IEC PAS 62264-6

Edition 1.0 2016-07

PUBLICLY AVAILABLE SPECIFICATION

PRE-STANDARD

colour inside

Enterprise-control system integration –
Part 6: Messaging Service Model

IEC PAS 62264-6:2016-07(en)

Copyright International Electrotechnical Commission

THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2016 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

Copyright International Electrotechnical Commission

IEC PAS 62264-6

Edition 1.0 2016-07

PUBLICLY AVAILABLE SPECIFICATION

PRE-STANDARD

colour inside

Enterprise-control system integration – Part 6: Messaging Service Model

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 25.040.99; 35.100; 35.100.50

ISBN 978-2-8322-3487-7

Warning! Make sure that you obtained this publication from an authorized distributor.

® Registered trademark of the International Electrotechnical Commission

Copyright International Electrotechnical Commission

CONTENTS

Copyright International Electrotechnical Commission

Copyright International Electrotechnical Commission

Copyright International Electrotechnical Commission

Copyright International Electrotechnical Commission

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

ENTERPRISE-CONTROL SYSTEM INTEGRATION –

Part 6: Messaging Service Model

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

A PAS is a technical specification not fulfilling the requirements for a standard, but made available to the public.

IEC PAS 62264-6 has been processed by subcommittee 65E: Devices and integration in enterprise systems, of IEC technical committee 65: Industrial-process measurement, control and automation.

The text of this PAS is based on the following document:	This PAS was approved for publication by the P-members of the committee concerned as indicated in the following document
Draft PAS	**Report on voting**
65E/476/PAS	65E/502/RVD

Following publication of this PAS, which is a pre-standard publication, the technical committee or subcommittee concerned may transform it into an International Standard.

Copyright International Electrotechnical Commission

This PAS shall remain valid for an initial maximum period of 3 years starting from the publication date. The validity may be extended for a single period up to a maximum of 3 years, at the end of which it shall be published as another type of normative document, or shall be withdrawn.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

Copyright International Electrotechnical Commission

INTRODUCTION

This PAS is based on the use of ISA-95 object models defined in ISA-95 Parts 2, 4 and 5 (Parts 1 and 3 do not contain object models) to define a set of services that may be used to exchange information messages. It is recognized that other, non-Part 6 sets of services are possible and are not deemed invalid as a result of this PAS. This PAS defines a Messaging Service Model (MSM) for exchanging data exchange messages in a publish/subscribe mode and a request/response mode. It defines a minimal interface subset to message exchange systems.

The Messaging Service Model provides a method for applications to send and receive messages from MSM service providers without regard to the underlying communication mechanism, as part of a complete application-to-application communication protocol.

This PAS defines a set of services definitions that are designed to provide the functionality needed for a vendor-independent method for sending and receiving data exchange messages on a message exchange system, such as an Enterprise Service Bus (ESB).

The knowledge requirements to interface to just one message exchange system can be immense, and are usually not transferable to a different system. MSM defines a single interface, independent of the underlying services, for Level 3-3 and Level 4-3 communications. This removes the need for vendors to build custom interface after custom interface, and for end users to get locked into a single vendor because their investment prevents them from reusing any of the integration efforts.

Enterprise-control system integration involves multiple different steps to exchange data between different computer system applications, as shown in Figure 1.

a) The applications usually have different internal representations of exchanged objects in their own local data stores. This representation is usually converted from the local format to a commonly accepted global format. The ISA-95 Part 2 standard defines representations of a global format for Level 4-3 data exchanges. The Part 4 standard defines representations of a global format for Level 3-3 data exchanges. This conversion, from local to global and global to local, is usually performed twice for any two-way communications.

   EXAMPLE 1 Assume two applications, ALPHA and BETA: the ALPHA application initiates a data exchange with the BETA application, and BETA responds back to ALPHA. The format conversions are: ALPHA's local format to global format for the request data, global format to BETA's local format for the request data, BETA's local format to global format for the response data, and global format to ALPHA's format for the response data.

b) Conversion is performed to align the namespaces among the exchanging applications, and is usually performed four times for any two-way communications.

   EXAMPLE 2 Names for elements of data may be codes, tag names, or equipment identifiers.

   EXAMPLE 3 Data which are represented in one element namespace, such as codes 1,2,3,4, may have a different namespace in another application, such as codes Ok, Done, Error, Delay.

c) Once information is in the global format with appropriate global names, the exchanged information is sent from one application to another application.

d) Messages are transported from one application to another, either within the same computer environment or across computers. Transport mechanisms are defined in other standards, such as TCP/IP and Ethernet standards.

e) When data exchange information is received, there are specific rules that define what resultant data are to be returned. The transaction rules are defined in the ISA-95 Part 5 standard.

Copyright International Electrotechnical Commission

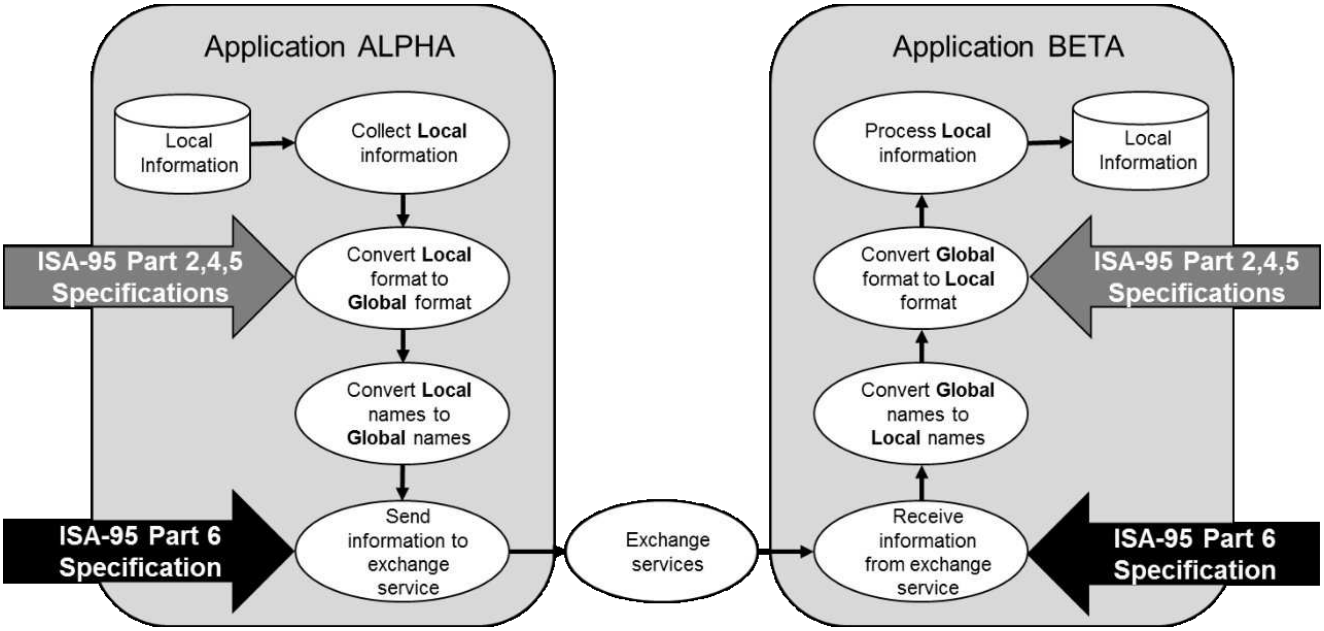

Figure 1 – Steps in application-to-application communication

Copyright International Electrotechnical Commission

ENTERPRISE-CONTROL SYSTEM INTEGRATION –

Part 6: Messaging Service Model

1 Scope

This part of IEC 62264, which is a PAS, defines a model of a set of messaging services for information exchanges across Levels 3 and 4, and within Level 3, between applications performing business and manufacturing activities. It defines a standard interface for information exchange between systems.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ANSI/ISA-95.00.01-2010 (IEC 62264-1 Mod), *Enterprise-Control System Integration – Part 1: Models and Terminology*

ANSI/ISA-95.00.02-2010 (IEC 62264-2 Mod), *Enterprise-Control System Integration – Part 2: Object Model Attributes*

ANSI/ISA-95.00.04-2012, *Enterprise-Control System Integration – Part 4: Objects and Attributes for Manufacturing Operations Management Integration*

ANSI/ISA-95.00.05-2013, *Enterprise-Control System Integration – Part 5: Business-to-Manufacturing Transactions*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1.1
channel description
text that describes a channel

3.1.2
channel type
primary use of a channel for publications or requests

3.1.3
channel URI
primary identifier for a channel

Copyright International Electrotechnical Commission

3.1.4
filter expression
filtering element that may be applied to messages on a channel

3.1.5
listener identification
implementation defined element that is used to indicate to an application when a new message has arrived

3.1.6
message content
body of the message

3.1.7
message expiry
duration until the expiration of a publication message on a publication channel

3.1.8
message ID
identifier generated upon posting of a message to a channel in a session

3.1.9
namespace
collection of names or words that define a formal and distinct set

3.1.10
security token
physical device or software code used to gain access to a channel

3.1.11
session ID
identifier generated upon an application creating a session on a channel and provided to the application for use in the MSM services

3.1.12
topic
identification of the information content in a message

3.2 Abbreviations

B2MML	Business to Manufacturing Markup Language
CB (radio)	Citizens' Band radio
CCOM-ML	Common Conceptual Object Model – Markup Language
ERP	Enterprise Resource Planning
ESB	Enterprise Service Bus
FTP	File Transfer Protocol
HTTP	Hypertext Transmission Protocol
JMS	Java Message Service
MSM	Messaging Service Model
MIMOSA	An Operations and Maintenance Information Open System Alliance
OAG	Open Applications Group
OAGIS	Open Applications Group Integration Specification
OMAC	The Organization for Machine Automation and Control
OpenO&M	Open Operations and Maintenance Group

Copyright International Electrotechnical Commission

OPC-UA	OPC-Unified Architecture
REST	Representational State Transfer
RSS	Really Simple Syndication
SOAP	Simple Object Access Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
UDDI	Universal Description, Discovery and Integration
URI	Universal Resource Identifier
WS_*	World Wide Web Service standards
XML	Extensible Markup Language
XSLT	Extensible Stylesheet Language Transformations

3.3 Conventions

Input and returned parameters defined in Clause 6 are required unless they are explicitly defined as optional.

4 The Messaging Service Model

4.1 Interface model

The MSM defines a standard set of services that shall be provided by an application or network service. The services provide a method for multiple applications to communicate using the transaction models defined in the ISA-95.00.05 and IEC 62264-5 standards. The MSM:

– does not define how the services are implemented,

– does not define the architecture of the supporting application or network service,

– does not define any specific underlying communication method.

The MSM provides a standard interface to an Enterprise Service Bus (ESB) system[1] or to any other message or file exchange system that offers guaranteed message delivery, message sequencing, and storage or caching of exchanged messages.

NOTE 1 Multiple different implementations are envisioned, such as a service using OPC UA, a service using FTP, or a service using an ESB.

NOTE 2 The MSM service will have to include some method for storage or caching of exchanged information, and some method of guaranteed message delivery.

The level of services not defined in this PAS, for example the type of security, reliability, guaranteed delivery, quality of service, transformation capability, and other features would be provided by the MSM Service Provider and provide differentiation between suppliers and solutions.

4.2 Application to application data exchange

Application to application data exchange is represented in communication models as a single “Application” layer. However, with the development of data object standards (such as ISA-95 models), data representation messages (such as B2MML, MIMOSA CCOM-ML and OAGIS Nouns), and transaction messages (such as IEC 62264-5 and OAGIS 9.0 Verbs), means that a simple single layer is insufficient to describe the complexity of object based application-to-application transactional communication.

1 See Annex B for a brief discussion on Enterprise Service Buses.

Copyright International Electrotechnical Commission

Two additional elements can be defined for application-to-application communication: a data object definition and transaction message definition which communicate to the application layer and the underlying exchange services, as shown in Figure 2.

MSM is a minimal interface subset that can reside on most exchange services and is based on well-defined and structured data objects and transaction messages.

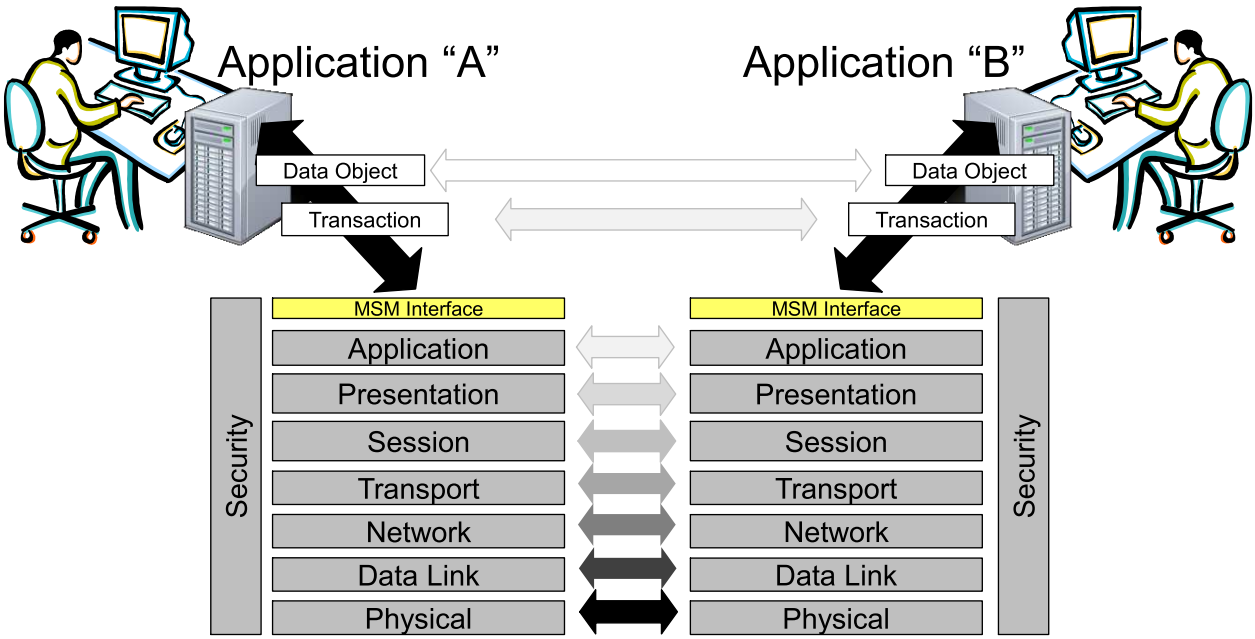

Figure 2 – Application communication stack

Each of these layers addresses a specific element of application data exchange, as shown in Figure 3:

a) A Data Object layer defines the meaning, format, and structure of the basic elements of exchanged information.

NOTE 1 This layer uses application space specific definitions, such as the ISA-95.02 object definitions, MESA B2MML, MIMOSA CCOM-ML objects, and "Nouns" defined in OAGIS.

b) A Transaction layer defines the meaning, format, and structure of actions to be taken on the data objects.

NOTE 2 This layer can use IEC 62264-5 transaction style specific definitions. Another transaction layer definition could be the OAGIS "Verb" definitions.

c) The MSM Service Interface defines a minimal interface to the Application layer's Exchange Services.

d) The application, presentation, session and lower level layers define the meaning, format, and structure for coordination, buffering, and exchange of messages or files. These layers contain transfer or exchange style specific definitions, such as Enterprise Service Buses, Enterprise Message Delivery Systems, the OPC-UA specification (IEC 62541 (all parts)), RSS, FTP, Named Pipes, Ethernet, TCP/IP, HTTP, and others.

Copyright International Electrotechnical Commission

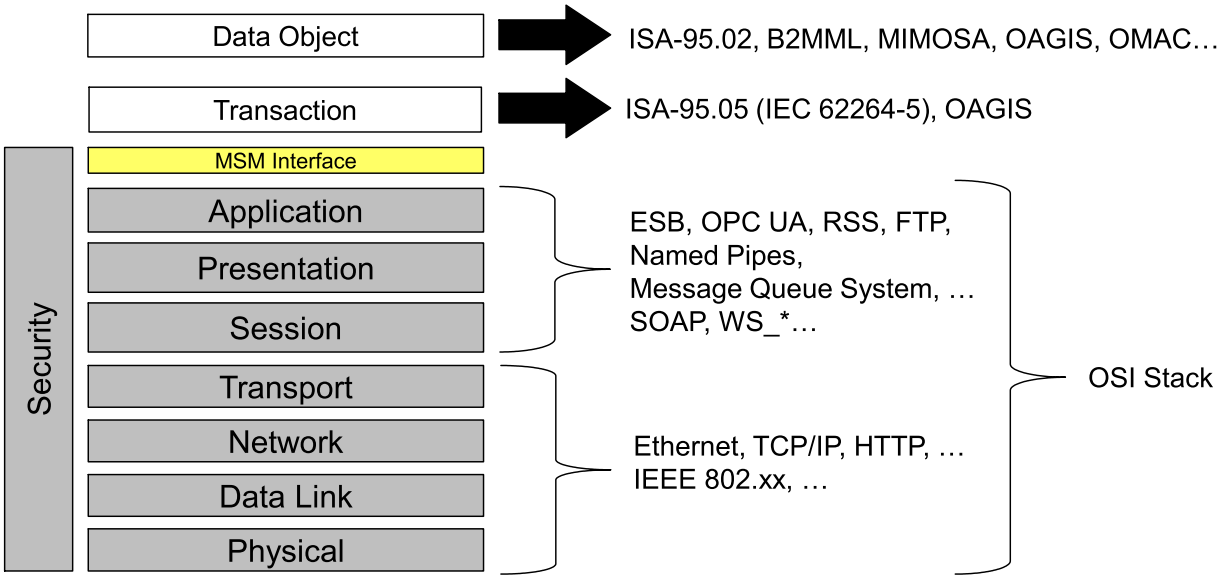

Figure 3 – Defined standards at each level

The ISA-95.05 and IEC 62264-5 standards define transactions on the information. The Messaging Service Model (MSM) defines an interface to methods for exchange. In a sense, MSM defines the standard “on-ramp” and "off-ramp" to a set of communication services. It defines how data is placed into exchange methods and how it is retrieved from the exchange methods.

NOTE 1 Message synchronization at the MSM interface is distinct from the message synchronization provided by ISA-95.05 transaction models as well as distinct from the synchronization mechanisms provided at lower levels of the communications stack.

NOTE 2 In this PAS, asynchronous message exchanges between consumers and producers can be considered to be pairs of distinct, unidirectional messages.

4.3 Transaction model

The ISA-95.05 and IEC 62264-5 standards define three models for business transactions: a publish model, a push model, and a pull model[2].

The MSM defines a standard interface for applications to exchange data following any of the ISA-95.05 transaction models using XML schemas to represent data.

The transactions supported by the MSM support:

a) A publish-subscribe model with multiple subscribers and multiple publishers, where the publishers and subscribers have no direct knowledge of other applications.

b) A push and pull model, also called a request-response model, where an application sends unsolicited requests for a service and has no direct knowledge of the receiving application that will process the request.

4.4 Communicating applications

ISA-95 and IEC 62264 define four roles:

1) Information Provider (to receive GET messages and send SYNC messages),

2) Information Receiver (to receive PROCESS, CHANGE, and CANCEL messages),

2 See the ISA-95 standards for a complete description of the types and format for transactions.

Copyright International Electrotechnical Commission

3) Information Users (to send GET messages and receive SYNC messages),

4) Information Sender (to send PROCESS, CHANGE, and CANCEL messages).

In the MSM model, these are simplified to Provider Application (Information Provider and Information Receiver) and Consumer Application (Information User and Information Sender), as shown in Figure 4.

The Provider Application is the owner of data. The Provider Application can publish changes to the data, can receive requests to change the data, and respond to queries for the data.

NOTE The phrase "owner of data" is used to identify the application that has responsibility for enforcing the consistency of data.

An application can be a provider application, consumer application or both. If an application is both, then it should be a consumer of different data than it provides.

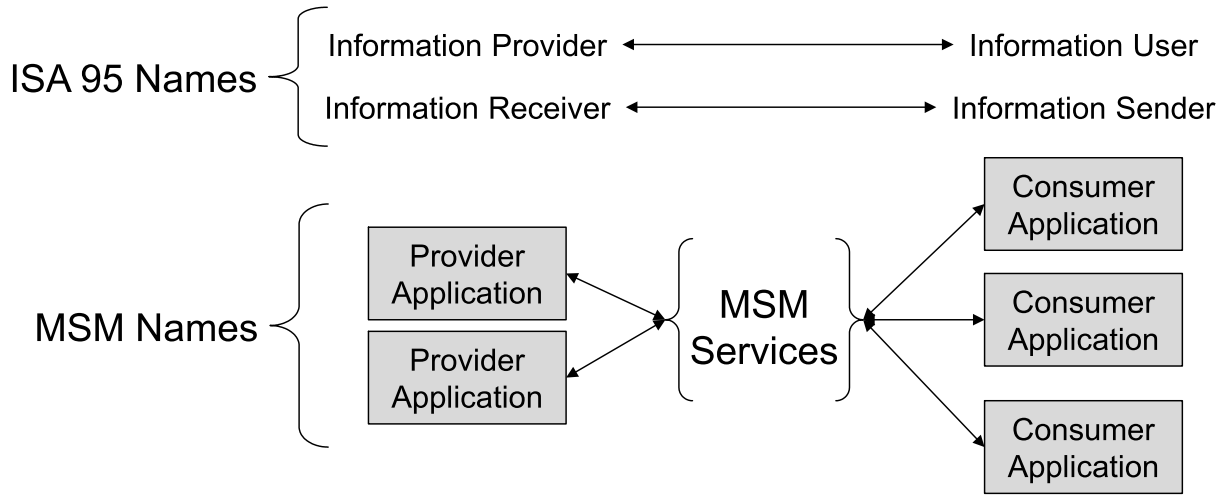

Figure 4 – Messaging service model names

4.5 Managed communication channels

The MSM is based on the concept of managed communication channels. A *channel* is a software object that represents a specific many-to-many communication conduit between applications. Some channels are for requests and responses, some channels are for general information distribution. Channels have topics.

NOTE 1 An analogy for an MSM channel is a channel on a CB radio.

NOTE 2 An analogy for a topic is a conversation topic on a CB channel. Users can choose to listen to some topics on the channel but ignore others.

NOTE 3 The assumption of this PAS is that the MSM services are provided by a communication application, middleware, or an ESB provider. The implementation method for the MSM services is not defined in this PAS and multiple architectures are possible, such as an OPC-UA implementation, an FTP based system, shared directories, a message queuing system implementation, or an RSS implementation.

The MSM provides a definition of the standard interfaces to the services (not how they are implemented).

A managed communication channel is called an MSM *Channel*.

The services provided for each MSM Channel are the *MSM Channel Services*.

An MSM *Channel* is identified using a URI or equivalent identifier. A URI is recommended to allow a hierarchy of channel definitions that match a company's physical or application structures, such as channels identified by plant site or major application suite name.

Copyright International Electrotechnical Commission

An MSM *Service Provider* is the application or network service that exposes and implements the *MSM Channel Services*.

A recommended structure for the *MSM Channel* hierarchy is defined in this PAS.

Each *MSM Channel* supports three general types of information exchange:

A – Publications – Information that may be sent to multiple consumer applications.

B – Requests – Information that may be sent to one or more provider applications.

C – Responses – Information returned from a request to a consumer application.

Each *MSM Channel* supports two way communications between provider applications and consumer applications.

a) An MSM *Channel* may be created to support either publication services or request services.
b) A *Provider Application* may post publications to an MSM *Publication Channel*.
c) *Consumer Applications* may subscribe to publication notifications (if supported by the specific *MSM Publication Channel Service*) and may read publications. If notifications are not supported, then the *Consumer Application* may poll the *MSM Publication Channel* using the read publication service.
d) A *Consumer Application* may post requests to an MSM *Request Channel*.
e) A *Provider Application* may subscribe to request notifications (if supported by the specific *MSM Request Channel Service*) and may read requests. If notifications are not supported, then the *Provider Application* may poll the *MSM Request Channel* using the read request service.
f) *MSM Channels* have associated *Topics*. Topics are identified when subscribing to a channel, when posting a publication, and when posting a request.

4.6 Notification services

The notification service shall be the means that the MSM Service Provider uses to indicate to a provider or consumer application that a message that meets their read criteria is waiting to be read. The notification services provide a method for an asynchronous callback alternative to polling the MSM services.

Notification services shall be accessible using a *Notify Listener* service on a subscriber, requester, or responder.

The notification services interface is optional for an MSM provider.

If a provider/consumer application does not provide a callback identification for the notification services, then notification shall not be provided to the application.

NOTE The format of the listener identification for notification will be defined by the implementation technology.

EXAMPLE A SOAP and Web Service implementation may define the Listener Identification as a valid URL that defines a Notify Listener service, which is managed by the application creating the session.

4.7 MSM channel services

The MSM Channel Management Services shall be used to create and delete channels and to control the Security Token specification for channels.

The MSM Channel Services are shown in Figure 5. These services would usually be called by a provider application, or by a dedicated channel management application.

Copyright International Electrotechnical Commission

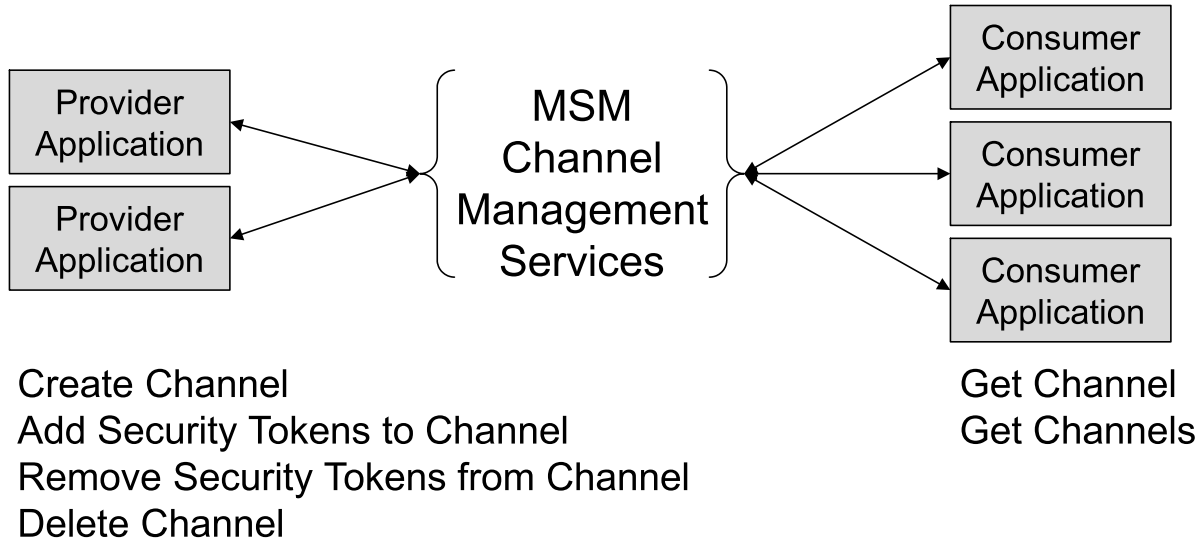

Figure 5 – MSM channel management services

4.8 MSM publication channel services

4.8.1 Publication channel services

The MSM Publication Channel Services shall be used to post, expire, remove, and read publication messages.

The MSM Publication Channel Services are shown in Figure 6. The services allow multiple Provider Applications to post publications to the same channel. Consumer Applications may subscribe to notifications (if supported by the channel) and may read publications.

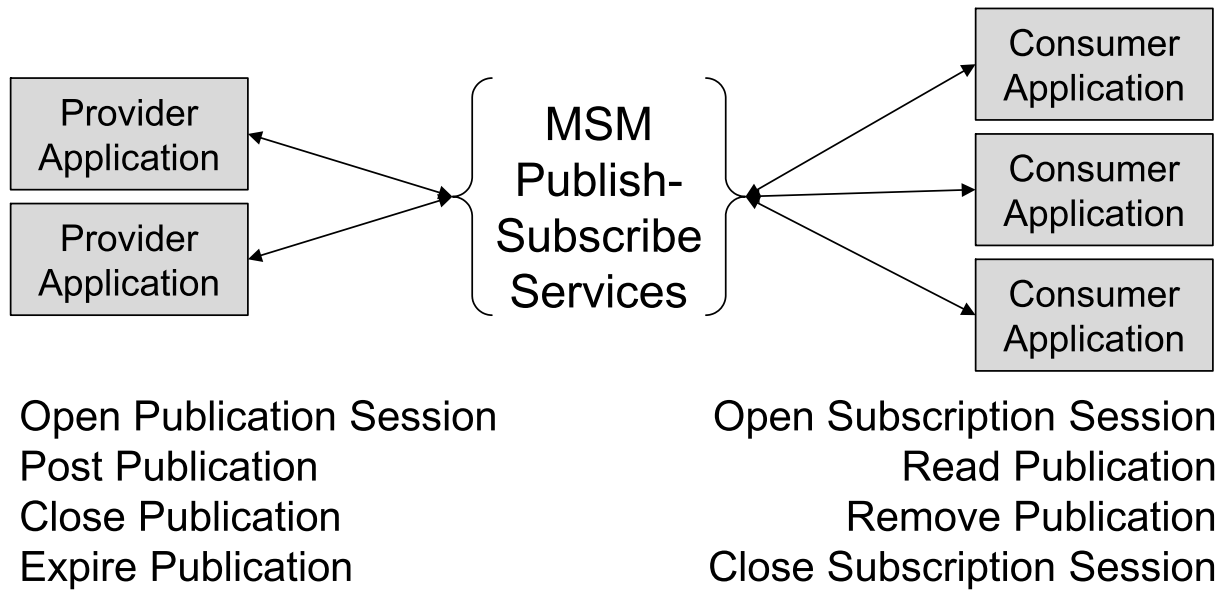

Figure 6 – MSM publication channel services

Copyright International Electrotechnical Commission

4.9 MSM request channel services

4.9.1 Request services

The MSM Request Channel Services shall be used to post request messages and read response messages.

The MSM Channel Services for the ISA-95.05 Push and Pull transactions are shown in Figure 7. These are the PROCESS, CHANGE, CANCEL, and GET transactions.

The services allow one or more Consumer Applications to post requests to Provider Applications, allow one or more Provider Applications to read requests and post responses, and for the Consumer Application to read the response. Each posted request includes an additional qualifier, called a “Topic”, which allows Provider Applications to determine if they should receive the request and post a response to the requestor.

EXAMPLE Topics may define the format and content of a message as identified by the XML Schema Definition (XSD) used to create and verify a message.

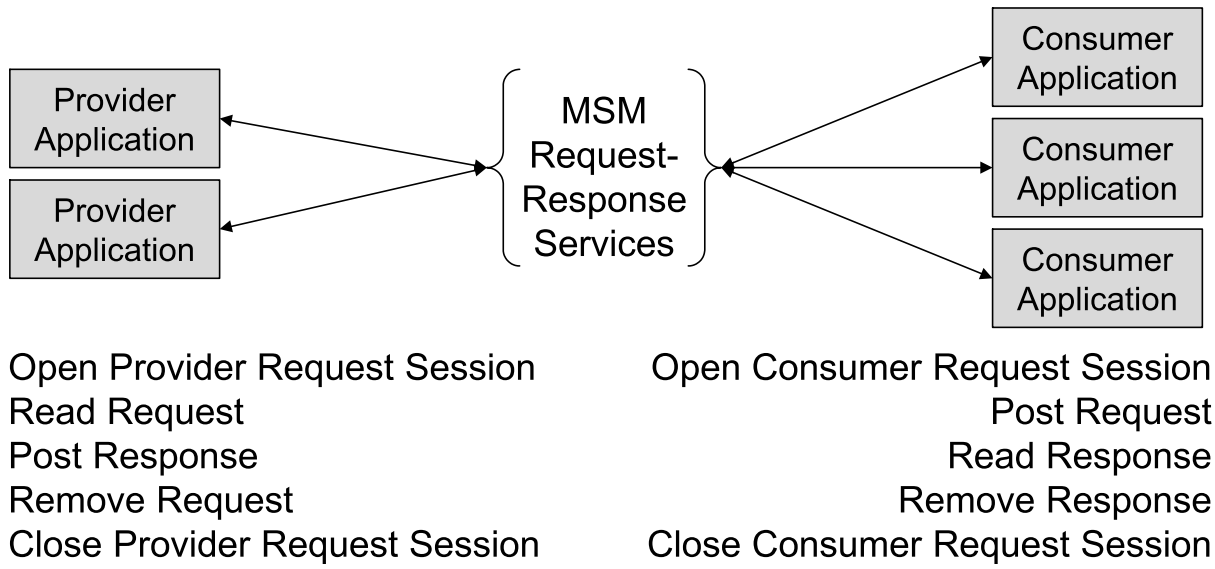

Figure 7 – Services for request/response

5 Methods of operation of MSM channels

5.1 Channel and topic identification

The two elements that shall be used for filtering messages are channels (for the scope of the information), and topics (for the type of information).

Subclause 5.1 defines a recommended MSM method for identifying channels IDs and topics that shall be used in order to ensure maximum interoperability.

There is no restriction on the use of Channels and Topics. However, there are two main elements that should be used for channels and topics: scope of information and type of information.

5.2 Channel names and hierarchy

5.2.1 Channel names

Channel names shall be defined as a name hierarchy using the URI syntax.

Copyright International Electrotechnical Commission

5.2.2 Channel name hierarchy

Channel names should follow the naming hierarchy:

\ <MSM root> \ <channel scope> \ <information scope> \ <channel use>

EXAMPLE 1 \AJAXEnterprises\Company\Material\Checkpoint

EXAMPLE 2 \AJAXEnterprises\Company\Material\Request

EXAMPLE 3 \SystemTest\Final\OurMaterialManager\Inventory\Changes

EXAMPLE 4 \AJAXEnterprises\France\Personnel\Checkpoint

5.2.3 MSM root

The MSM root shall be the root of a hierarchy defined when the MSM services are installed or initialized. Depending on the MSM Service implementation, there may be one or more roots allowed.

The MSM Service Provider may require specific values for MSM Root.

EXAMPLE

– AN MSM root may be the name of the company.
  - Such as: “AJAX” or “AJAXEnterprises\SpecialToolCo”.
– AN MSM root may be a related set of services, with sets for testing, deployment, and operations.
  - Such as: “SystemTest\Beta”, “SystemTest\Final”, “SpecialToolCo\Operations”.

NOTE The MSM services do not contain a method to browse the MSM Roots that are defined. These special services should be provided by an MSM service implementation and may have security restrictions that are outside the scope of the MSM services.

5.2.4 Channel scope

The channel scope shall contain a role equipment hierarchy (as defined in IEC 62264-1) that may correspond to a physical, geographical, or logical grouping determined by the enterprise, application or project. It may be used to limit the scope of the exchanged information, such as information only exchanged within one division of a company. The hierarchy may include site, area, workcenter, or any other enterprise defined equipment hierarchy element.

EXAMPLE

– A channel scope may include a site or region name to limit the number of distributed messages, such as: “*AsiaPacific*”, “*SouthAfrica*”, or “*France*”.
– A channel scope may be a software system, because the information is provided by a well-known system name, such as “*OurMaterialManager*”, “*PersonnelTracker*”, “*InventoryDatabase*”.
– A channel scope may be companywide because the information is intended for any application in the company. In this case the channel scope should indicate the entire enterprise or company, such as “*Enterprise*” or “*Company*”, or it may be null.

5.2.5 Information scope

The information scope shall define the range or general type of information exchanged. The information scope may be related to transaction nouns defined in IEC 62264-2 and IEC 62264-4, to other collections of objects.

EXAMPLE

– An application which handles all forms of material information may define a channel with an information scope of “*Material*”.
– An application that only handles Material Lot and Sublot inventories may define a channel with an information scope of “*Inventory*”.

Copyright International Electrotechnical Commission

5.2.6 Channel use

The channel use shall qualify the information scope to indicate how the information is being used. The channel use may be related to transaction verbs or other business or control process that deal with how the information on the channel is to be used.

To support interoperability, channel use should correspond to the classes of transaction message verbs, as defined in the ISA-95.05 and B2MML or other standards.

EXAMPLE 1 Classes of verbs from the ISA-95.05 standard

Query: GET / SHOW

Command: PROCESS / ACKNOWLEDGE, CHANGE / RESPOND, CANCEL

Publication: SYNC ADD, SYNC CHANGE, SYNC DELETE

EXAMPLE 2

– An application that sends GET messages may define a channel with a channel use of "*Query*".
– An application that sends PROCESS, CHANGE, and CANCEL messages may define a channel with a channel use of "*Command*".
– An application that sends SYNC messages may define a channel with a channel use of "*Publication*". This channel would be used as a publication channel for a snapshot of all of the exchanged information.

EXAMPLE 3

Publication Changes and *Publication Checkpoint* channel use can be used together by a provider application as shown in Figure 8.

– The *Checkpoint* channel should be used to publish a current snapshot of all of the exchanged information.
– The *Changes* channel should be used to publish all changes since the last snapshot.

  After a checkpoint is published, the provider application may clear all publications from the *Changes* channel and may clear previous *Checkpoint* publications.

  This dual publication channel method allows a consumer application to quickly sync all published information on a topic, without excessive interaction with the MSM services.

Copyright International Electrotechnical Commission

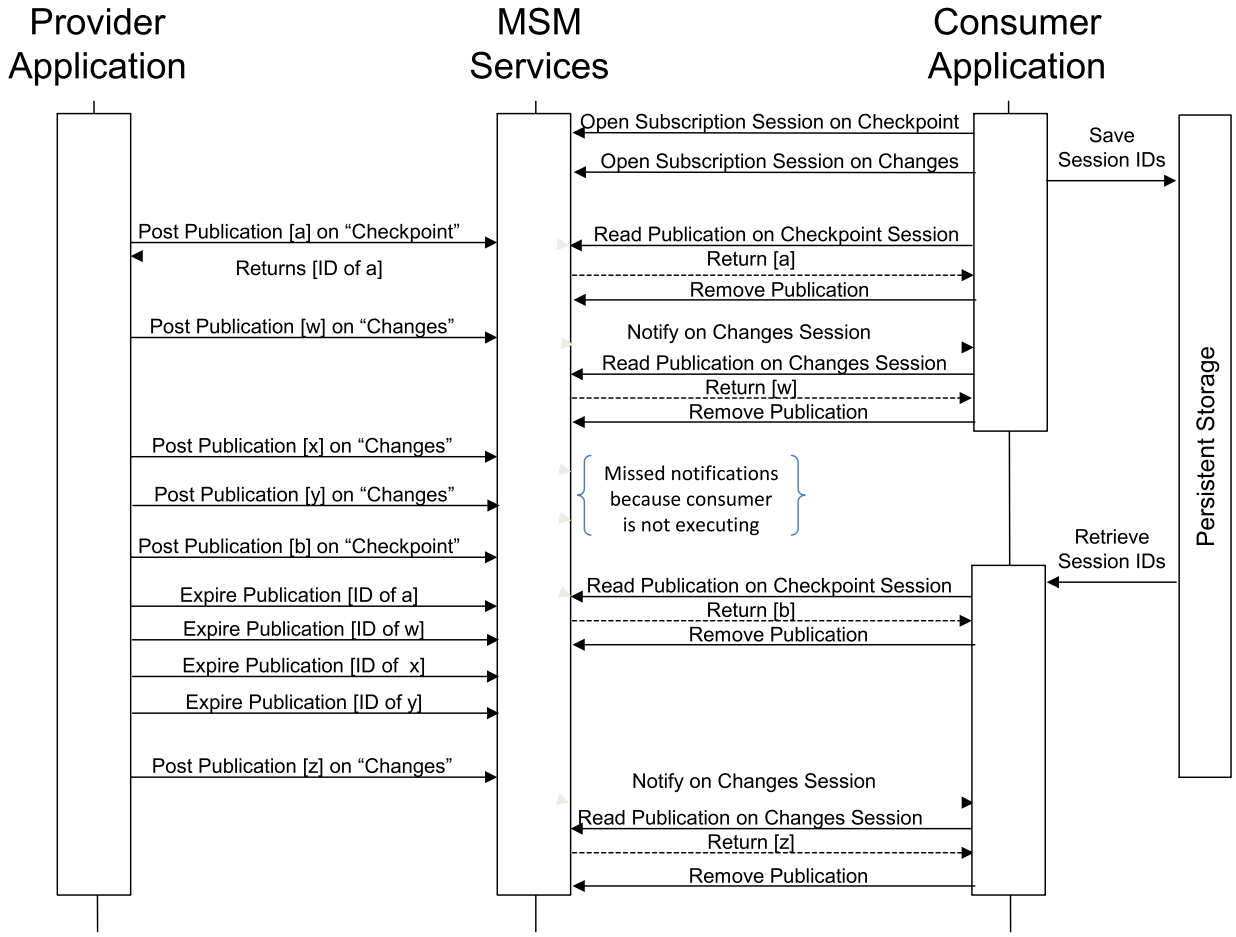

Figure 8 – Changes and checkpoint channel example

5.3 Message filtering

Topics shall be used in application services to limit or filter the type of information that is obtained from read and notify requests for Provider Applications and Consumer Applications.

Topics shall be used by Provider Applications to specify the type of information that they will be publishing or posting on an MSM *Channel*.

Topics allow a single channel to handle a collection of different types of data, yet still provide a method for the receiver of the data to limit the types of data that it is required to handle.

The same topic may be used across multiple channels.

EXAMPLE 1 There may be a *ProductionSchedule* topic defined for *CheckPoint* and *Changes* channels with a site channel scope, and a *ProductionSchedule* topic used for *Checkpoint* and *Changes* channels for an area channel scope.

EXAMPLE 2 There may be a *QualificationTest* topic used for a *Request* channel at the enterprise channel scope, and a *QualificationTest* topic used for a *Request* channel at the country channel scope.

5.4 Publication expiration

Expired publications shall not be available to subscribing consumer applications nor accessible to the provider application. If an already read message subsequently expires, it is still available to the consumer to ensure a Remove Publication call removes the correct message.

Copyright International Electrotechnical Commission

A publication can be flagged as expired by a provider application via the Expire Publication service or through an expiration time defined when the publication is posted.

With the time-based expiration, the expiration time is calculated based on the *completion of invocation* of the Post Publication service plus the specified duration.

Any publication message may be expired through the Expire Publication service.

5.5 Topics

5.5.1 Topic definition

Topics shall be used in application services to limit or filter the type of information that is obtained from read and notify requests for Provider Applications and Consumer Applications.

Topics shall be used by Provider Applications to specify the type of information that they will be publishing or posting on an MSM *Channel*.

Topics allow a single channel to handle a collection of different data, yet still provide a method for the receiver of the data to limit the types of data that it is required to handle.

5.5.2 Standard topics

To support interoperability, the *topics* should correspond to the transaction message verbs and nouns, as defined in the ISA-95.05 and B2MML or other standards.

EXAMPLE 1 Classes of nouns from the ISA-95.02 and ISA-95.04 standards

Equipment Class	Equipment	Capability Test
Personnel Class	Person	Qualification Test
Material Class	Material Definition	Material Lot
Material Sublot	Material Test	
Operations Capability	Operations Definition	Operations Performance
Operations Schedule	Process Segment	Production Capability
Product Definition	Production Schedule	Production Performance
Resource Relationship Network	Transaction Profile	Work Alert
Work Capability	Work Definition	Work Performance
Work Schedule	Workflow Specification	

The topic names should contain the associated standard and version number of the associated standard or noun.

EXAMPLE 2 One topic may be defined for messages using B2MML-V0402-MaterialLot definitions, another for B2MML-V0501-MaterialLot definitions and a third topic for messages using B2MML-V0600-MaterialLot definitions.

The same topic may be defined on multiple channels.

EXAMPLE 3 There may be a *ProductionSchedule* topic defined for *CheckPoint* and *Changes* channels with a site channel scope, and a *ProductionSchedule* topic defined for *Checkpoint* and *Changes* channels for an area channel scope.

EXAMPLE 4 There may be a *QualificationTest* topic defined for a *Request* channel at the enterprise channel scope, and a *QualificationTest* topic defined for a *Request* channel at the country channel scope.

Copyright International Electrotechnical Commission

5.6 MSM sessions

Communication to channels shall be through MSM sessions. MSM sessions are created through open session services, which return a session ID.

Session IDs shall be persistent and shall not be tied to the execution instance of the requesting program. A session ID remains valid even if the calling program stops and restarts, as long as the calling program maintains the session ID (in storage) and can read it on restart, then the MSM session is still available.

5.7 Security

5.7.1 Secure message exchanges

Security in message exchanges shall be defined as authenticated access to MSM channel services.

NOTE Security in the MSM services is of paramount importance. In the MSM Service model the communication applications have no knowledge of their communication partners, and do not know if there are none (for a publisher with no subscriptions), one, or many. Therefore, security cannot be defined as communication with trusted partners, but as communication through secure channels.

5.7.2 Security tokens on channels

Channel access security shall be managed through security tokens.

Security tokens are assigned to channels.

Security tokens on channels may be optionally added to channels by the users of the MSM services.

NOTE While the MSM service provider is required to provide security, the final users of the MSM services may decide not to assign any security tokens to one or more channels, in which case the channels may be accessed without any authentication control.

Security tokens shall be used by applications when opening or subscribing to a channel. If the application provided Security Token does not match a Security Token assigned to the channel, then no channel information is returned.

Security tokens are exchanged in an out-of-band communication channel, such as manual exchange of tokens, or electronic exchange through a secure point-to-point channel.

Copyright International Electrotechnical Commission

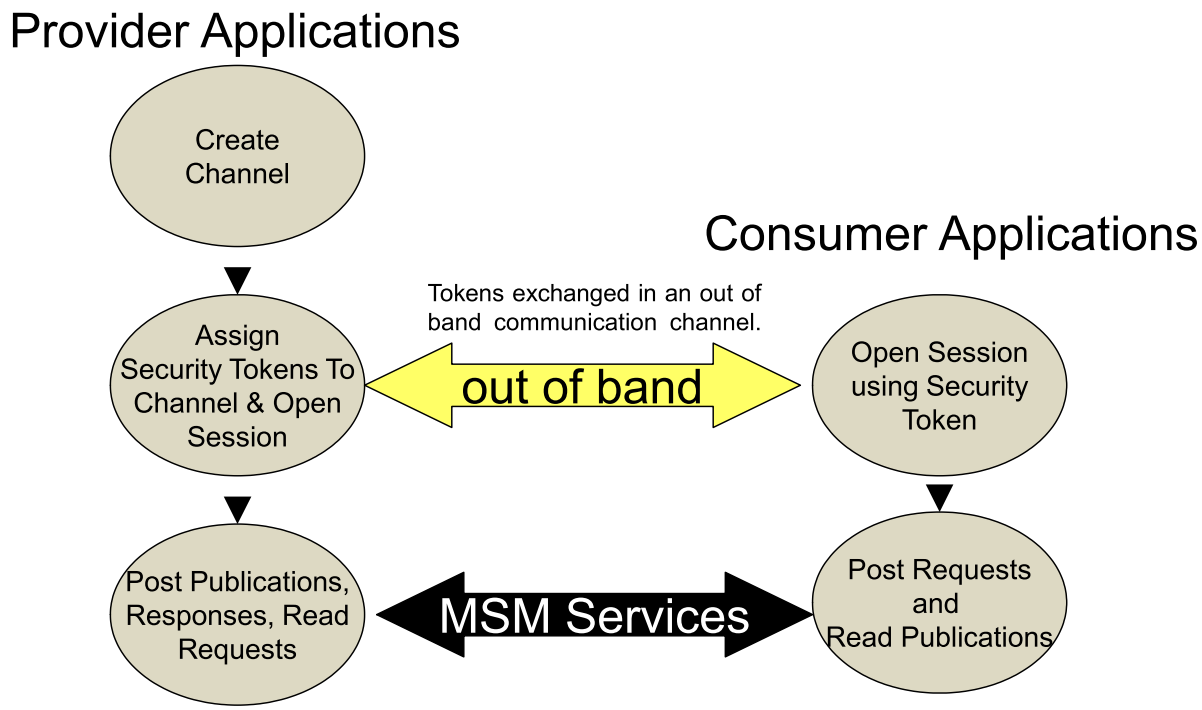

Figure 9 – Security of channels

5.7.3 Security token format

The Security Token format shall be defined in the MSM implementation specification. Different implementations may have different methods and formats for the security tokens.

5.7.4 MSM service provider implementations

1) All *MSM Service Providers* shall implement security tokens.
2) *MSM Service Providers* may limit the ability to use the MSM Channel Management services to approved applications, servers, or domains in order to increase security.
3) In an implementation, providers and consumers shall arbitrate the level of security to be used for a channel, if any. While there is a requirement that the services provide security services, there is no requirement that a specific implementation use the services.

EXAMPLE 1 A system may share information across companies through open Internet channels. In this case an MSM *Service Provider* implementation should provide a strong Security Token system through a public key mechanism with specific Security Token assigned to specific communicating companies.

EXAMPLE 2 A system may be entirely contained within a secure environment behind both corporate and operations firewalls. In this case the user may decide to not assign security tokens to channels and rely on other measures to ensure security.

6 MSM service definitions

6.1 Type definitions

Table 1 contains the type definitions that are associated with the service definitions.

Copyright International Electrotechnical Commission

Table 1 – MSM type definitions

Type	Definition
Channel Description	Text used in browsing channels and to provide assistance in maintenance of an MSM implementation.
Channel Type	Indicates whether the channel is for publications, requests or responses. The MSM implementation may use the channel type to ensure the correct session creation service is called for a channel. Defined Channel Types are “Publication” and “Request”.
Channel URI	The primary identifier for a channel. The Channel URI should be a wide string allowing channel names with international character sets. See 5.2 for details on the format.
Filter Expression	An optional filtering element that may be applied to messages on a channel. The format of the filter expression is not defined in this PAS, but would be defined in an MSM implementation specification.
Session ID	An identifier generated by the MSM upon an application creating a session on a channel and provided to the application for use in the MSM services.
Listener Identification	An implementation defined element that is used to indicate to an application when a new message has arrived. EXAMPLE A URI endpoint, reachable by the MSM Service Provider, that hosts an MSM Notification Service.
Message ID	An identifier generated by the MSM upon posting of a message to a channel in a session.
Message Content	The message content.
Message Expiry	The duration until the expiration of a publication message on a publication channel.
Security token	The security tokens assigned to the channel.
Session ID	A unique identification of the communication session used in using an MSM channel.
Topic	An identification of the topic of a message, see 5.5.

6.2 MSM service returns and faults

Table 2 contains the service returns and faults for the MSM service definitions.

Faults should contain a human readable explanation.

Table 2 – MSM service returns and fault definitions

Type	Definition
Channel Fault	Error returned when a Channel URI is invalid or the application does not have the appropriate Security Token to access the channel.
Listener Identification	An identification of a listener function, defined by the implementation technology.
Message ID	A unique identification of a message.
Operation Fault	Error returned when an illegal operation for the channel type is attempted.
Parameter Fault	Error indicating a missing or invalid parameter passed to a service.
Publication Message	A message which should be in the format defined by ISA-95 Part 5 SYNC messages.
Request Message	A message which should be in the format defined by ISA-95 Part 5 GET, PROCESS, CHANGE, and CANCEL messages.
Request Message ID	The Message ID of a request message.

Copyright International Electrotechnical Commission

Type	Definition
Response Message	A message which should be in the format defined by ISA-95 Part 5 SHOW, ACKNOWLEDGE, RESPOND, and CONFIRM messages.
Security Token Fault	Error returned when an invalid Security Token is used.
Session Fault	Error returned when an invalid Session ID is used in a service.

6.3 MSM channel management services

6.3.1 Create channel

The create channel service shall have the function, input parameters and returns defined in Table 3.

Table 3 – Create channel

Name	Create channel
Function	Creates an MSM channel of the specified Channel Type. If the channel already exists, then a *Channel Fault* is returned. Any specified security tokens are added to the channel.
Input Parameters	– Channel URI – Channel Type (Publication or Request) – Optional Description of the channel – Optional list of Security Tokens
Returns	– Success or error criteria

6.3.2 Add security tokens

The add Security Token service shall have the function, input parameters and returns defined in Table 4.

Table 4 – Add security token

Name	Add security tokens
Function	Adds security tokens to a channel. If the Channel URI does not exist, or if the specified channel is assigned security tokens and the Security Token does not match a token already assigned to the specified channel, then a *Channel Fault* is returned. If a new Security Token has already been assigned to the channel, then no action is taken.
Input Parameters	– Channel URI – Optional Security Token – List of Security Tokens to add
Returns	– Success or error criteria

6.3.3 Remove security tokens

The remove Security Token service shall have the function, input parameters and returns defined in Table 5.

Copyright International Electrotechnical Commission

Table 5 – Remove security token

Name	Remove Security Tokens
Function	Removes security tokens from a channel. If the Channel URI does not exist, then a *Channel Fault* is returned. If the specified channel is assigned security tokens and the Security Token does not match a token assigned to the specified channel, then a *Channel Fault* is returned. If any Security Token to be removed is not assigned to the channel, then a *Security Token Fault* is returned and no tokens are removed from the channel, even if they are valid.
Input Parameters	– Channel URI – Security Token – List of Security Tokens to remove
Returns	– Success or error criteria

6.3.4 Delete channel

The delete channel service shall have the function, input parameters and returns defined in Table 6.

Table 6 – Delete channel

Name	Delete Channel
Function	Deletes an MSM Channel. If the Channel URI does not exist, then a *Channel Fault* is returned. If the specified channel is assigned security tokens and the Security Token does not match a token assigned to the specified channel, then a *Channel Fault* is returned. The channel along with associated sessions and messages are no longer available. No notification is provided to any applications with active sessions.
Input Parameters	– Channel URI – Optional Security Token
Returns	– Success or error criteria

6.3.5 Get channel

The get channel service shall have the function, input parameters and returns defined in Table 7.

Table 7 – Get channel

Name	Get Channel
Function	Gets information about a channel. If the Channel URI does not exist, then a *Channel Fault* is returned. If the specified channel is assigned security tokens and the Security Token does not match a token assigned to the specified channel, then a *Channel Fault* is returned.
Input Parameters	– Channel URI – Optional Security Token
Returns	– Success or error criteria – Channel URI – Channel Type – Channel Description

Copyright International Electrotechnical Commission

6.3.6 Get channels

The get channels service shall have the function, input parameters and returns defined in Table 8.

Table 8 – Get channels

Name	Get Channels
Function	Gets information about all channels where the Security Token matches one of the channel's Security Tokens. If there is no match, then an empty list of channel URIs is returned.
Input Parameters	– Optional Security Token
Returns	– Channel URIs – Channel Types – Channel Descriptions

6.4 Notify listener service

6.4.1 Notify listener

The notify listener service shall have the function, input parameters and returns defined in Table 9.

Table 9 – Notify listener

Name	Notify Listener
Function	Receives a notification of a new message on a channel, using the Listener Identification specified when a session is opened. This is a call-back function provided by the Provider or Consumer application when subscribing to a channel. The interface is defined so that the applications can define their local call-back functions with the correct interface.
Input Parameters	Input parameters are defined by the specific MSM technology implementation
Returns	Returns are defined by the specific MSM technology implementation

NOTE Notify listener services will generally return a SessionID, MessageID, Topic, and optional RequestMessageID.

6.5 MSM provider publication services

6.5.1 Open publication session

The open publication session service shall have the function, input parameters and returns defined in Table 10.

Copyright International Electrotechnical Commission

Table 10 – Open publication session

Name	Open Publication Session
Function	Opens a publication session for a channel and returns an ID for the session. If the Channel URI does not exist, then a *Channel Fault* is returned. If the specified channel is assigned security tokens and the Security Token does not match a token assigned to the specified channel, then a *Channel Fault* is returned. If the channel type is not a Publication type, then an *Operation Fault* is returned.
Input Parameters	– Channel URI – Optional Security Token
Returns	– Success or error criteria – Session ID

6.5.2 Post publication

The post publication service shall have the function, input parameters and returns defined in Table 11.

Table 11 – Post publication

Name	Post Publication
Function	Posts a publication message to a channel and creates a message with the Message Content and a Message ID that uniquely identifies message, and makes it available for subscribers. If the Session ID does not exist or does not correspond to a publication session, then a *Session Fault* is returned. If a Topic is blank, then a *Parameter Fault* is returned.
Input Parameters	– Session ID – Publication Message – List of topics – Optional Expiration Duration for the publication
Returns	– Success or error criteria – Message ID of posted message

6.5.3 Expire publication

The expire publication service shall have the function, input parameters and returns defined in Table 12.

Table 12 – Expire publication

Name	Expire Publication
Function	The publication is no longer available to subscribers. If an already read message subsequently expires, it is still available to the consumer to ensure a RemovePublication call removes the correct message. If the Session ID does not exist or does not correspond to a publication session, then a *Session Fault* is returned. If the Message ID does not correspond with the Session ID or the corresponding message has already expired, then no action is taken. The message is expired for all topics associated with the message.
Input Parameters	– Session ID – Message ID
Returns	– Success or error criteria

Copyright International Electrotechnical Commission

6.5.4 Close publication session

The close publication session service shall have the function, input parameters and returns defined in Table 13.

Table 13 – Close publication session

Name	Close Publication Session
Function	Closes a publication session. All unexpired messages that have been posted during the session will be expired. If the Session ID does not exist (non-existent or already closed), then a *Session Fault* is returned. If the Session ID does not correspond to a Publication channel type, then a *Session Fault* is returned.
Input Parameters	– Session ID
Returns	– Success or error criteria

6.6 MSM consumer publication services

6.6.1 Open subscription session

The open subscription session service shall have the function, input parameters and returns defined in Table 14.

Table 14 – Open subscription session

Name	Open Subscription Session
Function	Open a subscription session for a channel. A subscription session will not pick up messages posted prior to the subscription session start. If the Channel URI does not exist, then a *Channel Fault* is returned. If the specified channel is assigned security tokens and the specified Security Token does not match a token assigned to the specified channel, then a *Channel Fault* is returned. If the channel type is not a Publication type, then an *Invalid Operation Fault* is returned. If a Topic is blank, then an Invalid *Parameter Fault* is returned.
Input Parameters	– Channel URI – List of Topics (subscribed to) – Optional Security token – Optional Listener Identification – Optional Filter Expression
Returns	– Success or error criteria – Session ID

6.6.2 Read publication

The read publication service shall have the function, input parameters and returns defined in Table 15.

Copyright International Electrotechnical Commission

Table 15 – Read publication

Name	Read Publication
Function	Returns the first non-expired publication message (if any) that satisfies the session message filters. If the Session ID does not exist, then a *Session Fault* is returned. If the Session ID does not correspond to a publication session, then a *Session Fault* is returned. If there are no publication messages, then a null publication message is returned.
Input Parameters	– Session ID
Returns	– Success or error criteria – Publication Message – Message ID – List of topics for the Publication Message

6.6.3 Remove publication

The remove publication service shall have the function, input parameters and returns defined in Table 16.

Table 16 – Remove publication

Name	Remove Publication
Function	Removes the first publication message in the subscription queue. If there is no publication message then no action is taken. If the Session ID does not exist, then a *Session Fault* is returned. If the Session ID does not correspond to a publication session, then a *Session Fault* is returned.
Input Parameters	– Session ID
Returns	– Success or error criteria

6.6.4 Close subscription session

The close subscription session service shall have the function, input parameters and returns defined in Table 17.

Table 17 – Close subscription session

Name	Close Subscription Session
Function	Close the subscription session. If notification has been defined, then there will be no more notifications. Any unread publications for the session are no longer available. If the Session ID does not exist, then a *Session Fault* is returned. If the Session ID does not correspond to a publication session, then a *Session Fault* is returned.
Input Parameters	– Session ID
Returns	– Success or error criteria

Copyright International Electrotechnical Commission

6.7 MSM provider request services

6.7.1 Open provider request session

The open provider request session service shall have the function, input parameters and returns defined in Table 18.

Table 18 – Open provider request session

Name	Open Provider Request Session
Function	Opens a provider request session for reading requests and posting responses. If the Channel URI does not exist, then a *Channel Fault* is returned. If the specified channel is assigned security tokens and the specified Security Token does not match a token assigned to the specified channel, then a *Channel Fault* is returned. If the Channel Type is not a *Request* type, then an *Invalid Operation Fault* is returned. If a Topic is blank, then an Invalid *Parameter Fault* is returned.
Input Parameters	– Channel URI – List of Topics – Optional Security token – Optional Listener Identification – Optional Filter Expression
Returns	– Success or error criteria – Session ID

6.7.2 Read request

The read request service shall have the function, input parameters and returns defined in Table 19.

Table 19 – Read request

Name	Read Request
Function	Returns the first request message in the message queue for the session. This service does not remove the message from the message queue. The returned Topic will correspond to the topic that matched the posted request. If the Session ID does not correspond to a provider request session, then a *Session Fault* is returned.
Input Parameters	– Session ID
Returns	– Success or error criteria – Returned Message – Returned Message ID – Topic of the returned message

6.7.3 Remove request

The remove request service shall have the function, input parameters and returns defined in Table 20.

Copyright International Electrotechnical Commission

Table 20 – Remove request

Name	Remove Request
Function	Removes the first request message from the request session. If the Session ID does not exist, then a *Session Fault* is returned. If the Session ID does not correspond to a provider Request session, then a *Session Fault* is returned.
Input Parameters	– Session ID
Returns	– Success or error criteria

6.7.4 Post response

The post response service shall have the function, input parameters and returns defined in Table 21.

Table 21 – Post response

Name	Post Response
Function	Posts a response message to a request message. If the Session ID does not exist, then a *Session Fault* is returned. If the Session ID does not correspond to a provider Request session, then a *Session Fault* is returned. If any parameter is malformed or blank, then an *Invalid Operation Fault* is returned. If there is no request message that can be matched to Request Message ID, then no action is taken.
Input Parameters	– Session ID – Request Message ID – Response Message
Returns	– Success or error criteria – Response Message ID

6.7.5 Close provider request session

The close provider request session service shall have the function, input parameters and returns defined in Table 22.

Table 22 – Close provider request session

Name	Close Provider Request Session
Function	Closes a provider request session. If the Session ID does not exist, then a *Session Fault* is returned. If the Session ID does not correspond to a provider request session, then a *Session Fault* is returned.
Input Parameters	– Session ID
Returns	– Success or error criteria

Copyright International Electrotechnical Commission

6.8 MSM consumer request services

6.8.1 Open consumer request session

The open consumer request session service shall have the function, input parameters and returns defined in Table 23.

Table 23 – Open consumer request session

Name	Open Consumer Request Session
Function	Open a consumer request session for posting requests and reading responses. If the Channel URI does not exist, then a *Channel Fault* is returned. If the specified channel is assigned security tokens and the specified Security Token does not match a token assigned to the specified channel, then a *Channel Fault* is returned. If the channel type is not a *Request* type, then an *Invalid Operation Fault* is returned.
Input Parameters	– Channel URI – Optional Security token – Optional Listener Identification
Returns	– Success or error criteria – Session ID

6.8.2 Post request

The post request service shall have the function, input parameters and returns defined in Table 24.

Table 24 – Post request

Name	Post Request
Function	Post a request message on the request-response channel and return the ID of the message. If the Session ID does not exist, then an *Invalid Operation Fault* is returned. If the Session ID does not correspond to a consumer request session, then a *Session Fault* is returned. If a Topic is blank, then an Invalid *Parameter Fault* is returned.
Input Parameters	– Session ID – Request Message – Topic of the request – Optional Request Timeout
Returns	– Success or error criteria – Request Message ID – Optional Expiration Duration for the request

NOTE Topics are coordinated as part of the system installation. If any system is posting requests that have no providers, then the messages will not be answered. Implementations may consider adding timeouts and return errors if a provider does not pick up a request within a reasonable time.

6.8.3 Read response

The read response service shall have the function, input parameters and returns defined in Table 25.

Copyright International Electrotechnical Commission

Table 25 – Read response

Name	Read Response
Function	Read the response message from a posted request. If the Session ID does not exist, then a *Session Fault* is returned. If the Session ID does not correspond to a consumer request session, then an *Invalid Operation Fault* is returned. If the Request Message ID does not correspond to a message in the message queue, then no message is returned.
Input Parameters	– Session ID – Request Message ID
Returns	– Success or error criteria – Response Message

6.8.4 Remove response

The remove response service shall have the function, input parameters and returns defined in Table 26.

Table 26 – Remove response

Name	Remove Response
Function	Remove a response message from the request-response channel. If the Session ID does not exist, then a *Session Fault* is returned. If the Session ID does not correspond to a consumer request session, then an *Invalid Operation Fault* is returned. If the Request Message ID does not correspond to a message in the message queue, then no action is taken.
Input Parameters	– Session ID – Request Message ID
Returns	– Success or error criteria

6.8.5 Close consumer request session

The close consumer request session service shall have the function, input parameters and returns defined in Table 27.

Table 27 – Close consumer request session

Name	Close Consumer Request Session
Function	Close a consumer request session. If the Session ID does not exist, then a *Session Fault* is returned. If the Session ID does not correspond to a consumer request session, then a *Session Fault* is returned.
Input Parameters	– Session ID
Returns	– Success or error criteria

Copyright International Electrotechnical Commission

7 Scenarios

7.1 Publish-subscribe scenarios

7.1.1 Simple publish-subscribe scenario

A simple publish/subscribe scenario with a single provider application and a single consumer application using the notification services, is shown in Figure 10.

NOTE 1 There will usually be multiple consumer applications receiving publications, but only one is shown in this example.

NOTE 2 It is assumed that the appropriate channels and topics have been created prior to the scenario.

In this scenario, the provider application opens an MSM publication channel with a channel URI and security token. When the provider application has determined that data should be published, it posts publications (using SYNC messages) with a message topic.

A consumer application subscribes to the MSM publication channel using a channel URI, security token, and list of topics. The session ID is saved in case the consumer application stops unexpectedly.

When a new message with the right topic is posted, the consumer application is notified of the posting and then reads the new publication message from the MSM channel.

When the consumer application no longer needs data, it unsubscribes from the subscription session and clears the session ID in persistent storage so that it will open a new session when restarted.

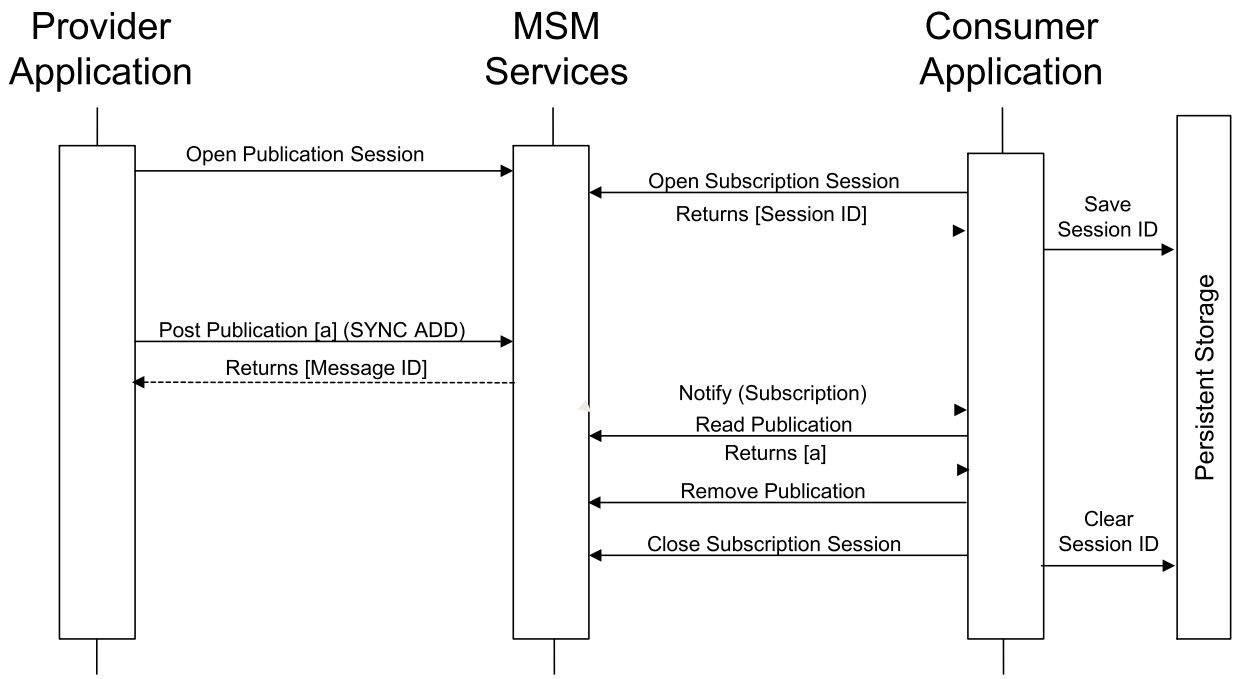

Figure 10 – Publication scenario with notification

7.1.2 Publish-subscribe scenario with multiple messages

A simple publish/subscribe scenario with a single provider application, notification services available, and consumer applications using the notification services, for multiple messages is shown in Figure 11.

Copyright International Electrotechnical Commission

NOTE See the Methods of Operation for a recommendation of the structure of channels for a more robust actual implementation.

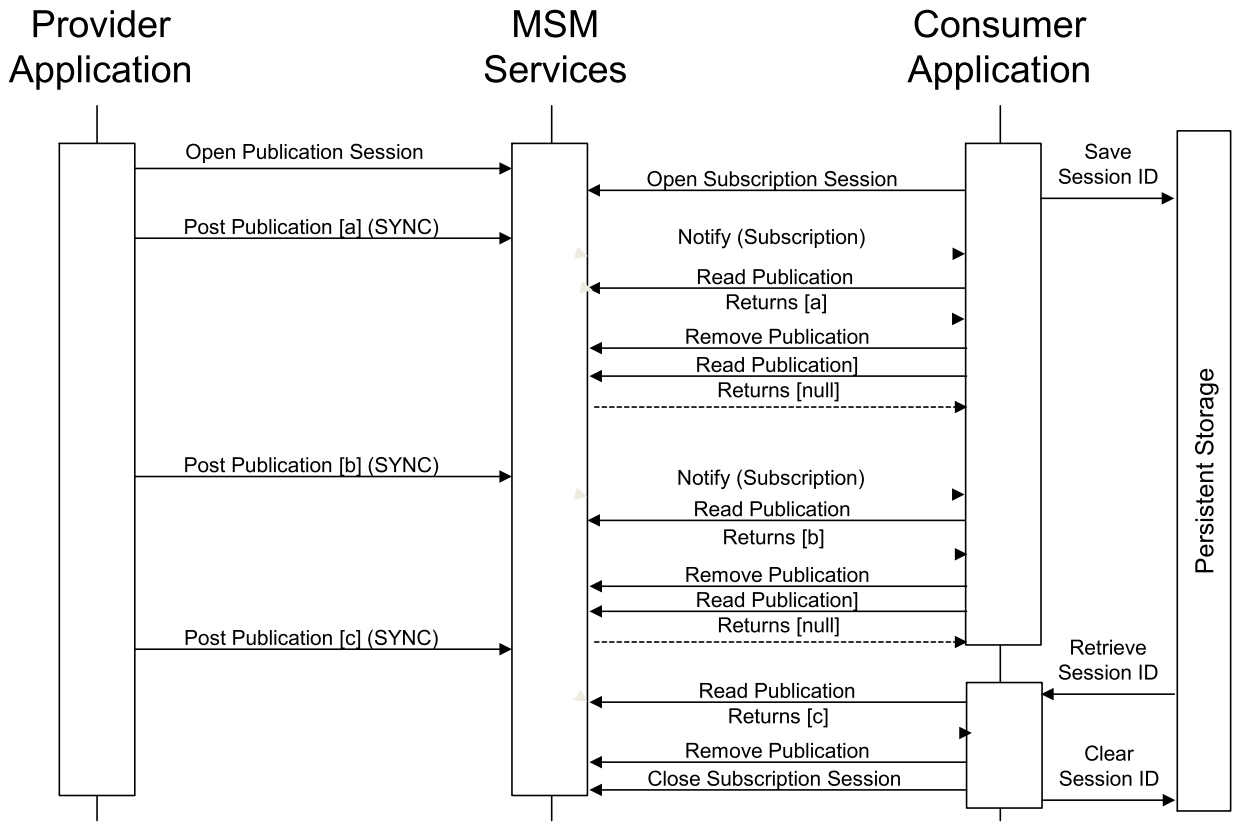

Figure 11 – Publication scenario with multiple messages

In this scenario, the provider application opens an MSM publication session for a given channel. When the provider application has determined that data should be published, it posts publication [a] with a message topic and no message expiry.

A consumer application opens a session to the MSM publication channel using the same channel and list of topics. The session ID is stored for later use when the consumer application stops and restarts.

When a notification is received, the consumer application reads and removes all publications until a null is returned from the Read Publication.

When the consumer application stops and restarts it retrieves the saved session ID. Because the consumer application was not active, there may have been a missed notification so the application reads and removes all new publications until a null is returned from the Read Publication.

When the consumer application has finished all processing and no longer wants to receive subscriptions it closes the subscription session and clears the saved session ID.

7.1.3 Publish-subscribe scenario without notification

A publish/subscribe scenario with a single provider application, where notification services are not available or the consumer application is not able to use notification services, is shown in Figure 12. In this scenario there is no change for the actions of the provider application from the scenario in 7.1.1.

Copyright International Electrotechnical Commission

In this scenario, the consumer application would poll the MSM channel for publications either periodically or based on some local event. The returned information from the read indicates if a new publication was returned.

The next *Read Publication* call returns either the next publication from the subscription queue or null if there are no more publications available.

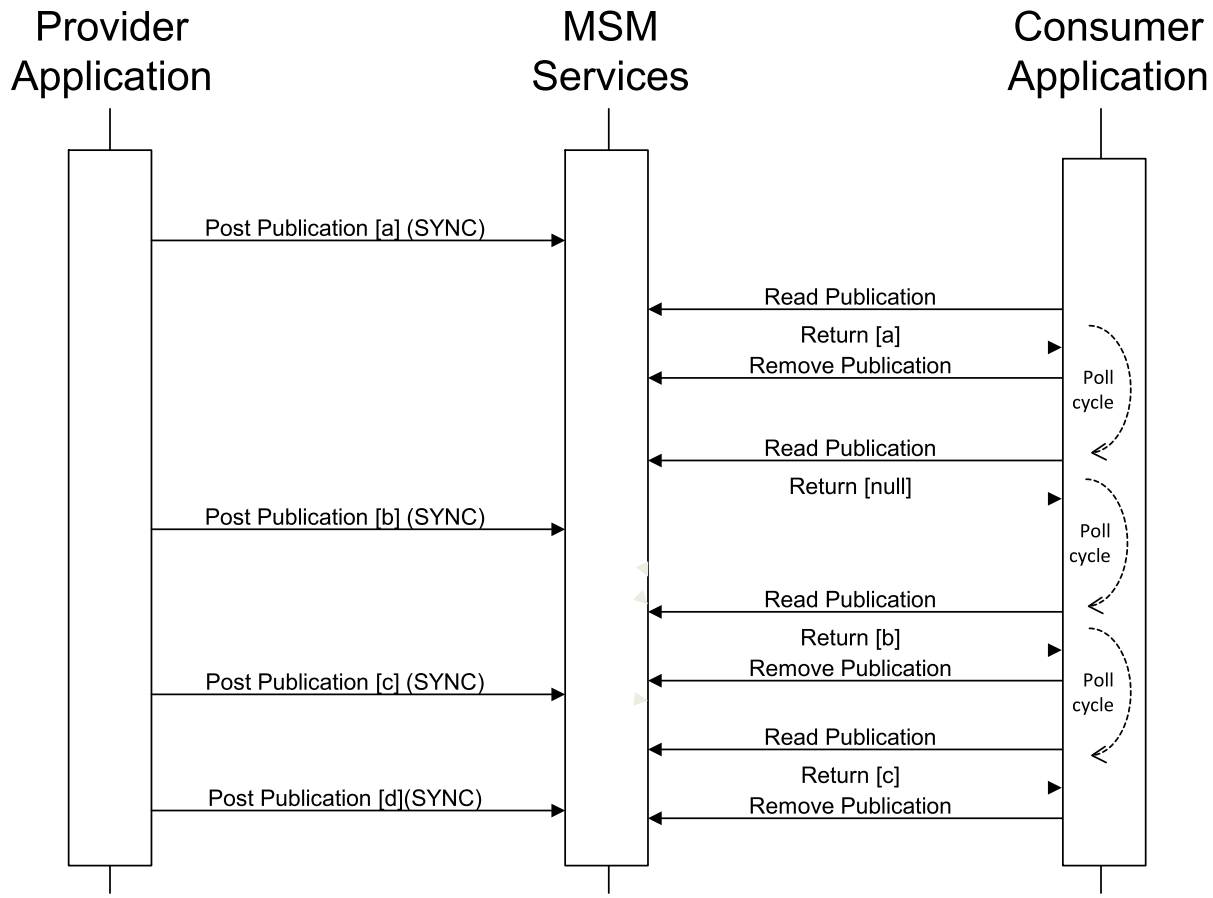

Figure 12 – Publication scenario without notification

7.1.4 Multiple publishers scenario

More than one provider application may use the same publication channel. The scenario shown in Figure 13 has two provider applications. For example, one application could publish changes with topics for Material Definitions while another may publish changes with topics for Material Lots.

Copyright International Electrotechnical Commission

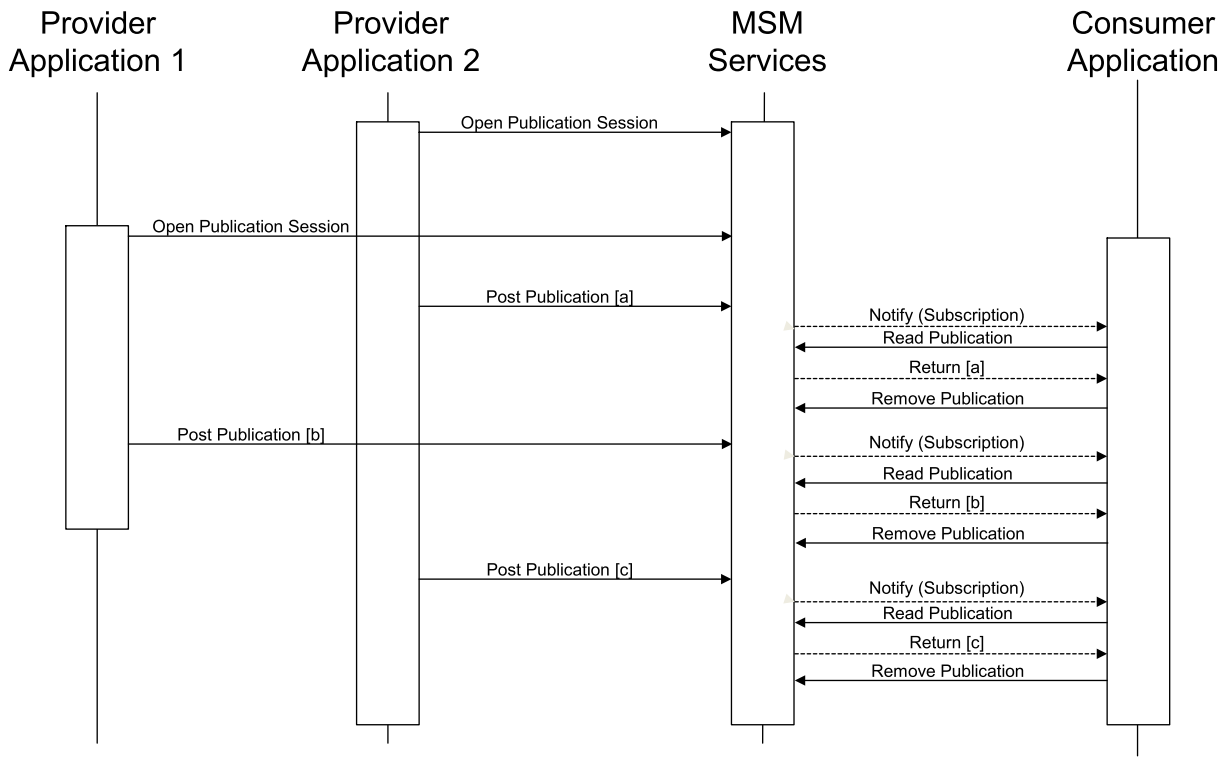

Figure 13 – Publication scenario with multiple provider applications

7.1.5 Publish-subscribe scenario with publication expiration

Message expiration can be used by provider applications to remove messages from a consumer application's visibility. This could be due to a number of reasons, including changing relevancy of the message or inaccuracies in the message. The scenario in Figure 14 highlights expiration behaviour in two cases:

– where a read message has expired, and

– where an unread message has expired.

On the second *Read Publication* call by the consumer application, the MSM Service Provider returns the next message in the subscription queue – although in this case, there is no message. The third *Read Publication* returns the next unexpired publication in the subscription queue, message [c].

Copyright International Electrotechnical Commission

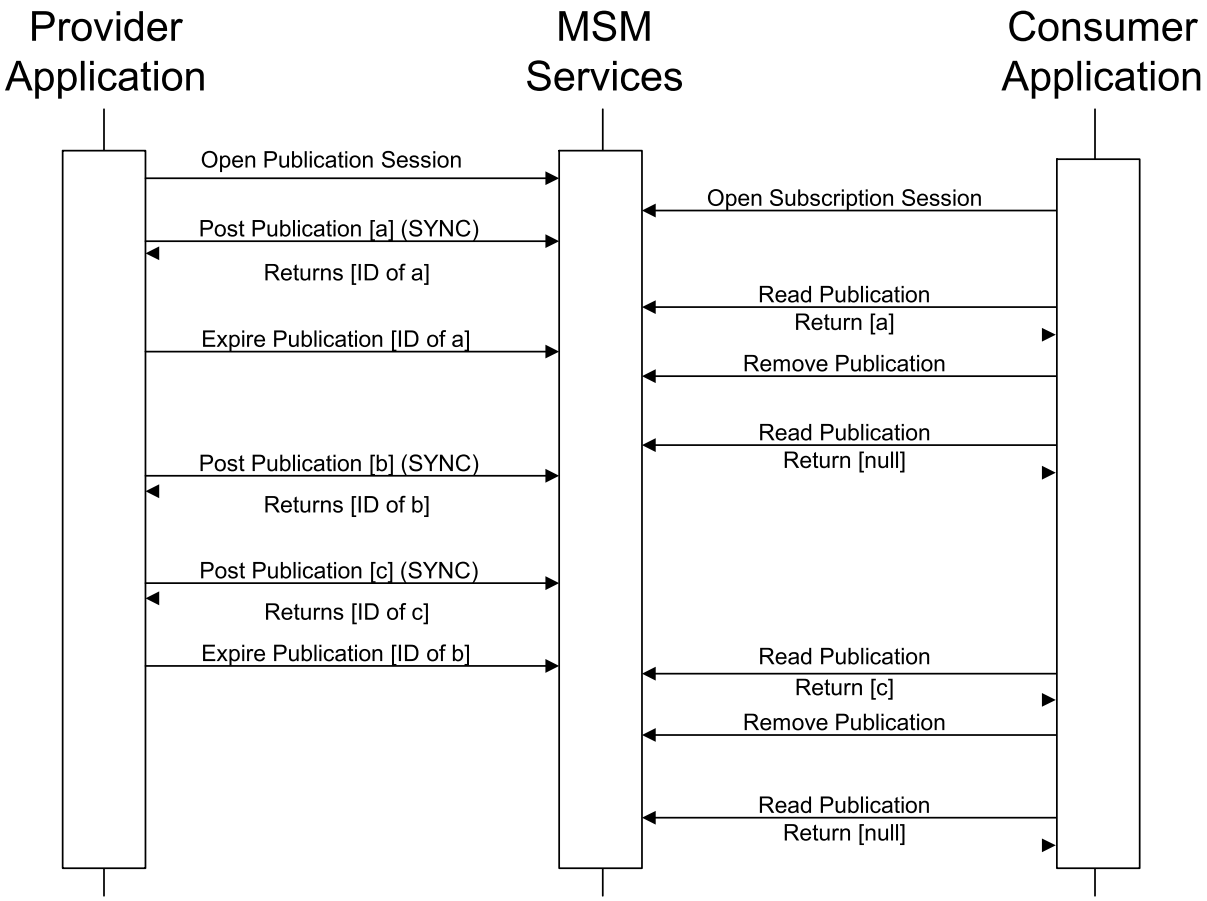

Figure 14 – Publication scenario with expired publications

7.2 Request channel scenarios

7.2.1 Request-response scenario with notification

Figure 15 illustrates a scenario for a GET/SHOW transaction with the provider application, consumer application, and a channel supporting notification.

Copyright International Electrotechnical Commission

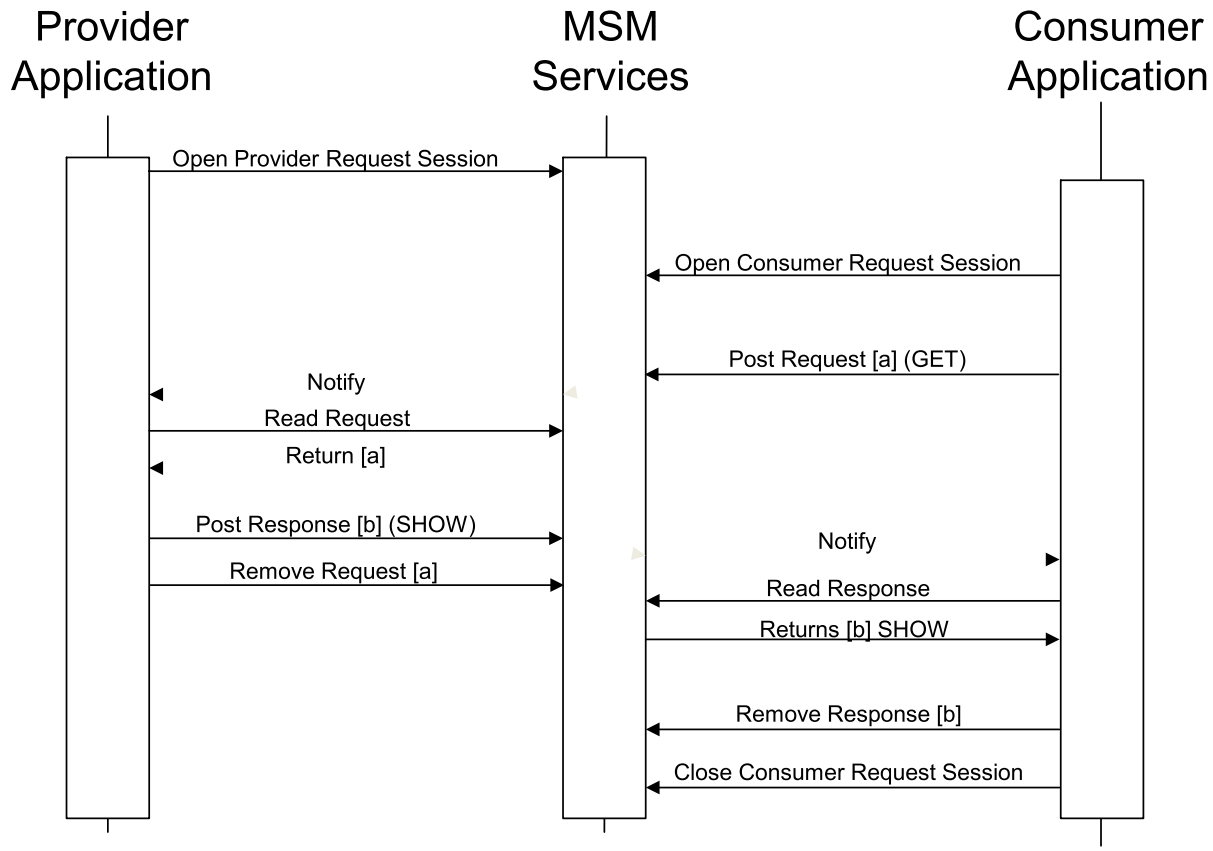

Figure 15 – GET/SHOW request service scenario

In Figure 15, a provider application opens a provider request session. A consumer application opens a consumer request session and posts a request [a]. The provider is notified and reads the request [a]. The provider application performs its appropriate function (in this case to get data) and sends the response message [b] (in this case a SHOW message) and then removes the request [a]. The consumer application is notified of the posting and reads the response [b] and then removes the response [b].

7.2.2 Request-response scenario without notification

If the applications or MSM services do not support notification, then the provider may poll for a request and consumer applications may poll for a response. Figure 16 illustrates a scenario using a CHANGE-RESPONSE transaction where the consumers and providers must poll for a response.

Copyright International Electrotechnical Commission

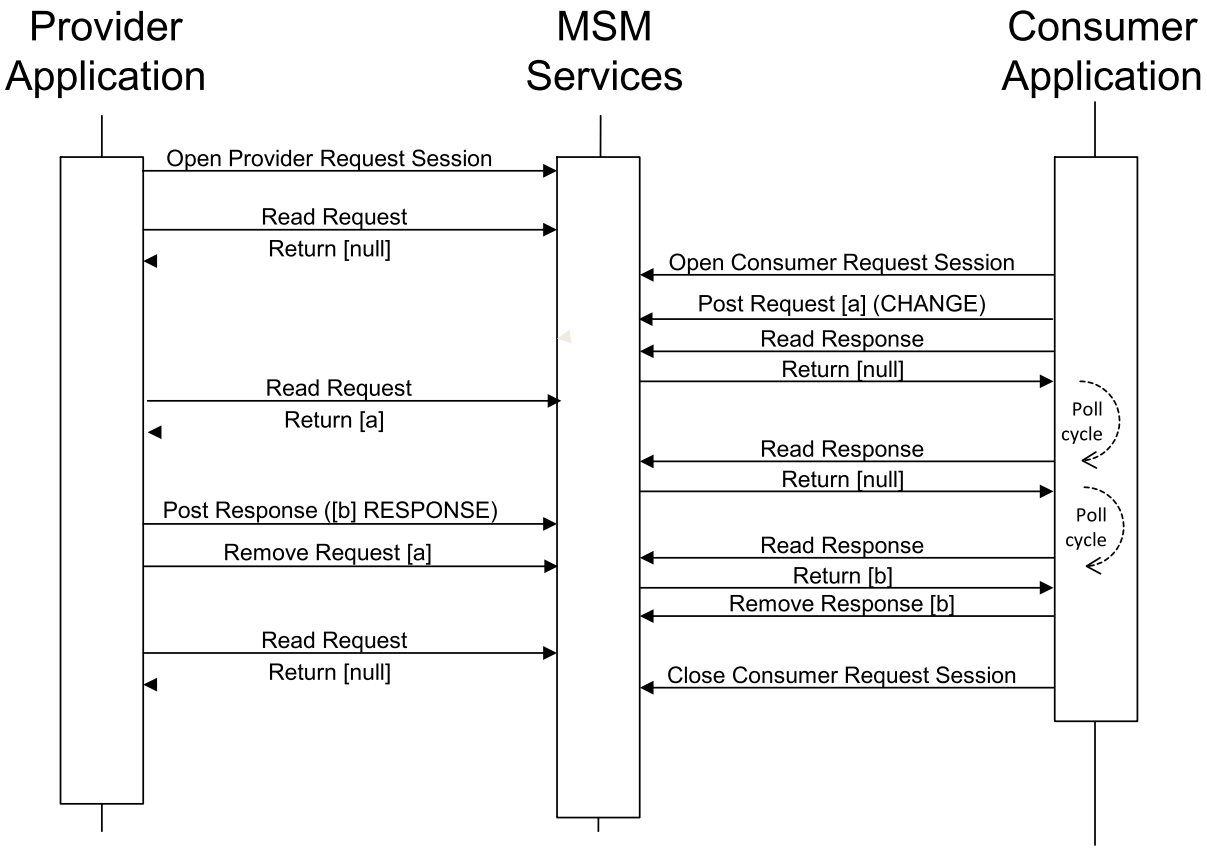

Figure 16 – CHANGE / RESPONSE request service scenario

The GET/SHOW, PROCESS/ACKNOWLEDGE, CHANGE/RESPONSE, and CANCEL transactions are all handled using request channels.

7.2.3 Multiple providers

Figure 17 illustrates a scenario with multiple provider applications. In this case, two provider applications have subscribed to requests on the same MSM channel.

The consumer application posts a CHANGE request with a specific topic (such as Personnel Information).

Application 1 is notified of a request that matches a topic that it subscribed to. Application 1 gets the CHANGE message [a] and generates the RESPONSE message [b]. Application 2 is not notified of the request, because the topic does not match a subscribed topic.

Copyright International Electrotechnical Commission

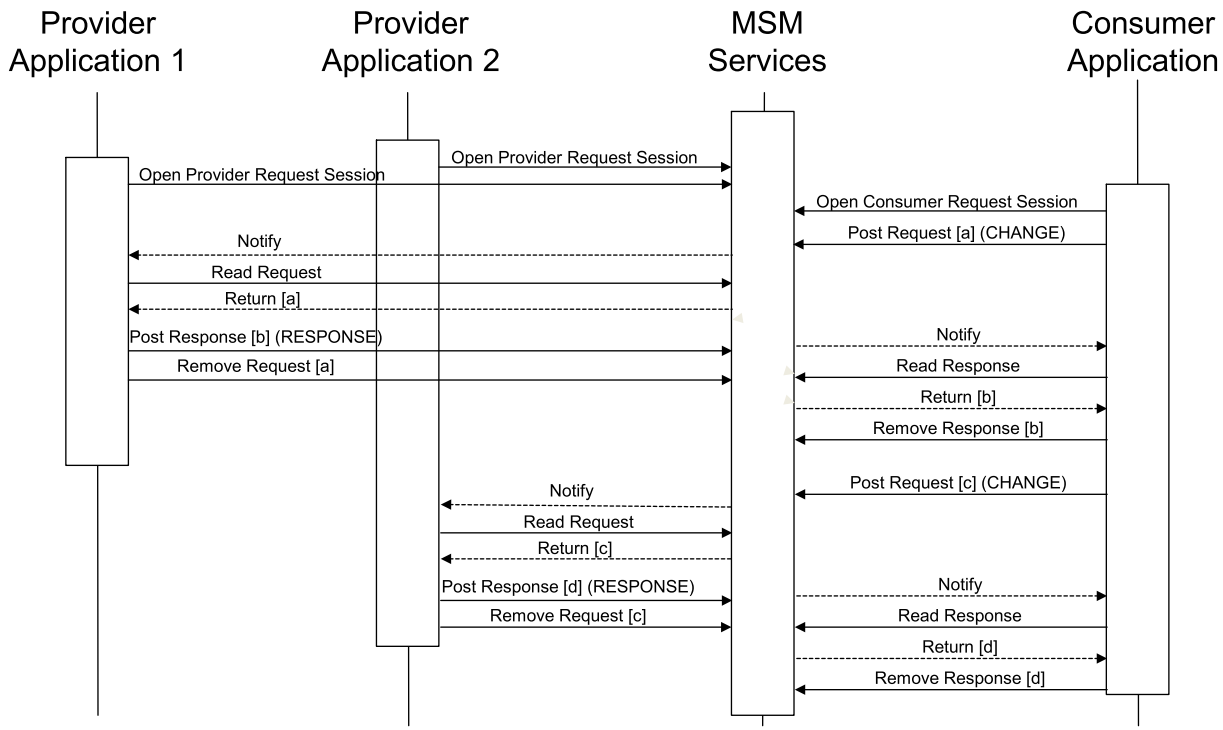

Figure 17 – Multiple providers CHANGE/RESPONSE scenario

NOTE A full system should not have multiple providers for the same topics on the same request channel. If this occurs then there is a possibility that an indeterminate number of response messages would be returned to the consumer application. This consideration requires careful design of a system of applications to remove dual responsibility for request topic provider applications.

8 Compliance

Although this PAS does not contain a statement of compliance, any assessment of compliance should address the following provisions in a separate conformity assessment specification:

a) the use of the terminology defined in this PAS,

b) for each service supported

   i) the support for notification services as defined in 4.6,

   ii) declaration of level of support for Filter Expressions,

   iii) a statement of the total compliance concerning definitions, services, and optional elements or, in case of partial compliance, a statement identifying explicitly the areas of non-compliance.

Copyright International Electrotechnical Commission

Annex A
(informative)

MSM service provider considerations

A.1 Service provider considerations

The following clauses define ESB type services that can be provided by MSM Service Providers. The services are not part of the MSM specification, but provide some of the areas in which vendors and others can provide differentiated service.

A.2 Notification

MSM Service Providers are not required to implement notification capability. This allows light weight MSM Service Provider implementations where polling is an acceptable method for synchronization of applications.

A.3 Security considerations

An MSM *Service Provider* should take the following concerns and issues into account:

a) The *MSM Service Provider* may store messages in a persistent data store. If this is the case and there is security on the channel, then the stored messages may need to be encrypted to prevent unauthorized access to the stored messages.

b) Requests for access with invalid security tokens should be logged. They either indicate a problem with configuration information or a possible attack of the system.

c) Requests for access to invalid channel URIs should be logged. They either indicate a problem with configuration information or a possible attack of the system.

d) Messages exchanged within the MSM Service implementation may require encryption or connection through secure channels. The method used may be dependent on the transport services used and is not defined in the MSM interface.

e) MSM session IDs should be globally unique and use restricted to a specific provider or consumer in order to prevent access to a channel without going through token security.

A.4 MSM application implementation considerations

Any MSM application implementation should take the following concerns and issues into account:

a) Security tokens will usually be stored in the provider and consumer applications so they can be used on startup or restart of the application. The tokens should be saved in a secure manner to prevent unauthorized discovery of the tokens.

b) In high security environments there may be a unique Security Token assigned for each possible communication path and security tokens may be changed on a regular basis, so mechanisms should be in place to exchange tokens on a regular basis.

c) The MSM services will not include validation of messages. The receiving applications should validate any received messages against the agreed to schema sets, such as B2MML.

A.5 MSM channel security considerations

Some implementations may require additional levels of security than defined in 5.2.6. For example, an implementation may require separate security for GET/SHOW messages than for PROCESS, CHANGE, CANCEL messages. Separate request channels may be set up for the query (GET/SHOW) and process (PROCESS, CHANGE, CANCEL) messages.

Copyright International Electrotechnical Commission

A.6 MSM session ID considerations

Consider making MSM session IDs very long numbers or strings, non-obvious, not easily guessable, and unique for each application and channel. This should be done in order to prevent access to a session without going through token controlled security. Several services rely on the MSM session ID for security. Because MSM session IDs are persistent, if an application stores it, then the storage mechanism should have security measures in place to ensure that only the storing application can retrieve the MSM session ID and use it for communication.

A.7 Data format validation

MSM Service Providers could provide data format checking services for messages. If a message is supposed to follow a predefined and well-specified format, such as B2MML or BatchML, then the service provider could provide a service to check the syntax correctness of posted messages.

This would provide a governance check on messages.

In this situation, the MSM Service Provider could maintain a map between topics and XML schema files. The service provider would use that map to check correctness on posted subscriptions, requests, and responses.

A.8 Allowed application checking

MSM Service Providers could provide governance checks that applications creating and subscribing to channels are allowed applications. This check would provide an additional level of security, which may be important if the MSM Services go outside the company.

A.9 Data exchange logging

MSM Service Providers could provide services to log all or selected messages for purposes of governance, compliance, and auditing. Because all messages are in an XML format, and the posting application is known, this could provide an audit or error tracing log that captures all in-band communications.

A.10 Common error handling

MSM Service Providers could provide services for a consistent method for handling errors detected by provider and consumer applications. An error handling service, provided as a dedicated channel, could be used to determine the response to the error. Depending on the error, such as invalid message received, lost message, incorrect data in message, or failure in MSM services, the error handling service could notify the appropriate person or entity with responsibility.

A.11 Data transformation services

MSM Service Providers could provide transformation services for messages. Typically, this would be from a provider or consumer application-specific format into a common format (such as B2MML or BatchML), and from a standard format to an application-specific format.

There is no requirement that an *MSM Service Provider* provide transformation services.

Copyright International Electrotechnical Commission

A recommended method to handle the transformation interfaces is through topics. Topics may be defined that match the application-specific format for the messages. The *MSM Service Provider* could provide a method for associating a topic to a transformation mapping. When a message is received with a transformation topic, then the *MSM Service Provider* would transform the message to a standard format. When a read request is received with a transformation topic, then the *MSM Service Provider* would transform the standard format into the application-specific topic format.

The *MSM Service Provider* would maintain the relationship between the application-specific topics, the transformation rules to a standard, and a “standard” topic definition.

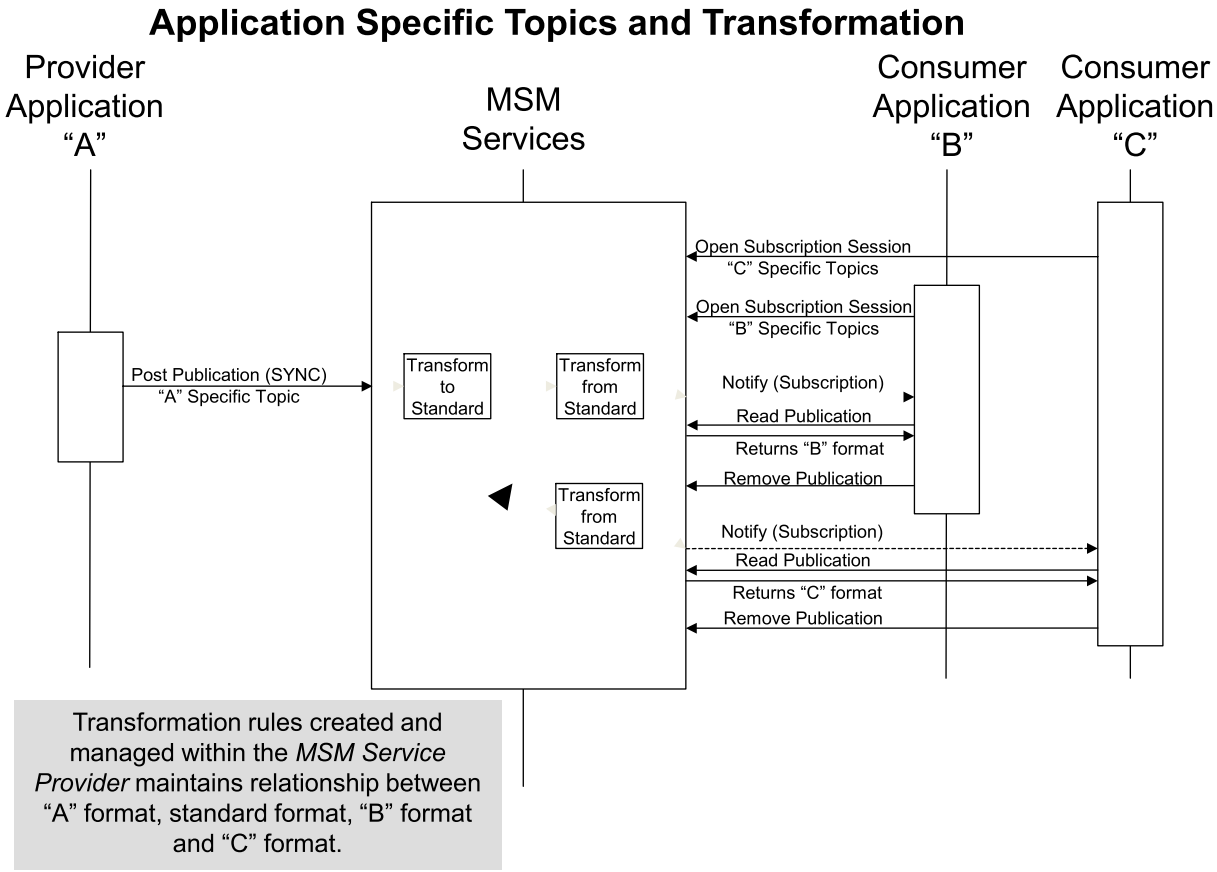

Figure A.1 – Transformation services with the MSM service provider

A.12 Cross company bridges

MSM Service Providers could provide cross company communication and authentication services for messages.

There is no requirement that an *MSM Service Provider* provide cross company services.

A method to provide chain of custody for published messages is shown in Figure A.2.. In this scenario, a proxy application (or part of the MSM) in Company A's environment would listen for publications from the MSM. The proxy would forward the publications using an authenticated or secure method to a proxy application in Company B's environment. The receiving proxy would publish the message in Company B's MSM environment. The bridge may also convert Channel and Topics from Company A's namespace to Company B's namespace.

NOTE The specification of secure or authenticated communication channels is outside the scope of this PAS.

Copyright International Electrotechnical Commission

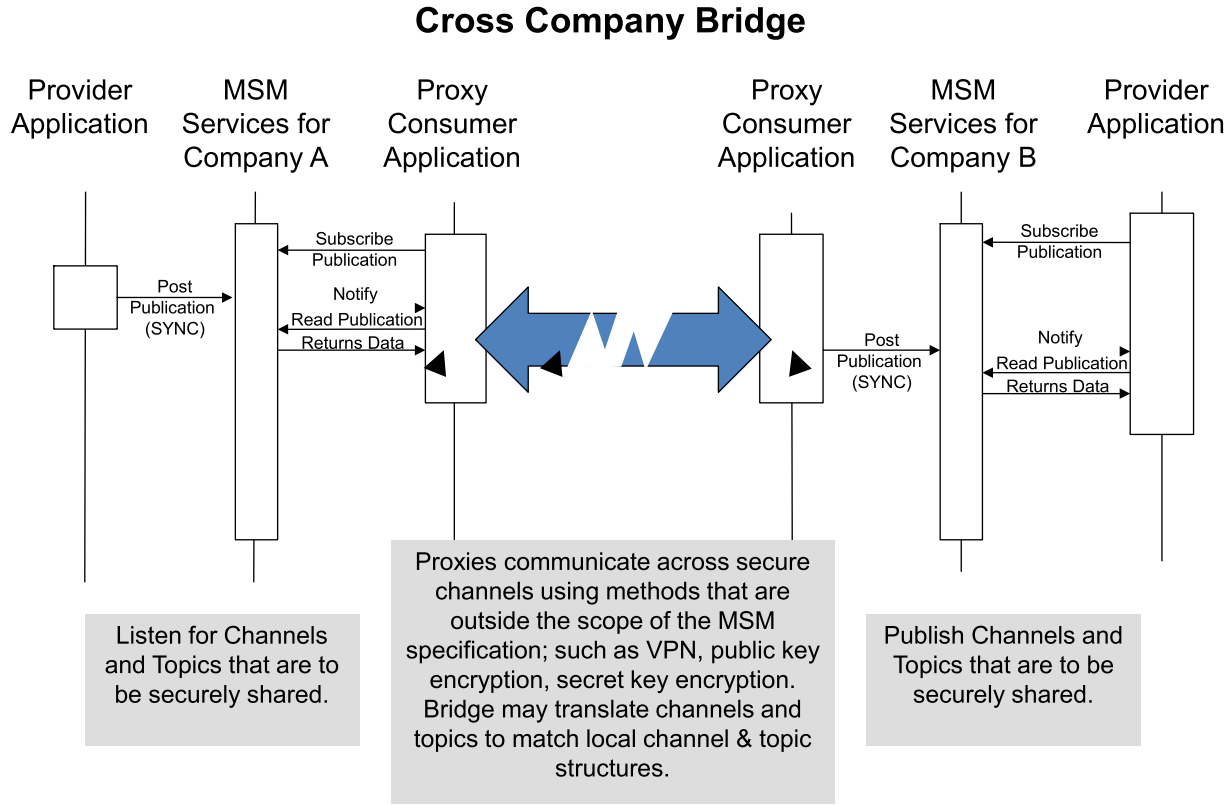

Figure A.2 – Cross company bridge between multiple MSMs

A.13 Message maintenance

MSM Service Providers could provide services for managing messages on channels, such as:

– the ability to delete orphan messages that have not been deleted because of a failure on a request or response transaction,

– the ability to monitor the length of message queues and notify appropriate people if the message queues become too long,

– the ability to monitor the hold time of messages and notify appropriate people if the message delivery delays become too long.

Copyright International Electrotechnical Commission

Annex B
(informative)

Enterprise Service Buses

The typical IT environment is a federation of systems. The term “federation” in the IT world is applied to collections of applications from multiple vendors that work together to support business processes. A federation may include separate applications for material management, order processing, supply chain management, customer relations, and production scheduling. Even when a company has selected a primary ERP (Enterprise Resource Planning) vendor, there is often a federation of legacy systems supporting unique business processes. Federated systems are expensive and integration efforts are often a major portion of IT budgets. An increasingly common method to reduce integration costs is an Enterprise Service Bus (ESB) sometimes called an Enterprise Integration Bus (EIB). These are not electronic buses in the sense of an electrical backplane bus. Instead they are specialized applications that run on redundant servers and act as concentrators and distributors of data. Manufacturing systems that must exchange data with business systems will probably need to connect to the company’s ESB.

Enterprise Service Buses are an architectural concept that includes open standards, message based communications, message routing capabilities, and service discovery mechanisms. There is no single definition of an ESB product, but a working rule is that it is a system that provides:

- a single source of shared information,
- a single location for discovering application services, and
- a single destination for using services.

Several vendors are providing ESB, but a few manufacturing companies have also built their own ESB systems based on open standards and focused on their unique integration problems. Once a company has selected an ESB system, then the IT department will usually attempt to have all applications that exchange data (including manufacturing applications) use the ESB instead of implementing point-to-point connections. Unfortunately, there is little interoperability between different ESB systems, so each application interface must be customized for the chosen ESB.

There are five main elements of ESBs that are important in connecting applications to an ESB:

a) a data transfer element,
b) a service discovery element,
c) a data transform element,
d) a transaction protocol element, and
e) a payload element.

All of the elements are based on XML technologies and newer ESBs are based on web services. The data transfer element handles transporting XML messages from one application to another through the common server. This eliminates point-to-point interfaces and provides a centralized mechanism to manage and view inter-application communication. HTTP (Hypertext Transmission Protocol) messages and JMS (Java Message Services) are common open-source implementations data transfer element layer implementations. OPC-UA (www.opcfoundation.org) may become the standard data transfer mechanism for manufacturing system integration.

The service discovery element allows applications to discover the services and data provided by the ESB. This is typically handled by UDDI services (www.uddi.org) in the IT environment and, for example, is included as part of OPC-UA services. The MSM implementation should define the service discovery mechanism.

Copyright International Electrotechnical Commission

The data transform element provides methods that convert data from the sender's format to the receiver's format through a set of application-specific transform rules. This is often performed using some form of XML transformation, such as XSLT scripts. This could be handled by the *MSM Service Provider*.

The transaction protocol element implements the formal definition of allowable message transactions and is often based on standards such as IEC 62264-5, OAGIS (www.openapplications.org), or RosettaNet (www.rosettanet.org) standards.

The payload element defines the data that makes up the body of the message. In the manufacturing area, the standards bodies which compose the OpenO&M Initiative (ISA, WBF, MIMOSA, and OPC) define the XML information payloads.

The basic MSM concept is to provide a common interface to any ESB or other message exchange system, as illustrated in Figure B.1.

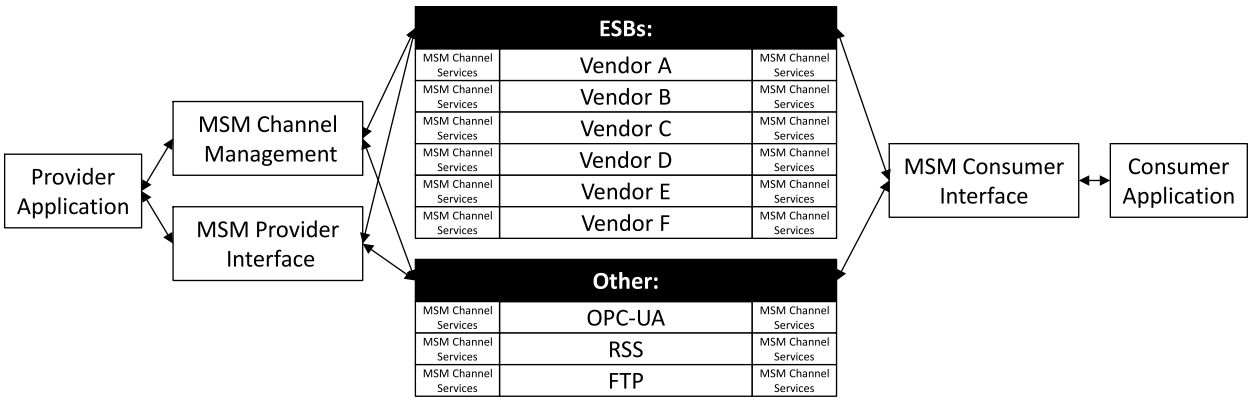

Figure B.1 – Standard interface to ESBs and other message exchange systems

Copyright International Electrotechnical Commission

Bibliography

[1] WBF B2MML Schemas, www.wbf.org, V0400 and later schemas [viewed 2016-06-06]

[2] MIMOSA OSA-EAI Common Conceptual Object Model (CCOM), www.mimosa.org [viewed 2016-06-06]

[3] [X509] X.509 Public Key Certificate Infrastructure, https://www.ietf.org/rfc/rfc2459 [viewed 2016-06-06]

[4] [IS Glossary] Internet Security Glossary, http://www.ietf.org/rfc/rfc2828.txt [viewed 2016-06-06]

[5] [NIST 800-12] Introduction to Computer Security, http://csrc.nist.gov/publications/nistpubs/800-12/

[6] IEC 62541, *OPC Unified Architecture, Parts 1-12*

_____

Copyright International Electrotechnical Commission

Copyright International Electrotechnical Commission

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch

Copyright International Electrotechnical Commission