



## **Equipment Data Acquisition (EDA) Usage Scenarios Rev. B**

**International SEMATECH Manufacturing Initiative  
Technology Transfer #04104579B-TR**

**SEMATECH** and the **SEMATECH logo** are registered service marks of SEMATECH, Inc.

**International SEMATECH Manufacturing Initiative** and the **International SEMATECH Manufacturing Initiative logo** are registered service marks of International SEMATECH Manufacturing Initiative, Inc., a wholly-owned subsidiary of SEMATECH, Inc.

Product names and company names used in this publication are for identification purposes only and may be trademarks or service marks of their respective companies.

**Equipment Data Acquisition (EDA) Usage Scenarios Rev. B**  
**Technology Transfer #04104579B-TR**  
**International SEMATECH Manufacturing Initiative**  
**May 5, 2005**

**Abstract:** This report from the MFGM026M project provides basic usage scenarios and common sequences of equipment data acquisition (EDA) interface behavior based on SEMI E120, E132, E134, and E125. The scenarios are a sample of usage scenarios for which the EDA interface can potentially be applied. Some possible unexpected cases that must be supported by the equipment and third-party software supplier are also included. This revision includes exception handling cases for the interface functions defined in the EDA standards suite. These exceptions provide further guidance on equipment behavior based on typical errors. Exception handling for the client or host is not included since only the expected behavior of the equipment is covered.

Exceptions cases are now part of this document for each of the functions defined in EDA. Integrated scenarios with GEM/300 functionality are not covered.

**Keywords:** Automated Data Collection, Computer Software, User Interfaces

**Authors:** Gino Crispieri

**Approvals:** Gino Crispieri, Author  
Steve Fulton, Project Manager  
Scott Kramer, Director  
Laurie Modrey, Technology Transfer Team Leader



## Table of Contents

1	PURPOSE .....	1
2	SCOPE .....	1
3	LIMITATIONS .....	1
4	REFERENCED DOCUMENTS.....	1
5	TERMINOLOGY .....	2
	5.1 Abbreviations .....	2
	5.2 Definitions.....	2
6	EDA USAGE SCENARIO OVERVIEW .....	3
7	EDA USAGE SCENARIO CLASSIFICATION.....	4
8	FUNDAMENTAL SEQUENCES AND UNIT SCENARIOS.....	5
	8.1 Authorization and Authentication Standard (E132) .....	6
	8.1.1 Setting-Up Equipment Credentials .....	6
	8.1.2 Setting Up Applications to Access the Equipment .....	7
	8.1.3 Administrator or Client Authorization .....	8
	8.1.4 Configuration Change Scenario .....	11
	8.1.5 General Exception Cases.....	11
	8.1.6 ACL Entry Management Services .....	12
	8.1.7 Add New ACL Entry Scenario .....	15
	8.1.8 ACL Role Modification Scenario .....	17
	8.1.9 Administrative Sessions Management Services .....	17
	8.1.10 Maximum Session Setting Change Scenario .....	21
	8.1.11 Session Operation Services.....	21
	8.1.12 Equipment Notification Services .....	23
	8.1.13 Administrator Closes Session Owned by Another User Scenario .....	25
	8.2 Equipment Self Description Standard (E125).....	26
	8.2.1 Metadata Query Services.....	26
	8.2.2 Equipment Metadata Query Scenario .....	31
	8.2.3 Metadata Management Services .....	31
	8.2.4 Metadata Notification Changed Scenario.....	33
	8.3 Data Collection Plan Management (E134) .....	34
	8.3.1 DCP Management Services .....	34
	8.3.2 DCP Activation Scenario.....	41
	8.3.3 DCP Deactivation Scenario .....	42
	8.3.4 DCP Query Services.....	43
	8.3.5 ObjType Instance and Parameter Query Scenario .....	45
	8.3.6 Equipment Data Report Service.....	45
	8.3.7 DCP Performance Related Services.....	46
	8.3.8 Performance Warning With Performance Restored Scenario .....	49

9	GENERAL USAGE SCENARIOS .....	50
9.1	Basic EDA Usage Scenario.....	50
9.2	Single Client Multiple DCP Activation .....	51
9.3	Multiple Client – Single DCP .....	52
9.4	Multiple Client – Multiple DCP .....	53
9.5	Deactivation With More Than One Client Receiving Data .....	54
10	EQUIPMENT RESTARTS .....	55
10.1	Equipment Restarts Persistent DCP Scenario .....	56
10.2	Equipment Restarts Persistent DCP With Metadata Change Scenario .....	57
10.3	Equipment Restart Non-Persistent DCP Scenario.....	58

## List of Figures

Figure 1	EDA Interface Normal Cases.....	3
Figure 2	EDA Interface Exception Cases.....	4
Figure 3	Authorization and Authentication Overview .....	6
Figure 4	Equipment Certificate Setting.....	7
Figure 5	Application Certificate Setting .....	7
Figure 6	E132-SEQ-01 Establish Session Service .....	8
Figure 7	E132-SEQ-01.1 Admin or Client Authentication Detail (SSL Enabled) .....	9
Figure 8	E132-SEQ-01.2 Admin or Client Authentication Detail (SSL Disabled) .....	10
Figure 9	E132-SCN-01 SSL Configuration Change Scenario .....	11
Figure 10	ACL Entry Management Services .....	12
Figure 11	E132-SEQ-02 Get Defined Privileges Service .....	12
Figure 12	E132-SEQ-03 Get ACL Query Service.....	13
Figure 13	E132-SEQ-04 Add ACL Entry Service .....	14
Figure 14	E132-SCN-02 Add New ACL Entry Scenario.....	15
Figure 15	E132-SEQ-05 Delete ACL Entry Service .....	16
Figure 16	E132-SCN-03 ACL Role Modification Scenario.....	17
Figure 17	Administrative Sessions Management Services .....	17
Figure 18	E132-SEQ-06 Get Active Sessions Service.....	18
Figure 19	E132-SEQ-07 Get Max Sessions Services .....	18
Figure 20	E132-SEQ-08 Set Max Sessions Service .....	19
Figure 21	E132-SEQ-09 Close Session Service.....	20
Figure 22	E132-SCN-04 Max Session Setting Change Scenario .....	21
Figure 23	Generic Session Operational Services.....	21
Figure 24	E132-SEQ-10 Persist Session Service .....	22
Figure 25	E132-SEQ-11 Session Ping Service [Client].....	23
Figure 26	Equipment Notification Services .....	23
Figure 27	E132-SEQ-12 Session Frozen Notification.....	24
Figure 28	E132-SEQ-13 Session Closed Notification.....	24
Figure 29	E132-SEQ-14 Session Ping Service [Equipment] .....	25
Figure 30	E132-SCN-05 Administrator Closes Session Owned by Another Client.....	25
Figure 31	Metadata Query Services.....	26
Figure 32	E125-SEQ-01 Get Equipment Structure Service.....	26
Figure 33	E125-SEQ-02 Get Equipment Node Description Service.....	27
Figure 34	E125-SEQ-03 Get Exceptions Service.....	28
Figure 35	E125-SEQ-04 Get Semi ObjTypes Service .....	28
Figure 36	E125-SEQ-05 Get State Machines Service .....	29
Figure 37	E125-SEQ-06 Get Type Definitions Service .....	29
Figure 38	E125-SEQ-07 Get Units Service .....	30
Figure 39	Equipment Metadata Query Scenarios.....	31
Figure 40	E125-SEQ-08 Get Latest Revision Service.....	32

Figure 41	E125-SEQ-09 Notify On Revisions Service .....	32
Figure 42	E125-SEQ-10 Metadata Revised Notification.....	33
Figure 43	E125-SCN-01 Metadata Notification Scenario .....	33
Figure 44	Data Collection Plan Management Services .....	34
Figure 45	E134-SEQ-01 Define Plan Service .....	34
Figure 46	E134-SEQ-02 Activate Plan Service.....	36
Figure 47	E134-SEQ-03 Deactivate Plan Service .....	37
Figure 48	E134-SEQ-04 Delete Plan Service .....	38
Figure 49	E134-SEQ-05 Get Active Plans Service .....	38
Figure 50	E134-SEQ-06 Get Plan Definition Service .....	39
Figure 51	E134-SEQ-07 Get Defined Plan IDs Service .....	40
Figure 52	E134-SCN-01 DCP Activation Scenario.....	41
Figure 53	E134-SCN-02 DCP Deactivation Scenario .....	42
Figure 54	E134-SEQ-08 Get ObjType Instance Service.....	43
Figure 55	E134-SEQ-09 Get Parameter Value Service.....	44
Figure 56	E134-SCN-03 Get ObjType Instance and Parameter Type Scenario .....	45
Figure 57	Equipment Data Report Service.....	45
Figure 58	E134-SEQ-10 New Data Notification.....	45
Figure 59	DCP Performance Related Services .....	46
Figure 60	E134-SEQ-11 Get Current Performance Status Service .....	46
Figure 61	E125-SEQ-12 DCP Deactivation Notification .....	47
Figure 62	E134-SEQ-13 DCP Hibernated Notification.....	47
Figure 63	E134-SEQ-14 Performance Warning Notification.....	48
Figure 64	E134-SEQ-15 Performance Restored Notification .....	48
Figure 65	E134-SCN-04 Performance Warning With Performance Restored Scenario .....	49
Figure 66	SCN-01 Basic EDA Usage Scenarios .....	51
Figure 67	Single Clients Multiple DCP .....	51
Figure 68	SCN-02 Single Clients Multiple DCP Activation Scenarios.....	52
Figure 69	Multiple Client Single DCP.....	52
Figure 70	SCN-03 Multiple Client Single DCP Scenario .....	53
Figure 71	Multiple Clients – Multiple DCPs .....	53
Figure 72	SCN-04 Multiple Client Multiple DCP Scenario .....	54
Figure 73	SCN-05 Deactivation With More Than One Client Receiving Data Scenario .....	55
Figure 74	E134-SCN-05 Equipment Restarts With Persistent DCP Scenario .....	56
Figure 75	E134-SCN-06 Equipment Restarts Persistent DCP and Metadata Change.....	57
Figure 76	E134-SCN-07 Equipment Restarts Without Persistence Scenario .....	58

## Acknowledgments

The author would like to thank the following contributors:

- IBM: Bob Wiggins, Karl Gartland
- Infineon: Ralf Georgi
- Intel: Xian Lu, Zimo Ma, Bahram Moinvaziri, James Martin, JB Ragothaman
- TSMC: Jonathan Chang, Jethro Jheng, Allan Chen, K.H. Chen
- ISMI: Harvey Wohlwend, Steve Fulton, Lance Rist, Charisse Rosier, Lorn Christal



## 1 PURPOSE

The equipment data acquisition (EDA) usage scenarios define a common approach to the use and applicability of the EDA interface. These EDA usage scenarios represent the accepted behavior and mode of operation the International SEMATECH Manufacturing Initiative (ISMI) member companies have agreed upon for the newly developed EDA interface. Additional scenarios may be required by IC makers to validate the EDA interface definition and usage. Besides a list of basic usage scenarios, exception cases that must be supported by the equipment and third-party software supplier are also included. Equipment suppliers are expected to conform to the EDA specifications and the proposed usage scenarios described in this document.

## 2 SCOPE

This document provides basic usage scenarios and common sequences of EDA interface behavior based on SEMI E120, E132, E134, and E125. Exception scenarios are included but they are limited to a minimum set because many of them depend on the user environment and host application architecture. Integrated scenarios with GEM/300 functionality are not covered. The approach used in the definition of the EDA scenarios is based on the common behavior defined by each of the standards. The unit functionality defines each capability described in the SEMI standard through examples and sequence of operations. General usage scenarios are defined based on the unit behavior but across multiple standards.

## 3 LIMITATIONS

The functionality of the EDA standards are clearly defined through the requests, replies, and notification services. The set of scenarios presented are identified as typical operations for the EDA interface. They represent only a subset of the complete functional scenarios; they illustrate how the interface would interact with a client under different situations.

## 4 REFERENCED DOCUMENTS

The following documents include applicable SEMI standards and other documents.

- **SEMI Standards<sup>1</sup>**
  - SEMI E134, *Specification for Data Collection Management (DCM)*
  - SEMI E120, *Specification for the Common Equipment Model (CEM)*
  - SEMI E125, *Specification for Equipment Self Description (EqSD)*
  - SEMI E132, *Specification for Equipment Client Authorization and Authentication (A&A)*

---

<sup>1</sup> **SEMI North America (Headquarters)**  
3081 Zanker Road, San Jose, California 95134-2127 USA  
Tel: 1-408-943-6900; Fax: 1-408-928-9600  
E-mail: [semihq@semi.org](mailto:semihq@semi.org); Web: <http://www.semi.org>

- **Other Documents**

- *Extensible Markup Language (XML) 1.0 (Second Edition)* – W3C Recommendation, 6 October 2000 (<http://www.w3.org/TR/2000/REC-xml-20001006/>)
- *XML Schema Part 1: Structures* – W3C Recommendation, 2 May 2001 (<http://www.w3.org/TR/xmlschema-1/>)
- *XML Schema Part 2: Datatypes* – W3C Recommendation, 2 May 2001 (<http://www.w3.org/TR/xmlschema-2/>)
- X.509 Specification - <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf> (see also: <http://www.faqs.org/rfcs/rfc2459.html>)

## 5 TERMINOLOGY

### 5.1 Abbreviations

ACL	Access Control List
CEM	Common Equipment Model
DCM	Data Collection Management
DCP	Data Collection Management
EDA	Equipment Data Acquisition
EqSD	Equipment Self Description
PKCS	Public Key Cryptography Standard
SSL	Secure Sockets Layer

### 5.2 Definitions

*Client* – any software entity that uses the EDA interface to manage sessions, metadata, or data collection on the equipment

*Conformance* – the ability and extent to which the software is able to support the functions needed to operate in a production factory, as defined in this document for the EDA scenarios by the IC manufacturers

*Metadata* – data used to describe data. For example, if a tool can report an event with several associated variables under certain conditions, the metadata for that event would provide a description of what condition will produce the event, what each variable’s type and units are, and the ID of the event itself

*EDA Usage Scenario* – the sequence of messages between an EDA application and EDA-compliant equipment that represent equipment behavioral requirements related to the EDA interface as defined to support the operational requirements by IC manufacturers

## 6 EDA USAGE SCENARIO OVERVIEW

To define a comprehensive set of usage scenarios, ISMI has created a novel approach that allows suppliers and users of the interface to build their individual scenarios based on pre-defined functional requirements. These functional requirements are described as a set of request and reply messages. Figure 1 depicts the EDA usage scenarios that ISMI member companies have agreed upon with single balloons to provide an overview of the EDA spectrum.

This document describes fundamental sequences that map to the unique messaging functionality each standard defines and general usage scenarios illustrating the expected behavior of the interface under normal conditions.

In Figure 1, the EDA communication requirements have been grouped by standards-defined functionality for normal cases.

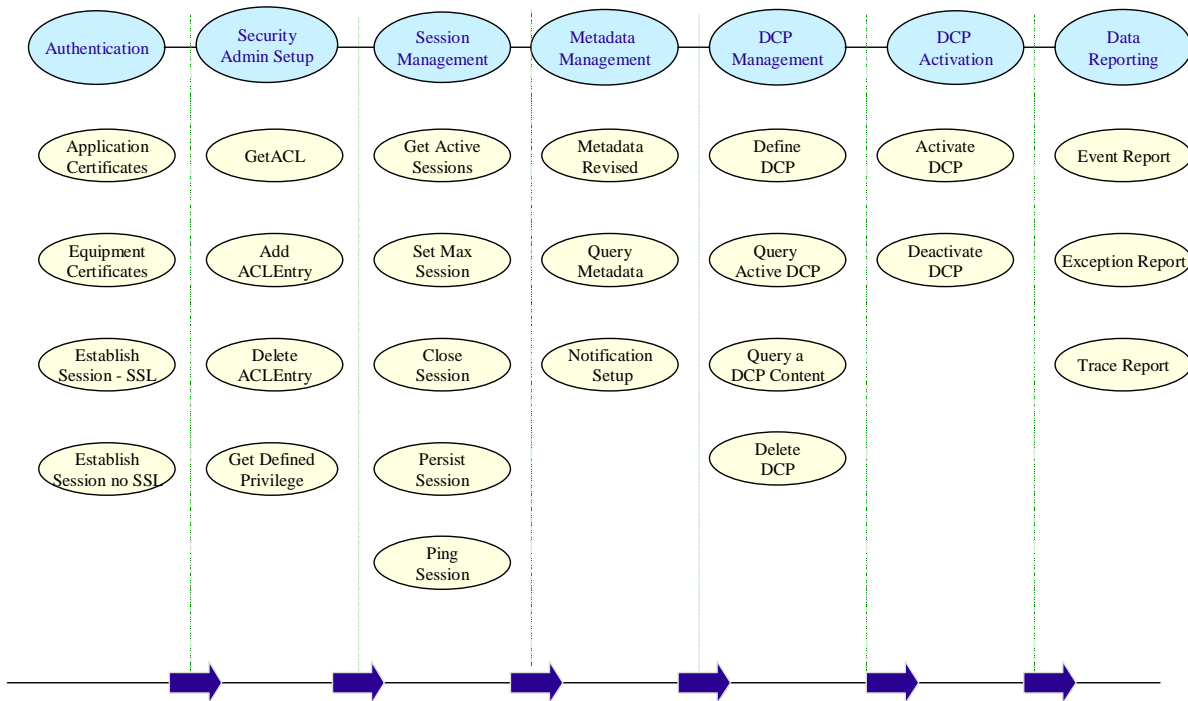
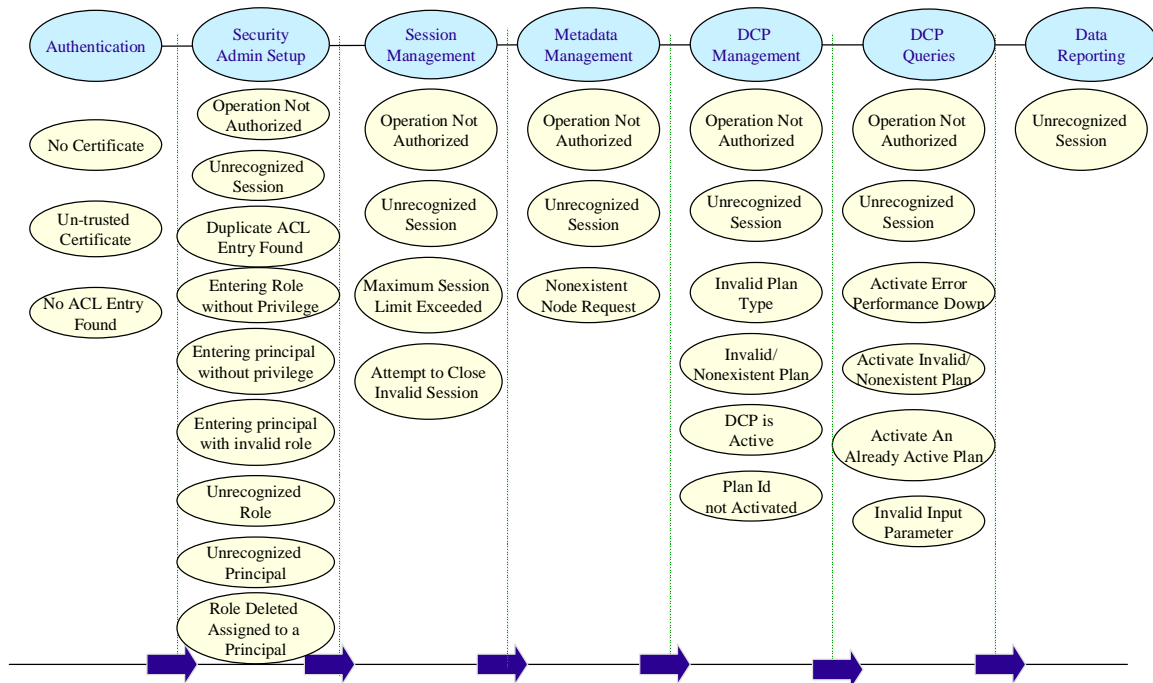


Figure 1 EDA Interface Normal Cases

Figure 2 lists a limited number of exception cases based on the functionality defined by each of the standards. Many of the exception cases depend on the client architecture; the ones listed reflect the minimum requirements based on a simple architecture.



**Figure 2 EDA Interface Exception Cases**

## 7 EDA USAGE SCENARIO CLASSIFICATION

The EDA usage scenarios defined in this document can be classified under three main groups:

- **Fundamental Sequences**
  - Small reusable functional cases
  - Represented by each function the standards define
  - Have an Exxx-SEQ-XX identifier number to distinguish them from other services
  - A given Exxx-SEQ-XX is given an .X number extension for different combinations of message content based on the XX functional case number. The content can be normal or be one of the exception cases.
- **Unit Scenarios**
  - Represented by a combination of fundamental sequences from a single standard
  - Have an Exxx-SCN-XX identifier number
  - Include normal and exception cases
- **Integrated Scenarios**
  - Represented by a combination of fundamental cases from multiple standards
  - Have an SCN-XX identifier number because they use fundamental sequences from multiple standards and are not specific to a particular standard.

## 8 FUNDAMENTAL SEQUENCES AND UNIT SCENARIOS

The fundamental sequences and unit scenarios are grouped by defined behavior as described in each of the EDA specifications. Three main specifications make up the functional behavior of the EDA interface. In hierarchical order, they are as follows:

- SEMI E132, *Specification for Equipment Client Authorization and Authentication (A&A)*
- SEMI E125, *Provisional Specification for Equipment Self Description (EqSD)*
- SEMI E134, *Specification for Data Collection Management (DCM)*

The lowest level behavior is defined by the equipment authorization and authentication. This standard describes how the administrator, the factory applications, and the equipment communicate in the factory. It defines session behavior as well as management of the sessions using services that can close a session, make it persistent, and activate or deactivate them.

- E132 – Authentication and Authorization Standard
  - Credential Setup for Equipment and Applications
  - Administrator or Client Authentication (with and without SSL)
  - ACL Entry Management Services
  - Administrative Session Management Services
  - Session Operation Services
  - Equipment Notification Services

The Equipment Self Description specification provides for services to query the equipment about its physical makeup and its logical data organization. This specification defines the actual metadata the equipment uses to communicate with the factory:

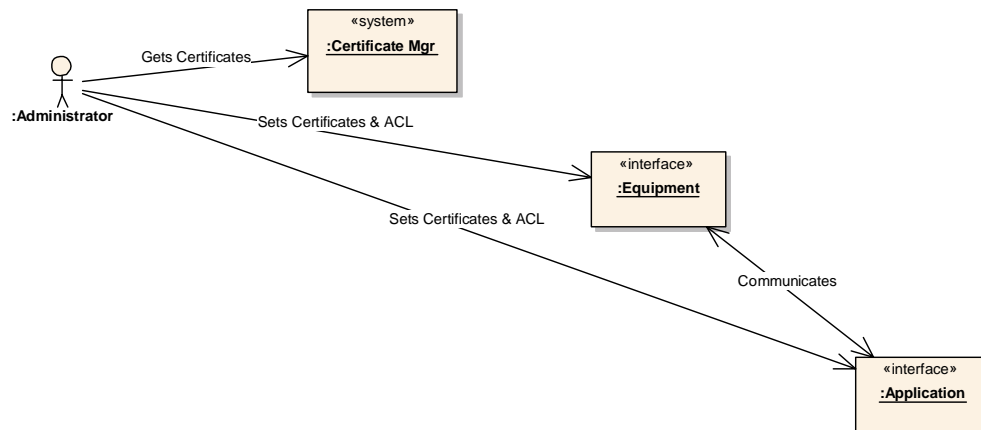
- E125 – Equipment Self Description Standard
  - Metadata Query Services
  - Metadata Management Services

The Data Collection Plan specification explains the mechanisms to define and manage data collection plans. It also defines the report structure and format. This specification also provides additional mechanisms to communicate with clients about data availability and when the equipment is going off line or coming back on line:

- E134 – Data Collection Management Standard
  - DCP Management Services
  - DCP Query Services
  - DCP Performance Warning Services

## 8.1 Authorization and Authentication Standard (E132)

Three interfaces are defined in the SEMI E132 specification (see Figure 3). Each plays an important role in the communication and the possible scenarios that use these capabilities. The Certificate Manager sets up certificates and possibly the Access Control Lists (ACL) for the equipment and the clients. The equipment manages the sessions it creates and the privileges for the services it provides. It maintains an ACL of all those clients that can potentially communicate with it. The setup of certificate authority servers or usage is not covered in this document.

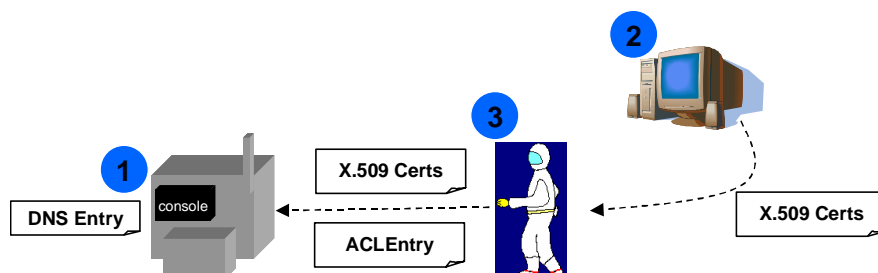


**Figure 3 Authorization and Authentication Overview**

### 8.1.1 Setting-Up Equipment Credentials

- **Step 1 – Tool is Installed**
  - Tool should have capabilities in the O/S for Certificate Management
  - TCP/IP and Ethernet must be ready for both equipment and factory networking applications
  - Equipment is placed on the network and given a valid DNS entry
- **Step 2 – Tool Credentials Created at the Certificate Manager Server**
  - Certificate Manager Server handles certificate creation as a Certificate Authority (CA)
  - Factory generates new private/public key pair and certificate for equipment, SSL Server for equipment, and SSL Client for other clients
  - When SSL is not used or enabled, the tool or client credentials are not needed. Otherwise, PKCS#10 file and key generation is requested
- **Step 3 – Tool Credentials are Installed, Bootstrapped (see E132.1 for additional details)**
  - PKCS#12 file contains equipment’s private/public keys, public key certificate, and factory-trusted Certificate Authority certificate chain installed on the equipment
    - Certificate contents:
      - Version Information
      - Serial number Issuer
      - Valid To/From

- Subject Common Name
- Public Key
- Authority Information Access
- PKCS#12 not required when SSL is disabled

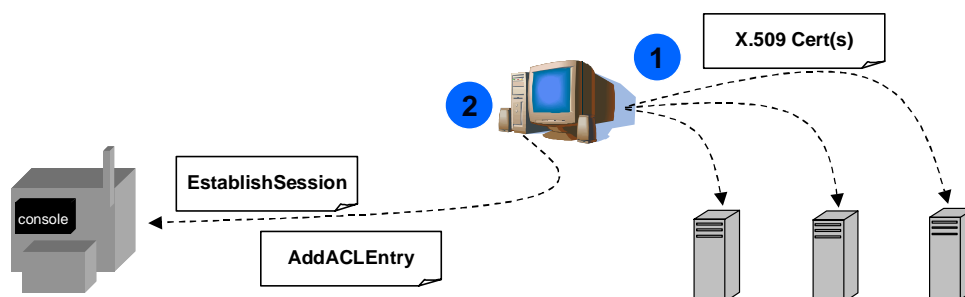


**Figure 4 Equipment Certificate Setting**

### 8.1.2 Setting Up Applications to Access the Equipment

- **Step 1 – Application Credentials Created and Installed**

- If SSL is disabled, applications attempting to connect to the equipment without a factory-issued certificate will be granted access if there is an ACL entry.
- Each application requiring access to any tool on the factory floor requires access to a private/public key pair, public key certificate, and Certificate Authority (CA) certificate chain.
- The factory chooses how these certificates are issued and accessed (not governed by E132).
- Before this step, any application attempting to connect to the equipment without a factory-issued certificate will be denied connection by the Security Socket Layer (SSL) protocol.



**Figure 5 Application Certificate Setting**

#### 8.1.2.1 Normal Setup of Certificates

Certificate assignment and enabling of Internet services depends on the operating system and therefore it is not covered in this document. The steps described above will be executed using the procedures defined by each of the operating systems used. These steps can vary even between operating system platforms as in the case of Microsoft NT, 95, 98, 2000, or XP.

### 8.1.2.2 Exception Cases

Exception cases for applying certificates and setting up Internet services are operating system- and platform-dependent. No exception cases have been defined. It is recommended that more information is derived from each of the operating system environments about the setup of certificates and steps to resolve any exceptions.

### 8.1.3 Administrator or Client Authorization

The first sequence expected by any client or equipment in the factory is an Establish Session Request (ESR) from the application trying to initiate communication. At the lowest level, authentication is invisible to the user but consists of several steps or low-level messages as shown. This document defines this sequence as one pair of messages where the client makes a request to establish a session and the equipment replies with a Session-granted response.

#### 8.1.3.1 ACL Entry Setup

The E132 ACLEntry for the factory Security Administrator is created at the tool console. This is usually application-specific, and knowledge of the operating system tools is necessary. Equipment and application ACL entry can be done through the console or an administrative application. A factory security administrator application connects to the equipment using the E132 “*EstablishSession*” request and creates an access control list ACLEntry for each application requiring equipment access. Before this step, the equipment denies all *EstablishSession* requests from any application that does not have an ACLEntry in the equipment.

#### 8.1.3.2 EstablishSession()

Clients and the security administrator use this service to connect with the equipment and initiate communication. An “*endPoint*” entry is required in the request so the equipment knows where to reply. Once the equipment authenticates, the client receives a session identifier (*sessionID*) that the client must use for every future communication. Once authenticated, the session is granted the privileges assigned to the client based on the corresponding ACLEntry for that client (Principal). Changes to the ACL do not affect the privileges of sessions established before the ACL change.

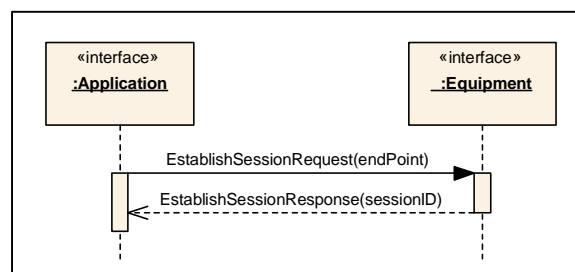


Figure 6 E132-SEQ-01 Establish Session Service

### 8.1.3.2.1 Normal Cases

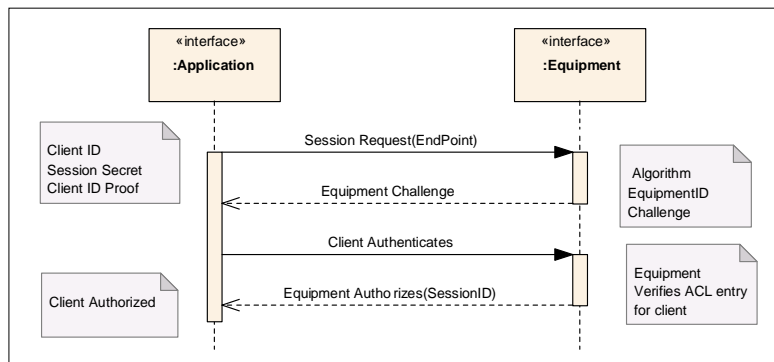
The following cases have been identified as normal cases:

- E132-SEQ-01.1 Client has a valid certificate and ACL entry when the session request is made
- E132-SEQ-01.2 Client does not use certificates but has a valid ACL entry when the request is made

Equipment not using SSL is just a special case in which the equipment skips or ignores the low-level authentication; authorization still applies even when the authentication is not required. This means that the equipment *must have* an ACL entry for the requester before it grants access to the client.

### 8.1.3.3 When SSL is Enabled

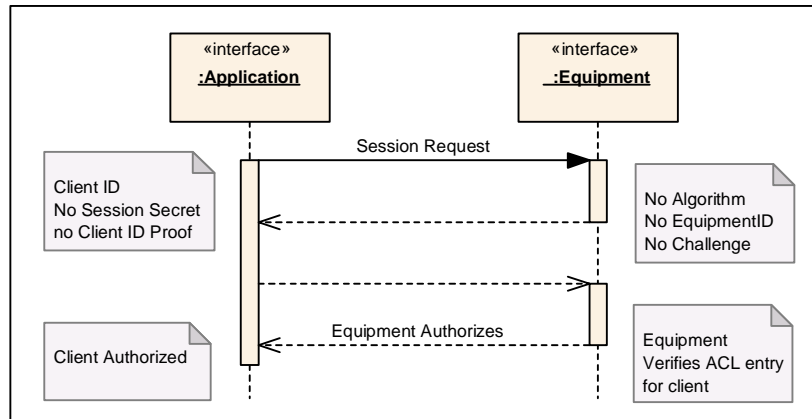
The requestor will be granted access to a session automatically if a subject in the ACL matches the ID in the “FROM” field from the service request or a subject in the ACL is equal to “anyPrincipal” that has assigned privileges. “anyPrincipal” is a special case allowing any client access to the equipment.



**Figure 7 E132-SEQ-01.1 Admin or Client Authentication Detail (SSL Enabled)**

### 8.1.3.4 When SSL is Disabled

When the equipment does not use SSL, the equipment skips all authentication steps as required by the SSL specification. Authorization still applies (i.e., an ACL entry must exist for the requestor). If SSL is disabled, the E132-based communication with the equipment occurs through the unauthenticated HTTP transport, not HTTPS. The client must provide a “*clientID*” in the “*From*” field to be able to obtain a session from the equipment.



**Figure 8 E132-SEQ-01.2 Admin or Client Authentication Detail (SSL Disabled)**

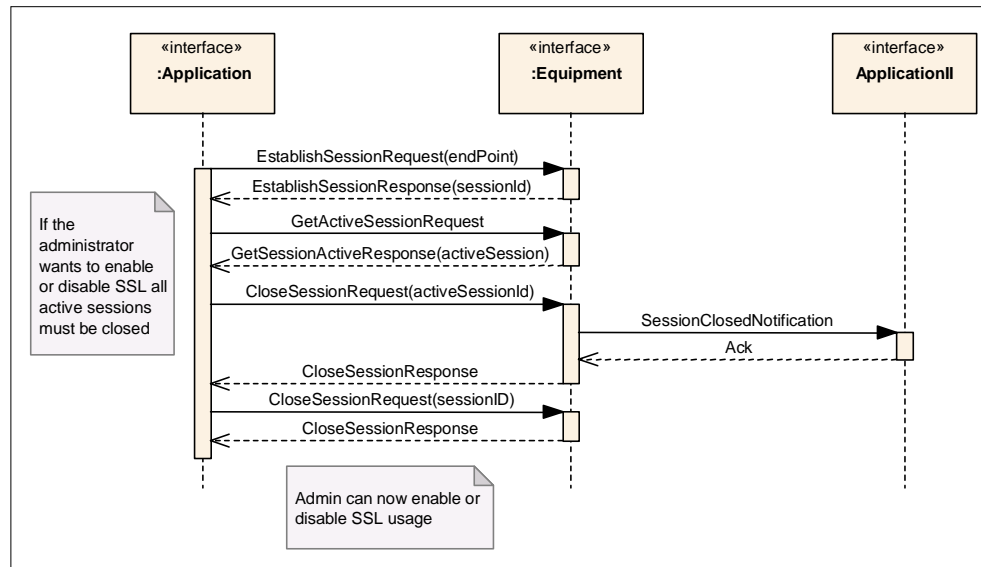
#### 8.1.3.4.1 Exception Cases

These exception cases can be encountered in many scenarios and will be repeated and/or described throughout this document.

- E132-SEQ-01.3 Client does not have a certificate at all (with SSL enabled). The equipment rejects the request and exits the AUTHENTICATING state (see SEMI E132). No SessionID is assigned to the requestor.
- E132-SEQ-01.4 Client has a certificate that is not trusted. The equipment rejects the request and exits the AUTHENTICATING state (see SEMI E132). No SessionId is assigned to the requestor.
- E132-SEQ-01.5 No ACL entry found in the equipment or application. The equipment rejects the requests and exits the AUTHENTICATING state (see SEMI E132). No SessionId is assigned to the requestor.

### 8.1.4 Configuration Change Scenario

This scenario is intended to demonstrate the importance of shutting down any active sessions before there is a change between SSL enabled and SSL disabled. The administrator is responsible for this operation, and the equipment must reject any requests to change the SSL settings as long as there are active sessions. Once all sessions are closed, the administrator can switch SSL ON or OFF.



**Figure 9 E132-SCN-01 SSL Configuration Change Scenario**

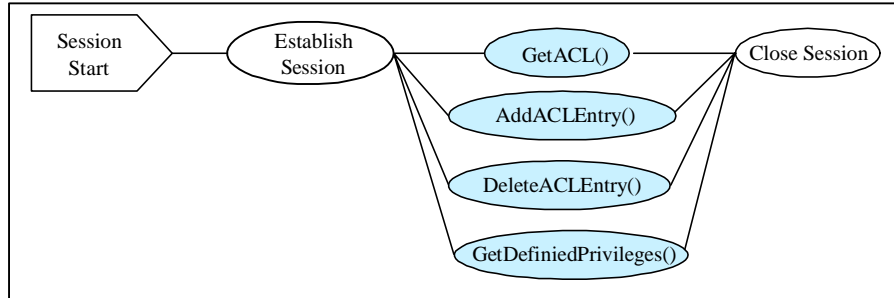
### 8.1.5 General Exception Cases

Notification services do not cause exception cases since there is no response expected from the client application. Two exception cases are encountered throughout this document. The Unrecognized Session exception deals with those requests from an established connection that includes the incorrect SessionID with its request. The Operation Not Authorized exception occurs for all the defined services described in this document if the requestor does not have the privilege to use the service. This depends on whether or not the ACL does or does not include the service authorization granularity to produce this denial of the service request.

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information about the denied request included). The equipment rejects the request, returns to READY, and continues to monitor its current session.

### 8.1.6 ACL Entry Management Services

Once the client application is granted communication by the assignment of a SessionID, further communication between the client and the equipment will be based on assigned privilege entries from the equipment ACL.



**Figure 10** ACL Entry Management Services

#### 8.1.6.1 ACL Entry Local Setup

The first ACLEntry for the factory security administrator is created at the tool console. The ACLEntry has SecurityAdmin privileges (see E132 for details on this account). Next, equipment and client application ACLEntry can be done through the console or remotely using defined E132 services and applying the assigned SecurityAdmin privileges.

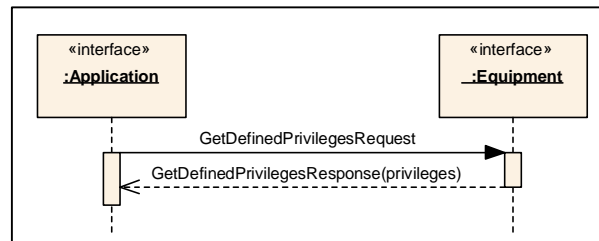
#### 8.1.6.2 ACL Entry Remote Setup

Once the factory security administrator application connects to the equipment or client application using the “*EstablishSession*” request, it can then create one or more ACL entries. The administrator must create an ACLEntry for each application requiring equipment access. (See E132 for details on the structure and definition of these entries.) Before this step, the equipment denies all “*EstablishSession*” requests from any application that does not have an ACLEntry in the equipment or the client application.

Four services are defined to manage ACL entries: GetDefinedPrivileges, AddACLEntry, DeleteACLEntry, and GetACL. There is no mechanism to update an ACL entry. If an ACL entry needs to be modified, the entry being modified must be deleted first and then reentered.

#### 8.1.6.3 GetDefinedPrivileges()

This operation retrieves the set of privileges supported by the equipment and client application. The list includes the assigned privileges as entered by the administrative application.



**Figure 11** E132-SEQ-02 Get Defined Privileges Service

### 8.1.6.3.1 Normal Case

During the normal case of the sequence of messages the user queries the equipment application for the privileges defined at the equipment. This service is used by an authorization management application.

- E132-SEQ-02.1 GetDefinedPrivileges request allows the management application check the current privileges defined in the equipment.

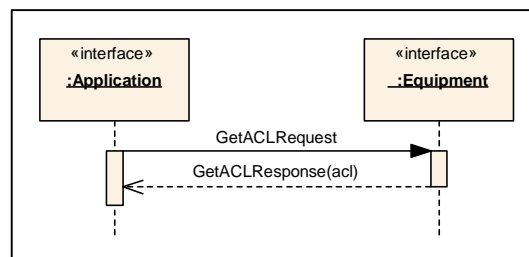
### 8.1.6.3.2 Exception Cases

There are two exception cases.

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information included about the denied request). The equipment rejects the request, returns to READY, and continues to monitor its current session. The Operation Not Authorized exception requires context about the request that initiated the error.

### 8.1.6.4 GetACLQuery()

This operation requests the contents of the entire ACL currently defined on the equipment.



**Figure 12 E132-SEQ-03 Get ACL Query Service**

#### 8.1.6.4.1 Normal Case

This request does not include any input parameters and is intended to retrieve the defined ACL in the equipment.

- E132-SEQ-03.1 Request to retrieve the Access Control List form the equipment. The equipment returns the current definition for the ACL entries.

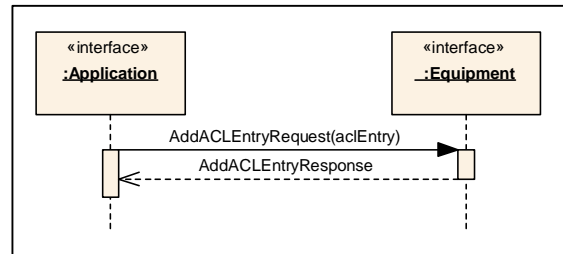
#### 8.1.6.4.2 Exception Case

Exception cases are similar to the ones identified above.

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information included about the denied request). The equipment returns to READY and continues to monitor its current session. The Operation Not Authorized error requires context information about the request that has been denied.

### 8.1.6.5 AddACLEntry() – Principal or Role

A principal is either assigned to one and only one role, or to one or more privileges. A role is defined as a unique, identifiable set of one or more privileges that cannot be composed from other roles. Zero or more principals can be assigned to one or more roles. This operation adds a new ACL entry to the equipment.



**Figure 13 E132-SEQ-04 Add ACL Entry Service**

#### 8.1.6.5.1 Normal Cases

Each of these cases results in a particular input with specific structured information (see E132):

- E132-SEQ-04.1 Entry added can be a principal with privileges
- E132-SEQ-04.2 Entry added can be a role with privileges
- E132-SEQ-04.3 Entry can be a principal assigned to an existing role

#### 8.1.6.5.2 Exception Cases

These cases are identified as potential errors:

- ACLEntry is a Privilege Assignment or a Role Assignment for a Principal or Role that already has a Privilege Assignment or Role Assignment ACLEntry.
- ACLEntry is a Privilege Assignment and refers to a privilege that is not supported by the equipment.
- ACLEntry is a Role Assignment and refers to a Role that does not have a Privilege Assignment ACLEntry defined.
- ACLEntry is a Role Assignment or Privilege Assignment that would result in more than one Principal having the Security Administrator privilege.

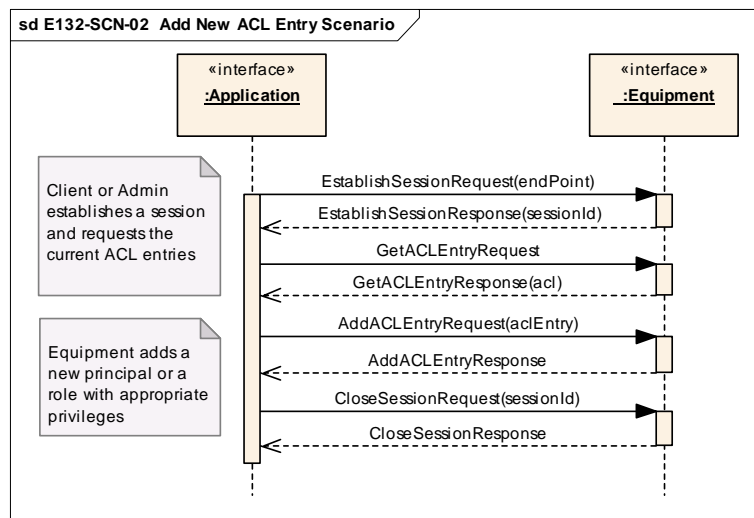
Otherwise, the equipment stores and updates the Access Control List in the equipment. The numbered list of exception cases below include the cases identified above.

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). The equipment returns to the READY state and continues to monitor its current session. No changes are made to the ACL or accepted by the equipment.

- E132-SEQ-04.4 Duplicate ACL Entry Found. The equipment returns to the READY state and continues to monitor its current session. No changes are made to the ACL or accepted by the equipment.
- E132-SEQ-04.5 Entering Role with no privileges. The equipment returns to the READY state and continues to monitor its current session. No changes are made to the ACL or accepted by the equipment.
- E132-SEQ-04.6 Entering a Principal with an invalid role. The equipment returns to the READY state and continues to monitor its current session. No changes are made to the ACL or accepted by the equipment.
- E132-SEQ-04.7 Entering a Principal without a privilege. The equipment returns to the READY state and continues to monitor its current session. No changes are made to the ACL or accepted by the equipment.

### 8.1.7 Add New ACL Entry Scenario

This scenario depicts a basic sequence of steps that occurs when an ACLEntry is added. These steps typically start when a client establishes a session and requests the current ACL entries to avoid duplicate or invalid entries and then adds new entries to the ACL.

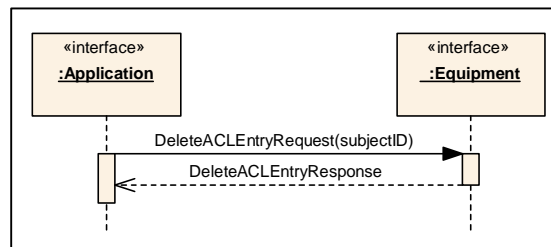


**Figure 14** E132-SCN-02 Add New ACL Entry Scenario

### 8.1.7.1 DeleteACLEntry()

This service removes an ACL entry from equipment or client. Deletion of an ACL entry that has been applied to one or more active sessions *neither affects* the privileges granted to that session nor terminates such sessions. An attempt to establish new sessions by a principal whose privilege assignment or role assignment ACL entry has been deleted will be rejected by the equipment.

Note: It is an error to delete a privilege assignment ACL entry for a role when principals are still assigned to that role.



**Figure 15 E132-SEQ-05 Delete ACL Entry Service**

#### 8.1.7.1.1 Normal Cases

This service is issued by a management application operation with the purpose of removing a role or a principal.

- E132-SEQ-05.1 Entry removal can be a role.
- E132-SEQ-05.2 Entry removal can be a principal.

#### 8.1.7.1.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). The equipment returns to the READY state and continues to monitor its current session. ACL does not get deleted.
- E132-SEQ-05.3 No Such Role Is Defined. The equipment returns to the READY state and continues to monitor its current session. No changes are made to any of the Roles in the ACL.
- E132-SEQ-05.4 No Such Principal Is Defined. The equipment returns to the READY state and continues to monitor its current session. No changes are made to any Principal in the ACL.
- E132-SEQ-05.5 Role being deleted still assigned to Principal(s). The equipment returns to the READY state and continues to monitor its current session. No changes are made to the ACL, and the role is not deleted until all Principals are removed.

### 8.1.8 ACL Role Modification Scenario

A typical usage scenario for these services for an ACL entry modification may be in the following order. The ACL request ensures there are no conflicts in the deletion as there is in the case of a role that is assigned to multiple principals. An entry must be deleted and then re-entered if the entry needs to be modified.

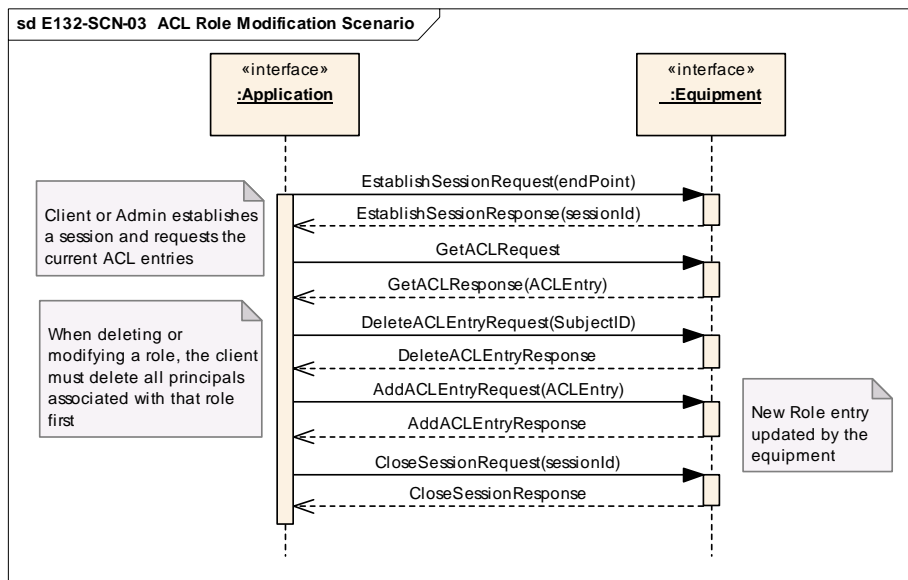


Figure 16 E132-SCN-03 ACL Role Modification Scenario

### 8.1.9 Administrative Sessions Management Services

Two typical query operations performed by the session-managing entity are getting the number of active sessions and resetting the equipment-allowed number of active sessions.

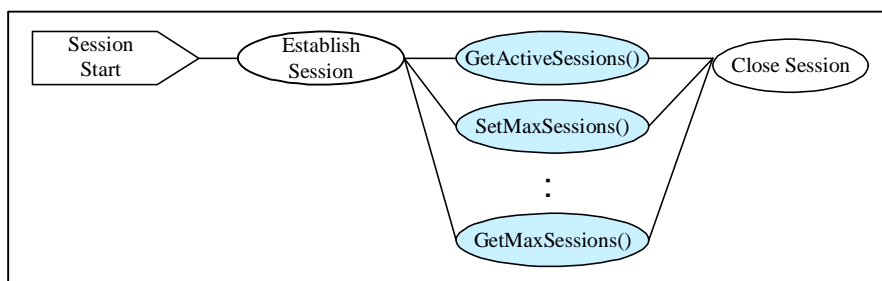


Figure 17 Administrative Sessions Management Services

### 8.1.9.1 GetActiveSessions()

This operation allows the security administrator to retrieve information for all active sessions currently established on the equipment. The response *does not* include the administrative session.

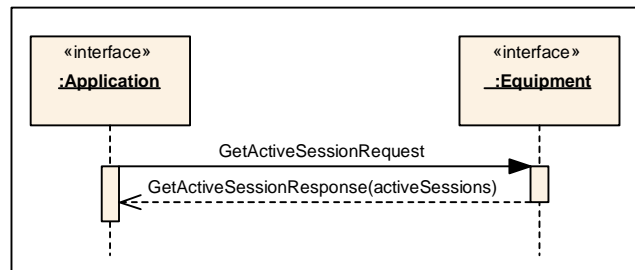


Figure 18 E132-SEQ-06 Get Active Sessions Service

#### 8.1.9.1.1 Normal Cases

This service is issued by a management application operation with the purpose of querying the equipment or application about its managed sessions.

- E132-SEQ-06.1 Request to find out active sessions in the equipment.

#### 8.1.9.1.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). The equipment returns to the READY state and continues to monitor its current session. The equipment or the client denies the request.

### 8.1.9.2 GetMaxSessions()

This operation retrieves the current maximum limit of simultaneous non-administrative sessions established currently on the equipment.



Figure 19 E132-SEQ-07 Get Max Sessions Services

### 8.1.9.2.1 Normal Cases

This service is issued by a management application operation with the purpose of querying the equipment about its maximum number of managed sessions.

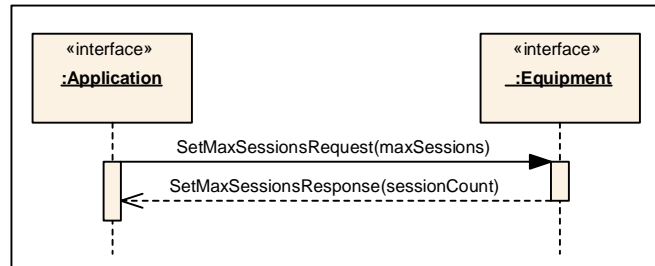
- E132-SEQ-07.1 Request to find out maximum number of allowed sessions currently set for this equipment.

### 8.1.9.2.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). The equipment returns to the READY state and continues to monitor its current session. The equipment denies the request.

### 8.1.9.3 SetMaxSessions()

This operation allows the security administrator to set the maximum number of simultaneous non-administrative sessions that the equipment will allow. This limit applies only to new session requests not coming from the security administrator session. Previously established sessions are not affected. If the number of current active sessions exceeds this limit, the equipment will reject any request by a “non-Admin” session. One important detail is that any new session requests are authenticated first to determine if the client is not the security administrator. Then the check on the limit is made to determine whether or not to reject the request. Setting this limit to “0” restricts security administrator sessions only.



**Figure 20 E132-SEQ-08 Set Max Sessions Service**

### 8.1.9.3.1 Normal Cases

This service is issued by a management application operation with the purpose of querying the equipment about its managed sessions.

- E132-SEQ-08.1 Request to setup maximum number of allowed active sessions. The equipment responds with the new constant value set confirming the change.

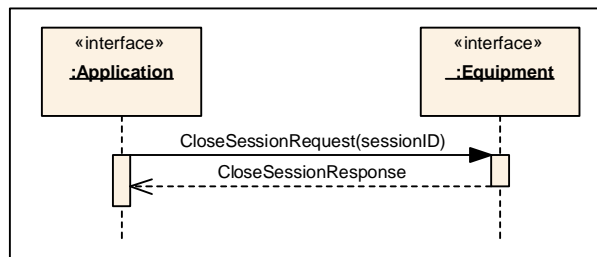
### 8.1.9.3.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.

- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). The equipment returns to the READY state and continues to monitor its current session. No changes are made to the equipment constant, and the current setting remains as previously defined.

#### 8.1.9.4 CloseSession()

This service is used to close a session. The equipment or application must send the Session Closed notification (see section 8.1.12.2) to the client whose session is being closed if this is done by an administrative application. The equipment deletes all information related to the client's session and closes any active connection to the client. The established equipment security administrator can terminate or close any third-party active session through the CloseSessionRequest. This administrator function can be used to clean up sessions when clients are no longer active or to force termination of any session even when a client is still active.



**Figure 21 E132-SEQ-09 Close Session Service**

##### 8.1.9.4.1 Normal Operations

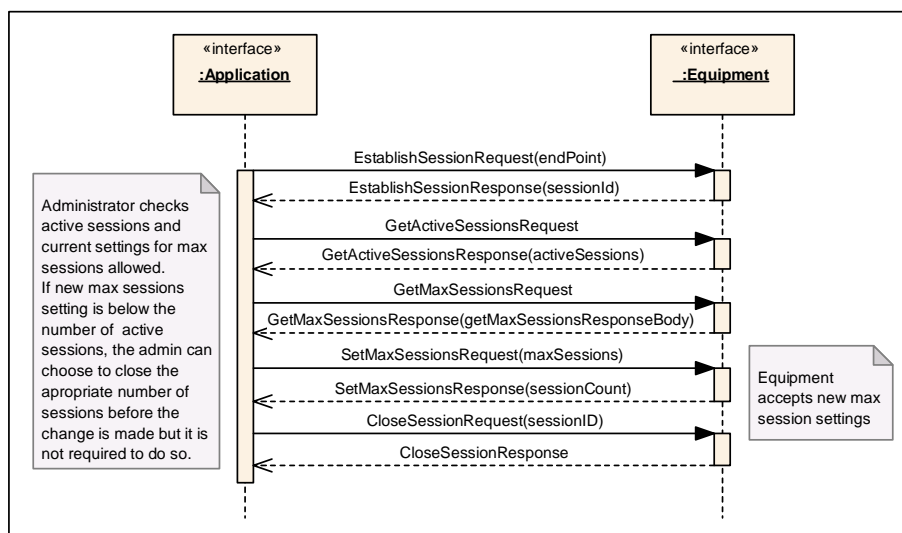
- E132-SEQ-09.1 Close Own Session. The requests include a SessionId that is the same as the one used to communicate with the equipment or application.
- E132-SEQ-09.2 Close Third Party Session. The requests include a SessionId that is different from the SessionId used to communicate with the equipment.

##### 8.1.9.4.2 Exceptions

- E132-SEQ-02.2 Unrecognized Session. The request made was for a SessionId that is different from the one used to communicate with the equipment, and it does not exist in the current list of active sessions. The equipment application returns to the READY state and continues to monitor its current session. No session is terminated or closed by the equipment or the client.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). The equipment returns to READY state and continues to monitor its current session. No session is terminated.
- E132-SEQ-09.3 Attempt to Close Invalid Session. A session manager application specifies in the request input parameter a nonexistent session. The equipment rejects the request and keeps its current sessions active.

### 8.1.10 Maximum Session Setting Change Scenario

The administrative application can set the session number below or above the number of sessions based on the equipment-allowed session number. There is no active session affected if the setting is below the current number of active sessions. The settings apply only to future requests. The administrator always gets a session granted even if the number of active sessions is equal to the maximum sessions allowed.

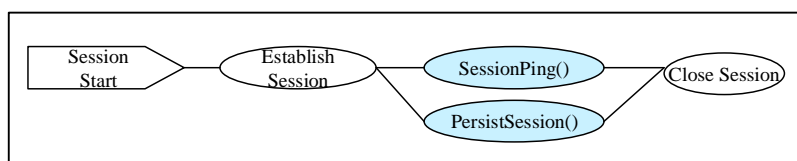


**Figure 22 E132-SCN-04 Max Session Setting Change Scenario**

The previous scenario demonstrates the use of session administration services. In the scenario, the managing application checks the number of active sessions, checks the current maximum allowed sessions, and changes to a new setting. This scenario is typical of those situations when the factory may want to limit the number of allowed sessions at the equipment. The administrative session is not required to close any session if the new setting is below the number of active sessions. It just means that once the sessions are closed, they will be limited by the allowed number of sessions.

### 8.1.11 Session Operation Services

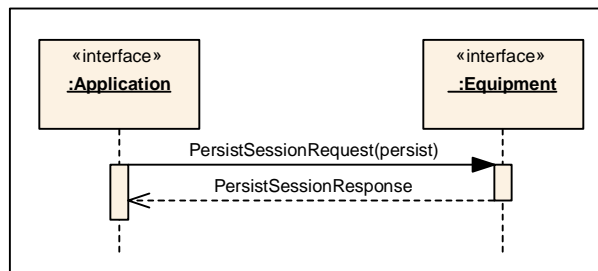
These two services are commonly used to ensure the equipment is aware that the client session is alive and to make it persistent. “SessionPing” notifies the equipment or application that the session is still open or alive. The request to have a session persist is always related to an application that will be interested in always receiving data from the tool. A “Fault Detection System” is an example of one of these systems.



**Figure 23 Generic Session Operational Services**

### 8.1.11.1 PersistSession()

If the client is requesting that the session persist (TRUE), the equipment stores the client's current session context that includes the session identifier, endpoint address information, and assigned privileges. (See SEMI E132 for a definition of this structure.) Once the session persists, it remains active across equipment shutdowns, being reactivated at power up as soon as the equipment is in a state where it can support communications. Persistent sessions can be terminated if the equipment determines that the client can no longer be reached. If the client uses this operation to remove persistence from the session state (FALSE), the equipment removes the client's session context from memory, and the session will not persist when the equipment is restarted.



**Figure 24 E132-SEQ-10 Persist Session Service**

#### 8.1.11.1.1 Normal Cases

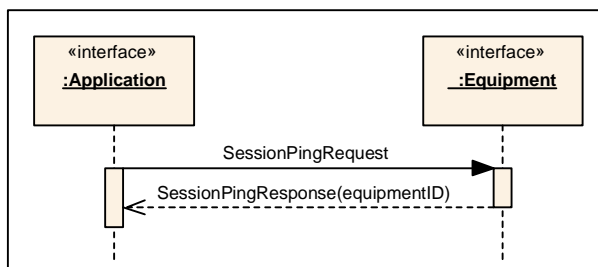
- E132-SEQ-10.1 Persist set to True. The equipment tries to set the session as persistent. This will not be needed in the future since the standard will require that all sessions be persistent.
- E132-SEQ-10.2 Persist set to False. (See description above.)

#### 8.1.11.1.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). The equipment returns to the READY state and continues to monitor its current session. No changes are made to the session setting.

### 8.1.11.2 SessionPing() [Client]

When the client issues this service, the equipment replies with its identifier. Identifiers are preconfigured by an administrator application and must be the same one as the one used during authentication. If an identifier was not assigned by the administrative application, the identifier used is an identifier assigned by the equipment.



**Figure 25** E132-SEQ-11 Session Ping Service [Client]

#### 8.1.11.2.1 Normal Case

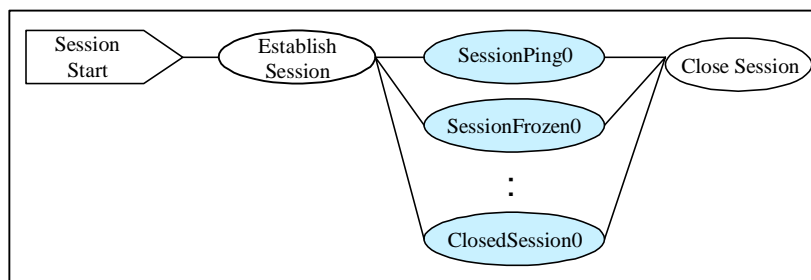
- E132-SEQ-11.1 Session Ping. The client tries to reconnect with the equipment.

#### 8.1.11.2.2 Exception Case

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the sender included an incorrect SessionID. The equipment rejects the request and returns to READY state.

### 8.1.12 Equipment Notification Services

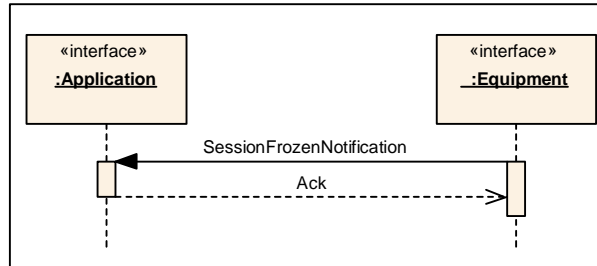
In particular cases, the equipment may be shut down for upgrades or put out of service for scheduled or unscheduled maintenance. Before these activities start, the client applications must be informed that the equipment is being taken off line by notification that the session is being closed or is hibernating. The equipment uses a ping service to wake up its clients once it comes back on line. SessionPing() [Equipment] is the service that enables the equipment to re-establish sessions with its clients.



**Figure 26** Equipment Notification Services

### 8.1.12.1 SessionFrozen()

This is a notification message sent by the equipment to indicate to clients that have persistent sessions that communications will stop because equipment communication is being shut down. From the client's perspective, the equipment will not answer the session pings it sends. The equipment sends only one notification for each persistent session before it goes off line.



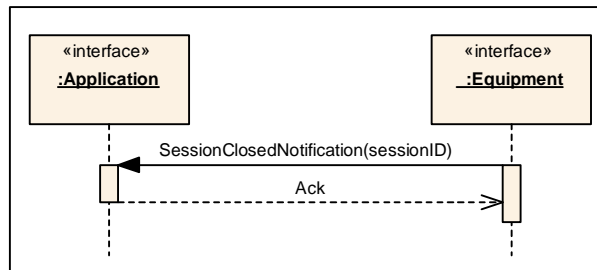
**Figure 27 E132-SEQ-12 Session Frozen Notification**

#### 8.1.12.1.1 Normal Case

- E132-SEQ-12.1 Session Frozen Notification. The equipment informs its clients that their session is being saved.

### 8.1.12.2 SessionClosed()

The behavior of this service is different from the CloseSession() service described above. This notification service is used by the equipment to notify a client that it's session is being terminated by the equipment. The session was not defined as a persistent session and is being closed by the equipment or an administrative application.



**Figure 28 E132-SEQ-13 Session Closed Notification**

#### 8.1.12.2.1 Normal Cases

- E132-SEQ-13.1 Session Closed Notification. The equipment informs its clients that their session is being closed.

### 8.1.12.3 SessionPing() [Equipment]

When the client receives this message from the equipment, the client replies with its assigned identification. The client identification returned must be the same one assigned by the administrative application and the one used by the client during the first EstablishSession() request. Otherwise, the equipment will have no record of the equipment identifier and will close the persistent session.

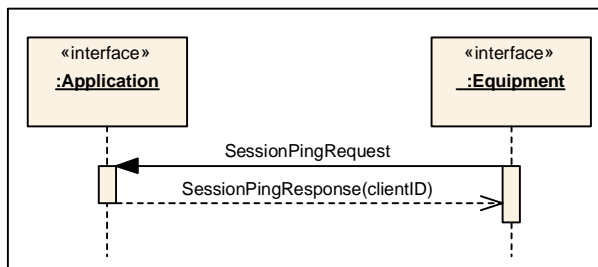


Figure 29 E132-SEQ-14 Session Ping Service [Equipment]

#### 8.1.12.3.1 Normal Case

- E132-SEQ-14.1 Session Ping Request. The equipment tries to reconnect with the client application.

#### 8.1.12.3.2 Exception Case

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the sender included an incorrect SessionID. The equipment rejects the request and returns to READY state.

### 8.1.13 Administrator Closes Session Owned by Another User Scenario

This scenario indicates that the administrative application has privilege to close any active session. This operation is possible when clients or equipment are being taken off line for maintenance or physical reconfiguration.

Additional scenarios showing the equipment behavior when the client goes away or when the equipment gets disconnected is described in section 10.

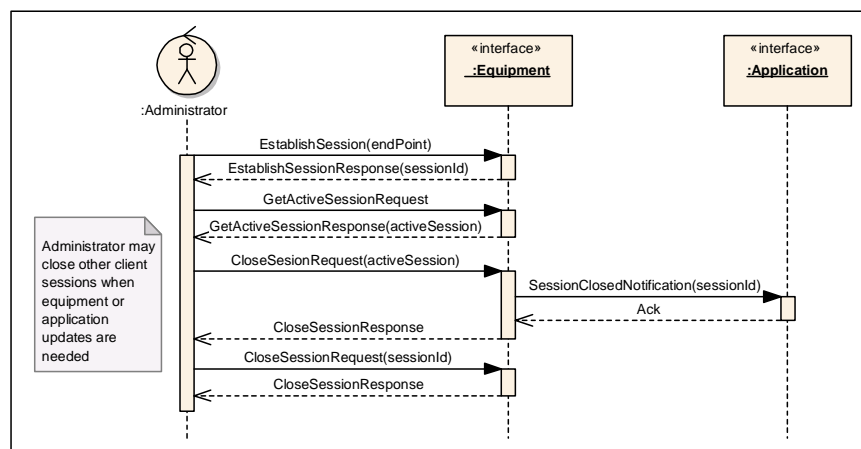


Figure 30 E132-SCN-05 Administrator Closes Session Owned by Another Client

## 8.2 Equipment Self Description Standard (E125)

SEMI E120, *Common Equipment Model Standard*, describes how the equipment's physical structure is used to describe the parameters, events, ObjTypes, and exceptions available from the equipment's internal element (or node) based on the equipment hierarchy. These descriptions indicate that the specified equipment node acts as the source of all Events, Exceptions, ObjTypes, and Parameters that are included in the node description. Two groups of services have been defined to separate a particular functionality:

- Metadata Query Services
- Metadata Management Service

### 8.2.1 Metadata Query Services

All Parameters, Exceptions, ObjTypes, and Events associated with a given equipment node are independent of the Events, Exceptions, ObjTypes, and Parameters associated with other equipment nodes. A collection of calls is used to retrieve this information from the equipment XML instance file. These services are GetUnits, GetTypeDefinitions, GetStateModels, GetSEMIObjTypes, GetExceptions, and GetEquipmentStructure.

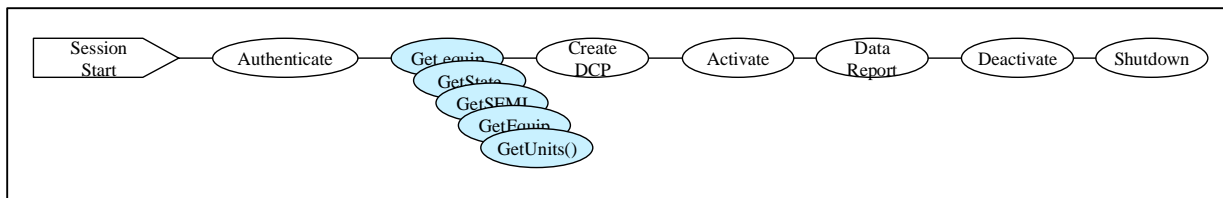


Figure 31 Metadata Query Services

#### 8.2.1.1 GetEquipmentStructure()

This service requests the complete structural metadata defined by the equipment. This service basically requests the SEMI E120 implementation from the equipment.

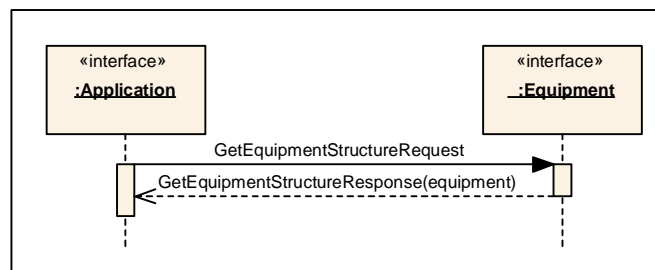


Figure 32 E125-SEQ-01 Get Equipment Structure Service

### 8.2.1.1.1 Normal Case

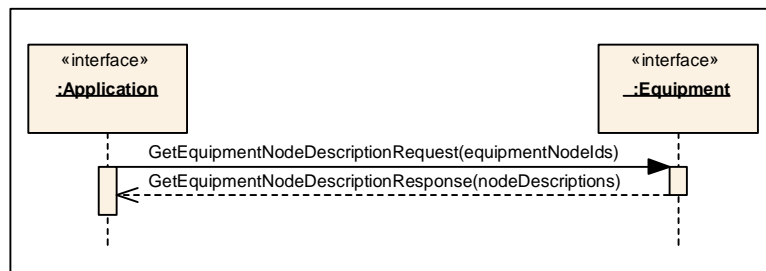
- E125-SEQ-01.1 Request to retrieve equipment structure defined in the metadata.

### 8.2.1.1.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). No metadata structure is returned with the response.

### 8.2.1.2 GetEquipmentNodeDescriptions()

This service requests the list of equipment node description metadata. If the request includes unrecognized equipment node identifiers, the equipment returns only descriptions for recognized node identifiers.



**Figure 33 E125-SEQ-02 Get Equipment Node Description Service**

### 8.2.1.2.1 Normal Case

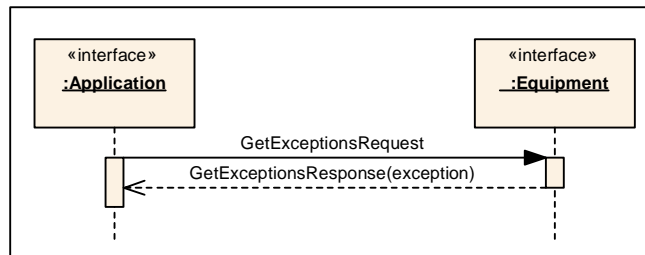
- E125-SEQ-02.1 Request to retrieve node information defined in the equipment metadata. If the request includes any non-valid node association, the service returns an empty value for those nodes that the equipment does not have instead of an exception.

### 8.2.1.2.2 Exception Cases

- E125-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E125-SEQ-02.3 Operation Not Authorized (context information required about the denied request). No node description returned with the equipment.

### 8.2.1.3 GetExceptions()

This service requests all exception metadata provided by the equipment. This service is not associated with any equipment node, module, or subsystem.



**Figure 34 E125-SEQ-03 Get Exceptions Service**

#### 8.2.1.3.1 Normal Case

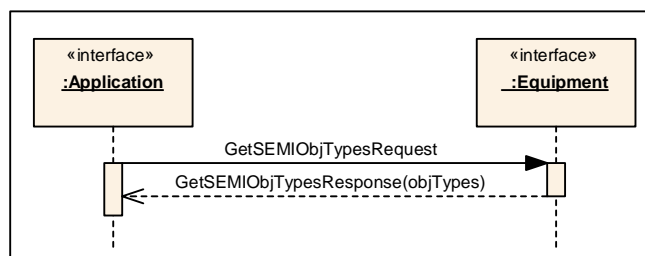
- E125-SEQ-03.1 Request to retrieve exceptions defined in the equipment metadata.

#### 8.2.1.3.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). No exception list is returned with the response.

### 8.2.1.4 GetSemiObjTypes()

This service returns all ObjType metadata provided by the equipment. This service is not associated with any equipment node and returns all ObjTypes currently defined for the equipment.



**Figure 35 E125-SEQ-04 Get Semi ObjTypes Service**

#### 8.2.1.4.1 Normal Case

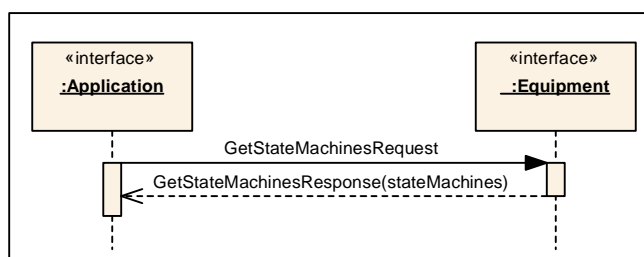
- E125-SEQ-04.1 Request to retrieve SEMI ObjTypes defined in the equipment metadata.

#### 8.2.1.4.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). No ObjTypes are returned with the request.

#### 8.2.1.5 GetStateMachines()

This service returns all the state machines defined at the equipment.



**Figure 36 E125-SEQ-05 Get State Machines Service**

#### 8.2.1.5.1 Normal Case

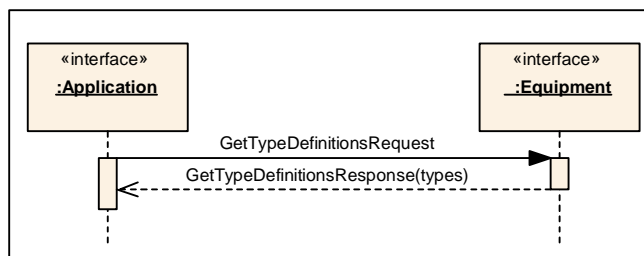
- E125-SEQ-05.1 Request to retrieve state machines defined in the equipment metadata.

#### 8.2.1.5.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). No state models are returned with the service response.

#### 8.2.1.6 GetTypeDefinitions()

This service retrieves all metadata type definitions provided by the equipment. This service is not associated with any equipment node or data parameter. This is a call to retrieve type definitions from the equipment in general.



**Figure 37 E125-SEQ-06 Get Type Definitions Service**

### 8.2.1.6.1 Normal Case

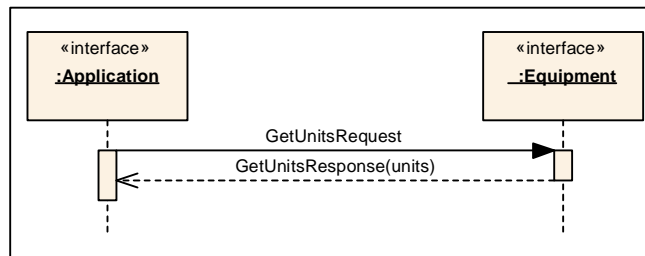
- E125-SEQ-06.1 Request to retrieve defined types in the equipment metadata.

### 8.2.1.6.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). No data types are returned with the response.

### 8.2.1.7 GetUnits()

This service retrieves all units provided by the equipment. This service is not associated with any equipment node or parameter definition. A unit represents a description of the magnitudes the equipment is capable of reporting from certain weighted values.



**Figure 38 E125-SEQ-07 Get Units Service**

#### 8.2.1.7.1 Normal Case

- E125-SEQ-07.1 Request to retrieve units defined in the equipment metadata.

#### 8.2.1.7.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). No Units list is returned.

## 8.2.2 Equipment Metadata Query Scenario

This scenario indicates a possible sequence of services that the client may send to the equipment to retrieve metadata information defined in the equipment XML instance file. A factory application sorts and creates a view of the equipment metadata information in a useful manner that is not defined or specified in this document. These query services are defined to optimize the retrieval of metadata information.

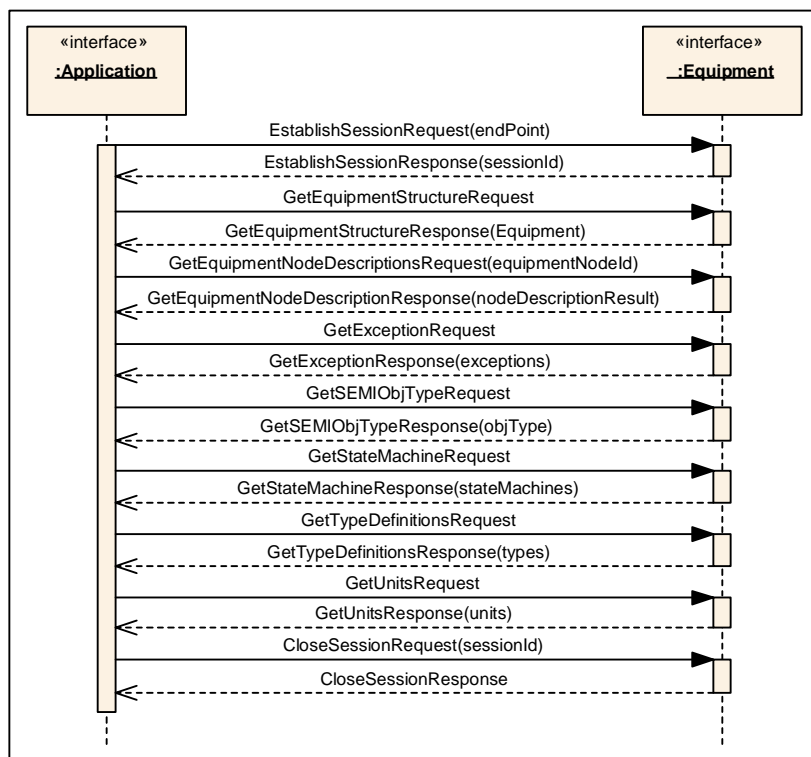


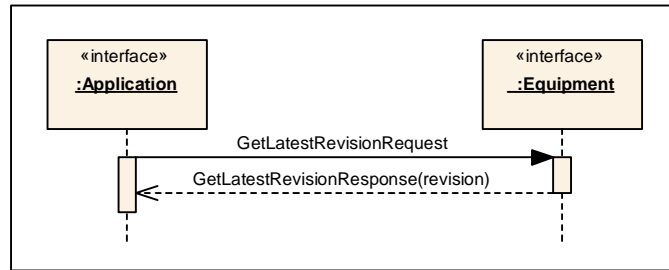
Figure 39 Equipment Metadata Query Scenarios

## 8.2.3 Metadata Management Services

When a change in the physical or logical equipment configuration results in a structural or metadata change, the equipment must update the metadata description accordingly. If clients subscribed to the equipment have requested revision notification, the equipment must notify each interested client after the metadata file is updated or at the first occasion its communication permits. The following services have been defined to allow a client to find out about the equipment metadata file version and metadata changes or register with the equipment to be notified of any changes.

### 8.2.3.1 GetLatestRevision()

This service requests the equipment to provide the most recent revision information of the metadata file. The equipment stores the date and time of the most recent change in non-volatile memory and makes it available to any client authorized to query this information.



**Figure 40 E125-SEQ-08 Get Latest Revision Service**

#### 8.2.3.1.1 Normal Case

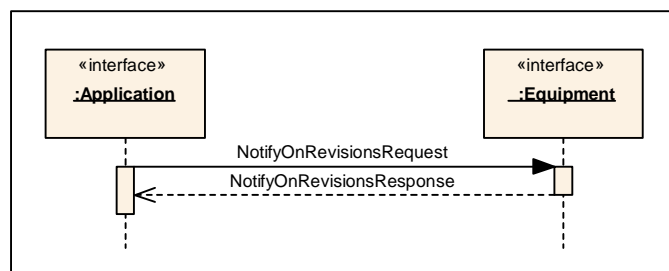
- E125-SEQ-08.1 Request to retrieve latest version of metadata defined in the equipment. Current version of the metadata information returned with the request.

#### 8.2.3.1.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). No value for revision is returned with the response.

#### 8.2.3.2 NotifyOnRevisions()

This service requests the equipment to either enable or disable metadata revision notices for the requesting client such that when the metadata information is updated, the client is informed of this change.



**Figure 41 E125-SEQ-09 Notify On Revisions Service**

#### 8.2.3.2.1 Normal Case

- E125-SEQ-09.1 Request to being notified when the metadata changes in the equipment

#### 8.2.3.2.2 Exception Case

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). The request is denied by the equipment.

### 8.2.3.3 MetadataRevisedNotification()

The equipment sends this notification whenever it detects a change in the metadata. The client must have made a previous request to be notified through the NotifyOnRevisions service previously.

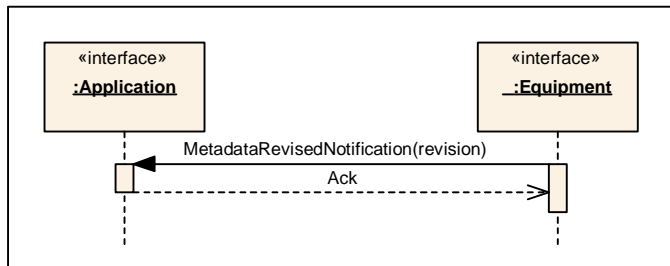


Figure 42 E125-SEQ-10 Metadata Revised Notification

#### 8.2.3.3.1 Normal Case

- E125-SEQ-10.1 Request to retrieve units defined in the equipment metadata.

### 8.2.4 Metadata Notification Changed Scenario

The following scenario shows the equipment-expected behavior after a change in the metadata file when the client has registered to be notified of any metadata changes in the equipment instance file. The client may retrieve the current revision date/time of the metadata and store it for future comparison. The notification includes new date/time information that will be used to update records or initiate a need to review current data collection plans.

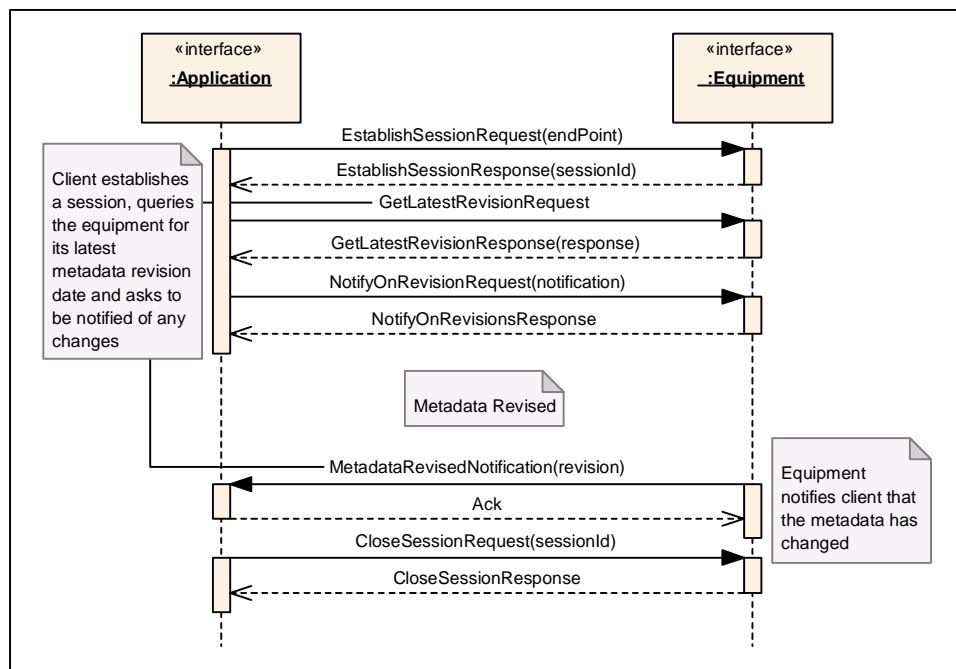
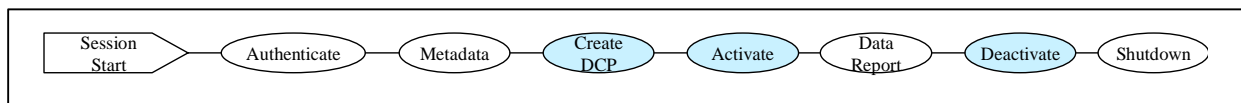


Figure 43 E125-SCN-01 Metadata Notification Scenario

### 8.3 Data Collection Plan Management (E134)

Data Collection Plan Management defines services that enable a client to collect data from the equipment. This data can be triggered by events or exceptions, and it can come as a single instance in time triggered by the plan or a collection of information through a fixed interval of time. Services are provided for clients to define one or more data collection plans off-tool and submit those definitions to the equipment. The Data Collection Manager interface provides operations to request the current equipment performance status as well as equipment data on demand. Three functional groups have been defined:

- DCP Management Services
- DCP Query Services
- DCP Performance Warning Services



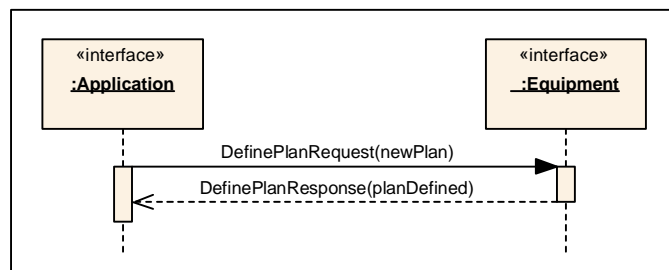
**Figure 44 Data Collection Plan Management Services**

#### 8.3.1 DCP Management Services

The Data Collection Manager interface provides clients with operations to manage data collection activities on the equipment, including submitting new Data Collection Plans, activating and deactivating plans, looking up existing plans, and deleting defined plans.

##### 8.3.1.1 DefinePlan()

The client application defining a new Data Collection Plan uses this service. The equipment validates the plan name for uniqueness and all referenced events, exceptions, parameters, and trace reports for existence and correctness. If there are any issues with the submitted plan, the equipment returns a description of all problems detected with the plan and the plan definition fails on the equipment.



**Figure 45 E134-SEQ-01 Define Plan Service**

##### 8.3.1.1.1 Normal Case

- E134-SEQ-01.1 Trace Plan, Events Plan, Exception Plan, and combinations are also possible.

### 8.3.1.1.2 Exception Cases

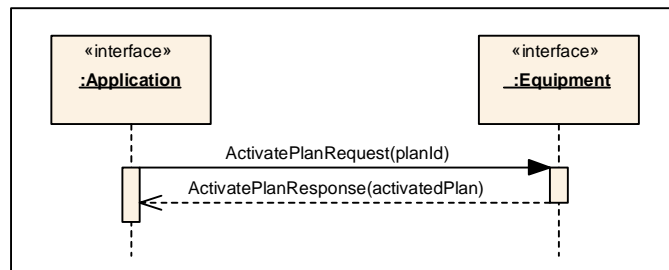
- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). The requested data collection plan is not created.
- E134-SEQ-01.2 Invalid Plan Type. This error includes the following set of cases:
  - Invalid Event
    - Invalid Parameter
      - Invalid Source Id
      - Invalid Event Id
      - Not Produced by Source
      - Is duplicate
    - Invalid Exception
      - Invalid Parameter
        - Invalid Source Id
        - Invalid Exception Id
        - Invalid Severity
        - Not Produced by Source
        - Is duplicate
  - Duplicate PlanId
  - Invalid Trace Request
    - Invalid Parameter
      - Invalid Source Id
      - Invalid Parameter Name
      - Not Produced by Source
      - Invalid Context
    - Invalid Trigger
      - Invalid Start Trigger
      - Invalid Event Trigger
      - Invalid Exception State
      - Invalid Source Id
      - Invalid Item Id
      - Not Produced by Source
      - Is Duplicate
    - Invalid Interval
    - Invalid Cycle
      - Needs Start Trigger
      - Needs Stop Trigger

No data collection plan created by the equipment. Equipment returns to the READY state.

- E134-SEQ-01.3 Invalid Argument Provided. Requested data collection plan is not created. Equipment returns to the READY state. This is a special case of an invalid PlanId that requires its own exception case because it is not covered in the case defined above.

### 8.3.1.2 ActivatePlan()

This service activates a defined DCP. The equipment begins sending all DCP events, exceptions, and trace data collection reports to the client according to buffering as specified in the DCP. The client can activate multiple plans. Multiple clients can activate the same DCP. The equipment must not activate a DCP more than once for the same client.



**Figure 46 E134-SEQ-02 Activate Plan Service**

#### 8.3.1.2.1 Normal Case

- E134-SEQ-02.1 Request to activate a defined plan

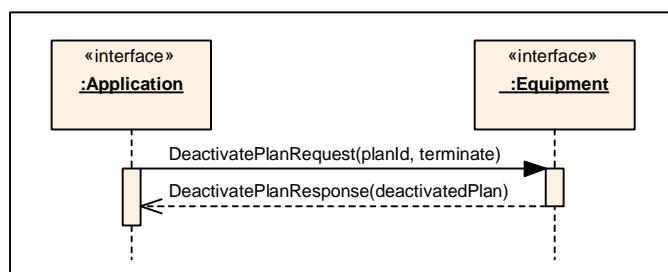
#### 8.3.1.2.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). The requested plan is not activated.
- E134-SEQ-02.2 Invalid/Non Existent Plan. Requested data collection plan is not activated. Equipment returns to the READY state.
- E134-SEQ-02.3 Already Active Plan. Equipment returns to the READY state. This case occurs only for a client that has already activated the requested plan. It does not apply to other clients trying to activate another client's active plan.

### 8.3.1.3 DeactivatePlan()

When the client issues this service, the equipment stops reporting data from the specified DCP. If no other clients are receiving data from the identified DCP, the equipment will disable all collection activity related to this DCP. When used together with a request to terminate (TRUE), the equipment terminates all DCPs currently active on the equipment for all clients, including those that have been activated by the requesting client. The equipment must notify each client of the reason for the termination using the DCPDeactivated notification. In some cases, the client may have activated several DCPs. If the client plans to shut down, it can issue a DeactivatePlan request with the argument “urn:semi-org:dcm:allDCPs.” This identifier instructs the equipment to deactivate all plans currently active for the requesting client. If other clients have activated any of the same plans, those clients continue to receive Data Collection Reports from those plans. The following exception cases have been identified for this service:

- The requesting client did not activate the DCP and the request is not a termination request.
- The request is a termination request, but a client did not activate the requested plan.
- The client does not have sufficient privileges to deactivate the requested DCP.



**Figure 47 E134-SEQ-03 Deactivate Plan Service**

#### 8.3.1.3.1 Normal Case

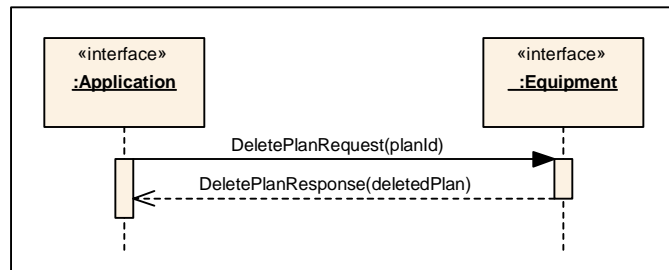
- E134-SEQ-03.1 DeactivatePlan() Terminate set FALSE. Requested plan is terminated for the requestor.
- E134-SEQ-03.2 DeactivatePlan() Terminate set to TRUE. Requested plan is terminated for all the clients using the plan.

#### 8.3.1.3.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). No changes are made to the requested plan and the equipment returns to the READY state.
- E134-SEQ-03.3 Invalid/Non Existent Plan. Equipment rejects the request and returns to the READY state.
- E134-SEQ-03.3 DCP Not Active. Equipment returns to the READY state.

### 8.3.1.4 DeletePlan()

The client deleting a DCP from the equipment uses this service. The equipment will reject this request if the requested plan is currently active for one or more clients. For a plan to be deleted, it must be deactivated (no client is currently receiving data produced by the plan). Built-in DCPs provided with the equipment cannot be deleted. The equipment must reject any request to delete a plan if the client does not have sufficient privilege



**Figure 48 E134-SEQ-04 Delete Plan Service**

#### 8.3.1.4.1 Normal Case

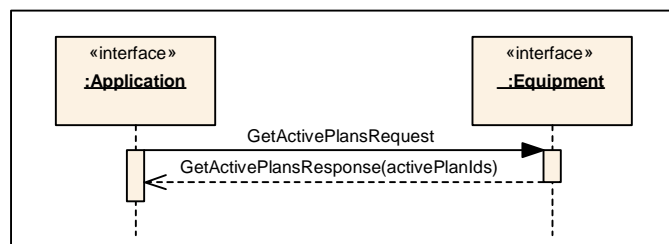
- E134-SEQ-04.1 Request to delete a defined plan. Requested plan deleted.

#### 8.3.1.4.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). Equipment returns to the READY state.
- E134-SEQ-04.2 Invalid/Non Existent Plan. Equipment returns to the READY state.
- E134-SEQ-04.3 DCP is Active. Equipment returns to the READY state.

### 8.3.1.5 GetActivePlans()

This service requests from the equipment a list of the DCP IDs that have been activated by the requesting client. If the client has sufficient privileges, the equipment returns the IDs of all active DCPs.



**Figure 49 E134-SEQ-05 Get Active Plans Service**

### 8.3.1.5.1 Normal Case

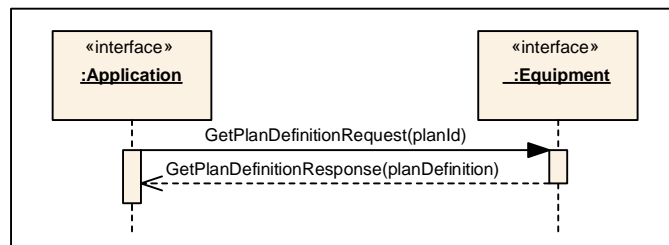
- E134-SEQ-05.1 Request to query all active plans. List of all active plans returned.

### 8.3.1.5.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). The equipment rejects the request and returns to READY state.

### 8.3.1.6 GetPlanDefinition()

This service allows the client to request the DCP definition of the specified DCP identifier. The equipment returns the requested plan definition to the client as it was originally submitted to the equipment.



**Figure 50 E134-SEQ-06 Get Plan Definition Service**

#### 8.3.1.6.1 Normal Case

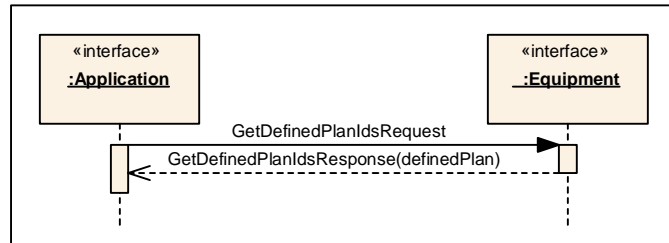
- E134-SEQ-06.1 Request to retrieve a particular defined plan. Requested plan definition returned.

#### 8.3.1.6.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). Equipment returns to the READY State.
- E134-SEQ-06.2 Invalid/Non Existent Plan. Request is rejected and equipment returns to the READY state.

### 8.3.1.7 GetDefinedPlanIDs()

This service returns a list of all currently defined data collection plan IDs that are accessible by the client. The list includes the time at which the IDs were defined and the ID of the client that defined them.



**Figure 51 E134-SEQ-07 Get Defined Plan IDs Service**

#### 8.3.1.7.1 Normal Case

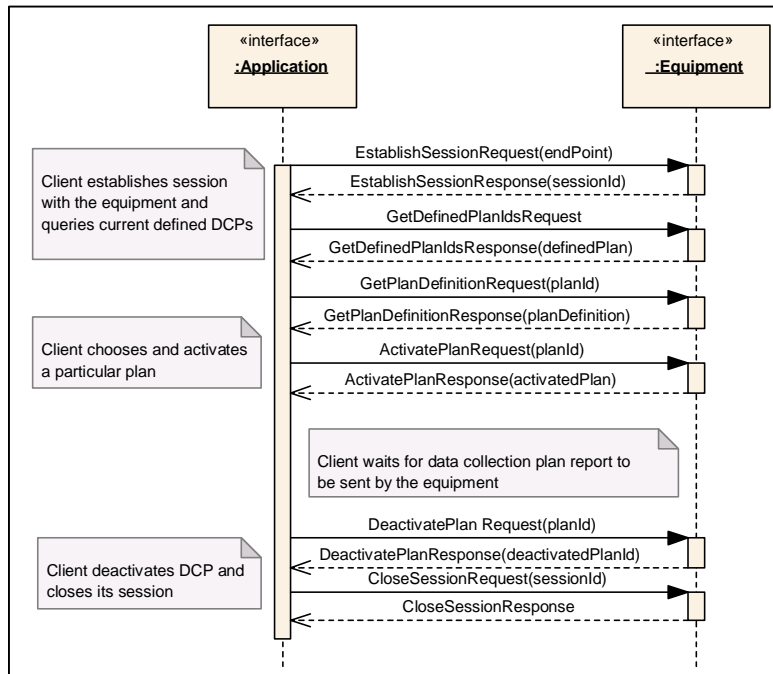
- E134-SEQ-07.1 Request to retrieve all the identifiers of the currently defined plans in the equipment. The equipment includes the identifiers of all plans defined in the equipment.

#### 8.3.1.7.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). Equipment rejects the request and returns to the READY state.

### 8.3.2 DCP Activation Scenario

This scenario shows a complete scenario for the creation, activation data reporting, and deactivations of a data collection plan. The equipment must verify the data collection plan specification before it stores the plan for validation. An invalid data collection plan cannot be activated. Data collection reporting depends on the tool type operation and the defined parameters. Event trace or exception reporting is possible. The deactivation of a data collection plan should not affect other clients receiving from the same DCP. Deactivation does not destroy or delete the plan from the equipment.

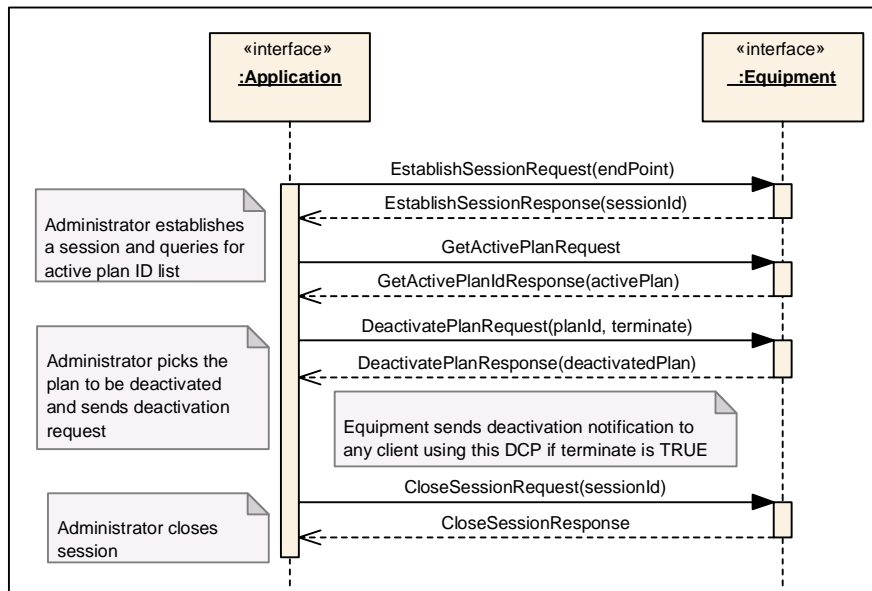


**Figure 52** E134-SCN-01 DCP Activation Scenario

### 8.3.3 DCP Deactivation Scenario

This scenario shows the usage of the attribute “terminate.” When the attribute is set to TRUE, any client receiving data from this DCP will be terminated and the equipment issues a notification indicating that the DCP has been terminated. If the client has multiple DCPs, it can then use the argument “urn:semi-org:dcm:allDCPs” to stop all DCPs activated by this client.

- E134-SCN-02 Terminate set to TRUE, All clients stop getting data



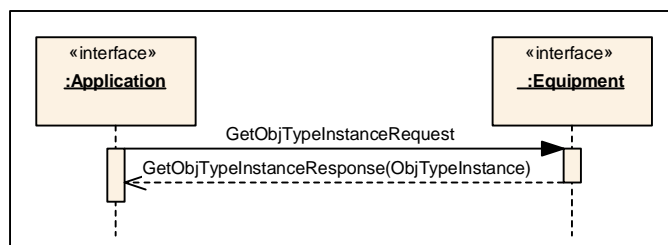
**Figure 53 E134-SCN-02 DCP Deactivation Scenario**

### 8.3.4 DCP Query Services

This service allows a client to query data ad hoc from E39-compliant objects that have been instantiated on the equipment or from data parameters that were defined with the metadata of the equipment node. A client interested in the attributes of specific E39 objects can make requests from a specific object instance only if the unique instance identification information for such objects is known. The client may then use that instance information to request E39-compliant object attribute values using either the GetParameterValues operation.

#### 8.3.4.1 GetObjTypeInstance()

This service is used to request the equipment to return a list of the instance identifiers of all SEMI E39-objects that are instantiated at the time of the request and are of the requested ObjType. Clients can request the list of all instances, all instances of a specific type, all instances from a specific source, or all instances of a specific type from a specific source. If the request includes unrecognized ObjTypes or sources, the equipment returns ObjTypeRequestError.



**Figure 54 E134-SEQ-08 Get ObjType Instance Service**

#### 8.3.4.1.1 Normal Case

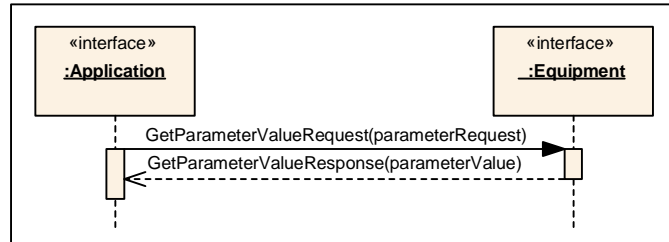
- E134-SEQ-08.1 Request to retrieve information about all ObjType instances. The equipment returns all object instances it currently has.

#### 8.3.4.1.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). Equipment rejects request and returns to the READY state.

### 8.3.4.2 GetParameterValue()

Clients trying to determine the current state of a parameter value in the equipment can use this operation. The equipment returns the most current values for the requested parameter at the time of the request.



**Figure 55 E134-SEQ-09 Get Parameter Value Service**

#### 8.3.4.2.1 Normal Case

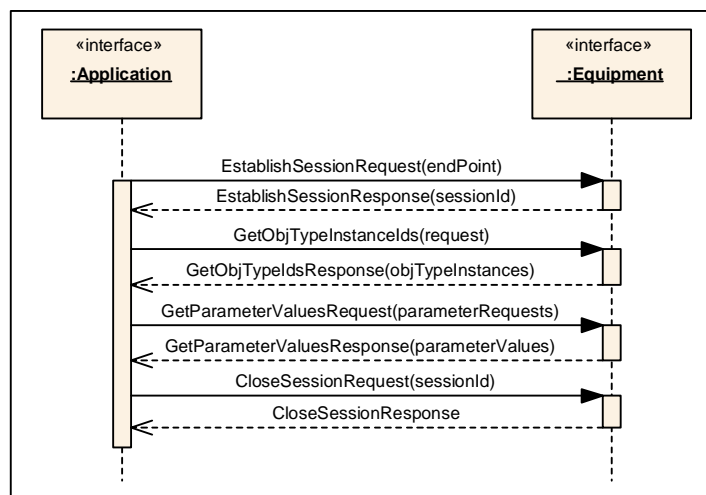
- E134-SEQ-09.1 Request to retrieve information about a particular parameter. The equipment returns the requested value.

#### 8.3.4.2.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the requestor included an incorrect SessionID. The equipment rejects the request and returns to READY state.
- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). Equipment rejects the request and returns to the READY state.
- E134-SEQ-09.2 Invalid Argument Provided. Equipment rejects the request and returns to the READY state.

### 8.3.5 ObjType Instance and Parameter Query Scenario

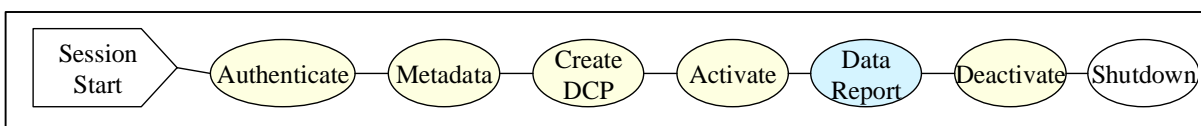
This simple scenario describes the service calls that the client application may perform to first look into a specific ObjType instance and then into a particular parameter value. It is quite possible that the client may query more than one parameter value content at a time. Since this is an ad hoc call, the equipment is responsible for returning the most recently updated parameter values.



**Figure 56** E134-SCN-03 Get ObjType Instance and Parameter Type Scenario

### 8.3.6 Equipment Data Report Service

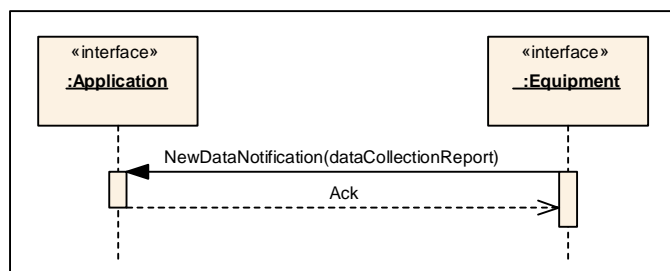
The equipment data report service refers to data collection report types that are created and sent to the client by the equipment. These report types can be events, alarms, or traces.



**Figure 57** Equipment Data Report Service

#### 8.3.6.1 New Data()

The equipment sends this notification whenever data from an active DCP is available for the client that activated the DCP.



**Figure 58** E134-SEQ-10 New Data Notification

### 8.3.6.1.1 Normal Case

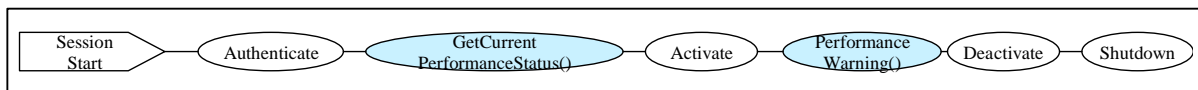
- E134-SEQ-10.1 Notification of data collection information based on previously activated plan. The equipment sends all requested values defined by the plan.

### 8.3.6.1.2 Exception Case

- E134-SEQ-10.2 Unrecognized Session. This error occurs when the notification included an incorrect SessionID. The client application rejects the request and returns to READY state.

## 8.3.7 DCP Performance Related Services

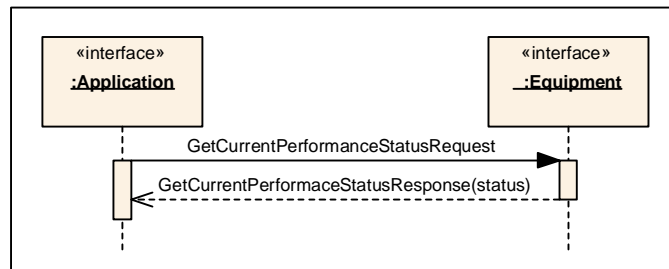
The equipment continuously monitors its operational performance status according to its established criteria (see SEMI E134). Each time the performance is evaluated, the equipment stores the job and DCP identifiers that were active when the evaluation was performed. This information is used to reply to the GetCurrentPerformanceStatus operation, the PerformanceWarning, and PerformanceRestored notifications. This information may help the application or the user decide to enable or disable a particular data collection plan. The equipment can also inform the client when it has recovered from a critical performance state into a normal state.



**Figure 59 DCP Performance Related Services**

### 8.3.7.1 GetCurrentPerformance()

This service requests the equipment about the most recently evaluated performance status.



**Figure 60 E134-SEQ-11 Get Current Performance Status Service**

#### 8.3.7.1.1 Normal Case

- E134-SEQ-11.1 Request to retrieve current equipment EDA interface performance. The equipment returns the defined performance parameter defined.

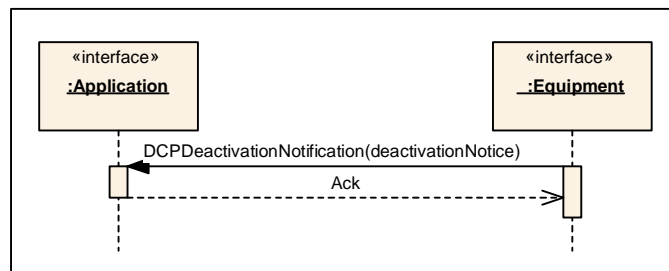
#### 8.3.7.1.2 Exception Cases

- E132-SEQ-02.2 Unrecognized Session. This error occurs when the notification included an incorrect SessionID. The equipment rejects the request and returns to READY state.

- E132-SEQ-02.3 Operation Not Authorized (context information required about the denied request). Equipment rejects the request and returns to the READY state.

### 8.3.7.2 DCPDeactivation()

The equipment sends this notification to a client whenever one or more DCPs that were activated by that client have been deactivated. The client may receive one or more data collection reports from the named DCPs after receiving this notification.



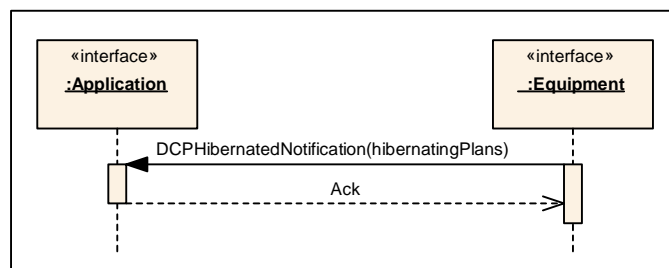
**Figure 61 E125-SEQ-12 DCP Deactivation Notification**

#### 8.3.7.2.1 Normal Case

- E134-SEQ-12.1 Notification to the client that its DCP is being deactivated. The equipment sends the deactivation notice.

### 8.3.7.3 DCPHibernation()

The equipment sends this notification to a client whenever one or more DCPs that were activated by that client are going into a hibernation state. The client may receive one or more data collection reports from the named DCPs after receiving this notification.



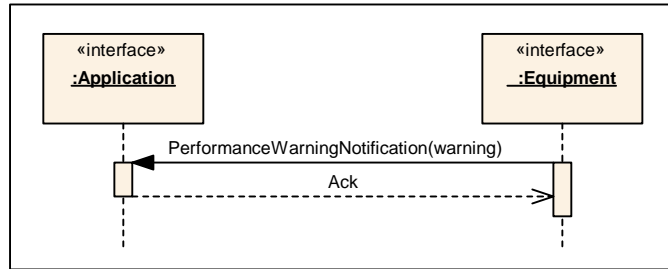
**Figure 62 E134-SEQ-13 DCP Hibernated Notification**

### 8.3.7.3.1 Normal Case

- E134-SEQ-13.1 Notification to the client that its DCP is being hibernated while the interface is taken out of service. The equipment sends the notification.

### 8.3.7.4 PerformanceWarning()

The equipment must send this notification to all clients that have Manage/Authoried DCP privileges or higher whenever operational performance has degraded below a supplier-specified threshold.



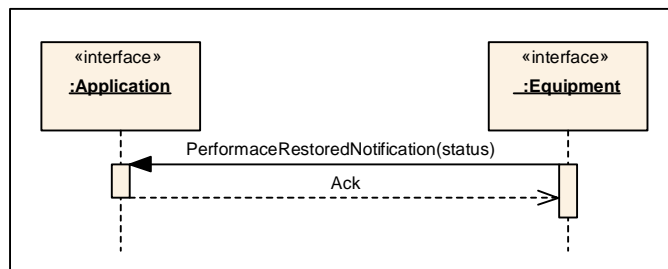
**Figure 63 E134-SEQ-14 Performance Warning Notification**

### 8.3.7.4.1 Normal Case

- E134-SEQ-14.1 Notification to the client that its DCP causing performance problems to the interface. After this notification the equipment sends the deactivation notice.

### 8.3.7.5 PerformanceRestored()

The equipment sends this notification to all clients with Manage Authoried DCP privileges or higher when the equipment operational performance has returned to normal thresholds.



**Figure 64 E134-SEQ-15 Performance Restored Notification**

### 8.3.7.5.1 Normal Case

- E134-SEQ-15.1 Notification to the client that the performance of the interface is now normal. The equipment sends the notice and returns to the READY state.

### 8.3.8 Performance Warning With Performance Restored Scenario

When the equipment has multiple clients or when the equipment is reporting for more than one data collection plan, the equipment needs to constantly check its performance such that the processing of material is not affected by the data collection and communication operations. The next scenario describes a situation where a client looks up the currently defined DCPs in the equipment and activates more than one plan. First the client activates one DCP and data is sent to the client. Then, the client decides to activate a second data collections plan. This plan affects performance of the equipment and the equipment sends the client notification that performance in the equipment has been affected. Since the equipment is responsible for shutting down any DCP request that affects performance, the scenario shows that the equipment notifies the client that the DCP is being deactivated and that performance has been restored. Finally, the client deactivates the first DCP and closes the session.

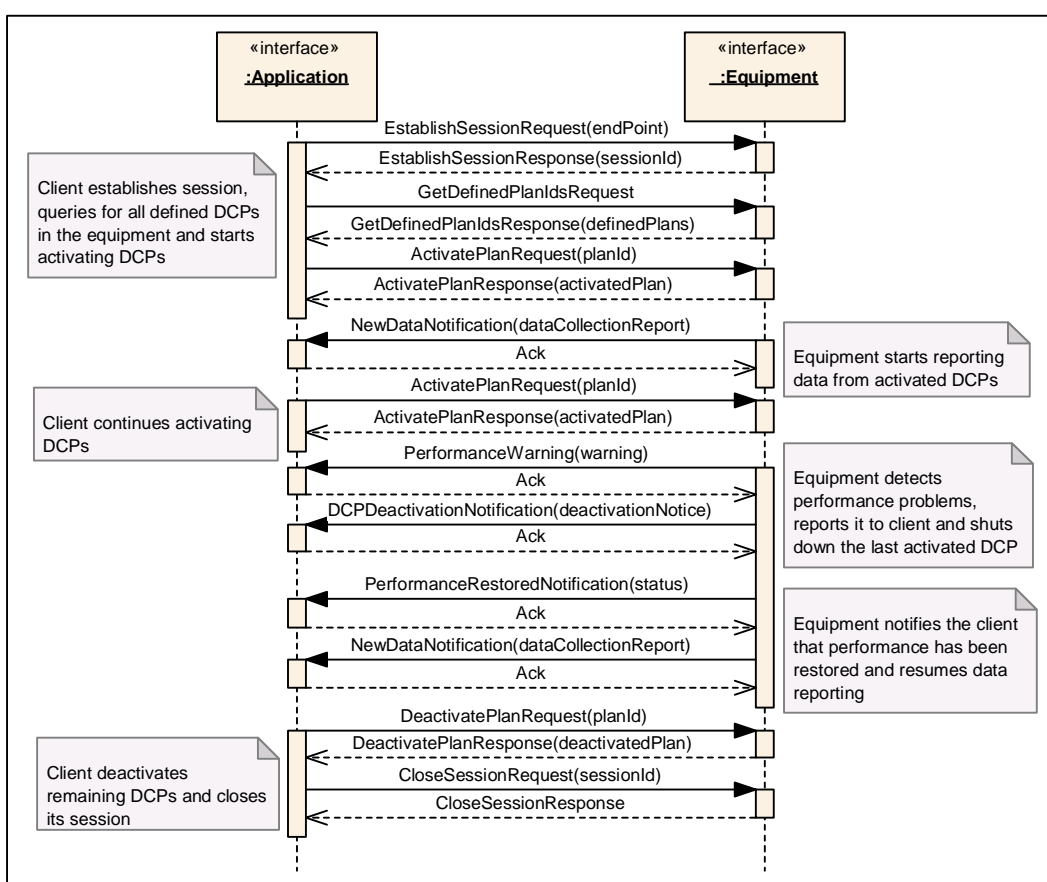


Figure 65 E134-SCN-04 Performance Warning With Performance Restored Scenario

## 9 GENERAL USAGE SCENARIOS

The next set of scenarios is a collection of interactions between multiple functions in the standards that describe situations where more than one client is involved. Single and multiple client and equipment combination scenarios are as follows:

- SCN-01 Basic EDA Usage Scenario
- SCN-02 Single Client Multiple DCPs Activate
- SCN-03 Multiple Clients Activating Same DCP
- SCN-04 Multiple Clients Multiple DCP
- SCN-05 Deactivate with More than One Client Receiving Data

No exceptions case scenarios have been defined yet for this section because the exception cases are already covered in the previous sections. Since there has not been enough learning accumulated by the factories in the use of the EDA interface, exception cases could not be created to be representative of the expected equipment or application behavior. Exception handling for general usage scenarios will be added at the future date.

### 9.1 Basic EDA Usage Scenario

An EDA basic scenario describes a general set of steps a client may take to activate a DCP. The request for establishing a session is the first step before engaging in a message exchange. This particular scenario does not describe creating a data collection plan, only the activation of one that has been already defined in the equipment. The client first gets the list of currently defined plans. Then, the client selects the one that it is most interested in reviewing. If the plan is one that the client can use, the client then activates it. The equipment reports the data as long as the data collection plan is activated. Once the client deactivates the plan, the equipment stops sending reports and then the client can close its session.

Another scenario not been included here is one in which the client retrieves the metadata from the equipment and then uses this information to create a DCP (Trace, Event, or Exception). It then sends the request to the equipment to create the DCP. Once the creation succeeds, it activates the plan and waits for data to be sent. After data collection is completed, the client deactivates the DCP and closes its session.

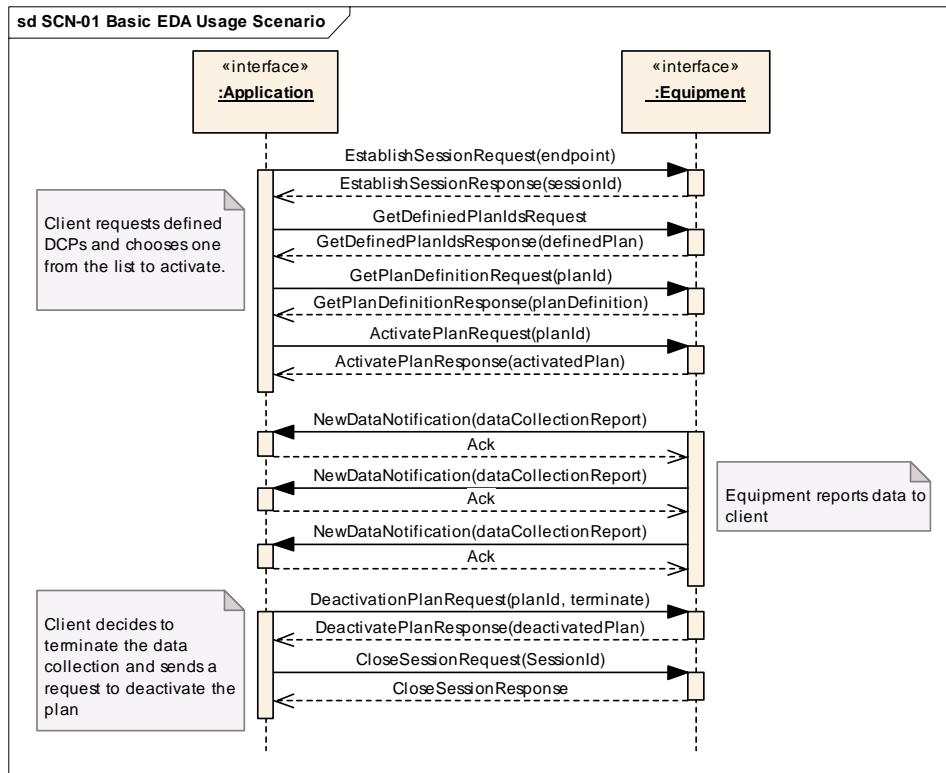


Figure 66 SCN-01 Basic EDA Usage Scenarios

### 9.2 Single Client Multiple DCP Activation

In this new scenario, one client is interested in receiving multiple reports from the equipment. Each report has a different purpose so two separate DCPs are created. First, the client creates a DCP and then activates it. While data is being reported to the client, it creates a second DCP and activates it. The equipment now reports two sets of data collection reports. After the client receives the requested data, the client deactivates the DCP. The remaining DCP continues to send data until it gets deactivated. The client then closes its session and disconnects from the equipment. This scenario demonstrates that it is possible to have one session and multiple DCPs reporting to the same client.

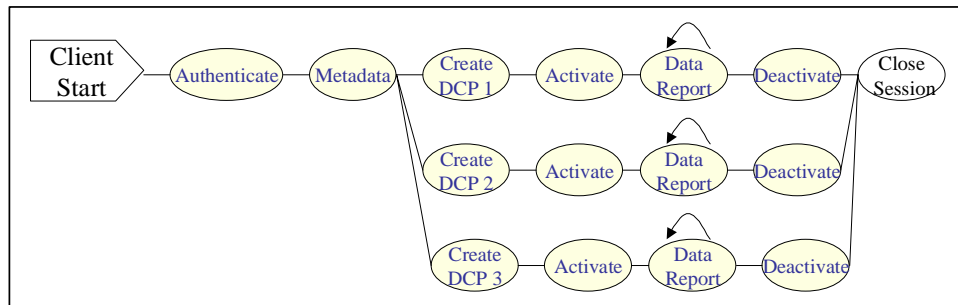


Figure 67 Single Clients Multiple DCP

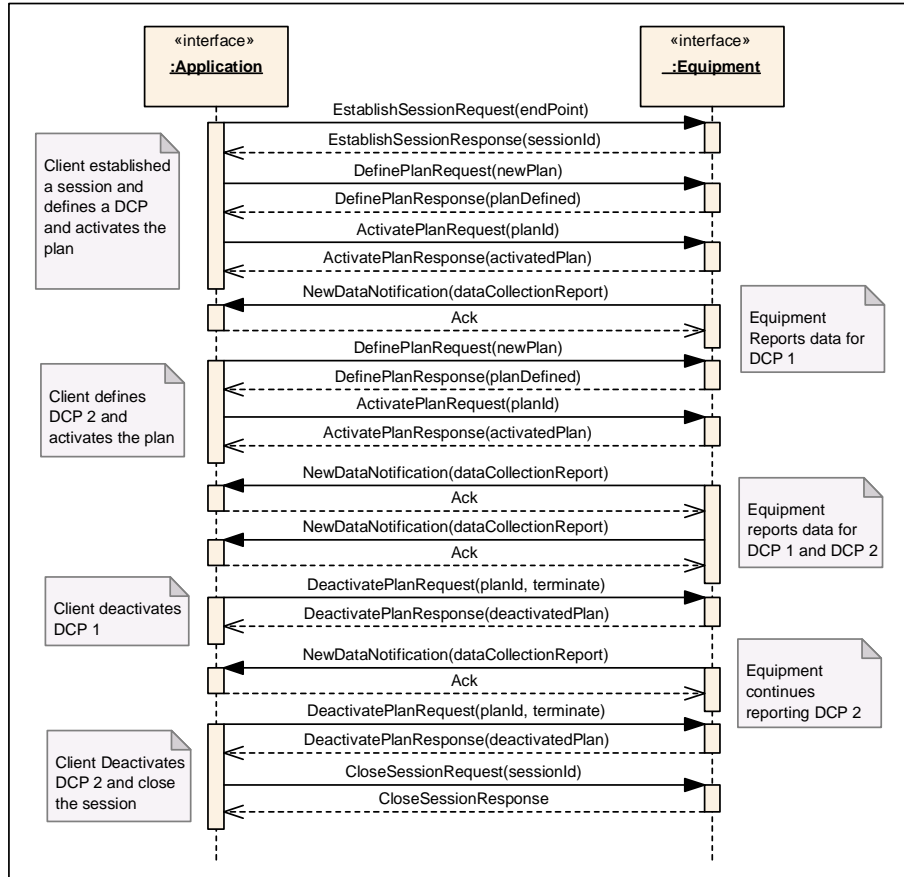


Figure 68 SCN-02 Single Clients Multiple DCP Activation Scenarios

### 9.3 Multiple Client – Single DCP

This scenario is included to demonstrate that it is possible to activate the same data collection plan from two independent sessions. In this scenario, the first application establishes a session and defines a DCP. Once the creation of the plan succeeds, the client activates the plan. At about the same time or shortly after the DCP activations, a second client establishes a session with the equipment. This client sends a request to query the current active DCPs. It asks the equipment for the definition of one of the active DCPs and then once it has verified its usability, the client activates the DCP. The newly activated DCP is the same one it created and activated by the first client depicted in the scenario. Data is then sent to both clients once the equipment has data to be reported for the activated DCP. The second client decides to stop receiving data, deactivates its DCPs, and closes its session without affecting the first client. The first client, as shown in the scenario, continues to receive data from the equipment until it deactivates the DCP and closes its session.

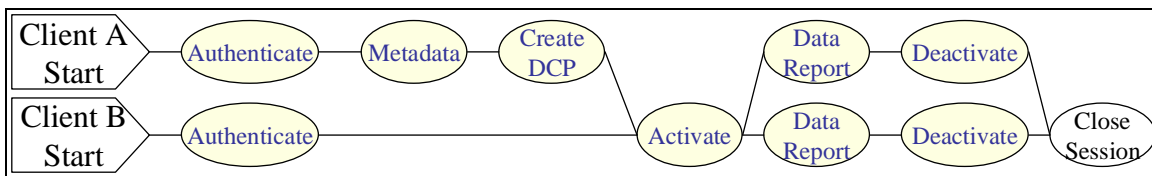


Figure 69 Multiple Client Single DCP

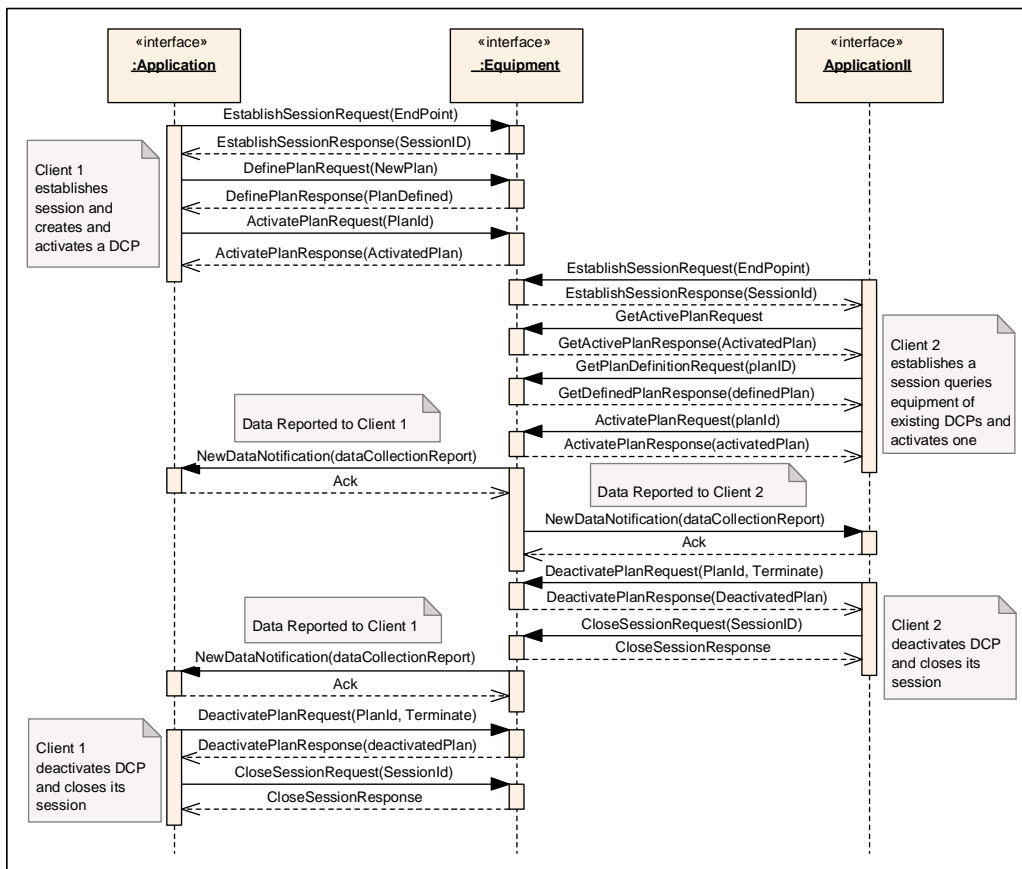


Figure 70 SCN-03 Multiple Client Single DCP Scenario

### 9.4 Multiple Client – Multiple DCP

This next scenario describes a different situation in which the equipment has been asked to activate two completely different and independent DCPs. Each of the clients creates its own DCP and activates it once the creation of the plan succeeds. As shown in the scenario, the equipment reports data for the first DCP that was activated and then reports data for the second DCP activated. At some point, the equipment reports data for both clients. The data reported might be different for each DCP or include some information that may be the same. Client 1 deactivates its DCP and closes its session without affecting the second client. The second client continues to receive data reports from the equipment until it deactivates its DCP and closes its session. This scenario demonstrates the equipment capability of reporting for more than one client using two independent DCPs.

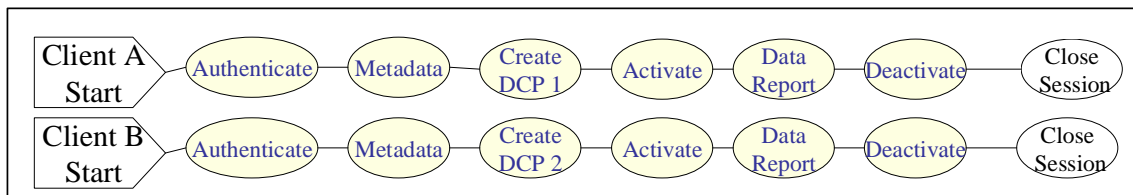
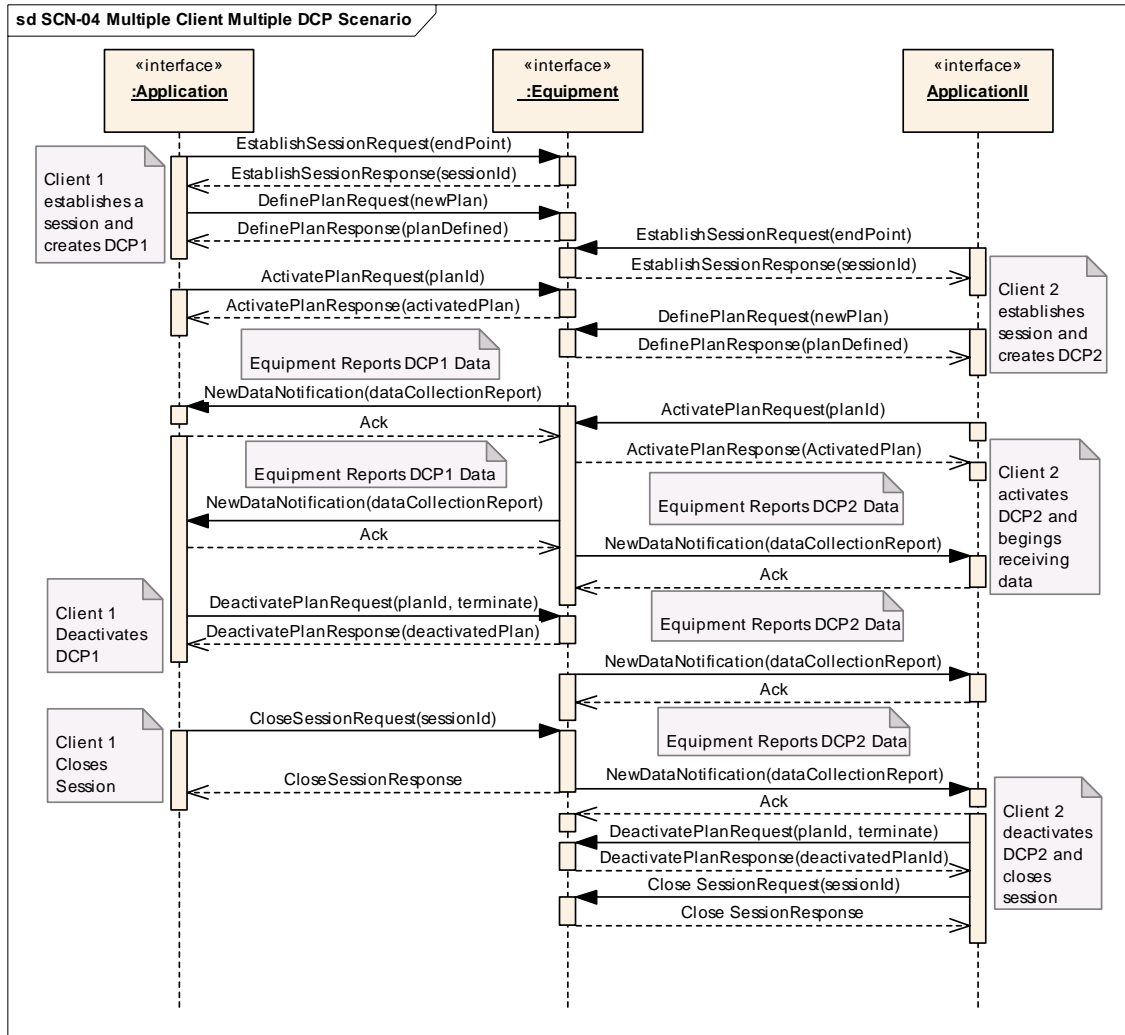


Figure 71 Multiple Clients – Multiple DCPs

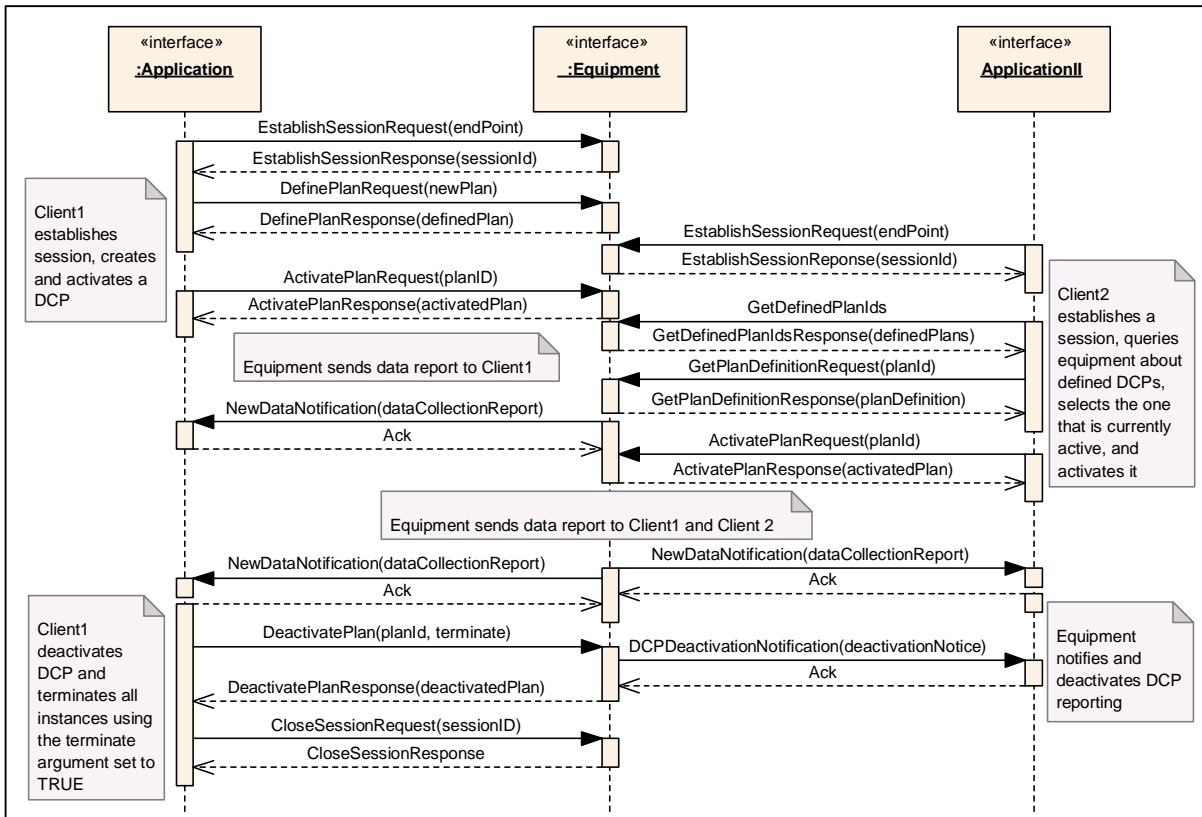


**Figure 72** SCN-04 Multiple Client Multiple DCP Scenario

### 9.5 Deactivation With More Than One Client Receiving Data

In this scenario, a client defines a plan and activates it. A second client establishes a session with the equipment and queries the tool for the defined plans. The second client requests the first client's DCP definition and while the first client is receiving data from this DCP, it activates the same DCP. Now the equipment reports to both clients. While this is happening, the first client decides to deactivate the DCP and delete it. It sends a deactivation request with the terminated attribute set to TRUE. This action affects all clients receiving from that DCP and requires the equipment to notify all its clients that the DCP is no longer available. Once the equipment terminates all data reporting for the terminated DCP, the equipment reports to the requesting clients that the DCP has been deactivated.

The clients subscribed to the equipment do not have their sessions closed until the administrator or the client itself closes its own session. This next scenario shows an example of how other clients are affected when more than one client is receiving data from the same DCP and the managing client decides to terminate and delete the DCP it owns.



**Figure 73** SCN-05 Deactivation With More Than One Client Receiving Data Scenario

## 10 EQUIPMENT RESTARTS

During normal factory operations, equipment can be taken off line for maintenance, upgrades, or unscheduled problems. Applications that subscribe to the equipment need to be notified when any of these situations occur. Factory applications expect the equipment to notify them during shutdown operations in a consistent way because they are responsible for collecting and storing information from multiple pieces of equipment. The following scenarios describe the expected behavior from the equipment when it has persistent sessions and data collection plans that need to be restarted automatically once the equipment comes back on line.

## 10.1 Equipment Restarts Persistent DCP Scenario

This scenario shows the effects of making a session persistent. In this example, a client activates a DCP and decides to make its session persistent. While the equipment is reporting data, the equipment shuts down. Before it completely closes communications, the equipment notifies that the DCP is going into hibernation and that the client's session is being frozen. This forces the client to stop sending pings and stops it from closing its session. The client then waits for the equipment to wake up and reconnect to the client through ping requests from the equipment. As shown in the scenario, the equipment starts sending ping services to the client who in turn uses the clientID to re-establish communication such that data collection can be resumed. Eventually, the client deactivates its plan and closes its session. It is not necessary to change the persistence status before closing a session. Closing a session terminates all future communication activities with that client.

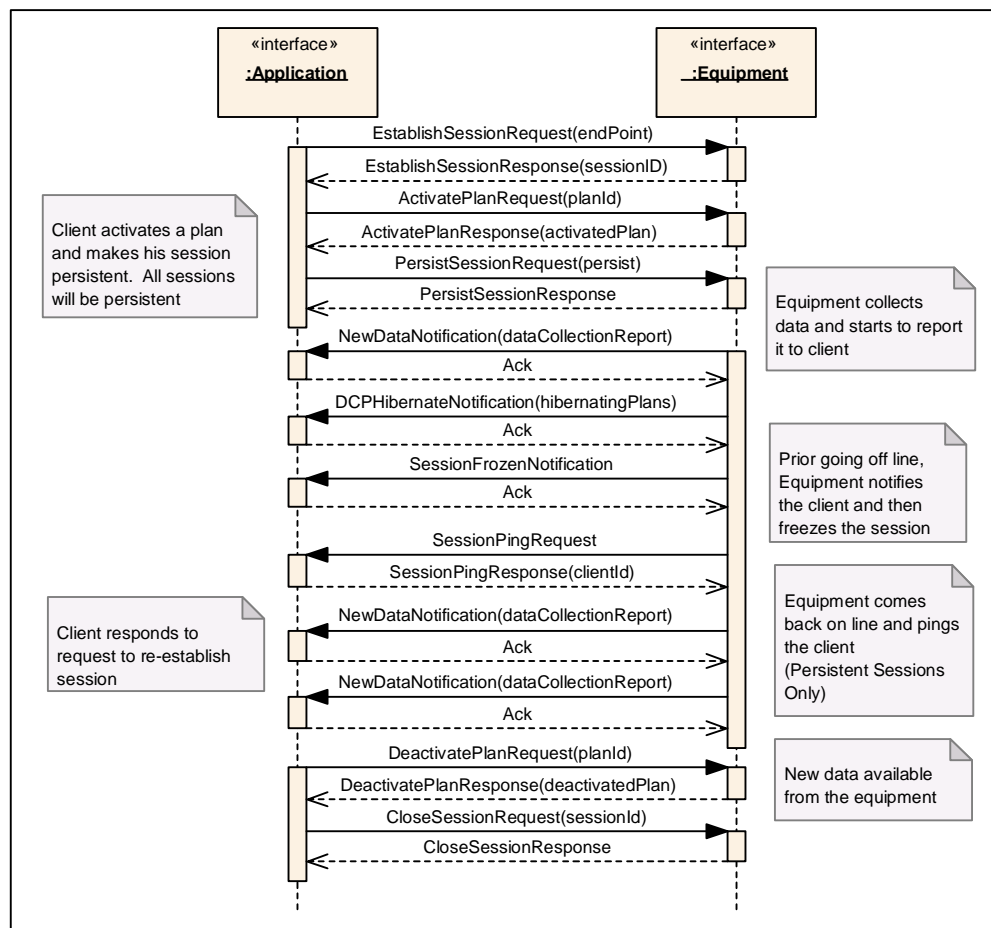


Figure 74 E134-SCN-05 Equipment Restarts With Persistent DCP Scenario

## 10.2 Equipment Restarts Persistent DCP With Metadata Change Scenario

This scenario is intended to demonstrate the importance of reporting metadata changes to all those clients that have subscribed to being notified. This scenario assumes that the client has requested to be notified of a metadata update. In the scenario, the client is interested in receiving data even after equipment shutdowns. Since the equipment will notify the client of the DCP hibernating and sessions being frozen, the interested client will re-establish communications once the equipment comes back on line.

Once the equipment re-establishes communication with its client, the equipment will first send a Metadata Notification service before a new data collection report is sent. The equipment is responsible for stopping any data collection plan that is affected by the metadata changes. The client may decide to stop receiving from the DCP but is not obligated to deactivate the plan. Notification of metadata changes is important for those applications that manage the creation of DCPs and use metadata for specific purposes. This is outside the scope of this document and therefore is not covered here. Once the notification has been sent, the tool resumes data reporting unless the DCP has been affected. In this case, the DCP is terminated by the equipment. All clients that are subscribed to the DCP receive notification that the DCP is being terminated.

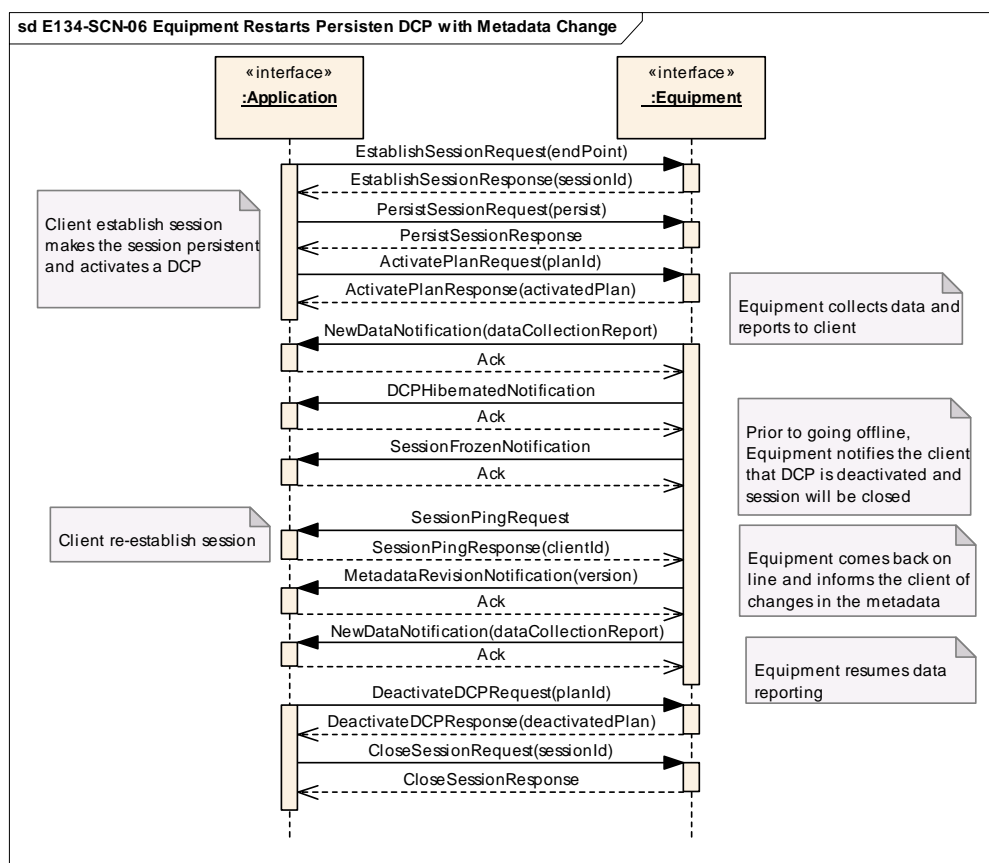


Figure 75 E134-SCN-06 Equipment Restarts Persistent DCP and Metadata Change

### 10.3 Equipment Restart Non-Persistent DCP Scenario

If a session is not persistent, when the equipment is going to be taken off line, the equipment notifies the sessions receiving from active DCPs using a deactivation notification and the equipment closes the session. In this scenario, no ping is sent by the equipment once it comes back on line since there are no persistent sessions defined.

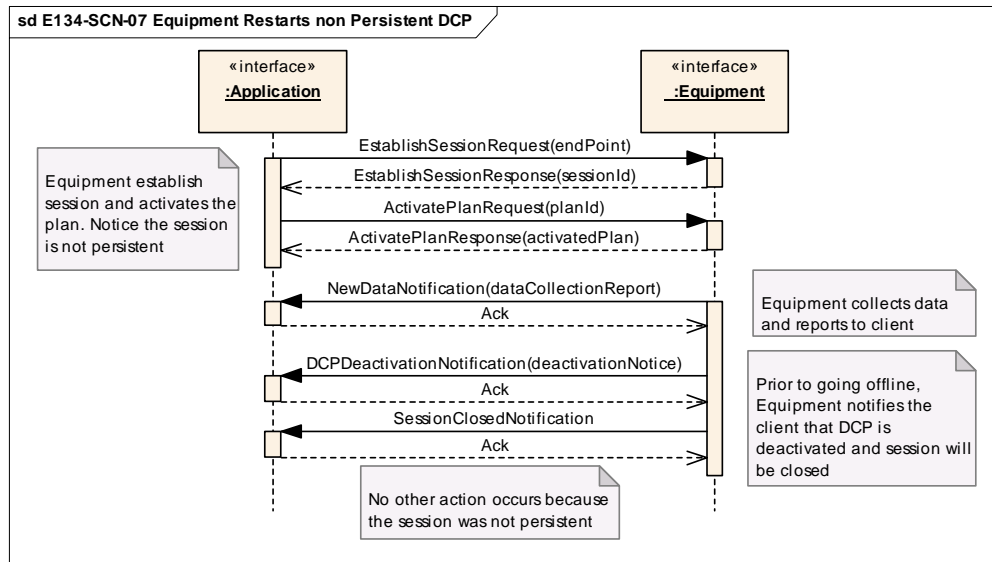


Figure 76 E134-SCN-07 Equipment Restarts Without Persistence Scenario



**International SEMATECH Manufacturing Initiative  
Technology Transfer  
2706 Montopolis Drive  
Austin, TX 78741**

**<http://ismi.sematech.org>  
e-mail: [info@sematech.org](mailto:info@sematech.org)**