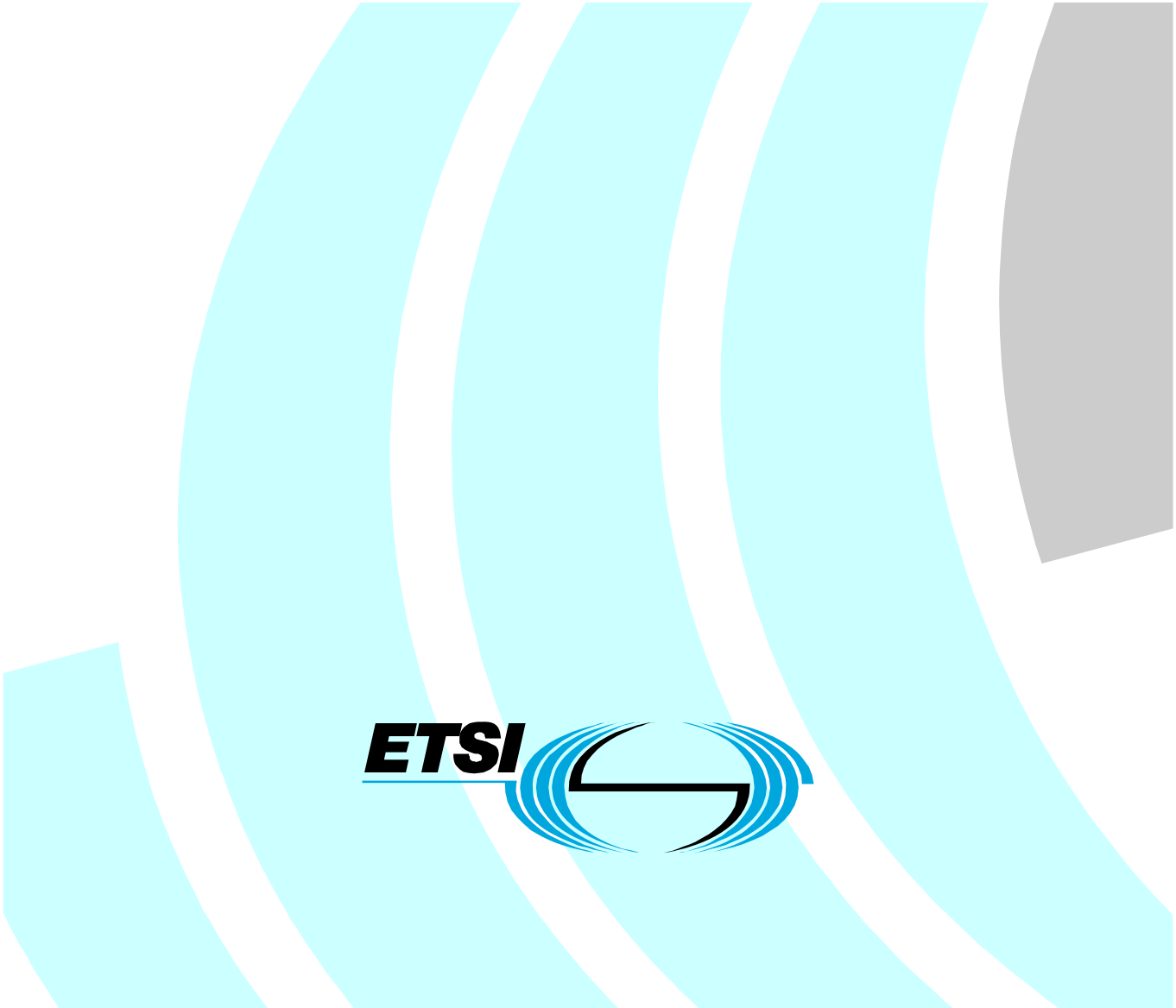
ETSI ES 202 336-1 V1.1.1 (2007-11)

ETSI Standard

Environmental Engineering (EE); Monitoring and Control Interface for Infrastructure Equipment (Power, Cooling and Building Environment Systems used in Telecommunication Networks) Part 1: Generic Interface



Reference
DES/EE-02037-1

Keywords
control, interface, management, power, system

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Standard (ES) has been produced by ETSI Technical Committee Environmental Engineering (EE).

The present document is part 1 of a multi-part deliverable covering power, cooling and building environment systems control and monitoring guidance, as identified below:

Part 1: "Generic Interface";

Part 2: "DC power system control and monitoring information model";

Part 3: "AC UPS power system control and monitoring information model";

Part 4: "AC distribution power system control and monitoring information model";

Part 5: "AC diesel back-up generator system control and monitoring information model";

Part 6: "Air conditioning system control and monitoring information model";

Part 7: "Other utilities system control and monitoring information model".

1 Scope

The present document applies to monitoring and control of Infrastructure Environment i.e. power, cooling and building environment systems for telecommunication centres and access network locations.

Interoperability of heterogeneous management interfaces and systems with multi-vendor equipment is the key issue. The present document gives a general approach from equipment to management system.

The multi-part deliverable is composed of a generic core part (part 1) and several specific parts for equipment category (part 2 and following).

The core document defines:

- The site equipment map and its division in functional subsets e.g. DC system which introduces part 2 and following.
- The generic set of exchanged information required at the interface of equipment, which is instanced for each equipment subset in part 2 and following.
- The minimum requirement for network architecture allowing some compatibility with old existing interface and the mechanism to exchange data between network element
- The data interface protocol for remote or local site management (Machine to machine interface MMI) and human machine interface HMI for monitoring and controlling.
- Recommendations for sure management network such as dependability, data back-up, data coherence and synchronization all along the management network, response time, fault detection and partial service in case of failure.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ETSI ETS 300 132-1: "Equipment Engineering (EE); Power supply interface at the input to telecommunications equipment; Part 1: Operated by alternating current (AC) derived from direct current (DC) sources".

[2] ETSI EN 300 132-2: "Environmental Engineering (EE); Power supply interface at the input to telecommunications equipment; Part 2: Operated by direct current (DC)".

[3] ETSI EN 300 132-3: "Environmental Engineering (EE); Power supply interface at the input to telecommunications equipment; Part 3: Operated by rectified current source, alternating current source or direct current source up to 400 V".

[4] ETSI EN 302 099: "Environmental Engineering (EE); Powering of equipment in access network".

[5] ITU-T Recommendation M.3010: "Principles for a Telecommunications management network".

[6] ITU-T Recommendation M.3100: "Generic network information model".

[7] ITU-T Recommendation X.733: "Information technology - Open System Interconnection - System Management: Alarm reporting function".

[8] IEC 60839-5-4: "Alarm systems - Part 5: Requirements for alarm transmission systems - Section 4: Alarm transmission systems using dedicated alarm transmission paths".

[9] ITU-T Recommendation X.25: "Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit".

[10] IETF RFC 2616: "Hypertext Transfer Protocol - HTTP/1.1".

[11] ISO/IEC 7498: "Open Systems Interconnection - Basic Reference Model".

[12] IEEE 802.series (all parts): "IEEE Standard for Telecommunications and Information Exchange Between systems - Local and metropolitan area networks ".

[13] ISO/IEC 10164 (all parts): "Information technology - Open Systems Interconnection - Systems Management".

[14] ISO/IEC 8879: "Information processing - Text and office systems - Standard Generalized Markup Language (SGML)".

2.2 Informative references

[15] ETSI TR 102 121: "Environmental Engineering (EE); Guidance for power distribution to telecommunication and datacom equipment".

[16] ETSI TR 102 336: "Environmental Engineering (EE); Power and cooling system control and monitoring guidance".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

NOTE: Terms referring to energy interface, equipment and distribution are described in power distribution guidance and standards ETS 300 132-1 [1], EN 300 132-2 [2], EN 300 132-3 [3] for ac and dc interface and EN 302 099 [4] for access network equipment powering.

alarm: any information signalling abnormal state, i.e. different to specified normal state of hardware, software, environment condition (temperature, humidity, etc.)

NOTE: The alarm signal shall be understood by itself by an operator and shall always have at least one severity qualification or codification (colour, level, etc.).

alarm loop: electrical loop which open or closed state correspond to alarm start (set) or end (clear) state

alarm message: text parts of the alarm structure

alarm structure: organized set of information fields in an alarm data frame (time stamp, set/clear, text, etc)

battery: complete arrangement of battery cells or blocks in one string or more in parallel

battery cell: basic electrochemical element (e.g. 2 V for lead acid battery)

battery string: a number of serially interconnected battery blocks or cells

client post: any device (laptop, PDA, console, etc.) connected to servers via the operation system networks to perform maintenance or supervision operations

NOTE: It is independent of object class and object properties. The most common functions are GET and SET, equivalent to monitor and control.

Common Management Information Protocol (CMIP): protocol using CMIS service to obtain remote monitoring and control. CMIP is much richer than SNMP but much more complex to implement

Common Management Information Service (CMIS): generic services to handle objects (operation and notification of results)

Control Unit (CU): integrated unit in an equipment to monitor and control this equipment through sensors and actuators

Control form Style Sheet (CSS): simple mechanism for adding style (e.g. fonts, colors, spacing) to Web documents. Tutorials, books, mailing lists for users, etc.

Dynamic Host Control Protocol (DHCP): protocol used for self configuration of TCP/IP parameters of a workstation assigning IP address and a subnetwork mask

NOTE: DHCP may also configure DNS.

Dynamic Name Server (DNS): associates a single domain name to an IP address

dynamic synoptic: dynamic display of geographical maps, networks, installations and equipment

Data Gathering Unit (DGU): functional unit used for several functions:

- collect serial, digital, and analog data;
- option to send (output) serial or digital commands;
- forward/receive information to/from the Local/Remote Management Application via agreed protocols;

- mediation between interfaces and protocols.

NOTE: This function may be integrated as part of specific equipment.

Ethernet: LAN protocol

NOTE: Equivalent to IEEE 802.1 to 11 [12].

event: any information signalling a change of state which is not an alarm: e.g. battery test, change of state of battery charge

NOTE: The alarm signal shall be understood by itself by an operator and shall always have at least one severity qualification or codification (color, level, etc.). It shall be transmitted in a formatted structure with text message and other fields like for alarm, e.g. an event can be coded as an alarm with severity "0".

Guidelines for Definition of Managed Objects (GDMO): syntax specification for the classification of objects and properties

NOTE: Associated to ASN.1 language for object definition.

infrastructure equipment: power, cooling and building environment systems used in telecommunications centres and Access Networks locations

EXAMPLE: Cabinets, shelters, underground locations, etc.

Intranet: internal company network generally using Ethernet protocol and extended IP addresses

logbook: chronological file that contains alarm and event messages may be paper or electronic

Management Information Base (MIB): dynamic data base that gathers all objects and should evolve to include automatic and manual configuration tools with self coherence tests

menu: list of possible input command choices that may be presented in different ways on a display

NOTE: Selection is normally made by a keyboard, a pointing device, a mouse or directly by finger on a sensitive screen.

object: class description of items that accept a set of properties or functions

NOTE: Generic objects can include more specific items and inherit from their properties. If correctly structured, object programming can allow the system to evolve, i.e. be more future-proof. The code should intrinsically be open and structured.

PHP: powerful tool for making dynamic and interactive Web pages

pop-up: information or command screen that appears when a menu choice is selected

NOTE: For example this may be a pop-up menu when the pointer is on a title button.

REpresentational State Transfer (REST): way to build an application for distributed system as www

Simple Object Access Protocol (SOAP): way to communicate between applications running on different operating systems, with different technologies and programming languages

NOTE: SOAP communicates over HTTP, because HTTP is supported by all Internet browsers and servers, SOAP traffic is not blocked by firewalls and proxy servers (see W3C).

Systems Management Function (SMF): object properties or classes with projection on CMIS application context communication

NOTE: Set of ISO system management functions according to ISO/IEC 10164 [13].

warning: low severity alarm

World Wide Web Consortium (W3C): consortium founded in October 1994 to develop common interoperable protocols and promote World Wide Web

NOTE: See http://www.w3c.org.

windows: virtual area on the display that corresponds to a specific application

web: common name for the Internet or Intranet

XCU: CU enabled to communicate using XML interface as defined in the present document

XHTML: stricter and cleaner version of HTML. XHTML consists of all the elements in HTML 4.01 combined with the syntax of XML. It can be read by all XML browser (see W3C)

eXtensible Mark-up Language (XML): application profile or restricted form of SGML

NOTE: By construction, XML documents are conforming SGML the Standard Generalized Markup Language (ISO/IEC 8879 [14]). documents.XML is designed to describe data and focus on what data is. XML must be discerned from the well known Hypertext Transfer Mark-up Language (HTML) which was designed to display data and to focus on how data looks.

XML Schema Definition (XSD): new more detailed XML description compared to the previous one, the DTD

Extensible Style sheet Language (XSL): language for expressing style sheets

NOTE: It consists of two parts, a language for transforming XML documents, and an XML vocabulary for specifying formatting semantics. An XSL style sheet specifies the presentation of a class of XML documents by describing how an instance of the class is transformed into an XML document that uses the formatting vocabulary.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AC	Alternative Current
ADSL	Asynchronous Digital Subscriber Line
API	Application Program Interface
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
CIM	Common Information Model
CMIP	Common Management Information Protocol (OSI)
CMIS	Common Management Information Service (OSI)
CSS	Cascading Style Sheets
CU	Control Unit
DC	Direct Current
DCF	Data Communication Function in TMN
DEG	Diesel Engine Generator
DHCP	Dynamic Host Configuration Protocol
DGU	Data Gathering Unit
DNS	Domain Name Server
DTD	Document Type Definition
EP	Exploitation Post
FTP	File Transfer Protocol
GDMO	Guidelines for Definition of Managed Objects
GSM	Global System for Mobile
HMI	Human-Machine Interface
HTML	HyperTex Transfer Make-up Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IEM&C	Infrastructure Equipment Monitoring & Control (mediation agent)
IP	Internet Protocol
ISDN	Integrated Service Digital Network

LAN	Local Array Network
LED	Light Emitting Device
LMA	Local Management Application
LON	Local Operated Network
MCF	Management Communication Function (in TMN)
M&C	Monitoring and Control
MIB	Management Information Base (in SNMP for example)
MEP	Mobile Exploitation Post
MF	Mediation Function (in TMN)
MMI	Machine-Machine Interface
MTTR	Mean Time to Repair
MTU	Maximum Transmission Unit
NEF	Network Element Function (in TMN)
NEM	Network Element Management
ODBC	Open Data Base Connectivity
OSF	Operating System Function (in TMN)
OSI	Open Service Interconnexion (in TMN)
POTS	Plain Old Telephone Service
PDA	Personal Digital Assistant
PHP	PHP: Hypertext Preprocessor
PLC	Programmable Logic Controller
PSTN	Public Switched Telephone Network
REST	REpresentational State Transfer
RFC	Request For Comments
RMA	Remote Management Application
RPC	Remote Procedure Calls
SCTP	Stream Control Transmission Protocol
SDH	Synchronous Data Hierarchy
SGML	Standard Generalized Markup Language

NOTE: See ISO/IEC 8879 [14].

SMF	Systems Management Functions
SMS	Short Message System
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
TCP	Transmission Control Protocol for IP
TMN	Telecommunications Management Network

NOTE: See ITU-T Recommendation M.3010 [5].

UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WSF	Work Station Function
WAN	Wide Array Network
W3C	World Wide Web Consortium
xDSL	Digital Subscriber Line
XCU	XML enabled CU
XML	eXtensible Mark-up Language (see W3C)
XHTML	eXtended HTML
XSD	XML Schema Definition
XSL	Extensible Stylesheet Language
XSLT	eXtensible Stylesheet Language Transformation

4 Monitoring & Control (M&C) overview

Monitoring and control of power, cooling and building environment systems are used to simplify operation, to reduce maintenance time and site intervention, to reduce human error risk, to give useful data for statistical analysis and management (i.e. operation cost, reliability or quality management, power consumption estimation).

To achieve this purpose, monitored information and control are needed.

- The information are alarms, events, measurements, data recordings and events logs.
- The controls are commands to the equipment, alarm acknowledge, configuration and settings.

Several management levels are possible for telecommunication installations and equipment. They are described considering complexity of the system, response time and required level of details from basic alarms to complex analysis level. In many cases, the same basic information is needed from the equipment-monitoring interface but address different services that prepares information as requested by users categories.

4.1 Infrastructure equipment management network general description

Infrastructure Equipment (powering, cooling, building facilities) management network is a subset of TMN.

The infrastructure equipment management network can be defined by functional interfaces between network elements.

Referring to ITU-T Recommendation M.3010 documents for nomenclature [5] and [6], the element can be understood as generic part of Telecommunication Management Network (TMN):

- The Control Unit (CU) is dedicated to control one or more equipment in a site.
- The XCU connects to e.g. a legacy equipment and translates its data to conform to the "TMN" standardized format X. The XCU may also be a unit that gathers building facilities alarm loops and makes them available in the standardized format X. These XCU are Network Element Function in ITU-T Recommendation M.3010 [5] (NEF).
- The Data Gathering Unit (DGU) is used to gather one or more CU field bus to adapt with TMN protocol and format. The DGU is a Mediation Function in ITU-T Recommendation M.3010 [5] (MF).
- CU and DGU may be combined in the same unit, especially in the case of small centers where there are few building facilities alarm loops and few equipment.
- The local Management Application (LMA) and Remote (RMA) servers process information received from the XCU and DGU to achieve the functionalities of the management system i.e. Operating System Function in ITU-T Recommendation M.3010 [5] (OSF).
- LMA can be combined with XCU or DGU.
- The Exploitation Post (EP) offers the man-machine interface. It can be integrated to the LMA/RMA or not e.g. on Mobile Exploitation Post (MEP). These entity manages the interactive presentation to the user to monitor and control the equipment. (Work Station Function (WSF) in ITU-T Recommendation M.3010 [5]).

Several XCU and DGU can be managed within this network by one (or perhaps several) LMA, RMA. There may also be several users connected through the network, to one server or one equipment. The application controlling such a network with multi-user and with different user rights levels is a Network Element Management system (NEM system in ITU-T Recommendation M.3010 [5]).

Figure 1 presents the network architecture in respect to scope requirements for communication interfaces:

- between the DGU or XCU and the LMA or RMA;
- between EP or MEP and the RMA or DGU or XCU;
- Alarms contacts or loops output interface backuping IP network.

NOTE: The field level interface of CU are out of the scope:

- Equipment or room sensors interfaces to XCU or DGU.
- Interface between XCU and DGU.

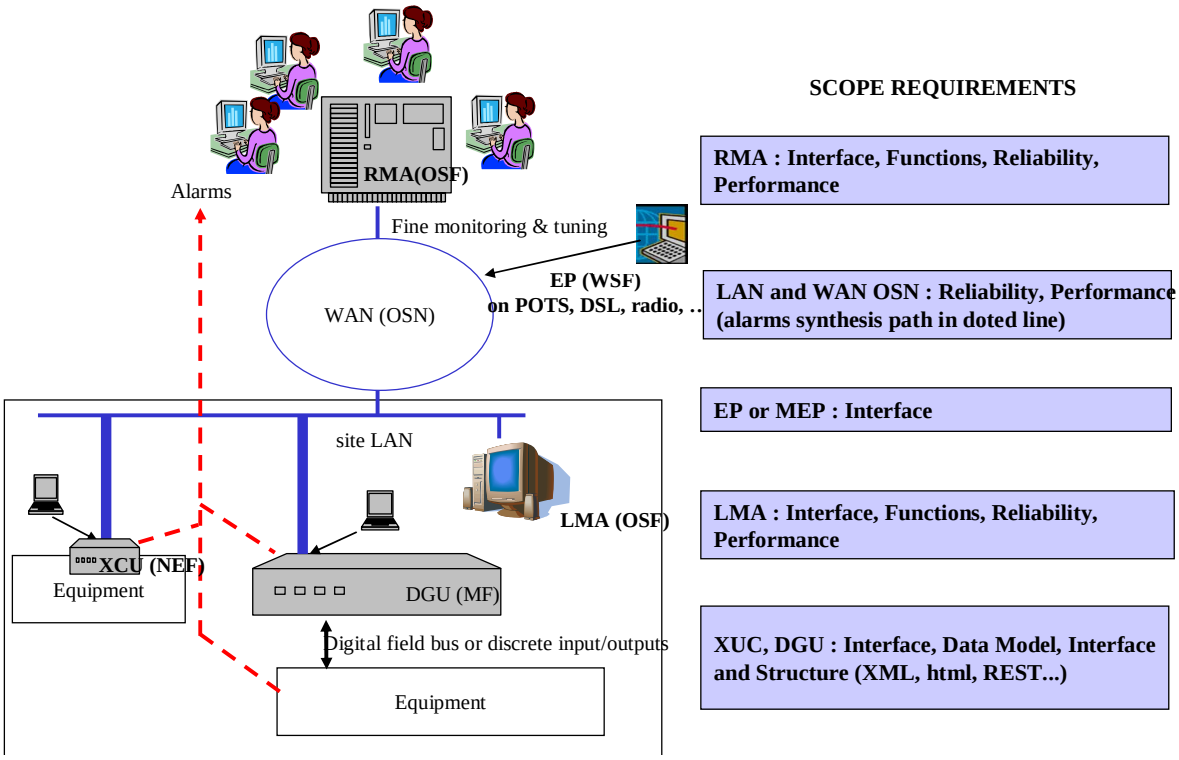


Figure 1: Scope requirements on Functional Diagram

In this infrastructure equipment management network, the use of CMIP and CMIS is not mandatory.

Each element (XCU, DGU) shall be a http node with a URL address able to exchange data formatted in XML language.

Data exchanges shall use at least REST procedure based on http command but RCP or SOAP may be possible as well. REST is the mechanism used for operation on the XML formatted data. This mechanism is supported by an agent: **IEM&C Agent.** REST commands are detailed in annex A.

4.2 IEM&C management network example

Figure 2 gives an example of the network and operation elements used for operating a medium size building.

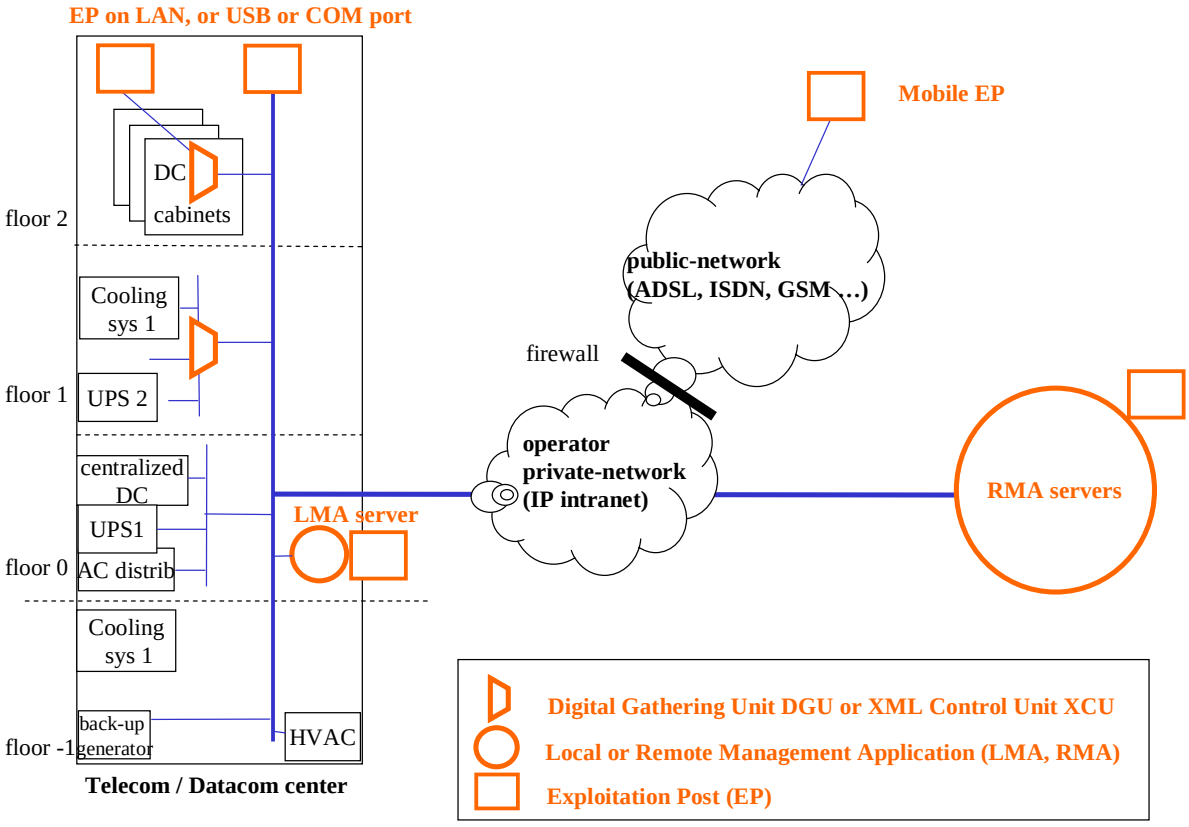


Figure 2: Example of IEM&C network implementation

4.3 IEM&C management network HMI description

Human Interfaces (displays) should be made available at the following locations:

On site:

- locally on the equipment control unit by connecting the Exploitation Post (EP) or mobile EP (MEP);
- on a centralized server through a LAN;
- on a client display (PC or PDA), through the LAN.

Or remotely:

- on one post of the supervision room, in the remote supervision of several centres, through a private or public network;
- on an EP or MEP, through a public network for field maintenance personnel.

Using the MEP connected to the XCU or from distant place, the display shall use a web-browser based interface and without the need for a proprietary software to simplify maintenance and avoid security problems in case of IP network failure, there shall be a mean to connect to the equipment without an IP address provided by the network. For example, the distant web file is transferred and used as a local file by the browser. See also clause 7.2 for details on HMI.

5 Equipment IEM&C main goals

5.1 Data in the IEM&C network

The following clauses describe the minimum set of information required from Infrastructure Equipment (power, cooling systems, etc.) at the interface of equipment.

Mandatory information shall be available at the output of the equipment. Optional information should be proposed to operators.

For low critical systems, at minimum, free of voltage alarm contacts shall be available at the monitoring interface of the equipment. These contacts can gather several information to send only generic signals such as partial failure or loss of redundancy. Generally, as the level of system complexity increases, additional supervisory information is required.

For critical systems, alarms should be more discriminated to improve maintenance analysis. This helps to ensure that:

- the correct spare materials are taken to site for efficient intervention;
- priority of intervention, i.e. in case of simultaneous alarms on several sites (crisis) is determined correctly.

A Control Unit (XCU) and/or Data Gathering Unit (DGU) shall be used to collect, concentrate information available in the equipment, and send or display it with the level of detail and functionality requested by the Local or Remote Management Application or by the a local display (MEP).

Several type of information shall be provided for this purposes at the equipment interface:

- alarms;
- events;
- state variables (i.e. on/off, physical measurements, counters);
- system command;
- system settings (communication, operational parameters except manufacturer setting only allowed locally on the equipment).

The following clauses introduce the monitoring and control information model requirement for different type and complexity of power supply and cooling system.

5.1.1 Mandatory data in the IEM&C network

The minimum set of information described in clause 6 are transmitted through the interface and network to LMA and RMA. Data can be classified as mandatory and optional depending on associated functions.

Mandatory data are used for:

- alarming and warning;
- alarm logging (alarm history files);
- event logging (event history files);
- control, i.e. local and remote process command (individual tests, and global operation, e.g. starting the engine);
- default values resetting (e.g. safe value for batteries or engine operation).

NOTE: The alarm and event history files may the combined. For alarm or events, start and clear are recorded, e.g.: mains failure start/clear alarm, engine running start/stop event, power capacity change event.

Different display can be obtained by filtering function or presentation means.

5.1.2 Optional data in the IEM&C network

In addition to the mandatory data described in clause 5.1, the following data are desirable but optional:

- equipment configuration and operating parameters saving and reloading;
- measurement records;
- software download (process and monitoring network elements software's, it may be for upgrading the CU or DGU or LMA);
- management (passwords, networks addresses, calendar-clock synchronization all along the networks);
- dynamic graphical synopsis;
- on line help;
- self diagnosis.

5.2 High level application and data structure flexibility

Equipment shall give the information as described in clause 6 at their monitoring interface in order that telecom operators collect data from heterogeneous equipment and bring the information to a common supervision room or to the Maintenance Mobile Client at any location. The supervision application servers (LMA and RMA) are intended to do treatments, monitoring, remote control and intervention management. Intervention management following alarm or for routine maintenance purpose is one of the major process. Detailed description of maintenance and repair routine is given in TR 102 336 [16]. The process operations needing the management network are:

- alarm start;
- alarm acknowledge (manual function carried out in RMA that starts the fault handling process);
- possible remote corrective command;
- maintenance on site if needed;
- test of the repairing effectiveness;
- alarm clear (end of alarm).

Management functions are provided to obtain a quality process with traceability of alarms or other events and intervention, to avoid repetitive alarm start, loss of alarm, bad repairing and to ensure high availability and dependability of power and cooling systems, and consequently of telecom network.

In addition to alarm, event message, are provided to help to understand failure and to make intervention decisions.

Alarms or events fields are described in clause 9, being based on previous standards described in annex C of TR 102 336 [16] as a result of telecom operator and telecom equipment manufacturer experience.

All the information useful for this quality process is often not available in a single level (i.e. at the XCU). It shall be possible to enrich the information by filling or adding fields at every network level (XCU, DGU, LMA, RMA).

For example, if there is a site local management application (LMA), it has a global site view of several equipment and can add or alter the information:

- site information (address, type, etc.);
- network information (addresses, etc.);
- change the technical severity of alarm compared to single equipment point of view of the technical failure.

Other treatments can also be done at DGU, LMA, or RMA level with influence on the field's contents and type:

- filtering of repetitive events in LMA or RMA;

- classification of alarms in a site by DGU or LMA;
- classification or alarms between site in RMA.

The "intelligent" work will probably be done at different level of the management network, depending on knowledge and co-existence of old and new interface generations, which impact the network functions and organizations.

5.3 Data interface complexity and structure

5.3.1 Information

Considering management requirements and "intelligence" distribution, 3 levels of information details are available at the output of the XCU/DGU:

- Alarm synthesis contacts in a few number. (These contacts e.g. dry voltage free relays or voltage presence signals on the monitored entity and information can be used in loops to be gathered by an acquisition unit. No polling is required to get them on the alarm supervision display).
- Detailed alarm supervision messages are available locally and remotely. These are formatted in messages and tables transferred on a high level and secure protocol.
- System supervision information: available locally and/or remotely. The system supervision extends the alarm supervision to information on systems and allows for detailed information for maintenance and analysis.

The information at the M&C interfaces will be defined in clause 6. The generic descriptions of information structuring not linked to one specific process or protocol is provided in clause 9. These information structures consist of:

- Equipment XCU, DGU self-registration (description and identification file equivalent to MIB object including site, equipment, sub-equipment, services resources such as one single or different XML files types).
- Alarms, events.
- Measurements and values.
- Control (remote command, default values, operation or customized parameters).
- Log files, records.
- Hexadecimal file (program download, help files, etc.).
- Dynamical graphics synopsis.

5.3.2 Status and event

Each component, sub-system or system shall be in one of the following status at any given time:

- Normal: this status is set when the component, sub-system or system is operating in the expected conditions.
- Alarms: this status is set for abnormal state, i.e. different to specified normal state of hardware, software, environment condition (thermal, EMC, etc.). The status "Alarm" is divided in four subcategories and 9 levels (see clause 5.3.3).
- Unknown: this status is set when the information is not available (either not controlled or not communicated).

An event is any change of status of a component, sub-system or system.

5.3.3 Alarm severity and event class

Alarms shall be classified by a severity level (1 to 9) indicating the importance of the fault (partial or total mission failure at the level of equipment, centre, network). This is used by operator on higher management level with other parameters (network impact, service impact, available resources, etc.) to define urgency and classify intervention priority of maintenance work on the site where equipment fail. This severity field is defined in clause 9. The more severe is 9.

This field describes technical severity at low level (equipment or site), but not high level priority decision taken by the operator to handle the alarm and intervention.

NOTE: The level 0 is reserved for event not generating an alarm (for message filtering or sorting purpose).

The fine technical severity levels (0 to 9) can be simplified in qualitative class (see EN 302 099 [4]):

- Critical: reinforced alarm from DGU or LMA for example if correlation of major equipment alarm through the site vision (e.g. presence of 2 major alarms or mains interruption + DEG failure + discharges battery should lead to a new alarm imminent site crash).
- Major: sometime referred as prompt, urgent i.e. the failure event may need an immediate maintenance intervention of the network operator.
- Minor: sometime referred as deferred, non urgent i.e. the failure event may need a maintenance intervention of the network operator but the service can be ensured for long time.
- Warning: sometime referred as hint i.e. an event happens which normally does not need a maintenance intervention of the network operator.

Each of these simple severity shall correspond to a range of values defined by the operator depending on the network impact of failure, equipment criticity, maintenance means, date and daytime, etc.

There shall be a function to change the alarm severity level by the operator and correspondence between simplified classes and fine values.

6 IEM&C management typical content subsets

Figure 3 describes typical subset of infrastructure equipment and thermal environment which are covered in the present standard. Detailed monitoring and control information requirements for each of these subsets are provided in part 2 to 7 of ES 202 336.

This information description method shall be open to other subsets in the future such as battery monitoring devices, high voltage DC power supply, new AC UPS structure, fuel cell system, photovoltaic plant, lightning protection or grounding monitoring, etc.

Every subset (i.e. DC) are generally divided in functions and sub-functions (rectifiers, battery, etc.), with associated information (alarms, events, measurements, parameter sets, controls) described in part 2 to 7 of ES 202 336. The information corresponding to a subset shall be provided at M&C management interface of these subset (generally on CU interface). But for each subset function, the information shall be provided in accordance to the equipment configuration. i.e. there is AC back-up switchgear information only if there is such a function in the AC distribution board equipment.

Each information are described as Mandatory or Optional in part 2 to 7 of ES 202 336. For example, partial AC metering is generally an option used only in large building.

Details on management information choices for each subsets and functions are provided in TR 102 336 [16] and standardized data format in part 2 and following.

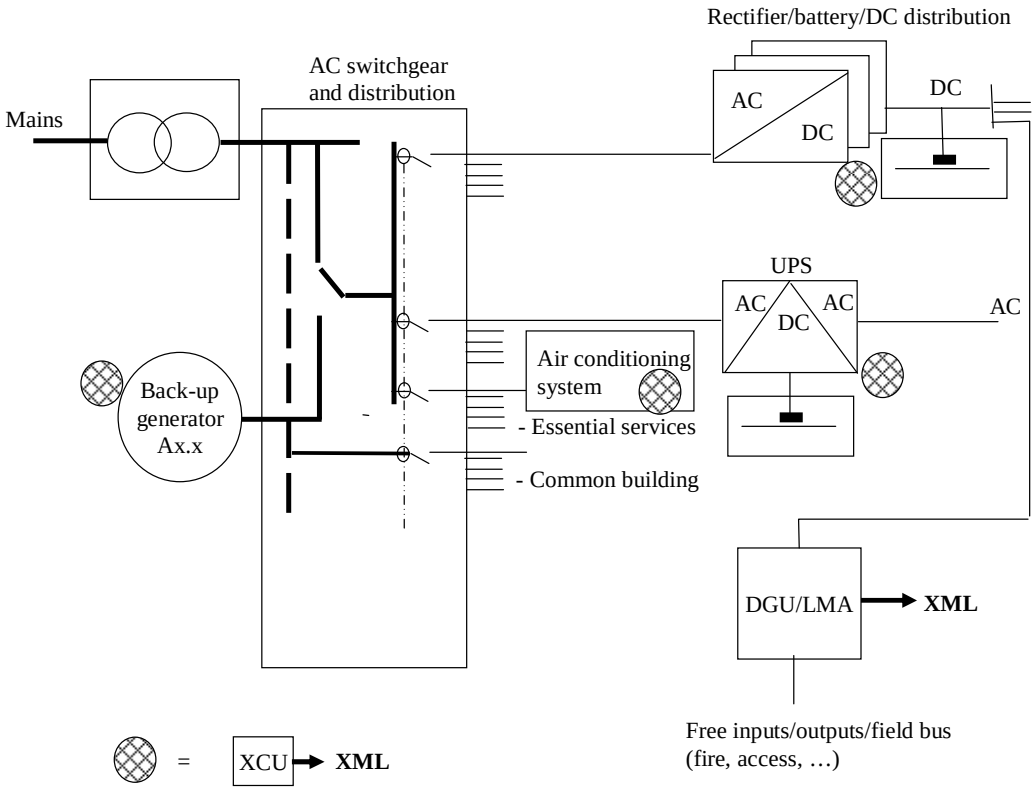


Figure 3: Typical subsets of infrastructure covered in the present document

6.1 DC system (part 2)

The DC system transforms AC interface from mains or back-up engine in DC voltage of interface A defined in EN 300 132-2 [2] or EN 300 132-3 [3] or defined for local or remote power supply of access network equipment in EN 302 099 [4].

DC system main functions are:

- rectifier (one or more in parallel) that converts AC voltage in DC voltage (i.e. 230 VAC to low voltage 48 VDC or high voltage < 400VDC);
- battery (one or more strings of cells) that stores energy and can power the loads when AC interruption or rectifiers failures occur. Test and permanent battery monitoring are of high importance to reduce the MTTR;
- protection and distribution (DC bus, breaker, voltage, current, power, etc.) to power different user loads and discriminate faults.

Several measurements are possible: rectifiers states, rectifier voltage, current, battery voltage, current, temperature, user load currents.

Several controls are possible to adjust rectifier voltage and current, to share the load, to initiate battery test procedure.

Minimal DC system without back-up, and rectifier-battery system M&C data model are described in ES 202 336-2.

6.2 AC distribution switchboard (part 3)

The AC distribution provides AC voltage from mains or backup generator.

It gathers several functions:

- protection made by one or more stage of protective devices;
- optional switch gear between mains and back-up generator;
- circuit breaker control (see note);
- voltage, current, phase shift monitoring;
- optional power and energy metering;
- optional HV/LV transformer monitoring.

NOTE: The circuit breaker control may be used for progressive power load on mains or back-up generator or for partial load disconnection in case of critical situation (e.g. mains and back-up overload condition).

The AC distribution frame or board is covered for high power plants, by a separate group of cabinets. For small power plants, it can be part of the DC cabinet and the back-up Generator. The final loads are a DC system with interface defined in EN 300 132-2 [2], inverters interface defined in ETS 300 132-1 [1], AC or DC interface defined in EN 300 132-3 [3] or UPS in TR 102 121 [15].

Other equipment loads of the AC distribution frame are cooling systems or building services.

There may be several AC bus backed-up or not by the standby supply, e.g. a standby generator.

Minimal AC distribution systems M&C data model is described in ES 202 336 part 3.

6.3 Back-up generator engine (part 4)

The back-up generator is generally of diesel type and is composed of several well defined functions or circuits:

- fuel tank and supply to the engine;
- general engine parameters (speed, temperature, etc);
- coolant circuit (fluid temperature, levels, circulation pumps, air, louvers, etc.);
- oil fluids (pressure, levels, etc.);
- electrical generator parameters;
- starting devices (battery voltage, starting speed, etc.);
- electrical auxiliary circuit (protection, power contactors, etc).

Permanent monitoring even when engine is stopped is performed to reduce the MTTR.

In addition, automatic starting/running test procedure and report are very important as for batteries for engine training and heath check-up.

Minimal AC backup generator M&C data model is described in ES 202 336 part 4.

6.4 AC UPS (part 5)

The AC UPS supplies permanent AC voltage as defined in TR 102 121 [15].

UPS can be static or rotative, but, for the time being, the ES 202 336 part 5 considers only static system.

AC UPS system main functions are:

- rectifier (one or more in parallel) that converts AC voltage in internal DC voltage;
- battery (one or more strings of cells) that stores energy and can power the loads when AC interruption or rectifiers failures occur. Test and permanent battery monitoring are of high importance to reduce the MTTR;
- inverters that converts DC in AC;
- AC/AC active switch between the mains input and the inverter output;
- AC/AC manual bypass used for free of voltage maintenance inside the UPS, without power interruption of the load;
- protection and distribution (AC and DC bus, breaker, voltage, current, power, etc) to power different user loads and discriminate faults.

Several measurements are possible: power modules states, input and output voltage and current, battery monitoring, temperature.

Several controls are possible to adjust voltage and current, to share the load between parallel modules, to initiate battery test procedure.

Minimal UPS M&C data model are described in ES 202 336 part 5.

6.5 External alarms input, other inputs or outputs (part 6)

This subset is for general purpose gathering of building facilities alarms coming from not supervised power or cooling systems, or from some other needs as access or fire protection.

The XCU/DGU shall allow:

- Configuring input-output (alarm message parameters, control parameters, etc.).
- Programming simple relations between them (timer, conditions, etc.).

Minimal facilities M&C data model is described in ES 202 336 part 6.

6.6 Thermal environment and cooling system (part 7)

This subset is for thermal environment monitoring and cooling system.

6.6.1 Thermal environment of equipment rooms

The telecommunication equipment rooms environment conditions (temperature, relative humidity) need to be monitored. Measurement and records shall be done. Minimum precision and frequency are defined. This may apply to access network equipment.

6.6.2 Fan system

Fan systems are cooling systems with no cold creation, but only heat air removal by circulating air from inside to outside though filters or exchanging heat in closed circuit from inside to outside to avoid dust.

With fan systems, detection of motor and louver faults and filters replacing test should be done.

Circuit breaker status shall be monitored and sensors may be used to detect airflow failure.

6.6.3 Cooling system with compressors

Environmental systems that provide a cooling function by using compressors for refrigeration circuits shall be monitored for failure and abnormal operation.

Circuit breaker status shall be monitored as should refrigerant pressures to detect leakage.

In the case of redundant cooling units, a sequencing device should equally share the running time between units.

6.6.4 Chilled water cooling system

Environmental systems that provide a cooling function using chilled water shall be monitored for failure and abnormal operation, e.g. water flow failure/temperature, pumps, valves and fans.

Circuit breaker status shall be monitored.

Water levels should be monitored to detect leakage. Leak detection within telecom facilities should be deployed if any of the cooling system is co-located with the telecom equipment.

All minimal thermal environment and cooling systems M&C data model are described in ES 202 336 part 7.

7 IEM&C management interface and network architecture

Interface and architecture is mainly determined by structuring principles following an OSI model layer approach (Open Service Interconnection) [11]. TCP/IP [10] shall be used for new interface with REST mechanism to exchange XML files or XML formatted data at application layers through http services and http parameters (annex A IEM&C agent) as previously introduced in clause 4.1.

In addition, network element may act as web server in html for direct access from any client post, and use FTP service to download/upload files (program or data).

The choice and difference between ISO-OSI and TCP/IP are more detailed in informative annex F.

Access service PPP over different networks Ethernet - intranet and internet are also introduced in annex F.

Referring to ITU-T Recommendation M.3010 [5], physical and logical network used to connect all units together in the network are DCF and MCF:

- Data Communication Function (DCF) covers the OSI layers 1 to 3. These layers are supported by every entity that has a physical connection to the network.
- Management Communication Function (MCF) covers OSI layers 4 to 7.

The following clauses describe a top (requirement from operators - high level layers) to down approach (technical aspects - low level layers) which explains the data structuring and formatting choice.

7.1 Location of intelligence

The great number of existing infrastructure and equipment in the operator premises, imposes the coexistence of several data interface types.

The preparation of high level readable and synthetic information structure and homogeneous formatting is the "intelligence". This intelligence is distributed through processing units along the management network.

7.2 XCU, DGU, LMA management interface

Based on this exchange protocol over the network, there are several data flows necessary for full TMN service (supervision, management, remote control, information and program back-up, etc.). These data flow can be split in 2 general categories MMI and HMI:

- Machine-Machine Interface (MMI):
  - MMI with equipment: the site machines XCU, DGU, LMA act as a client to get rough information from equipment on field bus or on various physical links using logical formats and protocols (i.e. modbus, jbus, LON, etc.).
  - MMI with remote supervision: the site machines (XCU, DGU, LMA) transmits data as follows:
    - in server mode: data transfer of xml structure on http client request;
    - in event mode: spontaneous sending of information (e.g. alarm, event). The network element acts as a client (POST command in http);
    - in service mode: data integrity test and restore mode, network test, date/time setting. The network Element acts as a server;
    - Detailed transmission exchange mechanisms are in annex A (REST mechanism using http service).
- Human-Machine Interface (HMI):
  - The local server gives readable information and accepts commands (e.g. about the state of the equipment under text or graphical format XML).
  - This may be achieved by XHTML and PHP for dynamic variable value refresh.
- (XSL) for ordering the text and CSS for style sheet should be used to ease evolution of HMI. LMA and RMA may use XLSTb to select parts of a full XML document describing the whole site. By example, it is possible to get only the active alarms, to get only the monitored data of a specific equipment, etc. See annex E.
- In the present document, XSLT will be used to select parts of a full XML document describing the whole site. By example, it is possible to get only the active alarms, to get only the monitored data of a specific equipment, etc.

The more work is done in the equipment CU towards creating a unified protocol, the less the local server or DGU have to do and its configuration management will be easier. At minimum, LMA could be a client of XCU only. LMA acts as a transparent routing unit with the XCU for the RMA, just added a site layer (synopsys, alarm severity re-qualification, etc.).

This interfaces and architecture clause, prepare data for the functions that must be performed at management level. The following clauses will go more in details on the functional requirement for LMA, RMA as performance, safety, data integrity and coherence.

7.3 Interface and protocol diversity

Figure 4 shows where the intelligence can be, depending of the more or less decentralization of intelligence. The location of "intelligence" has high influence on network and server capacity.

Intelligence should be distributed in the equipment XCU or DGU.

Interface and protocol types are the following:

- Low intelligent interface: (see clauses 7.5.1 and 7.5.2 for details) equipment sensors/actuators contact interface or a serial bit stream interface CU. This CU shall be connected to a DGU doing the mediation with a IEM&C agent. The encapsulation of alarms, states or bit stream in transport protocol TCP/IP to be transmitted towards LMA or RMA for high level message creation and for human understanding shall not be used for CU though it can be found in existing network.

NOTE 1: One reason not to encapsulate is that it requires a high data rate and powerful centralized server to keep real time operation with large number of CU.

- High intelligent interface: (see clauses 7.5.3) high level protocol over Ethernet interface is offered on the DGU or XCU. It shall be used at minimum http + XML formatted parameters or XML files exchanged with REST command.

NOTE 2: SNMP is also an existing high intelligent protocol but should not be used because of poor security and poor compatibility with TCP.

- Hybrid intelligent interface: (see 7.5.4) in real sites, the management network shall accept a mixture of every interface type previously described.

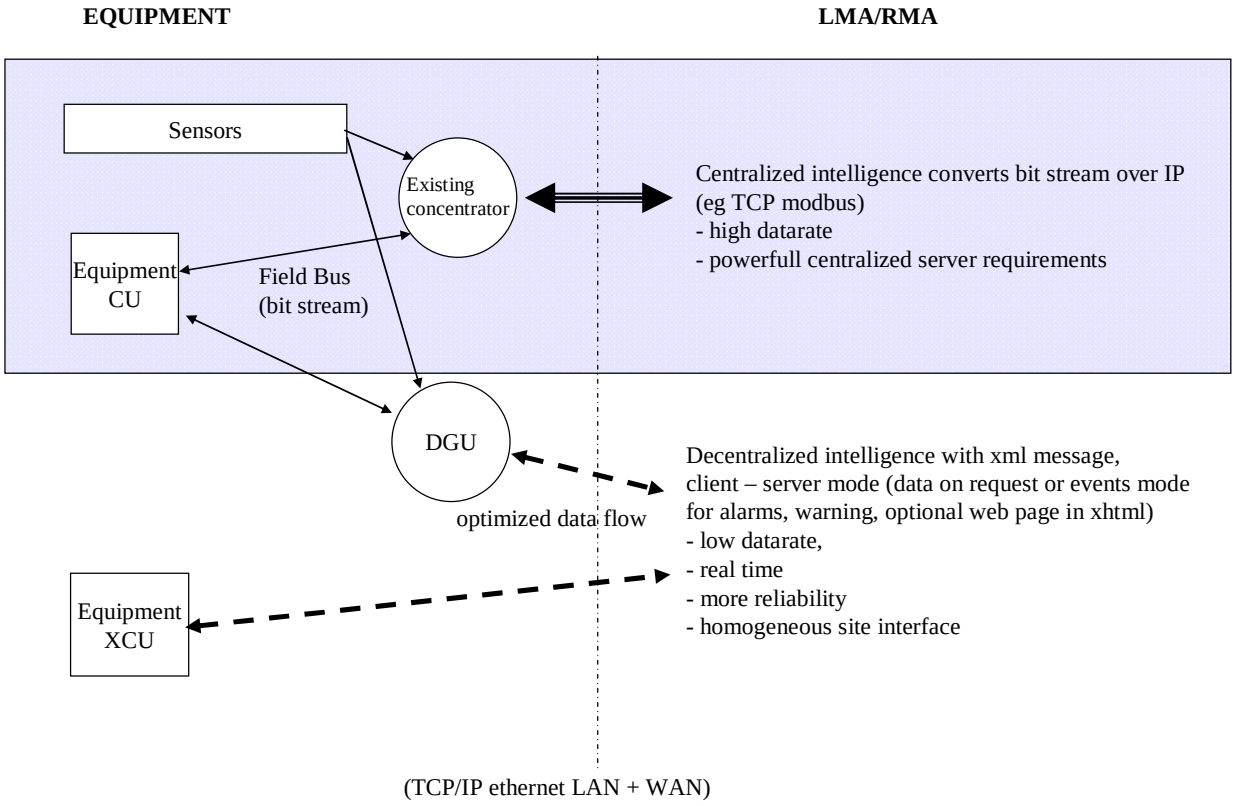


Figure 4: Interface types and intelligence location in the network

7.4 Open interface and software

As a consequence, any new interface of environment equipment, CU, XCU, DGU, LMA or RMA should be open and documented in detail to allow better inter-connection, mediation, inter-operability and further non proprietary software development.

At minimum, full details of interface (data, protocol, format) shall be provided without any restriction.

7.5 Interface levels

7.5.1 Alarm and state loops interface on XCU or DGU output

Equipment and XCUs/DGUs shall provide at least summary of alarms that shall be reliably transferred to the RMA. The alarm network can be different from the control and monitoring network to achieve a higher level of reliability (see figure 1).

Passive reliability: an alarm information is supplied as an open loop in order that a wire disconnection is seen as an alarm start.

If alarm relays are used, the open loop corresponds to the de-energized state of the relay, so that a power failure of the loop interface will set the circuit in alarm status.

3 alarm synthesis loops shall be provided at least at the interface of each equipment, using the qualitative alarm severity defined in clause 6.3.3:

- Major alarm.
- Minor alarm.
- User defined alarm (e.g.: AC mains interruption, second major alarm, warning, etc.).

In addition DGU or LMA that have a global site vision should provide at least another global alarm i.e. critical alarm.

For data coherence, any detailed discriminated alarm available in a message from XCU or DGU shall have correspondence with one of the alarm loops.

As the information interface includes alarm synthesis, as a minimum the availability of the alarm system shall be in accordance with IEC 60839-5-4 [8].

7.5.2 Low level protocol equipment CU mediation by DGU

CU can be an industrial programmable unit that has a field bus interface (binary field protocols like modbus, JBus, LON, CAN etc.). This bus may be of master-slave type or not.

Full detailed description of the bus and data shall be provided by the CU manufacturer.

Alternatively, the manufacturer shall propose a compatible XCU.

The data retrieval and conversion requires more or less work in the DGU to prepare high level user interface: readable and non repetitive standard message, XML interface, etc.

The DGU shall have an Application Protocol Interface (API) in order to enable development of the application by the equipment manufacturer or the DGU manufacturer or a third party.

NOTE: Manufacturer should help in the future to precise some mandatory API.

The bit stream bus can be transmitted to the RMA over TCP. This can be a solution for very small systems (shelters, street cabinets, underground location) where the cost of DGU in addition to CU is a problem, but this should be avoided. The risk is that the dataflow could be very heavy and saturate the network and the remote server.

7.5.3 XCU and DGU high level protocol interface

The XCU receives rough information via sensors, automation field bus and prepares filtered high level interface (standard XML structures, readable by user web pages, historical or measurement data records).

The equipment XCU shall have client and server function with open data protocol http and provide XML formatted data in conformity with clause 9.

For the existing CU, there is not a single standard protocol at the output of CU, and it is not implemented on all existing network or off-the-shelf equipment, so the DGU shall be open and take other protocol in order to integrate a power or cooling unit into a standard network management tool.

If SNMP is used on existing CU it shall be focussed on channelling the alarm information and site information. DGU shall convert SNMP to data structure in conformity with XML in clause 9 and standard equipment data interface part 2 to 7.

7.5.4 Hybrid network element solutions

It is highly probable that there will be a mix of all these interfaces because of a progressive evolution from the existing environment to a more "intelligent" one (see figure 5). Figure 5 shows combined CU, DGU, LMA functions in one unit.

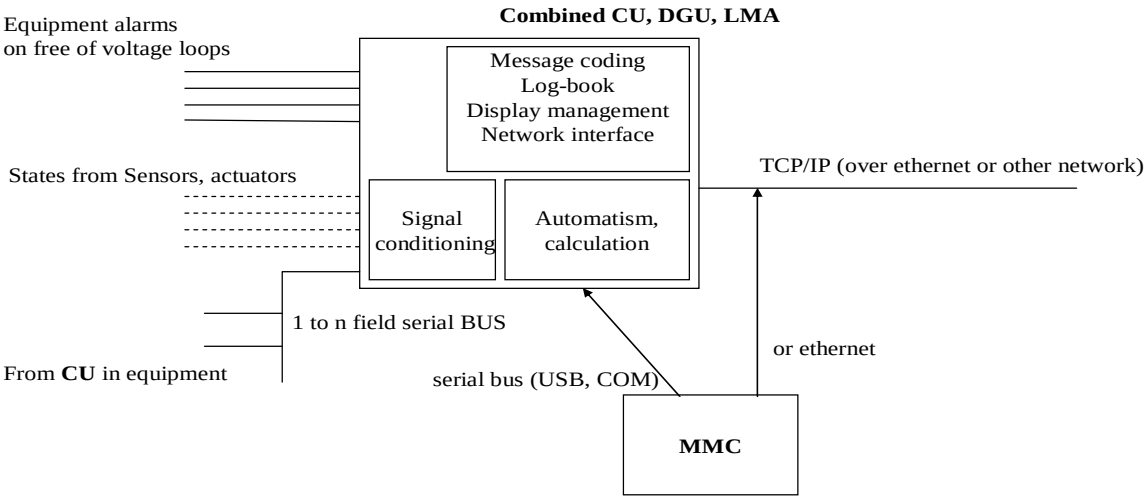


Figure 5: Principle of combined CU, DGU, LMA operation on small site

7.6 Transport Control Layer

Transport 4 layer and session 5 layer shall be TCP over IP for XCU, DGU, LMA or RMA connected to Ethernet LAN.

TCP over IP is also used for LMA or RMA through WAN with PPP services (see annex F).

TCP over IP is named TCP/IP in the following clauses.

7.7 Physical and network layer

In a building where Ethernet is used, Ethernet interface shall be at minimum 10Mb with RJ45 or M12 (IEC 61076-2-101) plug.

The power & cooling management local network should be a dedicated Ethernet, not the office Ethernet for reliability and safety purpose.

Alarm Input/output or monitoring field bus shall have connectors to allow maintenance test and easy replacement. Screw connexions should be used for sensors, actuators or bus interface with limited number of wires. A clear labelling should be used to identify physical link:

- type (RS232, 422, 485);
- logical link type e.g. Modbus;
- wire polarities (+ or - or ground);
- wire functions (transmitter, receiver, shield, clock, etc.)

7.8 Progressive Network Evolution

In Local Management of supervised places, it shall be possible:

- To keep the existing supervised power and cooling equipment without changing their output interfaces (i.e. old CU), adding a DGU that convert old CU protocols towards Ethernet XML.
- To add a new power or cooling equipment with XCU and to add a LMA that can dialog with DGU and XCU.

In Remote Management supervision room:

- It shall be possible, to progressively migrate from old supervision to new ones through Ethernet on an Intranet network.
- Existing X25 [16], POTS, GSM connections may be accepted at RMA level but through acquisition gateway interfacing this to TCP/IP Ethernet. The existing X25 equipment shall be connected though Ethernet with a gateway to the new M&C TCP/IP RMA (e.g. X25 in TCP/IP over ADSL).
- Existing higher level analysis and statistical application servers shall be able to get data though database interface with the new M&C RMA.

A laptop (MMC) can be connected anywhere on Ethernet or by direct connection to local equipment or to a distant client.

Figure 6 shows an example of compatibility with existing management networks.

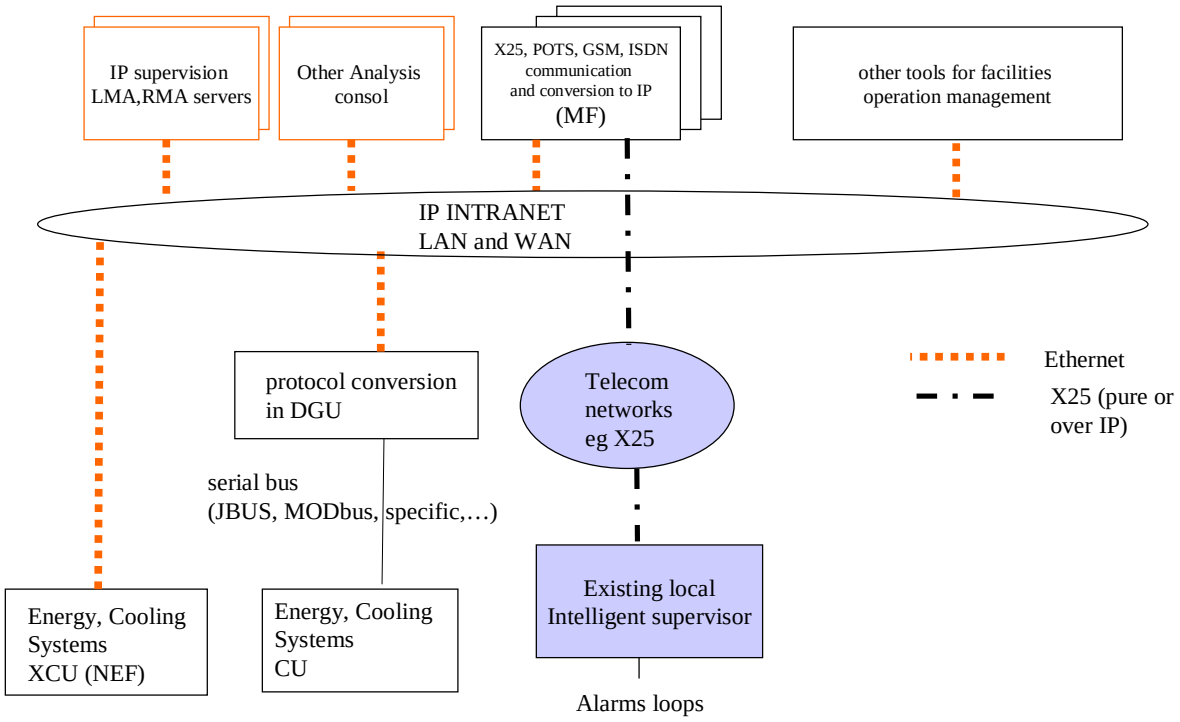


Figure 6: Principle of progressive evolution towards a unified supervision network (TCP/IP XCU, LMA, and RMA)

8 Supervisor functions and performance

The architecture and functions of LMA and RMA help the operator to increase the reliability and dependability of power and cooling system because in telecom network and servers concentration, the impact of a blackout can be countrywide. Another important target is to reduce the cost of energy, equipment and maintenance (e.g. reducing transportation to site), by a better sizing and efficiency for a sustainable development.

LMA shall at minimum provide:

- monitoring of several equipment on one site;
- a local site view with alarms and equipment states;
- data or message log functions;
- alarm notification towards RMA or local physical device.

RMA shall at minimum provide:

- monitoring of several site;
- a multi site view with alarms and equipment states;
- alarm notification mechanism.

Some of these functions (alarm notification, monitoring display, event logs and records) may be done also in XCU or DGU.

As a consequence recommendation for the generic following functions are provided:

- common XML format information stored in database as variables;
- site and equipment state display (web pages for example): web server on the intranet and/or through a (PSTN, ISDN or ADSL) modem from anywhere with defined logging control;
- access right administration for remote monitoring or control;
- synchronization of date-time of every device creating information events;
- help checklists associated to alarm to help to find possible failure origin and improve MTTR;
- events correlation is possible for expert analysis purposes; (quality, traceability);
- equipment tests results automatically checked;
- specific variables record to help diagnosis and analysis;
- tools for management of the equipment configuration, synopsis creation, messages (user can use and enrich a library of useful data as MIB, graphics, etc. to reduce design time and errors).

Alarm transfer shall comply requirement of IEC 60839-5-4 [8] 8].

In addition, for compatibility with existing supervision systems, the LMA and RMA shall be an open server to several protocol and application. It may be open to SNMP, OPC, .net.

- Network Element data reliability and coherence recommendations are in annex B.
- Network Element functional recommendations are in annex C.
- Network Element response time and capacity recommendations are in annex D.

9 Data Structure Format and Syntax of the XML Document, For Exchange Between CU or DGU and LMA or RMA by IEM&C agent

As the structure of a XML document is really free, the present clause describes some rules which shall be respected. This describes by example the structure of an alarm and the place at which it shall be placed. This part describes the XML document which shall be generated by a DGU. XCU will generate parts of this XML document, e.g. some field such as site Id are not available in XCU and should be added at a higher level of the management network.

The encoding of the XML document shall be given with the following standard line, as shown further. The present document recommends the use of "UTF8" encoding.

```
<?xml version="1.0" encoding="UTF8"?>
```

For people unfamiliar with the standard XML format and related terms, annex F gives an overview of the XML.

9.1 The description of XML elements

In the present document, the children and/or the attributes of an XML element are described with the help of a table. This one has one row by child/attribute. The "Description" column describes the element. The "Datatype" column specifies the type of data (see standard Datatype related to the XML language) contained in the child/attribute element. The "O/M" column is used to define if the child is mandatory (M) or optional (O). Example is given in table 1.

Table 1: Example of XML elements description

Child/Attribute element	Description	Datatype	O/M
<child_1>	The child 1 description	xs:string	M
<child_2>	The child 2 description	xs:decimal	O
<child_3>	The child 3 description	xs:complexType	M
<child_4>	The child 4 description	xs:complexType	O

9.2 The order of the XML elements

The children of an element must be ordered in the same order as in the tables defining the allowed children. If a child is optional, it does not need to be present. Also, any child can be present more than once, if the attribute "id" is different (see standard attributes).

If we take the example table of the previous clause, we could have for example:

- One child of each type:

```
<parent id="3">
    <child_1>A string</child_1>
    <child_2>23.456</child_2>
    <child_3>
        …
    </child_3>
    <child_4>
        …
    </child_4>
</parent>
```

- Only the mandatory children:

```
<parent id="3">
    <child_1>A string</child_1>
    <child_3>
        …
    </child_3>
</parent>
```

- Multiple children "child_3":

```
<parent id="3">
    <child_1>A string</child_1>
    <child_3  id="1">
        …
    </child_3>
    <child_3  id="2">
        …
    </child_3>
    <child_3  id="3">
        …
    </child_3>
    <child_4>
        …
    </child_4>
</parent>
```

9.3 The hierarchic rule

A **hierarchy** is a series in which each **element** is graded or ranked i.e. each element has a level in the hierarchy.

The highest level called root level corresponds to the **level** 0 and relate to a site. A sub element of an element is called a **child**. A child of an element of hierarchy level 0 has a hierarchy level of 1. Infinity of hierarchic levels can be defined like this. An element of hierarchic level of 3 can be called as the **parent** of the element of hierarchic level 4.

Figure 7 gives an illustration of this concept applied to EE M&C of a site. In this illustration, colours reflect the level of hierarchy.

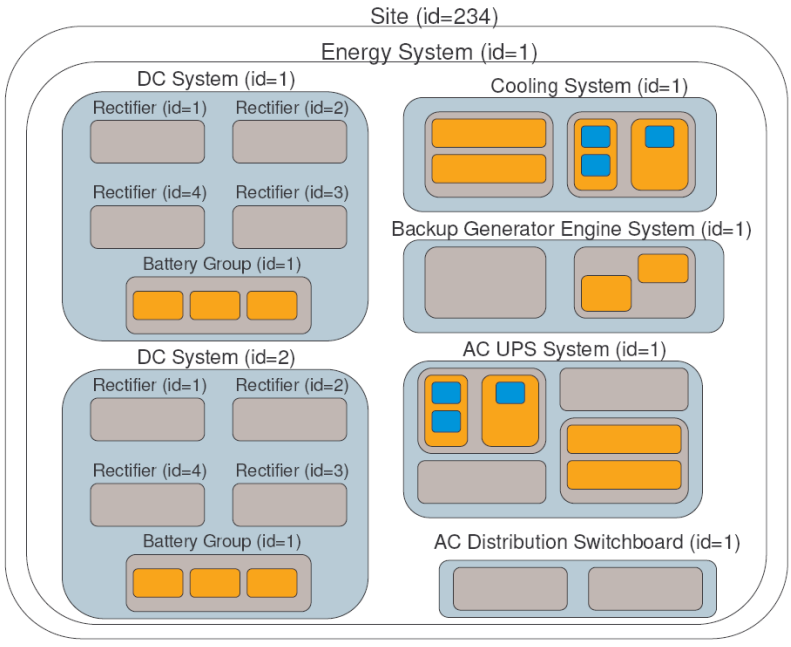


Figure 7: Element hierarchy example

The XML document shall reflect this hierarchy. For example, a DC system cannot be at the same level of hierarchy as a site. This rule allows a very flexible structure to describe any type of site.

The root element of the XML document generated by the highest unit of a site (DGU or LMA or XCU for small site) shall be <site> with attribute Site_location, equipment mapping, user_reference.

When multiple equipments/systems of the same type are present under one element, an identification number shall be used to easily distinguish and access the different elements.

The data type of the identification number shall be "xs:integer".

EXAMPLE:

```
<a_system id="3">
    <an_equipment id="1">
        …
    </an_equipment>
    <an_equipment id="2">
        …
    </an_equipment>
    <an_equipment id="3">
        …
    </an_equipment>
    <another_equipment id="1">
        …
    </another_equipment>
</a_system>
```

9.4 Standard elements of any equipment, system or subsystem

9.4.1 Standard elements

For each equipment, system or subsystem, the attributes are defined in table 2.

Table 2: Element attributes definition

Attribute	Description	Datatype	O/M
id	The id of the equipment, system or subsystem.	xs:integer	M
status	"normal" or "alarms" or "unknown". For any detailed alarm (clause 9.4.2) the equipment is in alarm status	xs:string	M
severity_type	If status is "alarms", this attribute gives the more severe "severity type" of the table of alarm. This attribute shall be present only when the attribute status is "alarms".	xs:string	M
severity_level	If status is "alarms", this attribute gives the more severe "severity level" of the table of alarm. This attribute shall be present only when the attribute status is "alarms".	xs:integer	M
short_description	A very short description of the equipment	xs:string	O
datetime	The datetime attribute can be used to know the date and the time at which the element was refreshed. It is possible to have different datetime in different elements because all the equipment/systems cannot provide the data at the same time.	xs:datetime	O

For each equipment, system or subsystem, child elements that can be used are described in table 3.

Table 3: Child element definition

Child Element	Description	Datatype	O/M
<description_table>	A table with description elements of the equipment/system.	xs:complexType	O
<alarm_table>	The table of alarms related to the equipment/system	xs:complexType	O
<event_table>	A log of events related to the equipment/system	xs:complexType	O
<data_table>	The table of the data (measurements, states and calculated values) related to the equipment/system	xs:complexType	O
<data_record_table>	Records of the historic of some data present in the data table	xs:complexType	O
<config_table>	The table of configuration of the equipment	xs:complexType	O
<control_table>	The table of control of the equipment	xs:complexType	O

All these complex type structured elements are described further.

NOTE: The information of very simple equipment with just 2 dry alarms (major, minor) could be stored by a XCU.

This simple equipment has no sub elements. For example:

<simple_equipment **id**="4" **status**="alarms" **severity_type**="major" **severity_level**="4 **datetime**="2006-12-15T15:34:23Z"/>

<simple_equipment **id**="5" **status**="normal" **datetime**="2006-12-15T15:34:23Z"/>

9.4.2 Alarm and event message

An alarm or event from the DGU/CU will be forwarded to the management application LMA/RMA in XML structured data format.

EXAMPLE:

Alarms or events messages can be posted without waiting a polling from LMA or RMA.

The event and alarms are composed of elements or fields of ITU-T Recommendation X.733 [7] corresponding to XML tags and attributes.

The result of XML structured data interface might be for example a complete record in mySQL database of RMA as described in table 4.

Table 4: Alarm and Event elements or fields in compatibility with ITU-T Recommendation X.733

SUB-ELEMENTS description of alarm field	Allowed Attributes	FORMAT Based on MySQL databyte	Example	CLASS O/M)	COMMENTS
Generic Message					
<site_id>		Varchar 16	Orvietto	M	The site ID shall be downloaded for each DGU/XCU from LMA/RMA. (ITU-T Recommendation X.733 [7])
<sending_equipment_id>		Varchar 16	XCU	M	This field identified alarm sending equipment. It can be XCU, DGU, LMA, RMA and its number

SUB-ELEMENTS description of alarm field	Allowed Attributes	FORMAT Based on MySQL databyte	Example	CLASS O/M)	COMMENTS
<equipment_mapping>		Varchar 24	cabinet 05room224	M	This is the localisation of the environment equipment with alarm or event. It can be DC cabinet N° x in room y.
<message_id>		Text	A2	M	This alpha-numerical chain defines the alarm with a unique ID defined by the XML path to the alarm or event element
<date>		Date (DD/MM/YYYY)	27/03/2007	M	DD=01 to 31, MM = 01 to 12, YYYY > 2005
<time>		Time (HH:MM:SS)	23:14:25	M	HH=00 to 24, MM=0O to 60, SS=00 to 60
<message_type>		Enum (Event, Alarm, Clear)	Alarm	M	Message type: alarm start, alarm clear or event with no start/clear. E.g. of event: equipment start.
<event_text>		Varchar 32	low level battery	M	Free text
<severity_level>		TinyInt	7	M	value from 1 to 9 for alarm, 0 for event 9=highest severity
<severity_type>		Varchar 16	Major	M	Text describing alarm (alarm start /alarm clear and qualitative severity level): Critical, Major, Minor, Warning This may be combined with Tag 4 in a smart expression (as in ITU-T Recommendation X.733 [7]): Equipment failure Start: $$$, $$,$ Equipment failure Clear: ###,##,## Network failure: ***,**,*
<equipment_category>		Varchar 8	ENE	M	The management system will translate the code number to the appropriate Equipment category, e.g. ENE for energy
<sequence_number>		SmallInt	25697	M	Message sequence number (0 to 65535) used to keep chronology in case of clock system or synchronization failure. This is also useful to ease message classification and retrieve procedure on LMA/RMA
<acknowledge_ request>		Boolean	1	O	1 = requested
Options For Helping					
<technical_indication>		Text (Alpha-numerical characters)	Persistent discharged current	O	Short complementary help line
<help_file>		Text (Alpha-numerical characters)	You should immediately recharge your battery	O	Long help file (text+graphical+internet link)
<URL>		Text (URL address)	*http://helpfileDCTP2A2.com*	O	Link to internet help

SUB-ELEMENTS description of alarm field	Allowed Attributes	FORMAT Based on MySQL databyte	Example	CLASS O/M)	COMMENTS
<value>		Float8	44,5	O	Decimal value e.g. 1234.56
	unit=	Varchar 8 (preferred in international unit system).	V	O	The units of measure of the Value parameter
	trend	Varchar16	Very low	O	E.g. Vhigh, High, Low, Vlow
<trigger_value>		Float 8	44,6	O	Threshold value to trig the alarm
	Trigger_ condition=	Varchart8	<	O	Element defining how to trig the alarm: [<, >, =, !=].
<status_element>		Varchar 8		O	On or Off or 1 or 0 or whatever
<reset_value>		Float8	50	O	Element allowing the reset of the alarm
<reset_condition>		Varchar 8	>	O	Element defining how to reset the alarm: [<, >, =, !=]
<filtering_timeout>		Varchar 8	60000	O	Time delay used to filter false alarms (in milliseconds)
<associated_relay>		Varchar 2	1	O	Relay number, indicating which system relay is physically associated to this alarm.

9.4.3 The <description_table> element

This element contains multiple <description> elements. It correspond to the table the description elements of the system/equipment.

The inner text of the <description> element is the data of the description.

The allowed attributes of the <description> element are:

Attribute	Description	Datatype
id	The id of the description, it shall be different for all the description, it correspond at the key of the table.	xs:integer
name	The name in English of the description element	xs:string
group	This attribute provide a way to group descriptions of a same category when they are displayed. By example, description related to the manufacturer of equipment could be grouped with the attribute value "Manufacturer".	xs:string
subgroup	This attribute allows to group data under the parent group	xs:string
unit	When a physical data must be represented, it is useful to know the unit of the data. By example, to describe the maximum output power of a dc system, the value of the attribute unit can be "watt". The units allowed by the present document are the same as the one of the International System Units.	xs:string
datatype	The format of the inner text. It can be any valid datatype ("xs:decimal", "xs:boolean", etc). This allows the parsing of the value if necessary.	xs:string
info	Short additional information on the parameter	xs:string
name_XX	The translation of the English name, where XX correspond to the abbreviation of a language. By example, name_fr represents the translation in French of the name attribute.	xs:string

EXAMPLE:

```
<description_table>
    <description id="1" name ="Manufacturer Name" group="Manufacturer">Best Manufacturer</description>
        …
    <description id="4" name ="Serial Number" group="Manufacturer">45623-5F-EG</description>
        …
    <description id="7" name ="Max Output Power" group="Manufacturer" subgroup="Specifications"
unit="watt">850</description>
        …
    <description id="10" name ="Reference" group="User">SEP1245-DC</description>
</description_table>
```

ETSI recommends the use of the followings descriptions for any equipment/system.

General Information:

Name	Group	Subgroup	Description	M/O
Name	General		The name of the system/equipment	M
Reference	General		Reference of the equipment given by the user	O
Short Description	General		A short description of the system/equipment	O
Mapping	General		This is the relative localisation of the equipment/system	O

Maintenance Information:

Name	Group	Subgroup	Description	M/O
Reference	Maintenance		An internal reference	O
Documentation	Maintenance		A link to the user documentation of the product	O
Purchase Date	Maintenance		The purchase date of the equipment/system	O
Installation Date	Maintenance		The installation date of the equipment/system	O
Last Maintenance Date	Maintenance		The date of the last maintenance	O
Next Maintenance Date	Maintenance		The date of the next maintenance	
Comment	Maintenance		A comment on the maintenance	O

Manufacturer Information:

Name	Group	Subgroup	Description	M/O
Manufacturer Name	Manufacturer		The name of the manufacturer	O
Product Name	Manufacturer		The commercial name of the product	O
Short Description	Manufacturer		A short description of the product written by the manufacturer	
Reference	Manufacturer		The internal manufacturer reference of the equipment/system	O
Serial Number	Manufacturer		The serial number of the system/equipment	
Manufacturing ID	Manufacturer		The manufacturing ID of the system/equipment	
Manufacturing Date	Manufacturer		The manufacturing date of the system/equipment	
Documentation	Manufacturer		A link to the documentation of the equipment/system	

9.4.4 The <alarm_table> element

This element contains multiple <alarm> elements. It corresponds to the table of all the possible alarms, with the associated severity type and severity level.

The information about the alarm is included in the attributes of the <alarm> element.

Attribute	Description	Datatype	O/M
id	The identification number of the alarm	xs:integer	M
active	This value is "true" if the alarm is active or "false" if the alarm is not active.	xs:boolean	M
name	The name of the alarm	xs:string	M
severity_type	Can be: critical major minor warning information	xs:string	M
severity_level	Value from 0 to 9	xs:integer	M
start_time	The date and time at which the alarm has started	xs:datetime	O
stop_time	The date and time at which the last active alarm has stopped. (When an alarm is active, this attribute cannot be present as it is nonsense).	xs:datetime	O
acknowledge_ requested	If the agent is configured to request an acknowledgement, this Boolean value will be true. true = requested, false = not requested	xs:boolean	O

EXAMPLE:

```
<alarm_table>
    <alarm id="1" active="false" name ="DC bus Low" severity_type="major" severity_level="5"/>
        …
    <alarm id="3" active="true" name ="Mains Fail" severity_type="major" severity_level="5" start_time="2006-
12-17T18:23:12Z"/>
</alarm_table>
```

Generally, the <alarm> has no child, except if the alarm requests more information for helping. In this case, the allowed child elements are:

Child element	Description	Datatype	O/M
<technical_indication>	Short complementary help line	xs:string	O
<documentation>	Link to internet help, or larger complementary help line	xs:string	O
<data>	the data related with the alarm, as described in clause about <data_table> element	xs:complexType	O
<trend>	E.g. Vhigh, High, Low, Vlow	xs:string	O
<trigger_value>	Threshold value to trig the alarm (in the same unit as the <data> related element	xs:decimal	O
<trigger_condition>	Element defining how to trig the alarm: [<, >, =, !=].	xs:string	O
<status_element>	On or Off or 1 or 0 or whatever	xs:string	O
<reset_value>	Data value allowing the reset of the alarm (in the same unit as the related <data> element)	xs:decimal	O
<reset_condition>	Element defining how to reset the alarm: [<, >, =, !=]	xs:string	O
<filtering_timeout>	Time delay used to filter false alarms (in milliseconds)	xs:string	O
<associated_relay>	Relay number, indicating which system relay is physically associated to this alarm.	xs:string	O

9.4.5 The <event_table> element

The <event_table > element is the parent of <event> elements, described as follows: an <event> element can only exist as a child of an <event_table>.

The inner text of the <event> element is a string (xs:string) describing the event.

The event element has the followings attributes.

Attribute	Description	Datatype	O/M
id	The id of the event	xs:integer	M
sequence_number	Event sequence number (0 to 65535) used to keep chronology in case of clock system or synchronization failure. This is also useful to ease message classification and retrieve procedure on LMA/RMA.	Xs:integer	M
type	The type of event, can be: alarm start alarm clear information	xs:string	M
datetime	The date and time at which the event has happened	xs:datetime	M
severity_type	This attribute exist if the event concern an alarm. Than, the severity type value is the one of the corresponding alarm.	xs:string	O/M
severity_level	This attribute exist if the event concern an alarm. Than, the severity level value is the one of the corresponding alarm.	xs:integer	O/M
alarm_id	This attribute exist if the event concern an alarm. Than, the alarm_id value is id of the alarm in the alarm table of the equipment.	xs:integer	O/M
acknowledge_ requested	If the agent is configured to request an acknowledgement, this boolean value will be true. true = requested, false = not requested	xs:boolean	O
info	Any additional information	xs:string	O

EXAMPLE:

```
<event id="1" type="information" datetime="2006-12-17T18:23:12Z">Equipment started</event>

<event id="2" type="alarm_started" severity_type="major" severity_level="5" alarm_id="2" datetime="2006-12-17T19:25:12Z">Alarm started: Mains fail</event>

<event id="3" type="alarm_stopped" severity_type="major" severity_level="5" alarm_id="2" datetime="2006-12-17T20:25:12Z">Alarm stopped: Mains fail</event>
```

9.4.6 The <data_table> element

This child contains multiple <data> elements. Each of these elements is identified by a unique id. The table is specific for each equipment, and describes by itself the all the available data related to this equipment.

The inner text of the <data> element is the value (xs:string) corresponding to the data.

The <data> element has the followings attributes.

Attribute	Description	Datatype	O/M
id	The id of the data, must be different for all the data, it correspond at the key of the table.	xs:integer	M
name	The English name of the data (standardized)	xs:string	M
group	This attribute provide a way to group data of a same category when they are displayed. By example, data related to the output of equipment could be grouped with the attribute value "output". All the temperature measurements could be grouped under "temperature".	xs:string	O
subgroup	This attribute allows to group data under the parent group	xs:string	O
Type	The type of data, this can be "measurement" or "calculated_value"	xs:string	O
Unit	When a physical data must be represented, it is useful to know the unit of the data. The units allowed by the present document are the same as the one of the International System Units.	xs:string	O
accuracy	Small text describing the accuracy of the data	xs:string	O
measurement_type	For electric and other measurement, there are multiple ways to measure a physical quantity. The following list gives the standardized measurement_type value: peak (the peak value) peak_to_peak (the peak to peak value) rms (the root mean square value) max (the maximum value) min (the minimum value)	xs:string	O
Datatype	The format of the inner text: can be any valid datatype ("xs:decimal", "xs:boolean", etc). This allows the parsing of the value if necessary.	xs:string	O
datetime	The date and time of the data recording	xs:datetime	O
info	Short additional information on the parameter	xs:string	O
name_XX	Where XX is correspond to the abbreviation of a language. By example, name_FR represents the translation in French of the name attribute.	xs:string	O

EXAMPLE:

```
<data id="1" name="Output Voltage" type="measurement" unit="volt" accuracy="1%" format="xs:decimal"
datetime="2006-12-17T18:23:12Z" name_FR="Tension de sortie">54</data>
```

The allowed name must be standardized for each type of equipment.

9.4.7 The <data_record_table> element

This child contains multiple <data_record> elements.

The <data_record> element has the same attributes as the <data> element, except for the datetime attributes which does not exist at this level.

The <data_record> is composed of multiple elements <data>. The inner text of the <data> element is the value of the data. Each <data> element must only have 2 attributes. The other attributes are already present at the <data_record> level.

Attribute	Description	Datatype	O/M
id	The unique id.	xs:integer	M
datetime	The date and time of the data recording	xs:datetime	M

```
<data_record_table>
    <data_record id="1" name="Output Voltage" type="measurement" unit="volt" accuracy="1%">
        <data id="1" datetime="2006-12-17T18:23:12Z">54</data>
        <data id="2" datetime="2006-12-17T18:24:12Z">53.5</data>
        <data id="3" datetime="2006-12-17T18:25:12Z">53.3</data>
        <data id="4" datetime="2006-12-17T18:26:12Z">54.2</data>
        <data id="5" datetime="2006-12-17T18:27:12Z">54.1</data>
    </data_record>
    <data_record id="56" name="Output Current" type="measurement" unit="ampere" accuracy="2%">
        <data id="1" datetime="2006-12-17T18:23:12Z">34.34</data>
        <data id="2" datetime="2006-12-17T18:24:12Z">23.54</data>
        <data id="3" datetime="2006-12-17T18:25:12Z">34.2</data>
        <data id="4" datetime="2006-12-17T18:26:12Z">23.4</data>
        <data id="5" datetime="2006-12-17T18:27:12Z">12.3</data>
    </data_record>
 </data_record_table>
```

9.4.8 The <config_table> element

This child contains multiple <config> elements. Each of these elements is identified by a unique id. The table is specific for each equipment, and describes by itself the entire available configurable element related to this equipment.

The inner text of a <config> element is the value (xs:string) corresponding to the config parameter.

The <config> element has the followings attributes.

Attribute	Description	Datatype	O/M
id	The unique id of the config element, it corresponds at the key of the table.	xs:integer	M
name	The English name of the configuration parameter	xs:string	M
group	This attribute provide a way to group config element, like for the <data> elements	xs:string	O
subgroup	This attribute allows to group data under the parent group	xs:string	O
type	The type of data, this can be "measurement" or "calculated_value"	xs:string	O
unit	The unit of the config parameter	xs:string	O
accuracy	Small text describing the accuracy of the data	xs:string	O
datatype	The format of the inner text: can be any valid datatype ("xs:decimal", "xs:boolean", etc). This allows the parsing of the value if necessary.	xs:string	O
datetime	The date and time of the last modification of the parameter	xs:datetime	O
info	Short additional information on the config parameter	xs:string	O
name_XX	Where XX is correspond to the abbreviation of a language. By example, name_FR represents the translation in French of the name attribute.	xs:string	O

9.4.9 The <control_table> element

This child contains multiple <control> elements. Each of these elements is identified by a unique id. The table is specific for each equipment/system, and describes by itself the entire available control element related to this equipment.

Writing to a control element is similar to start a function of the equipment. For example it can be used to start a battery test, to acknowledge alarms, upload alarms, etc. The target of the write is the inner text of the <config> element. If the argument to pass at the function is complex (a firmware for example), complex datatype can be used.

The inner text of a <control> is always empty in the read xml document, but is used to pass arguments to the control function.

The <config> element has the followings attributes.

Attribute	Description	Datatype	O/M
id	The unique id of the config element, it corresponds at the key of the table.	xs:integer	M
name	The English name of control function	xs:string	M
group	This attribute provide a way to group function element, like for the <data> elements	xs:string	O
subgroup	This attribute allows to group data under the parent group	xs:string	O
state	The state of the function (standby, stopped, started, finished, etc)	xs:string	M
datetime	The date and time of the last execution of the command	xs:datetime	O
info	Short information on the control function	xs:string	O
name_XX	Where XX is correspond to the abbreviation of a language. By example, name_FR represents the translation in French of the name attribute.	xs:string	O

9.4.10 Example: XML document related to a generic equipment

```
<generic_equipment id="3" status="alarms" severity_type="major" severity_level="4" refresh_datetime="2006-12-15T15:34:23Z" >
    <description_table>
        <description id="1" name="aname" … >The Value</description>
            …
    </description_table>
    <alarm_table>
        <alarm id="1" active ="true" name ="alarm name 1" severity_type="major" severity_level="5" start_time="2006-12-15T14:23:12Z"/>
        <alarm id="2" active ="false" name ="alarm name 2" severity_type="major" severity_level="5"/>
        <alarm id="3" active ="false" name ="alarm name 3" severity_type="major" severity_level="5"/>
            …
    </alarm_table>
    <event_table>
        <event id="" …./>
        …
    </event_table>
    <data_table>
        … about measurement and states of the generic equipment …
    </data_table>
    <data_record_table>
        … about measurement logging and state logging of the generic equipment
    </data_record_table>
    <config_table>
        …
    </config_table>
    <control_table>
        …
    </control_table>
    <another_equipment id="1" status="alarms" severity_type="major" severity_level="5">
        …
    </another_equipment>
    <yet_another_equipment id="1" status="alarms" severity_type="normal">
        …
    </ yet_another_equipment>
</generic_equipment >
```

9.5 XML Document Compliance Verification

A XML Schema (XSD) can be used to check the compliance of an XML document with the present document. This XSD file shall be made by ETSI EE and shall be available and maintained on a web server.

NOTE: Information on XSD can be found in annex E.

9.6 The <site> element

As introduced previously, the root element of the XML document is <site>. This <site> element can have standard attributes as described in the previous clause.

The specific child elements of a <site> are:

Child element	Description	Datatype	M/O
<energy_system>	Any type of energy system	xs:complexType	M

Other child element could be defined in future extension of the present document.

The <energy_system> element is described in the next clause.

Here follows an example of XML document, with some of the standard elements introduced previously.

```
<?xml version="1.0" encoding="UTF8"?>
<site id="34" status="alarms" severity_type="minor" severity_level="3" datetime="2006-12-15T15:34:23Z" >
    <description_table>
        …
    </description_table>
    <energy_system id="1">
        …
    </energy_sytem>
</site>
```

If there is more than one energy system, the XML structure becomes:

```
<?xml version="1.0" encoding="UTF8"?>
<site id="34" status="alarms"  severity_type="minor" severity_level="3" datetime="2006-12-15T15:34:23Z" >
    <description_table>
        …
    </description_table>
    <energy_system id="1">
        …
    </energy_system>
    <energy_system id="2">
        …
    </energy_system>
</site>
```

9.6.1 Recommendation about the <description_table> of the <site> element

Here follows some list of <description> elements recommended by ETSI.

General description:

Name	Group	Subgroup	Description	M/O
Name	General		The name of the site	M
Short Description	General		A short description of the site	M

The Address of the site:

Name	Group	Subgroup	Description	M/O
Street	Address		The street	O
City	Address		The city	O
State	Address		The state	O
Province	Address		The province	O
Postal Code	Address		The postal code	O
Country	Address		The country	O
Region	Address		The region	O
Room	Address		Additional information about the location of the room, for example: "floor 4, room 5A"	O

The GPS position of the site:

Name	Group	Subgroup	Description	M/O
Latitude	GPS Position		The latitude, in decimal degree. The value is comprised between [-90, +90]	O
Longitude	GPS Position		The longitude, in decimal degree. The value is comprised between [-180, +180].	O
Altitude	GPS Position		The altitude, in meters above the sea (can be negative)	O

9.7 The <energy_system> element

This element is introduced to gather systems and equipments related to the Energy. It allows to distinguish different group of energy systems, but also to extend the standard with other kind of systems.

The specific child elements of an <energy_system> are described in detail in the part 2 and followings of the present document. The specific elements are:

Child element	Description	Datatype	M/O
<dc_system>	A DC System (Described in part 2)	xs:complexType	O
<ac_distribution_switchboard>	An AC distribution switchboard (Described in part 3)	xs:complexType	O
<backup_generator_engine_system>	A back-up generator engine (Described in part 4)	xs:complexType	
<ac_ups_system>	An AC UPS (Described in part 5)	xs:complexType	O
<general_inputs_outputs>	General inputs and outputs system (Described in part 6)	xs:complexType	O
<thermal_system>	An environment monitoring and/or cooling system (Described in part 7)	xs:complexType	O

An example of corresponding XML structure, with some standard element, containing one element of each of the previous element is:

```
<energy_system id="1" status="normal">
    <description_table>
        …
    </description_table>
    <dc_system id="1" status="normal">
        …
    </dc_system>
    < ac_distribution_switchboard  id="1" status="normal">
        …
    </ ac_distribution_switchboard >
    < backup_generator_engine_system id="1" status="normal">
        …
    </backup_generator_engine_system>
    <ac_ups_system id="1" status="normal">
        …
    </ac_ups_system>
    <general_inputs_outputs id="1" status="normal">
        …
    </general_inputs_outputs>
    <thermal_system id="1" status="normal">
        …
    </thermal_system>
</energy_system>
```

Annex A (normative): Communication between LMA/RMA and IEM&C agent using REST

REST is a REpresentational State Transfer used to convey the data described by the XML documents. REST is an http Remote Procedure Call (RPC) protocol based on HTTP/1.1, defined in RFC 2616 [10]. REST is described in bibliography.

HTTPS shall be used for security reason in LMA, RMA. HTTPS should be used in XCU, DGU if these unit have enough performances.

An authentication mechanism is required on any unit.

HTTP is a request/response protocol. A client/server model will be used to illustrate this communication flow within this annex.

Figure A.1 describes the client-server interaction between the different elements. Each unit can be server or client.

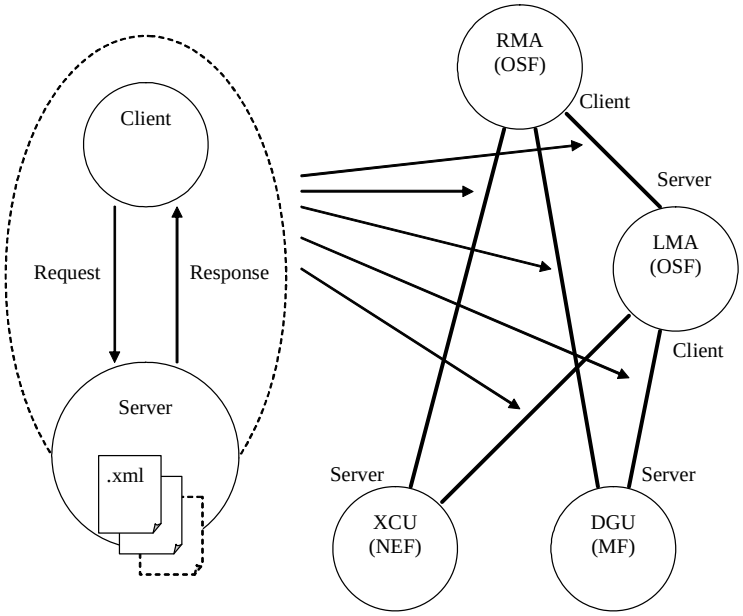


Figure A.1: Interaction between unit in the IEM&C network

A.1 Communication initiated by the LMA/RMA

Each DGU/XGU that can act as a server, holding one or more XML documents containing the data defined within the present document. Each existing document is within the HTTP standard referred to as a resource. Each resource is identified by a unique resource identifier known as a URI (Uniform Resource Identifier).

Examples of URI are:
"http://www.a-unit.com/site.xml" and *"http://127.0.0.1/site.xml"*.

The first part of the URI is always the IP address of the site or the IP of the sub-equipment. If hostname are defined, the IP address can be replaced.

A HTTP request from the LMA/RMA contains the reference to the unique URI and a method to be applied to it. The methods used within the scope of the present document are GET and POST.

All of these requests will result in a response message from the server with information about the status of the request and, in applicable cases, the data requested. The server entity shall, with exception only for specific behaviours stated within this document, respond in accordance with RFC 2616 [10] to received requests.

A.1.1 The GET method

The GET method is used to get any information (individual or full information) on a server. To retrieve an item, a GET request is issued with the URI identifying the specific data to be retrieved. To get the complete XML document related to a site, the following URI should be used:

URI: *http://the-site-ip/site.xml*

If the DGU or LMA gather information from equipment, the information will be retrieve at the URI:

URI: *http://the-equipment-ip/type_of_equipment.xml*

The name of the equipment corresponds to the tag name standardized in all the parts of the present document.

So, for example, if the equipment is a DC system, the URI will be:

URI: *http://the-equipment-ip/dc_system.xml*

If the equipment is a backup generator engine system, the URI will be:

URI: *http://the-equipment-ip/backup_generator_engine_system.xml*

Some parameters can be passed to request only parts of the documents.

Parameter name	Value	Description
description_table	true/false	Define if the description table must be included in the generated xml document (at each level of hierarchy)
alarm_table	true/false	Define if the alarm table must be included in the generated xml document (at each level of hierarchy)
event_table	true/false	Define if the event table must be included in the generated xml document (at each level of hierarchy)
data_table	true/false	Define if the data table must be included in the generated xml document (at each level of hierarchy)
data_record_table	true/false	Define if the data record table must be included in the generated xml document (at each level of hierarchy)
config_table	true/false	Define if the config table must be included in the generated xml document (at each level of hierarchy)
level	0, 1, 2, etc	Define the maximum level of hierarchy. 0 will retrieve only the site level, 1 will retrieve site and energy system level, etc.
option	0, 1, 3, etc	Generate the XML document according to a specific option (defined by the manufacturer)

The order of the parameters is free, and none is mandatory. The default XML document, when no parameter is provided, is defined by the manufacturer.

EXAMPLE:

If we want to retrieve the data table and the alarm table up to the third level of hierarchy, the URI will be:

URI: *http://the_site_ip/site.xml?description_table=false&alarm_table=true&event_table=false&data_table=true&data_record_table=false&config_table=false&level=3*

If we want to retrieve the XML document with the option 3, defined by the manufacturer (or configurable by some way), the URI will be:

URI: *http://the_site_ip/site.xml?option=3*

The manufacturer can define and describe other URI to get specific XML documents.

A.1.2 The POST method

The POST method is used to send requests requiring a set of parameters (e.g. item request type, item identification, authorized value update, configuration, etc). This method will allow requests for individual data items instead of complete XML files. Such request is written in XML language.

The receiving entity shall answer with xml formatted data structure that is either an acknowledge (e.g. ok, error code) or the requested values.

The allowed POST methods and arguments shall be provided by the manufacturer. The syntax must be clearly defined. The response shall also be described.

The following methods shall be defined.

Method	Description
GetValue(… arguments…)	To retrieve a specific data. The argument shall comprise the path relative to the data, in the XML structure
SetValue(… arguments…)	To set a specific data. The argument shall comprise the path relative to the data, in the XML structure, and the value to set
GetXML(… arguments…)	To retrieve a specific XML document
Other method.	Any other method can be defined.

A.2 Communication initiated by DGU/XCU

When an event appears on a site, the LMA/RMA must be aware of it.

The post method should be used, allowing the DGU/XCU to post events and data to the LMA/RMA. Rules can be defined by the operator to define when a post is requested.

The LMA/RMA can also get this event by asking the XCU/DGU, for example for data coherence control.

The polling can be used as single method to contact one by one each site (polling), but this is not efficient.

For example, when an alarm appears in a DC system, the DGU can post the file "site.xml" to the server. This file will be decoded by the server and the operator will be informed.

But it is also possible to post only the alarm with arguments defined by the operator.

It should be possible to post to multiple server, and to retry multiple times if the server is unavailable.

This mechanism, is a reliable and flexible equivalent of the classical SNMP traps.

Annex B (informative): Data Coherence and reliability for IEM&C

This annex gives recommendation to obtain reliable IEM&C data and functions.

B.1 Data integrity, coherence and management network reliability

Because it handles with intervention for maintenance on processes that can lead to an important blackout, the management network needs high reliability for data and application. The following description standardizes minimum requirements for dependability about data and application integrity and coherence, fast recovery.

Independence and redundancy of servers to avoid failure propagation is also addressed.

B.2 Application data coherence and integrity

This clause essentially refers to chronological events reports through the management network which constitutes the basis for safe operation.

The following functions should be provided:

- A global counters of pending alarms (start alarms with no end alarm message) for sites or equipment. That can be used as a good indicator of alarm integrity.
- In case of server restart, synchronization of detailed alarm list between XCU, LMA and RMA.
- Duplication of databases of events and configurations of sites in a mirror storage. There should be also server partial redundancy at least at RMA level.
- Every day a logbook should be requested automatically by LMA or RMA from XCU or alarm collector. A continuous logbook should be composed and stored in an archive on at least two redundant hard disks. This is useful for saving data and for coherent vision at any level.
- Every message should receive time stamp field from supervision level (LMA or RMA) in addition to its initial time stamp from XCU or DGU.
- Time/date for stamping events should be regularly self-tuned (synchronized) on a master clock through the network. In addition, all events should be assigned a unique identifier which can be used to generate the chronological sequence of events. However, it will not be possible to determine the order of events that occur within a minimum time period of each other e.g. 1 second. In such cases events will be given the same timestamp. (see time-date field in annex B).

B.3 Naming and data origin

It is of high importance to know where the data come from and this is much defined through management network configuration.

- Architecture and interface management: it should be always possible to know where the data are generated and stored to ensure integrity, coherence or unity: for example, a synopsis of management network units and links is displayed as well as list of possible alarms, events variables for each unit. This can be also referred as MIB.
- The reference name of a field should be single (for example the site name should be single).

- MIB manager tools, graphical tools, etc., should be associated to an object database, in order to maximize the re-use of existing patterns with a component architecture approach. This will help to reduce errors and save time. The object database should be a single reference to all console builders.
- Access from multiple points to modify the MIB (see annex C) shall not be allowed.

B.4 CU,DGU reliability

In the following, some of the previous requirements of this clause are detailed in hardware and basic application requirements to achieve high dependability.

XCU, DGU shall have minimum hardware securisation as follows:

- Watchdog + activity LED: microprocessor automation in equipment XCU, should be checked and automatically reset by a watchdog facility.
- Reset button.
- At minimum 3 alarms relays: for prompt, differed, and user defined severity alarm (e.g. prompt, deferred or warning).
- Permanent power supply interface: ETS 300 132-1 [1], EN 300 132-2 [2] or EN 300 132-3 [3].
- Configuration data and parameters stored in LMA or RMA.
- Detection of loss of integrity of configuration.
- Recovery mechanism: auto or manual if auto is impossible.

B.5 LMA reliability

LMA should have securisation as follows:

- Permanent power supply interface: ETS 300 132-1 [1], EN 300 132-2 [2] or EN 300 132-3 [3].
- CU data storage mirroring.
- Hardware selfcheck and failure indication to RMA.
- Loss of coherence/data integrity detection and indication to RMA.
- Selfrecovery of data application for coherence and integrity (for example after restarting).
- Manual recovery tool if auto impossible.

B.6 RMA reliability

RMA should have securisation as follows:

- Permanent power supply interface: ETS 300 132-1 [1], EN 300 132-2 [2] or EN 300 132-3 [3].
- Centralized server RMA unavailability shall be less than 5 minutes per year, this may be achieved using redundant servers and data storage redundancy (for example mirroring hard-disk at RMA level).
- More than one RMA client post, connected on the intranet.
- Every client post can handle every site.
- Failure of one client post does not affect the other posts.

- Speed performance in display, data storage and access can be affected by the failure of one post.

B.7 Ethernet and IP network reliability

Ethernet and IP network shall have securisation and management as follows:

- Network failure detection in less than 10 s.
- When using IP, the amount of access ports is limited to the minimum required for security reasons.
- On site a private TCP/IP Ethernet should be used at least for alarm synthesis collect.
- No hub allowed, a switch should be used to avoid collision.
- Router between sub network Encoding data transmission on public or private network.
    - When there is a possibility of using public media as transmission media e.g. Internet, the data transmission between site and management system should be encoded e.g. with SPIEC or other protocol.
    - If virtual private network VPN over ADSL intranet is used the encoded secured access is only done for external access through the firewall.

B.8 Computer and OS reliability

Computer and common OS shall be secured as follows:

- Update only under control of a super-user.
- There should be antivirus, troy horse, spyware and a firewall.
- There should be a diffusion tools to apply system patches and security updates as soon as available.

B.9 Application reliability

Application should be secured as follows:

- Every application should have a version checksum control and change indication report.
- There should be self storage of the latest version.
- There should integrity and code version checks.
- There should be recovery tools (see XCU, DGU, LMA, RMA).
- There should be a system log book of auto or manual application and data change and recovery.

Network access control: on XCU, DGU, LMA and RMA, password level shall be:

- Full power = read + command + changing installation parameters.
- Read site data and /change parameters.
- Read only.

They should be associated to a user identifier. Any access should be recorded in a system logbook. The change should be only on RMA by super user and downloaded on XCU and LMA.

Annex C (informative): Network Element Functions and software architecture and choices

This annex gives recommendation about network element functions and the organization of applications.

C.1 General description

The functions of LMA should be:

- concentrator of different equipment XCU interfaces with different protocols directly or through DGU;
- server with a single unified protocol towards the RMA;
- site overview and access portal to any equipment for control and monitoring (graphical synopsis display);
- alarm re-qualification or generation at site level;
- web server for remote access from anywhere with a light client browser on a personal computer.

Machine-machine

- auto XCU, DGU- time setting (clock synchronization);
- auto XCU, DGU configuration saving and recovery (i.e. there is a trace of changes);
- auto acquisition and saving of XCU, DGU events logbooks;
- auto acquisition and saving of XCU, DGU measurements records;
- global coherence control: mandatory for ongoing alarms;
- network management;
- alarm priority management: urgency classification, correlation between information of control unit in a site.

Man-machine

Real-time supervision:

- dynamic display + auto refresh;
- events logbook display;
- on line hypertext help;
- command sending to equipments.

Differed time analysis

- measurements value log on period: parameter are acquisition period and log size (or time);
- correlation between logbooks and databases.

Extra functions should be provided:

- replay events on dynamic display (using log-book message + states and values recording);
- GSM server with vocal or SMS messages;

- interface with existing supervision on site;
- DGU function in the same machine as LMA.

Figure C.1 can help to understand how applications services and protocol may be organized in LMA.

DGU or LMA should be structured and sized to be open to protocols and applications services. There is a principle of service subscriber through the protocols and routing. (i.e. modbus need data acquisition, processing, formatting in html and sending to smtp and http supervisor).

It shall be possible to load (download) applications or protocols in DGU or LMA.

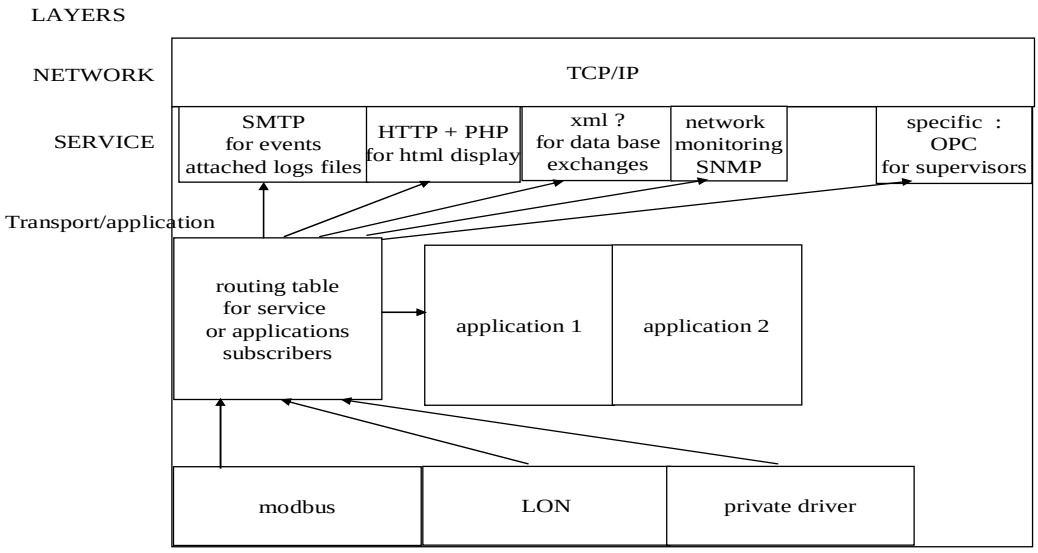


Figure C.1: Services and protocols organization in LMA

C.2 Functions of the RMA

The functions or RMA should be:

- real time functions of the LMA;
- distributed display posts;
- distributed data storage;
- decision tools: priority management between site intervention (i.e. autonomy calculation and display, with or without generator, site importance classification through impact of failure, etc.);
- differed time analysis of the LMA;
- correlation between logbooks and databases;
- output towards other analysis servers through database exchanges.

C.3 Data analysis

The system is used not only for collection of alarms, but also to manage the whole infrastructure in term of:

- quality and performance of operation;
- reliability derates of equipment (battery, rectifier, generator, etc.);

- energy consumption derates (that can hide bad setting or failures).

Not only information about alarm event is important, but also what site status (what measurements) were at that time.

Additionally, to be able to do analyses and statements such as: what voltage course was during mains supply occurrence it is necessary to correlate information on the alarm with the site status.

To be able to create statements (trends) of individual analogical signals and correlate them with the particular alarm, CU should it record measurements from devices on condition of a particular alarm or continuously with recording condition (i.e. change to limit memory and flow of data on network).

LMA and RMA should offer database interface for import/export data at this purpose: i.e. mySQL at minimum.

C.4 Safety monitoring input provision

There should be access provision to connect site video monitoring.

C.5 Software working and development environment

Servers often use standard environments like Microsoft Windows NT/XP, UNIX or LINUX.

Dynamic webs use PHP, a generalist language very close to the C language, with a reliable database e.g. MySQL.

PHP shall be used to generate dynamic html pages.

Java shall not be used because too dependant of browser release.

The most diffused web-server on the Internet Apache (literally, A patchy server) shall be provided on LMA or RMA.

This shall be able to answer a client calling a web page with an http request on port 80.

The same environment can be used at each level: XCU, DGU, LMA and RMA.

There should be specific architecture requirements to ease the upgrading of machine and software. For example, location of some system files and specific control configurations should be imposed to allow downloading of new software releases and patches.

Tools shall be available to operator to build the MIB and the graphical synopsis. It shall be possible to build or modified objects using a library of commonly described existing configurations and graphics, to avoid errors and save time.

LMA and RMA shall allow to define different user ergonomics with common tools on computers (colour of field in message, colour drawing mixed with scanned picture or photograph, etc.).

Graphic format shall be non proprietary and compressed to reduce data transfer time on network i.e. compressed bitmap, Jpeg, vector drawing, etc.

Annex D (informative): Network capacity and timing

This annex gives some recommendations about IEM&C management service performances.

D.1 Management and Network Capacity

The main capacity requirements are the following:

- the site supervision server LMA can monitor at least 32 control units XCU;
- the remote server RMA in monitoring room can monitor at least 500 sites per supervision server unit, i.e. an average of 5 000 XCU per RMA server with an average of 10 XCU/site;
- on failure or maintenance, one server can host another, that means it monitors 1 000 sites (partial performance derating is allowed);
- every servers hard disk operation information are mirrored on a back-up server or on every server; this can be useful to reduce network traffic, speed the access to data from any point, ease reallocation process in case of failure);
- supervision shall be possible on a minimum of 5 display terminals at the same time on different sites (i.e. on equipment XCU, on site LAN, on LMA, on RMA, on mobile terminal).

D.2 Memory capacity

The main performance requirements are the following:

- events logfile minimum size: 100 in XCU, 5000 per XCU in DGU or LMA or RMA;
- measurements records: 10 variables per XCU.

D.3 Timing performance

- Alarms: between emission by XCU and display on remote supervision, alarms shall be transmitted and refreshed in less than 5 s. This shall be tested on a dedicated private TCP/IP test network with no transfer delay.
- 100 ms maxi to access one event though data base query.
- Site or equipment dynamic supervision < 5s (synopsis access and refresh of a site or equipment when display).

Synopsis has to be refreshed in order to see real time alarms, acknowledgement, and remote command effect. Special consideration must be given to periods of crisis when, for example, several centres are affected by a general blackout or a climatic event. (Connection through analogical modem, time can add 60 s).

NOTE: A mechanism of alarm beginning requiring remote or local acknowledgement to end alarm should avoid repetitive alarms.

- LMA restart time in case of reset is automatic and less than 5 min.
- Considering access concurrency, the closer connection to equipment with writing right gives the higher priority. Other connexion becomes observers (read only). Priority shall be: XCU > LMA > LAN > mobile post > RMA Priority is loosed after an inactivity timeout (typically 5 min).

Annex E (informative): Overview of the XML format

The followings definitions are only an introduction for people unfamiliar with the XML. It allows understanding of the present document. For more details, it is recommended to consult the website of the World Wide Web consortium (W3C - www.w3c.org).

E.1 XML

XML is the abbreviation of eXtensible Markup Language. As defined by the World Wide Web consortium, the XML is a simple, very flexible text format. Originally designed to meet the challenges of large-scale electronic publishing, XML is also playing an increasingly important role in the exchange of a wide variety of data on the Web and elsewhere. XML is designed to describe data and focus on what data is. XML must be discerned from the well known Hypertext Transfer Markup Language (HTML) which was designed to display data and to focus on how data looks.

E.2 XML declaration

The first line of a XML document is the XML declaration. It defines the XML version and the character encoding used in the document.

EXAMPLE:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

E.3 XML element, XML root element and XML child element

Any XML document must contain a single tag to define a root element. All other elements must be within this root element. All elements can have child elements. These child elements must be correctly nested within their parent element. The text/data in the XML element is called the "inner text". All these element must be correctly tagged as shown in the following example:

```
<root>
  <child>
    <subchild>..the inner text...</subchild>
  </child>
</root>
```

For the present document an element can be a lot of different things, by example:

- A sub rack.
- A rectifier.
- A diesel engine.
- A temperature sensor.
- A door actuator.
- An UPS.

- A cooling system.
- A battery.
- A site.
- A measure of temperature.
- A measure of current.
- A measure of power.
- Etc.

E.4 XML document

An XML document is a text file composed of a XML declaration and at least the XML root element.

E.5 XML Attribute

XML elements can have attributes in name/value pair. This attribute must be quoted. A good practice rule is not to use attribute to store a data, but well for information about the data.

By example, for a voltage measurement data, we could have a structure as follows:

```
<data>
    <name>Output Voltage</name>
    <value>54</value>
    <unit> volt </unit>
    <type>measurement</type>
</data>
```

But the following structure is much better:

```
<data name="Output Voltage" type="measurement" "unit="volt">54</data>
```

The good practice rule is that the inner text of an element must only contain the data, and the description of how the data is coded and what means the data must be placed in the attributes.

E.6 XML Schema

A XML Schema describes the structure of a XML document. According to W3C standards, a XML Schema:

- defines elements that can appear in a document;
- defines attributes that can appear in a document;
- defines which elements are child elements;
- defines the order of child elements;
- defines the number of child elements;
- defines whether an element is empty or can include text;
- defines data types for elements and attributes;

- defines default and fixed values for elements and attributes;
- with the help of such an XML schema, it is possible to verify that the XML files generated by monitoring equipments are compliant with the structure defined by the present document.

E.7 XML Schema Datatypes

The W3C Schema standard defines a lot of datatypes.

NOTE: See http://www.w3.org/TR/xmlschema-2/.

The most common are briefly described in the table E.1. It is highly recommended to consult the W3C website for a better understanding.

Table E.1: XML schema datatype as described in W3C

Datatype	Description	Example
xs:string	Represents character strings	This is a string
xs:decimal	Represents a decimal value. It consists of a finite-length sequence of digits, separated by a period as a decimal indicator. An optional leading sign is allowed. If the sign is omitted, "+" is assumed. Leading and trailing zeroes are optional. If the fractional part is zero, the period and following zero(es) can be omitted.	-2335353,243353 1,23 210 +3450,234
xs:integer	Represents an integer value. It is derived from xs:decimal by fixing the value of the fraction digits to 0.	3425 -346 0
xs:boolean	Represents a Boolean value: true or false	true
xs:datetime (see note 1)	Date Time values may be viewed as objects with integer-valued year, month, day, hour and minute properties, a decimal-value second property, and a Boolean time zoned property. W3C website should be visited to have more details about this format. The first example means 10 November 2006, 17 hours 28 minutes and 5 seconds, in UTC time. The Z at the end means UTC time, and the T in the middle is the separation between the date and the time. If no information about time zone is specified, it is an UTC zone.	2006-11-10T17:28:05Z 2000-06-10T10:23:12Z 2002-10-10T12:00:00+05:00
xs:date	This format is a the part of the date time format related to the date	2006-11-10 2002-10-10
xs:time	This format is a the part of the date time format related to the time	17:28:05Z 12:00:00+05:00
xs:duration (see note 2)	Represents duration of time. It is composed of year, month, day, hour, minutes and seconds. Some examples introduce the representation but W3C website should be visited to have more details about this format.	3DT10H23M12S T10H23M18.45S T34M34S P0Y1347M
xs:complexType	A complex element which contains other elements and/or attributes	/
NOTE 1: See http://www.w3.org/TR/xmlschema-2/#dateTime. NOTE 2: See http://www.w3.org/TR/xmlschema-2/#duration.		

With the help of an XML Schema file, it is possible to check that the data (the inner text) contained in an element is of a defined type.

According to this method, the present document can define the data type of each of the standardized data.

E.8 XSL Languages

XSL stands for eXtensible Stylesheet Language. The World Wide Web Consortium (W3C) started to develop XSL because there was a need for an XML-based Style sheet Language.

XSL consists of three parts:

- XSLT: a language for transforming XML documents.
- XPath: a language for navigating in XML documents.
- XSL-FO: a language for formatting XML documents.

E.9 XSLT

XSLT stands for eXtensible Stylesheet Language Transformation. It is used to transform an XML document into another XML document, or another type of document that is recognized by a browser, like HTML and XHTML.

With XSLT, it is possible to add/remove elements and attributes to or from the output file. It is also possible to rearrange and sort elements, perform tests and make decisions about which elements to hide and display.

In the present document, XSLT will be used to select parts of a full XML document describing the whole site. By example, it is possible to get only the active alarms, to get only the monitored data of a specific equipment, etc.

E.10 XPath

XPath is a language for finding information in a XML document. It is used to navigate thought elements and attributes in a XML document.

By example, in the following example:

```
<root>
  <child>
     <subchild id=1>..the inner text...</subchild>
     <subchild id=2>..the inner text...</subchild>
  </child>
</root>
```

The Xpath syntax of the subchild with the id 2 is: /root/child/subchild[@id="2"].

Annex F (informative): Hints about the choice of OSI or IP models, physical network layers and intranet-Ethernet access protocols

More can be found on http://en.wikipedia.org/wiki/OSI_model.

This annex explains why message format in high level application layer still refers to ITU-T or CCITT, but and why ISO is not fully followed, due to the predominance and simplification brought by IP network and services specifications. For low level, physical and logical wired or wireless network layers, IEEE is the reference for Ethernet or WIFI and ITU-T for ISDN, xDSL, ATM or SDH.

F.1 OSI and IP models

The OSI reference model is a hierarchical structure of seven layers that defines the requirements for communications between two computers (see table 1). The model was defined by the International Organization for Standardization in the standard ISO/IEC 7498:1984 Open Systems Interconnection - Basic Reference Model [11].

It was conceived to allow interoperability across the various platforms offered by vendors.

Of course, by that time, TCP/IP (improved ARPANET) had been in use for years. (For significant differences between TCP/IP and ARPANET, see RFC 871.)

Only a subset of the whole OSI model is used today. It is widely believed that much of the specification is too complicated and that its full functionality has taken too long to implement.

The OSI model divides the functions of a protocol into a series of layers. Each layer has the property that it only uses the **functions of the layer below**, and only exports functionality to the layer above. A system that implements protocol behavior consisting of a series of these layers is known as a "protocol stack" or "stack". Protocol stacks can be implemented either in hardware or software, or a mixture of both. Typically, only the lower layers are implemented in hardware, with the higher layers being implemented in software.

Its main feature is in the interface between layers which dictates the specifications on how one layer interacts with another. This means that a layer written by one manufacturer can operate with a layer from another (assuming that the specification is interpreted correctly). These specifications are typically known as Requests for Comments or "RFCs" in the TCP/IP community and ISO standards in the OSI community.

Table F.1: OSI Model

OSI Model			
	Data unit	**Layer**	**Function**
Host layers	Data	Application	Network process to application
		Presentation	Data representation and encryption
		Session	Interhost communication
	Segments	Transport	End-to-end connections and reliability
Media layers	Packets	Network	Path determination and logical addressing (IP)
	Frames	Data link	Physical addressing (MAC & LLC)
	Bits	Physical	Media, signal and binary transmission

Table F.2 illustrates the OSI layers model compared with IP model and associates some implementation examples.

Table F.2: Comparison between OSI and IP model

	OSI Layer	IP layer	Examples
7	Application	4 Application	HTTP, SMTP, SNMP, FTP, Telnet, ECHO, SIP, SSH, NFS, RTSP, XMPP, Whois, ENRP
6	Presentation		XDR, ASN.1, SMB, AFP, NCP
5	Session	3 Transport	ASAP, TLS, SSL, ISO 8327 / CCITT X.225, RPC, NetBIOS, ASP
4	Transport		TCP, UDP, RTP, SCTP, SPX, ATP, IL
3	Network	2 Network	IP (V4, V6), X.25
2	Data Link		IEEE 802.3 Ethernet, HDLC, Frame relay, ISDN, ATM, IEEE 802.11 WiFi, PPP
1	Physical	1 Physical Network access LLC+MAC	RS 232,RS 422, RS 485, Ethernet (10BASE-T, etc.), SONET/SDH, T-carrier/E-carrier, various IEEE 802.11 physical layers (WIFI), POTS, GSM, ISDN, DSL

A Comparison between OSI model and IP model, is not easy. The IP suite (and corresponding stack) were in use before the OSI model. Though OSI model has more layers, it is not rich enough at the lower layers to capture the true workings of the IP suite. For example, an "internetworking layer" is needed to fit in between the network and transport layers. OSI is not suited for multiple data link layer (for example an ADSL user tunnelling into a corporate network could have IP over PPTP over IP over PPPoA over the ADSL link).

F.2 Details on IP layers

F.2.1 Application Layer

The application layer is used by most programs for network communication. Data is passed from the program in an application-specific format, then encapsulated into a transport layer protocol. The protocol layer is http in the present document for XML data.

NOTE: Other protocol exists such as SNMP, FTP, SMTP.

Since the IP stack has no layers between the application and transport layers, the application layer must include any protocols that act like the OSI's presentation and session layer protocols. This is usually done through libraries.

Data sent over the network is passed into the application layer where it is encapsulated into the application layer protocol. From there, the data is passed down into the lower layer protocol of the transport layer (i.e. TCP in the present document).

Common application services have specific ports assigned to them (http uses port 80; ftp uses port 21.) while clients can use ephemeral ports.

Routers and switches do not utilize this layer.

In IP, the presentation and session layers are merged with application layers:

- The Presentation layer encodes data (MIME encoding, data compression, data encryption and similar manipulation) to present the data for the service or protocol developer. Examples: serializing SQL objects into and out of XML.

- The Session layer controls the dialogues (sessions) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for either duplex or half-duplex operation and establishes check pointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for "graceful close" of sessions, which is a property of TCP, and also for session check pointing and recovery, which is not usually used in the Internet protocols suite.

F.2.2 Transport Layer

The transport layer's responsibilities include end-to-end message transfer capabilities independent of the underlying network, along with error control, fragmentation and flow control. End to end message transmission or connecting applications at the transport layer can be categorized as either:

1) connection-oriented e.g. TCP;

2) connectionless e.g. UDP (not used in the present document).

The transport layer can be thought of as a literal transport mechanism e.g. a vehicle whose responsibility is to make sure that its contents (passengers/goods) reach its destination safe and sound.

The transport layer provides this service of connecting applications together through the use of ports. Since IP provides only a best effort delivery, the transport layer is the first layer to address reliability.

For example, TCP is a connection-oriented protocol that addresses numerous reliability issues to provide a reliable byte stream:

- data arrives in-order;
- data has minimal error-correctness;
- duplicate data is discarded;
- lost/discarded packets are resent;
- includes traffic congestion control.

The dynamic routing protocols which technically fit at this layer in the TCP/IP Protocol Suite (since they run over IP) are generally considered to be part of the Network layer; an example is OSPF (IP protocol number 89).

The newer SCTP is also a "reliable", connection-oriented, transport mechanism. It is stream-oriented - not byte-oriented like TCP - and provides multiple streams multiplexed over a single connection. It also provides multi-homing support, in which a connection end can be represented by multiple IP addresses (representing multiple physical interfaces), such that if one fails, the connection is not interrupted. It was developed initially for telephony applications (to transport SS7 over IP), but can also be used for other applications.

F.2.3 Network Layer

As originally defined, the Network layer solves the problem of getting packets across a single network. An example of such protocols is ITU-T Recommendation X.25 [9].

With the advent of the concept of internetworking, additional functionality was added to this layer, namely getting data from the source network to the destination network. This generally involves routing the packet across a network of networks, known as an internet work or (lower-case) internet.

In the Internet protocol suite, IP performs the basic task of getting packets of data from source to destination. IP can carry data for a number of different upper layer protocols such as routing protocols.

F.2.4 Link Layer

The link layer, which is the method used to move packets from the network layer on two different hosts, is not really part of the Internet protocol suite, because IP can run over a variety of different link layers. The processes of transmitting packets on a given link layer and receiving packets from a given link layer can be controlled both in the software device driver for the network card, as well as on firmware or specialist chipsets. These will perform data link functions such as adding a packet header to prepare it for transmission, then actually transmit the frame over a physical medium.

For Internet access over a dial-up modem, IP packets are usually transmitted using PPP. For broadband Internet access such as ADSL or cable modems, PPPoE is often used. On a local wired network, Ethernet is usually used, and on local wireless networks, IEEE 802.11 is usually used. For wide-area networks, either PPP over T-carrier or E-carrier lines, Frame relay, ATM, or packet over SONET/SDH (POS) are often used.

The link layer can also be the layer where packets are intercepted to be sent over a virtual private network. When this is done, the link layer data is considered the application data and proceeds back down the IP stack for actual transmission. On the receiving end, the data goes up the IP stack twice (once for the VPN and the second time for routing).

The link layer can also be considered to include the physical layer, which is made up of the actual physical network components (hubs, repeaters, network cable, fiber optic cable, coaxial cable, network cards, Host Bus Adapter cards and the associated network connectors: RJ-45, BNC, etc), and the low level specifications for the signals (voltage levels, frequencies, etc).

Ethernet and WIFI

IEEE 802 [12] refers to a family of IEEE standards 802.1 to 802.22 about local area networks and metropolitan area networks. IEEE 802.3 Ethernet, IEEE 802.11 Wireless LAN (Wi-Fi certification) can be outlined.

More specifically, the IEEE 802 [12] standards are restricted to networks carrying variable-size packets. (By contrast, in uniform cell-based networks or Isochronous networks, where data is transmitted as a steady stream of octets, or groups of octets, at regular time intervals).

Enhanced data link for multiple network element: MAC address + LLC (CSMA/CD)

IEEE 802 [12] splits the OSI Data Link Layer into two sub-layers named Logical Link Control (LLC) and Media Access Control.

Every network element on Ethernet, shall have a **Media Access Control** (MAC) address. The MAC sub layer is the part of the OSI network model data link layer that determines who is allowed to access the physical media at any one time. It acts as an interface between the Logical Link Control sub layer and the network's physical layer.

The MAC sub layer is primarily concerned with the control of access to the physical transmission medium (i.e. which of the stations attached to the wire or frequency range has the right to transmit?) or low-level media-sharing protocols like CSMA/CD.

Ethernet is the classic CSMA/CD protocol (Carrier Sense Multiple Access With Collision Detection).

F.3 Internet - Ethernet access protocol PPPoE, PPPoA, PoS

F.3.1 PPPoE

PPPoE, Point-to-Point Protocol over Ethernet (RFC 2516), is a tunnel network protocol for encapsulating PPP frames in Ethernet frames. E.g. it is used with ADSL services. It offers PPP features as authentication (login + password), encryption, and compression though a connection between two Ethernet ports. Traditional PPP-based software handles a connection on a serial line, but also on a packet-oriented network like Ethernet. Also, the IP address on the other side of the link is only assigned when the PPPoE connection is open, allowing the dynamic reuse of IP addresses (DHCP service). After the link has been established, additional network (layer 3) Internet Protocol Control Protocol (IPCP) is available.

Both PPP and Dynamic Host Configuration Protocol (DHCP) offer support for automatic configuration of interfaces.

There can be trouble with firewall due to fixed MTU.

Maximum Transmission Unit (**MTU**) refers to the size (in bytes) of the largest packet that a given layer of a communications protocol can pass onwards. MTU parameters usually appear in association with a communications interface (NIC, serial port, etc.). The MTU may be fixed by standards (as is the case with Ethernet) or decided at connect time (as is usually the case with point-point serial links). A higher MTU brings higher bandwidth efficiency. However large packets can block up a slow interface for some time, increasing the lag on other packets. For example a 1500 byte packet, the largest allowed by Ethernet (and hence most of the Internet), would block up a 14.4k modem for about one second.

RFC 1191 describes "Path MTU discovery", a technique for determining the path MTU between two IP hosts with a view to avoiding IP fragmentation.

Most modern Ethernet LANs use an MTU of 1500 bytes. But systems like PPPoE will reduce this, causing path MTU discovery to come into effect with the possible effect of making some sites behind badly-configured firewalls unreachable.

F.3.2 PPP service

PPP was designed somewhat after the original HDLC specifications and is described by RFC 1661. PPP is encapsulated in a framing similar to HDLC, described by RFC 1662.

PPP uses a Frame Check Sequence (FCS) field to detect frame error. This is a checksum computed over the frame based on is a CRC code similar to Ethernet layer 2 protocol error protection schemes. It can be either 16 bits or 32 bits in size (default is 16 bits - Polynomial $x^{16} + x^{12} + x^5 + 1$). Fieldbus such as Jbus/modbus use also this CRC16.

The FCS is calculated over the Address, Control, Protocol, Information and Padding fields.

Link Control Protocol (LCP) is an integral part of PPP. LCP provides automatic configuration of the interfaces at each end and for selecting optional Password authentication protocol (PAP).

RFC 1994 describes Challenge-handshake authentication protocol (CHAP), preferred for establishing dialup connections with ISPs.

Although these are not standard applications, PPP is also occasionally used over broadband connections.

F.3.3 Other PPP

PPPOA or **PPPoA** Point-to-Point Protocol (**PPP**) over **ATM**, is a network protocol for encapsulating PPP frames in ATM AAL5. It is used mainly with cable modem, DSL and ADSL services.

It offers standard PPP features such as authentication, encryption, and compression. If it is used as the connection encapsulation method on an ATM based network it can reduce overhead slightly (around 0,58 %) in comparison to PPPoE. It also avoids the issues that PPPoE suffers from, related to having a MTU lower than that of standard Ethernet transmission protocols. It also supports (as does PPPoE) the encapsulation types: VC-MUX and LLC based.

PPPoA is specified in RFC 2364.

PoS Packet over SONET/SDH (RFC 2615).

Annex G (informative): Bibliography

IEC 61970-301: "Energy management system application program interface (EMS-API) - Part 301: Common Information Model (CIM) Base".

IEC/TR 62357: "Power system control and associated communications - Reference architecture for object models, services and protocols".

ISO/IEC Guide 73: "Risk management - Vocabulary - Guidelines for use in standards".

ISO/IEC 8824 (all parts): "Information technology - Abstract Syntax Notation One (ASN.1)".

REST.

NOTE: Described in: http://en.wikipedia.org/wiki/REST, http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm (Ref article from Roy Thomas) and http://www.peej.co.uk/articles/rest.html .

IETF RFC 2516: "A Method for Transmitting PPP Over Ethernet (PPPoE)".

IETF RFC 1191: "Path MTU discovery".

IETF RFC 871: "Perspective on the ARPANET reference model".

IETF RFC 1662: "PPP in HDLC-like Framing".

IETF RFC 1994: "PPP Challenge Handshake Authentication Protocol (CHAP)".

IETF RFC 2364: "PPP Over AAL5".

IETF RFC 2615: "PPP over SONET/SDH".

History

Document history		
V1.1.1	September 2004	Publication as TR 102 336
V1.1.1	September 2007	Membership Approval Procedure MV 20071102: 2007-09-04 to 2007-11-02
V1.1.1	November 2007	Publication