INTERNATIONAL STANDARD

ISO/IEC 9506-1

First edition
1990-10-15

AMENDMENT 2

Industrial automation systems — Manufacturing Message Specification —

Part 1: Service definition

AMENDMENT 2: Conditioned service response

Systèmes d'automatisation industrielle — Spécification de messagerie industrielle —

Partie 1: Définition de service

AMENDEMENT 2: Réponse conditionnelle de service

Reference number
ISO/IEC 9506-1:1990/Amd.2:1995(E)

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Amendment 2 to International Standard ISO/IEC 9506-1:1990 was prepared by Technical Committee ISO/TC 184, *Industrial automation systems and integration*, Subcommittee SC 5, *Architecture and communications*.

Introduction

This amendment details the changes to ISO/IEC 9506-1 to support conditioned service response. In developing these changes, it is assumed that the changes from the inclusion of the Data Exchange Service, ISO/IEC 9506-1/Amd.1, and the changes from technical corrigendum ISO/IEC 9506-1/Cor.1, have already been applied to the base document. All clause number references refer to the document as amended and corrected; page number references refer to the base document.

This amendment adds a new object, an Access Control List, to the structure of the MMS VMD. The VMD references one such object that provides conditions that constrain the successful access of any object within the VMD by an MMS Client. In addition, each named object within a VMD references some Access Control List object, and the conditions expressed in that Access Control List object constrain the use of the parent object by an MMS Client. The present MMS system allows an MMS Server to support or deny support for any MMS service to an MMS Client for all object instances within its implementation; this amendment allows an MMS Server to offer support for a MMS service to an MMS Client for some object instances but not for others. If support of object specific access control is negotiated in the Initiate dialogue, the MMS client may examine and manipulate the Access Control List object of individual object instances.

The attribute MMS Deletable is removed from the object description of all MMS objects. In its place, a derivation rule is provided such that services that report MMS Deletable can do so in a manner consistent with implementations not employing this amendment.

There are seven classes of constraint, called Service Classes, that are covered by this amendment. These classes are Read, Write, Load, Store, Execute, Delete, and Edit. Not all classes are applicable to all objects. The Edit class describes the ability to change the Access Control List characteristics of any object.

This amendment makes use of the Authentication Unit of the Association Control Service Element (ACSE) now available as an implementation option. It does so by allowing the conditions expressed in the Access Control List to depend on the Authentication Value present in the A-ASSOCIATE service primitives. Such use of the Authentication Unit is not required, however, to make use of the Access Control List mechanism.

By using the mechanisms present in this amendment, an implementation can restrict access to an object (for reading, writing, loading, storing, execution, deletion, or other modification) to MMS Clients that either (1) attempt access from known network nodes, (2) provide proper authentication (passwords), (3) have synchronized their use with other MMS Clients through use of the semaphores, or (4) an arbitrary combination of these methods. The specification of passwords requires the use of the Authentication Unit of ACSE.

This amendment also modifies the MMS Service model by adding an explicit Object Model for an Application Association. This model should be present in the basic MMS Object Model, independent of the use of Access Control Lists. Its omission in the base document should be considered an oversight, corrected by this amendment.

The introduction of an object model for the application association allows one to move the list of transactions objects from the VMD to the application association, thereby allowing the invoke ID to be the sole key attribute of the transaction. The case of processing of Event Actions, however, requires us to introduce a new attribute to the VMD, namely a list of transactions associated with Event Action processing that are not bound (necessarily) to an association.

Industrial automation systems — Manufacturing Message Specification

Part 1:
Service definition

AMENDMENT 2: Conditioned service response

1. Scope

(This amendment makes no changes to clause 1 of ISO/IEC 9506-1.)

2. Normative references

Immediately following the reference to ISO 8650, page 2, add the following:

ISO 8649:1988/Amd.1:1990, *Information processing systems - Open Systems Interconnection - Service definition for the Association Control Service Element Amendment 1: Authentication during association establishment.*

ISO 8650:1988/Amd.1:1990, *Information processing systems - Open Systems Interconnection - Protocol specification for the Association Control Service Element Amendment 1: Authentication during association establishment.*

Immediately following the reference to ISO/IEC 9506-2, add the following:

ISO/IEC 9506-1:1990/Amd.1:1993, *Industrial automation systems - Manufacturing Message Specification - Part 1: Service definition Amendment 1: Data exchange.*

ISO/IEC 9506-1:1990/Cor.1:1995, *Industrial Automation Systems - Manufacturing Message Specification - Part 1: Service definition Technical corrigendum 1.*

3. Definitions

(This amendment makes no changes to clause 3 of ISO/IEC 9506-1.)

4. Abbreviations

(This amendment makes no changes to clause 4 of ISO/IEC 9506-1.)

5. Conventions

(This amendment makes no changes to clause 5 of ISO/IEC 9506-1.)

6. MMS in the OSI Environment

(This amendment makes no changes to clause 6 of ISO/IEC 9506-1.)

7. The Virtual Manufacturing Device

In 7.2, page 19, in the VMD object model replace the line

Attribute: List of Transaction Objects

with

Attribute: List of Event Action Transaction Objects
Attribute: List of Application Associations

In 7.2, page 19, in the VMD object model, insert

Attribute: Reference to Access Control List

immediately before the line

Attribute: Additional Detail

In 7.2.6.2, page 20, insert

GetAccessControlListAttributes

into the list of services between Cancel and GetAlarmEnrollmentSummary, and insert

ReportAccessControlledObjects

into the list of services between ReadJournal and ReportEventActionStatus.

At the end of 7.2.10 on page 22, add new subclauses 7.2.11 and 7.2.12:

7.2.11 List of Event Action Transaction Objects

This attribute identifies those transaction objects (see 7.2.13) that do not explicitly depend on an application association. Such transactions occur through the processing of Event Actions (see 15.1.4.2.5). In all other respects, they are normal transaction objects.

7.2.12 Application Association

The Application Association identifies a specific instance of communication of the VMD with an MMS client.

Object: Application Association
Key Attribute: Application Association Identifier
Attribute: Application Reference of MMS Client
Attribute: AP Title of MMS Client
Attribute: AE Qualifier of MMS Client
Attribute: AP Invocation-identifier of MMS Client

Attribute: AE Invocation-identifier of MMS Client
Attribute: Authentication Employed (TRUE, FALSE)
Constraint: Authentication Employed = TRUE
Attribute: Authentication Value
Attribute: List of AA-Specific Named Objects
Attribute: List of Transaction Objects
Attribute: List of services supported
Attribute: List of parameter CBBs supported
Attribute: Nesting Level

Application Association Identifier

This attribute identifies the application association. Since this attribute is never communicated, its form is a local matter.

Application Reference of MMS Client

This attribute, which serves to identify the AE within the MMS Client with whom the association has been established. It is composed of the AP Title, the AE Qualifier, the AP Invocation-identifier, and the AE Invocation-identifier. (See 6.6.)

AP Title of MMS Client

This attribute, derived from application association establishment information (See ISO/IEC 9506-2, clause 17), identifies the MMS client present on this association.

AE Qualifier of MMS Client

This attribute, derived from application association establishment information (See ISO/IEC 9506-2, clause 17), identifies the MMS client present on this association.

AP Invocation-identifier of MMS Client

This attribute, derived from application association establishment information (See ISO/IEC 9506-2, clause 17), identifies the MMS client present on this association.

AE Invocation-identifier of MMS Client

This attribute, derived from application association establishment information (See ISO/IEC 9506-2, clause 17), identifies the MMS client present on this association.

Authentication Employed

This attribute indicates whether (true) or not (false) authentication (See ISO/IEC 9506-2, clause 17) was used in establishing this association. If this attribute is true, the following attribute also appears.

Authentication Value

This attribute is the value of the Authentication Value as presented by the MMS Client at application association establishment. This attribute may be either a character string (Graphic String), a bit string, or an external. The choice 'ANY DEFINED BY mechanism-name' shall not be used.

List of AA-Specific Named Objects

This attribute contains a list of all the named objects within the VMD that are declared to have AA-specific scope and identify this Application Association.

List of Transaction Objects

This attribute is the list of transaction objects (see 7.2.13) associated with this application association.

List of services supported

This attribute contains a list of all the MMS services supported as given in the MMS Initiate procedure (see 8.3.2 and 8.2.4).

List of parameter CBBs supported

This attribute contains a list of all the MMS parameter CBBs that have been negotiated in the MMS Initiate procedure (see 8.2.4).

Nesting Level

This attribute contains the value of the Nesting Level that was negotiated in the MMS Initiate procedure (see 8.2.1.2.4).

In (old) 7.2.11, bottom of page 22, in the Object Model, replace the line:

Key Attribute: Application Association Identifier

with:

Attribute: Application Association Identifier

In (old) 7.2.11, top of page 23, add the following sentence after the description of Application Association Identifier:

If no such application association exists, this attribute shall have the value NONE.

In (old) 7.2.11.2, replace the first paragraph with:

A transaction object shall be created either upon receipt of an indication service primitive for an MMS confirmed service or as part of the processing of an event occurrence (see). The transaction object shall be deleted after the MMS-user issues a response service primitive for that service instance. The number of transaction objects that may exist at any time is governed by the negotiated maximum number of services outstanding (see 8.2).

Renumber 7.2.11, 7.2.12, and 7.2.13 to be 7.2.13, 7.2.14, and 7.2.15 respectively. Renumber 7.2.11.1 and 7.2.11.2 to be 7.2.13.1 and 7.2.13.2 respectively.

Add a new subclause 7.2.16 as follows:

7.2.16 Reference to Access Control List

This attribute is a reference to an Access Control List object that specifies necessary (but not sufficient) conditions for an MMS service to succeed. The conditions specified in this Access Control List object shall be satisfied for the service class corresponding to the requested service in order for the service to succeed. Additional conditions for success may be imposed by an Access Control List object referenced by the object of the service request. If no other specification has been provided, this attribute should reference 'M_NonDeletable' (see 18.3.1.5).

Renumber 7.2.14 and 7.2.15 to be 7.2.17 and 7.2.18 respectively.

In 7.3.2, page 25, add a new entry at the end of table 1

Access Control List Objects	X			21

Replace the second sentence of 7.3.5, page 26, with the following:

Static objects usually may not be deleted through the use of MMS services, and dynamic objects usually may be deleted, but there may be exceptions to either rule.

Replace the first sentence of 7.3.6, page 26, with the following:

All MMS objects subordinate to the VMD may be deleted from the VMD through appropriate MMS service requests if such requests are permitted (see 7.3.8).

Replace the last sentence of 7.3.6, page 26, with the following:

This is true regardless of any conditions specified in the Access Control List object referenced by the object subordinate to the Domain.

Add the following new subclause after 7.3.7, page 26.

7.3.8 Control of Access to MMS Objects

MMS provides explicit control for the ability to access or alter MMS named objects. Each named object within an MMS implementation contains a reference to an access control object that specifies the conditions under which services directed at the named object may succeed. For the purposes of specifying the control conditions, services are grouped into seven classes, read, write, load, store, execute, delete, and edit. The control conditions include possession of a semaphore, identity of user (Application Reference), and the submission of a password (which may be arbitrarily complex). These conditions are necessary but not sufficient for the success of the service. If the conditions are not satisfied, the service is required to fail; the service may always fail for reasons beyond the scope of this standard. These conditions may be combined in arbitrary ways. Conditions may be specified separately for individual objects and for all objects of the VMD. Conditions restricting creation of objects can only be specified for the entire VMD.

The reference to Access Control List attribute of named objects replaces the MMS Deletable attribute of the earlier version of MMS. For backward compatibility, a derivation rule from the Access Control List is provided for services that report the value of the MMS Deletable attribute. Using this rule, implementations of earlier versions of MMS will be able to interwork with implementations of this version of MMS as long as the additional services specified in this version are not employed.

A parameter CBB named ACO is used to indicate whether or not the object reporting services shall report attributes related to the use of access control lists.

7.3.8.1 Access Control List Object Model

Object: Access Control List
Key Attribute: Access Control List Name
Attribute: Reference to Access Control List
Attribute: List of Access Control Elements
  Attribute: Service Class (READ, WRITE, LOAD, STORE, EXECUTE, DELETE, EDIT)
    Attribute: Access Condition (NEVER, SEMAPHORE, USER, PASSWORD, JOINT, ALTERNATE)
Constraint: Access Condition = SEMAPHORE
      Attribute: Semaphore Name
Constraint: Access Condition = USER
      Attribute: Application Reference
Constraint: Access Condition = PASSWORD
      Attribute: Password Value
Constraint: Access Condition = JOINT
      Attribute: List of Access Condition
Constraint: Access Condition = ALTERNATE
      Attribute: List of Access Condition
List of References to Access Controlled Objects

7.3.8.2 Access Control List Name

The Access Control List Name attribute uniquely identifies the Access Control List object within the VMD. The name shall be a VMD-specific Object Name formed according to the rules for MMS Object Names as specified in 7.4.

7.3.8.3 Reference to Access Control List

Each Access Control List object is itself subject to access control. This reference identifies the Access Control List object that governs access to this object.

7.3.8.4 List of Access Control Elements

An Access Control List may contain zero or more Access Control Elements. Each element shall identify one Service Class and provide one Access Condition. An Access Control List shall not contain more than one Access Control Element that identifies the same Service Class.

NOTE — Since there are only seven Service Classes, this means that there are at most seven Access Control Elements in the List of Access Control Elements. However, since most MMS objects do not use each class of access control, the number of Access Control Elements applicable to any object class will usually be less than seven. Access Control Objects may be used to apply to multiple object classes which means that in some cases an object may reference an Access Control List object that contains Access Control Elements that do not apply to the referencing object.

7.3.8.4.1 Access Control Service Classes

Each Access Control Element identifies the service class to which it applies. There are seven such service classes as follows:

a) Read - Services that obtain individual values associated with objects. These are:

i) Read
ii) Output

b) Store Services that obtain grouped values associated with objects. These are:

i) ReadJournal
ii) InitiateUploadSequence
iii) StoreDomainContent

c) Write - Services that change the individual value of an MMS object. These are:

i) Write
ii) Input
iii) ExchangeData

d) Load - Services that change the values or other attributes of an MMS object. These are:

i) InitiateDownloadSequence*

ii) LoadDomainContent*
iii) CreateProgramInvocation*
iv) DefineNamedVariable*
v) DefineScatteredAccess*
vi) DefineNamedVariableList*
vii) DefineNamedType*
viii) DefineSemaphore*
ix) TakeControl
xi) DefineEventCondition*
xii) DefineEventAction*
xiii) DefineEventEnrollment*
xiv) TriggerEvent
xv) AlterEventConditionMonitoring
xvi) AlterEventEnrollment
xvii) AcknowledgeEventNotification
xviii) CreateJournal*
xix) InitializeJournal
xx) WriteJournal
xxi) DefineAccessControlList*

* Since these services create the respective objects, the services can only be affected by the Access Control List referenced by the VMD.

e) Execute - Services that change the state of Program Invocation objects. These are:

i) Start
ii) Stop
iii) Resume
iv) Reset
v) Kill

f) Delete - Services that delete MMS objects. These are:

i) DeleteDomain
ii) DeleteProgramInvocation
iii) DeleteVariableAccess
iv) DeleteNamedVariableList
v) DeleteNamedType
vi) DeleteSemaphore
vii) DeleteEventCondition
viii) DeleteEventAction
ix) DeleteEventEnrollment
x) DeleteJournal
xi) DeleteAccessControlList

g) Edit - Services that change the value of the Reference to Access Control List attribute of the object or its attributes. These are:

i) ChangeAccessControl (New Service)
ii) Rename

7.3.8.4.2 Access Condition

This attribute specifies a condition that, if not satisfied, will require the MMS service to fail. Each condition shall specify one of the following types:

a) NEVER - This condition indicates that the class of service specified in the Service Class attribute shall always fail.

b) SEMAPHORE - This condition indicates that if the named semaphore is not owned by the MMS service requester, the class of service specified in the Service Class shall fail.

c) USER - This condition indicates that the class of service specified shall fail unless the Application Reference of the client matches the value of this field.

d) PASSWORD - This condition indicates that the class of service specified shall fail unless the client has provided the authentication values that match the value of this field.

e) JOINT - This Access Condition succeeds if all of the conditions in the List of Access Conditions succeed; otherwise this Access Condition fails.

f) ALTERNATE - This Access Condition succeeds if any of the conditions in the List of Access Conditions succeed; otherwise this Access Condition fails.

7.3.8.5 List of References to Access Controlled Objects

This attribute is a list of references to named objects that reference this Access Control List object. The following MMS objects may be governed by Access Control Lists. Following each object is a specification of the service classes that may be applied to that object. An Access Control List object may specify a service class that does not apply to the object for which the Access Control List is an attribute. In such cases, the conditions associated with that service class have no effect on that object. Note that while Unnamed Variables may have Access Control Lists as attributes, they are necessarily pre-defined since the only services provided in Clause 21 assume that the objects to be modified have names.

a) Domain (LOAD, STORE, DELETE, EDIT)

b) Program Invocation (LOAD, EXECUTE, DELETE, EDIT)

c) Named Variable (READ, WRITE, DELETE, EDIT)