variations:	Step	List of variations

Non-functional requirements:	
Frequency:	Routine Operation
Open Issues:	

9.7 Capability Level 3 Use Cases

This section contains e-Diagnostics use case descriptions for capability level 3.

Use Case Name:	Predictive/Proactive Equipment Self-Diagnosis
-----------------------	--

Actor(s):	FAB Maintenance Personnel, Equipment Supplier
Preconditions:	Level 2 Functionality
Postconditions (success):	A preemptive report is issued by the tool in order to avoid a problem.
Postconditions (failure):	An avoidable failure
Trigger:	State Estimator Determines that Corrective Action is Eminent

Main Success Scenario:	Step	Action
	1	Monitoring Software Identifies a Potential Problem
	2	A report is issues and understood
	3	Maintenance Engineer Initiates a Corrective Action
	4	Normal Operations Continue

Extensions:	Step Altered	Condition	Action or Other Use Case

Variations:	Step	List of variations

Non-functional requirements:	Parts must be available or else are delivered at the appropriate time.
Frequency:	
Open Issues:	

Use Case Name:	Decision Logic
-----------------------	-----------------------

Actor(s):	Tool, Tool Server, Factory Host
Preconditions:	Level 2 Functionality
Postconditions (success):	Tool Takes Corrective Action and Changes Operational Parameters to Assure Process Success
Postconditions (failure):	System does not make the right decision at the right time
Trigger:	Process Monitoring Suggests a change is necessary

Main Success Scenario:	Step	Action
	1	Monitoring Software Determines there is a Problem
	2	Tool Decision Software Determines an Appropriate Change
	3	Tool Implements the Change and Notifies the necessary monitors
	4	

Extensions:	Step Altered	Condition	Action or Other Use Case

Variations:	Step	List of variations

Non-functional requirements:	
Frequency:	
Open Issues:	

B Appendix B - Network Analysis Formulae and Computation

This section includes some of the elemental equations used in the Network Bandwidth Requirements investigations.

- Amount of data per real time period ($D=V*S$): 30,000 bytes (240,000 bits)
- Data overhead for full Ethernet packet: 7%
- Amount of data transported on Ethernet ($O=1.07*D$): 32,100 bytes (256,800 bits)
- Number of Ethernet Packets ($P=O/1530$): 21
- Data throughput at 20% Ethernet utilization (T): 250,000 bytes/sec (2 Mbps)
- Packet rate ($T/1530$) per second (N): 164
- Approximate time to send 21 packets ($P/N*1000$): 130 ms
- Number of Ethernet Packets for 40 concurrent tools: 840
- Number of Ethernet Packets for 80 concurrent tools: 1680
- Number of Ethernet Packets for 400 concurrent tools: 8400