ISO/IEC 18598

Edition 1.0 2016-09

INTERNATIONAL STANDARD

**Information technology –
Automated infrastructure management (AIM) systems – Requirements, data exchange and applications**

ISO/IEC 18598:2016-09(en)

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 It also gives information on projects, replaced and withdrawn publications.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.

ISO/IEC 18598

Edition 1.0 2016-09

INTERNATIONAL STANDARD

Information technology – Automated infrastructure management (AIM) systems – Requirements, data exchange and applications

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 35.200

ISBN 978-2-8322-3665-9

CONTENTS

INFORMATION TECHNOLOGY –

Automated infrastructure management (AIM) systems – Requirements, data exchange and applications

FOREWORD

1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

2) The formal decisions or agreements of IEC and ISO 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 and ISO member bodies.

3) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC National Committees and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO 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 and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO, IEC or ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.

5) ISO and IEC do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. ISO or IEC are 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 ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC National Committees or ISO member bodies 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 of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/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 ISO/IEC publication may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 18598 was prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

This International Standard has been approved by vote of the member bodies, and the voting results may be obtained from the address given on the second title page.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

INTRODUCTION

This International Standard is intended for

- premises owners and facility managers,
- suppliers of AIM solutions,
- planners of network infrastructures,
- network operation managers,
- data centre operation managers,
- IT process managers,
- suppliers of management system software,
- software integrators.

This International Standard is one of a number of documents prepared in support of International Standards and Technical Reports produced by ISO/IEC JTC 1/SC 25.

INFORMATION TECHNOLOGY –

Automated infrastructure management (AIM) systems – Requirements, data exchange and applications

1 Scope

This International Standard specifies the requirements and recommendations for the attributes of automated infrastructure management (AIM) systems.

This International Standard explains how AIM systems can contribute to operational efficiency and deliver benefits to

a) cabling infrastructure and connected device administration,

b) facilities and IT management processes and systems,

c) other networked management processes and systems (e.g. intelligent building systems),

d) business information systems covering asset tracking and asset management together with event notifications and alerts that assist with physical network security.

This International Standard specifies a framework of requirements and recommendations for data exchange with other systems

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

There are no normative references in this document.

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

3.1.1
AIM-enabled port
port which is able to automatically detect the insertion and removal of a cord and process that event as part of an automated infrastructure management system

3.1.2
AIM hardware
combination of patch panels and controllers that are designed to automatically detect the insertion or removal of cords, to record connectivity information, and to exchange connectivity information with AIM software

3.1.3
AIM system
integrated hardware and software system that automatically detects the insertion or removal of cords, documents the cabling infrastructure including connected equipment enabling management of the infrastructure and data exchange with other systems

3.1.4
alarm
event of sufficient importance to be highlighted within the AIM system

3.1.5
application programming interface
API
set of commands, functions and protocols that specify how software components should interact

3.1.6
basic connectivity configuration
list of information including, but not restricted to, number and type of ports, number of slots, expansion cards, MAC and IP address

3.1.7
business information system
system that is used to analyse and facilitate strategic and operational activities for an organization

3.1.8
building management system
BMS
computer-based control system installed in a building that controls and monitors mechanical and electrical equipment such as heating, ventilation and air-conditioning (HVAC), power systems and access control systems

3.1.9
cabling connectivity information
combination of connection information automatically detected by AIM and additional cabling infrastructure information from various sources

3.1.10
cabling infrastructure
cables, connecting hardware, panels and other closures, cabinets, frames, racks together with pathways and spaces providing their accommodation

3.1.11
circuit
series of electromagnetically connected components or devices

3.1.12
closure
fixture or fitting of either open or closed construction intended to contain connecting hardware

[SOURCE: ISO/IEC 14763-2:2012, 3.1.11]

3.1.13
command
defined method which either provides data or performs an internal operation within an AIM system based on a request

Note 1 to entry: A command may contain zero or more parameters.

3.1.14
configuration management database
repository of information related to all the components of an information system

3.1.15
connecting hardware
device or combination of devices used to connect cables or cable elements

[SOURCE: ISO/IEC 11801:2002, 3.1.17, modified]

3.1.16
connection information
record of an event generated by the insertion or removal of a connector at an AIM-enabled port

3.1.17
cord
cable, cable unit or cable element with a minimum of one termination

[SOURCE: ISO/IEC 11801:2002, 3.1.20]

3.1.18
data
value or set of values that describes information within an AIM system

3.1.19
data exchange
ability of an AIM system and other systems to work together reliably

3.1.20
discoverable equipment
equipment with a network address

Note 1 to entry: Discoverable equipment could be treated as non-discoverable equipment according to end user choice.

3.1.21
end device
equipment that is either the source or the destination of a message on a networked system

3.1.22
event
change in state of an element within the AIM system

3.1.23
information security management system
part of the overall management system, based on a business risk approach, that establishes, implements, operates, monitors, reviews, maintains and improves information security

Note 1 to entry: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

3.1.24
interoperability
ability for two or more independent systems to exchange data or information

3.1.25
managed network distribution equipment
discoverable network distribution equipment that uses communications protocols such as the simple network management protocol (SNMP) to exchange management information

3.1.26
network distribution equipment
electronic equipment that provides connectivity and supports data exchange between end devices

3.1.27
non-discoverable equipment
equipment without a network address

3.1.28
patch panel
closure designed to be mounted in a cabinet, frame or rack

3.1.29
permissions
set of rules which describe what a user or group of users may access or control within an AIM system

3.1.30
telecommunications infrastructure
cabling infrastructure together with the network distribution equipment, end devices and their accommodation

3.1.31
work order
set of one or more actions that should be performed by a technician or user of the system

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply.

AIM automated infrastructure management
API application programming interface
BMS building management system
CMDB configuration management database
DCIM data centre infrastructure management
HVAC heating, ventilation and air-conditioning
HTTP hypertext transfer protocol
IP internet protocol
IT information technology
ITIL Information Technology Infrastructure Library
JSON JavaScript object notation
MAC media access control
PC personal computer
PoE power over Ethernet
REST representational state transfer
SNMP simple network management protocol
SOAP simple object access protocol

WAP wireless access point

XML extensible markup language

4 Conformance

For an AIM system to conform to this International Standard, it shall

a) comprise hardware and software components which together meet the requirements of Clause 5,

b) meet the requirements of Clause 7,

c) be implemented in accordance with the requirements of Annex C.

5 Automated infrastructure management (AIM) systems

5.1 Functional elements

An AIM system shall include the following two functional elements:

a) hardware that automatically detects the insertion and removal of cords;

b) software that

- collects and stores the resulting connection information,
- relates the connection information to cabling connectivity information,
- relates the cabling connectivity information to information from other sources,
- makes the connection information accessible to either an authorized user or to other systems.

It is important to note that although the initial detection of connectivity is generally accomplished through electrical, electronic, electro-mechanical or optical means, the different functions and features using this data are implemented in software.

The software used for AIM systems shall include either application programming interfaces (APIs) or data exchange formats as described in Clause 7 to allow data from the AIM system to be shared with other systems used by the organization. This is an important aspect for enhancing and automating the management and operational functions in the building and data centres.

5.2 System requirements

An AIM system shall be able to

a) automatically detect connectivity between AIM-enabled panel ports,

b) automatically detect connectivity between AIM-enabled panel ports and other equipment (with AIM-enabled ports) or document and/or infer connectivity between AIM-enabled panel ports and other equipment (without AIM-enabled ports),

c) monitor the connections and disconnections of a) and b).

5.3 Functional requirements

5.3.1 Documentation and maintenance of information within AIM software

Once configured, an AIM system shall be able to

a) accommodate the chosen identification scheme for the items to be documented within the AIM software (including identification schemes in accordance with IEC 81346-1 and ISO/IEC 14763-2 – an implementation of which is described in ISO/IEC TR 14763-2-1),

b) record the connections between elements within the cabling infrastructure,

c) automatically detect, document and monitor the presence of discoverable equipment connected to the network and
   1) the basic connectivity configuration of managed network distribution equipment,
   2) the network-related information of end devices,
d) automatically update records when any monitored connections (including those of 5.2) are modified,
e) manually document asset information for non-discoverable equipment,
f) document the physical location of the network distribution equipment connected to the network,
g) document and/or infer connectivity between non-AIM enabled ports and other equipment,
h) document the presence and physical location of AIM hardware,
i) identify and track the physical location of end devices connected to the network,
j) maintain a history of events relating to items a) to i),
k) enable the display of mapped items documented within the AIM software to a physical location on building plans and layouts.

5.3.2 Management and usage of information within AIM software

An AIM system shall be able to

a) enable the user to define conditions in which an event generates an alarm,
b) enable a user to define the conditions in which an alarm generates a notification,
c) enable a user to view graphical representation of connectivity (circuit trace) and other relational information for the items documented within the AIM software,
d) provide recommendations on the cabling connectivity tasks required within work orders for service provision,
e) enable a user to manage work orders related to items documented within the AIM software:
   1) create,
   2) assign or re-assign,
   3) schedule or re-schedule,
   4) perform,
   5) track (status),
   6) close,
f) maintain a work order history,
g) provide access to electronic work orders and other information maintained by the AIM system in the spaces where the AIM hardware is located,
h) provide a means to automatically detect the accuracy of implementation of connect/disconnect work order tasks between AIM-enabled ports:
   1) provide a means to alert of an incorrect implementation,
   2) automatically update the task status following correct implementation,
i) generate reports (both automatically and on-demand) related to items documented within the AIM software.

5.3.3 Integrity of information within AIM software

Upon recovery from disruption to an AIM system or its components, the system shall provide the ability to

a) maintain the integrity of information within the AIM software,
b) reflect the current state of monitored connectivity.

5.4 Functional recommendations

An AIM system should be able to generate formatted data for the production of labels.

6 AIM solutions: business benefits

6.1 General

Clause 6 maps the intrinsic capabilities of AIM systems defined in Clause 5 to real-world benefits and provides examples of where the extension of the capabilities by linkage to external systems may provide additional benefits to an organization.

6.2 Intrinsic benefits of stand-alone AIM systems

6.2.1 Accurate documentation

Poorly documented systems are difficult to troubleshoot. AIM systems can provide automated up-to-date documentation that can improve system availability. Easily accessible and current documentation allows organizations to spend less time obtaining information necessary to troubleshoot cabling infrastructure and network problems.

6.2.2 Asset management

The purpose and intent of asset management is to improve the effective utilization and availability of business assets with the aim of reducing operating cost.

Assets include all elements of software and hardware that are found in the business environment.

Information technology (IT) asset management is an important part of an organization's strategy. It usually involves gathering detailed hardware and software inventory information which is then used to make decisions about hardware and software purchases and redistribution. IT inventory management helps organizations manage their systems more effectively. It also saves time and money by avoiding unnecessary asset purchases and promoting the harvesting of existing resources.

AIM systems are capable of manually documenting asset information for passive components and have the capability to discover the presence of, and maintain information about the network connectivity status and derived location of

a) network distribution equipment, e.g. routers, switches, wireless access points (WAPs),

b) end devices, e.g. servers, personal computers (PCs), internet protocol (IP) telephones, IP cameras, access control equipment, etc.

To limit disruption of business operations and information security, organizations utilize incident management processes. AIM systems are able to enhance these processes through recording events and generating notifications, alerts and alarms in response to the recorded events.

There are also potential benefits to the storage of acceptance test or configuration information within the record of the connected network distribution equipment or end devices (see 6.3.2.3).

6.2.3 Capacity management

An organization is able to use the record of capacity and utilization of telecommunications infrastructure facilities, network distribution equipment or end devices maintained by the AIM system to improve the speed and accuracy of planning of moves, adds and changes. Examples include the following.

a) In all situations, through its ability to analyse physical status of equipment ports and correlate that information to logical status of these ports, the AIM system is able to pinpoint unused ports that could be freed up for production use, thereby maximizing the utilization of existing network equipment and possibly eliminating future asset purchases.

b) In office environments, the record of switch ports with a patched connection may be related to the number of switch ports without an end-device connection and used to create a work order to remove cords from unused ports – ensuring the maximum use of existing ports and potentially negating the need to purchase additional capacity.

c) In data centres, the record of total telecommunications infrastructure space and occupied telecommunications infrastructure space may be used to accurately assess the available space to house incoming telecommunications infrastructure equipment and to assist in the planning of the new location.

6.2.4 Change management

Many industries have risk management regulations or recommendations that include requirements or recommendations for change management control. For example,

a) in the finance industry: Sarbanes–Oxley Act and BASEL III,

b) in data centres: the EU Code of Conduct and ITIL,

c) in the pharmaceutical industry: U.S. Food and Drugs Administration – Good Manufacturing Practices.

Changes to the cabling infrastructure, network distribution equipment and end devices are maintained within AIM systems and include but are not limited to the real-time information about

1) authorized and unauthorized patching activities,

2) generation of move, add, change work orders or a linkage with work order management systems in order to reduce the time required to implement connectivity changes, and to deliver improved accuracy by minimizing possibilities of human errors,

3) automated tracking of work order completion,

4) scheduled work order history,

5) monitoring changes to connectivity, providing user defined alerts, maintaining a change history as described in 6.3.5.

6.2.5 Incident management

AIM systems are able to record events and generate notifications, alerts and alarms in response to the recorded events. This facility can enhance security by notification of unauthorized connections, disconnections or access to the AIM system. This information can be provided to IT or physical security staff within the organization. The real-time event notification may be sent using a variety of methods depending on the functionality of the AIM system (e.g. email, text messaging, SNMP traps).

6.3 Extrinsic benefits of AIM when linked with other business information and network management systems

6.3.1 General

Exchange of data between an AIM system and business information or network management systems can provide enhanced functionality to both systems (IP telephony management, helpdesk applications, etc.).

Other business information systems are a broad category that may apply to many different systems or applications within customer owned premises. The following non-exhaustive list of systems and applications are covered because of their importance and impact when linked with AIM systems.

a) IT-related systems:
   - internet protocol (IP) telephony management,
   - network management systems,
   - helpdesk or incident management applications,
   - information security management systems.

b) Building management systems:
   - energy management systems,
   - lighting control systems.

c) Data centre infrastructure management (DCIM).

d) Configuration management database (CMDB) applications.

6.3.2 IT-related systems

6.3.2.1 IP telephony management

Traditionally, locating a call from a voice over IP (VoIP) phone means relying on a database that is updated and verified manually, meaning information could be out-of-date or incorrect. In times of emergency, corporate security needs to have the ability to quickly and accurately pinpoint the location from where an emergency call was originated. The AIM system tracks the physical location of end devices that are connected to the cabling infrastructure including VoIP phones. Through integration with a VoIP management system, the location information maintained by the AIM system can be displayed on the VoIP phone screens that are used by corporate security. In this way a security officer will have access to the location information as soon as an emergency call is received. Additionally, depending on features of VoIP phones, the AIM system could provide a snapshot of a floor plan with the location of the caller highlighted.

6.3.2.2 Network management systems

Network management systems manage the network elements, also called managed devices. Device management includes fault, configuration, accounting, performance, and security management.

Management tasks include discovering network inventory, monitoring device health and status, providing alerts to conditions that impact system performance, and identification of problems, their source(s) and possible solutions.

The benefits of interoperability with AIM systems include

a) the consolidation of all alerts related to network elements in a single console to streamline network fault management by correlating alerts received from network elements as well as from cabling infrastructure – this is provided by the ability of AIM systems to generate

events about a status change in cabling infrastructure and forward these events as SNMP traps to network management software applications,

b) an expansion of the existing ability for discovering network inventory based on a logical network map with an ability to display physical connectivity between network elements,

c) the ability to pinpoint the physical location of each discovered network element.

6.3.2.3 Helpdesk applications

The helpdesk is one of several ITIL functions. It covers handling of incidents and requests, and provides an interface for other IT service management processes. In other industry sectors, it is also known as “service desk”.

The primary purposes of a helpdesk include

a) incident management: life-cycle management of all service requests,

b) communication: keeping a customer informed of progress and advising on workarounds.

The benefits of interoperability with AIM systems include

1) real-time notification of changes to connectivity,

2) enhanced information relating to the physical network including network distribution equipment, end devices and cabling infrastructure,

3) automation of service ticket creation process related to move, add and change activities,

4) ability to remotely troubleshoot cabling connectivity incidents,

5) ability to automatically update service ticket status upon completion of move, add and change activities.

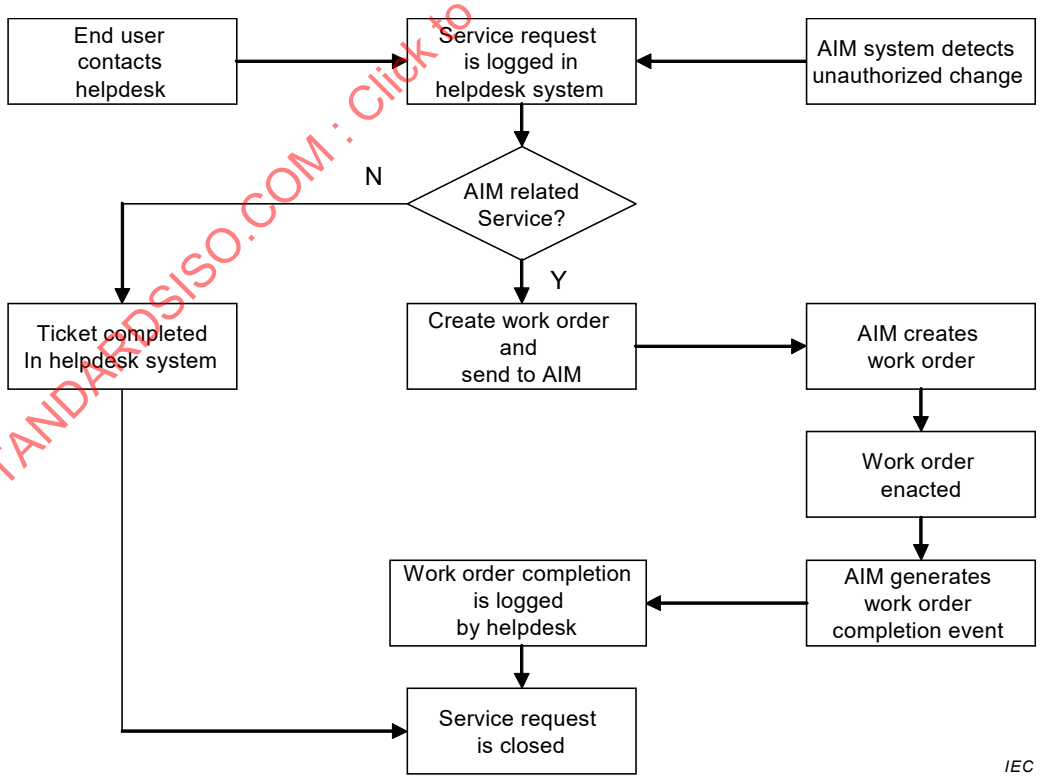


Figure 1 – Example of a helpdesk work flow integrated with an AIM system

The example shown in Figure 1 illustrates how using an AIM system tied to the helpdesk system can improve the efficiency of service request management.

6.3.2.4 Information security management systems

6.3.2.4.1 General

Network security, which is one of the domains described in ISO/IEC 27001, assumes importance to the organization. Networks change frequently as new users and devices are added. Newer data communication technologies are introduced, usage of various networking, communications, and computing technologies are employed to effectively meet these needs.

Sensitive data is increasingly transmitted over networks and proliferation of internet access has increased vulnerability as employees use the internet more for information and knowledge. The information security management system should communicate with the AIM system in such a way as to ensure that the data is not accessible or readable by unauthorized persons. Appropriate and secure authentication methods should be implemented to prevent unauthorized access to data at any AIM access point.

AIM should be considered as an additional means to enhance the network security via the cabling infrastructure.

6.3.2.4.2 Tracking of and response to unauthorized changes

Since the AIM system can track unauthorized changes, a linkage with the organization's physical security system would potentially allow the capture of photographic evidence of the person responsible for the unauthorized change. It may also be possible to automate a response to an unauthorized connection attempt, e.g. send SNMP trap.

6.3.2.4.3 Critical network circuits

Where the information security management system defines certain parts of the physical network as critical connectivity elements, a linkage with an AIM system would potentially enable the generation of real-time notification of breaches to these critical elements as required (audio alarm, urgent text, flashing pop-up, etc.).

6.3.3 Building management systems

6.3.3.1 General

An increasing number of building management systems (BMS) and security systems are adopting an IP-based communication and their control equipment and elements are becoming connected using generic, structured cabling infrastructure.

When used in combination with IP-based BMS, an AIM system is able to provide the BMS management software with valuable information about the physical location of its control equipment within a facility, as well as sending real-time alerts if any equipment gets disconnected from the network to assist with troubleshooting.

Subclauses 6.3.3.2 to 6.3.3.5 highlight particular linkages.

6.3.3.2 Energy management systems in buildings

Energy management is a key aspect of facility management that that can deliver increased energy efficiency and reduced energy costs while minimizing overall environmental impact.

With a considerable proportion of the world's electricity consumed inside office buildings, reducing that share is a key objective for all building stakeholders.

Cabling infrastructure that is connected to sensors and controllers or used for delivering power over Ethernet (PoE) to powered terminal devices plays a significant role in facilitating energy management systems, and an AIM system provides the capability for accurate identification of the physical locations of connected devices in real time.

Providing real-time physical location information for connected devices to energy management applications allows these applications to apply real-time location based energy policies.

6.3.3.3 Lighting management systems

Lighting in commercial buildings is often not turned off in unoccupied areas of a building leading to wasted energy, additional maintenance, and poor environmental impact. An AIM system may be integrated with a lighting management system to combine asset, location and usage data to better manage and control devices or implement energy savings plans.

6.3.3.4 Building security

Interaction between BMS and AIM systems may improve building security in some environments by relating connect/disconnect events with security events. For example, since the AIM system can infer the connection location associated with the arrival of a previously unknown MAC address, this information could be linked to an image or series of images from an IP security camera in that area. This information can then be passed to the network administrator and/or building security staff.

6.3.3.5 Access control

In conjunction with energy management of PoE and employee time and attendance systems and/or access control systems, AIM systems are able to utilize data from external sources, such as badge/card readers, to identify areas of the building which are not in use. This information may be used to control the power supplied to those areas including employees' equipment, e.g. IP phone. The resultant reduction in power consumption has potential financial and environmental benefits for an organization.

6.3.4 Data centre infrastructure management (DCIM)

At a high level, DCIM is able to help infrastructure managers to holistically manage the entire physical infrastructure across both telecommunications infrastructure and the wider data centre facility domains – all assets, systems and their interdependencies.

A DCIM application set is able to improve efficiency and lower costs across six key management areas:

a) operations,

b) resources,

c) assets and connectivity,

d) change,

e) availability,

f) capacity planning/demand.

DCIM is able to

1) identify and eliminate sources of risk to increase availability of critical IT systems,

2) identify interdependencies between IT and wider data centre facility assets to alert the manager to gaps in system performance or redundancy,

3) assist in modelling the cost structures of building and maintaining the huge accumulation of assets which form the data centre, over long periods of time.

To support this functionality, DCIM needs access to real-time data from both the telecommunications infrastructure and the wider data centre facilities.

AIM is able to provide the DCIM platform with real-time-data information from the cabling infrastructure.

The contribution of AIM to DCIM includes but is not limited to

- operations management: identifying unplanned or unauthorized changes to infrastructure connectivity and generating alarms to alert DCIM console about these changes,
- assets and connectivity management:
  - providing visibility into network path redundancy through the ability of an AIM system to discover the different physical network paths that can exist between assets,
  - maintaining complete physical connectivity documentation along with information about the presence of interconnected network distribution equipment and end devices (device discovery),
- change management: automated tracking of connectivity changes to support moves, adds, and changes of IT assets, such as the commissioning and decommissioning of servers,
- availability management: providing connectivity information to help with root cause analysis and other alarm management activities related to physical connectivity, such as diagnosing and resolving network issues,
- capacity planning: accurate port capacity information for patch panels and network distribution equipment to enhance the capacity planning of the DCIM software which may be enhanced if it can be related to the availability of power and cooling.

6.3.5 Configuration management database (CMDB) applications

A linkage to an AIM system can provide automated updating of the physical location of networked IT assets, which ensures the information accuracy that is maintained by CMDB applications.

A key success factor in implementing CMDB applications is the ability to automatically discover information about the items of the CMDB and to track changes as they happen.

Integration with an AIM system could benefit CMDB applications with automatically updated data related to IT assets and their interrelationship via connectivity information that is maintained, monitored and managed within the AIM system. For example, an AIM system could update the items within the CMDB with location information whenever that information changes either due to scheduled or unscheduled connectivity changes.

Figure 2 describes several modules within an AIM system that could be used for updating data in CMDB applications.

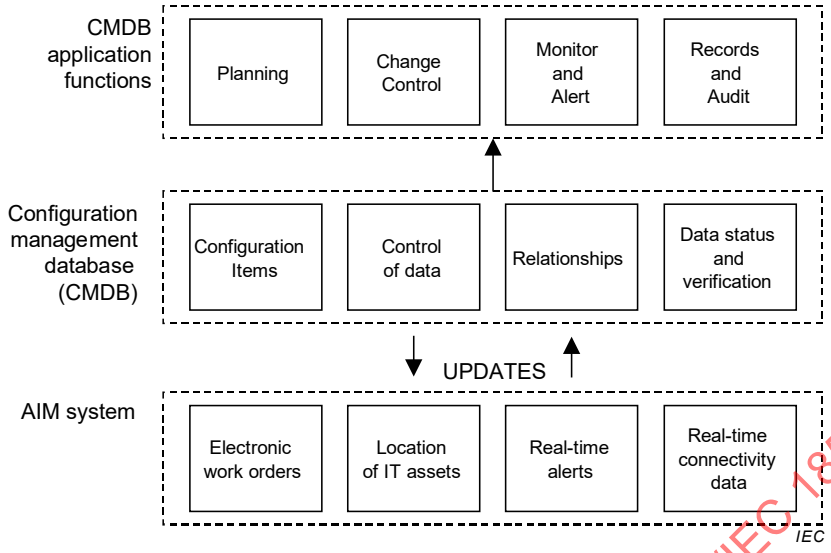


Figure 2 –Relationship between AIM systems and CMDB applications

7 AIM solutions: Data exchange framework

7.1 General

Clause 7 sets out a framework for interoperability between AIM systems and/or other third party applications. It addresses data exchange format, protocols and commands and defines a common data model describing elements (which may be assets or cabling infrastructure) contained within an AIM system.

The AIM system shall provide a system level data exchange framework as described in 7.3 using one of the formats or protocols described in 7.2.

Where a lower level data exchange framework is specified, it should conform to the commands and data model described in Annex D.

7.2 Data exchange format and protocols

The data exchange may be performed by one or more interfaces which are exposed by the AIM system. These interfaces shall conform to either

a) an HTTP SOAP (simple object access protocol) based web service or,

b) a RESTful HTTP based web service exposing XML or JSON objects

The data exchange format(s) and protocols shall be defined for an AIM system.

The data exchange interface or interfaces shall expose commands of 7.3.

7.3 Commands

Commands are used to query, create, delete or modify data (based upon defined permissions) within the AIM system. The specific naming of each operation may vary according to the AIM system, however they should conform to the input parameters and response parameters described in Table 1 to Table 4.

Operations may be supplemented by additional parameters. Where the parameter or response is surrounded by {}, it refers to a data object described in 7.4.

Table 1 – Work order management commands

Operation	Description	Parameters	Response
Create work order	Creates a new work order within the AIM system.	Name, Description, Start date, End date, Manager, Technician	Status, Work Order ID
Create work order task/step	Creates a work order step within an existing work order	Work Order ID, {Work Order Task}	Status
Query work order	Get information about an existing work order and its tasks	Work Order ID	Status, {Work Order}
Delete work order	Delete an existing work order and all its tasks	Work Order ID	Status

Table 2 – Asset management

Operation	Description	Parameters	Response
Create asset	Create a new asset within the system	Parent Element ID, Asset ({Premises/space}, {Furniture}, {Telecommunications equipment})	Status, Element ID
Query asset	Query an existing asset within the system	Element ID	Status, Asset ({Premises/space}, {Furniture}, {Telecommunications equipment})
Delete asset	Delete an existing asset within the system	Element ID	Status

Table 3 – Alarms and events

Operation	Description	Parameters	Response
Query events	Query all events matching a specified criterion	Event type, Start time, End time	Status, List of {Events}
Query event	Query an existing event within the system	Event ID	Status, {Events}
Query alarms	Query all alarms matching a specified criterion	Alarm type, Start time, End time	Status, List of {Alarms}

Table 4 – Circuit tracing

Operation	Description	Parameters	Response
Query circuit trace	Query a circuit trace based on a specified port	Element ID, Port ID	Status, {Circuit}

7.4 Common data model definition

7.4.1 General

The common data model definition defines all physical and non-physical elements within the system. This includes derived connectivity information such as circuit segment connections and circuits.

7.4.2 Element reference ID

All the elements, i.e. telecommunications or non-telecommunications objects, managed by the AIM software shall have a unique element reference ID.

7.4.3 Element and attribute definitions

7.4.3.1 General

Elements of AIM software are described by name and required attributes. Subclause 7.4.3 provides a reference to ISO/IEC TR 14763-2-1 where applicable. These are the minimal attributes for such elements within AIM software, and some software may provide more attributes. Annex B provides a description of AIM software fields.

Where elements have an attribute describing a parent element, they will be part of a defined hierarchy which should be adhered to; this is also described.

Table 5 provides a key for designations applied to attributes of the elements.

Table 5 – Attribute key

Key	Parameter	Description
D	Derived value	The value of this field may be immutable and automatically generated by the system
O	Optional	This field may not be present in all AIM systems

7.4.3.2 Connectivity

Connectivity represents either a connection, circuit segment or a circuit. A connection represents the connection of an A and B Element (for example, a patch cord connected to a port). A circuit segment represents a connection at A and a connection at B connected via a common element C (for example, ports A and B connected using a patch cord C). A circuit is a derived collection of circuit segment records. This represents an end-to-end connectivity in a network. See Table 6 for details.

Table 6 – Connectivity

Name	Attributes
Connection	ID A Element B Element
Circuit Segment	ID Name (D) A Element (D) B Element (D) C Common Element – (O)(D)
Circuit	ID Ordered List of Circuit Segments (D)

7.4.3.3 Premises/space

Premises/space represents a physical area whether it be an asset (i.e. building) or a designated area (region). See Table 7 for details and see Figure A.1 for hierarchical structure and containment rules.

Table 7 – Premises/space

Name	Attributes
Geographic Area	ID Name Description Location
Campus	ID Name Description Location
Building	ID Name Description Location

Name	Attributes
Room	ID Name Description Location
Zone	ID Name Description Location
Floor	ID Name Description Location

7.4.3.4 Furniture

Furniture represents any non-telecommunications equipment that may be managed or referenced in an AIM system. This may be office, data centre or outside equipment but is not part of the network infrastructure. See Table 8 for details. There are no current references to furniture in ISO/IEC TR 14763-2-1:2011.

Table 8 – Furniture

Name	Attributes
Desk (O)	ID Name Description Parent (Organizational Element)

7.4.3.5 Telecommunications equipment

Telecommunications equipment refers to any equipment which forms a physical part of the network infrastructure. IDs should be constructed using the ISO/IEC TR 14763-2-1 references. See Table 9 for details and see Figure A.2 for hierarchical structure and containment rules.

Table 9 –Telecommunications equipment

Name	Attributes
Cabinet	ID Name Description Vendor (O) Part Number (O) Colour (O) Space (D) U Capacity Catalogue image (O)
Rack	ID Name Description Vendor (O) Part Number (O) Colour (O) Space (D) U Capacity Catalogue image (O)
Frame	ID Name Description Vendor (O) Part Number (O) Colour (O) Space (D) U Capacity Catalogue image (O)

Name	Attributes
Port	ID Name Description Vendor (O) Part Number (O) Colour(O) Parent Element (D) Catalogue image (O) Port Type Performance Level (O) Port status Service (D) (O) Cord Length (O)
Module	ID Name Description Vendor (O) Part Number (O) Colour (O) Parent Element (D) Position List of front ports List of back ports Port front-back mapping Template (O) Catalogue image (O)
Cable	ID Name Part Number (O) Type Vendor (O) Colour (O) Catalogue image (O) Cable Bundle Identifier (O) Length (O)

Name	Attributes
Cord (O)	ID Name Part Number (O) Colour (O) Vendor Length Connector A Connector B Cable Catalogue image (O)
Closure	ID Name Description Vendor (O) Part Number (O) Colour (O) Parent Element (D) Catalogue image (O) U Height (O) List of modules (O) List of ports Template (O)
Patch Panel	ID Name Description Vendor (O) Part Number (O) Colour (O) Container (D) Position Catalogue image (O) U Height (O) List of modules (O) List of front ports List of back ports Port front-back mapping Template (O)

Name	Attributes
Connector (O)	ID Name Connector Type Catalogue image (O)
Network distribution equipment and end device (rack mounted)	ID Name Description Vendor (O) Part Number (O) Colour (O) Parent Element (D) Position (O) Catalogue image (O) U Height (O) List of modules (O) List of ports Template (O) Network Address (O) MAC Address (O) Maximum Port Power Delivery (O)
Network distribution equipment and end device (non-rack mounted)	ID Name Description Vendor (O) Part Number (O) Colour (O) Parent Element (D) Position (O) Catalogue image (O) U Height (O) List of modules (O) List of ports Template (O) Network Address (O) MAC Address (O) Maximum Port Power Delivery (O)

7.4.3.6 Organizational Element

An Organizational Element is an element which represents one or more people. All Organizational Elements can have a parent element (of type Organizational Element), but 'Person' cannot be a parent itself. See Table 10 for details.

Table 10 – Organizational Element

Name	Attributes
Organization	ID Name Description
Group	ID Name Description Parent (Organizational Element)
Department	ID Name Description Parent (Organizational Element)
Team	ID Name Description Parent (Organizational Element)
Cost Centre	ID Name Description Parent (Organizational Element)
Person	ID Name Description Parent (Organizational Element)

7.4.3.7 Work Order

A Work Order is a task or a set of tasks related to elements or attributes of elements within an AIM system. It may contain one or more Work Order Tasks, is assigned to an Organizational Element and implemented by an Organizational Element. See Table 11 for details and Figure A.3 for hierarchical structure and containment rules.

Table 11 – Work Order

Name	Attributes
Work Order	ID Name Description Scheduled Start Time Scheduled End Time List of Work Order Tasks Assigned (Organizational Element) Implementer (Organizational Element) WorkOrderState

7.4.3.8 Work Order Task

A Work Order Task is an actionable task which applies to an element or an attribute of an element. See Annex A for containment rules. See Table 12 for details.

Table 12 – Work Order Task

Name	Attributes
Work Order Task	ID Name Description Task Type List of affected Elements Scheduled Start Time Scheduled End Time Implementer (A member of WO Organizational Element) Dependencies (O) Task Status

7.4.3.9 Event

An Event is anything which creates or changes the state of an element, organizational element, connection, work order or work order task and shall have a timestamp. See Table 13 for details.

Table 13 – Event

Name	Attributes
Event	ID Name Description Event Type List of Related Elements Timestamp

7.4.3.10 Alarm

An Alarm is any event of sufficient importance to require a notification or escalation to a user of the AIM system. See Table 14 for details.

Table 14 – Alarm

Name	Attributes
Alarm	ID Event ID Name Description Alarm Type Notification Details

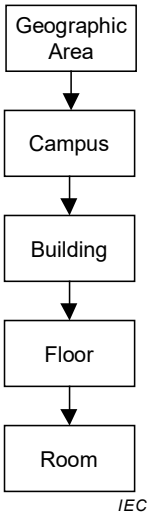
7.4.4 Containment rules and hierarchy

For an element with a parent attribute, a containment rule is defined. This states valid parent elements for the given element. An element lower in the hierarchy cannot contain one that appears higher. See Annex A for the hierarchical structure of the elements of the data model.

Annex A
(informative)

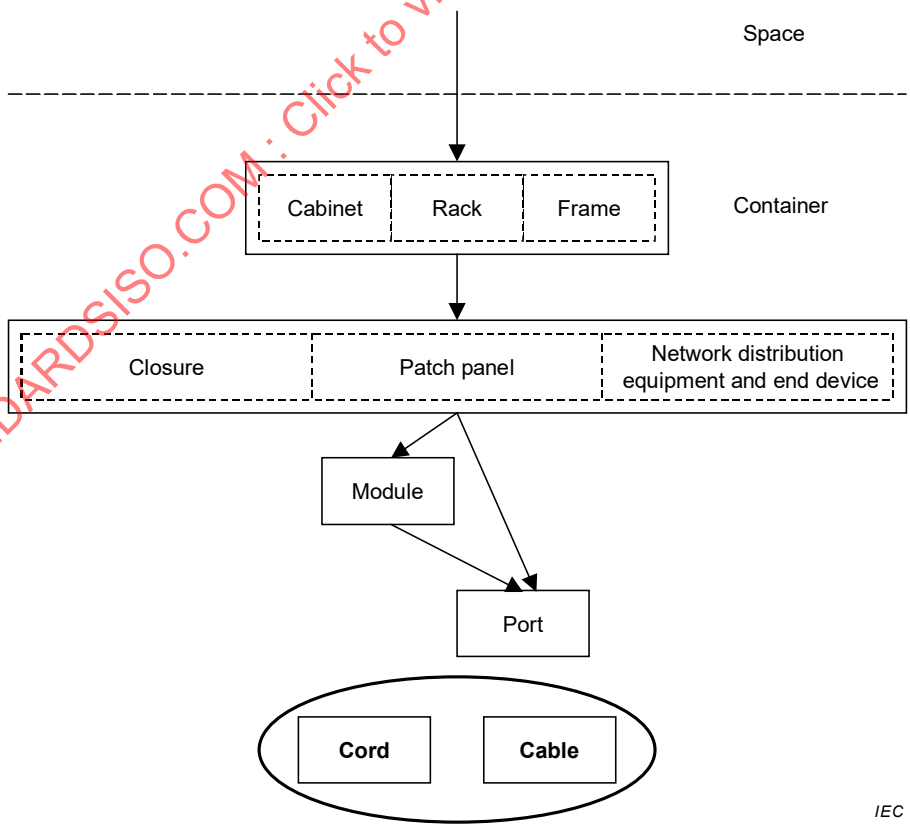
Hierarchy and containment rules

Figures A.1 to A.3 describe the hierarchical structure and containment rules for the elements of the data model of 7.4.



NOTE A Zone can be a child of any premises/space.

Figure A.1 – Spaces



Cord and Cable are not relevant to this hierarchy.

Figure A.2 – Telecommunications equipment