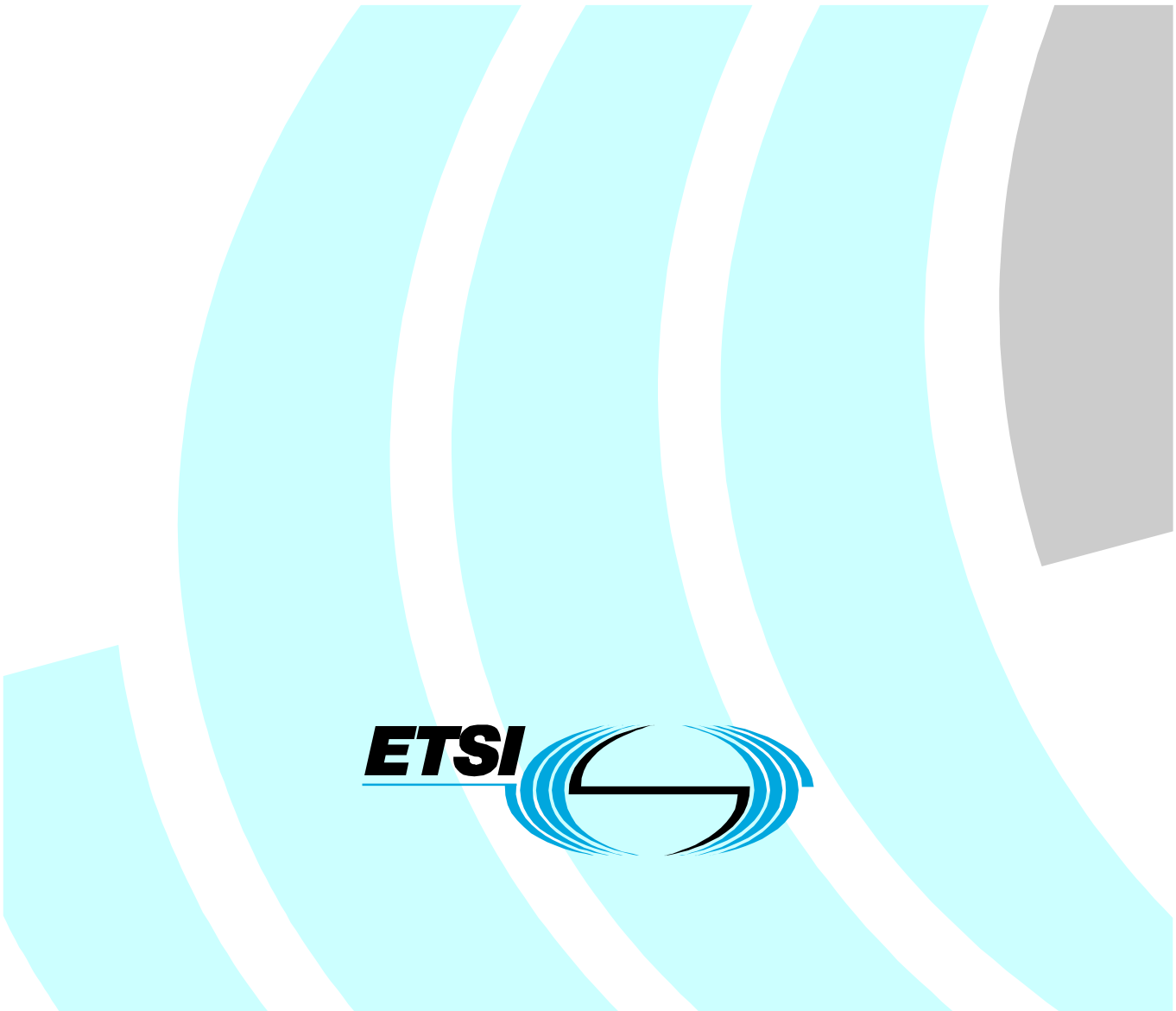
ETSI TR 102 336 V1.1.1 (2004-09)

Technical Report

Environmental Engineering (EE); Power and cooling system control and monitoring guidance



Reference
DTR/EE-02035

Keywords
control, interface, management, power, system

ETSI

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

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

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

Contents

Intellectual Property Rights

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

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

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Environmental Engineering (EE).

1 Scope

The present document applies to monitoring of power and cooling systems for telecommunication installations and equipment.

It describes the control, supervision and alarm interface of the equipment and how it may be connected to a local array or a distant network.

The influence of different power supply architectures on the network supervision architecture is taken into account.

Telecommunications Management Network (TMN) will be partially described because power and cooling system management can be part of more global existing management network.

The knowledge of how to create generic interfaces is outlined.

The present document helps to identify the type and minimum set of information required for monitoring and management and the possible network architectures for heterogeneous power and cooling system equipment.

2 References

For the purposes of this Technical Report (TR) the following references apply:

[1] ETSI EN 300 386: "Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; ElectroMagnetic Compatibility (EMC) requirements".

[2] IEC 60950-1: "Information technology equipment - Safety - Part 1: General requirements".

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

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

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

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

[7] Void.

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

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

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

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

[12] IEEE 802.11 (all parts): "IEEE Standard for Telecommunications and Information Exchange Between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (Mac) and Physical Layer (PHY) Specifications".

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

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

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

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

[17] ETSI TR 102 489: "Environmental Engineering (EE); European telecommunications standard for equipment practice; Thermal Management Guidance for equipment and its deployment".

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

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

[20] ITU-T Recommendation V.24: "List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE).

[21] ITU-T Recommendation X.21: "Interface between Data Terminal Equipment and Data Circuit-terminating Equipment for synchronous operation on public data networks".

[22] ITU-T Recommendation X21bis: "Use on public data networks of Data Terminal Equipment (DTE) which is designed for interfacing to synchronous V-Series modems".

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

3 Definitions and abbreviations

3.1 Definitions

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

Terms referring to energy interface, equipment and distribution are described in power distribution guidance and standards ETS 300 132-1 [3], EN 300 132-2 [4], EN 300 132-3 [5] for ac and dc interface and EN 302 099 [6] for access network equipment powering.

alarm: any information signalling an abnormal state, behaviour generally due to a hardware or software failure

NOTE: It may also be an associated message that is specifically formatted.

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

battery Jar: housing of battery-cell or block

battery Block: composition of more than one cell in one housing (jar) in serial arrangement

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

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

client post: any device (laptop, PDA, console, …) connected to servers via the supervision network to perform maintenance or supervision operations

CMISE: generic service to handle objects (operation and notification of results)

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

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

Ethernet: LAN protocol (equivalent to IEEE 802.1 to 11)

event: any information signalling a change of state

NOTE: It can be also a formatted message.

GDMO: syntax specification for the classification of objects and properties (associated to ASN.1 language for object definition)

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: a 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: an 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.

records: this is more generally physical value measurements

RS 232: electrical serial line interface driven by voltage levels (equivalent to ITU-T Recommendation V.24)

RS 422/485: electrical serial line interface driven by current levels

NOTE: RS 422 is single point, RS 485 allows multi-point.

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

NOTE: Set of ISO system management functions according to ISO/IEC 10164 [9].

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

web: common name for the Internet

3.2 Abbreviations

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

ADSL	Asynchronous Digital Subscriber Line
API	Application Program Interface
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
CIM	Common Information Model
CMISE	Common Management Information Service
CUE	Current Using Equipment
DNS	Domain Name Server (associate a single domain name to an IP address)
GDMO	Guidelines for Definition of Managed Objects
GSM	Global Mobile System
HMI	Human-Machine Interface
HTML	Hypertex Transfer Make-up Language
HTTP	Hypertex Transfer Protocol
IP	Internet Protocol (as specified by US DARPA)
ISDN	Integrated Service Digital Network

LAN	Local Array Network
MIB	Management Information Base
MMI	Machine-Machine Interface
MTTR	Mean Time to Repair
ODBC	Open Data Base Connectivity
PDA	Personal Digital Assistant
PLC	Programmable Logic Controller
PSTN	Public Switched Telephone Network
RB	Rectifier Battery
RDBMS	Relational Data Base Management System
RTDB	Real-Time DataBase
SCADA	Supervisory Control And Data Acquisition of industrial processes
SMF	Systems Management Functions
SMS	Short Message System
SNMP	Simple Network Management Protocol
SU	Service Unit
TCP	Transmission Control Protocol
TMN	Telecommunications Management Network
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VB	Visual Basic
WAN	Wide Array Network
WWW	World Wide Web

4 Monitoring information and functions

Several management levels are possible for telecommunication installations and equipment. They may be described considering complexity of the system, response time and required level of details from alarms to analysis level. In many cases, the same basic information is needed from the equipment-monitoring interface. General monitoring and supervision models are described for power distribution, industry and telecommunications:

- For power distribution and industry see IEC/TR 62357 [8], power system control and associated communications (from IEC TC 57) and annex D on SCADA.
- For telecommunications, see ISO/IEC 10164 [9], ITU-T Recommendation M.3010 [10] ITU-T Recommendation M.3100 [11].

Information can be displayed on site:

- locally on the equipment control unit;
- on a centralized server through a LAN;
- on a client display (PC or PDA), through the LAN, from any equipment on the site.

System interrogation can be achieved by:

- locally on the equipment control unit or using a laptop or PDA;
- remote supervision of several centres, in the supervision room, through a private or public network;
- remote supervision of a site, on a client terminal, through a public network (for field maintenance personnel e.g. mobile client post).

Figure 1 gives an overview of all these display and interrogation possibilities.

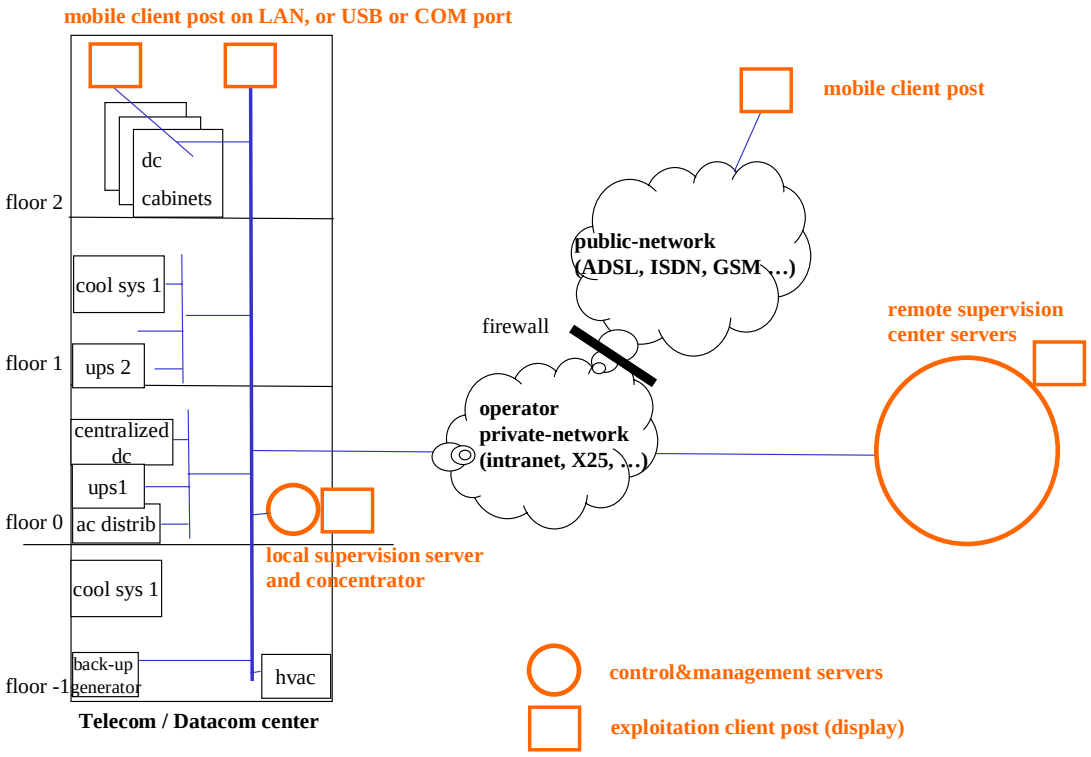


Figure 1: Local and remote equipment interrogation options through networks (LAN, private and public)

4.1 Basic information on power and cooling systems

The following clauses describe the minimum level of information required from power and cooling systems. Generally, as the level of system complexity increases, additional supervisory information is required. If microprocessor automation is used, this should be checked by a watchdog facility.

4.1.1 Power-supply without back-up

Operators generally require to be informed of functional failures. Considering the power-supply interface, it is important to get at least an alarm that informs of the presence or initial loss of power at the input of the powered equipment.

Dying gasp

For very simple CUE (see figure 1a), information about the beginning of power failure can be transmitted to the telecom management system if the equipment is self-monitored. It should have enough time with capacitor hold-up time to send the dying gasp alarm.

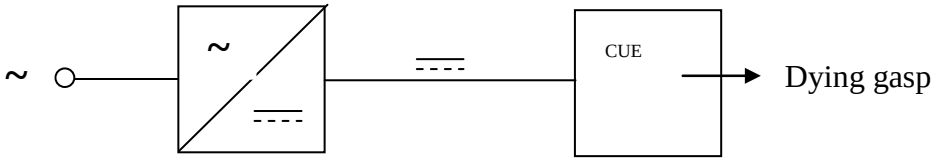


Figure 1a: Supervision of a basic power supply

Partial failure or loss of redundancy alarm

The power supply can be redundant (n+1 rectifiers, n+1 power lines and protections). Redundancy is only efficient if maintenance is done after a partial failure. That means that partial failure must be monitored.

For example in a dc power supply system each rectifier, each input protective device and each output protective device (supplying the CUE) should be monitored. However, for less critical systems, alarms can be gathered together to send only generic signals like partial failure or loss of redundancy. For critical systems, it is recommended that alarms discriminate to improve maintenance analysis. This helps to ensure that:

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

Power estimation

The measurement of current or power (if available) can be used to determine the size (capacity) of mobile power supply needed to support the load during an outage of the public mains supply. A mobile supply could be a diesel generator, temporary rectifiers, etc. It is also useful to measure energy consumption and to use this data to indicate over or under sizing of power supply equipment. This could be achieved by calculating the ratio between installed capacity and measured power consumption. For less critical equipment, the value of measured power may not be transmitted but only displayed locally.

4.1.2 Permanent power supply

The CUE is permanently powered by a rectifier-battery power supply (see figure 2) or an ac UPS.

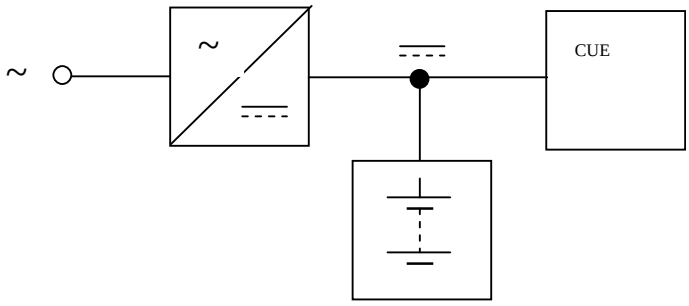


Figure 2: Principle of operation of a dc backed-up power supply

The CUE is connected to two sources of energy connected in parallel; a rectifier and a battery. The rectifier is dimensioned to cover the total power consumption of the CUE and, in addition, supply an appropriate charging current for the battery. This maintains the battery in a fully charged condition. If the mains ac voltage is outside of the specification (e.g. fails, reduction of voltage, high harmonics), the CUE continues to be supplied without interruption.

Battery discharge alarm

In battery discharge operation, there must be alarms when the battery condition (e.g. voltage) has fallen below threshold values.

The alarm can also be obtained from a known time in discharge (e.g. 30 min), if designed or achieved autonomy is known (e.g. 1 hour).

Information on the remaining autonomy will enable intervention to be prioritized. It can be estimated at the supervision centre from alarm and known autonomy or by calculation. One approach is to calculate the remaining capacity at the discharge rate using current measurement and the estimated full capacity of the battery.

Where values of measured current or discharged time are available they should be transmitted, which requires more than simple alarms loop transmission.

General blackout and overcharge

The previously described rectifiers and protection failure signals are useful to determine the reason for battery discharge. If all rectifiers are in a fault condition, there must be a mains supply outage or the general protection is open. In both cases manual intervention may be required.

Another reason for battery discharge can be a temporary overload condition of the power system. Monitoring voltage (e.g. a level below the battery float voltage), battery current or system current can be used to determine such a cause. Overload can be intermittent due to variation of load.

Battery replacement alarms and warnings

The more common question with batteries is to know when replacement is required, e.g. when capacity is below a threshold value. Permanent monitoring and periodic discharge tests can both give warnings or alarms. The conditions and parameters of the tests e.g. battery temperature, discharge current, etc. should be recorded during tests and stored to follow the ageing of batteries with some accuracy.

As ageing is temperature driven through Arrhenius positive grid corrosion and water loss, a record of ambient or jar temperature and a predictive algorithm can be used to estimate the end of battery life. Temperature measurement can also be used in the charging processes of some type of batteries.

Persistent unbalanced voltage of cells or unbalanced current of parallel branches should also lead to warnings.

There should be an alarm if one battery circuit protection is faulty or purposely open or for maintenance reason.

Charging alarms

To reduce risk of thermal runaway and to warn of unhealthy battery conditions, a permanent charging current should lead to an alarm and or a reduction of charging voltage.

Temperature alarms should be generated when:

- A persistent battery temperature significantly higher than ambient (e.g. charge failure with normal ambient condition).
- Battery temperature exceeds a predetermined threshold (e.g. in case of a fan failure).

4.1.3 Permanent power supply with back-up generator

The CUE is continuously connected to a rectifier-battery power supply (see figure 2) or an ac UPS. A long mains supply outage can be backed-up by a generator such as a standby diesel engine (see figure 3). An ac switchgear distribution board assumes the load transfer from mains to backup. The CUE is fed by a dc 48 V rectifier/battery, an ac UPS, or by a higher voltage dc supply (> 48 V and < 400 V). Other equipment loads such as cooling systems or building services may also need to be backed up by the standby supply, e.g. a standby generator.

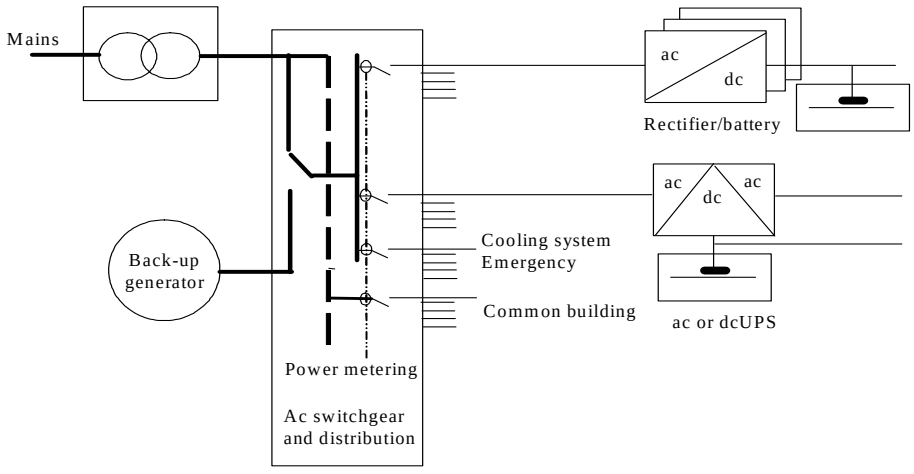


Figure 3: Principle of operation of a dc backed-up power supply

Fluids monitoring

A standby diesel generator requires fluids such as fuel and coolant for correct operation. It is important to be informed of fuel level or equivalent operating autonomy by either a continuous or real-time gauge or discrete levels for smaller engine sets. As a minimum, alarms are required for low fluid levels. A fuel leakage warning and leakage containment tank is also required to limit fire and pollution hazard. Fuel spillage containment can be achieved by providing double walled tanks or purpose built bunding/tanking in which the fuel tank stands.

Operation monitoring

It is of high importance to emit an alarm in cases where an engine fails to start, or stops under abnormal circumstances. This could occur during a routine test or during a mains supply outage as generally the starter battery autonomy is short. Detailed reasons are not necessarily useful but can be interesting for diagnostic purposes and may help to decide upon the appropriate action. Examples of detailed failure reasons include oil pressure, over-temperature, over-speed, urgent stop, starter circuit failure or alternator regulation failure.

All electrical protection of pumps, fans, auxiliary and main power supplies may to be monitored.

Maintenance

Maintenance of a diesel generator set and its associated switchgear is different to that carried out on battery/rectifier systems. This is maintenance of a hazardous mechanical machine that must be done without any voltage present and no mechanical movement possible. The fuel circuit and auxiliary electrical services that need to be isolated to make the generator system safe for maintenance must be monitored to ensure that they are returned to operational service when work is complete.

Test

To ensure correct operation, standby generator systems should be tested periodically. It is useful on large machines to make individual tests on automatic devices such as fans, pumps, heaters and switch gear etc. and to check manually operated switches, to verify that maintenance has been correctly carried out. For any test, it is important to record the sequence of test and the parameters used. This data can provide invaluable information for operational maintenance engineers.

4.1.4 Room thermal monitoring

For network equipment rooms it is useful to measure and record temperature and relative humidity with a sufficient precision and frequency.

4.1.5 Fan system

With fan systems, it is useful to detect motor and louvre faults and to be informed when filters need replacing. Circuit breaker status should be monitored and sensors may be used to detect airflow failure.

4.1.6 Cooling system with compressors

Environmental systems that provide a cooling function by using compressors for refrigeration circuits must be monitored for failure and abnormal operation. Circuit breaker status should be monitored as should refrigerant pressures to detect leakage. In the case of redundant cooling units, a sequencing device may be used to equally share the running time between units.

4.1.7 Chilled water cooling system

Environmental systems that provide a cooling function using chilled water must be monitored for failure and abnormal operation, e.g. water flow failure/temperature, pumps, valves and fans. Circuit breaker status should be monitored as should water levels to detect leakage. Leak detection within telecom facilities should be deployed if any of the cooling system is co-located with the telecom equipment.

4.2 Supervision functions

The functions detailed below are derived from the information given in clause 4.1:

- alarm and warning;
- event log-book;
- measurement records;
- dynamic graphical synopsis;
- remote control;
- on line help;
- local and remote process command (individual tests, and global operation, e.g. starting the engine);
- customized parameters and pattern saving;
- default values resetting (safe value for engine);
- software download for backup and upgrade (process and monitoring network elements programs);
- management (passwords, networks addresses, calendar-clock synchronization all along the networks).

Tables 1 and 2 give a summary of the information and functions obtained through sensors and automation for power and cooling systems respectively.

Table 1: Summary of the monitoring/supervision information and functions for power systems

Information	Power supply without back-up	Power supply with battery (added information)	Power supply with battery + back-up generator (added information)
Alarm	- Dying gasp - Partial failure (open protection, rectifier)	As for power supply without back-up plus : - discharge warning (timeout) - low voltage threshold - over-charge - over-temperature - unbalanced charge or discharge branch current, cell voltage - open circuit (open fuse holder, blown fuse link or circuit breaker trip for security during replacement or fire)	As for power supply with battery plus: - low level alarms (fuel, lubricant oil, coolant, etc.) - failed start - safety stop (oil pressure, oil, water overheating, overspeed, urgent stop button locked…) - undetermined/catastrophic stop - voltage or frequency out of limits (speed or alternator regulation failure) - fuel leakage - protection trip (fans, pumps, auxiliary, main power, etc.) - manual/maintenance mode, e.g. automatic control disabled - starter, fuel inhibited (for security during maintenance or fire)
Warning	- Loss of redundancy	As for power supply without back-up plus: - overload replacement needed float voltage out of limits (e.g. relative to battery temperature)	As for power supply with battery plus: - oil replacement needed - air filter replacement needed - transient or distortion on mains (mains quality)
Measurement		- dc voltage - dc current - battery temperature	As for power supply with battery plus: - fuel, oil gauge - ac voltage - ac current - ac frequency
Calculated value		- Estimated autonomy level during discharge - Estimated remaining full capacity (with ageing, temperature acceleration, global discharged Ah, abusive discharge like bad floating voltage, over-discharge, etc.) - Battery age since installation	As for power supply with battery plus: - estimated autonomy level of generator - running time (since installation, since last maintenance, since starting) - oil and water preheating operation time
Information	- Ratio of used/installed power (capacity management)	As for power supply without back-up plus: - battery tests execution report (recorded discharge curve, temperature, branch current, cell voltages, etc.	As for power supply with battery plus: - Generator and individual device tests execution report (starting test, running test, switch-gear operation, progressive loading, pump, fan tests) - starting reason (mains outage, poor mains quality, manual, test, undetermined)

Information	Power supply without back-up	Power supply with battery (added information)	Power supply with battery + back-up generator (added information)
Associated functions		- Event log-book - Measurement records - Dynamic graphical synopsis - Remote control - On line help - Back-up of customized parameters (e.g. can be used for system recovery) - Default values resetting (floating voltage, ...)	As for power supply with battery plus : - default values resetting (safe value for engine)
Power distribution monitoring (independent of back-up)	- Remote power feeding failure (for example loss of power on one pair) - Earth leakage detection on ac distribution. In some cases, there can be an automatic trial to eliminate the fault by opening the circuit breakers one by one - Earth leakage detection on dc remote feeding - Earth leakage detection on high voltage battery (e.g. 300 V to 500 V) - dc power, dc energy consumption - ac power, ac energy consumption (global metering, dedicated user metering), for variable use, consumption curve can be recorded as well as short power peaks		

Table 2: Summary of the monitoring/supervision information and functions for cooling systems

Information	Thermal environment	Fan cooled	Cooling systems with compressors/chillers
Alarm	- Temperature and humidity exceeds a maximum value, ETSI absolute maximum range is given in EN 300 019-x (all parts). - Rate of change of temperature	- Rate of change of Temperature when fans operate - Automatic control sequence failure - Speed variation default	- Problems on fans, pumps, etc. - Automatic control sequence failure - Speed variation default - Fluid leakage detection
Warning	- Out of normal ETSI ranges, for a longer duration than specified by ETSI EN 300 019-x (all parts)	- Filters, fans, Replacement needed (based on time counters or condition)	- Fluid replacement needed based on time counters or condition
Measurement	- T ± 0,5°C, ± 5 % relative humidity - At least, one sensor per room	- Operation time counter for filters and fans - Delta P to estimate filter or fans or louvre problems - Energy consumption	- Operation time counter for operation for filter, fans, fluid, pump, compressors - Energy consumption
Calculated value		- Estimated autonomy level if fan failure considering outside temperature	- Estimated autonomy in case of cooling system failure considering outside temperature - Running time (since installation, since last maintenance, since starting)
Information		- Efficiency = measured cooling system power consumption/measured telecom equipment power consumption - Fan test execution report (on/off, delta P)	- Efficiency = measured cooling system power consumption/measured telecom equipment power consumption - Tests execution report
Associated functions	- Temperature, relative humidity measurement records (for example 5 min period)	- Event log-book - Temperature, relative humidity measurement records (for example 5 min period) - Customized parameters saving - Default values resetting - Power and energy consumption records (every hour)	- Event log-book - Temperature, relative humidity measurement records (for example 5 min period) - Dynamic graphical synopsis - Remote control - On line help - Customized parameters saving - Default values resetting - Power and energy consumption records (every hour)
Remote control		- At least 2 level for summer/winter - Precise tuning but with min/max safety - Program download with default to previous release - Scheduled remote heating or cooling command for intervention with timer limit	- At least 2 level for summer/winter - Precise tuning but with min/max safety - Program download with default to previous release - Scheduled remote heating or cooling command for intervention with timer limit

5 Network architecture

Equipment should give the information described below at their monitoring interface. Network operators want to collect data from heterogeneous equipment and bring the information to a common supervision room or to the terminal of intervention agent at any location.

The SCADA [8] architecture (see annex D), is one of the possible target for the whole supervision layer.

However several possibilities still co-exist:

- Remote intelligence: serial data in a rough format produced from equipment automation or intelligent sensors (generally binary frames) or local concentrator are fully transmitted without filtering to a distant supervisor. The supervisor makes the intelligent tasks of filtering of repetitive and redundant information, translation in readable events, addition of time, display on screen in windows and data storage.
- Local intelligence: local conversions of protocol towards a single common high level message protocol and display (generally texts, colour and graphics, dynamic synopsis). Messages and data can be sent to a distant supervision centre for display, analysis and storage.
- Telecommunication Management Network (TMN) with a unified query language interface in the equipment, for example ASN.1 [14]. The supervisor speaks only in programming protocol to get or put values in the equipment. The equipment and possible functions must be described as objects in a Management Information dataBase (MIB).
- Hybrid solutions: this is a mixture of solutions used in old existing networks with equipment of various generations and in an existing part of the supervision network.

5.1 Alarm loops

It is generally the case for equipment without microprocessor. For example, environment alarms are collected on an external common device that creates a message. Several fields can be used to help intervention decisions. Typical fields include:

- date + time;
- alarm priority level e.g. critical, major, minor etc.;
- start or end of event;
- alarm or event code;
- circuit/subcircuit: for example dc cabinet N°x, rectifier N° y;
- text message: fault description;
- technical field: data about the possible cause of fault;
- alarm acknowledge: which test is necessary to clear the alarm.

Some field can be filled on local server and other on remote supervision server.

5.2 Local intelligence

A computer receives rough information via a field bus from automation unit or more readable data from equipment from intelligent units that make pre-process (including for example information filtering, presentation layers, etc.).

The basic functions of this local intelligence are:

- concentrator of different equipment interfaces with different protocols;
- server with a single unified protocol towards the remote supervision centre or a computer with specific software.

Extra functions include:

- web server for remote access from anywhere with a light client browser on a personal computer;
- GSM server with vocal or SMS messages;
- local data storage for equipment in the centre and for operational staff (e.g. electronic log-book, parameters, helps, configurations, manual intervention log-book).

Some equipment can have direct access to a LAN through a management protocol like SNMP or ASN.1. In this case, there is a common description of the equipment in a MIB that helps to standardize data exchange to various equipment and the post-treatment of information.

This could be the target solution, but it is still very complex and expensive for small facilities equipment. There is not a single standard protocol, and it is not implemented in the great majority of existing network or off-the-shelf equipment.

5.3 Remote intelligence

The network may transmit transparent information to intelligent terminals. For example this could be binary field protocols, ASCII for example modbus, JBus.

Field bus links are deported to be treated with specific drivers in supervision servers to prepare supervision screen, events logbook, etc.

The risk is that the dataflow is heavy and can saturate the network and the remote server.

5.4 Hybrid solutions

It is highly probable that there will be a mix of all these solutions because of a progressive evolution from the existing environment (see figure 4).

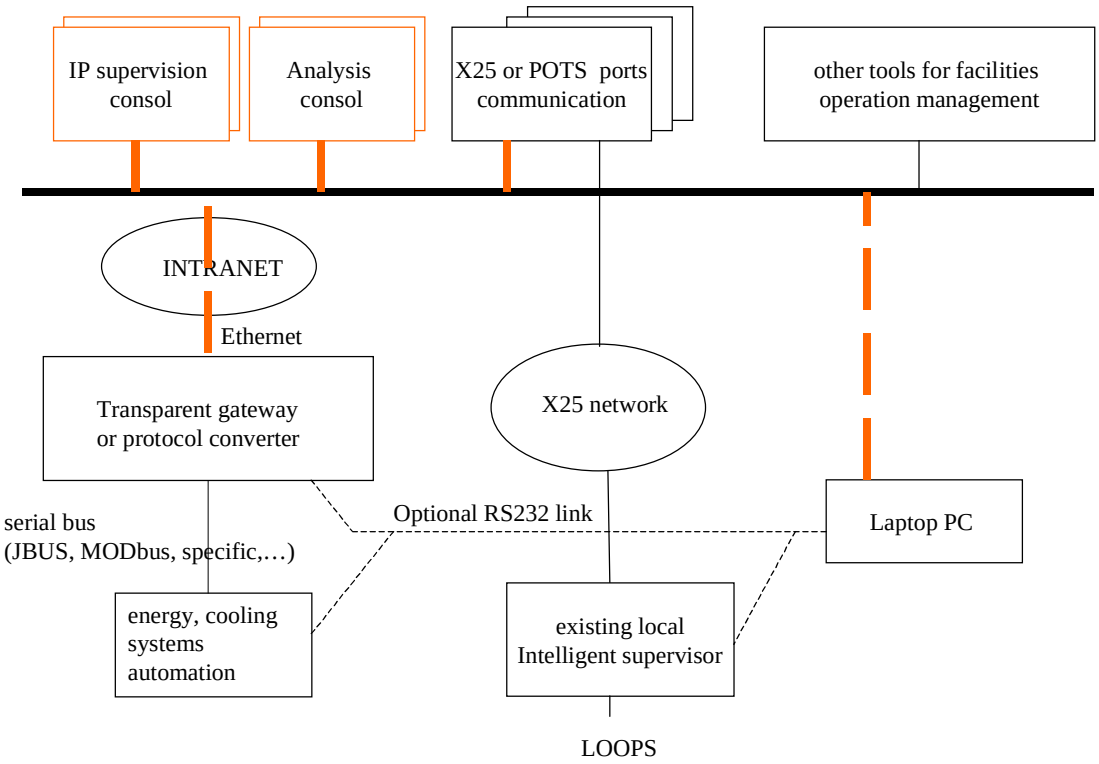


Figure 4: Principle of progressive evolution towards a unified supervision network

For example, loops and bus are collected on monitoring equipment connected through ITU-T Recommendation X.25 [23] on leased line towards a supervisor. Other equipment have bus output and are connected to protocol converters towards X.25 or IP over PSTN or ISDN or ADSL. Other equipment has for example direct Ethernet output with SNMP or other protocol.

In supervised places, it is possible to keep on the existing supervised equipment without changing interfaces, and to add a new one through an Ethernet IP gateway.

In the supervision room, it is possible to progressively migrate from old supervision posts to new ones through Ethernet on an Intranet network.

A laptop can be connected anywhere on Ethernet or by direct serial port (RS 232, USB) to local equipment or to a distant post.

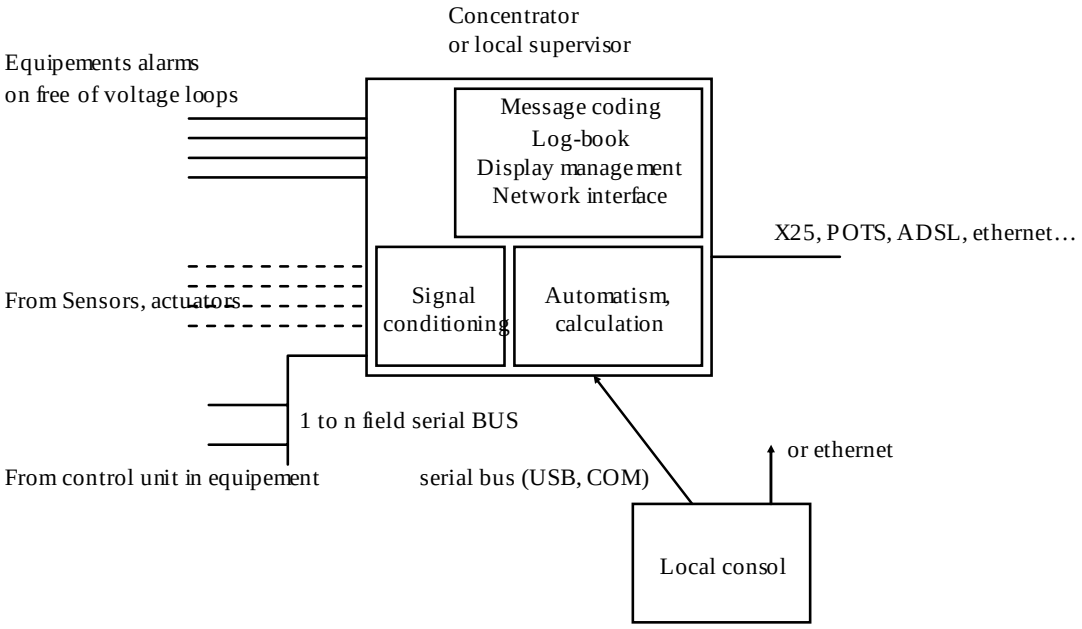


Figure 5: Principle of a concentrator/translator/local supervisor server unit on site

To achieve this unified network architecture, a basic node (concentrator server) is generally needed to accept very heterogeneous equipment interfaces and to translate these towards a common open interface (see figure 5).

Information coming from sensors must be conditioned and analysed (threshold comparison + combination + other algorithms). If this is done, alarm or information loops may be sufficient to transmit the information. In some cases further analysis may be needed. Sometimes a great variety of such data are gathered in a serial bus (field bus from equipment).

After receiving this rough data the concentrator server must process it to get significant and formatted information.

The information may then be sent continuously or immediately when a change occurs (event mode), but generally it is memorized to be given later (at request from a human client or regular polling from a machine). There are several data flows necessary within the local concentrator/server for remote control, management and supervision functions:

- Human-Machine Interface (HMI): the local server gives readable information and accepts commands (e.g. about the state of the equipment under text or graphical format html or equivalent).
- Machine-Machine Interface (MMI):
  - with equipment: the site machine acts as a client to get rough information from equipment on field bus or on various physical links using logical formats and protocols;

- with remote supervision: the site machine acts as a local server:
  - server mode: data transfer of log-book under request;
  - event mode: spontaneous sending of information (e.g. alarm, event);
  - service mode: data integrity test and restore mode, network test, date/time setting.

The more work done in the equipment towards creating a unified protocol, the less the local server has to do and its configuration management will be easier. At minimum, it could be a transparent routing unit.

6 Supervisor functions and performance

6.1 Supervision functions

The supervison servers (see figure 1) must receive all these protocols and propose a unified interface for data treatments, monitoring, remote control and intervention management (see annex A).

The following functions are required:

- messages are standardized to a common format (e.g.: ISO/IEC Guide 73 [13], ITU-T Recommendation X.733 [16]), then stored and used in a database (see annex A);
- synopsis of the equipment is stored in a library to reduce design time and errors;
- help checklists are associated to every alarm to explain possible causes. These help to give diagnosis of the failure and help with the reparation and verifying process;
- specific variables can be recorded to help diagnosis;
- events correlation is possible for expert analysis purposes;
- tests results are automatically checked;
- the supervisor is a web server on the intranet and/or through a (PSTN, ISDN or ADSL) modem from anywhere;
- there is a security management with different password-levels;
- there is synchronization of date-time of every device creating messages;
- there is configuration administration with remote up-down loading capability.

6.2 Supervision performance

Synopsis has to be refreshed in order to see real time alarms, acknowledgement, and remote command effect. Special consideration must be given to periods of crisis when, for example, several centres are affected by a general blackout or a climatic event.

- Alarms are transmitted and refreshed in 1 s.
- Synopsis is refreshed in less than 5 s.
- Restart time in case of reset is less than 60 s.
- Supervision can be done on a minimum of 5 display terminals at the same time on different sites.

6.3 Data integrity, coherence, reliability

Basic rules are:

- describe where the data is to ensure integrity, coherence or unity;
- know who will use the data/information today, tomorrow and also in the future;
- use a reference name that exists (for example the site name that must be single);
- avoid access from multiple points on the MIB (see annex B) or have coherence checking tools including self-storage of the latest version, recovery tools, integrity and code version checks;
- when using IP it is important to limit the amount of access ports for security reasons;
- system patches and security updates should be applied as soon as available.

Global counters of pending alarms for sites or equipment can be a good indicator of alarm integrity. It is also useful in cases of server restart to get the detailed alarm list.

Centralized server unavailability should be less than 5 minutes per year, this may be achieved using redundant servers. In any case equipment should be able to output differed and prompt alarms to avoid network blackout.

Databases of events and configurations of sites should be duplicated in mirror storage.

Every day a logbook should be requested. A continuous logbook should be composed and stored in an archive on at least two redundant hard disks.

Time/date for stamping events should be regularly self- tuned (synchronized) on a master clock through the network.

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.

MIB manager tools, graphical tools, etc., must 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.

6.4 Software working and development environment

Servers often use standard environments like Microsoft Windows NT/XP, UNIX or LINUX. Dynamic webs use PHP, a generalist language very close to the C language, with a reliable database e.g. MySQL. PHP very efficiently generates dynamic html pages.

The most diffused web-server on the Internet is Apache (literally, A patchy server). This is able to answer a client calling a web page with an HTTP request on port 80.

The same environment can be used in a supervision platform and in remote site data servers.

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

Tools must be available to build the MIB and the graphical synopsis. They can be built or modified using a library of commonly described existing configurations, to avoid errors and save time.

7 Cost consideration

The decision to install or upgrade monitoring tools and network supervision is generally based on optimization of global cost of plant. The installation must be sized with less material redundancy, with efficient automation and supervision. Automatic tests allow reduction of MTTR. Supervision allows precise management of failures, thanks to remote control facilities. For example engine starting, disconnection of non-critical loads to get longer battery autonomy), and priority management in case of zone crisis (storm, lightning, etc.).

In general, it is not easy to demonstrate the advantage of a plant supervisory platform because investment must be made before benefits are realized. However, there is great interest in remote supervision and control especially for:

- batteries (test reports) - to monitor the health condition and avoid service outage due to battery failure;
- standby/backup generator (test reports) - to ensure their ability to start and guarantee the reliability of the power system;
- remote tuning of cooling systems - to reduce power consumption and adapt to changes in equipment heat load within the room;
- diagnosis of equipment/system failures - data can be used to prevent similar occurrences in the future.

New equipment can now be fitted with an integrated control unit that can communicate with a local web-enabled communication interface. The overall cost of supervision may be reduced using IP (for example over Ethernet or xDSL link), but careful security consideration must be taken when such a system is planned.

Common practice is to limit the cost of supervision add-ons considering the following:

- cost and implication of service loss;
- power equipment cost;
- testing system pay back (with a gain in equipment lifetime, for example of the battery).

Annex A:
Common monitoring and supervision operation sequences

Preventative or corrective maintenance generally follows a common user supervision chart that is summarized in the following tables.

For faults that do not require to be acknowledged and fixed (short single or repetitive event): see table A.2.

For faults that do require to be acknowledged and fixed: see table A.3.

Data along the charts can be exchanged with real-time supervision and intervention functions, or off line analysis.

The different data types are described in table A.1. They may be located or not on the same server, and more or less mixed together in the same or separated database.

In this informative example (see table A.1) a separated name has been given to each database for simplicity.

Table A.1: Example of monitoring/supervision information databases

Data	Abbreviation	Comment
Site Name Server	SNSB	At national level (generally). Comparable to a DNS.
Access Base	AXB	Photo, maps of sites access, equipment access in the site.
Equipment Inventory Base	EIB	Database listing the equipment contained in the site.
Intervention Resource Base	IRB	For human staff and maintenance tools or spare parts. Intervention management. Spare parts management. (may be split in several data bases).
Diagnostic and maintenance help Base	HLPB	Informative database containing information to help the diagnostic of potential failures (and help correcting them).
Preventive maintenance Base	PMB	Generally a calendar of routine operation, coupled to IRB in order to optimize use of resources.
Graphic Base (Synoptic)	GRB	Graphical object library.
Logged events Base	LOGB	For real time alarms and chronologic events log-books.

Supervision staff use the synoptic (GRB base) and react as follows in the case of alarms or maintenance routines:

Table A.2: Example of alarm processing with no human intervention required (warning)

Origin	Alarm signalling	Data base	Intervention
Too short error	Nothing	Nothing	
Significant error	Alarm start (warning) Alarm end	Writing in LOGB LOGB	

EXAMPLE: When a communication line (or bus) is disturbed, an alarm start is generated when the communication fails, and an alarm end is automatically generated when the communication is re-established. Human intervention is not required unless the error repeats too often.

Table A.3: Example of alarm processing where human intervention is required

Origin	Alarm signalling	Data base	Intervention
Fault or preventive routine maintenance	Alarm start	Writing in LOGB [fault]	
		Writing in IRB	Intervention start
		Reading HLPB	Pre-diagnostic
		Reading/writing in IRB Reading in HLBP	Remote command trial If not enough Corrective intervention
Reparation, test, end of fault	Alarm end	Writing in LOGB, IRB	End of intervention Potential bases refresh (AXB, PMB, EIB)

Figure A.1 shows what happens with time. For example, the battery test will detect a battery loss of capacity, and then an alarm message is generated. The supervision centre is informed and manages intervention. First of all, maintenance staff are sent on site to determine which part of the battery (cells, strings) must be replaced. Then, the battery part must be provisioned. For the provisioning time, the alarm can be acknowledged in order not to mask another one. When the new battery is available, a new intervention is programmed and the battery is replaced and tested. If no alarm occurs, then end of intervention is declared.

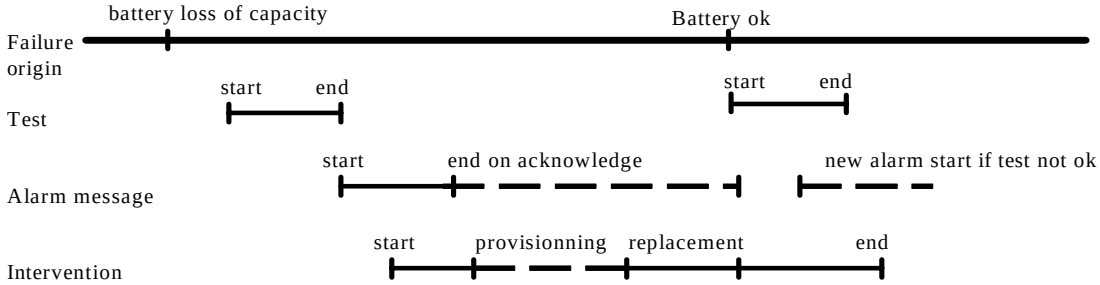


Figure A.1: Time diagram from a failure start to a reparation intervention

Annex B:
MIB template

Equipment is generally described as objects with a list of features to identify them and their applicable properties.

A partial example is given for a big site x with n plants, each plant having several ac and dc equipment, each equipment having sub-equipment. It is essential to list inheritance of properties and for this to be referenced to parent lists and children lists.

FACILITIES SITE x LIST (sub-list of zone site supervision list):

- Site (single name coming from SNSB database, IP address).
- Plant list: plant1, plant 2,…, plant n.
- Associated list (plant 1, plant 2, …, plant n, interconnection in the site).
- Actions: modify, create and link with other data, link with synopsis.

PLANT n LIST (sub-list of site x)

- Equipment list: Mains interface and ac board 1, backup engine 1, backup engine 2, dc rectifier battery cabinet 1, dcRB2, dcRB3, UPS1, UPS2 ... (It may be described as standard configuration if these configurations exist).
- Actions: modify, create, link with other data, link with synopses (GRB).

EQUIPMENT LIST (backup engine 1 list, a sub-list of plant 1)

Equipment function:

- backup Generator;
- associated sub-equipment list (alternator, cooling system, starting circuits, etc.).

Equipment Inventory Base (EIB):

- manufacturer;
- date;
- serial number.

Physical features:

- gas turbo-generator;
- power in kW or kVA;
- nominal voltage in V;
- dc, single phase ac, 3 phase ac;
- cooling by air;
- electric starters.

Properties (synopses script):

- synopsis (graphical representation on general synopsis of site with link with the ac board of the plant) (GRB);
- dynamic animation on synopsis;
- optional picture (AXB).

Option: sub-address of equipment monitoring device.

Actions: modify, create, link with other data (HLPB), link with synopsis.

SUB EQUIPMENT LIST (alternator, a sub-list of backup engine 1)

Equipment function:

- backup Generator alternator;
- associated sub-equipment list (no).

Equipment inventory:

- manufacturer;
- date;
- serial number.

Physical features:

- power;
- nominal voltage;
- dc, single phase ac, 3 phase ac.

Properties (synopses script):

- synopsis (graphical representation on general synopsis of equipment);
- dynamic animation on synopsis;
- optional pictures.

Actions: modify, create, link with other data, link with synopsis.

Annex C:
Message format

An example of a standard event or alarm message is proposed which is generally in accordance with ISO/IEC Guide 73 [13] and ITU-T Recommendation X.733 [16].

Example of internal machine record

Pos.	Information	Correspondence with CMIP (X.733)	Content	Car. number
1	Event nature (start/end) and seriousness serious fault fault warning undetermined End of event	Event type Perceived severity	 $$$sp, $$spsp $spspsp sp$$sp idem with # note: "$" indicates the start of event, "#" indicates the end of an event.	4
2	Recording number		*N=xxxx/ modulo 9999	8
3	Telecom domain (ENVironment for this guide, but more generally SWItch, ATM, aDSL, SDH, …)	Additional Information *** (other item gathered in this item)	xxx/	3
4	Time date code	Event time	yy-mm-jj/hhH-mm-ss	19
5	Geographical origin (single site name)	***	xxxxxxxxxxx/	13
6	Alarm type descriptor message (detected fault)	Probable cause	xxxxxxxxxxxxxxxxxxxx/	21
7	Delimiter		CR LF	2
8	emitter code	***	xxxxxxxxxx/	12
9	alarm type code (reference to an alarm dictionary)		xxxxxx/	8
10	affected resource identification (backup ac 1, dc A, …)	managed object instance	xxxxxxxxxxxxx/	17
11	monitored equipment identification (room, row, cabinet, board, …)	***		
12	affected resource type (backup ac, 48 V, permanent ac,…)	managed object class		
13	monitored equipment type (diesel engine 1, rectifier cabinet 6, …)	***		5
14	detector code (local supervisor IP address)	***		14
15	operator entity (responsible of the service or equipment)	***		3
16	Repetitive	specific problems		1
17	technical comment (detail about probable origin, …)	additional text		207
18	alarm category (EQUipment, QOS, ENV, etc.)		xxx	3

Other CMIP fields exists with no immediate correspondence: backed-up status, back-up object, trend information, threshold information, notification identifier, correlated notifications, state change definition, monitored attributes, proposed repaired actions.

The seriousness or degree of alarm is a technical evaluation. The intervention classification may be different because of priority management for example in the case of zone crisis on several sites or multiple alarms on a site.

Positions 11 and 13 must be filled together.

Not all this data is mandatory. The minimum set is:

- position 1: event nature (start/end);
- position 1: event gravity or seriousness;
- position 4: time/hour;
- position 6: event description message;
- position 12: affected resource type;
- position 10: instanced or identified resource.

Record number and emitter code must be entered by the data server. If not, they have to be entered by the receiver (supervisor), in order to keep integrity and coherence.

The 0000 record number is reserved to signal a sequence error. Such an event could be caused by supervision network collapse. In this case all pending alarms must be sent again once the supervision system is restarted.

Example of simple message display

The table below gives an example of simple message display (not all internal field are displayed here).

`$$ RB06-B: <50 % capa test MM/yy hh:min`	• $$ medium severity alarm start • RB06 : Rectifier Battery, cabinet number 06 • B: Battery alarm • < 50 % capa test: the battery has failed the automatic capacity test
`SU007: test branch/replace TST BATT` `12345678901234567890123456789012345678901234567890`	• 007: reference number of the message in the log book of the SU • SU: detected by control unit of RB cabinet • test branch/replace: technical help • TST BAT: automatic test to do. Manual operation required to reset the event and get an end of alarm message ## (generally to do after replacement of the battery)

In addition colour can be used, for example:

blinking RED:	pending $$$ alarm	fixed RED:	acknowledged from supervision
Yellow:	pending $$ alarm	fixed yellow:	acknowledged
White:	end of alarm or warning or common event		

Annex D:
SCADA systems

Widely used in industry for Supervisory Control And Data Acquisition of industrial processes, SCADA systems are used for the controls of power supply, cooling systems, etc.

SCADA is a purely software package interfaced to hardware, in general Programmable Logic Controllers (PLCs), or other commercial hardware 100 000 input/output (I/O) modules.

SCADA range is from 1 000 to several channels.

SCADA runs on UNIX, Windows XP or Linux.

The SCADA concept does not replace proper engineering or the need to reduce development effort. The aim is to reach a system that complies with the requirements, that is economical in development and maintenance and that is reliable and robust. Examples of engineering activities specific to the use of a SCADA system are the definition of:

- a library of objects (PLC, device, subsystem) complete with standard object behaviour (script, sequences, ...), graphical interface and associated scripts for animation;
- templates for different types of "panels", e.g. alarms;
- instructions on how to control e.g. a device;
- a mechanism to prevent conflicting controls, and maintain coherence of the supervision system through the network;
- alarm levels definition;
- intervention behaviour to be adopted in case of specific alarms and if multiple alarms;
- same "look and feel" wherever in the system (not guaranteed by SCADA itself but by SCADA configuration).

Architecture

SCADA has two basic layers:

- the "client layer" for man machine interaction;
- the "data server layer" for data control activities. The data servers communicate with process controllers, e.g. PLCs, either directly or via networks or field buses that are proprietary (e.g. Siemens H1, Merlin Gerin JBUS, Modicon Modbus, ...), or non-proprietary (e.g. Profibus, FIP). Data servers are connected to each other and to client stations via Ethernet LAN or intranet or internet.

SCADA software is multi-tasking and based upon a real-time database (RTDB) located in one or more servers. Servers are responsible for data acquisition and handling (e.g. polling controllers, alarm checking, calculations, logging and archiving) on a set of parameters.

Communications

Internal Communication

Server-client and server-server communication is in general on a publish-subscribe and event-driven basis and uses a TCP/IP protocol, i.e. a client application subscribes to a parameter, which is owned by a particular server application, and only changes to that parameter are then communicated to the client application.

Access to Devices

The products provide communication drivers for most of the common PLCs and widely used field-buses, e.g. Modbus. Both Profibus, Worldfip, CANbus. Some of the drivers are based on third party products (e.g. Applicom cards) and therefore have additional cost associated with them. A single data server can support multiple communications protocols. The effort required to develop new drivers is typically in the range of 2 to 6 weeks depending on the complexity and similarity with existing drivers, and a driver development toolkit is provided for this.

Interfacing

Application Interfaces/Openness

SCADA offers an Open Data Base Connectivity (ODBC) interface to the data in the archive/logs, but not to the configuration database, an ASCII import/export facility for configuration data, a library of APIs supporting C, C++, and Visual Basic (VB) to access data in the RTDB, logs and archive.

Database

The configuration data are stored in a database that is logically centralized but physically distributed and that may be of a proprietary format. The server RTDB may be of proprietary format for performance reason.

The archive and logging format is usually also proprietary for performance reasons, but some products do support logging to a Relational Data Base Management System (RDBMS) at a slower rate either directly or via an ODBC interface.

Scalability

Scalability of SCADA consists in adding more process variables, more specialized servers (e.g. for alarm handling) or more clients by having multiple data servers connected to multiple controllers. Each data server has its own configuration database and RTDB and is responsible for the handling of a sub-set of the process variables (acquisition, alarm handling, archiving).

Redundancy

SCADA may have software redundancy at a server level, which is normally transparent to the user.

Functionality

Access Control

There are defined access privileges to the process parameters of the system and to specific functionality.

Multi Media Interface MMI

SCADA is a multiple screens system, with combinations of synoptic diagrams and text, described in "generic" graphical object with links to process variables. These objects can be "dragged and dropped" from a library and included into a synoptic diagram and included in a library of standard graphical symbols.

Standard windows editing facilities are provided: zooming, re-sizing, scrolling, etc. On-line configuration and customization of the MMI is possible for users with the appropriate privileges. Links can be created between display pages to navigate from one view to another.

SCADA can support Web technology, ActiveX, Java, etc.

Alarm Handling

A lot of functions are provided to handle alarms:

- Visualization on several display.
- Acknowledgement function.
- Alarm filtering, prioritization.
- Group alarm handling.
- Generation on the server from limit or status checking or more sophisticated expression.
- E-mails, GSM message automatic sending, etc.

Logging/Archiving

Logging, medium-term storage of data on disk is typically performed on a cyclic basis, i.e. once a certain file size, time period or number of points is reached the data is overwritten. The logged data is time-stamped and can be filtered when viewed by a user. The logging of user actions is in general performed together with either a user ID or station ID. Logged data can be transferred to an archive (disk or on another permanent storage medium) once the log is full. There is often also a VCR facility to play back archived data.

Report Generation

Reports are produced using SQL type queries to the archive, RTDB or logs and other calculation tools. Automatic actions, triggered by events are also possible through a scripting language.

An expert system can be offered for diagnosis.

Trending

Parameters can be trended in predefined or defined on-line charts. Real-time and historical trending from archives is possible. Zooming and scrolling functions are provided as well as display of parameter values at the cursor position. The trending feature is either provided as a separate module or as a graphical object (ActiveX), which can then be embedded into a synoptic display.

Application Development

Configuration

First the process parameters and associated information (e.g. relating to alarm conditions) are defined through some sort of parameter definition template

Second the graphics, including trending and alarm displays are developed, and linked where appropriate to the process parameters.

An ASCII Export/Import facility, enables large numbers of parameters to be configured in a more efficient manner using an external editor and then importing the data into the configuration database. The different aspect of the configuration, including the graphics, can be stored in discriminated folders to clarify the configuration.

On-line modifications to the configuration database and the graphics is generally possible with the appropriate level of privileges.

Development Tools

The following development tools are provided as standard:

- a graphics editor, a library of generic symbols, a link editor to variables, and between views;
- a data base configuration tool (usually through parameter templates) with ASCII import/export/edit facilities;
- a scripting language;
- an Application Program Interface (API) supporting C, C++, VB;
- a Driver Development Toolkit.

Object Handling

SCADA can be of object type for graphic and configuration database.

New SCADA versions handle devices and even entire systems as full entities (classes) that encapsulate all their specific attributes and functionality.

History

Document history		
V1.1.1	September 2004	Publication