SIEMENS

MK8000 MP4.20
OPC Server for subsystems

OPC Interface Specifications

Building Technologies

Fire Safety & Security Products

About This Document

Purpose

This manual provides a conceptual overview of how components of SBT and 3rd party subsystems are mapped and represented in the MK8000 OPC Server, as well as a brief explanation of the main software architecture choices available.

Scope

This document applies to the MK8000 OPC Server for subsystems, market package MP4.20. It is intended as an overview to the general principles of the MK8000. Subsystem specific data can be found in the Interface Specifications documents that came with this document.

If you do not have these documents, you can download them from the Siemens Intranet as described in the Document Download section below, or you can request it from your Siemens representative. Please refer to the Reference documents section below to find the exact document title and number.

Target audience

This documentation is intended for the following users:

- Project Engineers
- Commissioning Personnel

This manual was written for software integrators responsible for connecting SCADA and OPC Client applications to subsystems via the MK8000 OPC Server. The reader should be familiar with OPC Specifications and software technologies such as COM/DCOM/OLE. The reader should also be familiar with the subsystems to be integrated.

Documentation Resource Information

This document assembles important information regarding documentation resources. It contains the following:

- Comprehensive definitions of the target audiences for FS DMS documents
- Training program information including the Siemens intranet link
- A complete list of all available DMS8000 documents
- Instructions for how to obtain a document via the Siemens intranet using the STEP Documentation Repository System
- A map of relevant documents for each target audience group
- Customer Support links & resources
- A glossary containing definitions of all terms and acronyms used in DMS8000 documentation

To access the *DMS8000 MP4.20 Documentation Resource Information Guide* (STEP #A6V10089056), go to the link and follow the instructions below:

https://workspace.sbt.siemens.com/content/00001123/default.aspx

1. Click on the **STEP WEB Client** image: 

2. Choose **04 Fire -3F** from the **Product Segment** box and select **Activate filter**.
3. Select **All** in the Documents section of the Quick Search page and select **Advanced Search**.

4. Enter the document number in the **Brochure No.** field (A6V10089056) and press **Enter**.

Operational and safety regulations

Before groups of persons begin work on any DMS system, they must have read and understood the related documents. In particular the Safety Regulations included in the Installation, Configuration, and Commissioning manual (ICC).

Liability disclaimer for damage or injuries

Before products are delivered, they are tested to ensure they function correctly when used properly. Siemens disclaims all liability for damage or injuries caused by the incorrect application of the instructions, or the disregard of danger advisories. This disclaimer applies in particular to personal injuries or damage caused by:

- Improper and/or incorrect use
- Disregard of safety instructions in the documentation or on the product
- Poor maintenance or a lack of maintenance

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual are reviewed regularly and any necessary corrections included in subsequent editions. Suggestions for improvement are welcome.

Modification index

Current version	Date	Notes
A6V10258594	06.2009	Latest update for market package MP4.20 of MK8000 OPC Server Software.
004971_h_en	06.2006	Latest update for market package MP3.20 of MK8000 OPC Server Software
004971_g_en	03.2006	Latest update for market package MP3.18 of MK8000 OPC Server Software
004971_f_en	12.2004	Corresponds to market package MP3.10 of MK8000 OPC Server Software
004971_e_en	02.2004	Corresponds to market package MP1.31 of MK8000 OPC Server Software
004971_d_en	10.2003	Corresponds to market package MP1.30 of MK8000 OPC Server Software
004971_c_en	07.2003	Corresponds to market package MP1.20 of MK8000 OPC Server Software
004971_b_en	03.2003	Corresponds to market package MP1.10 of MK8000 OPC Server Software
004971_a_en	05.2002	Corresponds to release 1.0 of MK8000 OPC Server Software

MK8000 OPC Server

In addition to the documents available through the EDMS documentation system, the OPC Foundation publishes a number of other documents that are necessary and/or useful for understanding the underlying principles used in the MK8000 OPC Server. These PDF documents can be downloaded from www.opcfoundation.org. Select “Latest Downloads” from the Tech Info drop-down menu on the main page of the site.

Name	Date	Comments
OPC Common 1.00	1998-10-27	
OPC DA 2.05 (Data Access Interface Specifications)	2001-12-17	
Using OPC via DCOM with Microsoft Windows XP Service Pack 2	2004	

Abbreviations

OPC	OLE for Process Control
OLE	Object Linking and Embedding
COM/DCOM	Component Object Model / Distributed Component Object Model
SCADA	Supervision Control And Data Acquisition
DMS	Danger Management Systems
BMS	Building Management Systems
N/A	Not-Applicable
Multi-state Item	The OPC Item shown in the MK8000 OPC Server as a status value.
Bit-mask item	The OPC Item shown in the MK8000 OPC Server as a mask of status bits.

1 Introduction

The MK8000 is an OPC server that can represent a number of safety and security objects as OPC items. It can use the Multi-state or Bit-mask representation and both are described in this manual.

Each point (object) is represented by as many as three OPC Items, providing the objects *status*, the list of *available commands*, and the *control commands*, respectively.

The following sections illustrate the possible system architectures, outline the basic concepts of the MK8000 OPC data model, and provide a list of all possible states and masks, as well as a brief description of the control commands.

For subsystem-specific states and commands, see the interface specifications that came with this manual (See Reference Documents in the About This Document section for document names and numbers).

1.1 What has been changed in MP4.20

This release does not include modifications in the general OPC interface specifications. This document has been updated with new references to the updated manuals.

In this edition, a specific correction (pag. 11 and 30) concerned the length of the Instance Number.

2 System architecture

2.1 Stand-alone configuration

In the stand-alone configuration both the OPC Client application and the MK8000 applications reside on the same machine, which is connected to the field network.

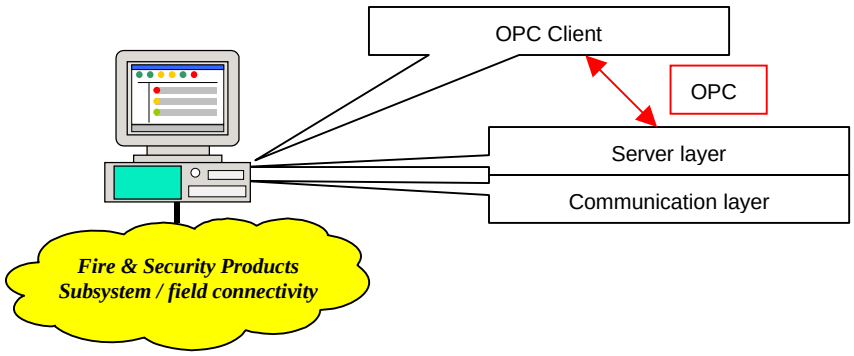


Fig. 1 Stand-alone system architecture

2.2 Client / Server – standard configuration

In the standard Client / Server configuration, the MK8000 resides on the server, which is connected to the field network. Client applications (one or more) can reside on the same and/or on other machines, which are connected to the server via LAN.

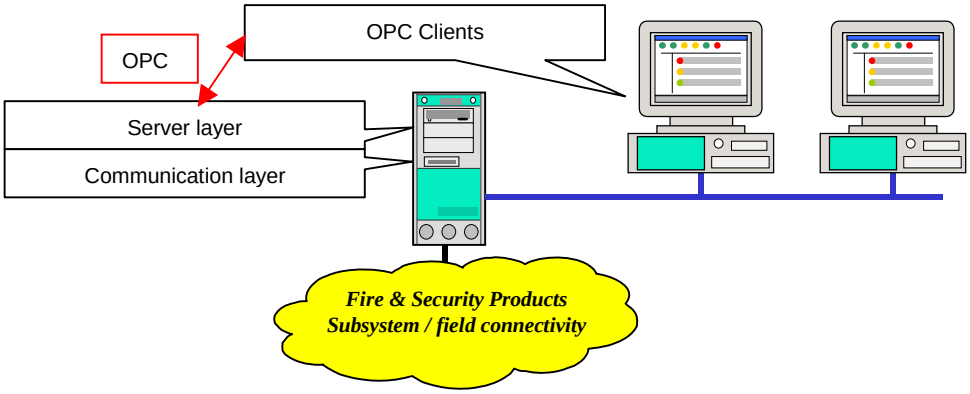


Fig. 2 Client / Server: standard architecture

2.3 Client / Server – distributed configuration

In the distributed Client / Server configuration the MK8000 can be split into two functional entities, the server layer and the communication front-end. These entities are connected via LAN. Client applications (one or more) can reside on the same and/or on other machines, which are connected to the server via LAN.

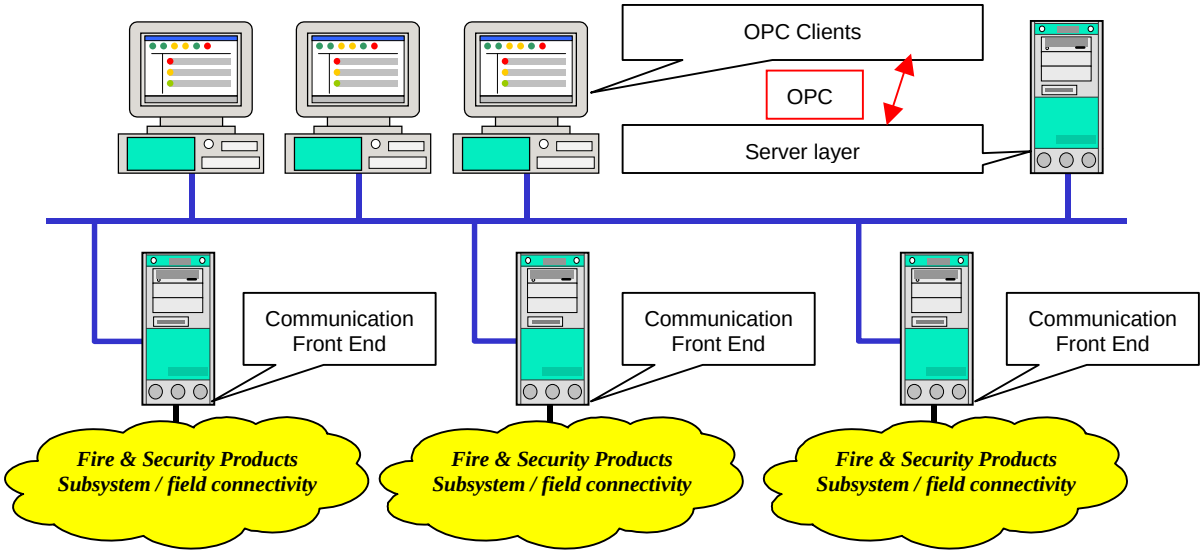


Fig. 3 Client / Server: distributed architecture

3 OPC Implementation

This section describes how the MK8000 OPC Server implements the OPC interfaces and concepts described in the OPC Data Access Server Custom Interface Specification.

3.1 OPC Interfaces

The MK8000 OPC Server is fully compliant with OPC Standard V2.0.

Specifically, it supports all the required COM interfaces described in the OPC Data Access Custom Interface Standard V 2.05 – section 3.1.

In addition, the following **optional interfaces** are supported in MK8000:

OPCServer:
- IOPCServerPublicGroups
- IOPCBrowseServerAddressSpace

OPCGroup:
- IOPCPublicGroupStateMgt

3.2 Address Space

The MK8000 OPC Server is able to manage different subsystems at the same time.

The MK8000 address space is a hierarchical organisation where each subsystem is represented by a Branch (i.e. OPC_BRANCH) positioned just under the root. A string that corresponds to the technical text associated with the subsystem contains those first level branches.

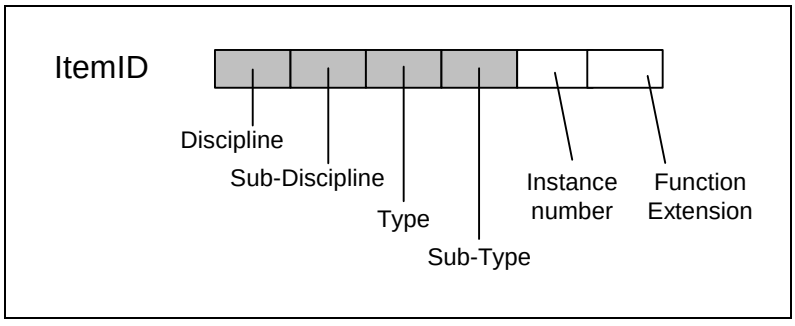
Each first level branch contains an OPC Item (i.e. an OPC_LEAF for the OPC Address Space) named ‘Application’. The ‘Application’ represents the general health of the physical subsystem. Specifically, (as describe later in the section describing the possible states) it shows a state of ‘fault’ when the communication between the MK8000 server and the subsystem is down (if it breaks or is disconnected). This is always the case, regardless of which subsystem is connected. The hierarchy below this level is always specific to each subsystem.

The MK8000 Address Space contains three types of objects:

- Branch
- “Label Branch”
- Item (leaf)

Brief Description of Item ID’s

Every branch and item has an Item ID. The Item ID (Object Name) consists of 8 characters, which indicate the object type, a hexadecimal number, which indicates the object instance and an optional function extension, which identifies one of the three possible OPC items per object (item 1: status, item 2: available command map; item 3: command execution).



The 8 characters of the object typology follow this pattern:

- 2 characters for the Object Discipline (see the ‘Object Discipline Type’ table for the complete list)
- 2 characters for the Object Sub-Discipline (see the ‘Object Discipline Sub Type’ table for the complete list)
- 2 characters for the Object Type (see the ‘Object Type’ table for the complete list)
- 2 characters for the Object Sub-Type (see the ‘Object Sub Type’ table for the complete list)

The instance number can be from 4 to 10 digit long.

The function extension can be (objects are represented by 3 items, see p.12):

- Item 1, reporting the object status: no extension;
- Item 2, containing the available commands: “_AC”;
- Item 3, used for issue control commands: “_CMD”.

Example:
An Item ID = INBUZOGE268153_CMD is decoded as follows:

- **IN**BUZOGE268153_CMD: 2 characters representing the Object Discipline (IN = intrusion).
- IN**BU**ZOGE268153_CMD: 2 characters representing the Object Sub-Discipline (BU = burglary)
- INBU**ZO**GE268153_CMD: 2 characters for the Object Type (ZO = zone).
- INBUZO**GE**268153_CMD: 2 characters for the Object Sub-Type (GE = generic).
- INBUZOGE**268153**_CMD: Object instance Number.
- INBUZOGE268153_**CMD**: Extension indicating the item function (CMD=Control Command)

Refer to section 4.3 on page 29 of this document for a complete list of Object Disciplines, Sub-Disciplines, Types and Sub-Types.

Branch

A branch always contains an Item and may contain other branches. A branch takes the name of the item (object) it contains.

- Note that “Label” Branches do not contain items.

“Label” Branch

A “Label” branch acts as an organisational folder. It can contain other branches, but not items. Therefore, it does not represent any physical point in the subsystem.

Item

An Item represents an object and takes the name of it. There actually are as many as three items per object:

1 Item 1, reporting the object **status** and receiving control commands without feedback. In the ID, this item has no function extension (e.g. INBU-ZOGE268153).

2 Item 2, for providing the map of **available commands**. In the ID, this item has function extension “_AC” (e.g. INBUZOGE268153_AC).

3 Item 3, for receiving **control commands** and reporting command feedbacks. In the ID, this item has function extension “_CMD” (e.g. INBU-ZOGE268153_CMD).

A client application can subscribe to the object by browsing the OPC Address Space.

About Full Item IDs

The ‘Full Item ID’ of an item is made up of the ‘Item ID’ of each of the objects in the hierarchical path (from the root to the specified item). For example, the item shown in Fig. 4, ‘INNOZOGE02’, is identified by the following ‘Full Item ID’:

CS4.LABEL1.INNOSEGE01.INNOZOGE02. INNOZOGE02

The ‘Full Item ID’ is then used for adding items to a group.

It is also possible to use a reduced string consisting of the ‘Item ID’ of the first branch and the ‘Item ID’ of the object you are interested in. For example, in the Address Space shown in Fig. 4, the item ‘INNOZOGE02’ can be identified by the following ‘Reduced Full Item ID’:

CS4. INNOZOGE02

The reduced address mechanism is used when the OPC client does not support long strings for addressing them.

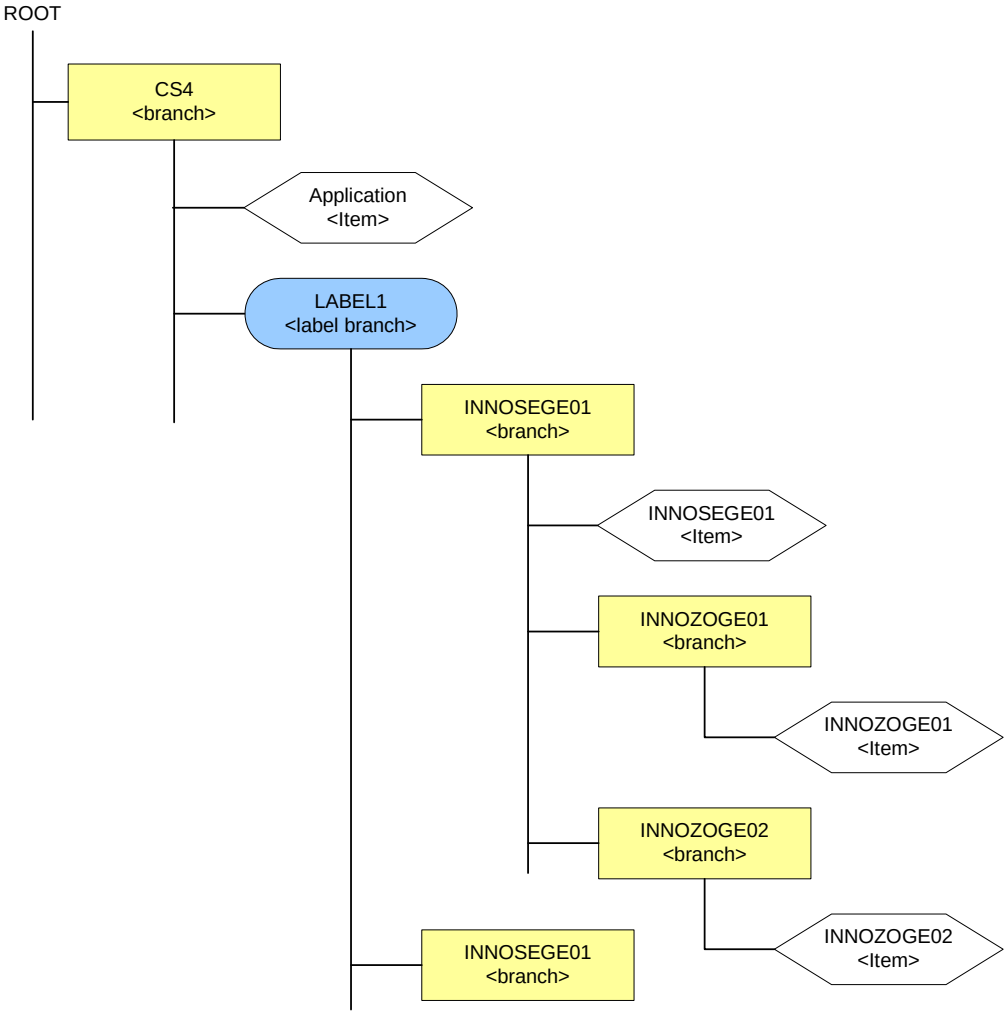


Fig. 4 MK8000 Address Space sample

Note: Clients not supporting long strings can import address space data from an excel compatible table with the following contents:

- Object Description
- Full Item Name
- Technical Text
- Short Item Name (no longer than 50 characters)
- Object Name

3.3 Item formats

3.3.1 Multi-state Items

One of the OPC Item format provided by the MK8000 OPC Server is called a Multi-state Item.

The following table shows the Multi-state Item properties.

OPC Mandatory Properties

ID	Data Type	Description
1	VT_I2	Item value type (it can indicate VT_I2 or VT_I4)
2	VT_I2 or VT_I4	Item value = Multi-state value VT_I2 for threshold mode format (item 1) and for command-related items (items 2 and 3) VT_I4 for bit-mask mode format (item 1).
3	VT_I2	Item quality
4	VT_DATE	Item time stamp
5	VT_I4	Item access rate
6	VT_R4	Server scan rate

OPC Recommended Properties

ID	Data Type	Description
101	VT_BSTR	Item description (corresponds to customer text imported from the subsystem)

OPC Vendor Specific Properties

ID	Data Type	Description
5001	VT_I2	Available commands
5002	VT_BSTR	Technical Text (corresponds to technical text imported from the subsystem)

Tab. 1 Multi-state item properties

The default data type of the Item Value is:

- VT_I2 (2-byte integer number) for threshold mode of item 1 and for items 2 and 3.
- VT_I4 (4-byte integer number) for bit-mask mode.

However, MK8000 is prepared to return data in other requested formats according to the general recommendations of the OPC Specification.

The acceptable values and their meaning are described in section 4.1.

In addition to the mandatory OPC properties, all Items show the recommended property 101 that corresponds to the Customer Text, the vendor-specific property 5001 for the available commands and the vendor specific property 5002 for the technical text. Item 1 can also receive control commands but does not provide direct feedback with the executed command value.

The command-related information is also provided in the additional items 2 and 3 that can be used as alternative to the access of vendor-specific property 5001 (item 2) and for getting a direct feedback with the executed command value (item 3).

Refer to the section 4.2 of this manual for command implementation details.

4 Multi-state model

This section describes the Subsystem model exposed by the MK8000 OPC Server. Section 4.1 describes the set of possible values for the Multi-state item more in detail, and section 4.2 explains the command mechanism.

4.1 States (Item Value)

4.1.1 Simple states

The Multi-state item implemented by the MK8000 OPC Server is a “discrete” item that can assume one state out of a predefined set of states. The values of the items are obtained from a smaller set of “simple states” that are described below.

Simple states list

Quiet

‘Quiet’ is the normal state of the Multi-state item; it indicates both a ‘healthy’ condition of the object (i.e. no fault) and no presence of dangerous situations (i.e. no alarm).

Alarm

An ‘Alarm’ condition is the most significant condition in a subsystem; it normally represents a highly dangerous situation in the controlled area.

Example: In a fire control subsystem, an Alarm can represent the presence of a fire, while in the intrusion environment, it can represent a burglary.

Note: This condition has to be reported to the management station operator.

Pre-alarm

Pre-alarm represents a first-level alarm. It occurs before the Alarm and indicates an abnormal situation that can escalate to an Alarm if other conditions are verified.

Example: In a fire control subsystem, a zone goes into Pre-alarm state if a detector notifies the presence of fire; instead the zone goes into Alarm state if at least two detectors notify the presence of fire.

Tamper

A ‘Tamper’ indicates that somebody is trying to sabotage the object.

Example: a detector link has been cut, or the cabinet of a subsystem has been opened without providing the required operator password at the panel.

Test

The subsystem is in ‘Test’ mode. This means that when a detector triggers an alarm, the subsystem does not generate “real” alarm conditions, but ‘Test-Alarm’ or ‘Test-Active’ conditions (see also section 4.1.2).

Example: the subsystem has been put into Test mode for routine tests on door blocks.

Active

The ‘Active’ state is not very specific. It is used in different situations for objects that have a binary behaviour (see examples).

Example 1: A door lock object can be in ‘Quiet’ state if closed and in ‘Active’ state if opened.

Example 2: In an extinguishing zone, the gas dispenser is active when discharging extinguishing gas and quiet when not.

Example 3: An input object can be active when the device can receive/is receiving an input; otherwise it will be ‘Quiet’.

Armed

The ‘Armed’ state indicates that the object is included in the system and that it is ready to generate alarms if needed (see examples in ‘Disarmed’ description).

Disarmed

The ‘Disarmed’ state indicates that the object is excluded from the system. In this state the object IS NOT ABLE to generate alarms.

An object normally not available in the system (‘Disarmed’) can be ‘Armed’ and it will remain available and ready to send alarms until the next transition (night/day or day/night occurs) or a ‘Disarmed’ command is sent.

An object normally available in the system (‘Armed’) can be disarmed and it will remain in that state until next transition (night/day or day/night occurs) or an armed command is sent.

Example: The ‘Armed’ and ‘Disarmed’ state could represent the situation of night and day condition in an intrusion subsystem.

Note: This concept should not be confused with the ‘Disconnect’ state. If a user wants to *permanently* include/exclude an object a Connect/Disconnect command has to be used.

Anomaly

The object is functioning, but not properly.

Example: A connection line works badly and the server receives partially or infrequently updated information from the field.

Disconnected

The object is not connected; no notification can be received from the object.

Fault

The object does not work anymore.

Example: A device is broken.

Not-Aligned

The OPC Server is not yet aligned to the Control Unit.

Example: Status request process in progress.

4.1.2 Compound states

The simple states described in the previous section can be present concurrently. For example, a system can be in ‘Test’ mode while an ‘Alarm’ occurs.

When more than one simple state is present there are two possibilities:

- One state is considered to be more important than the others and “hides” the other states;
- Two simple “significant states” arise at the same time. The word significant means information of both states needs to be sent to the client application, and that neither of them can be hidden. This situation requires the creation of a compound state.

Example 1: when an ‘Alarm’ and an ‘Anomaly’ condition are present at the same time, it is not necessary to report a compound state of ‘Alarm & Anomaly’, since ‘Alarm’ is much more dangerous/important than ‘Anomaly’. In this case the system reports only ‘Alarm’.

Example 2: when an ‘Alarm’ and a ‘Tamper’ condition are present at the same time, it is significant to report a compound state of ‘Alarm & Tamper’, since both pieces of information are significant. In an intrusion system for example, this could indicate an ongoing burglary and an ongoing sabotage of the panel. The compound state gives different/additional information than ‘Alarm’ or ‘Tamper’ state alone.

Therefore the table of Multi-state item values is enhanced with the compound states.

4.1.3 Latched States

In order to obtain the complete list of possible states, latched states need to be included. A latched state requires operator intervention, while a non-latched state can be described as a simple binary transition. Latched states are always passed through in critical situations as ‘Alarm’, ‘Pre-alarm’, ‘Tamper’ or ‘Fault’.

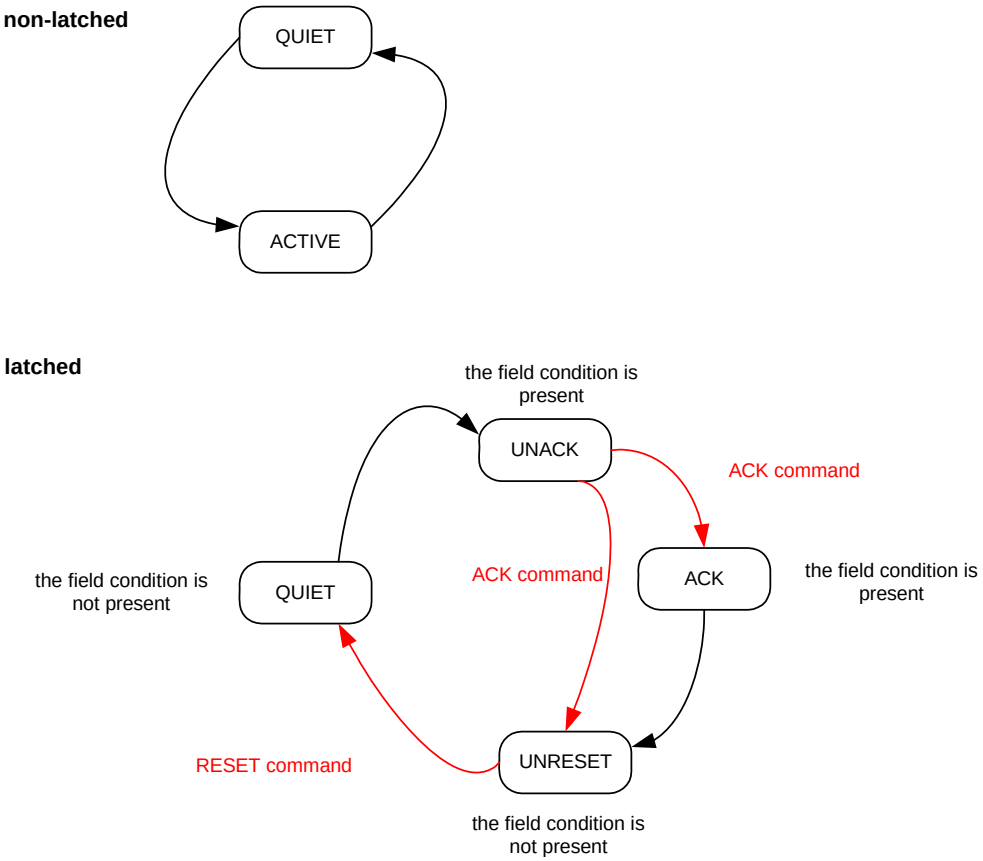


Fig. 5 Latched and non-latched conditions

Unacknowledged condition

When a critical condition is present in the controlled area, the related object goes into ‘Unacknowledged’ state and remains in this state until the operator issues an ‘Acknowledge’ command. A subsystem in an ‘Unacknowledged’ state normally calls the attention of the operator via audible and/or visual means. The management station needs to report this condition to the operator. The ‘Acknowledge’ command can move the state of the object into the ‘Acknowledged’ or the ‘UnReset’ state as described below.

Acknowledged condition

The cause of the critical situation is still present in the system but the operator has acknowledged it, and the critical situation is being handled. The audible/visible indicator of the subsystem normally stops.

UnReset condition

The cause of the critical situation is no longer present in the system. An additional operator command (‘Reset’) is required to force the state of the object back to its default value.

Note: The ‘UnReset’ condition is not applicable to the ‘Fault’ situation. Here usually the object needs just an ‘Acknowledged’ from the operator. Most probably the device is not working anymore so it will be not able to come back to the default state.

4.1.4 Item value: data mode formats

There are two possible data mode formats, based on a **threshold** or on a **bit-mask** concept. The selection of which mode to use is made in the Composer configuration, as described in the document 004972, MK8000 Installation, Configuration & Commissioning.

4.1.5 Threshold concept

Since many SCADA applications have been developed targeting to analogue values that are typical for the automation and process control world, the set of possible states can be organized using a “threshold concept”.

An analogue item is usually controlled by defining a number of thresholds. When the value of the analogue items goes above or below those thresholds, the system reacts in some way. Usually there are either two (High Limit, Low Limit) or four (High-High Limit, High Limit, Low Limit, Low-Low Limit) threshold levels.

In the threshold mode, the Multi-state item is in its “normal state” when its value assumes the ‘Quiet’ state. The ‘Quiet’ state has been set to the middle of the possible values. A value smaller than the ‘Quiet’ state value (in the direction of the Low Limit) indicates that the data point is in the ‘Alarm’ state. A value greater than the ‘Quiet’ state value (in the direction of the High Limit) indicates that the data point is in the ‘Fault’ state.

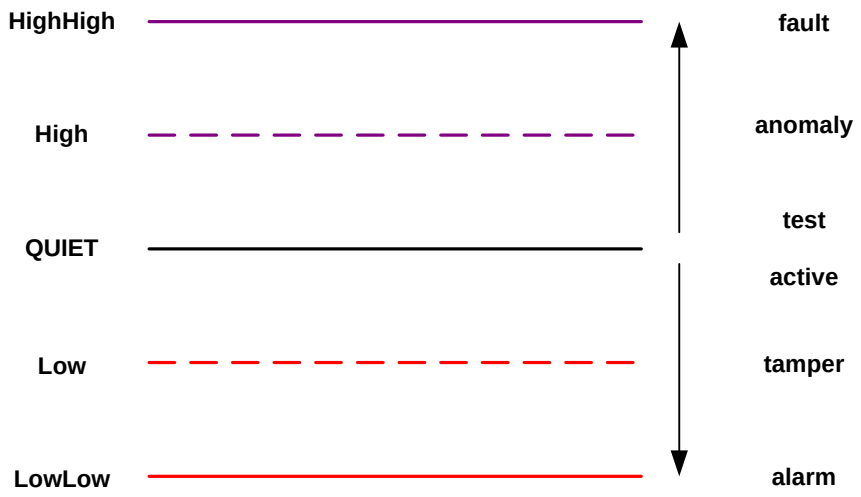


Fig. 6 Illustration of the threshold concept

Threshold state value:

The compound-states and the latched conditions are added to the simple states, and the complete list of the possible states of the Multi-state item is obtained.

Threshold indication	Value	Name	Note
	400	Alarm & Tamper Unack	Full level Alarm and Tamper situations are concurrently present in the controlled area. Visible/audible indicators of the Subsystem have been activated. This condition has to be reported to the operator immediately. In some subsystems, if an Alarm or a Tamper situation is not handled within in a specific period of time, the subsystem can trigger actions (i.e. calling the police or fire brigades).
	401	Alarm & Tamper Ack	Full level Alarm and Tamper situations are concurrently present in the controlled area. The operator is handling the situation. Visible/audible indicators of the subsystem have been stopped.
	402	Alarm & Tamper UnReset	The causes of the full level Alarm and Tamper situations are no longer present in the controlled area. The operator is required to send a Reset command in order to force the object into its default state.
	500	Alarm Unack	Full level Alarm situation is present in the controlled area. Visible/audible indicators of the subsystem have been activated. This condition has to be reported to the operator immediately. In some subsystems, if an Alarm or a Tamper situation is not handled within in a specific period of time, the subsystem can trigger actions (i.e. calling the police or fire brigades).

Threshold indication	Value	Name	Note
	501	Alarm Ack	Full level Alarm condition is present in the controlled area. The operator is handling the situation. Visible/audible indicators of the subsystem have been stopped.
	502	Alarm UnReset	The cause for generating a full level Alarm situation is no longer present in the controlled area. The operator is required to send a Reset command in order to force the object into its default state.
	510	Alarm & Fault Unack	Full level Alarm and Fault situations are concurrently present in the controlled area. Visible/audible indicators of the subsystem have been activated. This condition has to be reported to the operator immediately. In some subsystems, if an Alarm or a Tamper situation is not handled within in a specific period of time, the subsystem can trigger actions (i.e. calling the police or fire brigades).
	511	Alarm & Fault Ack	Full level Alarm and Fault situations are concurrently present in the controlled area. The operator is handling the situation. Visible/audible indicators of the subsystem have been stopped.
	512	Alarm & Fault UnReset	The causes for generating full level Alarm and Fault situations are no longer present in the controlled area. The operator is required to send a Reset command in order to force the object into its default state.
Alarm threshold			
	800	Prealarm Unack	The object is in a first level Alarm state. This condition has to be reported to the operator immediately.
	801	Prealarm Ack	The object is in a first level Alarm state. The operator is handling the situation.

Threshold indication	Value	Name	Note
	802	Prealarm UnReset	The cause for generating a first level Alarm situation is no longer present in the controlled area. The operator is required to send a Reset command in order to force the object into its default state.
	810	Prealarm & Fault Unack	First level Alarm and Fault situations are concurrently present in the controlled area. This condition has to be reported to the operator immediately.
	811	Prealarm & Fault Ack	First level Alarm and Fault situations are concurrently present in the controlled area. The operator is handling the situation.
	812	Prealarm & Fault UnReset	The cause for generating a first level Alarm situation and Fault are no longer present in the controlled area. The operator is required to send a Reset command in order to force the object into its default state.
Pre-alarm threshold	900	Tamper Unack	Sabotage is underway; the object has been tampered. This condition has to be reported to the operator immediately.
	901	Tamper Ack	Sabotage is underway; the object has been tampered. The operator is handling the situation.
	902	Tamper UnReset	The cause for generating a Tamper situation and Fault are no longer present in the controlled area. The operator is required to send a Reset command in order to force the object into its default state.
	910	Tamper & Fault Unack	Tamper and Fault situations are concurrently present in the controlled area. This condition has to be reported to the operator immediately.

Multi-state model

Threshold indication	Value	Name	Note
	911	Tamper & Fault Ack	Tamper and Fault situations are concurrently present in the controlled area. The operator is handling the situation.
	912	Tamper & Fault UnReset	The causes for generating a Tamper and Fault are no longer present in the controlled area. The operator is required to send a Reset command in order to force the object into its default state.
Tamper threshold			
	946	Active Unack	The object is in its active state. The operator is required to send an acknowledge command.
	947	Active Ack	The object is in its active state. Acknowledge command received.
	948	Active UnReset	The object is in its active state. The operator is required to send a Reset command in order to force the object into its default state.
	950	Active	The object is in its active state.
Active threshold			
	1000	Quiet	This is the default/normal state.
Test threshold	1100	Test	The Object has been put into Test mode.
	1104	Test UnReset	The Object has been put into Test mode. The operator is required to send a Reset command in order to force the object into its default state.
	1105	Test Ack	The Object has been put into Test mode. Acknowledge command received.
	1106	Test Unack	The Object has been put into Test mode. The operator is required to send an acknowledge command.
	1110	Test-Alarm UnReset	Testing of Alarm, waiting for a reset.
	1111	Test-Alarm Ack	Testing of Alarm, acknowledge command received.

Threshold indication	Value	Name	Note
	1112	Test-Alarm Unack	Testing of Alarm, need an acknowledge command.
	1140	Test-Active	Testing of Active state.
	1144	Test-Active UnReset	Testing of Active state, need an acknowledge command.
	1145	Test-Active Ack	Testing of Active state, acknowledge command received.
	1146	Test-Active Unack	Testing of Active state, waiting for a reset.
	1200	Armed	The object is included in the controlled area and ready to generate an alarm (for example).
Anomaly threshold	1300	Disarmed	The object is excluded from the controlled area and it is no longer able to generate alarms.
	1304	Disarmed UnReset	The object is excluded from the controlled area and it is no longer able to generate alarms. The operator is required to send a Reset command in order to force the object into its default state.
	1305	Disarmed Ack	The object is excluded from the controlled area and it is no longer able to generate alarms. Acknowledge command received.
	1306	Disarmed Unack	The object is excluded from the controlled area and it is no longer able to generate alarms. The operator is required to send an acknowledge command.
	1316	Manual	The object is in manual mode.
	1318	Manual UnReset	The object is in manual mode. The operator is required to send a Reset command in order to force the object into its default state.
	1319	Manual Ack	The object is in manual mode. Acknowledge command received.
	1320	Manual Unack	The object is in manual mode. The operator is required to send an acknowledge command. .

Threshold indication	Value	Name	Note
	1326	Blocked	The object is in Blocked.
	1328	Blocked UnReset	The object is in Blocked.. The operator is required to send a Reset command in order to force the object into its default state.
	1329	Blocked Ack	The object is in Blocked. Acknowledge command received.
	1330	Blocked Unack	The object is in Blocked. The operator is required to send an acknowledge command.
	1350	Anomaly UnReset	The object is working properly. The operator is required to send a Reset command in order to force the object into its default state.
	1351	Anomaly Ack	The object is in an anomaly condition meaning it is not working properly. Acknowledge command received.
	1352	Anomaly Unack	The object is in an anomaly condition meaning it is not working properly. The operator is required to send an acknowledge command.
	1369	Not Aligned	The OPC Server is not aligned to the control unit.
	1370	Alignment in progress	The OPC server is waiting the aligned answer from the control unit.
	1400	Disconnected	The object is disconnected from the controlled area.
	1500	Disconnected UnReset	The object is disconnected from the controlled area. The operator is required to send a Reset command in order to force the object into its default state.
	1501	Disconnected Ack	The object is disconnected from the controlled area. Acknowledge command received.

Threshold indication	Value	Name	Note
	1502	Disconnected Unack	The object is disconnected from the controlled area. The operator is required to send an acknowledge command.
Fault threshold	1998	Fault UnReset	The object is out of order. The operator is required to send a Reset command in order to force the object into its default state.
	1999	Fault Ack	The object is out of order. Acknowledge command received.
	2000	Fault Unack	The object is out of order. The operator is required to send an acknowledge command.
	2051	Vitality Fault	The control unit transmits a presence telegram every x seconds and these telegrams are supervised by the OPC-server. A Vitality Fault indicates that communication to the control unit has been lost.

Tab. 2 Multi-state Item: threshold state enumeration

4.1.6 Bit-mask concept

As alternative to the threshold mode, MK8000 can provide the object states as a 32-bit map representing the simple states, namely:

- Byte 1: Event condition in relation to acknowledgement and reset actions.
- Byte 2. Anomaly states.
- Byte 3: Fault states.
- Byte 4: Alarm states.

1st Byte LSB	Condition	0	Unreset
		1	Ack
		2	Unack
		3	
		4	
		5	
		6	
		7	
2nd Byte	Anomaly	8	
		9	
		10	Test
		11	Armed
		12	Disarmed
		13	Manual
		14	Blocked
		15	Anomaly
3rd Byte	Fault	16	
		17	
		18	
		19	
		20	Not Aligned
		21	Disconnected
		22	Fault
		23	Vitality Fault
4th Byte	Alarm	24	
		25	
		26	
		27	
		28	Active
		29	Tamper
		30	Pre-alarm
		31	Alarm

Tab. 3 Bit-mask structure

Referring to Tab. 2, Multi-state Item: threshold state enumeration, the table below illustrates the corresponding bit-mask value:

Threshold value	Description	Bit-mask value (hex)
400	Alarm & Tamper UnAck	A0 00 00 04
401	Alarm & Tamper Ack	A0 00 00 02
402	Alarm & Tamper UnReset	A0 00 00 01
500	Alarm UnAck	80 00 00 04
501	Alarm Ack	80 00 00 02

Threshold value	Description	Bit-mask value (hex)
502	Alarm UnReset	80 00 00 01
510	Alarm & Fault UnAck	80 40 00 04
511	Alarm & Fault Ack	80 40 00 02
512	Alarm & Fault UnReset	80 40 00 01
800	PreAlarm UnAck	40 00 00 04
801	PreAlarm Ack	40 00 00 02
802	PreAlarm UnReset	40 00 00 01
810	PreAlarm & Fault UnAck	40 40 00 04
811	PreAlarm & Fault Ack	40 40 00 02
812	PreAlarm & Fault UnReset	40 40 00 01
900	Tamper UnAck	20 00 00 04
901	Tamper Ack	20 00 00 02
902	Tamper UnReset	20 00 00 01
910	Tamper & Fault UnAck	20 40 00 04
911	Tamper & Fault Ack	20 40 00 02
912	Tamper & Fault UnReset	20 40 00 01
946	Active UnAck	10 00 00 04
947	Active Ack	10 00 00 02
948	Active UnReset	10 00 00 01
950	Active	10 00 00 00
1000	Quiet	00 00 00 00
1100	Test	00 00 04 00
1104	Test UnReset	00 00 04 01
1105	Test Ack	00 00 04 02
1106	Test UnAck	00 00 04 04
1110	Test-Alarm UnReset	80 00 04 01
1111	Test-Alarm Ack	80 00 04 02
1112	Test-Alarm UnAck	80 00 04 04
1140	Test Active	10 00 04 00
1144	Test Active UnReset	10 00 04 01
1145	Test Active Ack	10 00 04 02
1146	Test Active UnAck	10 00 04 04
1200	Armed	00 00 08 00
1300	Disarmed	00 00 10 00
1304	Disarm UnReset	00 00 10 01
1305	Disarm Ack	00 00 10 02
1306	Disarm UnAck	00 00 10 04
1316	Manual	00 00 20 00
1318	Manual UnReset	00 00 20 01
1319	Manual Ack	00 00 20 02
1320	Manual UnAck	00 00 20 04
1326	Blocked	00 00 40 00
1328	Blocked UnReset	00 00 40 01
1329	Blocked Ack	00 00 40 02
1330	Blocked UnAck	00 00 40 04
1350	Anomaly UnReset	00 00 80 01
1351	Anomaly Ack	00 00 80 02
1352	Anomaly UnAck	00 00 80 04
1369	Not Aligned	00 10 00 00
1370	Alignment in progress	00 10 00 04
1400	Disconnected	00 20 00 00

Threshold value	Description	Bit-mask value (hex)
1500	Disconnected UnReset	00 20 00 01
1501	Disconnected Ack	00 20 00 02
1502	Disconnected UnAck	00 20 00 04
1998	Fault UnReset	00 40 00 01
1999	Fault Ack	00 40 00 02
2000	Fault UnAck	00 40 00 04
2051	Vitality Fault	00 80 00 00

Tab. 4 Multi-state Item: bit-mask values

4.2 Commands

This section describes all possible commands that can be issued to a Multi-state item.

4.2.1 Command mechanism

The commands are sent by writing a value to the Multi-state Item using either the synchronous (IOPCSync:Write) or the asynchronous (IOPCASyncIO2) OPC I/O interface.

Async vs. Sync

Both interfaces are supported but the client application should always use the asynchronous interface for sending commands to the device in the field. This is mainly for performance reasons since the synchronous method blocks the client application call until the command result is received from the device, which can occasionally take quite some time depending on the field network and/or subsystem.

Executing commands

Referring to the 3-item structure described in 3.2 above, commands can be sent to item 1 (for compatibility with former versions) or item 3 (dedicated item for receiving commands). As consequence of the command execution, Item 1 will report the modification to the object state. Commands directed to Item 3 will also cause a direct command feedback, as that item will assume the value of the latest command received.

Which commands are applicable?

There is no predefined rule for knowing which commands are applicable in a specific situation. This depends on the type of subsystem, the object, and its current state.

This is true even for the ‘Acknowledge’ command (normally applicable when the object is in the ‘Unacknowledged’ state) and for the ‘Reset’ command (normally applicable when the object is in the ‘UnReset’ state).

Command map

Referring to the 3-item structure described in 3.2 above, the map of available commands is shown both by a vendor-specific property (ID = 5001) on any item, and more specifically, by the value of Item 2.

4.2.2 Multi-state command enumeration

In the following table the **Value** column contains the value that has to be written to the Multi-state Item in order to send the corresponding command to the subsystem.

The **Bit** column indicates the corresponding bit (starting from the less significant bit) of the 2 Byte map found in the vendor specific property (ID = 5001) of all items or in the value of Item 2.

Note: It is possible to have more than one applicable command concurrently.

The following table shows all the possible commands applicable to the Multi-state item.

Command	Value	Bit	Note
Ack	1	1	Acknowledge the current state; normally applicable when the object is in the Unack state.
Reset	2	2	Tries to set the object back in its default state; it is applicable when the object is in the UnReset state.
Arm	4	3	Arm/include the object in the controlled area.
Disarm	8	4	Disarm/exclude the object from the controlled area.
Test	16	5	Set the object in Test mode; it is applicable only in quiet state.
Active	32	6	Set the object in active state from quiet.
Quiet	64	7	Set the object in quiet state from active.
Disconnect	128	8	Disconnects permanently, applicable to disconnect able objects.
Connect	256	9	Connects permanently, applicable to disconnected objects.
Block	512	10	Set the object in blocked state from quiet.
Manual	1024	11	Set the object in manual state from quiet.
Status Request	2048	12	Forces the alignment of the OPC Server to the Control unit. This is usually done automatically but can also be forced by issuing this command.

Tab. 5 Multi-state Item command Map

Example 1:

Map = 1 $(00\ 01)_{16}$: the ‘Acknowledge’ command is applicable

Example 2:

Map = 32 $(00\ 20)_{16}$: the ‘Active’ command is applicable.

Example 3:

Map = 176 $(00\ B0)_{16}$: ‘Test’, ‘Active’, and ‘Disconnect’ commands are applicable.

4.3 Watch-dog item

MK8000 OPC server supports an item named:

"SYSTEM_DIAGNOSTIC.Watchdog".

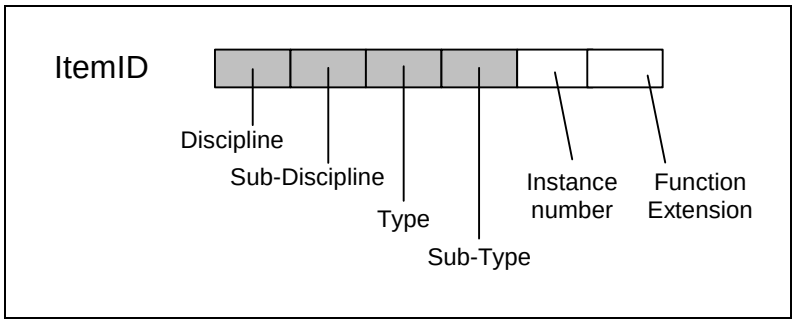
The item toggles every 30 sec. from Quiet to Active and vice versa. **Clients MUST subscribe to this item and use it to detect the communication faults**.

The OPC server will also be able to detect any fault and provide for disconnecting and zeroing the license counters.

5 Appendix

5.1 Item ID

The Item ID (Object Name) consists of 8 characters, which indicate the object type, a hexadecimal number, which indicates the object instance and an optional function extension, which identifies one of the three possible OPC items per object (item 1: status, item 2: available command map; item 3: command execution).



The 8 characters of the object typology follow this pattern:

- 2 characters for the Object Discipline (see the 'Object Discipline Type' table for the complete list)
- 2 characters for the Object Sub-Discipline (see the 'Object Discipline Sub Type' table for the complete list)
- 2 characters for the Object Type (see the 'Object Type' table for the complete list)
- 2 characters for the Object Sub-Type (see the 'Object Sub Type' table for the complete list)

The instance number can be from 4 to 10 digit long.

The function extension can be:

- Item 1, reporting the object status: no extension;
- Item 2, containing the available commands: "_AC";
- Item 3, used for issue control commands: "_CMD".

5.1.1 Object Discipline Type

Abb.	Extended name
AC	AccessControl
BS	buildingServices
FI	Fire
GS	Gas
HW	Hardware
IN	Intrusion
IO	InputOutput
MG	Management
SY	systemServices
UD	Undefined

5.1.2 Object Discipline Sub Type

Abb.	Extended name
BU	Burglary
CM	Communication
CO	Control
DC	DisCo
DE	Detection
DU	Duress
EX	Extinguishing
HO	Holdup
LN	Lon
NO	None
PA	Panic
TA	Tamper
TH	Theft
UD	Undefined
VD	Vds

5.1.3 Object Type

Abb.	Extended name
AD	alarmingDevice
AL	activationLine
AP	application
AR	Area
BD	BACnetDevice
CA	cabinetProtection
CC	controlPanel
CK	Gateway
CL	Clock
CP	callpoint
CR	cardReader
CS	commandSequence
CT	Terminal
DC	detectionController
DE	detector
DI	DigitalInput
DO	DigitalOutput
DR	Door
DS	display
EC	externController
EP	Expander
EX	Extinguishant
HC	hornController
HO	Horn
IB	IoBoard
IC	IoController
IN	Input
IO	IoDevice
KB	Keyboard
LI	Link
LL	LockLine

Abb.	Extended name
MS	managementStation
MO	monitoringStation
MX	Matrix
NC	notificationClass
NO	Node
NW	Network
OB	Output board
OL	ObjectList
OR	organization
OU	Output
PA	Panel access
PD	peripheralDevice
PG	program
PR	Printer
PS	powerSupply
RC	rtController
RD	rtDevice
RH	rtChannel
SB	strobelight
SE	section
SI	standbyInterface
SL	stopLine
SR	service
TC	tamperControl
TP	timeProgram
UD	undefined
UG	userGroup
US	User
VA	Valve
VC	videoCamera
VE	Verification module
VR	VideoRecorder
ZO	zone

5.1.4 Object Sub Type

Abb.	Extended name
AB	audible
AD	addressable
AL	Alarm
AM	antimask
AU	automatic
AX	auxiliary
BA	balanced
BI	Binary
CL	Client
CO	collective
DM	doorMonitor
EE	Emergency exit
EL	element
ET	external
FE	Fep

Abb.	Extended name
FL	Fault
FS	flowSwitch
GE	Generic
IT	internal
KC	keyCabinet
LC	Local
LM	lockMonitor
LO	Logical
MA	manual
MI	mirror
MN	Main
MU	Multi
OT	Other
PB	PUBLIC
PR	PRIVATE
PG	programmable
PH	Physical
PI	Pilot
PM	pmi
RE	Remote
RO	Root
SE	Server
SI	Single
SL	silence
SP	sprinkler
ST	standalone
SU	summary
SV	supervised
24	24 hours
UD	undefined

Siemens Switzerland Ltd
Building Technologies Group
International Headquarters
Fire Safety & Security Products
Gubelstrasse 22
CH-6301 Zug
Tel +41 41 724 24 24
Fax +41 41 724 35 22
www.sbt.siemens.com