NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
61850-3

Première édition
First edition
2002-01

Réseaux et systèmes de communication dans les postes –

Partie 3:
Prescriptions générales

Communication networks and systems in substations –

Part 3:
General requirements

Numéro de référence
Reference number
CEI/IEC 61850-3:2002

Numérotation des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000. Ainsi, la CEI 34-1 devient la CEI 60034-1.

Editions consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

Informations supplémentaires sur les publications de la CEI

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique. Des renseignements relatifs à cette publication, y compris sa validité, sont disponibles dans le Catalogue des publications de la CEI (voir ci-dessous) en plus des nouvelles éditions, amendements et corrigenda. Des informations sur les sujets à l'étude et l'avancement des travaux entrepris par le comité d'études qui a élaboré cette publication, ainsi que la liste des publications parues, sont également disponibles par l'intermédiaire de:

- **Site web de la CEI (www.iec.ch)**
- **Catalogue des publications de la CEI**

  Le catalogue en ligne sur le site web de la CEI (www.iec.ch/catlg-f.htm) vous permet de faire des recherches en utilisant de nombreux critères, comprenant des recherches textuelles, par comité d'études ou date de publication. Des informations en ligne sont également disponibles sur les nouvelles publications, les publications remplacées ou retirées, ainsi que sur les corrigenda.
- **IEC Just Published**

  Ce résumé des dernières publications parues (www.iec.ch/JP.htm) est aussi disponible par courrier électronique. Veuillez prendre contact avec le Service client (voir ci-dessous) pour plus d'informations.
- **Service clients**

  Si vous avez des questions au sujet de cette publication ou avez besoin de renseignements supplémentaires, prenez contact avec le Service clients:

  Email: custserv@iec.ch
  Tél: +41 22 919 02 11
  Fax: +41 22 919 03 00

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site (www.iec.ch)**
- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (www.iec.ch/catlg-e.htm) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.
- **IEC Just Published**

  This summary of recently issued publications (www.iec.ch/JP.htm) is also available by email. Please contact the Customer Service Centre (see below) for further information.
- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

  Email: custserv@iec.ch
  Tel: +41 22 919 02 11
  Fax: +41 22 919 03 00

.

NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
61850-3

Première édition
First edition
2002-01

Réseaux et systèmes de communication dans les postes –

Partie 3: Prescriptions générales

Communication networks and systems in substations –

Part 3: General requirements

International Electrotechnical Commission 3, rue de Varembé Geneva, Switzerland
Telefax: +41 22 919 0300 e-mail: inmail@iec.ch IEC web site http://www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE Q

Pour prix, voir catalogue en vigueur
For price, see current catalogue

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMUNICATION NETWORKS AND SYSTEMS IN SUBSTATIONS –

Part 3: General requirements

FOREWORD

1) The IEC (International Electrotechnical Commission) is a world-wide organisation for standardisation comprising all national electrotechnical committees (IEC National Committees). The object of the IEC is to promote international co-operation on all questions concerning standardisation in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes International Standards. Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organisations liasing with the IEC also participate in this preparation. The IEC collaborates closely with the International Organisation for Standardisation (ISO) in accordance with conditions determined by agreement between the two organisations.
2) The formal decisions or agreements of the IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested National Committees.
3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61850-3 has been prepared by IEC technical committee 57: Power system control and associated communications.

The text of this standard is based on the following documents:

FDIS	Report on voting
57/557/FDIS	57/572/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 3.

Annex A is for information only.

IEC 61850 consists of the following parts, under the general title: Communication networks and systems in substations:

Part 1: Introduction and overview[1]

Part 2: Glossary[1]

Part 3: General requirements

Part 4: System and project management

Part 5: Communication requirements for functions and device models[1]

Part 6: Substation automation system configuration description language[1]

Part 7-1: Basic communication structure for substation and feeder equipment – Principles and models[1]

Part 7-2: Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI)[1]

Part 7-3: Basic communication structure for substation and feeder equipment – Common data classes[1]

Part 7-4: Basic communication structure for substation and feeder equipment – Compatible logical node classes and data classes[1]

Part 8-1: Specific communication service mapping (SCSM) – Mapping to MMS (ISO/IEC 9506 Part 1 and Part 2)[1]

Part 9-1: Specific communication service mapping (SCSM) – Serial unidirectional multidrop point to point link[1]

Part 9-2: Specific communication service mapping (SCSM) – Mapping on a IEEE 802.3 based process bus[1]

Part 10: Conformance testing[1]

The committee has decided that the contents of this publication will remain unchanged until 2004. At this date, the publication will be

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

---

[1] Under consideration.

COMMUNICATION NETWORKS AND SYSTEMS IN SUBSTATIONS –

Part 3: General requirements

1 Scope and object

This part of IEC 61850 applies to substation automation systems (SAS). It defines the communication between intelligent electronic devices (IEDs) in the substation and the related system requirements.

The specifications of this part pertain to the general requirements of the communication network, with emphasis on the quality requirements. It also deals with guidelines for environmental conditions and auxiliary services, with recommendations on the relevance of specific requirements from other standards and specifications.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of IEC 61850. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of IEC 61850 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 60654-4:1987, *Operating conditions for industrial-process measurement and control equipment – Part 4: Corrosive and erosive influences*

IEC 60694:1996, *Common specifications for high-voltage switchgear and controlgear standards*

IEC 60870-2-1:1995, *Telecontrol equipment and systems – Part 2: Operating conditions – Section 1: Power supply and electromagnetic compatibility*

IEC 60870-2-2:1996, *Telecontrol equipment and systems – Part 2: Operating conditions – Section 2: Environmental conditions (climatic, mechanical and other non-electrical influences)*

IEC 60870-4:1990, *Telecontrol equipment and systems – Part 4: Performance requirements*

IEC 61000-4-3:1995, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 3: Radiated, radio-frequency, electromagnetic field immunity test*

IEC 61000-4-4:1995, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 4: Electrical fast transient/burst immunity test.* Basic EMC Publication

IEC 61000-4-5:1995, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 5: Surge immunity test*

IEC 61000-4-6:1996, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 6: Immunity to conducted disturbances, induced by radio-frequency fields*

IEC 61000-4-8:1993, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 8: Power frequency magnetic field immunity test*

IEC 61000-4-10:1993, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 10: Damped oscillatory magnetic field immunity test*

IEC 61000-4-12:1995, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 12: Oscillatory waves immunity test*

IEC 61000-4-16:1998, *Electromagnetic compatibility (EMC) – Part 4-16: Testing and measurement techniques – Test for immunity to conducted, common mode disturbances in the frequency range 0 Hz to 150 kHz*

IEC TS 61000-6-5:2001, *Electromagnetic compatibility (EMC) – Part 6-5: Generic standards – Immunity for power station and substation environments*

CISPR 22:1997, *IEEE Standard for Information Technology Equipment – Radio Disturbance Characteristics – Limits and Methods of Measurement*

IEEE C37.90.2:1995, *Withstand capability of relay systems to radiated electromagnetic interference from transceivers*

3 Definitions and abbreviations

For the purpose of this part of IEC 61850, the following definitions and abbreviations apply.

3.1 Definitions

See IEC 61850-2[1].

3.2 Abbreviations

a.c.	alternating current
AIS	air insulated switchgear
d.c.	direct current
GIS	gas insulated switchgear
HMI	human – machine interface
IED	intelligent electronic device
IP	inter-networking protocol
MTTF	mean time to failure
SAS	substation automation system
SCADA	supervisory control and data acquisition
SF_6	sulphur hexafluoride
TCP	transport control protocol

[1] Under consideration.

4 Quality requirements

4.1 General

This clause details the quality requirements such as reliability, availability, maintainability, security, data integrity and others that apply to the communication systems that are used for monitoring, configuration and control of processes within the substation.

This clause contains a number of references to other IEC normative documents – with frequent reference to IEC 60870-4. IEC 60870-4 specifies performance requirements for a telecontrol system, classifying these requirements according to those properties that influence the performance of the system. These properties include such headings as reliability, availability, maintainability, security and integrity. For each of these properties, IEC 60870-4 lists a number of classes for these requirements, for which the systems resident in the substation can be expected to have to meet virtually the complete range. Where applicable, the conformance to a particular level of these classes shall be stated by the manufacturer, as defined in IEC 60870-4.

4.2 Reliability

4.2.1 General

The substation shall continue to be operable, according to the “graceful degradation” principle, if any SAS communications component fails. There should be no single point of failure that will cause the substation to be inoperable. Adequate local monitoring and control shall be maintained. A failure of any component should not result in an undetected loss of functions nor multiple and cascading component failures.

For some applications, particular provisions are necessary in the SAS implementation and the communications system must take these into account. An example is that the substation master may be redundant with automatic failover.

If communication elements of the SAS are redundant, there shall be no single failure mode that would disable both redundant elements. Redundant communication elements of the SAS shall be powered by separate independent power sources (for example separate battery or station service circuit), where such power sources exist. Redundancy is not mandatory and depends upon the importance of the substation, in other words, the consequences of an outage of that substation and the operator’s philosophy.

A fail-safe design shall be provided (i.e. is required). There shall be no single failure mode that causes the SAS to initiate an undesired control action, such as tripping or closing a circuit breaker. In addition, SAS failures shall not disable any available local metering and local control functions at the substation.

The reliability requirements shall be as described in 3.1 of IEC 60870-4. The reliability class severity (R1, R2 or R3), as defined in 3.1.2 of IEC 60870-4, shall be agreed upon between the manufacturer and the user.

4.2.2 MTTF

The manufacturer shall clearly state the MTTF of equipment provided, including reference to a standard method of calculation.

4.2.3 Critical functions in the substation and their dependence on the SAS

A single point of failure should not disable critical functions (protection, primary control function, metering, etc.). To accomplish this requirement, the SAS shall have the following characteristics:

- Protective functions shall operate autonomously.
- The SAS may be used to execute control logic actions, such as automatic failover following a transformer fault, which are not considered time-critical. If such logic actions are used, then the manufacturer shall clearly state the time (in milliseconds) to accomplish the failover.
- The SAS HMI shall be capable of independent operation of the telecontrol interface to the control centre.

4.3 System availability

4.3.1 General

Availability shall mean the ratio of uptime of the SAS to total time, as defined in 3.2 of IEC 60870-4. Uptime is the time that the SAS is able to perform its vital functions. For example, where secondary protection exists, failure of the primary protection shall not be considered as contributing to downtime. As a second example, failure of an HMI shall not be considered downtime if an alternative point of control exists.

The availability requirements shall be as described in 3.2.1 of IEC 60870-4. The availability class severity (A1, A2 or A3), as defined in 3.2.2 of IEC 60870-4, shall be agreed upon between the manufacturer and the user.

The specification for availability of the substation automation system (SAS) is not within the scope of this standard.

4.3.2 Automatic recovery

System and data backup may be provided for the SAS. Where backup is provided, a single unit failure in the SAS shall not cause loss of data nor prevent normal activity of the system. After repair, the switch back to the normal configuration may require manual intervention.

Critical communication links for SAS functionality may be redundant or allow alternate routing to prevent system outage due to a cut in the information transport infrastructure.

4.3.3 Graceful degradation and error recovery/backup

Increasing error rates should not cause a sudden system outage but result in graceful degradation. There shall be facilities for error recovery to restore reliable operation of the SAS.

4.4 Maintainability

See 3.3 of IEC 60870-4. The maintainability requirements shall be as described in 3.3.1 of IEC 60870-4. The maintainability class severity (M1, M2, M3 or M4), as defined in 3.3.2 of IEC 60870-4, shall be agreed upon between the manufacturer and the user.

4.5 Security

See 3.4 of IEC 60870-4.

4.6 Data integrity

The SAS communication system shall deliver reliable data in the presence of transmission and procedural errors, varying delivery delays, and equipment failures in the communication facilities. It must thus provide:

- detection of transmission errors in the noisy substation environment;
- recovery from link congestion;
- optional support for link, media and equipment redundancy.

The integrity and consistency of the data delivered by the SAS shall be as defined for integrity classes I1, I2 and I3 (3.5 of IEC 60870-4). The use of a specific integrity class shall be determined by the application that uses the delivered data.

4.7 General network requirements

4.7.1 Geographic requirements

The communication network within the substation should be capable of covering distances up to 2 km.

4.7.2 Numbers of devices

The communication network within the substation should be capable of serving all typical bay configurations in a high voltage switchyard, including systems with 1½ circuit breaker arrangements and ring busbars (see IEC 61850-1[1] and IEC 61850-5[1] for more details of sub-station configurations).

5 Environmental conditions

5.1 General

This clause details the climatic, mechanical, and electrical influences that apply to the communications media and interfaces that are used for monitoring and control of processes within the substation. When communications equipment is an integral part of another device in the substation, then the environmental requirements for the device itself shall apply to the communications equipment.

This clause contains a number of references to other IEC normative documents – with frequent reference to IEC 60870-2 and IEC 60694. IEC 60870-2 itself lists a number of classes for environmental climatic conditions, and for each class considers a severity level (or set of levels) for the various environmental climatic parameters. The equipment resident in the substation is expected to need to meet virtually the complete range of environmental classes – with the process level equipment often being in outdoor locations, the bay level equipment in outdoor or sheltered locations and the station level equipment in sheltered/enclosed locations. Where applicable, the classification and severity level of environmental climatic

---

[1] Under consideration.

conditions shall be stated by the manufacturer, as defined in IEC 60870-2-2. Where equipment forms an integral part with high voltage switchgear and controlgear (for example components of the process bus), IEC 60694 shall apply.

5.2 Temperature

The communications equipment shall operate satisfactorily over an air temperature range as recommended in IEC 60870-2-2, table 1.

During storage and transportation, the equipment shall be able to withstand an air temperature range as recommended in IEC 60870-2-2, table 2.

Note that air temperature is as defined in 3.3.1 of IEC 60870-2-2.

Where equipment forms an integral part of high voltage switchgear and controlgear, clause 2 of IEC 60694 shall apply.

5.3 Humidity

The communications equipment shall operate satisfactorily with a relative humidity as recommended in IEC 60870-2-2, table 1.

Where equipment forms an integral part of high voltage switchgear and controlgear, clause 2 of IEC 60694 shall apply.

5.4 Barometric pressure

The communications equipment shall operate satisfactorily between air pressures as recommended in 3.3.2 of IEC 60870-2-2 .

Where equipment forms an integral part of high voltage switchgear and controlgear, clause 2 of IEC 60694 shall apply.

5.5 Mechanical and seismic

Mechanical and seismic qualification of communications equipment shall conform to national and international standards according to its location and service. Where applicable, the classification of mechanical conditions and seismic stress shall be stated by the manufacturer, as defined in clause 4 of IEC 60870-2-2.

Where equipment forms an integral part of high voltage switchgear and controlgear, clause 2 of IEC 60694 shall apply.

5.6 Pollution and corrosion

IEC publication 60654-4 is considered applicable as a guideline in respect to corrosive and erosive influences. Particular attention has to be paid to the effect of solid substances (for example sand, dust) since they may also affect the thermal behaviour of the communications equipment and to the effect of corrosive elements (for example salt) which may affect the connectivity of the equipment.

Where equipment forms an integral part of high voltage switchgear and controlgear, clause 2 of IEC 60694 shall apply.

5.7 EMI immunity

Communications equipment shall be designed and tested to withstand the various types of induced *conducted* and *radiated* electromagnetic disturbances that occur in substations. Sources of disturbances are, for example:

- lightning and switching surges;
- discharges and strokes in gaseous isolation media, like the commonly used SF_6, producing fast transients;
- travelling waves in GIS, producing fast transients.

The general immunity requirements for the industrial environment are considered not sufficient for substations. Therefore, dedicated requirements are defined in IEC 61000-6-5, details of these requirements and testing procedures are given in the parts of the IEC 61000 series. The most important cases and documents are referenced below.

The conformity to the standards has to be proven by type tests. Criteria for acceptance are summarized in 5.7.4.

5.7.1 Conducted disturbances

5.7.1.1 Induced disturbances

Radio frequency fields may induce disturbances that are conducted by wires in the substation. The equipment shall meet either IEC 61000-4-6 class 3 or IEEE C37.90.2 regarding induced disturbances. The specific requirement (IEC standard or IEEE standard) shall be agreed between manufacturer and user.

5.7.1.2 Surges

Surges as per IEC 61000-4-5 (test levels to class 4) with waveforms 1,2/50 μs and 10/700 μs and peaks up to 4 kV.

5.7.1.3 Oscillatory waves

Oscillatory waves as per IEC 61000-4-12 class 3 and common mode disturbances up to 150 kHz as per IEC 61000-4-16 level 4, except that data communications and signal circuits shall be tested in common mode only but at the same surge magnitude as specified for transverse mode tests.

5.7.1.4 Fast transients

Fast transients as per IEC 61000-4-4 class 4 and above. In addition, power supply and output circuits shall be tested with transverse mode applied voltages.

5.7.2 Radiated electromagnetic disturbances

The equipment shall meet either IEC 61000-4-3 class 3 or IEEE C37.90.2 regarding radiated, radio-frequency electromagnetic fields. The specific requirement (IEC standard or IEEE standard) shall be agreed upon between manufacturer and user. Criteria for acceptance are summarised in 5.7.4.

5.7.3 Power frequency disturbances

Communications equipment may be subjected to various kinds of electromagnetic disturbances conducted by power supply lines, signal lines or directly radiated by the environment. The types and levels of disturbance depend on the particular conditions in which the communications equipment has to operate. Reference should be made to IEC 61000-4-16, for magnetic fields as well as to IEC 61000-4-8 and IEC 61000-4-10.

In addition to these tests, it is recognized that some degree of power frequency induced voltage will appear on all copper circuits inside substations, especially when primary fault currents are flowing in and around the substation. This will be a common mode effect, resulting from magnetic flux linkages, resulting in almost equal voltages being induced in each of the cores. With the introduction of serial data communications, circuit tests are required to ensure equipment is capable of withstanding typical induced voltages without interfering with the correct operation of the equipment. The substation equipment shall operate correctly in the presence of a power frequency voltage in accordance with table 1 below.

Table 1 – Power frequency voltage classes

Class	Length of communications circuit m	Unbalanced communi-cations V	Balanced communications (1% unbalance) V	Balanced communications (0,1% unbalance) V
1	1 to 10	0,5	0,005	0,0005
2	10 to 100	5	0,05	0,005
3	100 to 1 000	50[a]	0,5	0,05
4	Greater than 1 000	500[a]	5	0,5

[a] The unbalanced class of communications circuit covers cases such as RS232. For practical reasons, such communications systems are considered to be run over very short distances within the substation or to link equipment to intelligent test equipment such as portable computers. It is not proposed that they be practical for substation applications covering distances above 20 m. Standard balanced circuits are of the class associated with PTO circuits where up to 500 V of common mode voltage is balanced to within 1 %. In addition, techniques such as transformer coupling can achieve impedance balancing to within 0,1 %.

The induced transverse voltages at the power system frequency are benchmark values for a substation environment, and represent acceptable operating withstand levels for equipment designs.

The equipment should be tested using an injection network to combine the required communications signals with a power frequency interference signal. With the interference suitably injected, the magnitude of the communications signal levels should be reduced to the receive level claimed by the manufacturer and correct operation of the communications equipment should be maintained.

5.7.4 Criteria for acceptance

5.7.4.1 Application criteria

The criteria listed shall apply to the equipment being directly tested, and any device linked to the equipment via direct or remote connections. Examples of connections are current loops and voltage circuits (d.c., audio, carrier or microwave). Serial, parallel, optical fibre and radio frequency connections are included.

5.7.4.2 Conditions to be met

The equipment shall be considered to have passed the tests if – during, or as a result of, the tests – all of the following conditions are met for the equipment and the connected devices:

- no hardware damage occurs;
- no change in calibration beyond normal tolerance is caused by the test;
- no loss or corruption of stored memory or data occurs, including active or stored settings;
- system resets do not occur, and manual resetting is not required;
- established communications are not permanently lost;
- if disrupted, established communications automatically recover within an acceptable time period;
- communication errors, if they occur, do not jeopardize the protective or control functions;
- no changes in the states of the electrical, mechanical, or communication signal outputs occur. This includes alarms and status outputs;
- no erroneous, permanent change of state of the visual, audible, or message outputs occurs. Momentary changes in these outputs during the tests are permitted;
- no error outside the normal tolerances for data communication signals (SCADA analogues) occurs.

5.7.4.3 Equipment functioning

During and after the tests, the equipment and the connected devices shall be completely and accurately functional as designed, unless otherwise stated by the manufacturer.

5.7.4.4 Exceptions

Exceptions to the acceptance criteria pertinent to the equipment shall be stated in the manufacturer's specifications for the equipment.

5.7.4.5 Test points

Tests shall be included for:

- power supply inputs to each device;
- alarm and auxiliary I/O connections;
- permanently connected substation computers;
- keying and output connections between bay equipment and telecommunications interface equipment;
- all metallic connections to any Ethernet hub, including power supply inputs, alarms, and ports utilizing balanced twisted pair inputs.

Items excluded from testing are:

- non-metallic connections, such as fibre;
- temporary connected maintenance computers;
- connections that, as stated by the manufacturer, must be less than 2 m in length.

5.8 EMI radiation

Communications equipment may also be the source of various kinds of electromagnetic disturbances in a wide frequency range, that may be conducted through power supply lines, control lines or directly radiated by the equipment.

The communications equipment shall meet the requirements of CISPR 22 classes A and B (EN 55022A and EN 55022B) or FCC rules part 15 for class A and B digital devices [1] (USA).

6 Auxiliary services

6.1 General

This clause specifies the characteristics of the power supplied to communications equipment considered in this standard. Electrical energy for operation of communications equipment may be provided by:

- direct connection to the power source;
- connection to a power supply device, interposed between the power source and the equipment;
- auxiliary stand-by or back-up supply, which provides for operation of the equipment in case of maintenance or failure of the main power supply.

6.2 Voltage range

For this clause, only alternating current supplies having the same general characteristics as those exhibited by the public network supply at 50 Hz or 60 Hz and d.c. supplies are considered.

The voltage range for a.c. supplies shall be as detailed in IEC 60870-2-1, table 1.

The voltage range for d.c. supplies shall be as detailed in IEC 60870-2-1, table 5.

6.3 Voltage tolerance

The classes of voltage tolerance for a.c. supplies shall be as defined in IEC 60870-2-1, table 2.

The classes of voltage tolerance for d.c. supplies shall be as defined in IEC 60870-2-1, table 6.

The relevant classes from IEC 60870-2-1 shall be agreed upon between the manufacturer and the user.

Equipment operating on direct current shall not sustain damage if the input voltage falls below the lower limit specified or is reversed in polarity.

---

[1] Code of federal regulations, Title 47 – Telecommunication, Part 15: Radio frequency devices. Published by the Federal Communications Commission (FCC), 2000.

6.4 Voltage interruptions

The performance of the communications equipment shall not be affected in the case of an interruption to the d.c. supply of duration up to 10 ms. No damage shall be caused to the equipment by supply interruptions of any duration, nor shall the equipment respond to an interruption in a manner that could cause danger to other equipment or personnel.

6.5 Voltage quality

a) AC supplies

The nominal frequency of a.c. supplies should be within the tolerances defined in IEC 60870-2-1, table 3.

The harmonic content of a.c. supplies should be within the tolerances defined in IEC 60870-2-1, table 4.

b) DC supplies

The earthing arrangements for d.c. supplies should be as defined in IEC 60870-2-1, table 7.

Ripple voltage (as defined in 4.3.3 of IEC 60870-2-1) should be within the tolerances defined in IEC 60870-2-1, table 8.

Annex A
(informative)

Access security

The SAS should implement security features that counter, within appropriate user and cost constraints, the following threats:

- Denial of service – this threat attempts to deliberately impede legitimate access.

  In order to counter a denial of service attack, a combination of communication link and communication association and object protections should be employed. Whereas the communication link protection should be determined by the type of communication media/data link being used, the communication association protection methodologies can be detailed at a minimum.

  There are two major forms of denial of service that need to be countered:

  1) Link layer denial – in this attack, the attacker attempts to block legitimate access for the use of a physical communication path.

     EXAMPLE: An attacker dials a dial-up modem attached to the SAS. The phone and modem connections are established and the attacker leaves the line open. This denies the availability to communicate with the SAS system on the remote side of the attacked modem.

     The appropriate counters for link layer denial of service depend largely upon the physical media and communication topology of the SAS and typically is only a concern in the instance of remote access to the SAS. Therefore, appropriate counters should be determined on a system by system basis and are not subject to standardization within the scope of this standard.

  2) Association denial (resource exhaustion) – in this attack, the attacker attempts to lock many or all of the communication resources of the system under attack. Connection oriented communication profiles are particularly susceptible to this class of attack. For a high security data access level association establishment should be secured with a user authentication mechanism.

     EXAMPLE: Socket exhaustion for an SAS system implemented over TCP/IP. TCP is a connection oriented transport layer that is typically susceptible to this class of attack. The attacker connects to the TCP port as many times as is possible. However, no legitimate application level activity occurs. Each TCP connection consumes a communication resource (socket) and those sockets are consumed until the attacker relinquishes the sockets or until the remote system disconnects the attacker.

     This class of attack can be detected in the SAS implementation by forcing application associations to occur within a given period of time. This timeout should start upon a connection oriented resource being consumed (for example a socket) at any layer within the SAS communication profile. The SAS implementation should reclaim the communication resource after the expiration of the timeout.

     NOTE This is a valid mechanism for protecting dial-in modems from attack as well.

- Illegitimate use – the attacker attempts to make use of the SAS system in an unauthorised way.

  The SAS system implementation should provide protections against illegitimate use. Access to the SAS system should be restricted by authorization validation during association establishment at a minimum. This validation should occur at the application level of the SAS communication profile and should support the concept of association access privileges.

  As a minimum, the privileges that need to be supported are:

  1) NO PRIVILEGE – this privilege indicates that the association is not validated to be allowed for even the most rudimentary access to the SAS system. This privilege is really a non-privilege and should result in the association being terminated non-gracefully. However, termination of the association does not allow SAS systems to indicate that an attack has occurred.

     In order to allow supervisory systems to detect such an intrusion, the SAS system should keep track of the number of associations that were terminated due to NO PRIVILEGE being detected.

     In order to allow prosecution/repudiation of the attacker, the SAS system should make a strong effort to record any relevant communication addressing information of the attacker. If the SAS resources allow this information to be recorded, the system should also allow retrieval of this information.

  2) MONITOR – this privilege indicates that the association is validated to be allowed to monitor (for example read) attributes/values from the SAS system. However, the association is not authorized to be able to perform any action that affects the operation of the SAS (for example CONTROL or configuration changes).

  3) CONTROL – this privilege indicates that the association is validated to be allowed to control the operation of the SAS system. This privilege should always be granted in conjunction with MONITOR. However, this privilege does not allow the association to make configuration changes.

  4) CONFIG – this privilege indicates that the association is validated to be allowed to make configuration changes of the SAS system. This privilege should always be granted in conjunction with MONITOR.

  5) SECURITY ADMIN – this privilege indicates that the association is validated to be allowed to change/retrieve security related attributes/values/configurations.

  Other privilege levels may be allowed and are not within the scope of this standard.

  The implementation of the privilege levels and their degree of granularity is an implementation issue and is not within the scope of this standard.

  There are several other threats that should be considered during the implementation of the SAS. However, these are not within the scope of this standard.

_____

Standards Survey

The IEC would like to offer you the best quality standards possible. To make sure that we continue to meet your needs, your feedback is essential. Would you please take a minute to answer the questions overleaf and fax them to us at +41 22 919 03 00 or mail them to the address below. Thank you!

Customer Service Centre (CSC)

International Electrotechnical Commission
3, rue de Varembé
1211 Genève 20
Switzerland

or

Fax to: **IEC**/CSC at +41 22 919 03 00

Thank you for your contribution to the standards-making process.

A Prioritaire

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

RÉPONSE PAYÉE

SUISSE

Customer Service Centre (CSC)
International Electrotechnical Commission
3, rue de Varembé
1211 GENEVA 20
Switzerland

Q1 Please report on **ONE STANDARD** and **ONE STANDARD ONLY**. Enter the exact number of the standard: *(e.g. 60601-1-1)*

.....

Q2 Please tell us in what capacity(ies) you bought the standard *(tick all that apply).* I am the/a:

purchasing agent ❑
librarian ❑
researcher ❑
design engineer ❑
safety engineer ❑
testing engineer ❑
marketing specialist ❑
other.....

Q3 I work for/in/as a: *(tick all that apply)*

manufacturing ❑
consultant ❑
government ❑
test/certification facility ❑
public utility ❑
education ❑
military ❑
other.....

Q4 This standard will be used for: *(tick all that apply)*

general reference ❑
product research ❑
product design/development ❑
specifications ❑
tenders ❑
quality assessment ❑
certification ❑
technical documentation ❑
thesis ❑
manufacturing ❑
other.....

Q5 This standard meets my needs: *(tick one)*

not at all ❑
nearly ❑
fairly well ❑
exactly ❑

Q6 If you ticked NOT AT ALL in Question 5 the reason is: *(tick all that apply)*

standard is out of date ❑
standard is incomplete ❑
standard is too academic ❑
standard is too superficial ❑
title is misleading ❑
I made the wrong choice ❑
other .....

Q7 Please assess the standard in the following categories, using the numbers:
(1) unacceptable,
(2) below average,
(3) average,
(4) above average,
(5) exceptional,
(6) not applicable

timeliness.....
quality of writing.....
technical contents.....
logic of arrangement of contents .....
tables, charts, graphs, figures.....
other .....

Q8 I read/use the: *(tick one)*

French text only ❑
English text only ❑
both English and French texts ❑

Q9 Please share any comment on any aspect of the IEC that you would like us to know:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

ISBN 2-8318-6147-0

ICS 33.200

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND