

## **Communications Gap Analysis for e-Diagnostics**

**Revision 2.0**

---

White Paper	SEMI, 2000	9/26/2002
-------------	------------	-----------

SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

**EXECUTIVE SUMMARY ..... II**

**1 INTRODUCTION ..... 1**

**2 BACKGROUND – SECS AND RELATED STANDARDS ..... 3**

    2.1 COMMUNICATION TECHNOLOGY ..... 3

    2.2 USAGE & INFORMATION MODELS ..... 4

**3 E-DIAGNOSTICS USAGE MODEL ..... 6**

**4 COMMUNICATION TECHNOLOGY – SECS GAP ANALYSIS ..... 8**

    4.1 LEVEL 0 – ACCESS AND COLLABORATION ..... 8

    4.2 LEVEL 1 – COLLECTION AND CONTROL ..... 8

        4.2.1 *SECS-I* ..... 9

        4.2.2 *HSMS* ..... 10

        4.2.3 *GEM Communication State Model* ..... 13

        4.2.4 *GEM Control State Model* ..... 15

    4.3 LEVEL 2 – ANALYSIS ..... 18

    4.4 LEVEL 3 – PREDICTION ..... 18

    4.5 SUMMARY ..... 19

    4.6 CONCLUSION ..... 19

SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

---

## Revision History

---

Author	Revision	Date	Description
Mark Pendleton, DomainLogix	0.0	5/2/2001	Initial revision
James Martin, Intel Corporation	0.1	6/5/2001	Reworked executive summary and introduction sections
James Martin, Intel Corporation	0.1	8/10/2001	Reworked gap analysis sections
James Martin, Intel Corporation	0.2	8/29/2001	Added analysis of HSMS/GEM state models, conclusion sections
Mark Pendleton, DomainLogix	1.0	9/3/2001	Fine-tuned document language in all sections
James Martin, Intel Corporation	1.0	9/12/2001	Final edit for 1.0 revision, added headers/footers, revision history.
James Martin, Intel Corporation	2.0	6/14/2002	Revision to correct interpretation of E30.

This is a white paper produced by the SEMI Diagnostic Data Acquisition Task Force. No part of this document is to be construed as an official or adopted standard.

SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

---

## **Executive Summary**

SECS provides the ability for computer-controlled process and metrology tools from a variety of vendors to communicate with various types of host computers using a standard protocol. The SECS communication protocol as defined is split into two standards. SECS-I (SEMI E-4) addresses the way in which messages are sent between the equipment and a factory host. SECS-II (SEMI E-5) describes a set of messages that can be exchanged using SECS-I as the medium.

These standards are the foundation for two related standards, which have become today's expectation for automation support in semiconductor manufacturing. HSMS (SEMI E-37) extends the SECS-I standard to function over IP instead of RS-232. GEM (SEMI E-30) describes which messages from the SECS-II message set should be used for communicating what kind of information.

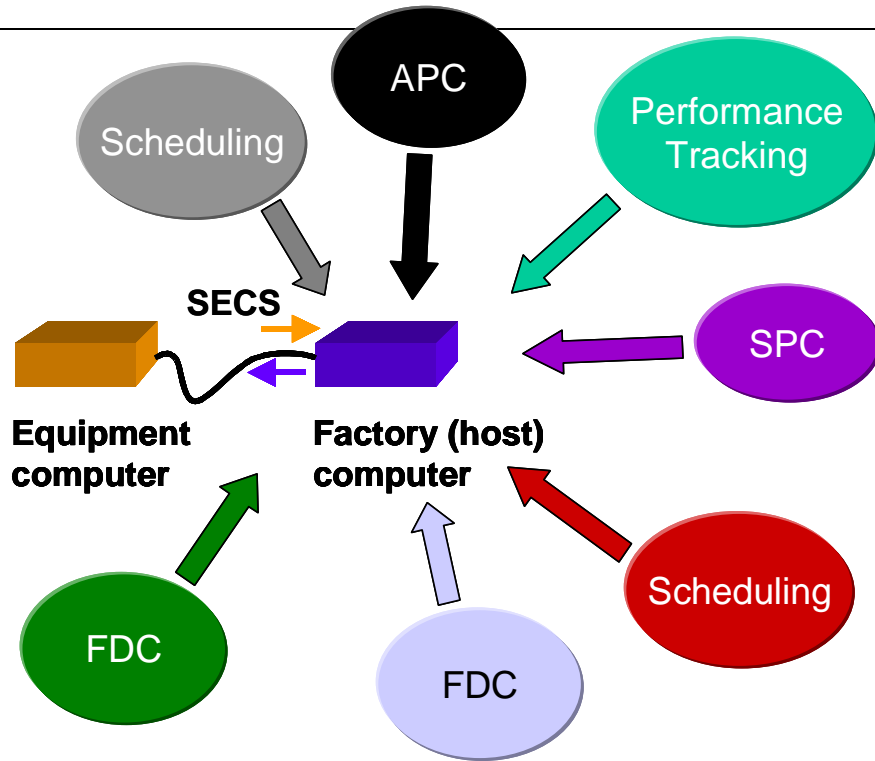
While these standards have evolved and matured, significant changes have taken place in the semiconductor automation environment in which they are used that limit their efficacy in modern manufacturing systems.

### **Increased Integration**

In the manufacturing environment, automation systems have become increasingly more integrated, and the expectation of what a factory host is required to do has become more sophisticated.

Typical expectations of a factory host system today include:

- Recipe selection, loading, and execution
- Extraction of engineering data for statistical process control
- Interpretation of event data for utilization tracking and status boards
- Coordination of equipment processing activity with material delivery systems
- Communication of equipment loading for scheduling systems
- Run-to-run recipe parameter modification for APC systems
- Extraction of trace data for fault detection systems



These responsibilities are assigned to the factory host in part as a result of the single-client nature of the SECS standards. It is not possible for arbitrary manufacturing services to obtain information directly from the equipment, so the factory host must be extended to facilitate these expectations.

### **Increased Computing Resources**

Compute power available on semiconductor equipment has increased significantly to the point where it could be considered on par with, or superior to, that of the factory host. These equipment typically include a workstation or server systems running commercial operating systems with complete network communication stacks. This is a significant advantage compared to resources available to smaller scale devices controlled via embedded logic.

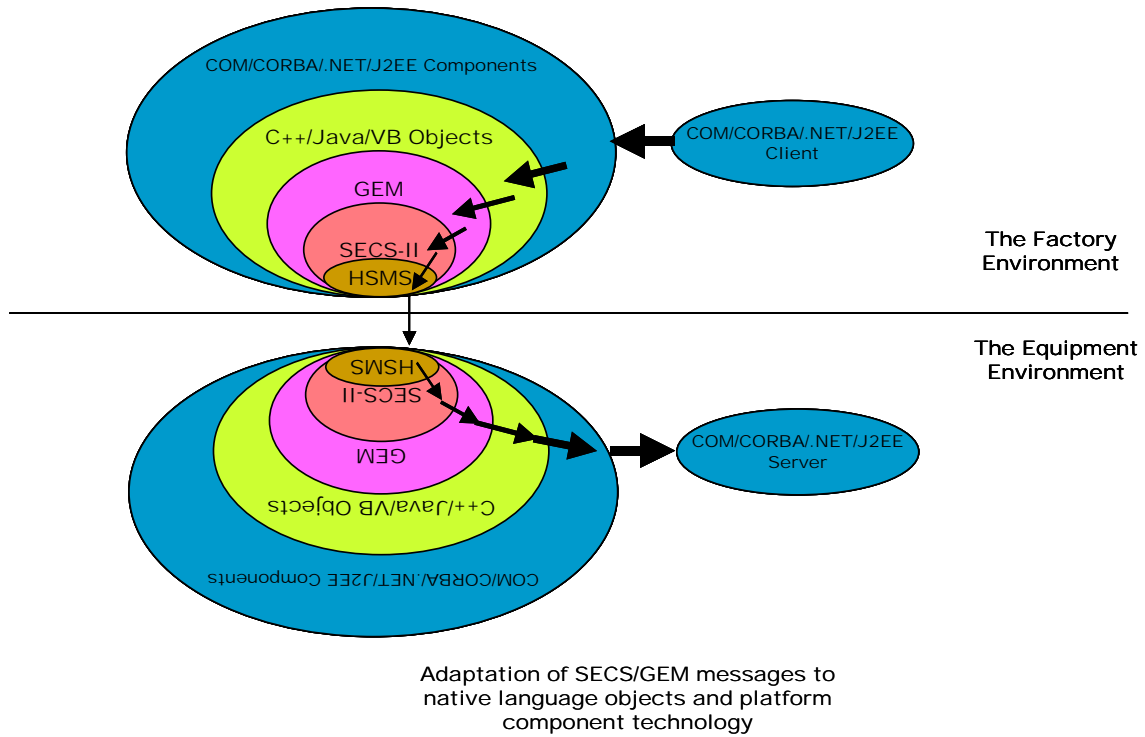
### **Evolving Software Technology**

Software development technologies and methodologies have evolved at a rapid rate since the adoption of SECS and the software industry investment in standardization has strengthened significantly. These changes have outpaced advancements in semiconductor equipment communication technology, yet the equipment and host systems software on either end of current semiconductor communication links has tended to evolve in step with current technologies.

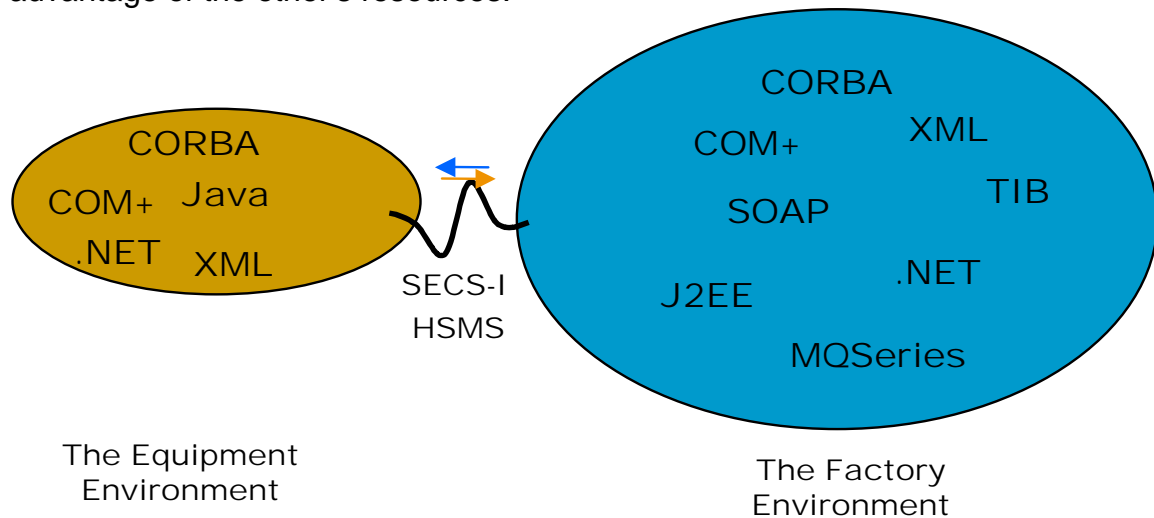
The gap between modern software development and the SECS communication technologies naturally leads to the development of adaptation software in both

SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

factory host and equipment systems to enable the two different paradigms to work together.



While this allows factory and tool systems to individually take advantage of modern technologies and standards, SECS represents a barrier to the expression of resources and services directly via these standards, since it remains proprietary to the semiconductor industry. The net effect of this is that neither side of the equipment—factory communication path is able to take direct advantage of the other's resources.



SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

---

## **The Network**

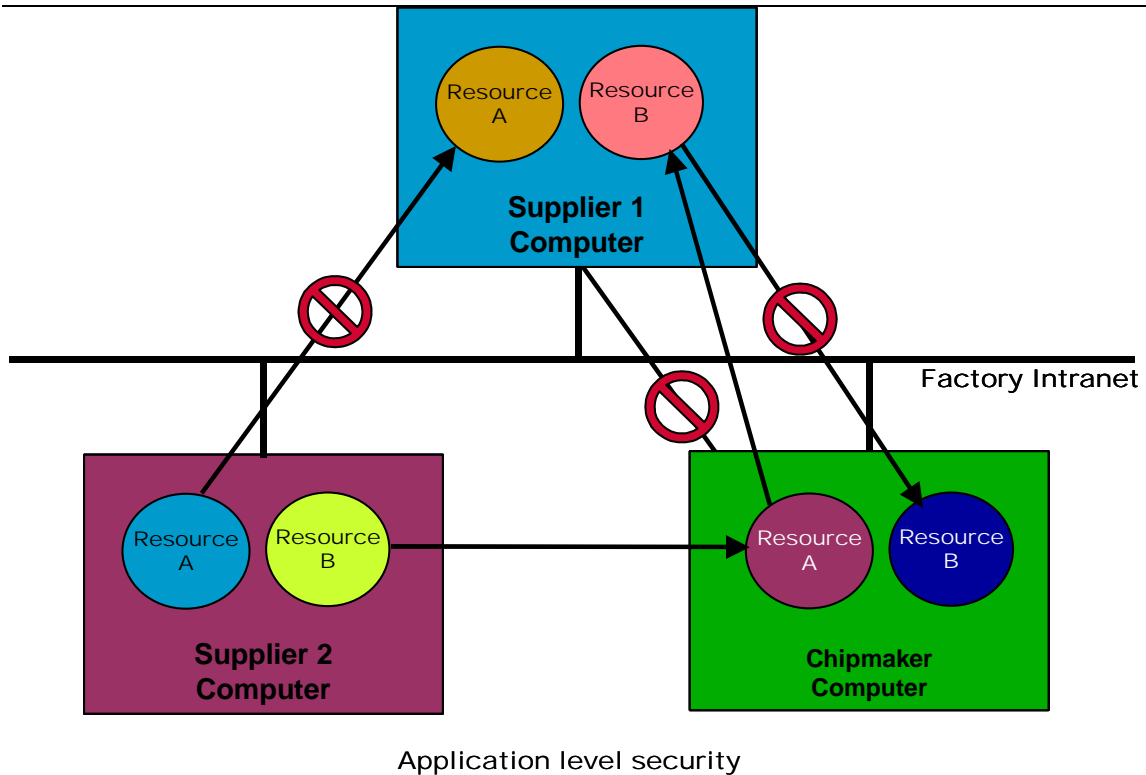
One aspect of the evolution of computing technologies of particular interest has been the increased viability of the Internet for enabling business transactions and relationships. The e-Diagnostics program baseline takes advantage of these developments to provide global, rapid, and efficient communication between semiconductor manufacturers and equipment suppliers in maintenance and problem resolution.

Providing network access to semiconductor equipment in order to support e-Diagnostics (or any other) objectives introduces new expectations with respect to security in equipment communication. Prior to placing equipment communications resources on the intranet, a factory could be relatively certain that exchange of information between the equipment and its environment was limited to the connection of the serial cable from equipment to the trusted factory host.

While placing equipment on factory networks improves the potential and flexibility for direct access to the equipment, it also increases the risk of accidental or malicious misuse of both equipment and factory resources by any entity connected to the network.

Some of this risk may be mitigated through careful planning of the network infrastructure that enables this communication, but this by itself is insufficient to protect such a distributed system. Each resource (files, services, objects, etc.) must have the ability to employ security mechanisms at both the operating system and application level to provide the best possible defense against accidental or intentional damage to the system or the business.

The following diagram illustrates the protection of supplier and chipmaker computing resources from unauthorized access by other resources on a factory intranet via application level security. With respect to equipment communication, this may correspond to controlling access to different types of requests (data acquisition vs. control requests such as executing a process program).



The SECS communication protocol does not currently support fundamental computing security constructs such as identity, authentication, or authorization. This gap in the SECS standard originates from the assumption that the only communication taking place between the equipment and its environment would come from a trusted computer on the other end of an RS-232 cable. This can no longer be considered a valid assumption when this communication occurs over a network.

The combination of the above factors, each one an important component of the approach used for e-Diagnostics and other programs in the semiconductor industry, highlights changes that would have to be made in the technology and in the current standards in order to enable such programs to achieve their goals.

This gap analysis details these issues and recommends that an alternative to the current SECS-II and GEM standards be developed for the implementation of e-Diagnostics capability.

SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

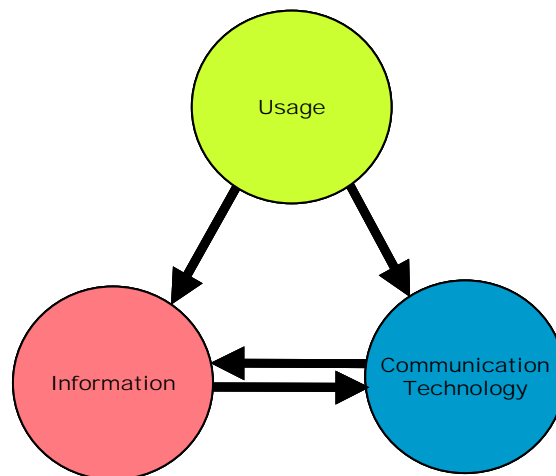
## 1 Introduction

This document examines and evaluates potential gaps that exist between e-diagnostic requirements as currently defined by International SEMATECH (ISMT e-Diagnostics Guidebook, Version 1.0) against the functionality provided by the SECS (SEMI E-4, E-5, E-37) communication standards.

Making changes to the communication standard for semiconductor equipment, however, is a non-trivial undertaking, so it is important to ensure that the motivation and associated impact of change is well understood.

The approach to this analysis has therefore been organized into the following 3 basic categories, each with a degree of interdependence as illustrated in the figure below:

1. Usage Model
2. Information Model
3. Communication Technology



The **Usage Model** describes what the system is supposed to do – what range of problems is to be solved by the system and how will it be used. How the system is to be used helps to determine an information model and the appropriate use of communication technology. “The system” in this case is understood to be semiconductor manufacturing equipment.

The **Information Model** organizes the concepts and behavior described by the usage model into components, classes, messages, data, and any other logical artifacts necessary to support the Usage Model with software. How information

SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

---

is modeled will be influenced by the communication technology used as well as the organization suggested by the Usage Model.

**Communication Technology** is the medium by which information is exchanged between the system and its clients/users/actors. Communication Technology is chosen according to the types of usage the system is expected to provide, and to the degree to which it can support the needs of the Information Model.

Because these aspects of system definition are interrelated it is important to consider each of them in suggesting changes to the communication technology.

The next section provides a high-level background description of the SECS protocol and SECS-related standards, followed by a discussion of the expected usage from an e-Diagnostics perspective (other perspectives will be considered as well). Subsequent sections consider gaps between the expected usage and what the SECS protocol provides.

SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

---

## **2 Background – SECS and Related Standards**

As discussed previously in this document, the current standard for communication with semiconductor equipment is based on SECS, the SEMI Equipment Communication Standard. SECS is actually made up of two separate standards, SECS-I (SEMI E-4) that defines the message transfer protocol and SECS-II (SEMI E-5) that addresses message content.

### ***2.1 Communication Technology***

#### **SECS-I / SEMI E-4 and E-37**

SECS-I defines how messages are transferred to and from semiconductor manufacturing tools. SECS-I divides the base level communication protocol into logical layers with each layer building upon the services offered by the previous layer. Specifically, the layers from bottom to top are: Physical, Block, Message and Transaction (see the SEMI E-4 standard for details on each of these layers).

The SECS-I protocol as defined by SEMI E-4 supports a point-to-point connection approach that is single client capable, based on the RS-232 standard. SECS-I is considered to be an asynchronous protocol where access is based on contention methods with line management addressed through collision detection methods.

To address issues with communication throughput inherent in the RS-232-based standard, SEMI developed HSMS (SEMI E-37, High-Speed SECS Message Services). HSMS provides for higher-speed communications over TCP/IP thereby improving throughput while retaining the SECS-I messaging concepts.

#### **SECS-II / SEMI E-5**

SECS-II defines messages which can be exchanged between the host and the tool. This standard addresses three major items; Data Item Formats, Standard Data Item Definitions and Standard Message Structure. These items can be viewed as upper layers of the logical protocol and rely on the lower SECS1 or HSMS layers.

In SECS-II, messages are grouped into Streams and the action associated with a Stream is called a Function. Streams 1-13 are currently defined in SECS-II and address message classes such as Equipment Constants, Alarms, Process Program Management. Streams 14-63 have been reserved for future use with Streams 64-127 categorized as user definable.

The Functions 0-63 are reserved by the SECS-II standard for use with supported Streams (note that the same function code may mean different things depending on what Stream it is associated with). Functions 64-255 are user definable. Odd

SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

---

number transactions are primary messages with even number messages being associated replies.

## **2.2 Usage & Information Models**

### **GEM / SEMI E-30**

As SECS-II was adopted it became clear that more definition was needed regarding the way Streams and Functions were used. This led to the development of the Generic Equipment Model (GEM/ SEMI E-30), which defines a minimum set of capabilities that must be supported by tools, and how they should use messages from the SECS-II message set to provide those capabilities.

Examples of GEM specifications are capability descriptions of connection management, data collection, alarm management, control messaging, and process program management. Each of these capabilities is mapped to an appropriate SECS-II message set.

### **Specific Equipment Models**

Even with the improvement in consistency introduced by the GEM standard, the specification was found to be too generic to accommodate the behavioral specification of a variety of manufacturing equipment. To address this issue, SEMI undertook the development of Specific Equipment Models (SEM's).

A SEM describes required state machines, which events should be communicated by the equipment under what circumstances, what the message content should be, and which data types are to be used in these messages. This information is intended to be valid for a specific class of equipment.

SEM's developed to date include E-30.1 (Inspection & Review SEM), E30.2 (Handler SEM), E30.3 (Tester SEM), E-82 (Inter/Intrabay SEM), E-88 (Stocker SEM), and E-91 (Prober SEM). Of these, E-82 and E-88 have the widest acceptance and implementation within the industry.

### **OSS / SEMI E-39**

Experience with standards development led to the desire to abstract the language of specifications so that they were not expressed solely in terms of the SECS messaging standard. Object-oriented modeling was chosen as a way to represent concepts and behavior in semiconductor equipment without committing to a specific communication technology.

To this end, the Object Services Standard (OSS) was developed in 1995. Its purpose was to "provide general terminology, conventions and notation for describing behavior and data in terms of objects and object attributes". OSS

SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

---

based its terminology and notation on Rumbaugh's Object Modeling Technique (OMT), one of the many precursors to the Unified Modeling Language.

OSS describes the terms, concepts and notation to be used in further SEMI standards development. In addition, OSS describes fundamental services that any entity modeled as a class must support. It also specifies concepts and terminology to be used when describing the instantiation of a system of classes in an object model, including a nomenclature for identifying specific objects in such a system.

All SEMI equipment software standards developed since the introduction of OSS have used the terminology and concepts presented in OSS as the basis for specification. Behavior not covered by GEM or the SECS-II mapping in OSS is mapped to the reserved stream range 15-64 or SECS-II messages not included in GEM.

Standards based on OSS include E-40 (Process Job Management), E-41 (Exception Management), E-42 (Recipe Management), E-53 (Event Reporting), E-54 (Sensor/Actuator Network Standard), E-87 (Carrier Management), E-90 (Substrate Tracking), E-94 (Control Job Management), and E-98 (Object Based Equipment Model).

### **OBEM/SEMI E-98**

The Object-Based Equipment Model (OBEM) standard (in provisional status as of this writing) has been developed to provide a mechanism for revealing a representation of the physical structure of manufacturing equipment to clients, information that is not currently supported by the existing SECS-II message set.

OBEM decomposes equipment into a hierarchy of Modules, Subsystems, and Sensors/Actuators. Each element in the OBEM class hierarchy has an associated minimal state model and a set of attributes and methods ("services" in OSS parlance) in support of its role in the hierarchy. These are mapped to the SECS-II stream 14 messages established by OSS. The existing SEMI OSS-based standards are deferred to for describing the functional capability supported by these classes.

SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

---

### **3 e-Diagnostics Usage Model**

In order to determine if a specific technology has merit it first must be discussed in the context of specific objectives. A technology is created to solve a specific class of problems, and if applied to problems outside of its domain will have either limited value or require additional integration work to achieve objectives.

This section describes the usage of the e-Diagnostics system in order to provide context for considering the applicability of the SECS communication protocol.

#### **Guidelines**

Additional detail on the capabilities described in this section may be found in version 1.0 of the International SEMATECH e-Diagnostics Guidebook.

#### **e-Diagnostics Capability Taxonomy**

Capabilities described in the Guidebook are organized into the following 4 levels:

Level 0 - Access and Remote Collaboration

Level 1 - Collection and Control

Level 2 - Analysis

Level 3 –Prediction

This section provides a brief review of each capability.

#### **Level 0 – Access and Collaboration**

Access refers to the ability of an e-Diagnostics system user to sign on to a system from anywhere internal or external to the factory, locate specific equipment installations, and transfer files to and from the equipment or equipment environment. It includes the ability to provide identity both people (users) and equipment so that privileges and access controls can be assigned and enforced.

Collaboration refers to the ability of an e-Diagnostics system user to participate in a virtual conferencing session with equipment engineers, owners, and operators for the purpose of troubleshooting a problem. It is expected that a user at the equipment console would be able to participate in collaboration sessions.

SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

---

### **Level 1 – Collection and Control**

Collection refers to the ability to extract various types of data (described in the Data Taxonomy guidelines) from the equipment to facilitate troubleshooting and equipment health monitoring.

It includes the movement of this data off-tool to storage systems and applications for subsequent analysis as well as live status monitoring. Movement of this data must be possible independent of the establishment of the control relationship (ONLINE or OFFLINE) with the factory host.

Control refers to the ability of an e-Diagnostics user to use the system to locate specific equipment installs and sign on to the tool as though they were physically present at the console with the ability to perform specific equipment actions as they would from the equipment console.

### **Level 2 – Analysis**

Analysis refers to the ability to process data extracted from the equipment (or data stored on-tool) to detect trends in equipment health and performance. This may also include comparative analysis between different tool installations.

At the time of this writing, no further details regarding this capability are defined. It is possible that this capability may include both near-real-time decision making and offline analysis.

### **Level 3 – Prediction**

Prediction refers to the ability to use the results of analysis performed on collected data in order to arrive at recommendations for corrective or preventive steps to take to maintain equipment health.

As with level 2, this capability is not well defined, and may or may not include both offline as well as real-time processing.

SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

---

## **4 Communication Technology – SECS GAP Analysis**

This section analyzes the high-level capabilities described in the previous section and identifies where the SECS communication technology might possibly play a role, describing if and what gaps might exist in meeting the needs of each capability.

### **4.1 Level 0 – Access and Collaboration**

There are three capabilities included in Level 0 that are specific to the gap analysis being performed and are as follows:

1. Registration
2. File Transfer
3. Collaboration

Each is discussed in the paragraphs that follow.

Implicit in the requirement for managing equipment identity at Level 0 is the need for the registration of specific equipment installations. In addition to enabling access controls on a tool-by-tool basis, equipment registration will likely include a naming system for equipment at manufacturing sites. This need does not impact requirements for communicating with the equipment; and instead is more applicable as a factory-level service that the equipment software can avail during installation and qualification.

In addition, neither file transfer nor collaboration are activities associated directly with the physical equipment. These are features associated with the environment in which the equipment operates. The closest technological fit for supporting these capabilities will be found in self-contained applications or operating system services.

Based on these determinations, the representation of the physical equipment in a software interface will not be a prerequisite for meeting the needs of Level 0 e-Diagnostics capability, thus the SECS communication protocol is not a consideration here.

### **4.2 Level 1 – Collection and Control**

There are three capabilities included in level 1 as follows:

1. Equipment console monitoring & control
2. Equipment data collection & storage
3. Equipment data monitoring

As with registration, file transfer and collaboration in Level 0, equipment console access is an activity more closely associated with the environment in which the equipment operates than the physical equipment itself. Again, for this feature,

SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

---

the closest technological fit will be found in self-contained applications or operating system services.

Data collection is the level 1 feature that most directly involves the software interface presented by the equipment. The ability to store this data as well as the ability to monitor the current status of the equipment are dependent on the extraction of data.

The SECS communication technologies will therefore be evaluated against data collection and access control requirements from the perspective of e-Diagnostics.

For data collection, the requirements are:

1. It must be possible to collect data from the equipment in near-real-time
2. It must be possible to collect data at any time, independent of the control relationship with the host

For access control, the requirement is:

1. A single point of control of the equipment must be preserved (e.g., data collection clients must not be able to control the processing of the equipment)

For communication technologies, the data collection requirements translate into the ability to establish multiple (at least 2, in the simplest case) concurrent communication sessions with the equipment. The access control requirements translate into the ability to distinguish between clients in such a way that only one is permitted access to process control commands.

## **4.2.1 SECS-I**

SECS-I is a serial communications protocol which defines how messages and transactions are represented at the block level and how they are exchanged between two endpoints. The physical communication medium is RS-232-C.

### **4.2.1.1 Multiple Clients**

SECS-I does not support multiple independent clients without physically inserting them in the communication path between the host and the equipment via cabling.

### **4.2.1.2 Single Point of Control**

Even if multiple clients are included in the communication path between the host and the equipment, there is no mechanism in place for the equipment to distinguish between the individual message sources. This means that every client in the communication chain can send control messages to the equipment.

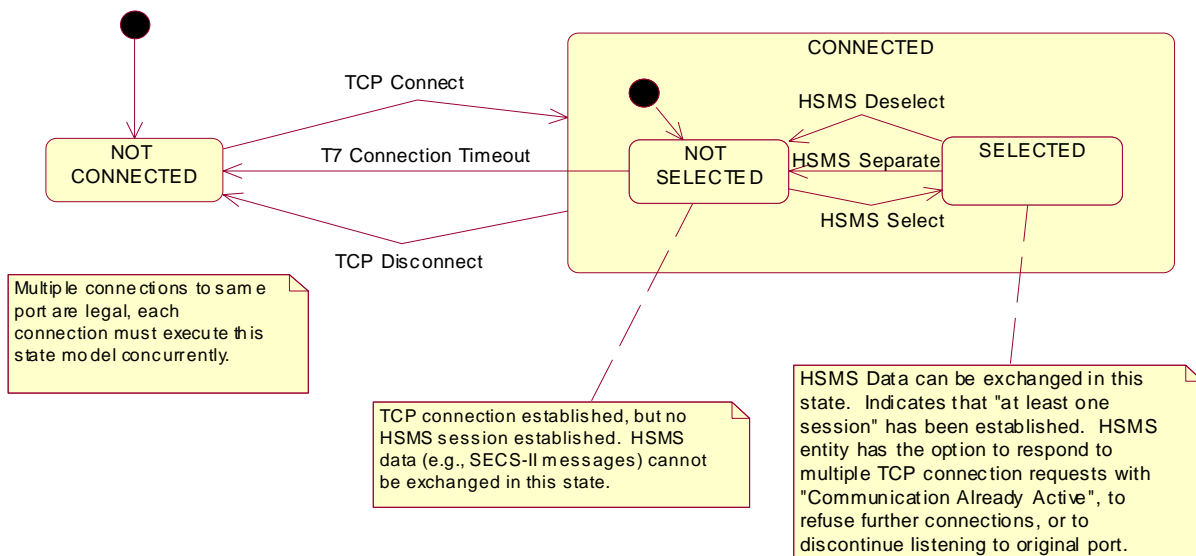
## 4.2.2 HSMS

HSMS is founded on TCP/IP, which does include support for the establishment of multiple connections to an IP/port duple. The HSMS standard is divided into 3 specifications: HSMS Generic Services (E37), HSMS Single Session (E37.1), and HSMS General Services (E37.2). Each of these will be discussed in turn.

### 4.2.2.1 HSMS Generic Services

HSMS communication begins by establishing a TCP/IP connection between two entities. The entities then agree to communicate using HSMS (via the HSMS "Select" procedure), and then begin exchanging data. The HSMS Generic Services state model is shown below:

HSMS State Model (Generic Services)



#### 4.2.2.2 Multiple Clients

As indicated in the diagram, HSMS Generic Services supports the establishment of multiple TCP/IP connections to the same IP/port combination, but requires that each individual connection retain this state model independent of all other sessions (E37-0298, section 9.2.4).

If an entity receiving TCP connect requests can only accept one connection, HSMS provides a "Communication Already Active" response code for the Select

SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

procedure which provides a graceful mechanism for supporting only a single connection (E37-0298, sections 8.2.3 and 9.2.4.1).

With this state model, HSMS Generic Services will support (but does not require those implementing HSMS to support) the establishment of multiple concurrent client sessions. Each client would establish a unique connection with the equipment (in our case), each connection communicating in parallel.

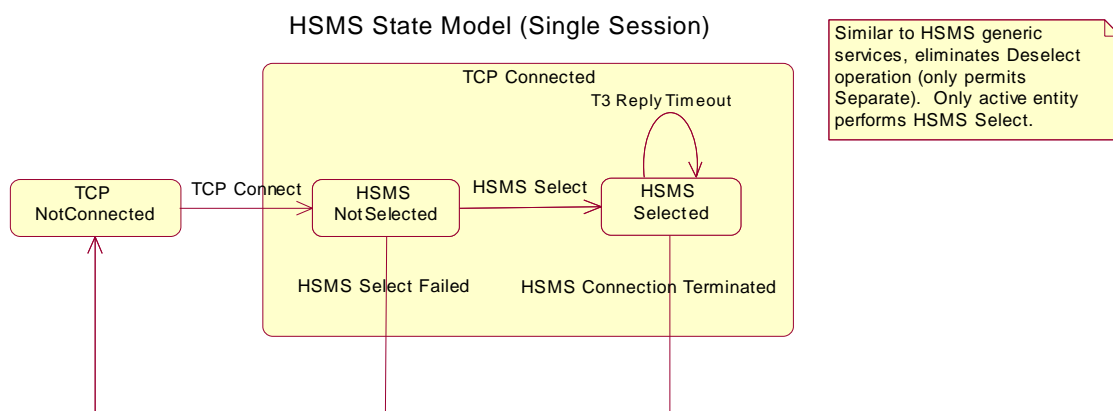
#### 4.2.2.3 Single Point of Control

HSMS does not provide a mechanism to distinguish between individual clients, except by their IP address (provided by TCP). HSMS therefore provides no facilities to enforce a single point of control. To achieve this, it would be necessary to place HSMS on top of an authenticating protocol layer, to extend HSMS to include authentication, or to build an authentication protocol into the layers above HSMS.

#### 4.2.2.4 HSMS Single-Session Mode

Single-session mode is a simplification of the HSMS Generic Services state and messaging model for entities which can only support a single connection (e.g., as a simple replacement of SECS-I communication). The following diagram illustrates the HSMS-SS state model:

As indicated in the diagram, the Deselect operation is removed, in preference to



“Separate”, and there is no session counter (a single Select procedure execution is permitted, and only while in the “Not Selected” state).

#### 4.2.2.5 Multiple Clients

Again, there is no technical limitation imposed by HSMS-SS on the establishment of multiple client connections. Each connection would maintain a separate HSMS-SS state machine.

SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

It is worth noting in the Related Information for E37.1, section R1-2, the following statement:

“For specialized applications, an equipment could accept more than one Host Connection. Coordination of activity by multiple hosts is equipment-defined.”  
 Limitations with multiple host connections will be discussed in a later section.

#### 4.2.2.6 Single Point of Control

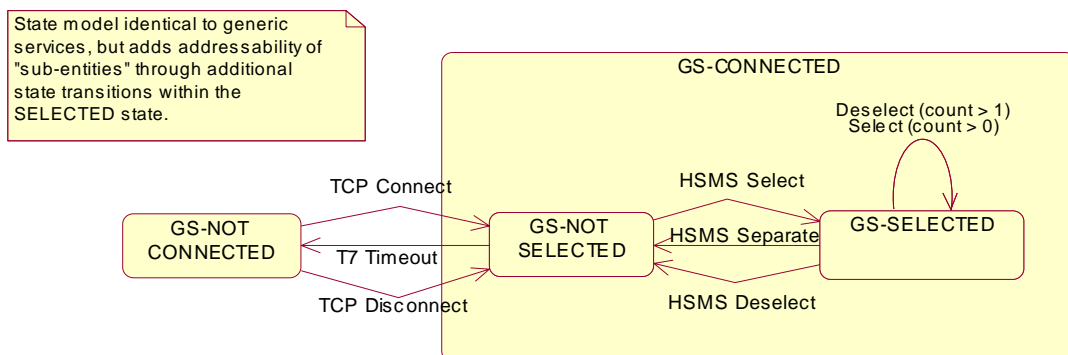
HSMS-SS does not provide authentication services, so it can not be used to support the enforcement of a single point of control.

#### 4.2.2.7 HSMS General Session (HSMS-GS)

The motivation for HSMS-GS is to subdivide one end (or both ends) of an HSMS connection into more than one individually-addressable entity (e.g., in support of complex equipment configurations where subsystems can communicate independently).

Each sub-entity receives its own session ID, established for each unique HSMS “Select” procedure. HSMS-GS adds some extensions to the HSMS Generic Services state model, shown below:

HSMS State Model (General Session)



The primary extension is in the management of selected entity lists resulting in the additional “Select” and “Deselect” transitions being permissible while in the “Selected” state.

#### 4.2.2.8 Multiple Clients

HSMS-GS does not introduce any new constraints or additional flexibility with respect to multiple clients. The state model must be maintained independently in each TCP connection as with HSMS Generic Services and HSMS-SS.

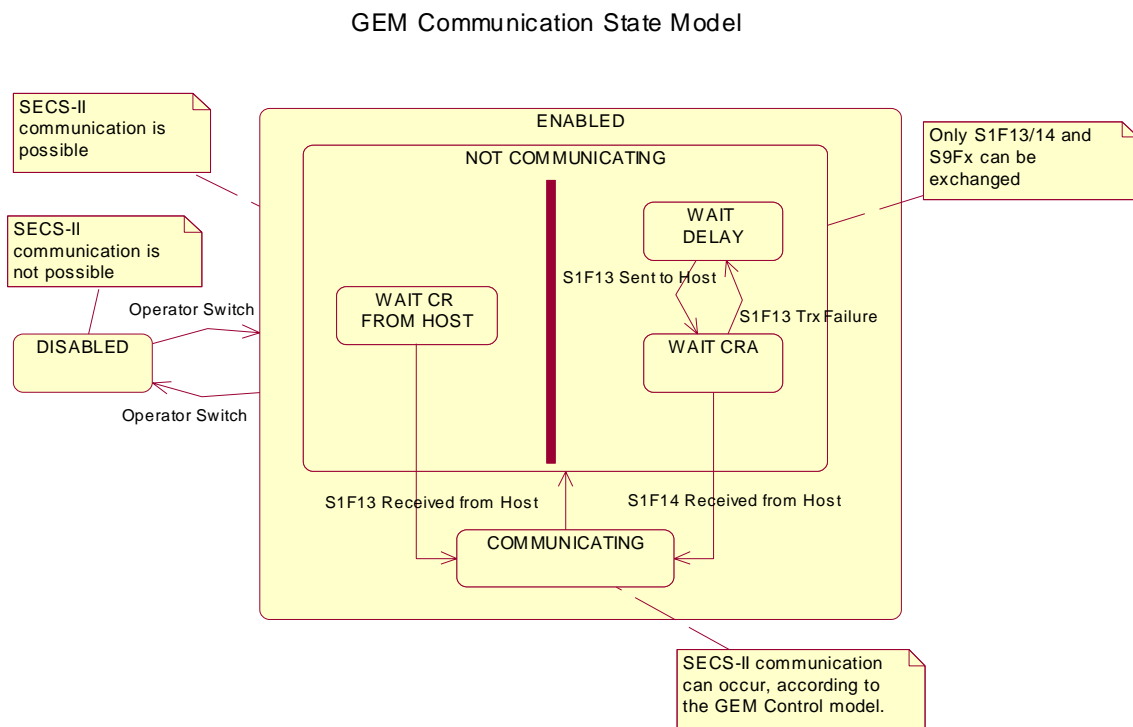
SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

#### 4.2.2.9 Single Point of Control

HSMS-GS does not provide authentication services and therefore may not be used to support the enforcement of a single point of control.

#### 4.2.3 GEM Communication State Model

The GEM Communication state model describes how equipment should regulate the ability of the controlling host to communicate using SECS-II. The following diagram provides a simplification of this state model:



Note that this state model applies to the equipment as a whole, and specifies that the operator is in ultimate control of whether or not an external entity is enabled to communicate with the host. Once the equipment has transitioned into the COMMUNICATING state, host communication is regulated by the GEM Control state model.

The specific terminology from E30 that addresses what kind of communication is controlled by the communication state model is found in section 3.2:

“The Communications State Model defines the behavior of the equipment in relation to the existence or absence of a communications link with the host.”

The term “host” is defined as: “the intelligent system that communicates with the equipment”. A “communications link” is considered established “following the

SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

---

first successful completion of any one S1,F13/F14 transaction with an acknowledgement of 'accept'."

#### 4.2.3.1 Multiple Clients

The GEM Communication state model does not directly address the issue of whether or not multiple clients can communicate with the equipment. Instead it is intended to provide a mechanism for a human operator to control whether or not the equipment is able to communicate with a client using SECS-II messages.

As E30 was originally written in an environment in which it was only possible to communicate with one client (SECS-I), it does not specify how to apply the Communication State Model in an environment where more than one concurrent SECS-II client is actively communicating with the equipment.

Specifically, in section 3.2.4, the DISABLED communication state is described as follows:

"In this state SECS-II communication with a host computer is non-existent. If the operator switches from ENABLED to DISABLED, all SECS-II communications must cease immediately."

While it is clear that this state model is intended to control communication with a "host", the definition of "host" is insufficient to clearly distinguish among multiple "hosts" with different responsibilities (a "control host" vs. a "data collection host", for example). As worded, the current GEM standard does not adequately address a multi-client SECS-II environment.

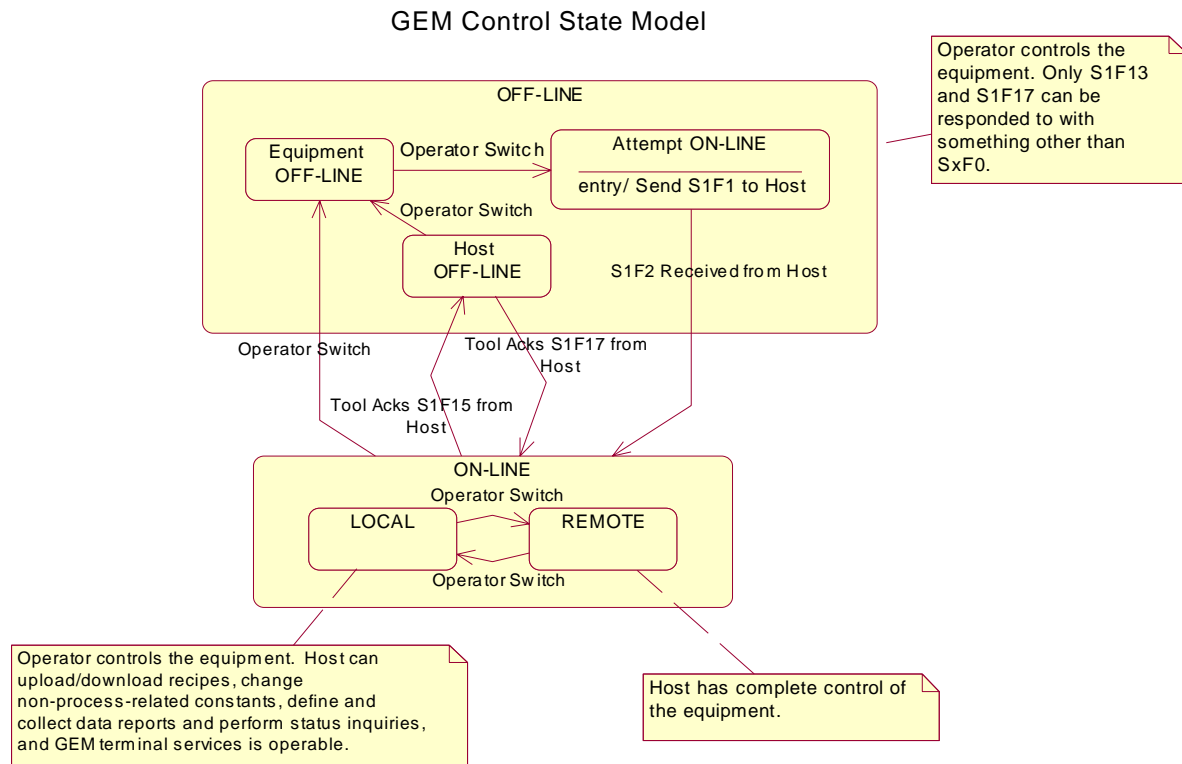
While it is a requirement to be able to disable e-Diagnostics data collection, it is not a requirement that this be controlled by the GEM Communication state model. It would therefore be necessary for E30 to distinguish between SECS-II messages originating from the controlling host and those originating from a data client, and to restrict application of the Communication State Model to communications with the controlling host only. E30 is not currently written to clearly permit this.

#### 4.2.3.2 Single Point of Control

As E30 makes no distinction in the Communication State Model between SECS-II messages originating from a controlling host and those from data-only clients, it cannot currently be unambiguously stated that the equipment can simultaneously be E30-compliant while also permitting simultaneous SECS-II sessions, some of which are not governed by the GEM Communication State Model. No conclusions can be drawn regarding any implications of the Communication State Model with respect to the single point of control requirement.

## 4.2.4 GEM Control State Model

The GEM Control state model defines three levels of control communication with equipment as well as the rules governing transitions between each level. The following diagram provides a simplification of this state model:



Note that this state model refers to the equipment as a whole, and specifies that the operator is in ultimate control of the types of control messaging that can occur between the equipment and “the host” communicating using SECS-II messages.

In the OFFLINE state, only requests to enter the ONLINE state are accepted from the host. In the ONLINE/LOCAL state, only data collection (and recipe storage, terminal services, etc.) messages are permitted. In ONLINE/REMOTE, all data collection and process control messages are permitted. Only the operator can change between LOCAL and REMOTE modes.

### 4.2.4.1 Multiple Clients

As with the Communication State Model, E30 cannot currently be unambiguously interpreted as specifying if or how the Control State Model should be applied in

SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

---

an environment where multiple “hosts” are simultaneously communicating using SECS-II.

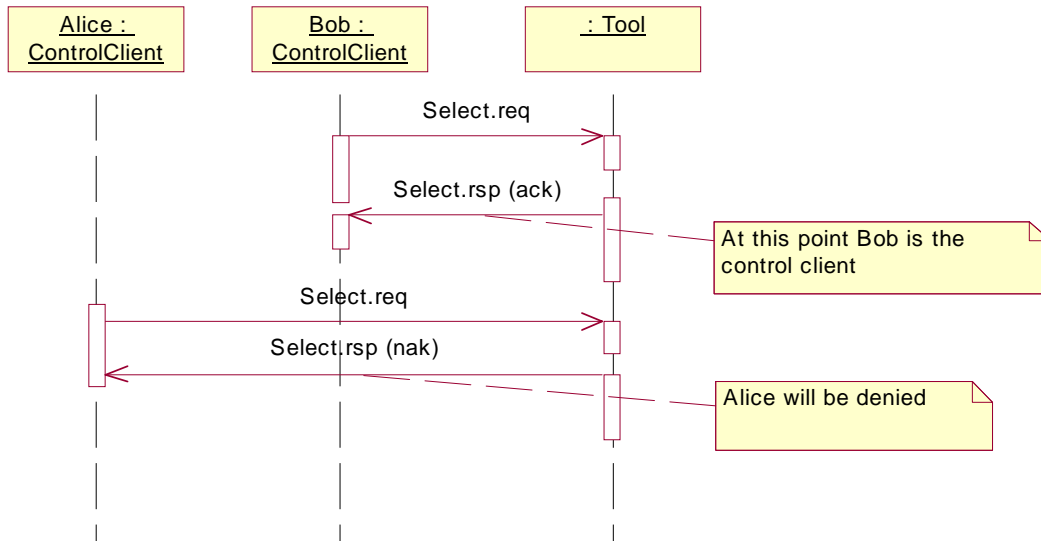
#### 4.2.4.2 Single Point of Control

As with the GEM Communication state model there is no provision in the Control state model for distinguishing between SECS-II messages originating from the controlling host and those originating from data-only clients. It cannot currently be unambiguously stated that the equipment can be E30-compliant while also permitting simultaneous SECS-II sessions, some of which are not governed by the GEM Control State Model. No conclusions can be drawn regarding any implications of the Control State Model with respect to the single point of control requirement.

It should be noted that even in an environment in which only one SECS-II client at a time can communicate with the equipment, the GEM Control state model, together with the HSMS protocol, effectively create a first-come, first-served equipment control model as illustrated by the following scenario.

A semiconductor manufacturer typically develops host controllers to control a specific type of equipment. If more than one instance of such a controller has been installed on the factory floor, it is possible to mis-configure two (or more) of the controllers such that they each are directed to the same IP address for equipment communication. The following diagrams help illustrate the problem:

### Single Session HSMS I



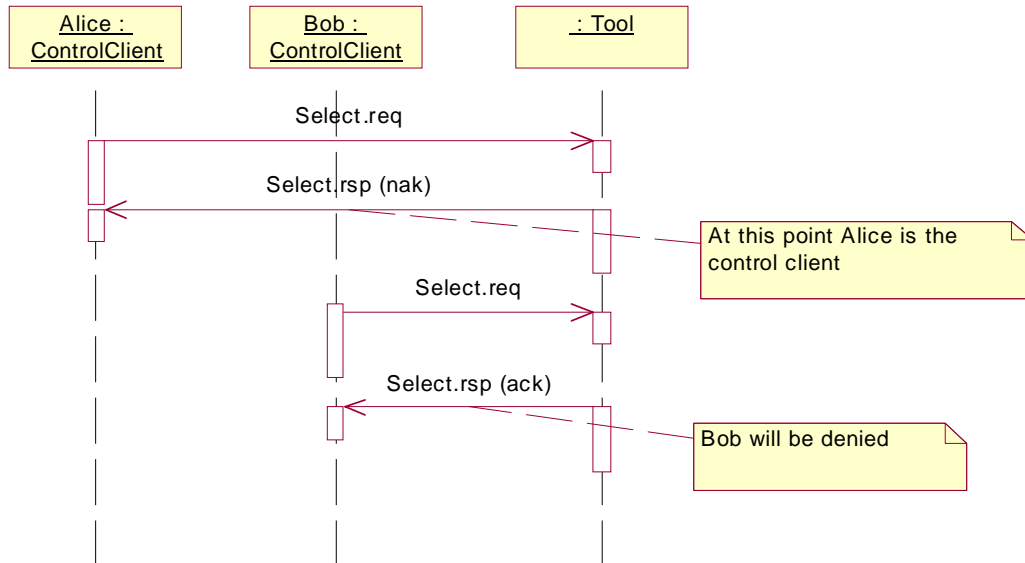
In this first exchange, Bob the host controller, establishes a TCP connection with the equipment at its configured IP address. Bob executes the HSMS “Select” procedure and creates a new HSMS session.

If the equipment is in the ENABLED/NOT-COMMUNICATING GEM Communication state, Bob then sends an S1F13 message to the equipment to transition to the ENABLED/COMMUNICATING state, and an S1F17 message to transition to the ONLINE state.

If the equipment is in REMOTE mode, Bob now has complete control of the equipment.

If Alice now attempts to establish an HSMS session with the equipment, and the equipment only supports a single session, Alice is denied and is unable to establish communications with the equipment.

### Single Session HSMS II



In this second exchange, Alice establishes an HSMS session with the equipment first and gains complete control of the equipment. If Bob now attempts to establish a new HSMS session with the equipment, Bob will be denied.

This first-come, first-served control model can lead to mis-processing and/or safety issues if not detected by manufacturing personnel. Neither HSMS nor the GEM specification provides a mechanism for the equipment or host(s) to detect or prevent this problem.

If the equipment supports the establishment of more than one HSMS session, and does nothing else, the GEM Control model permits both Alice and Bob to transition between Communication and Control states and to issue processing control commands to the equipment. This creates an environment with two simultaneous conflicting sources of control.

### 4.3 Level 2 – Analysis

While Level 2 capabilities depend on Level 1 data collection as a pre-condition, these requirements are focused on the higher-level expectations of applications that perform analysis on the data collected. No SECS communication technologies gap analysis will be completed against these requirements.

### 4.4 Level 3 – Prediction

While capability Level 3 capabilities depend on Level 1 data collection as a precondition, these requirements are focused on the higher level expectations of

SEMI Diagnostic Data Acquisition Task Force	Revision: 1.0
Communications Gap Analysis	Issue Date: 9/26/2002

the applications which perform predictive diagnostics. No SECS communication technologies gap analysis will be completed against these requirements.

#### **4.5 Summary**

The following gaps have been identified in the SECS communication technologies in evaluating them against e-Diagnostics requirements:

1. SECS-I does not support multiple independent clients
2. SECS-I does not provide an authenticating protocol
3. HSMS does not provide an authenticating protocol
4. The SECS-II message set does not provide an authenticating protocol
5. The GEM Communication state model does not differentiate between simultaneous SECS-II clients, and does not clearly specify how to apply the state model in a multi-client environment
6. The GEM Control state model does not differentiate between simultaneous SECS-II clients, and does not clearly specify how to apply the state model in a multi-client environment

#### **4.6 Conclusion**

The SECS communication technologies and the GEM Control and Communication state models, as defined today, do not meet the data collection and access control requirements of e-Diagnostics.

SECS-I can not support multiple independent clients without physical insertion of each client in the communication chain between the host and the equipment. Even with multiple participating clients, SECS-I does not have any mechanism for distinguishing between different message sources in order to preserve a single point of control.

While HSMS *does* support multiple independent client communication, it does not provide any facility for authenticating individual clients and distinguishing between them. Furthermore, there is no authentication mechanism supported by current SECS-II messages.

E30 is not currently worded to unambiguously specify whether or not GEM-compliant equipment can permit multiple clients, some of whose SECS-II sessions are not subject to the restrictions of the Communication and Control State Models.

Because this is the current state of the SEMI equipment communication standards, it will be necessary to develop an alternative solution in order to meet the objectives of e-Diagnostics.

To arrive at an alternative, more detailed criteria must be developed based on e-Diagnostics requirements, and the pros and cons of each option evaluated.