Final draft ETSI ES 202 336-1 V1.3.0 (2025-02)

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
RES/EE-02105

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This final draft ETSI Standard (ES) has been produced by ETSI Technical Committee Environmental Engineering (EE), and is now submitted for the ETSI Membership Approval Procedure.

The present document is part 1 of a multi-part deliverable covering Environmental Engineering (EE); Monitoring and Control Interface for Infrastructure Equipment (power, cooling and building environment systems used in telecommunication networks), 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";

Part 8: "Remote Power Feeding System control and monitoring information model";

Part 9: "Alternative Power Systems";

Part 10: "AC inverter power system control and monitoring information model";

Part 11: "Battery system with integrated control and monitoring information model";

Part 12: "ICT equipment power, energy and environmental parameters monitoring information model".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document will describe the generic monitoring and control interface for infrastructure equipment. The present document should follow a two-stage approach:

a) protocol-independent information modelling;

b) protocol-specific data modelling e.g. in YAML/JSON.

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; also the monitoring energy and environmental parameters for Information Communication Technology (ICT) equipment in telecommunications sites or datacenter or customer premises are considered.

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 (the present document) and several specific parts for equipment category.

The present document defines:

- The site equipment maps and its division in functional subsets e.g. DC system which introduces part 2 and following parts of this multi-part deliverable.
- The generic set of exchanged information required at the interface of equipment, which is instanced for each equipment subset in part 2 and following parts of this multi-part deliverable.
- The minimum requirement for network architecture allowing some compatibility with old existing interface and the mechanism to exchange data between network elements.
- 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 a 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.
- The Measurement accuracy of Power, Energy and Environmental parameters (PEE).

An architecture for monitoring Power, Energy and Environmental parameters (PEE) for data originated by different types of site infrastructure equipment is defined.

Introduction

The present document was developed jointly by ETSI TC EE and ITU-T Study Group 5. It is published respectively by ITU and ETSI as Recommendation ITU-T L.MCI Gen [i.33] and ETSI ES 202 336-1 (the present document), which are technically equivalent.

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; also, the monitoring of energy and environmental parameters: Power Energy Environmental (PEE) parameters for ICT equipment in telecommunications sites or datacenter or customer premises are considered.

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 (the present document) and several specific parts for equipment category.

The present document defines:

- The site equipment maps and its division in functional subsets e.g. DC system which introduces following parts of this multi-part deliverable.
- The generic set of exchanged information required at the interface of equipment, which is instanced for each equipment covered by following parts of this multi-part deliverable.
- The minimum requirement for network architecture allowing some compatibility with old existing interface and the mechanism to exchange data between network elements.
- 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 a 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.
- The Measurement accuracy of Power, Energy and Environmental Parameters (PEE).

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

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

The following referenced documents are necessary for the application of the present document.

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

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

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

[4] IEC 60839-5-1: "Alarm and electronic security systems – Part 5-1: Alarm transmission systems – General requirements".

[5] Void.

[6] IETF RFC 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".

[7] ISO/IEC 7498: "Open Systems Interconnection (OSI) — Basic Reference Model".

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

[9] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format".

[10] IETF RFC 7950: "The YANG 1.1 Data Modeling Language".

[11] ETSI EN 300 019-1-3: "Environmental Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment; Part 1-3: Classification of environmental conditions; Stationary use at weatherprotected locations".

[12] ETSI TS 132 130: "Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Network sharing; Concepts and requirements(3GPP TS 32.130)".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 102 336: "Environmental Engineering (EE); Power and cooling system control and monitoring guidance".

[i.2] Void.

[i.3] IETF RFC 2516: "A Method for Transmitting PPP Over Ethernet (PPPoE)".

[i.4] IETF RFC 1191: "Path MTU discovery".

[i.5] IETF RFC 871: "Perspective on the ARPANET reference model".

[i.6] IETF RFC 1662: "PPP in HDLC-like Framing".

[i.7] IETF RFC 1994: "PPP Challenge Handshake Authentication Protocol (CHAP)".

[i.8] IETF RFC 2364: "PPP Over AAL5".

[i.9] IETF RFC 2615: "PPP over SONET/SDH".

[i.10] IETF RFC 1661: "The Point-to-Point Protocol (PPP)".

[i.11] ISO/IEC 8327: "Information technology — Open Systems Interconnection — Connection-oriented Session protocol: Protocol specification".

[i.12] ETSI ES 202 336-2: "Environmental Engineering (EE); Monitoring and control interface for infrastructure equipment (Power, Cooling and environment systems used in telecommunication networks); Part 2: DC power system control and monitoring information model".

[i.13] ETSI ES 202 336-3: "Environmental Engineering (EE); Monitoring and Control Interface for Infrastructure Equipment (Power, Cooling and Building Environment Systems used in Telecommunication Networks); Part 3: AC UPS power system control and monitoring information model".

[i.14] ETSI ES 202 336-4: "Environmental Engineering (EE); Monitoring and Control Interface for Infrastructure Equipment (Power, Cooling and Building Environment Systems used in Telecommunication Networks); Part 4: AC distribution power system control and monitoring information model".

[i.15] ETSI ES 202 336-5: "Environmental Engineering (EE); Monitoring and Control Interface for Infrastructure Equipment (Power, Cooling and Building Environment Systems used in Telecommunication Networks); Part 5: AC diesel back-up generator system control and monitoring information model".

[i.16] ETSI ES 202 336-6: "Environmental Engineering (EE); Monitoring and Control Interface for Infrastructure Equipment (Power, Cooling and Building Environment Systems used in Telecommunication Networks); Part 6: Air Conditioning System control and monitoring information model".

[i.17] ETSI ES 202 336-7: "Environmental Engineering (EE); Monitoring and Control Interface for Infrastructure Equipment (Power, Cooling and Building Environment Systems used in Telecommunication Networks); Part 7: Other utilities system control and monitoring information model".

[i.18] ETSI ES 202 336-8: "Environmental Engineering (EE); Monitoring and Control Interface for Infrastructure Equipment (Power, Cooling and Building Environment Systems used in Telecommunication Networks); Part 8: Remote Power Feeding System control and monitoring information model".

[i.19] ETSI ES 202 336-9: "Environmental Engineering (EE); Monitoring and Control Interface for Infrastructure Equipment (Power, Cooling and Building Environment Systems used in Telecommunication Networks); Part 9: Alternative Power Systems".

[i.20] ETSI ES 202 336-10: "Environmental Engineering (EE); Monitoring and Control Interface for Infrastructure Equipment (Power, Cooling and Building Environment Systems used in Telecommunication Networks); Part 10: AC inverter power system control and monitoring information model".

[i.21] ETSI ES 202 336-11: "Environmental Engineering (EE); Monitoring and control interface for infrastructure equipment (Power, Cooling and environment systems used in telecommunication networks); Part 11: Battery system with integrated control and monitoring information model".

[i.22] ETSI ES 202 336-12: "Environmental Engineering (EE); Monitoring and control interface for infrastructure equipment (power, cooling and building environment systems used in telecommunication networks); Part 12: ICT equipment power, energy and environmental parameters monitoring information model".

[i.23] ETSI EN 300 132-1: "Equipment Engineering (EE); Power supply interface at the input to Information and Communication Technology (ICT) equipment; Part 1: Alternating Current (AC)".

[i.24] ETSI EN 300 132-2: "Environmental Engineering (EE); Power supply interface at the input of Information and Communication Technology (ICT) equipment; Part 2: -48 V Direct Current (DC)".

[i.25] ETSI EN 300 132-3: "Environmental Engineering (EE); Power supply interface at the input of Information and Communication Technology (ICT) equipment; Part 3: Up to 400 V Direct Current (DC)".

[i.26] Recommendation ITU-T 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".

[i.27] LT0511 RevB datasheet: "Linear Technology LTC 1966 precision micropower RMS to DC converter".

[i.28] Mark Strzegowski: "Realizing the Full Potential of Your AMI Deployment with Meter Diagnostic Data", Analog Device.

[i.29] ETSI EN 300 019-1-4: "Environmental Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment; Part 1-4: Classification of environmental conditions; Stationary use at non-weatherprotected locations".

[i.30] ETSI ES 203 700: "Environmental Engineering (EE); Sustainable power feeding solutions for 5G network".

NOTE: ETSI ES 203 700 is technically equivalent to Recommendation ITU-T L.1210: "Sustainable power-feeding solutions for 5G networks".

[i.31] Recommendation ITU-T L.1382: "Smart energy solution for telecommunication rooms".

[i.32] IEC 61557-12: 2018 /AMD (2021): "Electrical safety in low voltage distribution systems up to 1 000 V AC and 1 500 V DC. - Equipment for testing, measuring or monitoring of protective measures - Part 12: Power metering and monitoring devices".

[i.33] Recommendation ITU-T L.MCI Gen: "Monitoring and Control Interface for Infrastructure Equipment (Power, Cooling and Building Environment Systems used in Telecommunication Networks) Part 1: Generic Interface".

[i.34] W3C®: "XML Schema Part 2: Datatypes Second Edition".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

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 can be understood by itself by an operator and 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.)

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.

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

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

- collect serial, digital, and analogue 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 functional unit may be integrated as part of specific equipment.

Dynamic Host Configuration Protocol (DHCP): protocol used for self configuration of TCP/IP parameters of a workstation assigning IP address and a sub-network mask

NOTE: DHCP may also configure DNS.

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

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

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 can be understood by itself by an operator and have at least one severity qualification or codification (colour, level, etc.). It is 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".

eXtended HTML (XHTML): stricter and cleaner version of HTML

NOTE 1: XHTML consists of all the elements in HTML 4.01 combined with the syntax of XML.

NOTE 2: It can be read by all XML browser (see W3C).

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.

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.

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

warning: low severity alarm

3.2 Symbols

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

Tacq	Voltage and Current acquisition period

3.3 Abbreviations

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

A/D	Analog to Digital
AC	Alternating Current
ADSL	Asynchronous Digital Subscriber Line
AFP	Advanced Function Presentation
API	Application Programming Interface
ARPANET	Advanced Research Projects Agency Network
ASAP	Application Specific Access Profile
ASN.1	Abstract Syntax Notation One
ASP	Abstract Service Primitive
ATM	Asynchronous Transfer Mode
ATP	Access Transport Protocol
BNC	Bayonet Nut Connector
BS	Base Station
CAN	Controller Area Network
CHAP	Challenge-Handshake Authentication Protocol
CIM	Common Information Model
CM	Configuration Management
CRC	Cycle Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSV	Comma Separated Values
CU	Control Unit
DC	Direct Current
DCF	Data Communication Function in TMN
DCU	Data Control Unit
DGU	Data Gathering Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Dynamic Name Server
DSL	Digital Subscriber Line
EEPROM	Electrically Erasable and Programmable Read Only Memory
ENRP	Endpoint Name Resolution Protocol
EP	Exploitation Post
FCS	Frame Check Sequence
FIFO	First In First Out
FM	Fault Management
FTP	File Transfer Protocol
GDMO	Guidelines for Definition of Managed Objects
GPS	Global Positioning Systems
GSM	Global System for Mobile
HDLC	Hierarchical Data Link Control
HMI	Human-Machine Interface
HTML	HyperText Transfer Mark up Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
HW	Hardware
ICT	Information and Communication Technology
ID	Identifier
IEM&C	Infrastructure Equipment Monitoring & Control (mediation agent)
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
ISDN	Integrated Service Digital Network
ISP	Internet service Provider

JSON	JavaScript Object Notation
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Device
LLC	Logical Link Control
LM	Logs Management
LMA	Local Management Application
LON	Local Operated Network
M&C	Monitoring and Control
MAC	Media Access Control address
MCF	Management Communication Function (in TMN)
MEP	Mobile Exploitation Post
MIB	Management Information Base

NOTE: In SNMP for example.

MIME	Multi purpose Internet Mail Extension
MMI	Machine to Machine Interface
MNO	Mobile Network Operator
MOP	Master Operator
MTTR	Mean Time To Repair
MTU	Maximum Transmission Unit
mW	milliWatt
MySQL	multithreaded, Database Management System
NCP	Network Control Policy
NEM	Network Element Management
NETCONF	Network Configuration Protocol
NFS	Network File System
NIC	Network Interface Controller
NMS	Network Management System
OA	Operational Amplifier
OA&M	Operation, Administration and Maintenance
OPC	OLE for Process Control
O-RAN	Open RAN
OS	Operating system
OSF	Operating System Function (in TMN)
OSI	Open Service Interconnexion (in TMN))
OSS	Operations Support System
PAP	Password Authentication Protocol
PDA	Personal Digital Assistant
PEE	Power, Energy, Environmental parameters
PF	Power Factor
PFC	Power Factor Correction
PHP	Hypertext Preprocessor
PM	Performance Management
PMD	Power Monitoring devices
POP	Point Of Presence
PoS	Packet over SONET
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPPoA	Point-to-Point Protocol over ATM
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunnelling Protocol
PSTN	Public Switched Telephone Network
PSU	Power Supply Unit
RAN	Radio Access network
RC	resistor–capacitor
REST	REpresentational State Transfer
RESTCONF	Representational State Transfer Configuration protocol
RFC	Request For Comments
RMA	Remote Management Application
RMS	Root Mean Square

RPC	Remote Procedure Calls
RTP	Real-time Transport Protocol
RTSP	Real Time Session Protocol
SCTP	Stream Control Transfer Protocol
SDH	Synchronous Data Hierarchy
SIP	Session Initiation Protocol
SMB	Server Message Block
SMS	Short Message System
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SPICE	Simple Protocol for Independent Computing Environments)
SPX	Sequenced Packet Exchange
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol for IP
TF	Transformation Function
THD	Total Harmonic Distortion
TLS	Transport Layer Security
TMN	Telecommunications Management Network

NOTE: See Recommendation ITU-T M.3010 [1].

UDP	Use Datagram Protocol
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VC-MUX	Virtual circuit multiplexing
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAN	Wide Array Network
WIFI	Wireless Fidelity
WSF	Work Station Function
XDR	Cross-Enterprise Document Reliable Interchange
xDSL	Digital Subscriber Line
XHTML	eXtended HTML
XMPP	Extensible Messaging and Presence Protocol
XSL	Extensible Stylesheet Language
XSLT	eXtensible Stylesheet Language Transformation
YAML	Yet Another Markup Language

4 Monitoring and Control (M&C) overview

4.0 General

Several management levels are possible for telecommunication installations and equipment. They are described considering the complexity of the system, response time and required level of details from basic alarms to complex analysis level.

Performance Management (PM), Configuration Management (CM), Fault Management (FM), and Logs Management (LM) can be used for monitoring, controlling, and alarm handling of all site equipment, such as power, cooling, and other environment sensors information used to simplify operation, reduce maintenance time, reduce site intervention, reduce human error risk, and to give useful data for statistical analysis and management operations in the network.

The objective of the system is to reduce operational costs, improve reliability, improve the quality of the management system, and collect data from all available sensors to make statistical decision and estimation.

To achieve this purpose, monitoring information and control are needed, divided into four categories:

- Performance Management (PM) includes:
  - Measurements of all equipment sensors reported, time stamp, time report.
- Configuration Management (CM) includes:
  - The controls are commands to the equipment, configuration, and settings.
- Fault Management (FM) includes:
  - The information about alarms, alarm acknowledge, events, time stamp, time report.
- Logs Management (LM) includes:
  - Data and logs recordings of sensors, events, traces, time stamps of all available equipment sensors, and logs transmission to a central location.

In many cases, the same basic information from the equipment-monitoring interface is needed to address different services that prepare information as requested by users' categories.

A list of mandatory and optional sensors is provided in clause 6.1, and the detailed descriptions are contained in the different parts of the present document.

4.1 Infrastructure equipment management network general description

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

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

Referring to Recommendation ITU-T M.3010 documents for nomenclature [1] and [2], the following elements can be understood as generic parts of Telecommunication Management Network (TMN):

- The Control Unit (CU) is dedicated to controlling one or more pieces of equipment in a site.
- The Data Gathering Unit (DGU) is used to gather one or more CU field buses to adapt to TMN protocol and format. The DGU is a Mediation Function in Recommendation ITU-T M.3010 [1] (TF).
- CU and DGU may be combined in the same unit optionally, especially in the case of a site with little equipment installed there (e.g. POP, small radio site).
- The Local Management Application (LMA), if present, typically only on big telecom site installations, and Remote Management Application (RMA) servers process information received from the CU and DGU to achieve the functionalities of the management system, i.e. Operating System Function (OSF) in Recommendation ITU-T M.3010 [1].
- LMA can be combined with CU or DGU in related small installations.
- The Exploitation Post (EP) offers the man-machine interface. It can be integrated into the LMA/RMA or not (e.g. on Mobile Exploitation Post (MEP)). This entity manages the interactive presentation to the user to monitor and control the equipment. (Work Station Function (WSF) in Recommendation ITU-T M.3010 [1]).

Several CU and DGU can be managed within this network by one (or perhaps several) LMA or 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 Recommendation ITU-T M.3010 [1]).

Figure 1 presents a general network architecture:

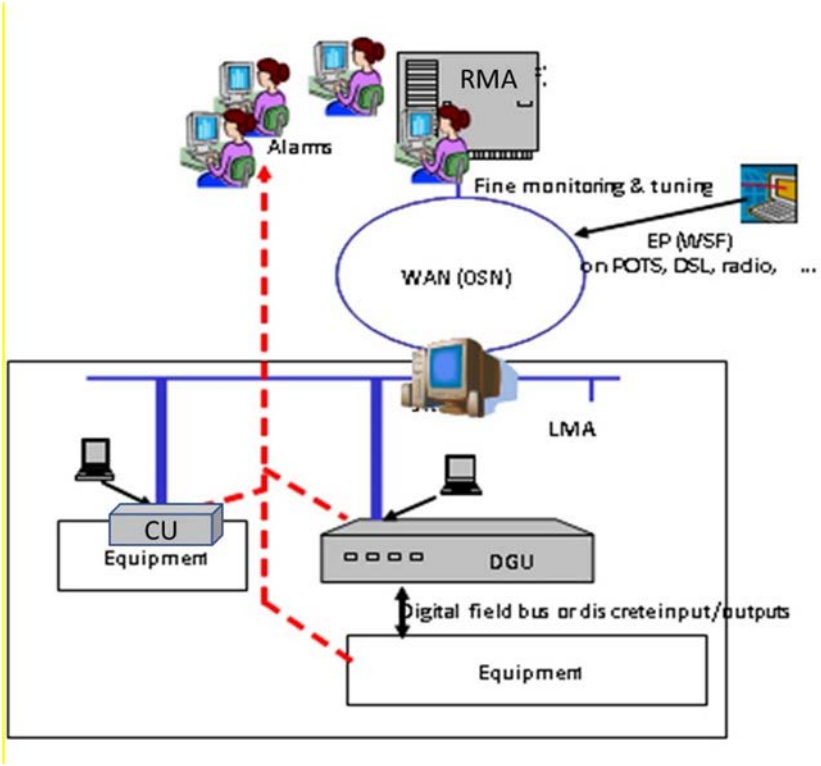


Figure 1: General network architecture

Each element (CU, DGU) shall be an HTTP node with a URL address able to exchange data as described in clause 10 "Data structure format for exchange between CU or DGU and LMA or RMA by infrastructure equipment monitoring & control agent".

4.2 Site Internal Communication Architecture

On a site, site equipment, site control unit(s), cooling equipment, and power equipment(s) may come from different vendors and support different levels of capabilities and versions of protocols for control and monitoring.

These units should include a higher level of intelligence as described below:

CU based architecture

The site equipment, cooling equipment, power equipment(s), and site control unit(s) are each connected to one CU, as presented in Figure 2. The CU monitors and controls the connected equipment through sensors and actuators (via serial, digital, or analogue interfaces). This functional unit is used for several functions:

- to collect data from one equipment via serial/digital/analogue interface/protocol and forward it to external NMS(s) via the Entry Point DGU;
- to receive commands from external NMS via the Entry Point data control unit (DCU) and forward them to the equipment as serial/digital/analogue commands;
- to act as a mediation between serial/digital/analogue interface/protocol and latest technologies communication protocols.

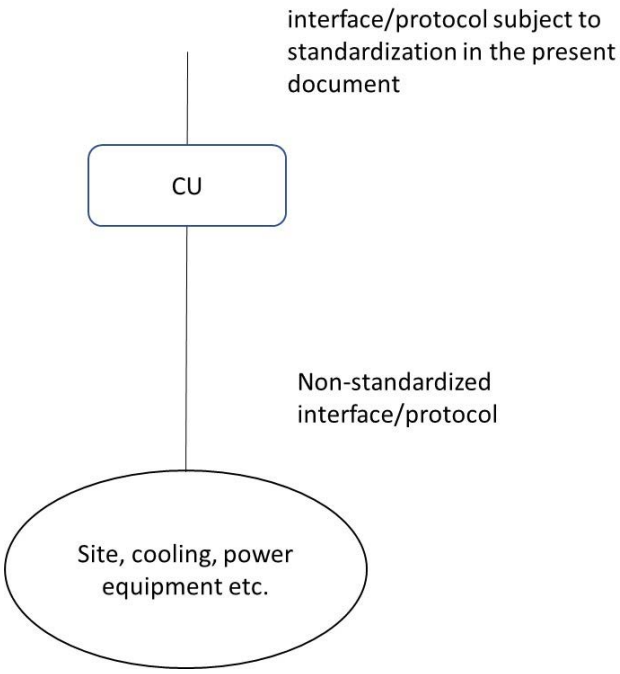


Figure 2: CU Based Architecture

DGU based architecture:

The site equipment, cooling equipment, power equipment(s), and site control unit(s) from the same vendor are connected to a DGU, as presented in Figure 3. This functional unit performs several functions:

- collects data from several pieces of equipment via serial/digital/analogue interface/protocol and forwards it to external NMS(s) via the Entry Point DGU;
- receives commands from external NMS via the Entry Point DGU and forwards them to the equipment as serial/digital/analogue commands;
- acts as a mediation between serial/digital/analogue interface/protocol and latest technologies communication protocols;
- supports the latest technologies communication protocols i.e. REST/HTTP/YAML/YANG.

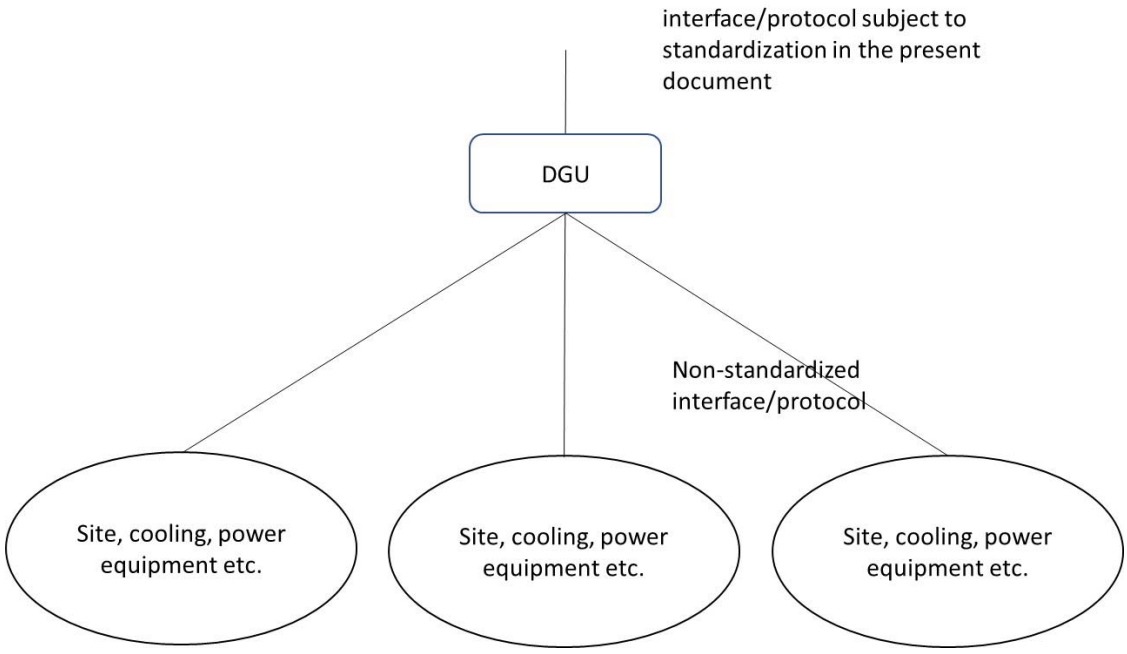


Figure 3: DGU Based Architecture

Entry Point, as reported in Figure 4, is the input/output point between the site and the external NMS(s).

Entry Point it is used as input in the telecom site for the control and monitoring of the following type of on-site equipment:

- Power (e.g. rectifiers, batteries, solar panels, solar regulators, generators, fuel cells) via their CU/DGU.
- Cooling systems via their CU/DGU.
- Building controls via their CU/DGU.

Collection links of sensors, CU, and DGU internal to the site can be wired or wireless.

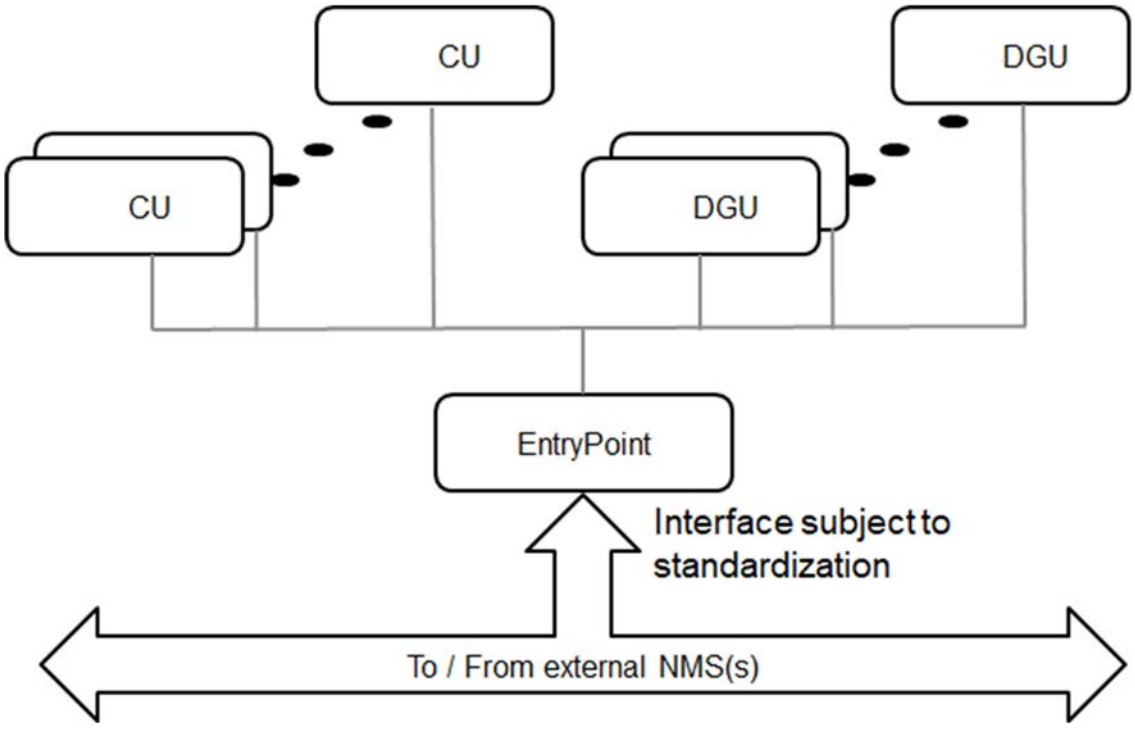


Figure 4: Entry Point

4.3 Infrastructure Equipment Monitoring & Control management network example

Figure 5 gives an example of the network and operation elements used for operating a medium size building.

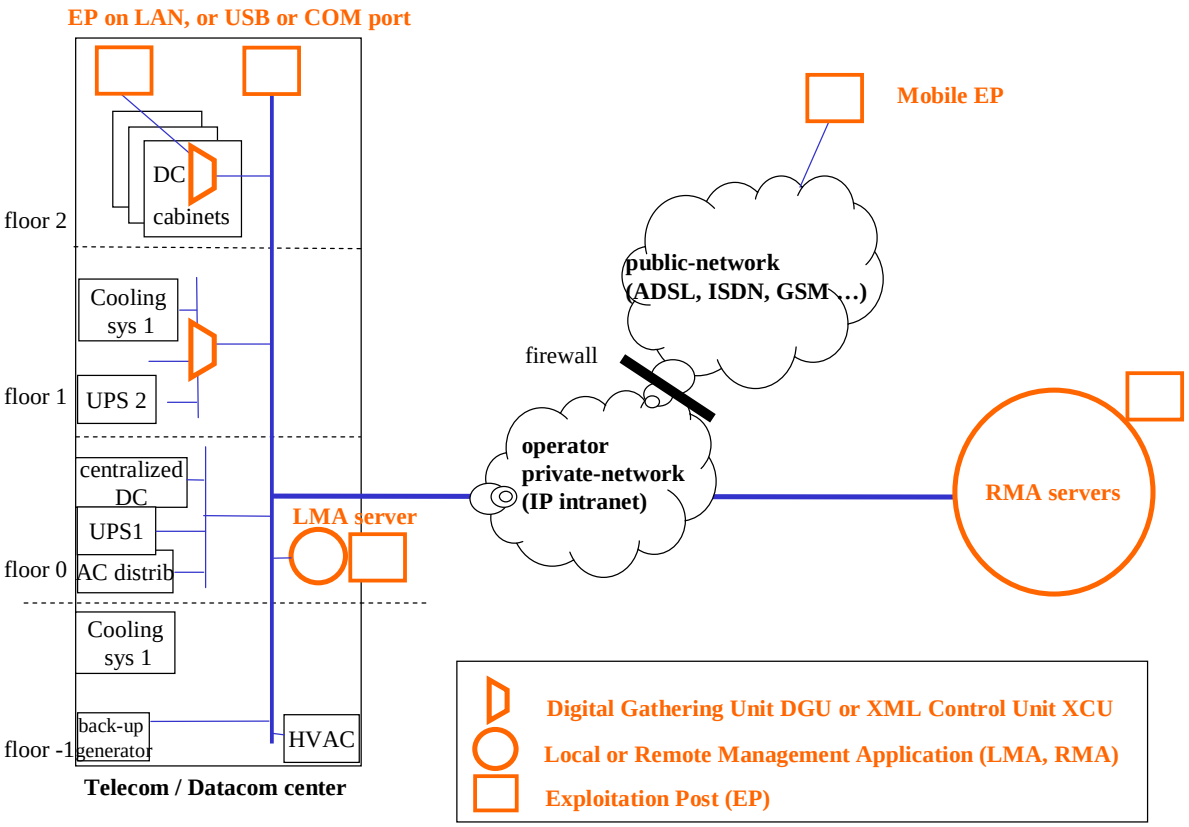


Figure 5: Example of IEM&C network implementation

In this case, a Local Management Application is present on-site located on a dedicated local server.

A user connection point to the Infrastructure equipment monitoring & control management network should be made available at the following locations:

On-site:

- locally on the equipment control unit via an integrated display or connection to laptops, tablets, smartphones, or similar devices;
- on a centralized server through a LAN;
- on a client display (e.g. laptops, tablets, smartphones, or similar devices), through the LAN or wireless connection (wifi, Bluetooth or similar).

Remotely:

- on one post of the supervision room, in the remote supervision of several centres, through a private or public network;
- In a non-dedicated supervision room by maintenance/operation people using internet connection and laptop, smartphone, tablet or similar ICT equipment.

Connecting directly to CU or from a remote connection, the user equipment shall use a web-browser-based interface, and without the need for proprietary software. To simplify maintenance and avoid security problems in case of IP network failure, there shall be a means 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 5.2 for details on HMI.

4.4 Infrastructure Equipment Monitoring & Control management scenario

The overall architecture, including how the Entry point communicates with NMS(s), is described here according to three scenarios.

Different scenarios of ICT sites are discussed, considering responsibility and equipment management.

The scenarios are described for typical mobile network cases but can be easily expanded to other types of networks.

Scenario #1: Site and network equipment owned by the operator

This scenario considers that the site is owned and managed by a single operator.

In this scenario, the following actors are involved:

- Operator: owns and operates the ICT site and site equipment, but also controls and monitors site equipment and on-site ICT equipment related PEE data. The operator owns the following elements:
  - Telecom site.
  - Site equipment (incl. cooling systems), equipped with CU or DGU.
  - Site control unit(s), equipped with CU or DGU.
  - Power unit(s), equipped with CU or DGU.
  - ICT equipment with embedded sensor.

As observed in Figure 6, the following principles apply:

- The OA&M channel used by the operator to collect ICT equipment performance measurements (as well as to collect alarms, provision configuration parameters, etc.) also serves to collect and monitor PEE data via the same API and protocol.
- All collected data is sent in-band via the OA&M channel to Operators NMSs via the latest technologies telecom protocol.
- Entry Point collects PEE data from/to all site CUs/DGUs and interfaces with the NMSs via OA&M.
- ICT equipment send their PEE data, as well as any other ICT equipment performance measurements, directly via the OA&M channel.

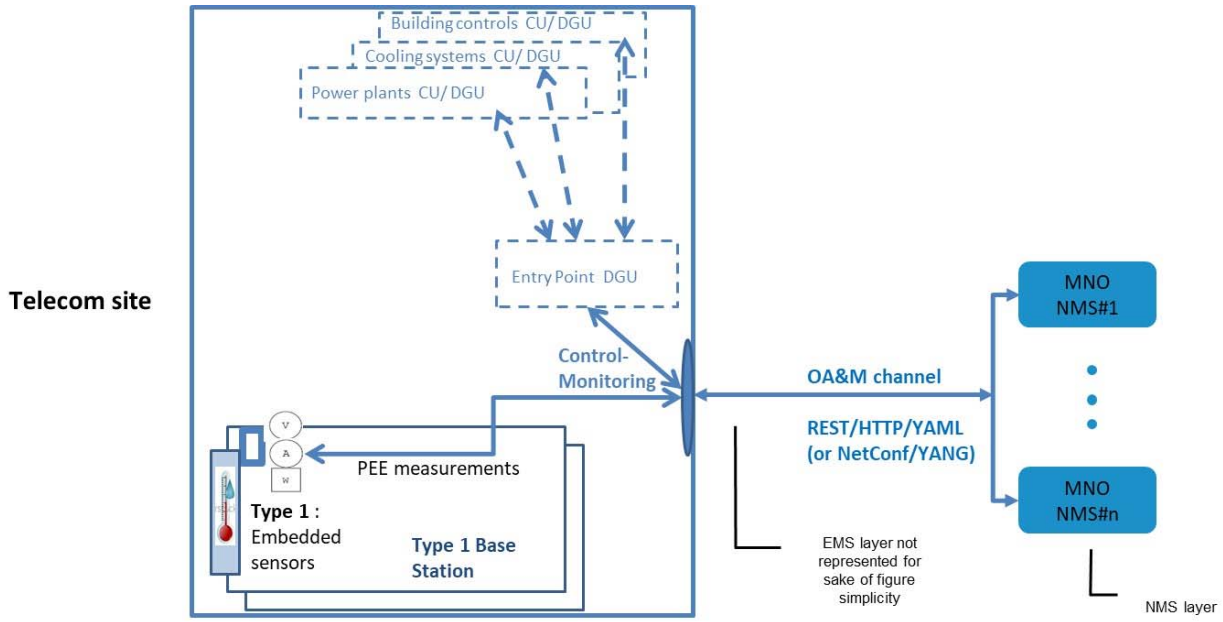


Figure 6: Architecture for Scenario #1

NOTE: The blue circle is a virtual interface that should be implemented also via a router.

In this scenario, the Entry Point is deployed and managed by the operator.

Scenario #2: Site owned by Tower Company with one or more operators on the site

This scenario includes architecture such as Passive RAN sharing, involving Tower Company and operators:

- Tower Company owns and operates site and site equipment, controls and monitors site equipment related PEE data.
- Operator owns and operates on-site ICT equipment (e.g. BS), controls and monitors its BS, including related PEE data.

For any given BS site owned by a Tower Company, on-site BS equipment may be owned by different MNOs. Currently, Tower Companies owning BS sites do not use the OA&M channel of the BS(s) located on-site to communicate site equipment-related PEE data to/from the NMS(s). Tower companies use a different communication channel. The OA&M communication channel between the site Entry Point and the Tower Company NMS should use the same latest technologies APIs and communication protocols.

As represented in Figure 7:

- The telecom site belongs to Tower Company.
- Two Type 1 BSs (equipped with embedded sensors) are deployed on-site. It is possible that there can be more than two MNOs present on the site:
  - One belongs to MNO#1.
  - Another one belongs to MNO#2.

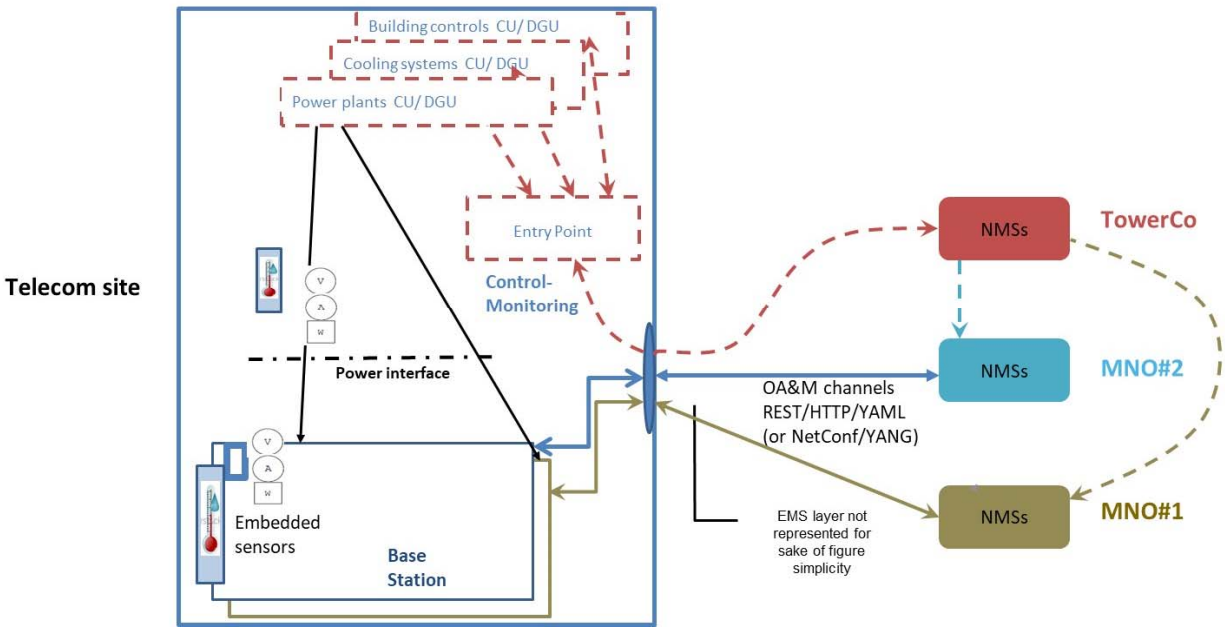


Figure 7: Architecture for Scenario #2

In this scenario, the following principles apply:

- Tower Company collects all site-related PEE data as well as BS PEE data.
- MNO#1 and MNO#2 collect their own BS-related PEE data.
- Tower Company could provide MNO#1 and MNO#2 with (part or all of) their BS PEE data. In this way, Tower Company can monitor all the site and optimize the site utilization, increasing the efficiency at site level and as a consequence of all the network.
- Interface and information exchange between the Tower company NMS and MNO NMS is outside the scope of the present document.

In this scenario, it is possible to consider one single Entry Point deployed and managed on-site by the Tower Company, as a separate unit. This Entry Point should enable communication between Tower Company NMS and all on-site CUs/DGUs.

Scenario #3: Active RAN sharing

This scenario considered operators with different rule: Master and participating operator, their roles are involved as defined in ETSI TS 132 130 [12]:

- Master Operator (MOP): owns and operates site and site equipment, controls and monitors site equipment related PEE data, owns and operates on-site BSs, controls and monitors BS-related PEE data.
- Participating Operator: Participating MNOs are service providers who share, alongside other Participating MNOs, the RAN facilities provided by the Master Operator.

As presented in Figure 8:

- The site belongs to the Master Operator.
- Two BSs are deployed on-site and owned by the Master Operator.
- Both BSs are managed by the MOP. The Master Operator is the only one to have a direct NMS connection to the site and shared BS(s).
- Master Operator provides Participating MNOs with (part or all of) its BS(s) PEE data as well as site-related PEE data, based on their RAN sharing agreement.

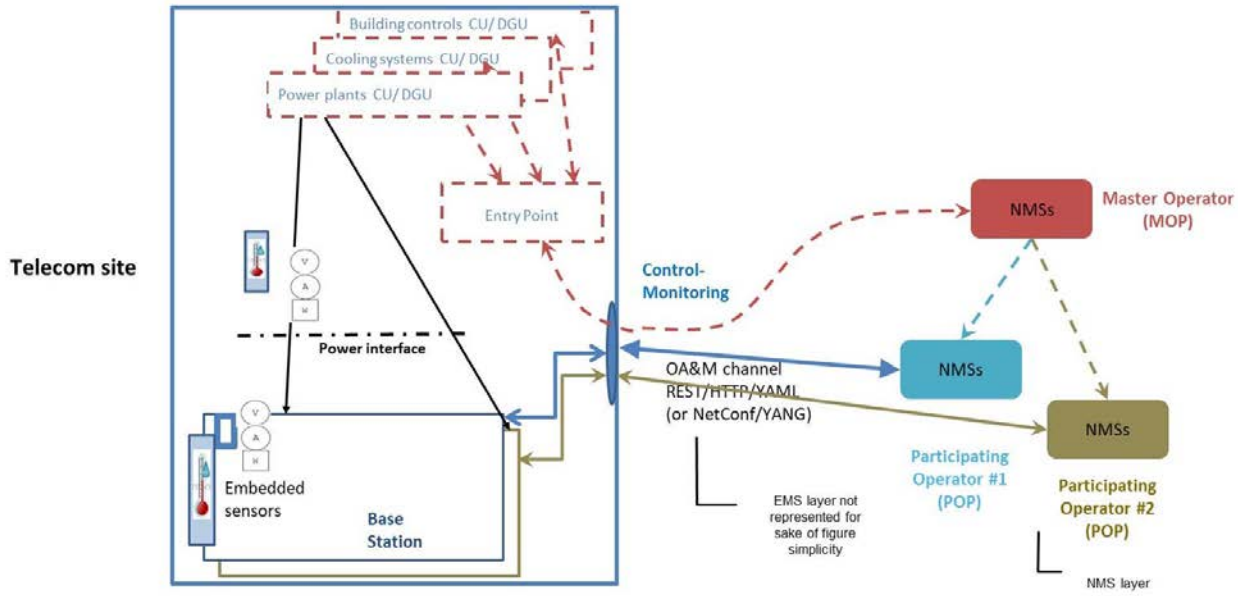


Figure 8: Architecture for Scenario #3

In this scenario, two options exist regarding Entry Point:

- one single Entry Point is deployed and managed on-site by the Master Operator, as a separate unit, when the Master Operator is different from any Participating Operator; or
- one single Entry Point is deployed and managed on-site by the Master Operator, as part of a BS equipment, for instance when the Master Operator is also a Participating Operator.

This Entry Point should enable the communication between Master Operator NMS and all on-site CUs/DGUs. Note that CU, DGU and Entry Point may be co-located.

5 Infrastructure equipment monitoring & control management interface and network architecture

5.0 General

Interfaces and architecture are mainly determined by structuring principles following an OSI model layer approach (Open Service Interconnection) ISO/IEC 7498 [7]. TCP/IP [6] shall be used for new interfaces with REST mechanism to exchange formatted data at application layers through HTTP services and HTTP parameters (Annex A, IEM&C agent) as previously introduced in clause 4.

In addition, network elements may act as web servers 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 Annex F.

Access service PPP over different networks, such as Ethernet, intranet, and internet, are also introduced in Annex F.

Referring to Recommendation ITU-T M.3010 [1], the physical and logical networks used to interconnect all units in the network provide DCF and MCFfuntions:

- Data Communication Function (DCF) covers the OSI layers 1 to 3. These layers are supported by every entity with 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.

5.1 Distributed 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.

5.2 CU, DGU, LMA management interface

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

- Machine-Machine Interface (MMI):
  - MMI with equipment: the site machines CU, 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 (e.g. CU, DGU, LMA) transmit data as follows:
    - in server mode: data transfer 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, in text or graphical format).
  - This should be achieved by XHTML and PHP for dynamic variable value refresh.

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 the easier its configuration management. At a minimum, LMA could be a client of CU only. LMA acts as a transparent routing unit with the CU for the RMA, just adding a site layer (synopsis, alarm severity re-qualification, etc.).

The present interfaces and architecture clause covers the preparation of data for the functions that shall be performed at management level.

The following clauses will detail the functional requirement for LMA, RMA, such as performance, safety, data integrity, and coherence.

5.3 Interface and protocol diversity

Figure 9 shows where the intelligence can be, depending on the more or less decentralization of intelligence. The location of "intelligence" has a high influence on network and server capacity.

Intelligence should be distributed in the equipment CU or DGU.

Interface and protocol types are the following as illustrated in Figure 9:

- interface 1 from sensor to CU;
- interface 2 from sensor to concentrator;
- interface 3 from CU to DGU;
- interface 4 from CU to concentrator.
- Low intelligence interface: (see clauses 5.5.1 and 5.5.2 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.

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 a large number of CU.

- High intelligence interface: (see clause 5.5.3) no protocol is standardized by the present document; any available protocol could be used.

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 clause 5.5.3) in real sites, the management network shall accept a mixture of every interface type previously described.
- The initiation, management and termination of measurement jobs from an Operations Support System (OSS) and the reporting of performance measurements can be done via either Representational State Transfer (REST)/HTTP/Yet Another Markup Language (YAML) or Yet Another Next Generation data modelling language (YANG)/NETCONF APIs.
- Operations of Control/configuration are also possible using either REST/HTTP/JavaScript Object Notation (JSON) or Network Configuration Protocol (NETCONF)/YANG APIs.

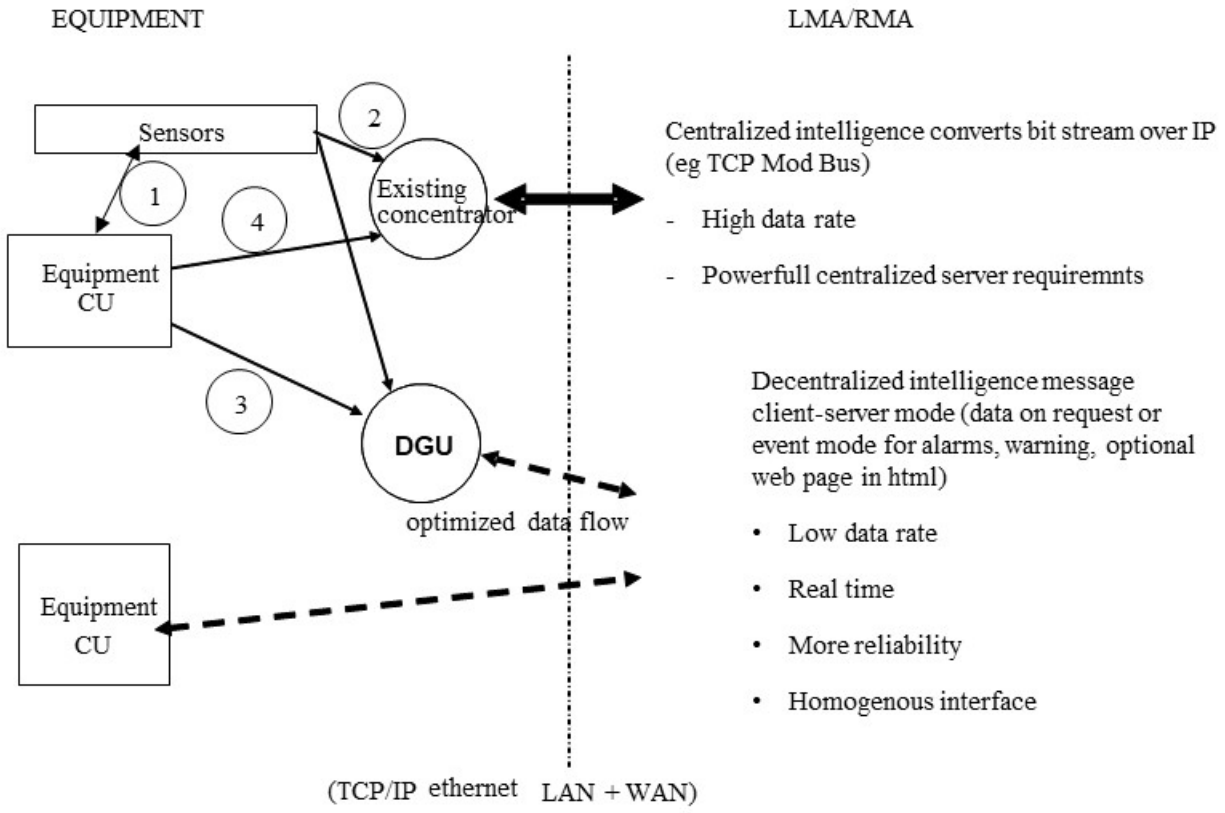


Figure 9: Interface types and distributed intelligence in the network

5.4 Open interface and software

Consequently, any new interface of infrastructure equipment, CU, DGU, LMA or RMA should be open and documented in detail to allow better interconnection, mediation, inter-operability, and further non-proprietary software development. A non-proprietary interface is necessary.

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

5.5 Interface levels

5.5.1 Alarm and state loops interface on CU or DGU output

Equipment and CUs/DGUs shall provide at least a summary of alarms that shall be reliably transferred to the RMA.

Network reliability should be considered for the development of control and monitoring network.

NOTE: In some existing installations there is the coexistence of alarm connection made by electronic contacts and relay contacts.

Passive reliability: an alarm information is supplied as an open loop so 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.

Three alarm synthesis loops shall be provided at least at the interface of each piece of equipment, using the qualitative alarm severity defined in clause 6.4.3:

- Major alarm.
- Minor alarm.
- Warning.

In addition, DGU or LMA with 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 CU or DGU shall correspond with one of the alarm loops.

As the information interface includes alarm synthesis, the availability of the alarm system shall be in accordance with IEC 60839-5-1 [4].

5.5.2 Low level protocol equipment CU mediation by DGU

In Figure 9, this interface is identified with the number 3.

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

The CU manufacturer shall provide a complete and detailed description of the bus and data.

The data retrieval and conversion require more or less work in the DGU to prepare a high-level user interface that is readable (e.g. avoiding repetitive standard messages.

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

The bit stream bus can transmit to the RMA over TCP. This option can be a solution for very small systems (shelters, street cabinets, underground locations) where the cost of DGU in addition to CU is a problem, but should be avoided.

5.5.3 CU and DGU high level protocol interface

The CU receives information (e.g. PEE) via sensors (Interface 1).

For 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 protocols in order to integrate a power or cooling or other facilities unit into a standard network management tool.

If SNMP is used on existing CU, it shall focus on channelling the alarm information and site information. DGU shall convert SNMP to a data structure in conformity with what is defined in clause 10 and standard equipment data interface described in other parts of this multi-part deliverable.

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. Figure 10 shows combined CU, DGU, LMA functions in one unit.

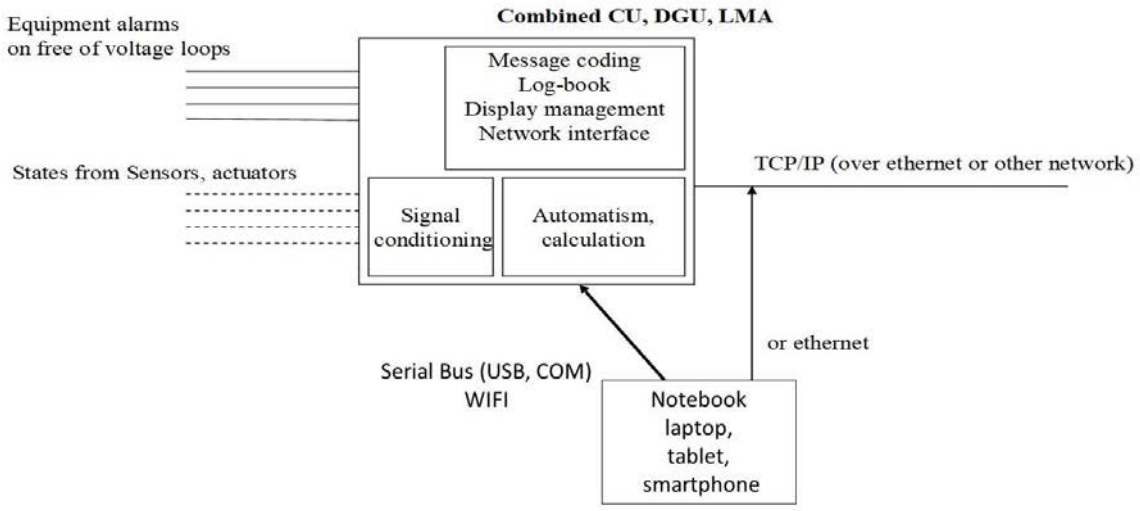


Figure 10: Principle of combined CU, DGU, LMA operation on a small site

5.6 Transport Control Layer

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

Interfaces between facilities equipment and CU or DGU should be other protocols, e.g. Modbus, CAN.

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 present document.

5.7 Physical and network layer

In a location where Ethernet is used, Ethernet interface shall be at least 100 Mbs.

For reliability and security purposes, the power and cooling management local network should be a dedicated Ethernet, not a shared office Ethernet.

Alarm input/output or monitoring field bus shall have connectors to allow maintenance tests 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.).

5.8 Network Management system upgrade

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 converts old CU protocols towards Ethernet XML.
- To add a new power or cooling equipment with CU and to add a LMA that can dialog with DGU and CU.

In Remote Management supervision rooms:

- It shall be possible, to progressively migrate from old supervision to new ones through Ethernet on an Intranet network.
- Existing higher level analysis and statistical application servers shall be able to get data though database interface with the new M&C RMA.

It shall be possible to connect a laptop, used for monitoring and control function, anywhere on Ethernet or by direct connection to local equipment or to a distant client.

6 Infrastructure equipment monitoring & control main goals

6.1 Data in the infrastructure equipment monitoring & control network

6.1.0 General

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

The structure is divided into mandatory minimum information that shall be available at the output of the equipment and optional data information.

NOTE: The optional information be/should be proposed to operators.

Mandatory information is required to sustain sufficient operation of the network.

Furthermore, the information is divided in low critical (minor) or critical (major) information for monitoring the structure of information will be defined in the structure reported in Figure 11.

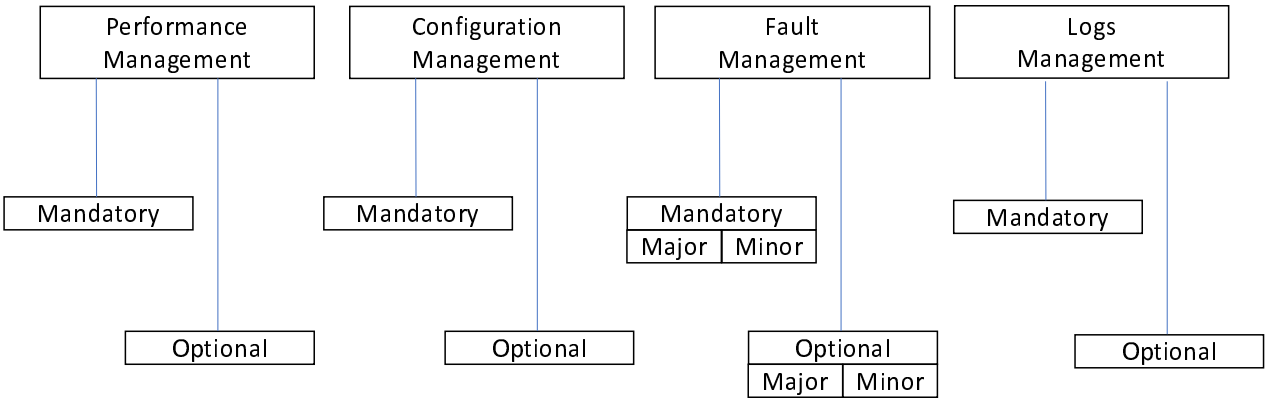


Figure 11: Information structure

- Performance Management (PM) includes:
  - Measurements of all equipment sensors reported, time stamp, time report.
- Configuration Management (CM) includes:
  - The controls are commands to the equipment, configuration and settings.
- Fault Management (FM) includes:
  - The information are alarms, alarm acknowledge, events, time stamps, time report.

- Logs Management (LM) includes:
  - Data logs, integers, vectors, events.

Energy management shall use performance management information and configuration management adding the functionality of site energy management. This give the possibility to perform energy efficiency, and management of energybased on energy cost.

A Control Unit (CU) 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 local display (MEP).

6.1.1 Mandatory data in the infrastructure equipment monitoring & control network

The mandatory information is transmitted through the interface and network to LMA, if present, and RMA. Data is classified as mandatory or optional depending on associated functions.

Mandatory data is used for:

- Performance & energy Management (PM):
  - Power, energy and environmental values reported, time stamps, and time reports. Included in this category, data indicating the minimum declared performance (e.g. energy stored in a battery, operational temperature, energy from different sources, etc.).
- Configuration Management (CM):

  The controls are commands and acknowledgment to the equipment, configuration and settings, several types of information shall be provided for this purpose at the equipment interface:
  - System command.
  - Default values resetting (e.g. safe value for batteries or engine operation).
  - Operational, state variables (i.e. on/off, physical measurements, counters).
  - Values resetting for all equipment (e.g. safe value for batteries or engine operation).

  Control could be local or remote process command individual test and global operation.
- Fault Management (FM):
  - The information are alarms, alarm acknowledge, events, time stamp, time report.
  - Alarming (e.g. Power Supply unit HW fault, battery fault, etc.). Mandatory are alarm classified as critical or major (see clause 6.4.3).
- Logs Management (LM):
  - Alarm logging (alarm history files).
  - Event logging (event history files).
  - Traces logging (event history files).
  - HW inventory log (eg Type of product, product number, revision) for maintenance.

NOTE 1: The alarm and event history files may be 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.

NOTE 2: For critical systems, major 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.

NOTE 3: Major, minor classification are present in the other parts of this multi-part deliverable.

6.1.2 Optional data in the infrastructure equipment monitoring & control network

In addition to the mandatory data described in clause 6.1.1, the following data are desirable but optional:

- Performance Management (PM) include: data reporting not impacting the minimum guaranteed performance. The definition of optional performance parameter classification is present in the other parts of this multi-part deliverable.
- Fault Management (FM): the definition of optional fault parameter classification is present in the other parts of this multi-part deliverable.

The information consists of alarms, alarm acknowledge, events, time stamps, time reports:

- Alarming and warning (e.g. Single fault in a duplicated unit) optional are alarm classified as minor or warning (see clause 7.5.1).
- Self-diagnosis results.
- Anti-theft alarm.

Free of voltage alarm contacts (defined by user) shall be available at the monitoring interface of the equipment. These contacts can gather several information to send only generic signals as major alarm or minor alarm. Generally, as the level of system complexity increases, additional supervisory information is required.

Logs Management (LM) shall contain the following information:

- measurement records (long duration);
- information on software download (process and monitoring network elements softwares, it may be for upgrading the CU or DGU or LMA);
- Information of change of management (passwords, networks addresses, calendar-clock synchronization all along the networks);
- dynamic graphical synopsis.

6.3 High level application and data structure flexibility

Equipment shall give the information as described in clause 6 at their monitoring interface so that telecom operators collect data from heterogeneous equipment and bring the information to a central supervision room or to the user equipment . 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 purposes is one of the main processes.

The management network shall manage the process operations reported below:

- 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 the telecom network.

In addition to alarms, event messages are provided to help understand failure and make intervention decisions.

Alarms or events fields are specified in clause 10. The requirements in the present document derives from telecom operators' and telecom equipment manufacturers' experience.

All the necessary information for this quality process is often not available in a single level (i.e. at the CU). It shall be possible to enrich the information by filling or adding fields at every network level (CU, 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 an 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 contents and type of the fields:

- filtering of repetitive events in LMA or RMA;
- classification of alarms in a site by DGU or LMA;
- classification or alarms between sites in RMA.

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

6.4 Data interface complexity and structure

6.4.1 Information

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

- Alarm synthesis contacts. (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).

NOTE: These alarm synthesis should be not the same number of alarm managed by monitoring system to avoid hardware overdevelopment.

- 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 is defined in clause 6. The generic descriptions of information structuring not linked to one specific process or protocol are provided in clause 10. These information structures consist of:

- Equipment CU, DGU self-registration (description and identification file).
- 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.

6.4.2 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 operates in the expected conditions.
- Alarms: this status is set for abnormal state, i.e. different to the specified normal state of hardware, software (e.g. load failure, updating failure, environment condition (thermal, humidity, etc.).
- 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 an infrastructure equipment, sub-system or system.

6.4.3 Alarm severity and event class

The technical severity levels can, for example, be classified in the following way:

- 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 + Diesel Engine failure + discharges battery should lead to a new alarm imminent site crash).
- Major: sometimes referred to as prompt, urgent i.e. the failure event may need an immediate maintenance intervention of the network operator.
- Minor: sometimes referred to 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 a long time.
- Warning: sometimes referred to as hint i.e. an event happens which normally does not need a maintenance intervention of the network operator.

NOTE: In some realizations, critical and major alarms can be combined.

Each of these simple severity levels shall correspond to a range of values defined by the operator depending on the network impact of failure, equipment, maintenance complexity 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 values.

7 Infrastructure equipment monitoring & control management typical content subsets

7.0 General

Figure 12 describes typical subset of infrastructure equipment and thermal environment covered in the present document. More detailed description can be found in ETSI ES 203 700 [i.30] and Recommendation ITU-T L.1382 [i.31]. Detailed monitoring and control information requirements for each of these subsets are provided in the standard dedicated to a particular infrastructure equipment (e.g. power station, battery, UPS).

Every subset (i.e. DC) is generally divided into functions and sub-functions (rectifiers, battery, etc.), with associated information (alarms, events, measurements, parameter sets, controls) described in the other parts of this multi-part deliverable. The information corresponding to a subset shall be provided at M&C management interface of this subset (generally on the CU interface). But for each subset function, the information shall be provided in accordance with the equipment configuration.

EXAMPLE 1: There is AC back-up switchgear information only if there is such a function in the AC distribution board equipment.

Each information is described as Mandatory or Optional in the relevant part.

EXAMPLE 2: Partial AC metering is generally an option used only in large buildings.

Details on management information choices for each subset and function are provided in ETSI TR 102 336 [i.1] and standardized in the applicable parts of this multi-part deliverable.

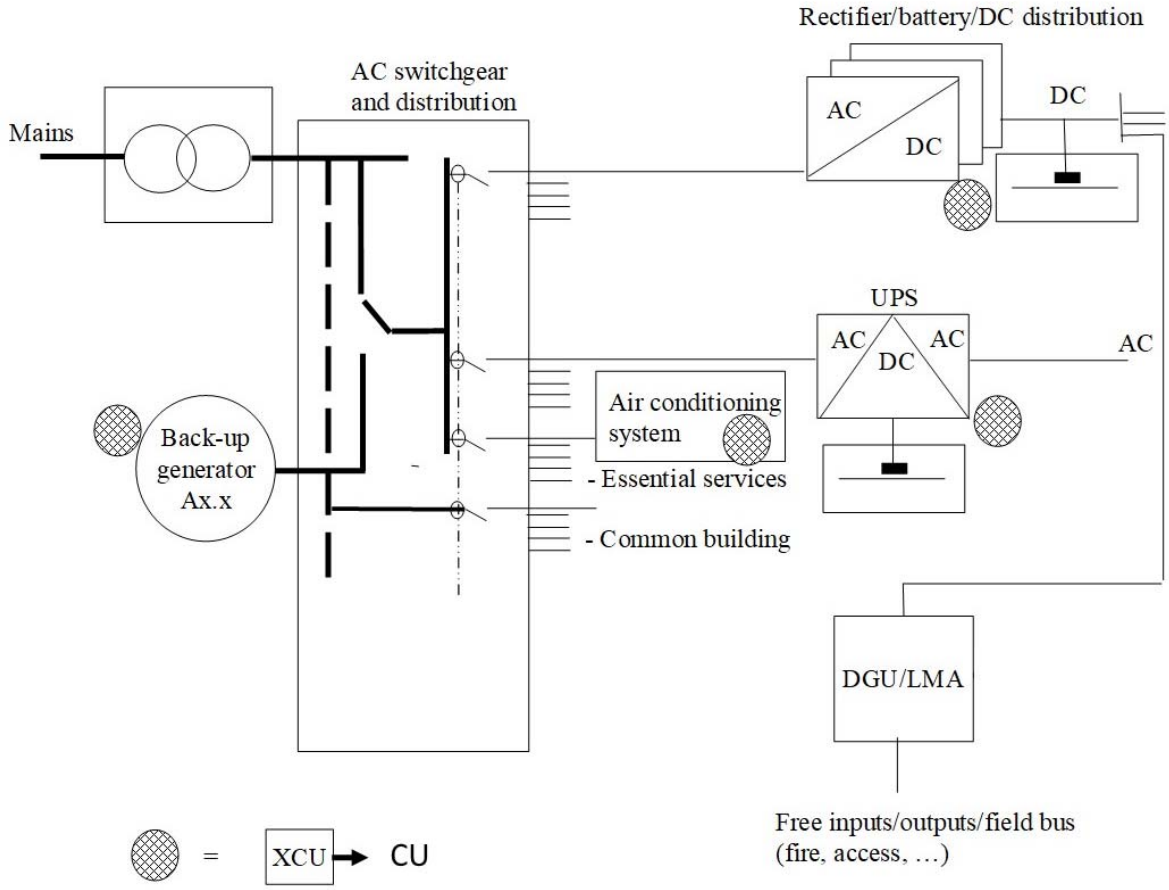


Figure 12: Typical subsets of infrastructure covered in the present document

Here is a not exhaustive tree summary of all the facilities and ICT equipment covered by the standard. All the bolded equipment is quickly described in the following paragraphs, and in more detail in the multi-parts deliverables of ETSI ES 202 336 series:

- **site** (the present document):
  - energy_system (the present document):
    - **dc_system** (ETSI ES 202 336-2 [i.12]):
      - rectifier (ETSI ES 202 336-2 [i.12]);
      - battery (ETSI ES 202 336-2 [i.12]) and ETSI ES 202 336-11 [i.21]).
    - sensors_actuators (the present document).

- ac_ups_system (ETSI ES 202 336-3 [i.13]):
  - rectifier;
  - inverter;
  - static_bypass_switch;
  - battery;
  - protection_and_distribution.
- **ac_distribution_switchboard** (ETSI ES 202 336-4 [i.14]).
- **diesel_backup_generator_system** (ETSI ES 202 336-5 [i.15]):
  - starting_circuit;
  - fuel_circuit;
  - oil_circuit;
  - air_circuit;
  - cooling_circuit;
  - power_circuit;
  - auxiliary_power_circuit.
- air_conditioning_system (ETSI ES 202 336-6 [i.16]).
- remote_power_feeding_system (ETSI ES 202 336-8 [i.18]):
  - up_converter_system (ETSI ES 202 336-8 [i.18]);
  - remote_site (ETSI ES 202 336-8 [i.18]):
    - down_converter_system (ETSI ES 202 336-8 [i.18]);
    - sensors_and_actuators (the present document);
    - air_conditioning_system (ETSI ES 202 336-6 [i.16]);
    - (other parts like a site).
- inverter_system (ETSI ES 202 336-10 [i.20]).
- alternative_power_system (ETSI ES 202 336-9 [i.19]):
  - solar_converter (ETSI ES 202 336-9 [i.19]);
  - wind_power_rectifier (ETSI ES 202 336-9 [i.19]);
  - fuel_cell (ETSI ES 202 336-9 [i.19]).

- other_utilities_system (ETSI ES 202 336-7 [i.17]):
  - access_system (ETSI ES 202 336-7 [i.17]);
  - video_system (ETSI ES 202 336-7 [i.17]);
- sensors_actuators (the present document).
- ICT equipment (ETSI ES 202 336-12 [i.22]).

7.1 DC power system ETSI ES 202 336-2

ETSI ES 202 336-2 [i.12] covers power station system control and monitoring.

7.2 AC UPS power system ETSI ES 202 336-3

ETSI ES 202 336-3 [i.13] covers AC UPS power system control and monitoring.

7.3 AC distribution switchboard ETSI ES 202 336-4

ETSI ES 202 336-4 [i.14] covers AC distribution power system control and monitoring.

7.4 AC diesel back-up generator ETSI ES 202 336-5

ETSI ES 202 336-5 [i.15] covers AC diesel back-up generator system control and monitoring.

7.5 Thermal environment and cooling system ETSI ES 202 336-6

ES 202 336-6 [i.16] covers Air conditioning System control and monitoring.

7.6 Other utilities system ETSI ES 202 336-7

ETSI ES 202 336-7 [i.17] covers other utilities system control and monitoring.

7.7 Remote power feeding system ETSI ES 202 336-8

ETSI ES 202 336-8 [i.18] covers Remote Power feeding System control and monitoring.

7.8 Alternative power systems ETSI ES 202 336-9

ETSI ES 202 336-9 [i.19] covers Alternative power System control and monitoring.

7.9 AC inverter power system ETSI ES 202 336-10

ETSI ES 202 336-10 [i.20] covers AC inverter power System control and monitoring.

7.10 Battery system with integrated control and monitoring information model ETSI ES 202 336-11

ETSI ES 202 336-11 [i.21] covers Battery system with integrated System control and monitoring.

7.11 ICT equipment power, energy, and environmental parameters monitoring information model ETSI ES 202 336-12

ETSI ES 202 336-12 [i.22] covers ICT equipment power, energy, and environmental parameters monitoring information model.

8 Principle of Power, Energy, Environmental parameters (PEE) measurement

8.0 General

The principle of the measured data acquisition, local processing, and robust data saving for reliable remote monitoring and control are described in clauses 8.1 to 8.7. More details are given in Annex F on the data measurement chain and state-of-the-art measurement with fair accuracy.

PEE measurement type, accuracy, test methods and data preparation for remote transmission are defined in order to provide the mandatory monitoring/supervision information defined in the relevant parts of this multi-part deliverable.

8.1 Power and energy consumption measurement

The power and energy metering are mandatory. Monitored values are defined in the part covering specific equipment type. The power is in Watt and the energy is the cumulated active energy metering in Wh or kWh at the input of the considered Equipment.

NOTE 1: For equipment used in network, normally the energy consumption is measured in kWh.

Considering the record period Tr defined in clause 8.4, the physical expression of instant power P(t), power consumption E(Tr), and mean power P(Tr) over Tr are:

- $P(t) = u(t).i(t)$
- $E(Tr) = \int_0^{Tr} P(t)dt$
- $P(Tr) = \frac{1}{Tr}E(Tr)$

Where u(t) and i(t) are instant values of voltage and current at the AC or DC power interface of the Network Element under measurement.

The equivalent discrete expressions are:

- $P(j) = u(j).i(j)$
- $E(j) = P(j).Tacq$
- $E(Tr) = \sum_{j=1}^{n} E(j)$
- $P(Tr) = \frac{1}{Tr}E(Tr)$

Where u(j) and i(j) are values of voltage and current acquired over the Tacq period by analog-digital conversion equipment of measurements at the AC or DC power interface of the Network Element under measurement.

NOTE 2: The physical formula applies to any variable signal (i.e. any combination of AC and DC) with no limit in frequency. The discrete formula includes the limits of the sampling period Ta of voltage and current.

NOTE 3: The reactive power and energy are not measured and recorded as most often Network Element defined in Table 1 are powered in DC at their power interface and when they are powered by AC they generally use power supply with a true power factor very close to one, corresponding to reactive power close to zero.

The True Power Factor is defined as follows:

- True Power Factor = [Displacement Factor] x [Distortion Factor], where:
  - The Displacement Factor is cosine of ø, where ø = the phase angle between AC current and voltage of 50/60 Hz fundamental signals.

- The Distortion Factor depend on how well the PFC (Power Factor Correction) present in a equipment is working and should be as close to the value one ("1") as possible:

  DF)$DF) = \left(\frac{V_{01}}{V_{or}}\right)$ where V01 is the fundamental RMS value and Vor total RMS value

8.2 Voltage, current measurement

The electric voltage and current measurement defined in Annex B are optional. When required or used for power/energy calculation, they shall be of RMS type in order to achieve accurate measurement of dynamic waveform as they are more and more observed on equipment e.g. with power adaptation to performance demand. To this intention, the RMS value informs on the heating potential (i.e. active power when applied to a pure resistive load) of a measured voltage or current independently of its waveform.

The evaluation formula of RMS value of variable measured value X over T_{rms} period is:

$$X\,rms = \sqrt{\frac{1}{Trms}\int_0^{Trms} X^2(t)dt}$$

where X can be the current or the voltage.

NOTE 1: The true RMS value is the more accurate and is evaluated as the root of the fast integration of the squared measured raw value over the T_{rms} period. The approximative RMS determination based on peak detection and average rectification should not be used as it is only accurate for a given waveform for which it is calibrated. For some other waveforms, the error can reach -40 % as reported in LT0511 [i.27].

NOTE 2: The period T_{rms} of RMS calculation should be of one second at maximum as it is used to determine maximum and minimum values that will be recorded as defined in clause 8.4.

NOTE 3: The true RMS integration is considered as fast enough when it gives the defined accuracy at the maximum waveform frequency intended to be measured in the accuracy tests described in clause 8.5. The acquisition period of measured values used in the RMS integration is Tacq. A low frequency pass filter averaging the measured value over Tacq can be used as described in Annex H.

NOTE 4: There is no physical equivalent of RMS Power or Energy. Only active power or energy are defined in clause 8.1 to account for fast variations waveforms of power mainly resulted from fast variation of current.

8.3 Accuracy of PEE measurement

8.3.1 Electrical measurement accuracy

The sensors, measurement and value processing chain shall provide a defined accuracy the derating with temperature over their whole lifetime should be considered. Other part of this standard series shall use the accuracy defined in this clause or, if that is not possible due to the specificity of the equipment, the Manufacturer should declare the accuracy/standard used and also give the information on the information sent to the management system (see clause 10.1.6). The accuracy defined here applies to all parts of this standard series, if no other accuracy is defined in the respective to parts of the multi-part standard series.

The end-to-end measurement and processing chain from sensor to end recorded value is critical for maintaining accuracy over the whole lifetime time, including the evolution of the ICT equipment and power distribution in the site.

The measurement and processing chain includes pre-filtering (e.g. against noises and anti-aliasing as illustrated in LT5011 [i.27]), data-acquisition and analog/digital conversion, calculation such as RMS value and software settings for better accuracy (e.g. corrections of offset, linearity, noises, etc.). The defined settings and processing software shall be saved locally and on remote server for restoration in case of maintenance or failure.

NOTE 1: Embedded self-calibrations and tests of the measurement chain can be proposed to maintain measurement accuracy over the whole lifetime. Example of this solution is reported in [i.28] from one energy metering chip manufacturer.

The measurement of active power and the energy metering shall have the following accuracy:

- Accuracy 1 ±3 % from 25 % to 100 % of maximum load of the equipment (load range 1)
- Accuracy 2 ±5 % between 5 % and 25 % of maximum load of equipment (load range 2)
- For both accuracy, equipment the 100 % load is specified as the maximum power of each considered ICT network

The accuracies of the voltage and the current measurement are defined in order to obtain the defined accuracy of power and energy and as optional in Annex B: they should be as follows:

- Voltage accuracy ±1 %
- Current accuracy 1 ±3 % from 25 % to 100 % of maximum load of the equipment (load range 1)
- Current accuracy 2 ±3 % between 5 % and 25 % of maximum load of the equipment (load range 2)

NOTE 2: When power calculation is based on product of voltage and current. Power accuracy is driven by current accuracy.

The accuracies of power measurement and energy metering shall be defined in the normal indoor operating temperature range of the relevant class according to ETSI EN 300 019-1-3 [11] for which the equipment is designed.

When operating the equipment in an outdoor environment defined in ETSI EN 300 019-1-4 [i.29], the power measurement and energy metering accuracy can be extended to ±5 % in load range 1.

The accuracy verification tests are defined in clause 8.6.

The frequency measurement accuracy is not mandatory, and such accuracy is not defined in the present document. The monitoring of frequency is defined for AC distribution system control-monitoring in ETSI ES 202 336-4 [i.14]:

- Environment measurement type and accuracy.
- The temperature measurement shall have an accuracy of ±1 °C.
- The humidity should be measured with a sufficient accuracy e.g. ±3 % (see Table B.1).

For Indoor equipment the temperature accuracies shall be defined in normal indoor operating temperature range of the relevant class according to ETSI EN 300 019-1-3 [11] for which the equipment is designed.

For outdoor equipment operating in an outdoor environment defined in ETSI EN 300 019-1-4 [i.29], the temperature accuracy can be reduced to ±2 °C.

NOTE 3: The accuracy of temperature and hygrometry are defined when the temperature is stable i.e. when the variation is lower than ±1 °C over 5 s.

8.3.2 Compatibility with IEC standard

IEC 61557-12 [i.32] specifies requirements for fixed or portable PMDs that measure and monitor the electrical parameters quantities (U, I, P, E, THD, etc.) within electrical distribution systems in single- and three-phase AC or DC networks having rated voltages up to 1 000 V AC or up to 1 500 V DC.

Power Monitoring Device (PMD) are defined in IEC 61557-12 [i.32].

The classification depends on the use of monitoring devices:

- PMD-I can be used in several applications, including basic Energy Efficiency applications.
- PMD-II can be used in basic power monitoring applications and advanced Energy Efficiency applications.
- PMD-III can be used in advanced power monitoring applications and for network performance.

Depending on the type, different performance classes are defined.

The accuracy defined for power meter in IEC 61557-12 [i.32] is higher than the accuracy defined in the present document, so sensors in in line with IEC 61557-12 [i.32] are in line with the requirement of the present document.

8.4 Local acquisition record

A local acquisition record of data over a defined record period T_{rec} consists in a set of voltage, current, temperature/humidity, power, energy, and some indirect data such as minimum and maximum values.

Recorded values are defined as follows:

- Electric values (current, voltage, power) shall be average of the true RMS measurements over T_{rec} period.
- Energy shall be a cumulated value over T_{rec} period.
- Temperature and hygrometry are average value over T_{rec} period.
- Minimum and maximum values of current, voltage, power, temperature/humidity are captured during the same period and recorded.

NOTE: These minimum, average and maximum values are useful for site engineering optimization.

Considering periodic data recording:

- It shall be possible to set remotely the record period at 5 to 60 minutes.
- The recommended acquisition period is 15 minutes.
- A record period option of 1 minute should be also proposed.

All data records shall be associated with a time stamp (date/hour at 1 s accuracy) and an identifier including equipment reference and site reference to allow further services of analysis of data integrity and correlation of energy consumption to telecom performance state and activities on remote analysis servers.

8.5 Accuracy verification

The defined accuracy of recorded data defined in clause 8.3 shall be verified with a true RMS laboratory meter with 1 % accuracy for electrical measurements and with a laboratory thermometer at ±0,5 °C for temperature.

The hygrometry measurement verification should be made with sufficiently accurate relative humidity laboratory measurement:

- The accuracy 1 and 2 defined in clause 8.2 for power, energy, voltage and current shall be verified with the following current waveform applied over on the local record period T_{rec} at the power interface of Network Element ICT equipment:
  - DC:
    - DC current at 5 %, 10 %, 25 %, 50 %, 75 %, 100 % of maximum load of equipment defined in clause 4.4.3.2, with an accuracy of ±1 %;
    - with a constant reference voltage (Ut) of 54 V for interface A defined in ETSI EN 300 132-2 [i.24] or the testing voltage Ut defined in ETSI EN 300 132-3 [i.25] for interface A3 with an accuracy of ±1 %;
    - at least for 10 % and 50 % load at minimum and maximum voltage of the DC interface with an accuracy of ±1 %.
  - AC:
    - AC current at 5 %, 10 %, 25 %, 50 %, 75 %, 100 % load;
    - with sinusoidal reference voltage 230 V 50 Hz with an accuracy of ±1 %;

        - at least at 10 % and 50 % load at minimum and maximum voltage of the AC interface (considering narrow European voltage range) with an accuracy of ±1 %.

    - Fast electric waveform:

        - a load variation from minimum to maximum load of the range at a period of 1 ms using a sinus waveform;

        - the test is done:

            a) in DC at reference voltage of 54 V DC for interface A defined in ETSI EN 300 132-2 [i.24] or the testing voltage Ut defined in ETSI EN 300 132-3 [i.25]; or

            b) in AC at reference voltage 230 V 50 Hz depending on equipment input type with an accuracy of ±1 %.

Considering temperature conditions and possible impact, the accuracy shall be verified at:

- at 25 °C ±2 °C for all loads and voltage defined in this clause;
- at 5 °C and 40 °C for 10 %, 50 %, and fast electric waveform loads only at the reference voltage with an accuracy of ±1 %.

8.6 Data transmission period

The transmission period is a parameter that can be set remotely from 5 to 60 minutes.

T_{trans} shall be equal or higher to T_{rec}.

When T_{rec} is lower than T_{trans}, several data records are transmitted together in a single transmission.

Transmission of local records shall be synchronized with NMS data transmission period.

8.7 Local record saving

The local data record defined in clause 8.5 shall be stored locally in case of network failure or delay in transmission. In general, local storage shall include data records for a few days.

Local storage shall save data records for a minimum of 4 days. In case of normal operation with NMS, the storage duration should be aligned with NMS requirement.

For longer saving time requirement, there can be in addition an aggregation of the recorded values taking a longer averaging period in order to keep minimum data retention over long time. For example, the memory capacity is of several months of hourly averaged values on a remote BS on standalone energy and difficult access to the site.

9 Supervisor functions and performance

9.0 General

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 provide:

- monitoring of several pieces of 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 provide:

- monitoring of several sites;
- 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 also be done in CU or DGU.

Following generic functions should be provided:

- 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).

In addition, for compatibility with existing supervision systems, the LMA and RMA shall be an open server. 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.

10 Data structure format for exchange between CU or DGU and LMA or RMA by infrastructure equipment monitoring & control agent

10.0 General

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 document which shall be generated by a DGU. CU will generate parts of this document, e.g. some field such as site Id are not available in CU and should be added at a higher level of the management network.

10.1 Standard elements of any equipment, system or subsystem

10.1.1 Standard elements

For each equipment, system or subsystem, the attributes are defined in Table 1.

Table 1: Element attributes definition

Attribute	Description	Datatype	Optional/Mandatory
id	The id of the equipment, system or subsystem.	integer	M
status	"normal" or "alarms" or "unknown". For any detailed alarm (clause 10.4.2) 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".	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".	integer	M
short_description	A very short description of the equipment.	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.	datetime	O

For each equipment, system or subsystem, child elements that can be used are described in Table 2.

Table 2: Child element definition

Child Element	Description	Datatype	Optional/Mandatory
<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 of structured elements are described further.

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

10.1.2 Alarm and event message

An event (alarm set, alarm clear, information or cold start) generated by an equipment will be forwarded by the DGU to the management application LMA/RMA. This means that alarms or events messages can be posted without waiting polling from LMA or RMA.

Elements/Fields recommended in Recommendation ITU-T X.733 [3] can be found in the whole structure of the posted structure.

HTTP makes use of Transmission Control Protocol (TCP) which is a core element of the Internet Protocol Suite. Unlike UDP, TCP provides a reliable service where messages are delivered in order. This means that the application level does not have to care about the good transmission of messages.

When a DGU posts events upon an alarm change of state, this event is acknowledged by the NMS by accepting the posted message. In case the event is not acknowledged, it is resent periodically by the DGU. No event can remain unnoticed, this is 100 % reliable. The maximum event delay in case of connection failure is equal to the duration of connection failure + event "resending period". The solution is resource efficient (passive NMS). Figure 13 illustrates the mechanism.

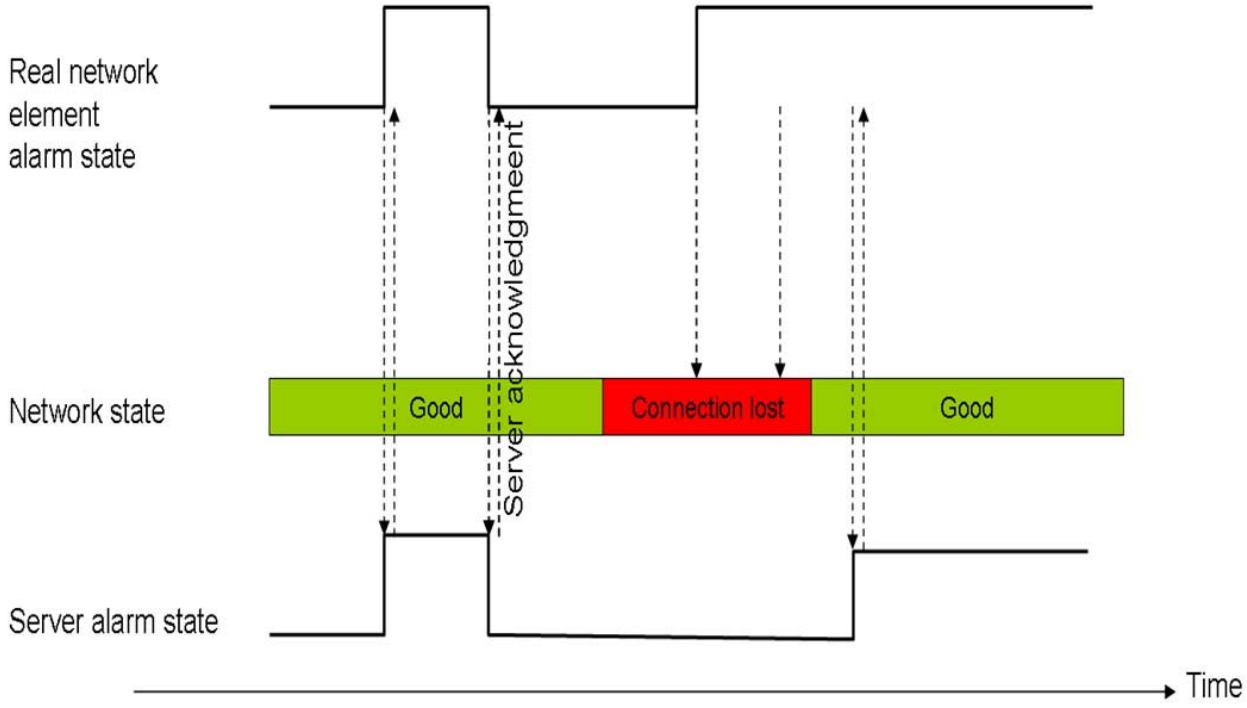


Figure 13: Communication mechanism

When an event happens on a site, a part of the full xml file, with the relevant information, is sent to the NMS, with an HTTP POST over TCP/IP. The DGU shall have configuration elements to define the post address.

10.1.3 The <description_table> element

This element contains multiple <description> elements. It corresponds 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 contained in Table 3.

Table 3

Attribute	Description	Datatype
id	The id of the description, it shall be different for all the description, it corresponds to the key of the table.	xs:integer
name	The name in English of the description element.	xs:string
group	This attribute provides 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 shall 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

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

General Information:

Table 4

Name	Group	Description	Optional/Mandatory
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 localization of the equipment/system.	O

Maintenance Information:

Table 5

Name	Group	Description	Optional/Mandatory
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:

Table 6

Name	Group	Description	Optional/Mandatory
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.	

10.1.4 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.

Table 7

Attribute	Description	Datatype	Optional/Mandatory
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 10.	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

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

Table 8

Child element	Description	Datatype	Optional/Mandatory
<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

10.1.5 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 following attributes.

Table 9

Attribute	Description	Datatype	Optional/Mandatory
id	The id of the event	xs:integer	M
sequence_number	Event sequence number (0 to 65 535) 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 set**: an event of this type is sent each time an alarm is set on the equipment. - **alarm clear**: an event of this type is sent each time an alarm is cleared on the equipment. - **information**: for any information which is not related to an alarm - **cold start**: when the equipment reboots, an event is sent with this type. This allows forcing a full discovery of the equipment by the NMS. This allows to clear alarms which could be set before the restart.	xs:string	M
datetime	The date and time at which the event has happened.	xs:datetime	M
severity_type	This attribute exists if the event concerns an alarm. Then, the severity type value is the one of the corresponding alarm.	xs:string	O/M
severity_level	This attribute exists if the event concerns an alarm. Then, the severity level value is the one of the corresponding alarm.	xs:integer	Optional/mandatory
alarm_id	This attribute exists if the event concerns an alarm. Then, the alarm_id value is id of the alarm in the alarm table of the equipment.	xs:integer	Optional/mandatory
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

10.1.6 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 following attributes.

Table 10

Attribute	Description	Datatype	Optional/Mandatory
id	The id of the data, shall be different for all the data, it corresponds at the key of the table.	xs:integer	M
name	The English name of the data (standardized).	xs:string	M
group	This attribute provides 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 shall 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
measurement_standard	Standard defining the measurement method.	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

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

10.1.7 The <data_record_table> element

This child contains multiple <data_record> elements. The <data_record> element has the same attributes as the <data> element.

The <data_record> is composed of multiple elements:

All the inner text of the following elements are either data values or datetime, in a CSV format, separated by the semicolon character ';'. For data values, the decimal separator is a point '.'.

Table 11: Child element definition for data_record element

Child Element	Description	Datatype	Optional/Mandatory
<last_seconds_datetime>	The format of the CSV datetimes is: YYYY-MM-DDThh:mm:ss	xs:string	O
<last_seconds>	Average values of the data, during one second, in CSV format	xs:string	O
<last_seconds_min>	Minimum values of the data, during one second, in CSV format	xs:string	O
<last_seconds_max>	Maximum values of the data, during one second, in CSV format	xs:string	O
<last_minutes_datetime>	The format of the CSV datetimes is: YYYY-MM-DDThh:mm	xs:string	O
<last_minutes>	Average values of the data, during one minute, in CSV format	xs:string	O
<last_minutes_min>	Minimum values of the data, during one minute, in CSV format	xs:string	O
<last_minutes_max>	Maximum values of the data, during one second, in CSV format	xs:string	O
<last_hours_datetime>	The format of the CSV datetimes is: YYYY-MM-DDThh:00	xs:string	O
<last_hours>	Average values of the data, during one hour, in CSV format	xs:string	O
<last_hours_min>	Minimum values of the data, during one hour, in CSV format	xs:string	O
<last_hours_max>	Maximum values of the data, during one hour, in CSV format	xs:string	O
<last_days_datetime>	The format of the CSV datetimes is: YYYY-MM-DD	xs:string	O
<last_days>	Average values of the data, during one day, in CSV format	xs:string	O
<last_days_min>	Minimum values of the data, during one day, in CSV format	xs:string	O
<last_days_max>	Maximum values of the data, during one day, in CSV format	xs:string	O
<last_month_datetime>	The format of the CSV datetimes is: YYYY-MM	xs:string	O
<last_month>	Average values of the data, during one month, in CSV format	xs:string	O
<last_month_min>	Minimum values of the data, during one month, in CSV format	xs:string	O
<last_month_max>	Maximum values of the data, during one month, in CSV format	xs:string	O
<last_year_datetime>	The format of the CSV datetimes is: YYYY	xs:string	O
<last_year>	Average values of the data, during one year, in CSV format	xs:string	O
<last_year_min>	Minimum values of the data, during one year, in CSV format	xs:string	O
<last_year_max>	Maximum values of the data, during one year, in CSV format	xs:string	O

All the child elements of the <data_record> related to datetime (<last_minutes_datetime>, <last_hours_datetime>, etc.) can have the following attributes.

Attibute	Description	Datatype	Optional/Mandatory
period	Describes the polling period, in the unit of the relative CSV data record. For example, <last_minutes_datetime period=20> means that a measurement is stored every 20 minutes.	xs:integer	O

It is recommended to have a configurable alarm at the relative equipment level in order to inform that the data record storage is almost full. The NMS system has to download the records to avoid any loss of data record historic.

10.1.8 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 piece of 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 following attributes.

Table 12

Attribute	Description	Datatype	Optional/Mandatory
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 provides 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	M
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

10.1.9 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 following attributes.

Table 13

Attribute	Description	Datatype	Optional/Mandatory
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 provides 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

10.2 The <site> element

10.2.0 General

As introduced previously, the root element of the document is <site>. This <site> element can have standard attributes.

The specific child elements of a <site> are as indicated in Table 14.

Table 14

Child element	Description	Datatype	Optional/Mandatory
<energy_system>	Any type of energy system	xs:complexType	M
<sensors_actuators>	Any type of sensors and actuators equipment	xs:complexType	O

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

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

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

Here follows some list of <description> elements recommended by the present document.

General description:

Table 15

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

The Address of the site:

Table 16

Name	Group	Subgroup	Description	Optional/Mandatory
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:

Table 18

Name	Group	Subgroup	Description	Optional/Mandatory
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

10.3 The <energy_system> element

This element is introduced to monitor energy information of systems and equipment. 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 ETSI ES 202 336-2 [i.12] and following parts of this multi-part deliverable. The specific elements are indicated in Table 18.

Table 18

Child element	Description	Datatype	Optional/Mandatory
<sensors_and_actuators>	Sensors And Actuators (the present document)	xs:complexType	O
<dc_system>	DC System (ETSI ES 202 336-2 [i.12])	xs:complexType	O
<ac_ups_system>	AC UPS (ETSI ES 202 336-3 [i.13])	xs:complexType	O
<ac_distribution_switchboard>	AC distribution switchboard (ETSI ES 202 336-4 [i.14])	xs:complexType	O
<diesel_backup_generator_system>	Back-up diesel generator (ETSI ES 202 336-5 [i.15]).	xs:complexType	O
<air_conditioning_system>	Air conditioning System (ETSI ES 202 336-6 [i.16]).	xs:complexType	O
<other_utilities_system>	Other Utilities System (ETSI ES 202 336-7 [i.17]).	xs:complexType	O
<remote_power_feeding_system>	Remote Power Feeding System (ETSI ES 202 336-8 [i.18]).	xs:complexType	O
<alternative_power_system>	Alternative Power System (ETSI ES 202 336-9 [i.19]).	xs:complexType	O
<inverter_system>	Inverter System (ETSI ES 202 336-10 [i.20]).	xs:complexType	O
< intelligent battery >	Energy System (ETSI ES 202 336-11 [i.21]).	xs:complexType	O
<ict_equipment>	ICT equipment (ETSI ES 202 336-12 [i.22]).	xs:complexType	O

Annex A (informative): Communication between LMA/RMA and infrastructure equipment monitoring & control agent using YANG/NETCONF and REST

A.0 Introduction

Main reason for REST/JSON and YANG/NETCONF approach is to be compatible with the O-RAN alliance and 3GPP interfaces. The idea is that an CU or DGU should be easy to manage within an O-RAN and that equipment designed for O-RAN should easily map into an environment following the present docuemnt.

Yet Another Next Generation, YANG, is a data modelling language for the definition of data sent over network management protocols such as the NETCONF and RESTCONF. The data modelling language can be used to model both configuration data as well as state data of network elements. YANG can be used to define the format of event notifications emitted by network elements. YANG, being protocol independent, can be converted into any encoding format, e.g. JSON, that the network configuration protocol supports.

REST is a REpresentational State Transfer used to convey the data described by JSON [9]/YANG [10]/XML documents. REST is an http Remote Procedure Call (RPC) protocol based on HTTP2, defined in IETF RFC 7540 [6]. REST is described in article in bibliography.

HTTPS is used for security reason in LMA, RMA. HTTPS should be used in CU, 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.

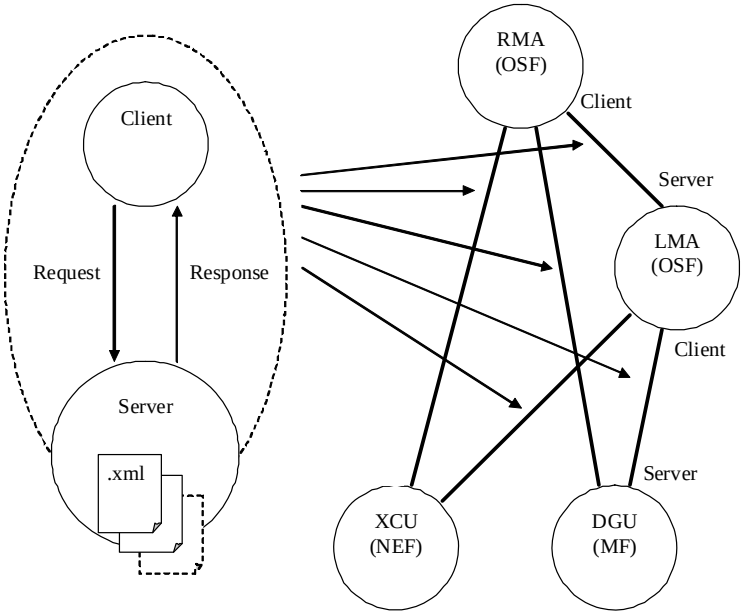


Figure A.1: Interaction between unit in the IEM&C network

A.1 Communication initiated by the LMA/RMA

A.1.0 Introduction

Each DGU/CU that can act as a server, holding one or more JSON 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 " and "http://127.0.0.1/site".

The first part of the URI is always the IP address of the site or the IP of the sub-equipment. If hostname is 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 should, with exception only for specific behaviours stated within the present document, respond in accordance with IETF RFC 7540 [6] 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 retrieved 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.

Table A.1

Parameter name	Value	Description
notable	true/false	Ask the generation of the XML file without any tables. This allows to retrieve only the site structure without any detail, but with the state of all the equipment.
description_table (or description)	true/false	Define if the description table is included in the generated xml document (at each level of hierarchy).
alarm_table (or alarm)	true/false	Define if the alarm table is included in the generated xml document (at each level of hierarchy).
event_table (or event)	true/false	Define if the event table is included in the generated xml document (at each level of hierarchy).
data_table (or data)	true/false	Define if the data table is included in the generated xml document (at each level of hierarchy).
data_record_table (or data_record)	true/false	Define if the data record table is included in the generated xml document (at each level of hierarchy).
config_table (or config)	true/false	Define if the config table is included in the generated xml document (at each level of hierarchy).
control (or control)	true/false	Define if the control table is included in the generated xml document (at each level of hierarchy).

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: 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

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.

In order to lower the bandwidth usage, the XML file may also be available in ZIP compressed format. The URI is the same except that ".zip" is added after the ".xml"? Here follows an example of URI:

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

This method can be very useful for retrieving large data record tables. The bandwidth required can be divided by up to 10.

Other compression algorithms can be used, if documented.

HTTP GET of any description, data, configuration, etc.

It should be possible to retrieve easily element values through a simple HTTP get request. This can be considered as an equivalent of an SNMP get, but over HTTP. The path is like an XML XPath but simplified to be compliant with URI format. The following examples illustrate some requests.

Get the data with the id 21 at the site level

```
http://the_ip/get.txt?path=/site/data_table/21
```

Get the data with id 11, of the dc system 1, in energy system 1

```
http://130.145.57.71/get.txt?path=/site/energy_system/1/dc_system/data_table/11
```

Get severity type of the alarm 1 of the dc system:

```
http://130.145.57.71/get.txt?path=/site/energy_system/dc_system/alarm_table/1/severity_type
```

Note that when no equipment id is specified, the first equipment, with this name, at this level, is selected.

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 should 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 should be provided by the manufacturer. The syntax should be clearly defined. The response should also be described.

The DGU should support the followings command on the following URI:

- SetValue.cgi or SetValue

The URI is: http://the_site_ip/SetValue.cgi or http://the_site_ip/SetValue

The arguments to pass in the HTTP POST body are:

- path: this is the path to the parameter to change
- value: this is the new value

Here is an example of post body content:

```
path = /site/1/energy_system/1/dc_system/1/config_table/12
value = 54.50
```

- ProcessXML or ProcessXML.cgi

The URI is: http://the_site_ip/ProcessXML.cgi or http://the_site_ip/ProcessXML

This function can be used to configure multiple parameters in one command. It is possible to send a full XML structure (like the configuration.xml) in the post data. All the valid elements will be updated with the new value.

This allows multiple configuration parameters to be changed remotely by posting on each IP where a DGU is running.

The content of the body is the complete XML structure.

A.2 Communication initiated by DGU/CU

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

The post method should be used, allowing the DGU/CU 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 CU/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 infrastructure equipment monitoring & control

B.0 Introduction

This annex gives recommendations to obtain reliable INFRASTRUCTURE EQUIPMENT MONITORING & CONTROL 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 makes recommendations 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 CU, 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 CU 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 CU 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) are not allowed.

B.4 CU, DGU reliability

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

CU, DGU have minimum hardware secured functions as follows:

- Watchdog + activity LED: microprocessor automation in equipment CU, 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: ETSI EN 300 132-1 [i.23], ETSI EN 300 132-2 [i.24] or ETSI EN 300 132-3 [i.25].
- 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 secured functions as follows:

- Permanent power supply interface: ETSI EN 300 132-1 [i.23], ETSI EN 300 132-2 [i.24] or ETSI EN 300 132-3 [i.25].
- CU data storage mirroring.
- Hardware selfcheck and failure indication to RMA.
- Loss of coherence/data integrity detection and indication to RMA.
- Self recovery 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: ETSI EN 300 132-1 [i.23], ETSI EN 300 132-2 [i.24] or ETSI EN 300 132-3 [i.25].
- Centralized server RMA unavailability is 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 have secured functions 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 SPICE 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 are 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 CU, DGU, LMA and RMA).
- There should be a system log book of auto or manual application and data change and recovery.

Network access control: on CU, DGU, LMA and RMA, password level are:

- 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 CU and LMA.

Annex C (informative): Network element functions and software architecture and choices

C.1 General description

The functions of LMA should be:

- concentrator of different equipment CU 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 CU, DGU- time setting (clock synchronization);
- auto CU, DGU configuration saving and recovery (i.e. there is a trace of changes);
- auto acquisition and saving of CU, DGU events logbooks;
- auto acquisition and saving of CU, 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;
  - online hypertext help;
  - command sending to equipment.
- 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 is possible to load (download) applications or protocols in DGU or LMA.

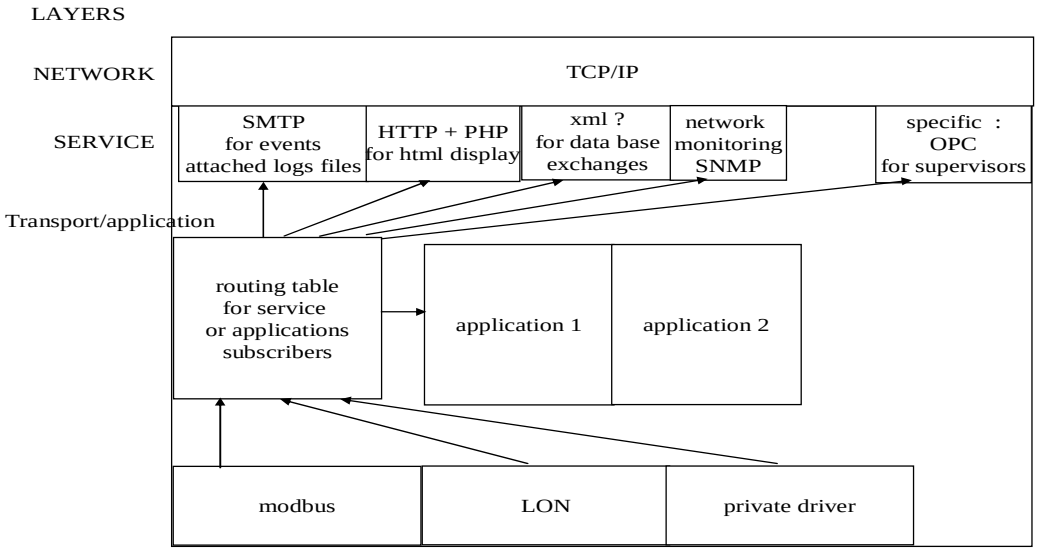


Figure C.1: Services and protocols organization in LMA

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 deratings 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 use different standard environments.

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

PHP is used to generate dynamic html pages.

Java is not used because too dependent of browser release.

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

This is 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: CU, DGU, LMA and RMA.

There should be specific architecture specifications 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 are available to operator to build the MIB and the graphical synopsis. It is 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 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 is 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

D.0 Introduction

This annex gives some recommendations about infrastructure equipment monitoring & control management service performances.

D.1 Management and Network Capacity

The main capacity recommendations are the following:

- the site supervision server LMA can monitor at least 32 control units CU;
- the remote server RMA in monitoring room can monitor at least 500 sites per supervision server unit, i.e. an average of 5 000 CU per RMA server with an average of 10 CU/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 is 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 is possible on a minimum of 5 display terminals at the same time on different sites (i.e. on equipment CU, on site LAN, on LMA, on RMA, on mobile terminal).

D.2 Memory capacity

The main performance recommendations are the following:

- events log file minimum size: 100 in CU, 5 000 per CU in DGU or LMA or RMA;
- measurements records: 10 variables per CU.

D.3 Timing performance

- Alarms: between emission by CU and display on remote supervision, alarms are transmitted and refreshed in less than 5 s. This is 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 < 5 s (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 is 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 minutes.

- Considering access concurrency, the closer connection to equipment with writing right gives the higher priority. Other connexion becomes observers (read only). Priority is: CU > LMA > LAN > mobile post > RMA Priority is loosed after an inactivity timeout (typically 5 minutes).

Annex E (informative): Overview of the XML format

E.0 Introduction

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 Mark-up 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 are discerned from the well known HyperText Transfer Mark up 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 present document.

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

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

Any XML document contains a single tag to define a root element. All other elements are within this root element. All elements can have child elements. These child elements are correctly nested within their parent element. The text/data in the XML element is called the "inner text". All these element is 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, for 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 is 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, the structure could be 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 only contains the data, and the descriptions of how the data is coded and of the meaning of the data are 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 equipment 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/ [i.34].

The most common are briefly described in 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.	-2 335 353,243353 1,23 210 +3 450,234
xs:integer	Represents an integer value. It is derived from xs:decimal by fixing the value of the fraction digits to 0.	3 425 -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 https://www.w3.org/TR/xmlschema-2/#dateTime. NOTE 2: See https://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

F.0 Introduction

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, 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 [7].

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 IETF RFC 871 [i.5].)

Only a subset of the whole OSI model is used today. It is widely believed that much of OSI 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 behaviour 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 OSI 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/IEC 8327 [i.11]/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	1 Physical Network access LLC+MAC	IEEE 802.3 Ethernet, HDLC, Frame relay, ISDN, ATM, IEEE 802.11 Wi-Fi™, PPP
1	Physical		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) was 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.

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 includes 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.
- 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.

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. Examples of such protocols is Recommendation ITU-T X.25 [i.26].

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 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, fibre 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 [8] 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 standards [8] 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 [8] splits the OSI Data Link Layer into two sub-layers named Logical Link Control (LLC) and Media Access Control (MAC).

Every network element on Ethernet, has a **Media Access Control** address (MAC). 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 (IETF RFC 2516 [i.3]), 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 1 500 byte packet, the largest allowed by Ethernet (and hence most of the Internet), would block up a 14,4k modem for about one second.

IETF RFC 1191 [i.4] 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 1 500 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 IETF RFC 1661 [i.10]. PPP is encapsulated in a framing similar to HDLC, described by IETF RFC 1662 [i.6].

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).

IETF RFC 1994 [i.7] 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 IETF RFC 2364 [i.8].

PoS Packet over SONET/SDH (IETF RFC 2615 [i.9]).

Annex G (informative): Common API

Nowadays, communications from BS PEE and site data PEE use different communication protocols and channels. The standardization of a common API for all the scenarios described above is expected to control and monitor PEE data from site equipment, cooling, power, building control units and BSs.

This API should serve in all interactions between:

- NMS(s) and Entry Point(s);
- Entry Point and CU(s)/DGU(s).

Through this API,

- NMS:
  - May request to collect PEE data from site equipment, power units, building control units and BSs.
  - May assign values to configurable parameters related to site, site equipment, power units, building control units and BSs.
  - May configure threshold values related to PEE data so as to receive alarms when these threshold values are crossed by site equipment, power units, building control units and BSs.
  - May subscribe to receiving notifications such as alarms, event notifications (e.g. configuration changes related to site, site equipment, power units, building control units and BSs, CU(s), DGU(s)), etc.
- CU, DGU, Entry Point:
  - May send PEE data from site equipment, power units, building control units and BSs to NMS(s).
  - May issue alarms if configured threshold has been crossed to NMS(s) which subscribed to such alarms.
  - May issue event notifications to NMS(s) which are subscribed to such event notifications.
- Common Protocol.

It is expected that the API be supported by state of the art communication protocols. A secured RESTful HyperText Transfer Protocol (HTTP)-based communication is recommended, with payload in JSON [9]/YANG [10].

Integration of PEE data into BS OA&M channel

As described in clause 4.4 in some scenarios, it is expected that BSs are capable to embed the Entry Point in order that PEE data from site equipment, power unit(s), building control unit(s) are carried from the Entry Point to NMS(s) over the NMS channel of BS(s).

As site equipment, power unit(s) and building control unit(s) are external to BSs, this PEE data should be transported through the BSs NMS channel as 'encrypted' data, i.e. it is not considered by BSs as their proper OA&M data. Instead, this PEE data is meaningful only for CU, DGU, Entry Point and NMS side.

It would be desirable that vendors of site equipment, power unit(s) and building control unit(s) CU/DGU provide MNO/Master Operator (depending on scenario - see clause 4.4) with a 'PEE data Description File', i.e. file providing the data model supported by their CU/DGU. The overall procedure could be as follows:

1) Vendor of site equipment, power unit(s) and building control unit(s) CU/DGU provide MNO/Tower Company/Master Operator (depending on scenario - see clause 4.4) with a 'PEE data Description File', i.e. file providing the data model supported by their CU/DGU.
2) MNO/Tower Company/Master Operator 'integrate' the PEE data Description File into its NMS(s). So, it is capable to control and monitor this equipment.

3) Related site equipment and/or power unit(s) and/or building control unit(s) together with their CU(s)/DGU(s) are installed on site. Some sort of plug-and-connect procedure is automatically triggered at the NMS(s) so that all new equipment and/or power unit(s) and/or building control unit(s) and their CU(s)/DGU(s) are recognized by NMS(s).

4) NMS(s) can now request PEE data to be collected on this equipment and/or power unit(s) and/or building control unit(s).

5) When CU(s)/DGU(s) send their PEE data and/or alarms and/or event notifications to NMS(s), NMS(s) can check against PEE data Description Files if the received data is compliant to the data schema provided by the vendors. If received data is not compliant, it should be discarded. If received data is compliant, it should be appropriately treated by the NMS(s).

Annex H (informative): State of the art of power, energy measurement and monitoring systems

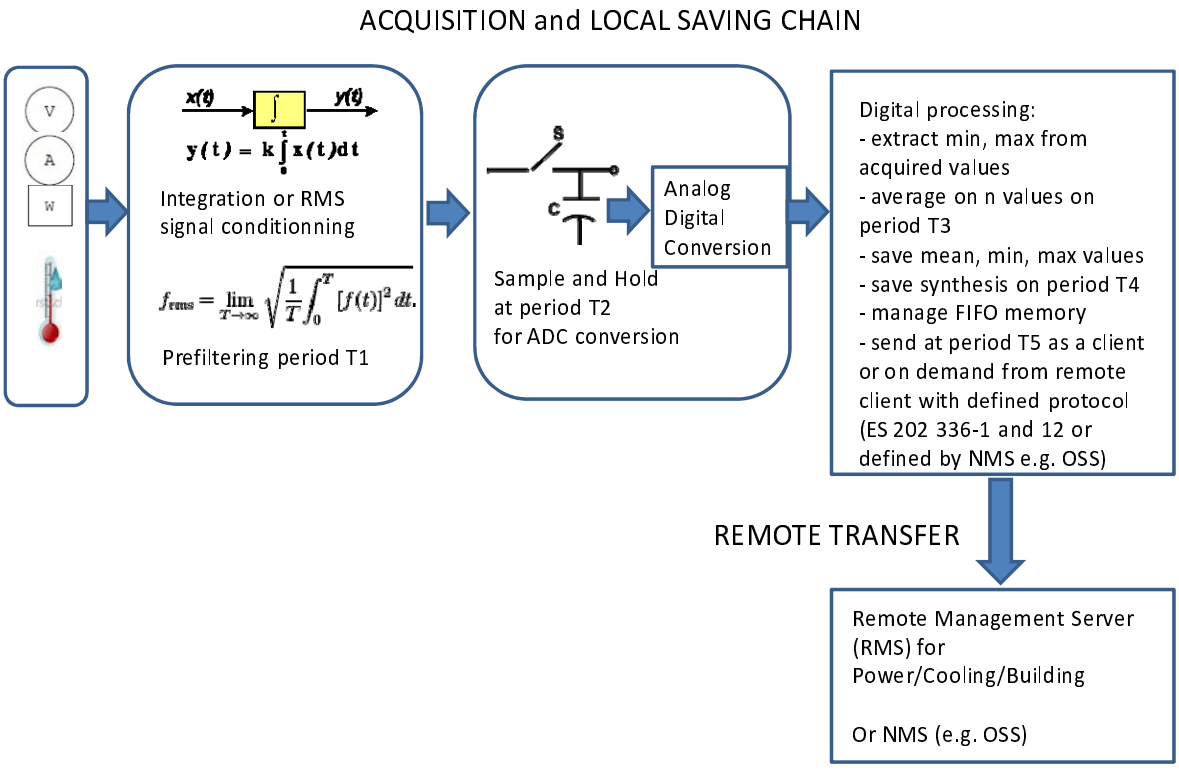
H.0 Introduction

The goal of Annex H is mainly informing on state of the art of mass production electrical power/energy metering chain giving a fair accuracy.

It is based on industrial know-how and documentation of already available monitoring systems and components used in electrical voltage, current and power/energy parameters measurements.

There may be other solutions not described here.

H.1 Acquisition and remote metering principles



NOTE: The ideal RMS calculation is a mathematical limit at infinite time, but a very precise RMS value may be practically obtained on an integration period much lower than 1 second when the acquisition frequency is of some kHz as achieved by many common integrated chips.

Figure H.1: Principle of measured data acquisition, local processing, robust saving and transmission to remote servers

Measurement and signal conditioning (period or time constant T1)

In Figure H.1 sensors referred with symbols V, A, W and a thermometer are giving electrical measurements signal x(t) and in general there is a prefilter or signal conditioner on the rough analog measurement. For environmental parameters, it could be a simple averaging circuit by a low bandpass or integration filter over the period T1.

For more precision on electrical currents signals with a lot of harmonics due to fast and strong dynamic variations, a RMS value is a Root Mean Square calculation. For example RMS is root of a summation of squared rough measurement acquired at 1 ms period. The analog prefilter would then be of about 1 ms time constant. The integration period can be T1 as well using 1 ms sampled values from analog prefilter output. In [i.17] the described circuit can measure up to 100 kHz sinus signal. The true RMS calculation is done by analog circuitry and the prefiltering period could be even much smaller than 1 ms.

- T_{rms}, T1:
  - T1 = 1 s and T_{rms} <= 1 s for electrical analog averaging time constant or RMS integration period.
  - T1 can be the same as T2 for environmental parameters temperature or hygrometry, as their variation is very slow compared to electrical parameters.

Local Acquisition

The value is saved at period T3 used for first signal processing, and is in general acquired at minimum at period T2 equal to some period of the measurement prefiltering:

- T2:
  - T2 = 1 s between analogic/digital conversion of electrical parameters.
  - It can be T2 = 5 s for slow variation environmental parameters.
  - Minimum and maximum values should be captured for site engineering optimization at that level.
- T3:
  - T3 = 5 s to 1 minute and T3 can be set as a parameter for averaging the RMS values and store them locally in a FIFO memory. The minimum and maximum values over this period.
  - T3 = 1 minute is sufficient as default value in many case of small power variations.
  - T3 = 5 s is recommended only if there are fast and strong changes of values which would be more common with fast dynamic power and settings managements. This could allow a special focus on one site and in case of special event, and when the event is finished the period could be extended to reduce data storage memory.
- T4:
  - It can be decided to keep synthesis of data every minute for example, ready to be gathered in a data record frame that will be sent at period T5. More can be found on this possibility this clause on progressive data aggregation.

Data transmission period and data record details

The data transmission period T5 is the period of the record of collected set of values at period T3. The record of data consists in voltage, current, temperature/humidity, power, energy, min/max over the record period. All data record should be associated to a time stamp (date/hour at 1 s accuracy) and to an identifier including equipment reference and site reference in order to allow further analysis of data integrity and correlation to telecom state and activities.

- T5:
  - Default value is 15 minutes. T5 parameter can be set from remote site from 5 to 60 minutes. There could be different levels of aggregation T5 for each measured value to prepare data for transmission to remote server in order to limit amount of data stored in remote servers.
  - For example every T5 = 15 minutes, are sent all sets of values of U, I, P (referred as V, A, W on Figure 1), synthesis of every min (T4 = 1 minute) while just one data set of Energy and Temperature average are sent every 15 minutes. The minimum and maximum of the measured values over the 15 minutes and time stamp can be given at beginning and end of the global data record corresponding to a file. Exceptionally this transmission may contain a specific data record used for monitoring fast changes of electrical parameters as defined in T3 local acquisition description.

Long Data Record local saving period

The data to be transmitted, should be stored in case of network failure or delay for a retransmission, after reparation of the network. In general the period is of some days with a minimum of 4 days.

Progressive data aggregation for long term data retention

There can be an aggregation of the saved value at period T4 equal to some T3 period in order to have a long data retention of the synthesis of values (several months), in case of very long period between data retrieval.

The aggregation can be progressive, i.e. save 4 days all detailed values (U, min, max, I, min, max, P, min, max, W, T), same 6 months hourly average data (U, I, P, min, max, W, T, min, max), save 2 years daily average data (U, P, W, T).

- T4 = 60 minutes by default and T4 can be set as a parameter from 1 minutes to 24 hours.

NOTE: For difficult access sites, the record period of data synthesis can be greater of 1 month to avoid loss of value, when the repair time of the network is very long. For example it can be useful to have memory of several months, with synthesis every hours on a remote BS on standalone energy and difficult access to the site.

H.2 General description of measurement

H.2.1 General principle

The following clause gives an indication of state of the art medium accuracy measurement solutions of Voltage, Current, Power and Energy reachable. In general, the measurement subsets consist in sensor, followed by signal conditioner, A/D conversion and calculation in a digital circuitry (logic array or specialized or general purpose programmable controller). These subsets are more or less integrated in the same chip.

Last clause gives an assessment of local and remote data storage volume.

On new electronic device, power and energy metering are obtained from voltage and current multiplication and then integration or summation on time.

Some circuit can do directly the RMS power calculation as in multimeter for voltage or current and as in power meter e.g. in pass through plugs with display for a very low cost and accuracy of ±1 % on a wide range from some Watt to some kW.

In this later case, the true RMS value is obtained by integrating or summing the instant power (product of instant voltage by instant current) over a defined time. For example voltage and current are acquired at ms, while averaging is done on 1 second. For AC measurement the meter is also able to give the phase shift between U and I in term or cosines value, or even the power factor integrating many harmonics of AC 50 Hz till rank 7 or 9 times the fundamental period.

H.2.2 Measurement sensors

Voltage measurement

There is no sensor. The only error comes from bad connexion of measurement points, parasitic voltage in case of very low voltage due to electrochemical potential between 2 metals or asymmetrical metal connexion, creating a thermoelectric See beck voltage.

This is not a problem for measurement of power with ten's of Volt at interface A.

An accuracy of ±1 % is easy to obtain as will be explained in the section about AC or DC signal conditioning of clause H.1.

Current Hall sensors effect

The Hall sensor uses the Hall effect which is a creation of voltage in a semi-conductor material when crossed by a current in a magnetic field.

There are 2 types of Hall effect sensors:

- open loop: giving the absolute value, in general low cost but not accurate and stable with time and temperature. The variation of field will affect the offset of the measure (small residual value observed at Zero current due to magnetization of the sensor);
- closed loop: a current in a coil is compensating the measured field to read 0 volt on the Hall effect sensor. They are in general more accurate as they work in a linear zone and with no persistent field so no magnetical hysteresis issue. It is reducing the offset value derating. There can be some improved demagnetization solution.

Even on laboratory measurement device reaching ±2 % accuracy is difficult, and especially impossible for long period without frequent calibration.

It is even more difficult for open clips, because of the leakage of the magnetic circuit where it opens so that it is more disturbed by external magnetic fields. This is currently observed on best of class laboratory clip.

To sum-up many sources of errors are affecting the accuracy at long run of Hall effect sensors:

- Persistent magnetic field.
- Proximity field and magnetic disturbance created by other conductors.
- Centering of the wire in the clip.
- Sensitivity to temperature and power supply voltage fluctuation of the device itself as it affects the offset.

Shunt measurement

The shunt is a very stable resistance with time. In general it has a very low temperature coefficient thanks to the use of some special metallic alloy. The basic measurement principle is based on Ohm law:

$$U = R.I$$

with:

- U: the voltage drops at resistance terminals;
- R: the value of the resistance;
- I: the current passing through the resistance.

As R is chosen to be constant, independently of temperature, the read voltage corresponds precisely to the current and it is very linear with no offset at 0 A, corresponds 0 V with only some noise. In general, resistance of Shunt type is used and currently gives ten's of mV at the maximum current to be read in order to avoid losses and temperature rise of the metal from which it is built.

A very common accuracy is ±1 %. It is possible to have a ±0,25 % with 4 points (2 for power terminals, 2 for reading terminals).

For example, a 50 mV 100 A shunt, dissipates 5 W. 10 mV is better for this with only 1 W, but there is a trade off to find as the difficulty will be on the amplifier precision and noise to be able to increase the voltage for a proper A/D conversion.

Measurement of the current I on a shunt is sensible to parasitic voltages. So it is recommended to (see also AC or DC signal conditioning section in this clause):

- Use symmetrical power supply on OA to have specified offset when voltage close to zero.
- Avoid noise on power supply by proper PSU design and close filtering on OA and A/D circuitry.
- Avoid capacitor with some residual potential in filtering circuits.
- Avoid asymmetrical battery effect on contact (use unoxidized contact metals and waterproof contacts).
- Avoid symmetrical See beck thermo-electric effect contacts.

- Use the shortest as possible measurement cables with same length with no loop to avoid induction. Shielded cables are used in high class solution.

AC transformer sensor or Rogowski coil sensor

The well known current transformer or Rogowski coil sensor are measuring the fields though a magnetic flow variation with time in a precisely designed secondary coil. The measurement based on these sensors are precise and stable with time. Hysteresis is not a problem with non persistent magnetic field finely devised magnetic core with very small Eddy current losses at 50 Hz and very small hysteresis.

A ±1 % accuracy is very common with high linearity and there is no offset at condition of PF close to 1.

This sensor can read distorted current but may have problems with non sinusoidal current and bad power factor that may create saturation of the core and consequently measurement errors.

Other current sensors

It exists some other effect that can be used to read current with stable accuracy. The effect discovered by Louis Néel of giant non linear superparamagnetism begins to be used with good result. But in general sensors based on this effect are very expensive, and so not adapted to the application presented in the present document.

AC or DC signal conditioning

The proposed solutions of sensors signal conditioning are worth for DC or AC.

Method 1

This method is based on operational amplifier (OA) and microcontroller (µC) with A/D channels.

The OA are defined as follows:

- high precision (OA) with very low offset and bias current are used;
- they are arranged in differential mode to accept common mode voltage drop;
- for voltage measurement a simple voltage attenuator can be used e.g. divide by 25. 50 V will give 2 V;
- for current, amplification is required, e.g. a gain of 50 will give 2,5 V for 50 mV voltage on the shunt which is a common value to have low power loss in the shunt. At 20 A - 50 mV, the loss is 1 W for 1 kW load in 48V;
- a 0,25 % precision shunt for less than 100 A could have low cost. A 0,5 % could be very low cost.

Then the acquisition is done by the µC on A/D channel with precision corresponding to 1 bit over 10 to 12 bit, which means a resolution of less than 1/1 000 of full scale e.g. 5 V. 10 bit resolution corresponds to 5 mV. With gain 50, the input will be 100 µV on the 50 mV shunt corresponding to 0,2 %.

To obtain the required accuracy between 1 and 2 %, the following choices are recommended:

- Use 0,1 % accuracy resistance for voltage measurement gain or attenuation, these high precision resistances having very low ageing and temperature derating.
- Use lower than 50 µV offset OA with no derating for 0,1 % accuracy at full scale of the shunt.
- Chose OA of chopper type for regular offset compensation by periodical measure of artificial zero at input. Non chopper OA exists and is much less noisy which is better for very low voltage measurement on shunt.
- The major manufacturers of precision OA have these components with detailed datasheet and application notes to obtain the best of these components.

The A/D should use a voltage reference of 1 % error maximum that can be internal or external. When external, it can be the power supply of the µC, or a specific voltage reference. 1 % accuracy is reachable on the reference.

The µC can acquire every ms the U and I values, calculate the U.I product and sum-up them over 50 to 100 ms. An average value of P RMS can be obtained every 1 s. In addition Pmin and Pmax can be logged.

The precision of time can be of 1 % with the internal RC timer of the µC, but can reach some ten's of ppm, on an external Quartz then the µC can aggregate over 1 to 60 minutes as required.

All parameters are easy to set.

All values can be logged in EEPROM not to be lost in case of power supply interruption.

Additional calibration tuning can be done to allow higher accuracy when required.

Method 2

Another alternative is to use a low cost specialized integrated circuit for AC power measurement. The circuit has build-in analog amplifier and 24 bit A/D converter and 25 ppm voltage reference of high precision and an arithmetic and logic unit able to calculate instant power and RMS values. The circuit has a serial bus of serial type for communication or record on serial EEPROM or to a host processor.

It requires only some passives components (resistors and capacitors) to operate and consumes less than 20 mW under 3 to 5 V. A voltage divider is used for voltage input, and a differential amplifier for current input from shunt or current transformer or Rogowski coil.

For example the circuit of Figure H.2 is showing the typical precision of the AC power measurement with different PF on a dynamic of 1 to 4 500 for a single phase AC energy meter and Figure I.3 was result of one measurements of linearity done in Laboratory on an energy meter integrated circuit.

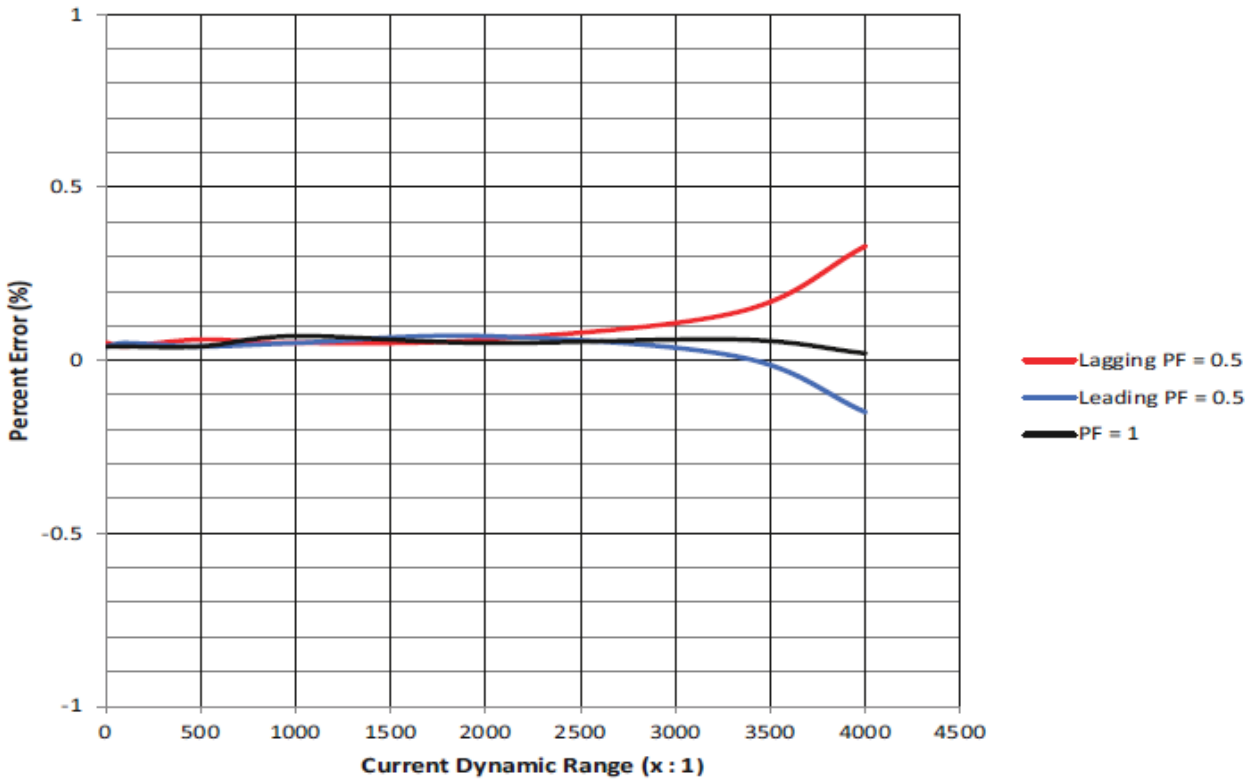


Figure H.2: Example of electric AC energy metering accuracy

Measurements have also been done on DC with an older version of the component and have resulted in the following linear graph (Figure H.3). The linearity is quite good on a wide area of load. ±1 % RMS power precision is achievable on a wide range of measurements and there is about no offset.

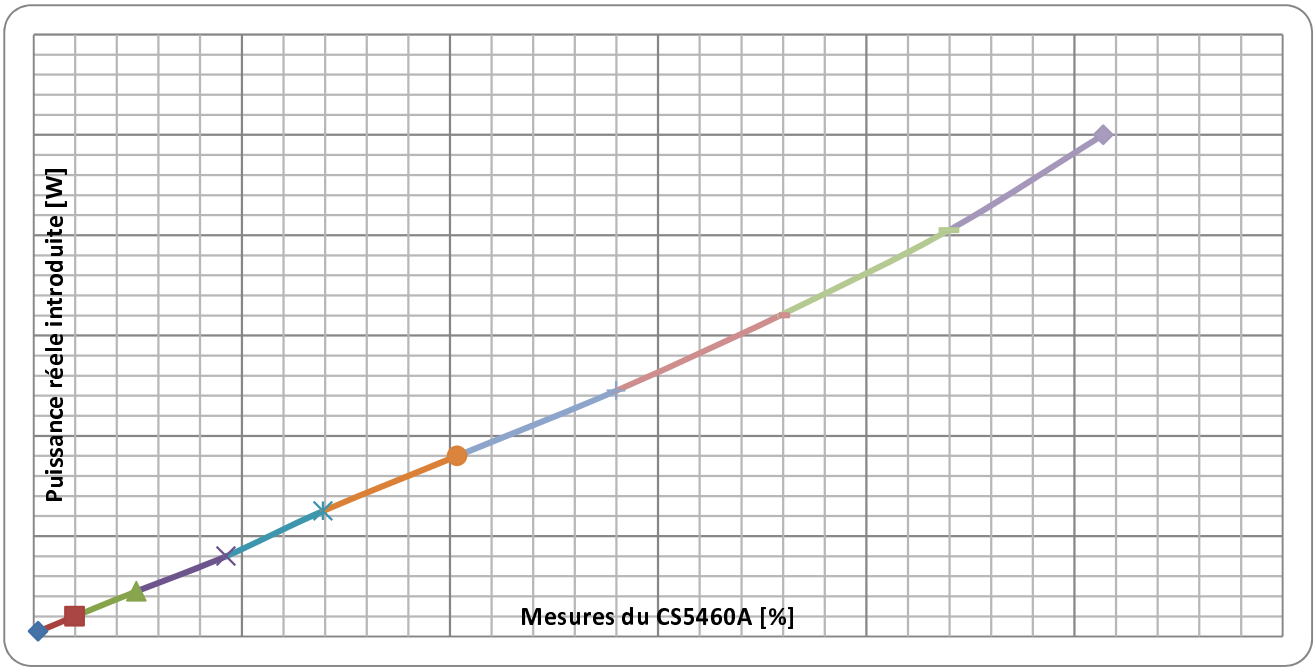


Figure H.3: Circuit linearity test done on a older generation of energy meter component

Annex I (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. Are 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)
- http://www.peej.co.uk/articles/rest.html

Annex (informative): Change history

Date	Version	Information about changes
November 2024	1.3.1	Added parameter definition and parameter accuracy. Delete references to XMLand give possibility to use different communication protocol

History

Document history		
V1.1.1	September 2004	Publication as ETSI TR 102 336
V1.1.1	November 2007	Publication
V1.1.2	September 2008	Publication
V1.2.1	July 2011	Publication
V1.3.0	February 2025	Membership Approval Procedure MV 20250408: 2025-02-07 to 2025-04-08