PD IEC/TS 62603-1:2014

BSI Standards Publication

Industrial process control systems — Guidelines for process control systems

Part 1: Specifications

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of IEC/TS 62603-1:2014.

The UK participation in its preparation was entrusted by Technical Committee GEL/65, Measurement and control, to Subcommittee GEL/65/2, Elements of systems.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2014

ISBN 978 0 580 85539 9
ICS 25.040.40

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 June 2014.

Amendments/corrigenda issued since publication

Date	Text affected

IEC TS 62603-1

Edition 1.0 2014-05

TECHNICAL SPECIFICATION

colour inside

Industrial process control systems – Guideline for evaluating process control systems –
Part 1: Specifications

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE XE

ICS 25.040.40

ISBN 978-2-8322-1623-1

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL PROCESS CONTROL SYSTEMS – GUIDELINE FOR EVALUATING PROCESS CONTROL SYSTEMS –

Part 1: Specifications

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). 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 organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of 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 IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC TS 62603-1, which is a technical specification, has been prepared by subcommittee 65B: Measurement and control devices, of IEC technical committee 65: Industrial-process measurement, control and automation.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
65B/875/DTS	65B/905/RVC

Full information on the voting for the approval of this technical specification 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 2.

A list of all parts in the IEC 62603 series, published under the general title *Industrial process control systems – Guideline for evaluating process control systems*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- transformed into an International standard,
- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This International Technical Specification defines a procedure for verifying if a given Process Control System (PCS) satisfies the technical requirements specified by the end-user or by an engineering company for a specific application. The basic concept of this document is that “you can test what you have specified”. A testing procedure is meaningless if it does not include a procedure for specifying the technical requirements to be tested.

This Technical Specification was developed in the framework of the existing standards that define the general concepts of PCS design and testing, that is:

IEC 61069 Industrial process measurement and control – Evaluation of system properties for the purpose of system assessment – Parts 1,2,3,4,5,6,7,8

IEC 62381 Automation systems in the process industry – Factory acceptance test (FAT), site acceptance test (SAT), and site integration test (SIT)

The group of standards 61069 defines the general methodology, definitions, and procedures for assessing the functional characteristics of a PCS (Part 1 and 2) in terms of functionalities (Part 3), performances (Part 4), dependability (Part 5), operability (Part 6), safety (Part 7), and non-task-related properties (Part 8). IEC 62381 gives additional details about the general procedures for testing a PCS in factory, on site, and after the general integration of the complete system.

The IEC 62603 fully complies with these standards and gives a detailed guidance for specifying a PCS and for testing the specified functions. IEC 61069 and 62381 create a framework that is valid for any PCS as a system, while 62603, inside this framework, gives the users guidance for specifying the PCS he needs for carrying out the required functions.

INDUSTRIAL PROCESS CONTROL SYSTEMS – GUIDELINE FOR EVALUATING PROCESS CONTROL SYSTEMS –

Part 1: Specifications

1 Scope

This International Technical Specification describes methods and provides guidance for the evaluation of Process Control Systems (PCS) during the phase of selection between different proposals.

The methods of evaluation proposed in this technical specification are intended for use mainly by users, engineering companies, or independent test laboratories, to verify manufacturers' proposals during the tender (as described in IEC 62603-1) or the provided Process Control System during the FAT procedure.

The specification and test procedures specified in this technical specification apply to a large variety of automation systems, both based on conventional technology (e.g. 4 mA to 20 mA field devices) and based on Intelligent Field Devices (IFD) with serial communication of any kind. For this reason, the tests specified in this technical specification are not necessarily sufficient for automation systems specifically designed for special duties. In such cases, user and manufacturer should define additional tests for assessing specific functions or performances.

The procedure for specifying the PCS technical requirements, evaluating the different offers, and carrying out the tests on the chosen PCS differs from one company to another and from one project to another, but some common steps exist, as Figure 1 shows. The IEC 62603 considers this process divided into two steps: definition of the PCS technical requirements (in the scope of IEC 62603-1) and test of the chosen PCS.

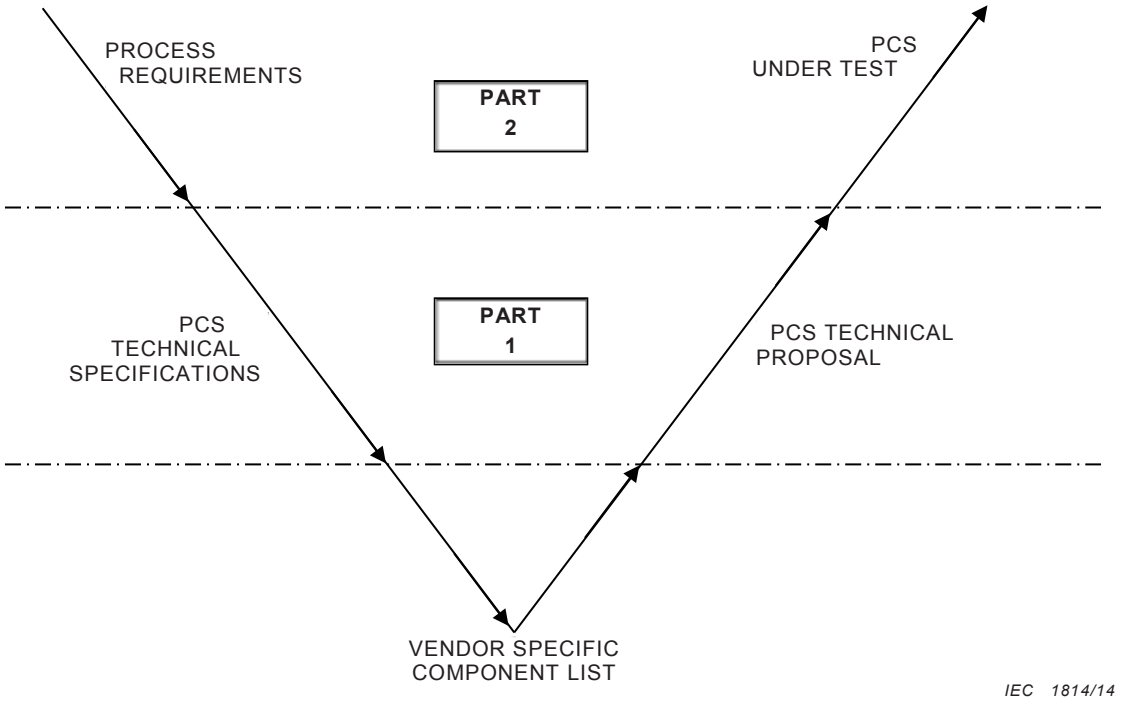

Figure 1 – Procedure for specifying and testing a PCS

The first step of the specification of a PCS is to define the process requirements, in terms of required performances to achieve a satisfactory control of the process. Normally these requirements are defined with a joint effort of process engineers, automation, and instrumentation experts. From the process requirements, the automation engineers derive the PCS technical requirements, that is the functionalities the PCS should offer to achieve the required goals. Based on the process requirements and the PCS technical requirements, suppliers prepare their technical offers, and the evaluation procedure starts. IEC 62603-1 suggests a possible procedure for assessing the fitness of a proposed PCS to the specifications, based on a simple algorithm that considers the weight (importance) of each single required function.

After the selection of the PCS maker, the implementation stage starts. When the PCS is ready, prior to shipping the PCS on site and sometimes even during the implementation stage, the user/engineer may perform a set of Factory Acceptance Tests.

The technical evaluation of the tenders (IEC 62603-1) is mostly based on the evaluation of documents and data-sheets, and it may require simple calculations, e.g. for performance calculation. These verifications are based on general data of the proposed automation systems, not dedicated to any specific piece of hardware of software.

On the contrary, the FAT is mostly based on testing activities in laboratories or factories on a specific PCS including both the physical devices and the application software.

Figure 2 shows the typical process of PCS evaluation in an automation project.

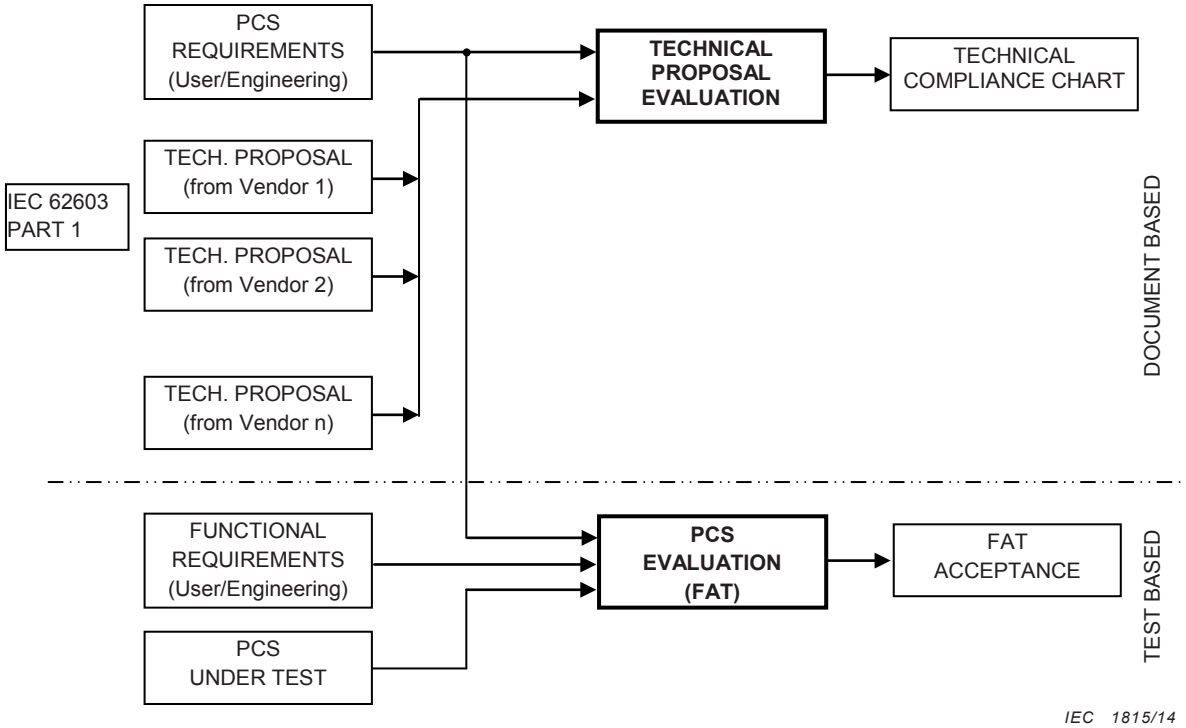

Figure 2 – The process of PCS evaluation

The first evaluation is needed to select one supplier from a number of proposals. The reference document is the PCS technical requirements provided by the user or by a delegated engineering company. Scope of the evaluation at this stage is to verify if the proposed systems support the specified functions and performances. Evaluation is mostly based on the documents supplied by the supplier, such as technical data-sheets, manuals, conformity declarations, and so on. The PCS technical requirements should include the description of the required FAT procedure.

After the supplier's selection, the detailed engineering stage starts, and the user (or the delegated engineering company) produces a document that describes the software requirements in details. The PCS supplier assembles the PCS and implements the logic. After the completion of in-house tests, the Factory Acceptance Tests starts.

Several aspects of process control systems are in the scope of existing IEC standards that are to be considered together with the present document. This technical specification reports abstracts of the cited IEC standards based on the revisions available at the date of submission. Users should consult the most recent versions of the referenced standards for the actual requirements.

2 Normative references

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

IEC 60038:2009, *IEC standard voltages*

IEC 60050 (all parts), *International Electrotechnical Vocabulary* (available at <http://www.electropedia.org>)

IEC 60079-10, *Electrical apparatus for explosive gas atmospheres – Part 10: Classification of hazardous areas*[1]

IEC 60079-10-1, *Explosive atmospheres – Part 10-1: Classification of areas – Explosive gas atmospheres*

IEC 60079-10-2, *Explosive atmospheres – Part 10-2: Classification of areas – Combustible dust atmospheres*

IEC 60079-11, *Explosive atmospheres – Part 11: Equipment protection by intrinsic safety "i"*

IEC 60079-14, *Explosive atmospheres – Part 14: Electrical installations design, selection and erection*

IEC 60300-3-4, *Dependability management – Part 3-4: Application guide – Guide to the specification of dependability requirements*

IEC 60654-1, *Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions*

IEC 60654-2, *Operating conditions for industrial-process measurement and control equipment – Part 2: Power*

IEC 60654-3, *Operating conditions for industrial-process measurement and control equipment – Part 3: Mechanical influences*

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

IEC 60721-3-1, *Classification of environmental conditions – Part 3: Classification of groups of environmental parameters and their severities – Section 1: Storage*

IEC 60721-3-2, *Classification of environmental conditions – Part 3: Classification of groups of environmental parameters and their severities – Section 2: Transportation*

IEC 60721-3-3, *Classification of environmental conditions – Part 3-3: Classification of groups of environmental parameters and their severities – Stationary use at weatherprotected locations*

[1] Withdrawn.

IEC 60721-3-4, *Classification of environmental conditions – Part 3: Classification of groups of environmental parameters and their severities – Section 4: Stationary use at non-weatherprotected locations*

IEC 60848, *GRAFCET specification language for sequential function charts*

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

IEC 61000-4-2, *Electromagnetic compatibility (EMC) – Part 4-2: Testing and measurement techniques – Electrostatic discharge immunity test*

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

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

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

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

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

IEC 61000-4-9, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 9: Pulse magnetic field immunity test. Basic EMC Publication*

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

IEC 61000-4-11, *Electromagnetic compatibility (EMC) – Part 4-11: Testing and measurement techniques – Voltage dips, short interruptions and voltage variations immunity tests*

IEC 61000-6-4, *Electromagnetic compatibility (EMC) – Part 6-4: Generic standards – Emission standard for industrial environments*

IEC 61025, *Fault tree analysis (FTA)*

IEC 61069-1, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 1: General considerations and methodology*

IEC 61069-4, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 4: Assessment of system performance*

IEC 61069-5, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 5: Assessment of system dependability*

IEC 61069-6, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 6: Assessment of system operability*

IEC 61069-7, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 7: Assessment of system safety*

IEC 61069-8, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 8: Assessment of non-task-related system properties*

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

IEC 61131-2, *Programmable controllers – Part 2: Equipment requirements and tests*

IEC 61131-3, *Programmable controllers – Part 3: Programming languages*

IEC 61140*, Protection against electric shock – Common aspects for installation and equipment*

IEC 61158 (all parts), *Industrial communication networks – Fieldbus specifications*

IEC 61158-2, *Industrial communication networks – Fieldbus specifications – Part 2: Physical layer specification and service definition*

IEC 61326-1, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 1: General requirements*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

IEC 61512 (all parts), *Batch control*

IEC 61784 (all parts), *Industrial communication networks – Profiles*

IEC 62305-1, *Protection against lightning – Part 1: General principles*

IEC TR 62380, *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment*

IEC 62381, *Automation systems in the process industry – Factory acceptance test (FAT), site acceptance test (SAT), site integration test (SIT)*

IEC 62347, *Guidance on system dependability specifications*

IEC 62443-2-1, *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*

IEC 62443-3-3,*Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

ISO/IEC 14764:2006, *Software Engineering – Software Life Cycle Processes – Maintenance*

IEEE 802 (all parts), *IEEE Standards for Local and Metropolitan Area Networks*

ISA 18.1-1979 (R1992), *Annunciator sequences and specifications*

ISA 18.2-2009, *Management of alarm systems for the process industries*

ISA 37.1-1975 (R1982), *Electrical transducer nomenclature and terminology*

ISA S88 (all parts), *Batch Control*

3 Symbols and abbreviated terms

ADC	Analog-to-Digital Converter
BMS	Burner Management System
BPCS	Basic Process Control System
CFC	Continuous Function Chart
CR	Control Room
CT	Counter
DCS	Distributed Control System
EMC	ElectroMagnetic Compatibility
EFT/B	Electric Fast Transient / Burst
ERP	Enterprise Resource Planning
ESD	Emergency Shut-Down
FAT	Factory Acceptance Test
FBD	Function Block Diagram
F&G	Fire and Gas
HMI	Human Machine Interface
KPI	Key Performance Indicator
IFD	Intelligent Field Device
IIS	Internet Information Server
ICT	Information Communication Technology
ISM	Industrial Scientific and Medical
IPC	In-plant Point of Coupling
LD	Ladder Diagram
LOI	Local Operator Interface
LPZ	Lightning Protection Zone
MES	Manufacturing Execution System
OLE	Object Linking and Embedding
OPC	OLE for Process Control
OS	Operator Station
PAM	Plant Asset Management
PFD	Probability of Failure on Demand
PFH	Average Probability of Failure per Hour

PLC	Programmable Logic Controller
PCS	Process Control System
PCU	Process Control Unit
PCC	Point of Common Coupling
RF	Radio Frequency
SAT	Site Acceptance Test
SCADA	Supervisory, Control, And Data Acquisition
SELV	Safety Extra Low Voltage
SFC	Sequential Function Chart
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SIT	Site Integration Test
SLA	Service Level Agreement
SLC	Single Loop Controller
SOE	Sequence Of Events
SSL	Secure Socket Layers
VBA	Visual Basic for Applications

4 Technical specifications of a PCS

For the technical evaluation of a Process Control System, it is necessary that the Technical specification of the required PCS include a clear list of requirements to check-out. For the sake of simplicity, it is useful to split the technical requirements into homogeneous groups, each one containing a set of specific items. An example of a possible structure of the technical requirements is shown in Figure 3. The itemised content of each group is described in the subclauses of this technical specification reported in Figure 3. Application software specifications are not included in the general PCS technical requirements since they do not impact on the selection of the PCS.

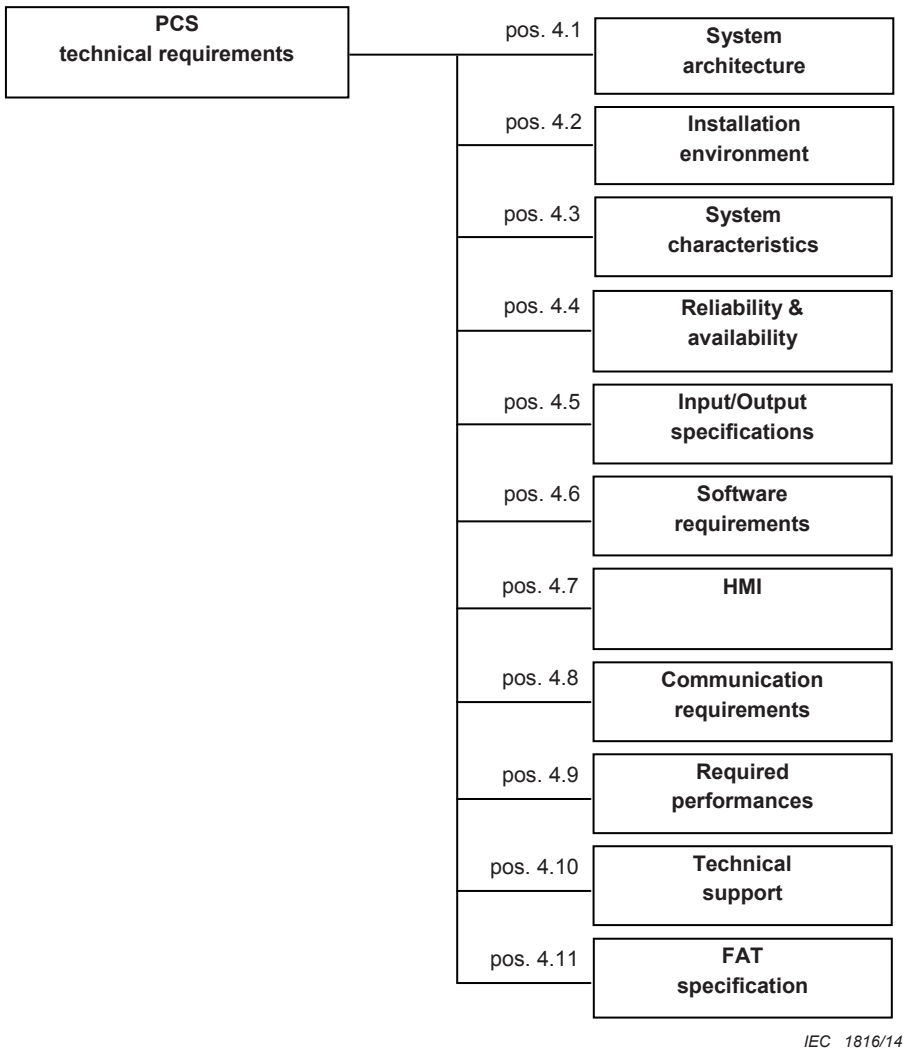

Figure 3 – Content of the PCS technical specifications

The end-user or the delegated engineering company indicates the required functions and performances of the PCS, and checks if the proposed system fulfils the requirements. This phase can be accelerated if requirements are presented in table form in a spreadsheet with boxes where the supplier can write down his answers.

The process of evaluating a proposal can become quantitative if a voting system is defined. A voting system is very useful for comparing different proposals. To do this, a weight should be assigned to each requirement. Weights can vary from one application to another, and they can be defined according to a heuristic scale such as:

- the function is ***optional*** weight D
- the function ***would help*** weight C
- the function ***should*** be implemented weight B
- the function ***shall*** be implemented weight A

Similarly, the suitability of the proposed PCS for each requirement can be rated according to the following scale:

– the PCS ***does not meet*** the function vote 0
– the PCS does not meet the function, but ***it can be applied or created*** vote 1
– the PCS ***meets the function*** vote 2
– the PCS ***meets the function and is clearly stated*** vote 3

Proposals may not state whether specific specification requirements are met or not. In such cases, the evaluator should use judgment whether to

- attribute a rating (vote) based on the evaluator's own knowledge, experience and judgment, possibly reducing the vote by 1 to make an allowance for uncertainty, or
- seek additional specific information from the supplier.

Votes of all the offers are summarised in a table that shows each technical requirement, its weight (A-B-C-D), and vote (0-1-2-3). The proposal of each supplier has its column (see Table 1).

Table 1 – Summary table for proposal evaluation

Technical requirement	Weight	Bid #1	Bid #2	Bid #3
Item #1	w_1	v_{11}	v_{21}	v_{31}
Item #2	w_2	v_{12}	v_{22}	v_{32}
.....	...	...	...	...
Item #n	w_n	v_{1n}	v_{23}	v_{33}

Of course, the function weight and the PCS votes are derived from the specific process category to which the plant belongs. For example, the same PCS may fulfil some requirements for a manufacturing plant, but it may not be adequate for a chemical plant, and so on.

For considering a proposal acceptable, all the functions with weight A and B should have a vote not lower than 2. Proposals receiving a vote of 1 for a function with an A or B weight can be made acceptable through including the means of getting the function applied or created (e.g. additional cost) included in the evaluation.

For defining a global proposal vote, first a numerical value should be assigned to weights and votes, then the average vote can be calculated with Equation (1):

$$Bid_k\ value = \frac{\sum_{i=1}^{n}(w_i \cdot v_{ki})}{\sum_{i=1}^{n}(w_i)} \quad (1)$$

where

– n is the number of functions;
– w_i is the i-th function weight;
– v_{ki} is the vote of proposal "k" for the i-th function.

A simplified example of a proposal vote calculation is shown in Table 2, where a set of typical values for weights and votes is selected. Three imaginary proposals are compared on the base of the respective votes for ten generic functions. Obviously, different numerical values of weights and votes can lead to different global votes, even if with reasonable choices the ranking is likely to remain unaffected.

In the following subclauses, a list of requirements is reported as a base for PCS evaluation. Users have the possibility either of removing requirements not applicable to the specific application or to add special requirements not listed here.

Table 2 – Example of proposal global vote calculation

WEIGHT	
A	8
B	4
C	2
D	1

VOTE	
3	10
2	8
1	4
0	0

FUNCTION	WEIGHT		BID 1		BID 2		BID 3	
1	3	8	3	80	2	64	3	80
2	3	8	3	80	3	80	2	64
3	2	4	2	32	3	40	3	40
4	0	1	2	8	2	8	1	4
5	1	2	1	8	3	20	1	8
6	2	4	3	40	2	32	2	32
7	2	4	3	40	1	16	3	40
8	3	8	1	32	2	64	3	80
9	1	2	3	20	3	20	3	20
10	2	4	2	32	2	32	2	32
	Σw	45	8,27		8,36		8,89	

4.1 System architecture

4.1.1 General

This subclause describes the general characteristics of the PCS, namely the physical structure and the preliminary sizing of the components. The scope of this subclause is to identify the general characteristics of the desired PCS, the fundamental technologies, the topology of the system and its size. Non-programmable technologies for PCSs, such as hard-wired, non-programmable electronics and single-loop controllers (SLC) are not covered by this document.

The user/engineer should specify the system architecture in accordance with the technical definitions of the following subclauses. Annex A may be used as a guidance.

4.1.2 Technology and scope of the PCS

According to today's terminology, the available technologies for PCSs can be selected amongst:

– PLC based;
– Soft PLC based;
– DCS;
– SCADA;
– others (to be specified).

The basic function or functions of the required PCS are selected amongst one or more of the following choices:

– supervisory;
– control;
– protection, including interlocking, trips and ESD;
– batch;
– others (to be specified).

4.1.3 Basic architecture

User/engineer normally show the requested PCS topology in a drawing attached to the technical specification, where all the main components are indicated and named. In case of complex systems, the drawing can be split into several sheets: outline, subsystems, control room layout, etc. Figure 4 shows an example of a layout for a medium-size PCS. The supplier can propose modifications to the PCS architecture in his technical proposal.

This Guideline assists the user in defining the user requirements for the components of the PCS, from field devices to the control room, and the requirements of the interfaces for connecting the PCS to other digital and communication systems of the factory, e.g. ICT, not in the scope of this document.

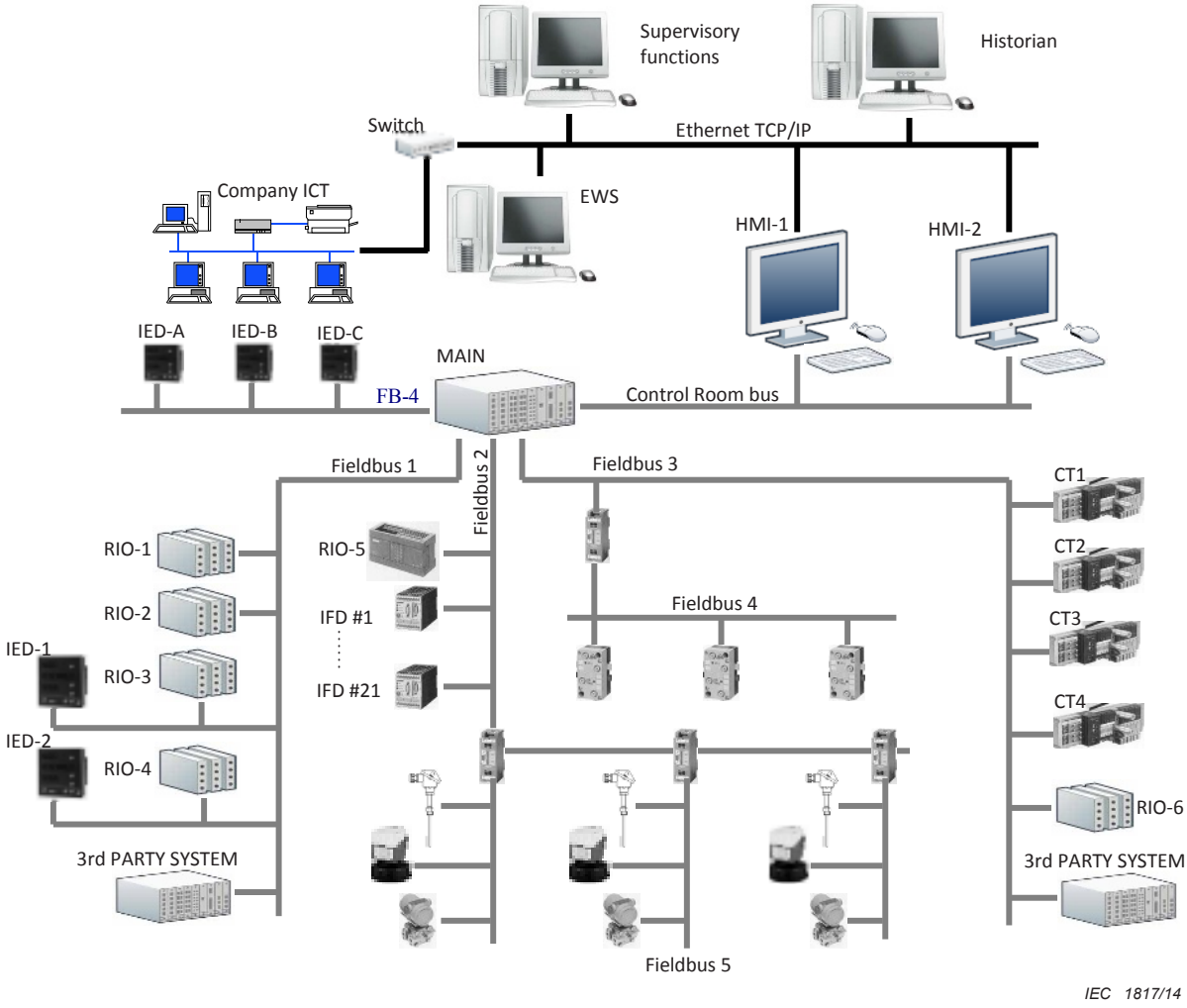

Figure 4 – Example of a layout drawing

4.1.4 Total number of I/Os

The total number of estimated I/Os is generally used to define the overall size of the PCS. Physical I/Os are divided into the conventional analogue/digital input/output. If a serial communication technology is required, the total number of intelligent devices and/or remote input/output devices connected to the PCS is indicated as well. The user should specify the estimated number of I/Os for the various categories.

4.1.5 Number of tags

A tag indicates an elementary piece of information used or produced by the PCS. Tags are often grouped into Process Objects (transmitters, valves, circuit breakers, etc.) and divided into two categories:

– tags for process control: a limited set of information or commands necessary for process control. For example, the process object “valve” may include the following tags: valve position, open/close status, set point;

– tags for additional functions, such as device remote setting, diagnostic, alarm setting, etc. These functions are possible only with intelligent devices connected through serial communications, and the relevant number of tags may become very high.

The user should specify:

- the tag naming scheme;

- requirements on length of tags;
- all classes of data which require to be tagged.

4.1.6 Number of control loops

A control loop is based on the use of a software controller with PID functions or similar. The total number of loops gives an idea of the complexity of the system, mainly in terms of software performances. The system should be able to handle the total amount of control loops within the specified time requirements. Advanced controls of special control functions are not to be accounted at this point.

The user should specify the estimated number of control loops to handle and the required time cycle.

4.1.7 Reference standards and marking

Local laws or rules, corporate policies or industry sector definitions of good practice may require specific marking or certification of the electrical devices composing the PCS, mainly for safety reasons. Special standards may be requested for the specific application, e.g., marine installation, nuclear plants, oil and gas, etc.

4.2 Installation environment

4.2.1 General

This subclause describes the general characteristics of the environment in which the PCS and its components are installed. The user/engineer should specify the installation environment in accordance with the technical definitions of the following subclauses. Annex B may be used as a guidance.

The operating conditions for the PCS components are divided into four main categories, according to the classification made by the IEC 60654 family of standards:

- the climatic conditions of the location in which the components are installed (e.g., temperature, humidity, etc.);
- the power supply to which the components are connected: electrical specification of the power supply and the EMC requirements in terms of immunity and emission;
- mechanical influences to which the components are exposed during their operation (e.g., vibration, shock, etc.);
- corrosive and erosive influences to which the components are exposed during their operation (e.g., sand, gases, corrosive liquids, etc.).

4.2.2 Climatic conditions

Considered climatic conditions are air temperature, humidity and barometric pressure in the specific location where the system and its components are installed. Location classes are classified into four severity levels that define the expected climatic conditions of the site. Location classes apply for operation, storage and transportation. Specific classes may apply for storage and transportation as stated in IEC 60721-3-1 and in IEC 60721-3-2.

Location classes are:

- ***Class A***: weather-protected locations, air-conditioned locations. In these locations, both air temperature and humidity are controlled within specified limits;
- ***Class B***: weather-protected locations, heated and/or cooled enclosed locations. In these locations, only air temperature is controlled within specified limits;
- ***Class C***: weather-protected locations, sheltered and/or unheated enclosed locations. In these locations, neither air temperature nor humidity is controlled and equipment is

protected against direct exposure to such climatic elements as direct solar radiation, rainfall, full wind pressure, etc.

- ***Class D***: non weather-protected locations, outdoor locations. In these locations, neither air temperature nor humidity are controlled and the equipment is exposed to atmospheric conditions such as direct solar radiation, rainfall, full wind pressure, etc.

Table 3 is extracted from IEC 60654-1:1993, and reports the limit values of the climatic conditions for each location class.

Table 3 – Climatic condition parameters and severities for classes of location

Environmental parameter	Unit	Class of location (Notations in brackets are climatic classes of IEC 60721-3-1, IEC 60721-3-3 and IEC 60721-3-4)												
		A1[a] (3K1) /	Ax[b] / /	B1 (3K2) /	B2 (3K3) (1K2)	B3 (3K4) /	Bx[b] / /	C1 (3K5) (1K3)	C2 (3K6) /	C3 (3K7) (1K5)	Cx[b] / /	D1 (4K2) (1K8)	D2 (4K3) /	Dx2) / /
Low air temperature	°C	+20		+15	+5	+5		-5	-25	-40		-33	-50	
High air temperature	°C	+25		+30	+40	+40		+45	+55	+70		+40	+40	
Low relative humidity	%	20		10	5	5		5	10	10		15	15	
High relative humidity	%	75		75	85	95		95	100	100		100	100	
Low absolute humidity	g/m^3	4		2	1	1		1	0,5	0,1		0,26	0,03	
High absolute humidity	g/m^3	15		22	25	29		29	29	35		25	36	
Solar radiation	W/m^2	500		700	700	700		700	1 120	1 120		1 120	1 120	
Rate of change of temperature[c]	°C/min	0,1		0,5	0,5	0,5		0,5	0,5	0,1		0,5	0,5	
Condensation		No		No	No	Yes		Yes	Yes	Yes		Yes	Yes	
Wind-driven precipitation (rain, snow, hail, etc.)		No		No	No	No		No	Yes	Yes		Yes	Yes	
Formation of ice		No		No	No	No		Yes	Yes	Yes		Yes	Yes	
Low air pressure	kPa	86[d]		86[d]	86[d]	86[d]		86[d]	86[d]	86[d]		86[d]	86[d]	
High air pressure		106		106	106	106		106	106	106		106	106	

a Tolerance of ± 2 °C on stated temperature values.

b For "special" classes Ax, Bx, Cx e Dx, values should be selected from IEC 60721-3-1, IEC 60721-3-2, IEC 60721-3-3 and IEC 60721-3-4.

c To be considered when significant.

d 70 kPa for high altitude and/or transportation.

For each location class A,B,C, or D several levels are defined (e.g., B1, B2, C1, C2, etc.) according to different values of the environmental parameters defining the class of location.

4.2.3 Power supply

4.2.3.1 AC power supply

4.2.3.1.1 General

The values of the nominal voltages of the power supply are in accordance with the requirements of IEC 60038. The allowed frequencies are 50 Hz and 60 Hz and the nominal voltages applicable to PCSs are:

- 120/240 V for single phase systems (60 Hz);
- 230/400 V for three phase systems (50 Hz);
- 277/480 V for three phase systems (60 Hz).

If required, the power supply distribution of the PCS may internally generate different voltages to feed devices or assemblies (i.e., 110 V, 50 Hz).

The AC power supply characteristics are: voltage, frequency, harmonic distortion and switching time between alternative power supplies. As indicated in the following subclauses, IEC 60654-2:1979 defines a set of different classes for each characteristic.

4.2.3.1.2 AC power voltage classes

Power voltages are classified in accordance with the percentage of variation of the voltage from its nominal value. Four classes are defined:

- Class AC1: ± 1 % V_{nom};
- Class AC2: ± 10 % V_{nom};
- Class AC3: from 10 % V_{nom} to –15 % V_{nom};
- Class AC4: from 15 % V_{nom} to –20 % V_{nom}.

A special class exists for the cases where the power supply voltages are not included in the requirements of the above listed classes.

4.2.3.1.3 AC power frequency classes

The frequency variation is stated as a percent deviation from the nominal frequency vale. Three classes are defined:

- Class F1: ± 0,2 % F_{nom};
- Class F2: ± 1 % F_{nom};
- Class F3: ± 5 % F_{nom}.

A special class exists for the cases where the power supply frequency is not included in the requirements of the above listed classes.

4.2.3.1.4 Harmonic content

The total harmonic distortion is defined as the percentage of the square root of the sum of square the harmonic voltages divided by the fundamental power supply frequency voltage (r.m.s.), as reported in formula [1].

$$THD = \frac{\sqrt{\sum_{h=2}^{h=10} V_h^2}}{V_{1N}} \qquad [1]$$

where

h is the harmonic order;

V_k is the RMS value of the voltage harmonic component of order h;

V_{1N} is the RMS value of the fundamental voltage component.

Four classes are defined:

H1: harmonic content is less than 2 %;

H2: harmonic content is less than 5 %;

H3: harmonic content is less than 10 %;

H4: harmonic content is less than 20 %.

A special class exists for all the cases where the harmonic content is not included in the above listed classes.

4.2.3.1.5 Switching time

For a system with alternative power supplies (i.e., main and back-up), switching time is the time interval between the deviation of voltage in the primary supply that initiates switching, and the restoration of normal voltage by the auxiliary supply. After the switching time, the voltage has to be within the limit values for the specified class of power. The value of deviation required to initiate switching is, in general, a characteristic of the switching system.

Five classes for the switching time are defined:

ST1: switching time less than 3 ms;

ST2: switching time less than 10 ms;

ST3: switching time less than 20 ms;

ST4: switching time less than 200 ms;

ST5: switching time less than 1 s.

A special class exists for all the case where the switching time is not included in the above listed classes.

4.2.3.2 DC power supply

4.2.3.2.1 General

In accordance with the requirements of IEC 60038 the values of the nominal voltages of the DC power supply are: 12 / 48 / 110 / 220 V.

If required, the power supply distribution of the PCS may internally generate different voltages to feed devices or assemblies (i.e., 24 V).

The DC power supply characteristics are: voltage, ripple and switching time between the power supply failure and an auxiliary power supply taking over. As indicated in the following subclauses, IEC 60654-2:1979 defines a set of different classes for each characteristic.

4.2.3.2.2 DC power voltage classes

DC power voltages are classified by their percent variation of the voltage from the nominal value. Four classes are defined:

DC1: ± 1 % V_{nom};

DC2: from 10 % V_{nom} to –15 % V_{nom};

DC3: from 15 % V_{nom} to –20 % V_{nom};

DC4: from 30 % V_{nom} to –25 % V_{nom}.

A special class exists for all the cases where the voltage variations are not included in the above listed classes.

4.2.3.2.3 DC power voltage ripple classes

Ripple voltage is defined as the percentage of the peak-to-peak value of the total AC component of the power supply voltage to the measured (average) power supply voltage, as measured at rated load. Four classes are defined:

DC1: ripple voltage less than 0,2 %;

DC2: ripple voltage less than 1 %;

DC3: ripple voltage less than 5 %;

DC4: ripple voltage less than 15 %.

A special class exists for all the cases where the power supply ripple is not included in the above listed classes.

4.2.3.2.4 Switching time

For a system with an auxiliary or back-up power supply, switching time is the time interval between the deviation of voltage in the primary supply, which initiates switching, and the restoration of normal voltage by the auxiliary supply. After the switching time, the voltage has to be within the limit values for the specified class of power.

Five classes for the switching time are defined:

STDC1: switching time less than 1 ms;

STDC2: switching time less than 5 ms;

STDC3: switching time less than 20 ms;

STDC4: switching time less than 200 ms;

STDC5: switching time less than 1 s.

A special class exists for all the cases where the switching time that is not included in the above listed classes.

4.2.3.2.5 Earth connection

One of the following three possibilities for grounding DC power supply should be specified:

a) positive to earth;

b) negative to earth;

c) floating.

4.2.4 EMC requirements

4.2.4.1 General

The requirements for immunity and emission levels regarding electromagnetic compatibility (EMC) are referred to electrical equipment operating with a voltage level lower than 1 000 V a.c. or 1 500 V d.c.

4.2.4.2 Immunity

The general performance criteria for the evaluation of the immunity of the devices are as listed below:

Class A normal operation, within the specification limits, during the exposure to the EM disturbance

Class B during the EM exposure temporary degradation, or loss of function or performance which is self-recovering

Class C during the EM exposure temporary degradation, or loss of function or performance which requires operator intervention or system reset

The performance criteria should be applied to each single disturbance to which the device can be exposed. The limit values for every disturbance are reported in the next subclauses.

The base immunity requirements for a generic application are given in Table 4 extracted from IEC 61326-1:2005.

Particular immunity requirements for equipment intended for use in industrial locations are reported in Table 5 (from IEC 61326-1:2005).

Table 4 – Base immunity requirements

Port	Phenomenon	Basic standard	Test value	Performance criteria
Enclosure	Electrostatic discharge (ESD)	IEC 61000-4-2	4 kV/4 kV contact/air	B
	EM field	IEC 61000-4-3	3 V/m (80 MHz to 1 GHz) 3 V/m (1,4 GHz to 2 GHz) 1 V/m (2,0 GHz to 2,7 GHz)	A
AC power (including protective earth)	Voltage dip	IEC 61000-4-11	0 % during half cycle 0 % during 1 cycle 70 % during 25/30[e] cycles	B B C
	Short interruptions	IEC 61000-4-11	0 % during 250/300[e] cycles	C
	Burst	IEC 61000-4-4	1 kV (5/50 ns, 5 kHz)	B
	Surge	IEC 61000-4-5	0,5 kV[a]/1 kV[b]	B
	Conducted RF	IEC 61000-4-6	3 V (150 kHz to 80 MHz)	A
DC power[d] (including protective earth)	Burst	IEC 61000-4-4	1 kV(5/50 ns, 5 kHz)	B
	Surge	IEC 61000-4-5	0,5 kV[a]/1 kV[b]	B
	Conducted RF	IEC 61000-4-6	3 V (150 kHz to 80 MHz)	A
I/O signal/control (including lines connected to functional earth port)	Burst	IEC 61000-4-4	0,5 kV[d](5/50 ns, 5 kHz)	B
	Surge	IEC 61000-4-5	1 kV[b, c]	B
	Conducted RF	IEC 61000-4-6	3 V[d] (150 kHz to 80 MHz)	A
I/O signal/control connected directly to mains supply	Burst	IEC 61000-4-4	1 kV(5/50 ns, 5 kHz)	B
	Surge	IEC 61000-4-5	0,5 kV[a]/1 kV[b]	B
	Conducted RF	IEC 61000-4-6	3 V (150 kHz to 80 MHz)	A

a Line to line.

b Line to earth (ground).

c Only in the case of long-distance lines.

d Only in the case of lines >3 m.

e “25/30 cycles" means "25 cycles for 50 Hz test" and "30 cycles for 60 Hz test.

Table 5 – Immunity requirements for industrial applications

Port	Phenomenon	Basic standard	Test value	Performance criteria
Enclosure	Electrostatic discharge (ESD)	IEC 61000-4-2	4 kV/8 kV contact/air	B
	EM field	IEC 61000-4-3	10 V/m (80 MHz to 1 GHz) 3 V/m (1,4 GHz to 2 GHz) 1 V/m (2,0 GHz to 2,7 GHz)	A
	Rated power frequency magnetic field	IEC 61000-4-8	30 A/m[e]	A
AC power	Voltage dip	IEC 61000-4-11	0 % during 1 cycle 40 % during 10/12[h] cycles 70 % during 25/30 [h] cycles	B C C
	Short interruptions	IEC 61000-4-11	0 % during 250/300 [h] cycles	C
	Burst	IEC 61000-4-4	2 kV(5 kHz)	B
	Surge	IEC 61000-4-5	1 kV[a]/2 kV[b] (1,2/50 μs)	B
	Conducted RF	IEC 61000-4-6	3 V[f] (150 kHz to 80 MHz)	A
DC power[g]	Burst	IEC 61000-4-4	2 kV (5 kHz)	B
	Surge	IEC 61000-4-5	1 kV[a]/2 kV[b] (,12/50 μs)	B
	Conducted RF	IEC 61000-4-6	3 V[f] (150 kHz to 80 MHz)	A
I/O signal/ control (including functional earth lines)	Burst	IEC 61000-4-4	1 kV (5 kHz)[d]	B
	Surge	IEC 61000-4-5	1 kV[b, c] (1,2/50 μs)	B
	Conducted RF	IEC 61000-4-6	3 V[d, f](150 kHz to 80 MHz)	A
I/O signal/ control connected directly to power supply network	Burst	IEC 61000-4-4	2 kV (5 kHz)	B
	Surge	IEC 61000-4-5	1 kV[a]/2 kV[b] (1,2/50 μs)	B
	Conducted RF	IEC 61000-4-6	3 V[f] (150 kHz to 80 MHz)	A

a Line to line.

b Line to ground.

c Only in the case of long-distance lines (see 3.6).

d Only in the case of lines > 3 m.

e Only to magnetically sensitive equipment. CRT display interference is allowed above 1 A/m.

f The test level for the conducted RF test is lower than the level for the EM field test because the conducted RF test simulates the resonance condition at each frequency and is thus a more severe test.

g DC connections between parts of equipment/system which are not connected to a d.c. distribution network are treated as I/O signal/control ports.

h “25/30 cycles" means "25 cycles for 50 Hz test" and "30 cycles for 60 Hz test”.

4.2.4.2.1 Electrostatic discharge (ED)

Four installation and environmental classes are defined according to the humidity and the type of material, as Table 6 shows, extracted from IEC 61000-4-2:2008, reports:

Table 6 – ED classed

Class	Relative humidity as low as [%]	Antistatic material	Synthetic material
1	35	X	
2	10	X	
3	50		X
4	10		X

The installation classes are related to the test levels, which give a quantitative measure of the stress to which the device is exposed (see Table 7).

Table 7 – Test levels for ED

Class	Test voltage [kV] Contact discharge	Test voltage [kV] Air discharge
1	2	2
2	4	4
3	6	8
4	8	15
X	Special	Special

4.2.4.2.2 Radiated radio-frequency electromagnetic field

IEC 61000-4-3 defines five classes of environments, as listed below:

Class 1: low-level electromagnetic radiation environment. Levels typical for local radio/television stations located at more than 1 km, and transmitters/receivers with low power;

Class 2: moderate electromagnetic radiation environment. Low power portable transceivers (typically less than 1 W rating) are in use, but with restrictions on use in close proximity to the equipment (typical commercial environment);

Class 3: severe electromagnetic radiation environment. Portable transceivers (2 W rating or more) are in use relatively close to the equipment but not less than 1 m. High power broadcast transmitters are in close proximity to the equipment and ISM equipment may be located close by (typical industrial environment);

Class 4: portable transceivers are in use within less than 1 m of the equipment. Other sources of significant interference may be within 1 m of the equipment;

Class x: x is an open level which might be negotiated and specified in the product standard or equipment specification.

The installation classes are related to the test levels, which give a quantitative measure of the stress to which the device is exposed (see Table 8, extracted from IEC 61000-4-3:2006).

Table 8 – Test levels for RF fields

Class	Test field strength [V/m]
1	1
2	3
3	10
4	30
X	Special

4.2.4.2.3 Electrical Fast Transient/Burst immunity test

IEC 61000-4-4 defines five classes of environment, as listed below:

– Class 1: well-protected environment

The installation is characterized by the following attributes:

- suppression of all EFT/B in the switched power supply and control circuits;
- separation between power supply lines (a.c. and d.c.) and control and measurement circuits coming from other environments belonging to higher severity levels;
- shielded power supply cables with the screens earthed at both ends on the reference earthing of the installation, and power supply protection by filtering.

A computer room may be representative of this environment.

The applicability of this level to testing of equipment is limited to the power supply circuits for type tests, and to the earthing circuits and equipment cabinets for post-installation tests.

– Class 2: protected environment

The installation is characterized by the following attributes:

- partial suppression of EFT/B in the power supply and control circuits which are switched only by relays (no contactors);
- poor separation of the industrial circuits belonging to the industrial environment from other circuits associated with environments of higher severity levels;
- physical separation of unshielded power supply and control cables from signal and communication cables.

The control room or terminal room of industrial and electrical plants may be representative of this environment.

– Class 3: typical industrial environment

The installation is characterized by the following attributes:

- no suppression of EFT/B in the power supply and control circuits which are switched only by relays (no contactors);
- poor separation of the industrial circuits from other circuits associated with environments of higher severity levels;
- dedicated cables for power supply, control, signal and communication lines;
- poor separation between power supply, control, signal and communication cables;
- availability of earthing system represented by either conductive pipes or earth conductors in the cable trays connected to the protective earth system.

Heavy industrial processes may be representative of this environment.

– Class 4: severe industrial environment

The installation is characterized by the following attributes:

- no suppression of EFT/B in the power supply and control and power circuits which are switched by relays and contactors;
- no separation of the industrial circuits belonging to the severe industrial environment from other circuits associated with environments of higher severity levels;
- no separation between power supply, control, signal and communication cables;
- use of multicore cables in common for control and signal lines.

The outdoor area of industrial process equipment where no specific installation practice has been adopted, power plants, the relay rooms of open-air H.V. substations and gas insulated substations of up to 500 kV operating voltage (with typical installation practice) may be representative of this environment.

– Class 5: special situations to be analysed

The minor or major electromagnetic separation of disturbance sources from equipment circuits, cables, lines etc., and the quality of the installations may require the use of a higher or lower environmental level than those described above. It should be noted that equipment lines of a higher environmental level can penetrate a lower severity environment.

Table 9, extracted from IEC 61000-4-4:2004, reports the installation classes and the corresponding test levels, which give a quantitative measure of the stress the device is exposed to:

Table 9 – Test levels for Electrical Fast Transient/Burst

Open circuit output test voltage and repetition rate of the impulses				
Level	On power port, PE		On I/O (input/output) signal, data and control ports	
	Voltage peak	Repetition rate	Voltage peak	Repetition rate
	kV	kHz	kV	kHz
1	0,5	5 or 100	0,25	5 or 100
2	1	5 or 100	0,5	5 or 100
3	2	5 or 100	1	5 or 100
4	4	5 or 100	2	5 or 100
X [a]	Special	Special	Special	Special
NOTE 1 Use of 5 kHz repetition rates is traditional; however, 100 kHz is closer to reality. Product committees should determine which frequencies are relevant for specific products or product types.				
NOTE 2 With some products, there may be no clear distinction between power ports and I/O ports, in which case it is up to product committees to make this determination for test purposes.				
[a] "X" is an open level. The level has to be specified in the dedicated equipment specification.				

4.2.4.2.4 Surge

IEC 61000-4-5 defines seven classes of environment, as listed below:

– Class 0: well-protected electrical environment, often within a special room

All incoming cables are provided with overvoltage (primary and secondary) protection. The units of the electronic equipment are interconnected by a well designed grounding system, which is not significantly influenced by the power installation or lightning. The electronic equipment has a dedicated power supply (see Table 10). Surge voltage may not exceed 25 V.

– Class 1: partly protected electrical environment

  All incoming cables to the room are provided with overvoltage (primary) protection. The units of the equipment are well-interconnected by a ground connection network, which is not significantly influenced by the power installation or lightning. The electronic equipment has its power supply completely separated from the other equipment. Switching operations can generate interference voltages within the room. Surge voltage may not exceed 500 V.

– Class 2: electrical environment where the cables are well-separated, even at short runs.

  The installation is grounded via a separate connection to the grounding system of the power installation which can be subjected to interference voltages generated by the installation itself or by lightning. The power supply to the electronic equipment is separated from other circuits, usually by a dedicated transformer for the mains power supply. Non-protected circuits are present in the installation, but well-separated and in restricted numbers. Surge voltages may not exceed 1 kV.

– Class 3: electrical environment where power and signal cables run in parallel

  The installation is grounded to the common grounding system of the power installation which can be subjected to interference voltages generated by the installation itself or by lightning. Current due to ground faults, switching operations and lightning in the power installation may generate interference voltages with relatively high amplitudes in the grounding system. Protected electronic equipment and less sensitive electric equipment are connected to the same power supply network. The interconnection cables can be partly outdoor cables, but close to the grounding network. Unsuppressed inductive loads are present in the installation and usually there is no separation of the different field cables. Surge may not exceed 2 kV.

– Class 4: Electrical environment where the interconnections are running as outdoor cables along with power cables, and cables are used for both electronic and electric circuits

  The installation is connected to the grounding system of the power installation which can be subjected to interference voltages generated by the installation itself or by lightning. Currents in the kA range due to ground faults, switching operations and lightning in the power supply installation may generate interference voltages with relatively high amplitudes in the grounding system. The power supply network can be the same for both the electronic and the other electrical equipment. The interconnection cables are run as outdoor cables, even to the high-voltage equipment. A special case of this environment is when the electronic equipment is connected to the telecommunication network within a densely populated area. There is no systematically constructed grounding network outside the electronic equipment, and the grounding system consists only of pipes, cables, etc. Surge voltage may not exceed 4 kV.

– Class 5: Electrical environment for electronic equipment connected to telecommunication cables and overhead power lines in a non-densely populated area

  All these cables and lines are provided with overvoltage (primary) protection. Outside the electronic equipment there is no widespread grounding system (exposed plant). The interference voltages due to ground faults (currents up to 10 kA) and lightning (currents up to 100 kA) can be extremely high. The requirements of this class are covered by the test level 4

– Class x: Special conditions specified in the product specifications

The installation classes are related to the test levels reported in Table 10, extracted from IEC 61000-4-5:2005, which give a quantitative measure of the stress to which the device is exposed.

Table 10 – Test levels for surge protection

Installation class	Test levels (kV)											
	AC power supply and a.c. I/O directly connected to the mains network Coupling mode		AC power supply and a.c. I/O not directly connected to the mains network Coupling mode		DC power supply and d.c. I/O directly connected thereto Coupling mode		Unsymmetrical operated [d,f] circuits/lines Coupling mode		Symmetrical operated[d,f] circuits/lines Coupling mode		Shielded I/O and communication lines [f] Coupling mode	
	Line-to-line	Line-to-ground	Line-to-line	Line-to-ground	Line-to-line	Line-to-ground	Line-to-line	Line-to-ground	Line-to-line	All lines-to-ground	Line-to-line	Line-to-ground
0	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
1	NA	0,5	NA	NA	NA	NA	NA	0,5	NA	0,5	NA	NA
2	0,5	1,0	NA	NA	NA	NA	0,5	1,0	NA	1,0	NA	0,5
3	1,0	2,0	1,0[e]	2,0[b,e]	1,0 [e]	2,0[b,e]	1,0 [c]	2,0[b,c]	NA	2,0[b,c]	NA	2,0[c]
4	2,0	4,0[b]	2,0[e]	4,0[b,e]	2,0 [e]	4,0[b,e]	2,0 [c]	4,0[b,c]	NA	2,0[b,c]	NA	4,0[c]
5	a	a	2,0	4,0b	2,0	4,0b	2,0	4,0b	NA	4,0b	NA	4,0 c

a Depends on the class of the local power supply system.

b Normally tested with primary protection.

c The test level may be lowered by one level if the cable length is shorter or equal to 10 m.

d No test is advised at data connections intended for cables shorter than 10 m.

e If protection is specified upstream from the EUT, the test level should correspond to the protection level when the protection is not in place.

f High speed communications lines could be included under unsymmetrical, symmetrical, shielded I/O and/or communications lines.

4.2.4.2.5 Conducted disturbances induced by radio-frequency fields

IEC 61000-4-6 defines four classes of environment, as listed below:

Class 1: Low-level electromagnetic radiation environment. Typical level where radio/television stations are located at a distance of more than 1 km and typical level for low-power transceivers.

Class 2: Moderate electromagnetic radiation environment. Low-power portable transceivers (typically less than 1 W rating) are in use, but with restrictions on use in close proximity to the equipment (typical commercial environment).

Class 3: Severe electromagnetic radiation environment. Portable transceivers (2 W and more) are in use relatively close to the equipment but at a distance not less than 1 m. High-powered broadcast transmitters are in close proximity to the equipment and ISM equipment may be located close by (typical industrial environment).

Class x: x is an open level which may be negotiated and specified in the dedicated equipment specifications or equipment standards.

Table 11, extracted from IEC 61000-4-6:2008, reports the installation classes and the corresponding test levels that represent a quantitative measure of the stress to which the device is exposed:

Table 11 – Test levels for RF induced disturbances

Frequency range 150 kHz – 80 MHz		
Level	Voltage level (e.m.f.)	
	U_0 dB(μV)	U_0 V
1	120	1
2	130	3
3	140	10
X [a]	Special	
[a] X is an open level.		

4.2.4.2.6 Power frequency magnetic field

IEC 61000-4-8 defines six classes of environment, as listed below:

– Class 1: Environmental level where sensitive device using electron beam can be used.

Monitors, electron microscope, etc., are representative of these devices.

– Class 2: Well protected environment

The environment is characterized by the following attributes:

- absence of electrical equipment like power transformers that may give rise to leakage fluxes;
- areas not subjected to the influence of H.V. bus-bars.

Household, office, hospital protected areas far away from earth protection conductors, areas of industrial installations and H.V. sub-stations may be representative of this environment.

– Class 3: Protected environment

The environment is characterized by the following attributes:

- electrical equipment and cables that may give rise to leakage fluxes or magnetic field;
- proximity of earth conductors of protection systems;
- M.V. circuits and H.V. bus-bars far away (a few hundred metres) from equipment concerned.

Commercial areas, control building, field of not heavy industrial plants, computer room of H.V. sub-stations may be representative of this environment.

– Class 4: Typical industrial environment

The environment is characterized by the following attributes:

- short branch power lines as bus-bars, etc.;
- high power electrical equipment that may give rise to leakage fluxes;
- ground conductors of protection system;
- M.V. circuits and H.V. bus-bars at relative distance (a few tens of metres) from equipment concerned.

Fields of heavy industrial and power plants and the control room of H.V. sub-stations may be representative of this environment.

– Class 5: Severe industrial environment

The environment is characterized by the following attributes:

- conductors, bus-bars or M.V., H.V. lines carrying tens of kA;

- ground conductors of the protection system;
- proximity of M.V. and H.V. bus-bars;
- proximity of high power electrical equipment.

Switchyard areas of heavy industrial plants, M.V., H.V. and power stations may be representative of this environment.

– Class x: Special environment

The installation classes are related to the test levels defined in Table 12, extracted from IEC 61000-4-8:2009, which give a quantitative measure of the stress to which the device is exposed.

Table 12 – Test levels for power frequency magnetic fields

Level	Magnetic field strength [A/m]
1	1
2	3
3	10
4	30
5	100
x[a]	special
[a] "x" is an open level. This level can be given in the product specification.	

4.2.4.2.7 Pulse magnetic field

IEC 61000-4-9 defines six classes of environment, but only four are applicable to industrial application. The useful classes are listed below:

– Class 3: Protected environment

The environment is characterized by the proximity of earth conductors of lightning protection systems and metallic structures. Commercial areas, control building, field of not heavy industrial plants provided with lightning protection system or metallic structures in the proximity, computer room of H.V. sub-stations may by representative of this environment.

– Class 4: Typical industrial environment

The environment is characterized by the down conductors of the lightning protection system or structures. Fields of heavy industrial and power plants and the control room of H.V. sub-stations may be representative of this environment.

– Class 5: Severe industrial environment

The environment is characterized by the following attributes:

- conductors, bus-bars or M.V., H.V. lines carrying tens of kA;
- ground conductors of the lightning protection system or high structures like the line towers carrying the whole lightning current.

Switchyard areas of heavy industrial plants, M.V., H.V. and power stations may be representative of this environment.

– Class x: Special environment

The installation classes are related to the test levels reported in Table 13, extracted from IEC 61000-4-9:1993, which give a quantitative measure of the stress the device is exposed to.

Table 13 – Test levels for pulse magnetic field

Class	Pulse magnetic field strength [A/m]
3	100
4	300
5	1 000
X	Special

4.2.4.2.8 Damped oscillatory magnetic field

IEC 61000-4-10 defines four classes that are applicable to the industrial environment in which the devices of the PCS are installed:

Class 3: protected environment;

Class 4: typical industrial environment;

Class 5: severe industrial environment;

Class x: special environment.

Each environmental class is related to test levels that give a quantitative measure of the stress applied to the device, as Table 14, extracted from IEC 61000-4-10:1993, reports:

Table 14 – Test levels for damped oscillatory magnetic field

Level	Damped oscillatory magnetic field strength [A/m]
3	10
4	30
5	100
X	Special

4.2.4.2.9 Voltage dips and short interruptions

IEC 61000-4-11 defines three classes of environment, as listed below:

– Class 1: This class applies to protected supplies and has compatibility levels lower than public network levels. It relates to the use of equipment very sensitive to disturbances in the power supply, for instance the instrumentation of technological laboratories, some automation and protection equipment, some computers, etc. Class 1 environments normally contain equipment which requires protection by such apparatus as uninterruptible power supplies (UPS), filters, or surge suppressers.

– Class 2: This class applies to points of common coupling (PCC for consumer systems) and in-plant points of coupling (IPC) in the industrial environment in general. The compatibility levels in this class are identical to those of public networks; therefore components designed for application in public networks may be used in this class of industrial environment.

– Class 3: This class applies only to IPCs in industrial environments. It has higher compatibility levels than those of Class 2 for some disturbance phenomena. For instance, this class should be considered when any of the following conditions are met:

  - a major part of the load is fed through converters;
  - welding machines are present;
  - large motors are frequently started;
  - loads vary rapidly.

The installation classes are related to the test levels in Table 15 and Table 16, extracted from IEC 61000-4-11:2004, which give a quantitative measure of the stress to which the device is exposed. The voltage used as a basis for the specification of the test levels is the rated voltage of the equipment (U_T).

Table 15 – Test levels for voltage dips

Class[a]	Test level and durations for voltage dips (t_s) (50 Hz/60 Hz)				
Class 1	Case-by-case according to the equipment requirements				
Class 2	0 % during ½ cycle	0 % during 1 cycle	70 % during 25/30[c] cycles		
Class 3	0 % during ½ cycle	0 % during 1 cycle	40 % during 10/12[c] cycles	70 % during 25/30[c] cycles	80 % during 250/300[c] cycles
Class X[b]	X	X	X	X	X

a Classes as per IEC 61000-2-4; see Annex B.
b To be defined by product committee. For equipment connected directly or indirectly to the public network, the levels must not be less severe than Class 2.
c "25/30 cycles" means "25 cycles for 50 Hz test" and "30 cycles for 60 Hz test".

Table 16 – Test levels for short interruptions

Class[a]	Test level and durations for short interruptions (t_s) (50 Hz/60 Hz)
Class 1	Case-by-case according to the equipment requirements
Class 2	0 % during 250/300[c] cycles
Class 3	0 % during 250/300[c] cycles
Class X[b]	X

a Classes as per IEC 61000-2-4; see Annex B.
b To be defined by product committee. For equipment connected directly or indirectly to the public network, the levels must not be less severe than Class 2.
c "250/300 cycles" means "250 cycles for 50 Hz test" and "300 cycles for 60 Hz test".

4.2.4.3 Emission

IEC 61000-6-4 defines the EMC emission requirements that apply to electrical and electronic apparatus intended for use in industrial environments. The frequency range is between 0 Hz and 400 GHz. Table 17 reports the emission limits defined in IEC 61000-6-4:2006.

Table 17 – Table for emission limits

Port	Frequency range	Limits	Basic standard	Applicability note	Remarks
1) Enclosure port – Open area test site or semi-anechoic method	30 MHz – 230 MHz 230 MHz – 1 000 MHz	40 dB(μV/m) Quasi-peak at 10 m 47 dB(μV/m) Quasi-peak at 10 m	CISPR 16-2-3	a	May be measured at 30 m distance using the limits decreased by 10 dB.
2) Low voltage AC mains port	0,15 MHz – 0,5 MHz	79 dB(μV) quasi-peak 66 dB(μV)average	CISPR 16-2-1, 7.4.1 CISPR 16-1-2, 4.3	b	
	0,5 MHz – 30 MHz	73 dB(μV) quasi-peak 60 dB(μV) average			
3) Telecommunications/network port	0,15 MHz – 0,5 MHz	97 dB(μV) – 87 dB(μV) quasi-peak 84 dB(μV) – 74 dB(μV) average 53 dB(μA) – 43 dB(μA) quasi-peak 40 dB(μA) – 30 dB(μA) average	CISPR 22	c,d,e	
	0,5 MHz – 30 MHz	87 dB(μV) quasi-peak 74 dB(μV) average 43 dB(μA) quasi-peak 30 dB(μA) average		c,e	

[a] If the internal emission source(s) is operating at a frequency below 9 kHz then measurements need only to be performed up to 230 MHz.

[b] Impulse noise (clicks) which occur less than five times per minute is not considered. For clicks appearing more often than 30 times per minute, the limits apply. For clicks appearing between 5 and 30 times per minute, a relaxation of the limits is allowed of 20 log 30/*N* dB (where *N* is the number of clicks per minute). Criteria for separated clicks may be found in CISPR 14-1.

[c] At transitional frequencies the lower limit applies.

[d] The limits decrease linearly with the logarithm of the frequency in the range 0,15 MHz to 0,5 MHz.

[e] The current and voltage disturbance limits are derived for use with an impedance stabilization network (ISN) which presents a common mode (asymmetric mode) impedance of 150 Ω to the telecommunication port under test (conversion factor is 20 $\log_{10}$ 150 / *I* = 44 dB).

No specification about EM emission is necessary, if the PCS components comply with IEC 61000-6-4.

4.2.5 Mechanical vibrations

The classification criteria used for a vibrational environment for a PCS and its components are very much dependent on the nature of the equipment such as size, mass, wiring, etc. For such a reason, the technical approach of IEC 60654-3 is here considered. The stresses on the components are expressed both in terms of vibrational severity and duration of the vibrations.

The vibrational severity is expressed as the velocity expressed in mm/s at which the component is exposed during the vibration. The frequency range of the vibration is considered between 1 Hz and 150 Hz.

There are five classes for vibrational severity:

- V.S.1: velocity < 3 mm/s (i.e., control room and general industrial environment);
- V.S.2: velocity < 10 mm/s (i.e., field equipment);
- V.S.3: velocity < 30 mm/s (i.e., field equipment);
- V.S.4: velocity < 300 mm/s (i.e., field equipment including transportation);
- V.S.X: velocity > 300 mm/s.

The duration of the vibration for the considered device is selected between one the following three classes:

- V.T.1 permanent: 100 % of time;
- V.T.2 occasional: 10 % of time;
- V.T.3 unusual: 1 % of time.

4.2.6 Corrosive and erosive influences

4.2.6.1 General

There is a broad distribution of contaminant concentrations and reactivity levels existing within industries using process measurement and control equipment. Some environments are severely corrosive while others are mildly corrosive. Thus, as reported in IEC 60654-4, there are four different classes of environment according to the contaminant severity levels:

- Class 1: industrial clean air: an environment sufficiently well controlled that corrosion is not a factor in determining equipment reliability;
- Class 2: moderate contamination: an environment in which the effects of corrosion are measurable and may be a factor in determining equipment reliability;
- Class 3: heavy contamination: an environment in which there is a high probability that corrosive attack will occur. These harsh levels should prompt further evaluation resulting in environmental controls or specially designed and packaged equipment;
- Class 4: special: an environment in which the levels of contaminants are higher than in all the other classes.

4.2.6.2 Gases and vapours

The classes in Table 18 extracted from IEC 60654-4:1987 recognize that average concentrations and peak values should both be considered to properly classify an environment. Peak values are integrated on a ½ hour basis. Chemical agents (i.e., SO2 or HF) may vary greatly in their reactivity rate over a ½ h period. Therefore, the relationship of peak value to average value may vary with each contaminant. The classification of environment by category should be determined by the highest class if average and peak values are not in the same category.

Table 18 – Concentration of gas and vapour contaminants (in cm^3/m^3)

	Class 1		Class 2		Class 3		Class 4	
Chemically active contaminants in air	Industrial clean air		Moderate contamination		High contamination		Special	
	Mean Value	Peak Value	Mean Peak	Value Value	Mean Peak	Value Value	Mean Value	Peak Value
Hydrogen sulphide (H2S)	< 0,003	< 0,01	< 0,05	< 0,5	< 10	< 50	≥ 10	≥ 50
Sulphur dioxide (SO2)	< 0,01	< 0,03	< 0,1	< 0,3	< 5	< 15	≥ 5	≥ 15
Wet chlorine (Cl2)relative humidity > 50 %	< 0,0005	< 0,001	< 0,005	< 0,03	< 0,05	< 0,3	≥ 0,05	≥ 0,3
Dry chlorine (Cl2) relative humidity < 50 %	< 0,002	< 0,01	< 0,02	< 0,10	< 0,2	< 1,0	≥ 0,2	≥ 1,0
Hydrogen fluoride (HF)	< 0,001	< 0,005	< 0,01	< 0,05	< 0,1	< 1,0	≥ 0,1	≥ 1,0
Ammonia (NH3)	< 1	< 5	< 10	< 50	< 50	< 250	≥ 50	≥ 250
Nitrogen oxides (NO3)	< 0,05	< 0,1	< 0,5	< 1,0	< 5	< 10	≥ 5	≥ 10
Ozone (03) or other oxidants	< 0,002	< 0,005	< 0,025	< 0,05	< 0,1	< 1,0	≥ 0,1	≥ 1,0
Solvents Trichlorethylene	—	—	< 5	—	< 20	—	≥ 20	—
Special (other non-specified)	—	—	—	—	—	—	—	—
NOTE Solvent vapours can precipitate to form puddles which can become corrosive, especially to electrical parts of instruments.								

4.2.6.3 Aerosols

Aerosols are liquids carried in gas or air in the form of small droplets generating mists. Two common examples of aerosols are classified “oils in air” and “sea salt mists”.

For oils in air, the classes are defined as reported in Table 19 extracted from IEC 60654-4:1987.

Table 19 – Aerosol contaminants

	Class 1	Class 2	Class 3	Class 4
Oils (*μg/kg-dry air*)	< 5	< 50	< 500	> 500

For sea salt mists, the classes are defined as listed below:

- Class 1: location near sea coasts more than 0,5 km away from the sea;
- Class 2: on the sea coast (less than 0,5 km away);
- Class 3: off-shore installations.

4.2.6.4 Solid substances

There is no possibility to classify the environments according to the levels of solid substances that are affecting the installation. For such a reason, the way to define the contamination of the environment by means of solid substance is to answer a list of questions:

- nature of solid substances in the environment which could affect the instruments and PCS components (e.g., sand, cement dust, textile fibres, etc.);
- frequency of occurrence: i.e., continuous, occasional, unusual, etc.
- average particle size: i.e., < 3 μm, between 3 μm and 30 μm, more than 0,3 mm, etc.
- concentration in mg/kg of dry air: this applies only to airborne solid particles.

4.2.6.5 Liquids

There is no possibility to classify the environments according to the levels of liquid substances that are affecting the installation. For such a reason, the way to define the contamination of the environment by means of liquid substances is to answer a list of questions:

- nature of liquid substances in the environment which could affect the instruments and PCS components;
- frequency of occurrence: i.e., continuous, occasional, unusual, etc.;
- electrical conductivity.

4.2.7 Lightning protection

According to the definition in IEC 62305-1 it is possible to define a Lightning Protection Zone (LPZ) as the zone where the lightning electromagnetic environment is clearly defined.

The LPZ is defined by protection measures such as Lightning Protection System (LPS), shielding wires, magnetic shields and Surge Protective Device (SPD). LPZ downstream of the protection measure are characterized by significant reduction of LEMP (Lightning Electromagnetic iMPulse, which is electromagnetic effect of lightning current) than that upstream of the LPZ.

With respect to the threat of lightning, the following LPZs are defined:

- LPZ 0_A: zone where the threat is due to the direct lightning flash and the full lightning electromagnetic field. The internal systems may be subjected to full or partial lightning surge current;
- LPZ 0_B: zone protected against direct lightning flashes but where the threat is the full lightning electromagnetic field. The internal systems may be subjected to partial lightning surge currents;
- LPZ 1: zone where the surge current is limited by current sharing and by SPDs at the boundary. Spatial shielding may attenuate the lightning electromagnetic field;
- LPZ 2,…,n: zone where the surge current may be further limited by current sharing and by additional SPDs at the boundary. Additional spatial shielding may be used to further attenuate the lightning electromagnetic field.

4.2.8 Hazardous area

4.2.8.1 Hazardous area classification according to IEC standards

4.2.8.1.1 General

This subclause requires the user to define the areas where the different parts of the PCS are installed in term of explosion hazard. The classification considers the potential hazard due to the presence of inflammable substances, e.g., gases, vapours, and/or dusts that may create explosive atmospheres.

4.2.8.1.2 Classification of hazardous areas for explosive gas atmosphere

According to the definition in the IEC 60079-10-1, a hazardous area is an area in which an explosive gas atmosphere is present, or may be expected to be present, in quantities such as to require special precautions for the construction, installation and use of apparatus.

Hazardous areas are classified into zones based upon the frequency of the occurrence and duration of an explosive atmosphere, as follows:

Zone 0: Place in which an explosive atmosphere consisting of a mixture with air of flammable substances in the form of gas, vapour or mist is present continuously or for long periods or frequently;

Zone 1: Place in which an explosive atmosphere consisting of a mixture with air of flammable substances in the form of gas, vapour or mist is likely to occur in normal operation occasionally;

Zone 2: Place in which an explosive atmosphere consisting of a mixture with air of flammable substances in the form of gas, vapour or mist is not likely to occur in normal operation but, if it does occur, will persist for a short period only.

4.2.8.1.3 Classification of hazardous areas for the presence of combustible dusts

According to the definition in the IEC 60079-10-2, an explosive dust atmosphere is mixture with air, under atmospheric conditions, of flammable substances in the form of dust, fibres or filings in which, after ignition, combustion spreads throughout the unconsumed mixture.

A hazardous area for combustible dust is an area in which combustible dust in cloud form is, or can be expected to be, present in quantities such as to require special precautions for the construction and use of equipment in order to prevent ignition of an explosive dust/air mixture.

Areas classified for explosive dust atmospheres are divided into zones, which are identified according to the frequency and duration of the occurrence of explosive dust/air atmospheres.

Zone 20: Place in which an explosive atmosphere, in the form of a cloud of combustible dust in air, is present continuously, or for long periods or frequently for short periods;

Zone 21: Place in which an explosive atmosphere, in the form of a cloud of combustible dust in air, is likely to occur occasionally in normal operation;

Zone 22: Place in which an explosive atmosphere, in the form of a cloud of combustible dust in air, is not likely to occur in normal operation but, if it does occur, will persist for a short period only.

4.2.8.2 Equipment classification for hazardous area according to IEC standards

This subclause deals with the classification of the equipment that are intended for use in potentially explosive atmosphere.

In this scenario, equipment means machines, apparatus, fixed or mobile devices, control components and field instruments that are capable of causing an explosion through their own potential sources of ignition.

The standard classifies the equipment in two groups, according to their installation:

- Group I: applies to equipment intended for use in underground parts of mines, and to those parts of surface installations of such mines, liable to be endangered by firedamp and/or combustible dust;
- Group II: applies to equipment intended for use in other places liable to be endangered by explosive atmospheres.

In the following, the reference is for equipment of Group II. The classification of the electrical apparatus refers to the specific measures applied to the electrical apparatus for avoiding ignition of a surrounding explosive atmosphere.

The classification of the electrical apparatus is based on IEC 60079-14:

- flameproof enclosure “d”: type of protection in which the parts which can ignite an explosive atmosphere are placed in an enclosure which can withstand the pressure developed during an internal explosion of an explosive mixture and which prevents the transmission of the explosion to the explosive atmosphere surrounding the enclosure;

- increased safety “e”: type of protection applied to electrical apparatus in which additional measures are applied so as to give increased security against the possibility of excessive temperatures and of the occurrence of arcs and sparks in normal service or under specified abnormal conditions;
- intrinsic safety “i”: type of protection based upon the restriction of electrical energy within apparatus and of interconnecting wiring exposed to an explosive atmosphere to a level below that which can cause ignition by either sparking or heating effects;
- pressurization “p”: technique of guarding against the ingress of the external atmosphere into an enclosure by maintaining a protective gas therein at a pressure above that of the external atmosphere;
- type of protection “n”: type of protection applied to electrical apparatus such that, in normal operation and in certain specified abnormal conditions, it is not capable of igniting a surrounding explosive atmosphere;
- equipment protection by powder filling “q”: type of protection in which the parts capable of igniting an explosive gas atmosphere are fixed in position and completely surrounded by filling material to prevent the ignition of an external explosive gas atmosphere;
- equipment protection by oil immersion “o”: type of protection in which the electrical equipment or parts of the electrical equipment are immersed in a protective liquid in such a way that an explosive gas atmosphere which may be above the liquid or outside the enclosure cannot be ignited;
- construction, test and marking of type of protection, "n" electrical apparatus: type of protection applied to electrical apparatus such that, in normal operation and in certain specified abnormal conditions, it is not capable of igniting a surrounding explosive gas atmosphere

4.2.9 Earth connection

IEC 61140 defines three classes of earth connections for electrical devices or control panels. These classes are related to the type of protection against electric shocks that is required, as reported below:

– Class I: these appliances should have their chassis connected to electrical earth (ground) by an earth conductor. A fault in the appliance that causes a live conductor to contact the casing will cause a current flow in the earth conductor. The current should trip either an over current device or a residual current circuit breaker, which will cut off the supply of electricity to the appliance.

– Class II: a Class 2 or double insulated electrical appliance is designed in such a way that it does not require (and should not have) a safety connection to electrical earth (ground).

– Class III: designed to be supplied from a SELV power source. The voltage from a SELV supply is low enough that under normal conditions a person can safely come into contact with it without risk of electric shock. The extra safety features built into Class 1 and Class 2 appliances are therefore not required.

4.3 System characteristics

4.3.1 General

This subclause defines the main characteristics that influence the PCS structure and capability in general terms, with a special focus on its integration and scalability.

The user/engineer should specify the system characteristics in accordance with the technical definitions of the following subclauses. Annex C may be used as a guidance.

4.3.2 System scalability

Scalability is the ability of a system and/or an application to grow incrementally larger without total replacement of hardware or software, and without the need to re-engineer the entire architecture of the system.

4.3.3 System expandability

The system expandability is the possibility of the system to be enlarged without changing the architecture and/or the used equipment. The expandability can be both for the entire system and for each apparatus.

The system expandability means that it is possible to add usable components to the system.

For a component, for example a programmable logic controller, expandability means that it is possible to add usable spare part to the component (i.e., the free memory or CPU in a PLC).

4.3.4 Integration of sub-systems

Integration of subsystems needs a procedure for combining separately developed modules of components so that they work together as a unique system. A subsystem is a set of components that operates as a part of a system and that is capable of performing a specific task within a system. A subsystem could be an existing system, which means that an already installed and operating system could be included in a new (larger) system.

Another option is that a subsystem has been provided by other suppliers and manufactures (i.e., third party subsystem).

4.3.5 System configuration

4.3.5.1 General

The system configuration is the construction of a control system by selecting functional or modular units out of a given set and by defining their interconnections. Configurability of the system defines the extent to which the system facilitates selection, setting up and arrangement of its modules to perform its mission.

The configuration can be both hardware and software.

The main functionalities for the software configuration of the system are:

- definition of the system architecture by means of the configuration tool;
- inserting software modules;
- selecting and setting parameters;
- selecting options;
- programming;
- compiling and downloading programmes;
- basic engineering.

Some of the software configuration actions may be permissible also if the system is running. Some configuration tools allow the configuration of the entire system even if there is no hardware connected (emulated mode).

The basic functionalities for the hardware configuration of a PCS are:

- inserting modules;
- mounting devices;
- connection by soldering and/or by wiring;
- setting jumpers;
- setting switches;
- inserting printed circuit boards.

Normally, for performing the hardware configuration, it is necessary that the system is disabled from process operation.

4.3.5.2 On-line configuration

If the system supports on-line configuration, then it is possible to run the system configuration procedure whilst the PCS is running with no loss of functionality and with only known and acceptable disturbance of functionality (i.e., a 3-seconds freeze). On-line configuration may have different levels:

- both hardware and software full re-configuration is possible;
- only minor hardware changes are allowed;
- only minor software changes are possible.

On-line configuration is often related to the redundancy policy of the PCS (see 4.4.3).

4.3.5.3 Off-line configuration

Off-line configuration means that for setting up the functional parameters of the PCS it is necessary to switch the PCS into off-line, to load the changes and then to switch the system on-line again, after the validation of the parameter changes.

4.3.5.4 Configuration in simulation mode

Configuration in simulation mode means that before loading any configuration change in the PCS it is possible to run a simulation of the system with the new parameters for a preventive evaluation of the effect of changes.

4.3.5.5 Graphical resources

Graphical resources are software tools that support the engineering and the configuration phases. The PCS architecture is drawn starting from a library of devices (click-and-drag) with a graphic tool for defining data exchange and component interconnection. It is also possible to input parameters and functions with graphic procedures (pop-up menus, forms, etc.).

4.3.6 Automatic documentation

The PCS automatically generates the documentation after the configuration phase. Documents may include:

- system architecture;
- configuration parameters;
- list of material;
- application software;
- wiring table for terminations;
- cables and plugs configuration;
- others.

4.3.7 Programming languages for control

4.3.7.1 General

The control part of the system should support specific programming languages for implementing the control logic. According to the type of functions required to the PCS, a different standard programming language can be used.

In the following subclauses, the term Programmable (Logic) Controller (PLC) means a digitally operating electronic system, designed for use in an industrial environment, that uses a programmable memory for the internal storage of user-oriented instructions for implementing specific functions such as logic, sequencing, timing, counting and arithmetic. A PLC can control, through digital or analogue inputs and outputs, various types of machines or processes. In large scale PCS, the term *controller* is often used with the same meaning. Both the PLC and its associated peripherals are designed so that they can be easily integrated into an industrial control system and easily used in all their intended functions.

The term PLC-system means user-built configuration, consisting of a programmable controller and associated peripherals, that is necessary for the intended automated system. It consists of units interconnected by cables or plug-in connections for permanent installation and by cables or other means for portable and transportable peripherals.

4.3.7.2 Programming languages for programmable controllers

IEC 61131-3 defines a set of languages for programming PLCs and controllers. The standard programming languages are divided into two categories:

– graphical languages:
  - Ladder: (LD) it is a symbolic representation that schematically illustrates the control functions in the form of electrical circuit diagrams;
  - Function Block Diagram (FBD): it allows program elements (i.e., PID and other algorithms) to appear as blocks that are connected together as shown in a visual presentation similar to a logic diagram;

– textual languages:
  - Instruction List (IL): it is a low level language similar to assembler in which only one elementary operation, such as storing a value in a register, is allowed per line;
  - Structured Text (ST): it is a high-level, block-structure language, whose syntax resembles Pascal. ST allows express complex statements involving variables that represent a wide range of different types of data.

4.3.7.3 Sequential Function Chart (SFC) programming tool

In addition to the programming languages defined in IEC 61131-3, SFC programming tool allows a graphical representation and structuring of the control software (see IEC 60848). SFC is a way of graphically representing a complex control program as a sequence of alternating steps and transitions.

4.3.7.4 Continuous Function Chart (CFC) programming tool

Continuous Function Chart (CFC) allows the straightforward conversion of technological specifications into executable automation programs: it works using function blocks that are linked together and configured individually. The CFC is mainly used to show the top-level structure of the resources and programs.

The CFC can be intended as a special form of FBD. The main difference between CFC and FBD is that it also shows the resources and task assignments. Each function block shows the name of the task that controls its execution.

There is no standard for CFC, and each PCS supplier describes the syntax and semantics of CFC in informal way, very often with proprietary functions or features.

4.3.7.5 Definition of custom function block

IEC 61131-3 defines a set of standard function blocks common to all the programmable controllers. A function block is a set of elements consisting of:

1) the definition of a data structure partitioned into input, output, and internal variables; and
2) a set of operations to be performed upon the elements of the data structure when an instance of the function block type is invoked.

Examples of standard function blocks are:

- latch;
- edge detection;
- counter;
- timer.

In addition to the standard Function Blocks, it may be useful to define custom function blocks implementing specific functions. Once defined, a custom function block behaves like standard ones.

4.3.7.6 Batch programming tool

Batch control is in the scope of the family of standards IEC 61512 (also ISA S88) that define:

- models and terminology;
- data structures and languages;
- recipe models and representation;
- production records.

The PCS may support the environment for batch control defined in either IEC 61512 or ISA S88.

4.3.7.7 Multitasking operating software for controller

Multitasking operating software is a method for managing the resources of the controller CPU in order to allow multiple tasks to share common processing resources. The multitasking facility allows the programmer to make use of the multiprogramming capability of the controller. The term multiprogramming refers to a programming method in which more than one task is in an executable state contemporaneously.

4.3.7.8 Advanced Process Control (APC)

The APC can be simply defined as the process control strategies beyond straightforward PID control loops. APC are software tools, often sold as additional packages that can be either interfaced or installed in the PCS. APC allows a better control and optimization of the process, especially where the process dynamics contain unknown, un-measurable or non-linear characteristics, and it normally makes use of sophisticated control techniques, such as expert systems, sliding mode control, multi-variable control, etc.

4.3.8 PCS localisation

Localisation is the ability of a PCS to support local languages for different functions, such as:

- programming;
- documentation;
- HMI.

The required language(s) and function(s) are to be specified.

4.4 System dependability

4.4.1 General

Dependability is the collective term that describes the availability of a device or system, and its influencing factors: reliability, maintainability, and maintenance support (see Figure 5).

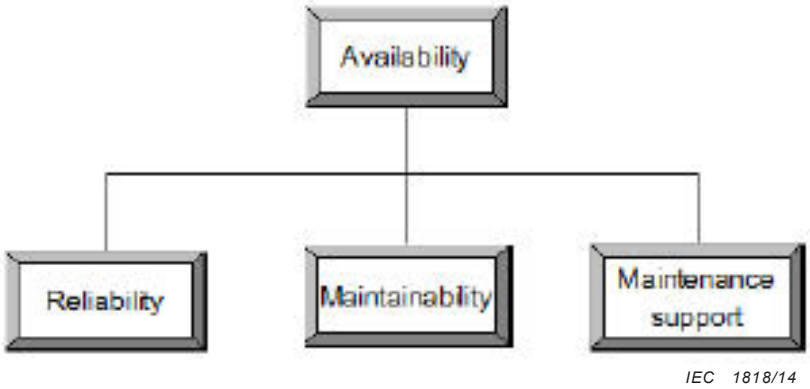

Figure 5 – The dependability concept

In other words, the system dependability is the extent to which a system can be relied upon to perform exclusively and correctly a task under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided.

A system dependability specification is the allocation of dependability requirements for each relevant function of the system from a dependability perspective. Dependability specification may vary with system configuration, mode of operation, and the applicable influencing conditions. The specification provides a set of key dependability requirements of relevant system functions and related characteristics for the initiation of system design.

The specification of the system dependability is a complex procedure and it may be a qualitative process. IEC 62347 and IEC 60300-3-4 describe the procedures for the dependability specification. For the purposes of this guideline, only the most relevant features affecting the system dependability are indicated.

The user/engineer should specify the system dependability in accordance with the technical definitions of the following subclauses. Annex D may be used as a guidance.

4.4.2 Reliability

Reliability of the system is the ability of the system to perform a required function under given conditions for a given time interval.

Reliability of a system depends upon the reliability of the individual parts of the system and the way in which these parts cooperate in performing the system task(s). The way in which parts cooperate may include functional redundancy (homogeneous or diverse), functional fallback and degradation. Reliability of the system may differ with respect to each of its tasks. Reliability can be quantified for individual tasks, with varying degrees of predictive confidence. The reliability of the individual hardware parts of the system can be predicted using the parts count method (see IEC TR 62380). Reliability of the overall system can be calculated by analytical tools and methods (see IEC 61078 and IEC 61025). It should be noted that for the software modules of systems, there are no reliability prediction methods available that provide high levels of confidence.

Reliability parameters and specifications are in the scope of IEC 61069-5.

4.4.2.1 System self-diagnostic

System self-diagnostics can help to improve the availability of a PCS through rapidly recognizing faults and failures and, thus, reducing the mean time to restoration. It could be necessary to implement self-diagnostic routines for the basic components of the PCS, such as the I/O cards or modules, the processor card, the memory cards and the communication links.

The results from the field device self-diagnostics should be used in the control logic to actuate safety or recovery actions in the case of detected field device faults or failures. The results from self-diagnostics of other components of the PCS should be used as appropriate, including annunciation through the alarm management system (see 4.7.8).

4.4.2.2 Single component fault tolerance

Fault tolerance is the built-in capability of a system to provide the continued, correct execution of its assigned function(s) in presence of a hardware or software failure of a single component. In other words, the system is able to perform its mission even after the first failure (hardware or software).

4.4.2.3 Hot swappable components

Each component of the PCS is hot swappable if it can be removed and substituted while the PCS is operating. The requirement for automatic configuration of hot-swapped components by the PCS (i.e., that the new component should be configured to match the removed component) should be considered. Hot-swap is possible both with faulted components, and with sound ones.

Hot swap capability is often desirable for critical components, whose failure might jeopardize one or more critical functions of the PCS. For this reason, critical components often have an installed back-up that allows the failed component to be hot-swapped without loss of critical functionality.

4.4.3 Availability

4.4.3.1 General

Availability of the system depends upon the availabilities of the individual parts of the system and the way in which these parts cooperate in performing the system tasks.

The way in which parts cooperate may include:

- functional redundancy (homogeneous or diverse): the redundancy of a specific function can be obtained using the same hardware both for the master and the stand-by (homogeneous) or with different hardware (diverse). If functional redundancy is available, the first failure does not reduce the functionality and the performance of the system;
- functional fall-back: a predefined alternative functionality in the case of detected failure or abnormal operation;
- degradation: in case of failure of a part of the PCS, the performance and the functionality of the system are reduced. In degraded working condition all the critical functions are working properly.

Availability depends upon the procedures used and the resources available for maintaining the system. There are several different approaches to defining availability requirements, including annual accumulated down times of PCS system components or tasks or the frequency of PCS faults or failures with different grades of process impacts.

In addition to the desired downtime or runtime, further special needs, if any, for increasing the availability of some critical functions should be specified.

4.4.3.2 Admissible degraded conditions

In the case of faults in the system, the system might not be able to implement all the functions that represent its mission. If degraded working conditions are admissible, it is possible to keep parts of the process and the system running even if one or more functions abort.

It is necessary to identify which are the functions that are not critical for the operation of the system and that can be lost in degraded conditions. The capacity of operating in degraded conditions increases the availability of the PCS.

4.4.3.3 Stand-by configurations for functional redundancy

If some critical components are functionally redundant, it is necessary to define the stand-by configuration. Basically, there are two possible stand-by configurations:

- hot stand-by: the primary and the back-up components or systems run simultaneously. Data, if the component should process data, are mirrored to the back-up component in real-time so that the two components are identical. The system can perform a hot swap between the primary and the back-up component without losing any data;
- cold stand-by: in this configuration, the back-up component is called up only when the primary component fails. Data, if needed, are mirrored in the back-up component with an update rate lower than in the case of the hot stand-by. This configuration is used for non-critical applications.

Intermediate solutions between hot and cold stand-by may exist, and are sometime referred as “warm stand-by”.

4.4.3.4 Protection action in fail-safe mode

The concept of fail-safe is where the predominant failure mode or modes of a component are such as to cause a safe response of the plant and process. For example a valve actuator that is air-on-to-open and spring-close is generally more likely to fail closed – if this is a safe state for the plant and process, the valve actuator can be described as "fail-safe". For performing a fail-safe protection, it is necessary to define the fail-safe devices (e.g., components, systems, control devices, etc.) that are designed so that they set the controlled parameters in a predetermined (safe) condition when the most probable failures happen.

4.4.4 Functional redundancy criteria

When specifying a control system, the effects of component failure should be assessed in relation to the controlled process, and redundancy should be requested accordingly.

Functional redundancy should cover components that are critical or vital for proper and safe operation of the entire system. When defining redundancy criteria, the following requirements should be addressed, when applicable according to the type of component:

- the type of stand-by, if any, as described in 4.4.3.3;
- the management of the software and data back-up between the redundant components;
- redundancy policy (1-out-of-2, 2-out-of-3, m-out-of-n);
- synchronization of data between the active and the stand-by machines;
- configuration of the active and stand-by machine.

Redundancy can be requested or needed for the following components/devices:

- controllers;

- control room networks;
- field communication networks;
- power supply;
- server system;
- HMI clients/monitors (no redundancy is needed if each HMI client can support and show all the data stored in the database);
- I/O cards or modules.

4.4.5 Maintainability

4.4.5.1 General

Maintainability is the ability of an item under given conditions of use, to be retained in, or restored to, a state in which it can perform a required function, when maintenance is performed under given conditions, with a defined impact on plant and process operation, and using stated procedures and resources.

4.4.5.2 Generation of maintenance requests

Some systems can be provided with the facility to generate maintenance requests if the operating status of a component changes. The capacity of generating a maintenance request is a way towards the preventive-predictive maintenance – in which devices or sub-systems can sometimes recognize autonomously the need for a repair intervention before failure of a function occurs. This capacity is mainly related to Intelligent Field Devices such as analytical instruments, valve positioners, etc.

4.4.5.3 Strategies for maintenance

Different strategies for maintenance exist, as described in the following:

- corrective or breakdown maintenance: response to detected faults and failures – to repair or replace the faulted element;
- preventive or scheduled maintenance: appropriate maintenance measures are initiated, generally before a failure occurs – to perform a time-dependent or status-dependent servicing, repair or replacement;
- predictive or condition-based maintenance: predictive diagnostics, measurements and/or record-keeping for timely detection of potential problems and to determine the remaining service life – to schedule appropriate servicing, repair or replacement interventions based on predicted component condition.

In the definition of the requirements, the requested strategies for maintenance should be defined.

4.4.5.4 System software maintenance

According to ISO/IEC 14764, the software maintenance is the modification of a software product after delivery to correct faults, to improve performance or other attributes, or to adapt the product to a modified environment.

The PCS software maintenance includes the installation of patches, upgrades or new releases of firmware.

4.4.6 Spare capacity of the system

4.4.6.1 General

After the final configuration of the system, this should have a spare capacity in order to allow adding functionalities or upgrade the system over the time. The spare capacity is installed and

immediately available with a simple system re-configuration. No additional piece of hardware or software is required to use the spare capacity of the system.

The desired or needed spare capacity of the system should be specified in the design of the system for the different sub-systems (memory, I/O, terminations, etc.).

4.4.6.2 Spare PCU memory

The user should indicate the spare PCU memory needed after the final configuration of the system. The spare memory gives the possibility to expand and change the control software in the future. The spare memory is expressed as a percentage of the total available memory installed (including PROM, EPROM, RAM, and any other type of storage available), and strictly depends on the implemented software applications.

4.4.6.3 Expandability of control room communications

Expandability of CR communications defines the possibility of adding new communication ports and devices to the control network. The added communication ports can be configured without modifications in the existing software and with no need of re-configuring the entire communication network.

4.4.6.4 Expandability of field communications

Expandability of field communications defines the possibility of adding new field devices to the PCS through the existing communication ports. When necessary, the added communication ports can be configured without modifications in the existing software and with no need of re-configuring the entire communication network.

4.4.6.5 Field device expandability

Field device expandability is the possibility of adding new field devices to the existing communication fieldbus(es) or the possibility of adding new field devices to the I/O cards. The maximum number of field devices that can be added to the PCS without any hardware intervention should be indicated. Also as a percentage of the existing devices.

4.4.6.6 Available room for PCS expansions

It should be specified the amount of room that should remain available after the PCS completion. Available room is indicated as a percentage of used space:

- inside the control cubicle, for adding new devices inside;
- in the cabinet room, for adding new control cabinets.

4.4.7 Safety

4.4.7.1 General

The concept of functional safety and the associated requirements relating to a PCS are addressed in IEC 61508 and more specific indications for process industries are given in IEC 61511. Requirements related to functional safety should be specified according these standards.

Each safety-related function has an associated Safety Integrity Level (SIL), which is defined by engineers according to the risks resulting from the function failure. The calculation of SIL requires performance based data for each item composing the safety loop, namely: sensors, logic solver, actuators. The typical logic of a safety loop is in the form: if <variable x is higher than X> then <open valve Y>, or similar. The SIL is associated with the Probability of Failure on Demand (PFD) or the frequency of dangerous failures of a given safety function.

4.4.7.2 Safety Instrumented Systems (SIS)

In a complex process, safety cannot be achieved with simple logic and the actuation of a single device. If a potentially hazardous event occurs, a number of actions shall be performed in a fixed sequence. Safety Instrumented Systems (SIS) are designed to implement the required functionality with the required integrity (as defined by the desired SIL). Safety Instrumented Systems come in different forms such as Emergency Shutdown Systems (ESD), Fire and Gas Systems (F&G), leakage detection systems, Burner Management System (BMS), etc.

Generally, SIS are functionally separated from the Basic Process Control System (BPCS), but parts of the systems may be common, as Figure 6 shows:

a) BPCS and SIS are separated, and data are exchanged through a serial link. A Bridge may be necessary if protocols are different or for separating the two systems;

b) as a), with the data exchange based on conventional signals (contacts and/or 4 mA - 20 mA);

c) BPCS and SIS are parts of a common PCS. A physical separation is possible (different cubicles), but the operating environment is common;

d) common: a common PCS performs both the basic control functions and the safety related functions;

e) separated: no interaction, either physical or logical, exists between BPCS and SIS.

The selection between the possible architectures comes from the requirements to achieve the required SIL. User should specify the basic architecture of the SIS, if any.

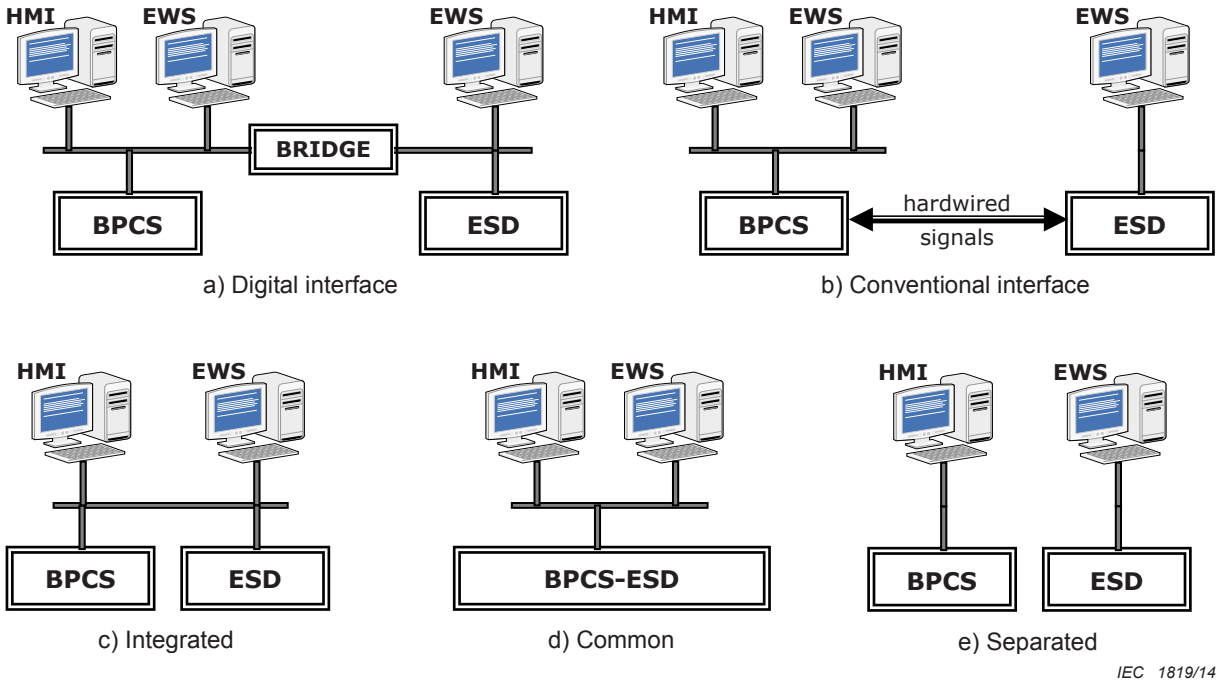

Figure 6 – Architectures of BPCS and ESD

4.4.7.3 Safety requirements

The SIL necessary to assure safety of a given process is the result of an activity of Risk Analysis, and it is outside the scope of this document. A safety-related function that operates continuously is characterised by the Average Probability of Failure per Hour of operation (PFH), while a function that triggers only in case a given event occurs is characterised by the

Probability of Failure on Demand (PFD). IEC 61508 specifies the values of PFH and PFD for the four levels of SIL, as summarized in Table 20.

Table 20 – PFD and PFH related to SIL

Safety Integrity Level (SIL)	Average Probability of Failure on Demand (PFD_{AVG})	Average Probability of Failure on Hour (PFH_{AVG})
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

Users shall ensure that the required SIL of each safety-related function, and hence of each SIS, is properly determined and that the determination is carried out by an appropriate person or organization.

4.5 Input/Output specifications

4.5.1 General

The considered types of Input/Output are: conventional analog I/O (i.e., 4 mA - 20 mA, 0 V - 10 V, etc.), digital I/O, Hart I/O and fieldbus. For each type of I/O, the user should specify the resolution, the accuracy and the repeatability.

According to IEC 60050, the following definitions apply:

- resolution (for measurement): smallest change in the measurand, or quantity supplied, which causes a perceptible change in the indication;
- resolution (for analog converters): the maximum capability of a system that is used to convert an analog signal into a proportional digital value. Generally, resolution is expressed in bits, from which the actual resolution may be determined;
- accuracy: the ratio of error to the full-scale output or the ratio of the error to the output, as specified, expressed as a percentage or the error in terms of the relevant engineering units;
- repeatability (cfr. ISA-37.1-1975 (R1982)): the ability of a transducer to reproduce output readings when the same measurand value is applied to it consecutively under the same conditions and in the same direction.

The user/engineer should specify the input/output characteristics in accordance with the technical definitions of the following subclauses. Annex E may be used as a guidance.

4.5.2 Conventional Input/Output

4.5.2.1 General

Technical requirements and tests for conventional input/output ports and devices are reported in IEC 61131-2. The following subclauses describe the typical parameters the user should specify in the technical requirements of a PCS.

4.5.2.2 Digital Input

The specification of the digital inputs may include:

- the rated input voltage (e.g., 24 V d.c.) and current (e.g., 10 mA);
- the sampling interval (fixed or variable) and whether interrupts on state change are employed the local status display of the inputs;

- the electrical insulation between inputs and between inputs and any earth/power supply potential referencing;
- the insulation level (e.g., 1 kV d.c.);
- whether the field contact is energized from the digital input or is externally powered.

4.5.2.3 Digital Output

The specification of the digital output may include:

- the type of output: static or relay;
- the connected load, e.g., solenoid valves, contactors, lights, etc.;
- the rated output voltage (e.g., 24 V d.c.);
- the rated output current (permanent and short time);
- the local display of outputs (e.g., LED);
- the electrical insulation between inputs and between inputs and any earth/power supply potential referencing;
- the insulation level (e.g., 1 kV);
- whether the digital output is energized from the field device or is self-energized.

4.5.2.4 Analog Input

The specification of the analog input may include:

- the type of inputs, i.e., thermo-couple, RTD (2-3-4 wires), 4 mA - 20 mA (active and/or passive[2]);
- the reverse polarity protection;
- the electrical insulation between inputs and between inputs and any earth/power supply potential referencing;
- the insulation level (e.g., 500 V d.c.);
- the sampling interval (fixed or variable);
- the number of bits used for ADC;
- any filtering and whether integration time is used (e.g., 16,7/20 ms).

4.5.2.5 Analog Output

The specification of the analog output may include:

- the type of output, e.g., 4 mA - 20 mA, ± 10 V, 0 V - 5 V, etc.;
- the resolution (or the number of conversion bits);
- the electrical insulation between outputs and between outputs and any earth/power supply potential referencing;
- the insulation level (e.g., 500 V d.c.);
- the individual output protection with fuse;
- whether the analogue output is energized from the field device or is self-energized.

4.5.3 Input/Output from/to Smart Devices

It is common practice to use Smart Devices, such as instruments and actuators. In such cases, the analogue input/output signals are generally in the form defined in 4.5.2.3 and

---

2 Active means that the PCS powers the current loop. Passive means that the loop is powered from the field instrument or an external power source.

4.5.2.4, but often with additional encoded information (e.g., HART). Making use of the additional encoded information requires additional equipment or suitably enhanced I/O equipment.

4.5.4 Serial connection to Remote I/O

The user specifies if a serial connection is used for connecting the Remote I/O and the controllers. The serial connection may be either a standard IEC 61158 fieldbus or a proprietary protocol.

4.5.5 Hot-swap

The concept of Hot-Swap is defined in 4.4.2.3. Hot-swap for I/O cards or modules should be specified separately, considering the higher stress and rate of failure of these devices.

4.5.6 Module diagnostic

The PCS monitors the operating status of each I/O card or module. Both normal and abnormal operation, i.e., faults or withdrawal, are displayed on the HMI.

4.5.7 Input validation

There are many forms of input signal validation that can be applied; examples include inappropriate combinations of separate valve open and valve closed digital inputs, analogue signal out of range, analogue signal rate of change and the use of multiple field devices to make the same measurement. Any required signal validation should be described in the PCS specification.

4.5.8 Read-back function

Analogue and digital outputs of the PCS are sent back to input cards to implement validation logic. For example, this function may be used to verify the emission of open/close commands or the value of emitted set points.

4.5.9 Forced output

Each digital and/or analogue output is forced to a pre-defined value, settable either by channel or by card, on PCS start-up and in the case of detected faults or abnormal operation. This is sometimes achieved by a watchdog function removing motive power from individual outputs or output cards.

4.5.10 Special inputs

Specific requirements for inputs different from the usual ones are to be specified.[3]

4.5.11 Intrinsically safe I/Os

If the PCS is requested to operate into Zone 0 or Zone 1 (IEC 60079-10),the I/O cards are certified as Intrinsically Safe (Ex ia as per IEC 60079-11).

4.5.12 Monitoring functions

The input cards and any associated additional wiring or end-of-wire equipment are designed to detect the most common failures in field, i.e., open or broken circuit.

---

[3] Fieldbus communication is in the scope of 4.8.

4.6 Software requirements

4.6.1 General

In a PCS, the system database provides the information needed by various system transactions (functions) to perform their tasks. Input data comes from the field devices (sensors, transmitters, switches, etc.) via the controller's data acquisition interfaces, from supervisory control systems (PC, DCS, PLC), via external controller links, and from other controllers via inter-controller connections. Output data are directed to field control and indication devices, supervisory systems, and other controllers.

The system database is a real-time database, i.e., it should provide a predictable response time to guarantee the completion of time-critical transactions.

The user/engineer should specify the software requirements in accordance with the technical definitions of the following subclauses. Annex F may be used as a guidance.

4.6.1.1 Physical layout of database (implementation)

The system database may have two possible physical layouts:

- distributed database: data are distributed across multiple physical locations. The control of the entire database is under a central Database Management System (DBMS) that has the role of coordinating all the data files;
- concentrated database: all the data are stored into a central database, i.e., all the records are recorded on an unique machine (server, possibly functionally redundant) and can be accessed by the Database Management System (DBMS).

4.6.1.2 Compatibility with external database

If the system database should guarantee the compatibility and the connection with other databases, it is necessary to specify which are the databases that have access or that are accessed by the system database.

4.6.1.3 Type of software

The software for implementing the database can be a commercial product or a proprietary one. If some specific requirement or constraint applies, it is necessary to specify the required programming language for the database. Normally, this choice is up to the PCS manufacturer.

4.6.2 Cyber security

4.6.2.1 General

In a modern PCS, the role of computers and digital communication is crucial and the cyber security is a critical goal that may influence the dependability of the overall system. This subclause deals with the measures that can be implemented in order to protect the entire system from cyber attacks.

The concept of cyber security and the associated requirements relating to a PCS are addressed in the IEC 62443 series. Requirements related to cyber security should be specified according these standards.

More specific references could be the IEC 62443-2-1 (requirements on the security management system) and IEC 62443-3-3 (requirements on system security capabilities).

4.6.2.2 Security software requirements

The software tools needed to guarantee the operating system integrity of the machine installed in the PCS should be specified.

Typical software security tools are:

- antivirus: this tool detects and removes the viruses eventually found on the machine;
- firewall: this tool protects files and databases from being improperly accessed through open networks;
- SSL and IIS: levels of security should be implemented for applications with internet access. This will restrict the levels of access that are available to remote users. This security form is available by means of Internet Information Server (IIS), Secure Socket Layers (SSL), digital certificates and encryption;
- digital certificates: for the machines that can access the internet, another layer of security can be added by means of the digital certificates. A digital certificate involves an encrypted digital identification to secure the authenticity of the parties involved in the transaction.

4.6.2.3 Access management

Different users groups may have different rights of access to the resources. An account is defined by means of a user name and its password.

The requested specifications are:

- the maximum number of accounts that can access to the system;
- the definition of the user groups (e.g., administrator, programmer, maintenance, etc.) and the trustee rights assigned at each user group (Read, Write, Open, Create and Delete);
- the definition of the functions and applications that can be accessed by each user groups.

4.6.2.4 Login and password security

Login and password security are closely connected. To log into a file server, a person should correctly enter a valid user name, which is unique to each user of the network, followed by a correct password for that user account.

Login security depends on account restrictions, which include password restrictions and time restrictions that determine when a user can log in.

The functionalities that can be requested are:

– account restriction:
  - ability to invalidate temporarily an account without deleting it;
  - set an expiration date on any user account;
  - limit the number of concurrent logins a user can perform.

– password restrictions:
  - define a special set of information that can not appear in the password (e.g., the middle name or the surname of the user, the birth date, etc.) and the minimum length of the password;
  - periodic password changes;
  - support for dynamic passwords: each time users log in, they have a new password. To accomplish this, users have a personal remote password generator device and special software shall be run on the network.

4.6.3 Software simulator

4.6.3.1 General

A software simulator is a program that allows the user to observe an operation through simulation without actually running the real system.

The simulation software allows a better debugging performance in a simulation environment before the downloading the program or the configuration on the real system. In this subclause, the possible simulators that can be required for a PCS are listed.

4.6.3.2 Simulator of the control logic

The implemented control logic can be tested on the configuration PC or workstation. The simulator allows testing the logics without having the hardware connected. The simulation is useful for checking the overall consistency of the control logic program and the effect of modifications.

4.6.3.3 On-line debugging

On-line debugging allows checking and correcting a program during its execution even if other programs are running simultaneously. Debug allows detecting and correcting any program faults.

4.6.3.4 Simulator of the I/O

The I/O simulator allows simulating the operation of the I/Os. In this case, it is possible to force the values of the I/Os in order to check a specific logic or control loops.

4.6.4 Remote supervisory functions

A remote computer with the proper trustee rights can supervise the PCS. Remote supervision extends to displays, tags or variables, control-loop setting, alarm acquisition, etc. User should specify the functions the remote supervision can carry on.

4.6.5 On-line documentation

The documentation, including the technical documentation on the components of the PCS, are in file formats and are available to be browsed by a computer. It is possible to access them directly from a PC.

4.7 Human Machine Interface (HMI)

4.7.1 General

In this guideline, the term HMI refers to the displays, computers and software that serve as an interface with a PCS. The HMI has three primary functions:

- provide visualization of process parameters and methods with which to control the process;
- provide alarms and indications to the operator that the process is outside limits or behaving abnormally or that the PCS has detected faults or failures;
- provide a method to allow the operator to understand where the process is going and how fast (trending functionality).

The user/engineer should specify the Human Machine Interface in accordance with the technical definitions of the following subclauses. Annex G may be used as a guidance. It is important to distinguish the functions of the HMI in the control room and the local operator interface. The user should specify the hardware and software requirements for both the locations, where relevant.

4.7.2 Control room HMI hardware – architecture

The minimum set of information for the control room hardware definition includes:

- the required number of operator stations;

- the number of workstations and monitors making up each operator station;
- the required number of monitors;
- the functionality, features and facilities of each operator station;
- special display, e.g., overhead projectors, wide screens, etc. (if any);

The control room architecture can be effectively specified by a layout drawing.

4.7.3 Control room HMI hardware – operator stations

The specifications of the HMI operator stations include:

- Processor type;
- Memory RAM;
- Type and size of hard disk;
- Operating system;
- Communication ports;
- Connection and communication with external data storage;
- Keyboards, number pads, mice, tracker balls and other entry devices.

The control room network can be effectively specified by a drawing of the hardware architecture.

4.7.4 Control room HMI hardware – monitors

The specifications of the HMI monitors include:

- Screen technology used;
- Screen size;
- Screen resolution;
- Number of multiple monitors on the console;
- Number of supported colours.

4.7.5 Control room HMI hardware – special displays

Special displays are specified according to the required technology, e.g., overhead projectors, plasma or LED large screens, back projectors, etc.

4.7.6 Control room HMI software

The specifications for the HMI software include several families, as listed hereinafter:

– Technology
  - Operating system, e.g., Windows XP;
  - Supports ActiveX controllers;
  - Based on OPC architecture;
  - VBA client or server;

– Architecture
  - Primary application:
    a) Single station;
    b) Single server;
    c) Multiple-server;
    d) Multiple client;
  - Tag-based HMI;

- Maximum number of servers/clients;
- Supporting of thin clients;
- Supporting of multi-user;
- Supporting of remote configuration at runtime;
- Redundancy of data server;
- Redundancy of HMI server;

– Features for navigation and displaying
- Animation;
- Number of pages to be created;
- Number of pages displayed;
- Visibility;
- Colour;
- Horizontal and vertical position;
- Horizontal and vertical slider;
- User practices and policies with respect to colors, icons, templates and format layout;
- Supporting of remote alarming; i.e., e-mail or SMS.

4.7.7 Requirements for Local Operator Interface

It should be defined how many Local Operator Interface (LOI) should be installed in the system. For each LOI, the requirements that should be defined are:

- Panel technology: touch or function key;
- Special keyboard: buttons for operating process parameters, buttons for calling up displays and buttons for alphabet keys;
- Screen size;
- Screen resolution in pixels;
- Supported operating system;
- Supported communication ports;
- the functionality, features and facilities of each Local Operator Interface.

4.7.8 Alarm management

4.7.8.1 General

The alarm management system of the PCS supports the selection of the events to be considered as alarms, the setting of the alarm priorities, the acknowledgement procedures, etc.

The alarm management should be designed in order to avoid a flood of alarms prompted to the operator interface. The alarm management should be designed following some rules:

- simple alarms to show location and recommended action;
- access to appropriate screen views should be quick, decisive and with minimum keystrokes;
- handling techniques should be implemented, in particular priority settings and annunciating;
- techniques should be easily reconfigurable;
- the user should specify the technical requirements of the alarm management system according to the item defined in the next subclause.

4.7.8.2 Types of alarms

Different types of alarm can be set or defined. Typical alarm functions include:

- absolute threshold: a given parameter reaches a certain set threshold;
- single delta: an additional alarm notifies that the signal continues to rise. The signal has overcome a certain percentage above the defined threshold;
- repetitive delta: there is an alarm at every selected change beyond that has been selected for the single delta alarm;
- rate of change: there is an alarm if there is a rapid rate of change of the variable even though a threshold has not been passed. The rate of change is normally expressed either in per units per second or per cent per time;
- return to normal: when required, the operator needs to be notified when a parameter returns to normal, not just when that parameter goes into an alarm;
- time delay: some parameters are relatively unstable, or just continually fluctuate, such as pressures and flows. Often it is useful to set some time delay on those alarms to act as a dead band, so that a spike does not trip an unnecessary alarm;
- “snooze” alarm: the “snooze” alarm re-alarms if the conditions persists beyond some selected time after acknowledging. In some cases, this type of alarm can be set to acknowledge itself if the condition clears;
- hysteresis alarm: a hysteresis alarm has different thresholds in each direction, up or down. Used much like the time delay, this dead band reduces unnecessary alarms in dynamically active fluids.

4.7.8.3 PCS failure alarms

Any failure or abnormal operation of the PCS should be signalled to the operator with an indication of the alarm severity. Alarm severity indicates the order in which users should handle that event relative to alarms of other severities. Levels of severity can help schedule the maintenance and repair activities, and are an important feature of self-diagnostic messages (system alarms). Severity is not relevant to process alarms.

A possible definition of severity levels is:

- down: no response from the monitored entity or device;
- high (critical): alarm condition that seriously impairs service and requires immediate correction;
- medium (advisory): alarm condition impairing service but not seriously;
- low (journal): alarm condition that does not currently impair service, but the condition needs to be corrected before it becomes more severe.

The definition of severity levels should be based on a combination of the effect of the detected PCS failure or abnormal operation and the consequences or potential consequences for the plant and process operation.

4.7.8.4 Alarm priority level

Alarm priority indicates the urgency of operator response, i.e., seriousness of consequences and allowable response time. Four levels of priority are defined[4]:

- Highest: immediate operator action. Endangerment of personnel, catastrophic equipment failure/environmental impact, unit shutdown or shutdown of other units imminent;
- High: rapid operator action required. Unit shutdown possible. Partial shutdown has occurred. Highest priority alarm possible;

---

4 See ANSI/ISA 18.2 or IEC 62682 (in preparation).

- Medium: prompt operator action required. High-priority alarm possible. Off-spec or production loss imminent;
- Low: operator investigation of sub-optimal operation required. Medium priority alarm possible.

User should specify if the PCS alarm management system shall support the priority levels.

4.7.8.5 Alarm grouping

Alarms can be organized into groups according to geographical or functional criteria. The purpose of alarm grouping is to allow the operator to quickly recognize patterns in a sequence of alarms and to find-out the PCS components or functions or the plant and process areas or machines involved.

4.7.8.6 Alarm acknowledgment

All the alarms should be acknowledged by the operator(s). For each alarm, according to its group, severity and priority, a sequence of actions that indicate that the alarm has been recognized is defined. Different acknowledgment sequences can be implemented according to ANSI/ISA-18.1-1979 (R2004).

4.7.8.7 “Smart” alarming/alarm hiding

To reduce the effort for the operator to understand the causes of an abnormal event, alarms that are obvious or redundant should not be displayed. The PCS supports “smart” alarming whereby pre-defined alarms can be automatically hidden to the operator on the occurrence of specific process or plant conditions.

The system should provide tools and capability for easy configuration of which alarms will be “hidden” based on plant state or process condition.

Hidden alarms are not presented to the operator on the standard alarm displays or on process graphics, but their occurrence is recorded in the event history. A “hidden alarm” display will be provided which lists all of the alarms that are currently hidden from the operator.

4.7.8.8 Alarm annunciation

Alarm annunciation is the capacity of the system to notify the alarms to the operators. The annunciation process can include, for example:

- Activation of an external audible alarm or lights;
- Activation of the internal PC audio card (i.e., to play .wav files);
- Updating an alarm display with the current alarm;
- Updating an alarm overview screen to indicate the occurrence of an alarm in a specific process area / display;
- Printing the alarm message on an alarm printer;
- Any graphic object associated with the alarm point will change colour, shape, appear, disappear, etc. as configured.

4.7.8.9 Alarm summary display lists

A summary of the alarms could be useful, and it can include:

- Active (Standing) Process Alarms;
- Cleared Process Alarms;
- Acknowledged Process Alarms;

- Active (Standing) System Alarms;
- Cleared System Alarms;
- Acknowledged System Alarms;
- Alarm History;
- Operator Action List;
- Suppressed (Locked) Alarm List;
- Hidden Alarm List;
- Alarm Frequency Display (Hit) List.

Accessing an alarm summary display from any other display should require the minimum number of operator actions.

Multi-page displays may be used. If so, it should be possible to page forward or backward. The display should list alarms in tabular format in order of occurrence.

4.7.9 Events management

4.7.9.1 General

Event is a change of the status of any variable in the process. Typical events are:

- change of status of selected digital inputs;
- reaching a pre-defined threshold for selected analog variables;
- commands from operator, etc.

An event may start or not a control action.

The user should specify the required functions for event management according to the following subclauses.

4.7.9.2 Sequence Of Events (SOE)

Time resolution is the minimum time by which two events should be separated in order that the corresponding time tags are different. Separating capability is the minimum time by which two events should be separated such that the sequence of their occurrence is determined correctly. Time resolution cannot be shorter than separating capability, and it is normally specified.

If events generated by other systems are to be included in the SOE, issues such as clock synchronization and passing of time stamps need to be considered.

4.7.9.3 Integration of SOE with third parties systems

If the data processed by the SOE can be accessed by other applications and/or systems, it is necessary to specify them and if some particular driver or communication interface is required (i.e., OPC Alarm and Event).

4.7.9.4 Types of events

The types of events are classified according to their sources:

- operator: operator changes such as set points changes, control output changes or controller mode changes. Reactions to alarms, such as acknowledgments;
- alarm: each alarm presents always two events: switching into alarm condition and switching out of alarm condition;

- process: the events are related to the state of the monitored system, such as protecting events, quality changes in the measures, etc.

4.7.10 Historical archiving

4.7.10.1 General

Events can be archived in the historical database, which means recording in a centralised machine a particular signal from the controller where the event was either generated or acquired from a sensor. Only some events should be archived in the historical database. The following subclauses report the methods for archiving and the specifications to define data that should be archived.

4.7.10.2 Archiving method

The historical database can store events according to different methods:

- cyclically: there is a fixed collection frequency, that is used to sample the data;
- on variation: on/off data are stored only when they change their status; analogue data are stored when their value changes more than a given threshold;
- on event: data are collected on the basis of a triggering event or interrupt.

The number of events to archive should be defined.

4.7.10.3 Back-up of the archives

The historical database is a critical part of the entire PCS and for such a reason a back-up media should be chosen. The back-up archives are important to restore the data after a disaster or after the corruption of some data.

In order to select the best back-up archive for the historical database, the following features should be defined:

- hardware type of back-up depository;
- expected life span of the back-up;
- software tools to manage the back-up and restoration processes and the back-up files;
- frequency of the back-up (daily, weekly, monthly, etc.);
- format required for the stored data.

4.7.11 Trend and statistics management

4.7.11.1 General

For process or plant supervision and control, HMI should show both instantaneous and recorded values in different format according to process requirements. Next subclauses define the most important features to specify.

4.7.11.2 Features of the trend

The main features defining the trending application are:

- number of traces available per screen/window;
- type of variables to trend;
- min/max sampling rate;
- the span time or the total capacity of data displayed on the same trend.

4.7.11.3 Analog values trending

The trend of an analog value can include the following features:

- current value;
- average;
- minimum;
- maximum;
- standard deviation.

4.7.11.4 Discrete value trending

The trend of a discrete value can include the following features:

- current state;
- start state;
- transition count;
- statistics.

4.7.11.5 Trend navigation requirements

The trend system should have some requirements for a effective and user-friendly navigation:

- panning: moving “back and forth” along the same time divisions within a much longer trend than fits in a single screen;
- time-zoom: moving to different time divisions;
- trace-zoom: moving to different ranges for each trace.

In addition to the function of panning and zooming, cursor may have additional functions, such as:

- time/date of placement;
- value/state of intersected traces;
- tags and titles of all traces viewed;
- select area of zoom for more detail.

4.8 Communication requirements

4.8.1 General

Communication plays a key role in a PCS. Different communication networks co-exist in a PCS, each one with specific features and requirements. Usually communication networks may be divided into three or four levels according to the technology used. Figure 7 schematically shows these alternatives.

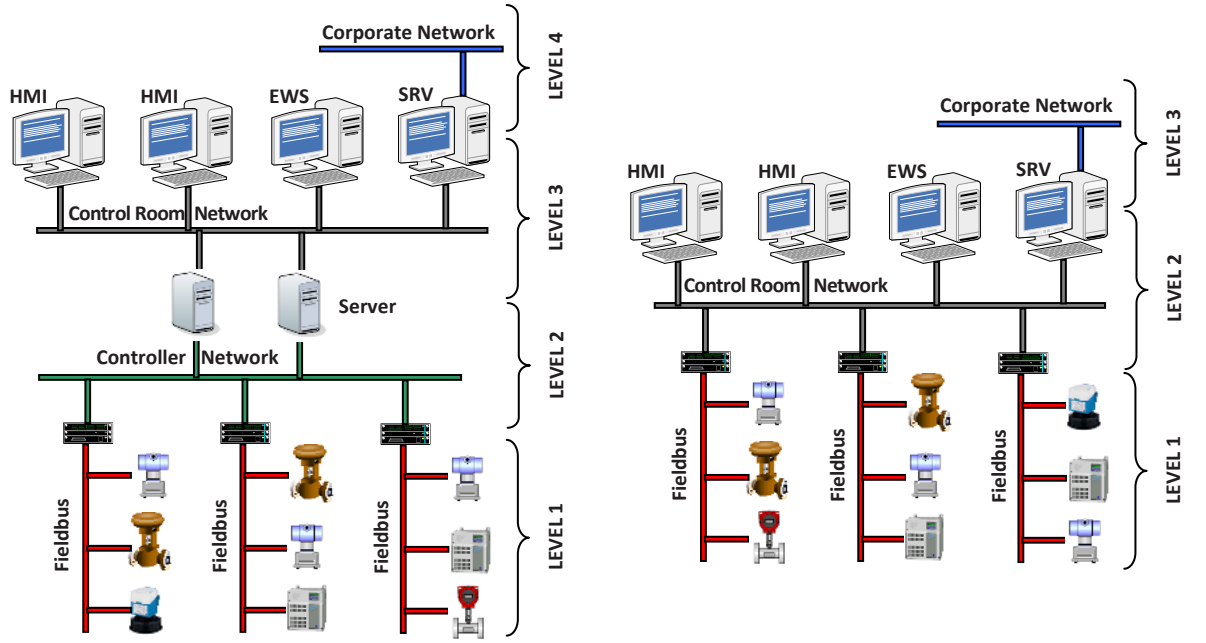

Figure 7 – Communication networks in a PCS

The levels of communication networks are:

- fieldbus: it manages the communication between the field devices and the controllers. It has tight real-time requirement of high predictability and reliability. Field networks are in the scope of the family of standards IEC 61158 that include all the most popular fieldbus;
- controller network: it guarantees horizontal communication between controllers and between controllers and server(s). It may be based either on proprietary protocols or based on a standard fieldbus (IEC 61158) or network (IEEE 802-Ethernet);
- control room network: it supports the interface between the controllers (or the servers in case of 4-level systems) and the workstations in control room. This network is today mostly based on IEEE 802-Ethernet;
- corporate network: it allows the communication between the PCS and the ICT environment of the company and remote. This interface may support ERP or MES systems.

The user/engineer should specify the communication requirements in accordance with the technical definitions of the following subclauses. Annex H may be used as a guidance.

4.8.2 Field equipment serial communication

According to the IEC 61158 family, the principal requirements for field equipment serial communication that should be specified are:

– the physical layer: copper, IEC 61158-2, fiber optic or wireless;
– communication profile family (CPF) according to IEC 61784, such as
  - CPF 1 – Foundation Fieldbus (include High Speed Ethernet);
  - CPF 2 – ControlNet (include Ethernet/IP v1);
  - CPF3 – Profibus (include Profinet);
  - CPF4 – P-NET;
  - CPF5 – WorldFIP;
  - CPF6 – Interbus;

- CPF7 – SwifNet;

– number of devices connected to the network;
– installation in hazardous areas;
– redundancy of the communication medium required;
– maximum distance between the field device and the controller;
– whether galvanic isolation is required between parts of the network.

4.8.3 Controller network

The requirements for the controller network that should be specified are:

– type of protocol used:
  - a standard of the IEC 61158 family;
  - standard Ethernet protocol IEEE 802;
  - proprietary protocol;
– the physical layer;
– installation in hazardous areas;
– redundancy of the communication medium required;
– maximum distance of the connection;
– whether galvanic isolation is required between parts of the network.

4.8.4 Control room network

The requirements for the controller network that should be specified are:

– type of protocol used:
  - standard Ethernet protocol IEEE 802;
  - proprietary protocol;
– the physical layer;
– redundancy of the communication medium required;
– maximum distance of the connection;
– whether galvanic isolation is required between parts of the network.

4.8.5 External link

The external link allows the implementation of communication with different networks, for example between the control room network and the corporate network (refer to Figure 7).

The user should specify:

– the networks that need the communication link;
– the security level needed;
– the need for firewall;
– the need for antivirus.

4.8.6 Communication interfaces

Several communication networks can exist within a PCS, thus it is necessary to define the interfaces between the networks and between different systems.

The user should specify:

- the communication protocol between the networks that exchange data and information;
- the quantity of data exchanged;
- the refresh time required for using valid data;
- the physical medium of connected networks;
- the desired security level.

A communication interface allows sharing and passing data and information between different communication systems that use different physical medium and/or different data structure. In this way, the data can be moved across the entire PCS communication system and they can be used where they are need.

4.8.7 Communication with ERP system

Enterprise resource planning (ERP) integrates internal and external management information across an entire organization, embracing finance/accounting, manufacturing, sales and service, etc. ERP systems automate this activity with an integrated software application. Its purpose is to facilitate the flow of information between all business functions inside the boundaries of the organization and manage the connections to outside stakeholders.

The ERP needs to communicate and exchange data with the control system, where the productivity data are generated. ERP systems connect to real-time data and transaction data in a variety of ways:

- Direct integration: ERP systems connectivity (communications to control system) as part of their product offering. This requires the suppliers to offer specific support for the control system that their customers operate.
- Database integration: ERP systems connect to control system through staging tables in a database. Control systems deposit the necessary information into the database. The ERP system reads the information in the table.
- Enterprise appliance transaction modules (EATM) – These devices communicate directly with control system and with the ERP system via methods supported by the ERP system. EATM can employ a staging table, Web Services, or system-specific program interfaces (APIs).
- Standard protocols – Communications drivers are available for control system and separate products have the ability to log data to staging tables. Standards exist within the industry to support interoperability between software products, the most widely known being OPC.

4.8.8 Communication with Manufacturing Execution System (MES)

MES is a production scheduling and tracking system used to analyse and report resource availability and status, schedule and update orders, collect detailed execution data such as material usage, labour usage, process parameters, order and equipment status, and other critical information. It accesses bill of material, routing and other data from the base ERP system and is typically the system used for real-time shop floor reporting and monitoring that feeds activity data back to the base system.

The methods for connecting with the MES are:

- Direct integration: MES systems connectivity (communications to control system) as part of their product offering. This requires the suppliers to offer specific support for the control system that their customers operate;

- Database integration: MES systems connect to control system through staging tables in a database. Control systems deposit the necessary information into the database. The MES system reads the information in the table.
- Standard protocols – Communications drivers are available for control system and separate products have the ability to log data to staging tables. Standards exist within the industry to support interoperability between software products, the most widely known being OPC.

4.9 Required performances

4.9.1 General

This subclause specifies the performances the PCS should guarantee for satisfying the requirements of the controlled process. The focus is mainly on the time performances that the system or a part of it should meet for satisfying the requirements.

The user/engineer should specify the required performances of the PCS in accordance with the technical definitions of the following subclauses. Annex I may be used as guidance.

4.9.2 Time performances of the PCS

4.9.2.1 Absolute time synchronisation

Evaluation of process data requires that all the components of the process control system work synchronously, allowing messages to be assigned in a correct time sequence.

To ensure that the time base of the PCS is unique, time synchronization should be configured for each controller and workstation.

Time synchronization is based either on a centralised architecture, or on a distributed one. In case of centralised architecture, one “time master” sends a synchronisation signal to all the “time slaves”. On the contrary, in distributed architectures each node has its own synchronisation device (i.e., GPS).

User should specify the type of required architecture and the number of nodes to synchronise.

4.9.2.2 Requirements of the time stamping

The capacity of discriminating events very close in time is defined in IEC 60870-4 that is specific for Telecontrol Equipment and Systems but can be applied to any PCS. The basic concepts and definitions are:

- discrimination capacity: the minimum time between two events that allows to detect their proper sequence;
- time resolution: the minimum time between two events so that their time tags are different;
- suppression time: period of time when the acquisition of changes of status is suppressed to avoid errors due to noise or bounces;
- acquisition time: the minimum duration of a status variation to be detected and properly elaborated.

The required time resolution and discrimination capacity of the PCS can be defined using the classes defined in Table 21.

Table 21 – Time resolution and discrimination capacity

	Classes				
Discrimination capacity		SP1	SP2	SP3	SP4
	ms	< 50	< 10	< 5	< 1
Time resolution		TR1	TR2	TR3	TR4
	ms	<1 000	< 100	< 10	< 1

4.9.2.3 Overall response time of the PCS

The maximum overall response time of the PCS should be indicated. The overall response time of the PCS measures the time elapsed between the input of a command through a given HMI device, its transmission to the field device, its physical execution, and its feedback on the HMI. The time of the physical execution of a command does not depend on the PCS, so it should not be considered in the evaluation of the response time.

4.9.2.4 Switch-over time for redundant CPUs

The switch-over time is the time necessary to switch, after a fault, from the faulted CPU to the back-up CPU and for normal functionality to be resumed.

The maximum admissible switch-over time should be defined.

4.9.3 Controller performances

4.9.3.1 General

In this subclause, all the requirements that a controller should satisfy in order to accomplish its functions are reported, with a focus on the time constraints.

4.9.3.2 Real-time constraints for control functions

Some functions shall satisfy real-time constraints, i.e., the function shall perform within a determined time span.

Real-time requirements can be divided into two categories according to the effects on the system deriving from missing a deadline:

- hard real-time: a specific function shall be performed at a given time that cannot be missed without losing the performance. This means that if a function is defined hard real-time, the completion of this function after the scheduled deadline is useless or, worst, may cause a critical failure of the system;
- soft real-time: the function has to be performed within a specific deadline. If the function is not completed within the deadline, the system can work but in degraded conditions.

For each function with real-time constraints, the following features have to be addressed:

– type of real-time constraint: hard or soft;
– deadline that shall be satisfied for the completion of the real-time function.

4.9.3.3 Controller cyclic time

The controller cyclic time is the period needed by a controller to execute all the control programs, including the update of the involved I/O signals. The maximum admissible controller cyclic time should be specified. In case the controller supports multitasking, the maximum time considers all the tasks running simultaneously.

4.9.4 HMI performances

4.9.4.1 General

This subclause focuses on the performances needed by the graphical interface and the main attention is on the time requirements that the HMI application needs to satisfy.

4.9.4.2 Time constraints for display

The HMI functions that require an execution within a specified time delay should be defined. The maximum time to show-up a display variation should be specified, starting from the physical variation of the driving signal.

4.9.4.3 Call-up time

The call-up time of an HMI page is the time necessary to up-load, open and fully populate a standard graphic page after the operator request.

The maximum admissible call-up time should be specified.

4.9.4.4 Video screen page refresh time

The refresh time is an indication on how often the displayed page is updated, i.e., the frequency of acquisition of data displayed on the HMI pages.

The maximum admissible refresh time should be specified.

4.9.5 Plant Asset Management

4.9.5.1 General

PAM is a bunch of software applications aimed at improving the plant operation. PAM normally includes functions for: performance indexes calculation and monitoring, balance-of-plant calculation, statistical analysis, predictive maintenance algorithms, etc. The core of PAM is a historical database that stores process and diagnostic data for the high-level algorithms.

4.9.5.2 Generation of maintenance requests

PAM generates diagnostic messages and maintenance requests by means of specific algorithms applied to the historical data-base populated with the information collected by the PCS. The basic information from the field devices, the required functions, and the communication technology should be declared in the PCS technical requirements.

4.9.5.3 List of asset alarms

PAM may generate different levels of warning or alarms, related both to device diagnostic and to plant or sub-systems performances. A preliminary list of these alarms should be defined in the PCS technical requirements.

4.9.5.4 Definition of the system benchmarks

A benchmark is the application of a set of programs, events, or operating conditions, in order to assess the relative performance of a PCS, normally by running a number of standard tests and trials against it. A benchmark may be defined both for the complete system and for specific sections or functions. The definition of a benchmark is linked with the FAT (see 4.11), even if it is not dependent on the specific application. Normally benchmarks are proposed by third party associations or groups.

4.9.5.5 Definition of the Key Performance Indicator (KPI)

Key Performance Indicators are quantifiable measurements, agreed to beforehand, that reflect the critical success factors of an organization. They will differ depending on the organization and on the type of industry to which will be applied. KPI may be calculated either by the ERP system or by the PCS.

Where KPIs are required, the algorithm and parameters required need to be defined.

4.9.5.6 Definition of the OEE index

Overall Equipment Effectiveness (OEE) is one of the most important Key Performance Index in manufacturing and batch processes. OEE is the measurement of overall output efficiency of a given process in relation to availability, performance, and quality. By calculating OEE, losses in productivity can be accurately pinpointed while also providing information on where improvement efforts should be based.

OEE breaks the performance of a manufacturing unit into three separate but measurable components: Availability, Performance, and Quality:

$$\text{OEE} = \text{Availability} \times \text{Performance} \times \text{Quality}$$

Each component points to an aspect of the process that can be targeted for improvement:

- availability: this portion of the OEE index represents the percentage of scheduled time that the operation is available to operate;
- performance: this portion of the OEE index represents the speed at which the work centre runs as a percentage of its designed speed;
- quality: this portion of the OEE index represents the good units produced as a percentage of the total units started.

4.10 Life cycle support

4.10.1 General

The technical and commercial support provided by the manufacturer is important for the whole life cycle of the PCS. The user/engineer should specify the life cycle support for the PCS in accordance with the technical definitions of the following subclauses. Annex J may be used as a guidance.

4.10.2 Training of the personnel

The training of the personnel is intended for creating the needed skills for the user personnel on the new or updated PCS. The training is identified by the following characteristics:

– required level of training, according the function of the personnel (e.g., operation, maintenance, engineering, project team, etc.);
– number of person/hours needed for the training;
– number of people to be trained;
– place of the training:
  - on the user's system after or during the commissioning and start-up;
  - on the manufacturer facilities on the user system, even if in a demo layout;
  - on the manufacturer facilities using a demo unit, different from the real system that will be installed in the user's plant.

4.10.3 Technical support for operation

The user should define the type of support he needs after the commissioning of the system.

The type of support includes the following aspects:

– Engineering: any activity devoted to the modification of the system, both in terms of hardware and software configuration, such as design modification, configuration changes, adding new I/O points, etc.

– Service: type of support guaranteed by the manufacturer when a failure or malfunction of the system appears. Should be identified by a SLA (Service Level Agreement), which is a part of a service contract and it is sometimes used to refer to the contracted delivery time or performance. The user should specify some minimum levels of intervention that should be guaranteed, e.g., time to answer to a call, time for intervention, etc.

– Spare parts: the required amount of hardware spare parts and the time interval, in years, during which the spare parts of the system are available should be identified for the main parts of the PCS.

– Support: the type of guaranteed support should be required or declared according to the type of failure or malfunction:

  - On-site;
  - On-line;
  - Daytime or 24/7.

4.10.4 Warranty

The warranty begins after the final acceptance by the customer. The warranty is expressed in terms of years of support, both for hardware and software failures or malfunctions. The warranty should be specified with an agreed SLA.

In some cases, the contract includes an availability period that is a period during which the system should not experience failures. If any failure or malfunction occurs during the availability period, the manufacturer has to restore the system to full operation within a contractual amount of time, i.e., one hour, otherwise the counter of availability period is reset. In these cases, warranty starts after the availability period expiration.

4.10.5 Software upgrade

The user should require a service of software upgrade from the contractor, covering operating system, contractor's system software and application software. This service includes any new release (major or minor, depending on the contract) or patch that is developed by the contractor during the service period.

The software upgrade service can be limited to the sole delivery of the new releases and patches, or can also include the installation of the upgraded software on the system itself.

The contractor should notify the user about the compatibility of all major official Operating System patches or security updates with the system. If required, the user should include in the software upgrade service also the installation of the official Operating System patches and security updates.

4.10.6 References of the supplier

4.10.6.1 General

The contractor should provide additional information regarding the references of the company. This information is useful for knowing the background, the core competencies and the experience of the company in similar applications. The contractor should declare limitations in supplying services or products in some countries (if applicable).

4.10.6.2 Core competencies

The user should identify which are the core competencies needed by the contractor.

4.10.6.3 Application experience

The contractor should provide a description of its knowledge and experience in the relevant areas, backed up by references to and descriptions of relevant previous work.

4.10.6.4 References for similar applications

The user should request a list of similar applications, already successfully done by the contractor, relevant sub-contractors or OEM.

The number of required references is set by the user.

The reference list should report:

- Name of the company that bought the application;
- Reference person(s) to contact;
- Year of installation;
- Type of system provided.

4.11 FAT specification

4.11.1 General

The specification of general definitions and methodologies for assessing the properties of a PCS are in the scope of the group of standards IEC 61069. Definitions and general procedures of the Factory Acceptance Test (FAT), Site Acceptance Test (SAT), and Site Integration Test (SIT) for a PCS are described in IEC 62381.

The following subclauses show the items that are to be specified for defining the functions to test and the level of tests during the FAT. A clear definition of the coverage of the FAT and of the depth of the tests is mandatory in the PCS technical requirements, since it represents an important item to be accounted by suppliers. SAT and SIT are not in the scope of this document.

A scheme for a FAT specification is described in the following subclauses. The user/engineer should specify the FAT level and coverage in accordance with the technical definitions of the following subclauses. Annex K may be used as a guidance.

4.11.2 FAT for Hardware Supply

For the FAT, the entire system is set up and tested with all its components, unless otherwise agreed. The hardware test has three main goals:

- verify that the scope of supply complies with the specifications (bill of materials);
- verify that all the components are operating as expected;
- verify that the system as a whole works as expected.

4.11.2.1 Check of the scope of supply

This section of the FAT has the scope of verifying the following items:

- all the drawings are both legible and understandable;
- all the manuals are available;

- visual inspection of the whole supply;
- check of the identification tags and labels;
- check of the terminations and cables labelling;
- spare capacity.

4.11.2.2 Check of the device operation

This section of the FAT has the scope of verifying the following items:

- power and grounding connections are as per drawings (if necessary, measurements are carried out);
- auxiliary devices are operating (fans, service plugs, internal lighting, etc.);
- power supply units operation, including test of back-up power supply (if any);
- check of the connections of peripherals and their operation;
- verify the operation of the control room bus (if any) in its complete configuration;
- check the operation of redundant equipment by unplugging redundant modules (if any).

4.11.3 FAT for Application Software

A PCS is composed of several interacting sub-systems. There are several ways for splitting a PCS into sub-systems, depending on the specific goal. For testing the application software, it is convenient to split the PCS into physical sub-systems that can be associated to the level of depth of the FAT, as shown in Figure 8. The FAT required level should be clearly stated in the PCS technical requirements.

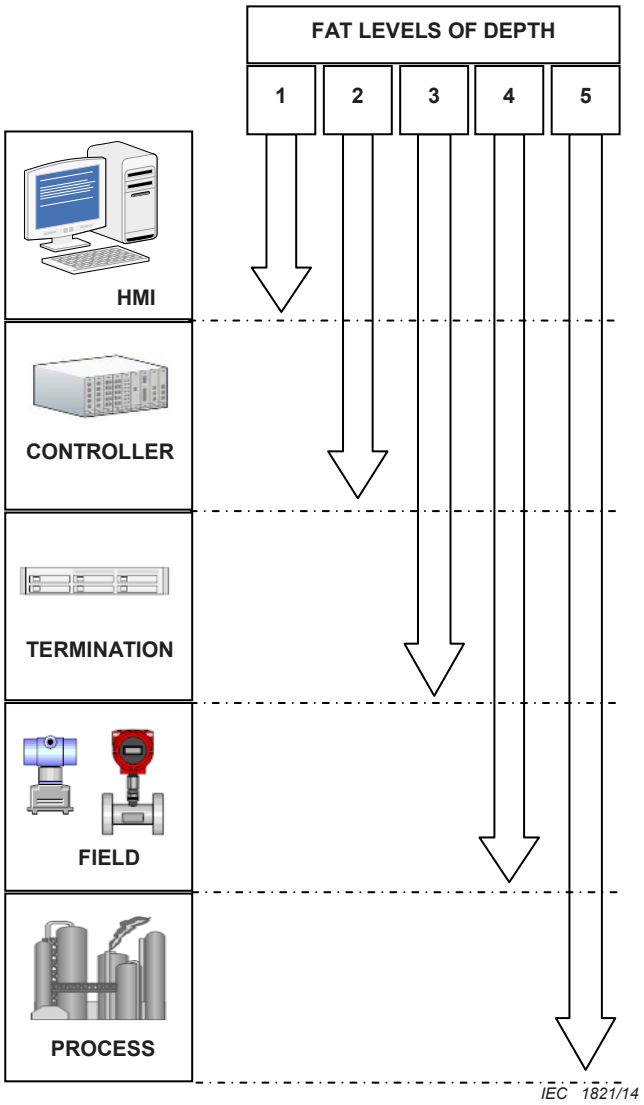

Figure 8 – FAT levels of depth

The meaning of the five levels is explained below:

Level 1: the goal of a Level 1 test is to check the HM interface, the software structure, the database completeness. No external mock-up is required.

Level 2: with a Level 2 test, the programs implemented in the controllers or CPUs that compose the PCS are checked into details. The input/output of each program are simulated with proprietary software that allows the engineers to force the required variables in the system database. To achieve realistic feedbacks from the plant, simulation software may be used. Small adaptations of the software under test may be required during testing.

Level 3: Level 3 tests verify the integrity and the correctness of the input/output connections starting from the terminations strips of the PCS cabinets. Conventional I/Os (4 mA - 20 mA, dry contacts, etc.) are forced via a hardware simulator, while fieldbus links are simulated using fieldbus-specific cards. Level 3 and Level 2 procedures may be mixed to check separately the application software and the communication from/to the field. Fieldbus loading measurements are possible.

Level 4: this level extends the tests from the cabinet terminations to the field. Level 4 is mainly useful with integrated PCSs, with fieldbus link to the field. Intelligent Field Devices are either physically present, or individually simulated using fieldbus-specific emulation cards.

Level 5: a simulation software is used to calculate the process feedback starting from the test architecture defined al Level 4. The degree of accuracy of the process models should be adequate for the purpose of testing the application software.

A further data that should be defined in the PCS technical requirements is the coverage of the FAT. In many applications, it may be not necessary for the testing to cover the complete PCS, and a partial test is sufficient. Other functions may require comprehensive testing. A sample of specification table is reported in Table 22.

Table 22 – Example of FAT Specification

Function	Level	Coverage	Notes
System configuration	1	100 %	
Graphic screens	1	100 %	
Control loops and sequences	3	30 %	Only critical functions
Safety related functions	4	100 %	
Interface with external systems	4	5 %	Only selected data
Redundancy check	3	100 %	
Alarm check	2	5 %	
Advanced control functions	5	100 %	Specific

Partial tests during the software design stage may be agreed for preliminary check of commonly used functions, such as:

- frequently recurrent functions (e.g., motor and valve control);
- standards for sequence control functions (e.g., recipe control);
- complex control functions.

Annex A
(informative)

Table for “System Architecture”

The following table contains guidance suggestions, which should be expanded and adapted as required. The table should not be used without reference to the documented clauses of this Guideline. The table may not address every possible PCS technical specification requirement.

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**SYSTEM ARCHITECTURE**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
4.1.2	TECHNOLOGY AND SCOPE OF THE PCS				
	- TECHNOLOGY				
	- FUNCTION				
4.1.3	BASIC ARCHITECTURE				
4.1.4	TOTAL NUMBER OF I/OS				
	- DIGITAL INPUT NO.				
	- DIGITAL OUTPUT NO.				
	- PTC INPUT NO.				
	- ANALOGUE INPUT NO.				
	- ANALOGUE OUTPUT NO.				
	- INTELLIGENT FIELD DEVICE NO.				
4.1.5	NUMBER OF TAGS				
	- TAGS FOR PROCESS CONTROL				
	- TAG FOR ADDITIONAL FUNCTIONS				

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**SYSTEM ARCHITECTURE**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
4.1.6	NUMBER OF CONTROL LOOPS				
4.1.7	REFERENCE STANDARDS AND MARKING				
	SPECIAL REQUIREMENTS				
4.1.A					
4.1.B					

Annex B
(informative)

Table for “Installation Environment”

The following table contains guidance suggestions, which should be expanded and adapted as required. The table should not be used without reference to the documented clauses of this Guideline. The table may not address every possible PCS technical specification requirement.

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**INSTALLATION ENVIRONMENT**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
4.2.2	CLIMATIC CONDITIONS				
	- FIELD DEVICE INSTALLATION				
	- CONTROL ROOM INSTALLATION				
	- OUTDOOR INSTALLATIONS				
	- STORAGE ENVIRONMENT				
4.2.3	POWER SUPPLY				
4.2.3.1	AC POWER SUPPLY				
	- VOLTAGE CLASS				
	- FREQUENCY LASS				
	- HARMONIC CONTENT				
	- SWITCHING TIME				
4.2.3.2	DC POWER SUPPLY				
	- VOLTAGE CLASS				
	- RIPPLE CLASS				

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**INSTALLATION ENVIRONMENT**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
	- SWITCHING TIME				
	- EARTH CONNECTION				
4.2.4	EMC REQUIREMENTS				
4.2.4.2	IMMUNITY				
4.2.4.2.1	ELECTROSTATIC DISCHARGE				
	- FIELD INSTALLATION				
	- CONTROL ROOM				
4.2.4.2.2	RADIATED RF ELECTROMAGNETIC FIELD				
	- FIELD INSTALLATION				
	- CONTROL ROOM				
4.2.4.2.3	ELECTRICAL FAST TRANSIENT				
	- FIELD INSTALLATION				
	- CONTROL ROOM				
4.2.4.2.4	SURGE				
	- FIELD INSTALLATION				
	- CONTROL ROOM				
4.2.4.2.5	CONDUCTED DISTURBANCES				
	- FIELD INSTALLATION				
	- CONTROL ROOM				
4.2.4.2.6	POWER FREQUENCY MAGNETIC FIELD				

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**INSTALLATION ENVIRONMENT**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
	- FIELD INSTALLATION				
	- CONTROL ROOM				
4.2.4.2.7	PULSE MAGNETIC FIELD				
	- FIELD INSTALLATION				
	- CONTROL ROOM				
4.2.4.2.8	DAMPED MAGNETIC FIELD				
	- FIELD INSTALLATION				
	- CONTROL ROOM				
4.2.4.2.9	VOLTAGE DIPS AND SHORT INTERRUPTIONS				
	- FIELD INSTALLATION				
	- CONTROL ROOM				
4.2.4.3	EMISSION				
	- FIELD DEVICES				
	- CONTROL ROOM				
4.2.5	MECHANICAL VIBRATIONS				
	- VIBRATIONAL SEVERITY				
	- TIME DURATION CLASS				
4.2.6	CORROSIVE AND EROSIVE INFLUENCES				
4.2.6.2	- CLASS FOR GASES AND VAPOURS				
4.2.6.3	AEROSOLS				

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**INSTALLATION ENVIRONMENT**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
	- CLASS FOR OILS IN AIR				
	- CLASS FOR SEA SALT MISTS				
4.2.6.4	SOLID SUBSTANCES				
	- TYPE OF SOLID SUBSTANCES				
	- FREQUENCY OF OCCURRENCE				
	- AVERAGE PARTICLE SIZE				
	- CONCENTRATION				
4.2.6.5	LIQUIDS				
	- TYPE OF LIQUID SUBSTANCES				
	- FREQUENCY OF OCCURRENCE				
	- ELECTRICAL CONDUCTIVITY				
4.2.7	LIGHTNING PROTECTION ZONE				
	- FIELD INSTALLATION				
	- CONTROL ROOM				
4.2.8	HAZARDOUS AREA				
4.2.8.1	EX AREA CLASSIFICATION				
4.2.8.1.2	EXPLOSIVE GAS ATMOSPHERE				
	- FIELD INSTALLATION				
	- CONTROL ROOM				
4.2.8.1.3	COMBUSTIBLE DUSTS				
	- FIELD INSTALLATION				

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**INSTALLATION ENVIRONMENT**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
	- CONTROL ROOM				
4.2.8.2	*EQUIPMENT CLASSIFICATION*				
	- FIELD INSTALLATION				
	- CONTROL ROOM				
4.2.9	*EARTH CONNECTION*				
	CLASS OF THE DEVICE				
	SPECIAL REQUIREMENTS				
4.2.A					
4.2.B					

Annex C
(informative)

Table for “System characteristics”

The following table contains guidance suggestions, which should be expanded and adapted as required. The table should not be used without reference to the documented clauses of this Guideline. The table may not address every possible PCS technical specification requirement.

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**SYSTEM CHARACTERISTICS**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
4.3.2	SYSTEM SCALABILITY				
4.3.3	SYSTEM EXPANDABILITY				
4.3.4	INTEGRATION OF THE SYSTEM				
	- EXISTING SYSTEMS				
	- EXISTING SUB-SYSTEMS				
	- PACKAGES FROM DIFFERENT SUPPLIERS				
	- SUB-SYSTEMS FROM DIFFERENT SUPPLIERS				
4.3.5	SYSTEM CONFIGURATION				
	- ON-LINE				
	- OFF-LINE				
	- CONFIGURATION IN SIMULATION MODE				
	- GRAPHICAL RESOURCES FOR SUPPORTING ENGINEERING				
4.3.6	AUTOMATIC GENERATION OF DOCUMENTATION				

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**SYSTEM CHARACTERISTICS**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
4.3.7	PROGRAMMING LANGUAGES				
	- STANDARD IEC 61131-3 PROGRAMMING LANGUAGES				
	- SFC PROGRAMMING TOOL SUPPORTED				
	- CFC PROGRAMMING TOOL SUPPORTED				
	- DEFINITION OF CUSTOM FUNCTION BLOCK				
	- BATCH PROGRAMMING TOOL				
	- MULTITASKING OPERATING SOFTWARE FOR CONTROLLER				
	- ADVANCED PROCESS CONTROL (APC) SUPPORTED				
4.3.8	*PCS LOCALISATION*				
	SPECIAL REQUIREMENTS				
4.3.A					
4.3.B					

Annex D
(informative)

Table for “System dependability”

The following table contains suggestions, which should be expanded and adapted as required. The table should not be used without reference to the documented clauses of this Guideline. The table may not address every possible PCS technical specification requirement.

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**SYSTEM DEPENDABILITY**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
4.4.2	RELIABILITY				
	- SYSTEM SELF-DIAGNOSTIC				
	- SINGLE COMPONENT FAULT TOLERANCE				
	- HOT-SWAPPABLE COMPONENTS				
4.4.3	AVAILABILITY				
	- ADMISSIBLE DEGRADATED CONDITIONS				
	- STAND-BY CONFIGURATIONS				
	- PROTECTION ACTION IN FAIL SAFE MODE				
4.4.4	REDUNDANCY CRITERIA				
	- CONTROLLERS				
	- CONTROL ROOM NETWORKS				
	- FIELD COMMUNICATION NETWORKS				
	- POWER SUPPLY MODULES				

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**SYSTEM DEPENDABILITY**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
	- DATABASE				
	- HMI MONITORS/CLIENTS				
	- I/O CARDS				
4.4.5	MAINTAINABILITY				
	- GENERATION OF MAINTENANCE REQUESTS				
	- STRATEGIES FOR MAINTENANCE				
	- SOFTWARE MAINTENANCE				
4.4.6	SPARE CAPACITY OF THE SYSTEM				
	- CPU MEMORY				
	- PROCESSING TIME CPU				
	- EXPANDABILITY OF CONTROL ROOM COMMUNICATIONS				
	- EXPANDABILITY OF FIELD COMMUNICATIONS				
	- FIELD DEVICE EXPANDABILITY				
	- CABINETS AVAILABLE ROOM				
4.4.7	SAFETY				
	- EMERGENCY SHUT-DOWN				
	- SAFETY REQUIREMENTS				
	SPECIAL REQUIREMENTS				
4.4.A					
4.4.B					

Annex E
(informative)

Table for “Input/Output specification”

The following table contains suggestions, which should be expanded and adapted as required. The table should not be used without reference to the documented clauses of this Guideline. The table may not address every possible PCS technical specification requirement.

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**INPUT/OUTPUT SPECIFICATION**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
4.5.2	CONVENTIONAL I/O				
4.5.2.2	DIGITAL INPUT				
	- RATED INPUT VOLTAGE				
	- INPUT DELAY				
	- LOCAL STATUS DISPLAY				
	-ELECTRICAL INSULATION				
	- INSULATION LEVEL				
4.5.2.3	DIGITAL OUTPUT				
	- TYPE OF OUTPUT				
	- CONNECTED LOAD				
	- RATED OUTPUT VOLTAGE				
	- PERMANENT RATED OUTPUT CURRENT				
	- SHORT TIME RATED OUTPUT CURRENT				

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**INPUT/OUTPUT SPECIFICATION**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
	- ELECTRICAL INSULATION				
	- INSULATION LEVEL				
4.5.2.4	ANALOG INPUT				
	- TYPE OF INPUT				
	- REVERSE POLARITY PROTECTION				
	- ELECTRICAL INSULATION				
	- INSULATION LEVEL				
4.5.2.5	ANALOG OUTPUT				
	- TYPE OF OUTPUT				
	- RESOLUTION				
	- ELECTRICAL INSULATION				
	- INSULATION LEVEL				
	- INDIVIDUAL OUTPUT PROTECTION				
4.5.3	I/O FROM/TO SMART DEVICE				
4.5.4	SERIAL CONNECTION TO REMOTE I/O				
4.5.5	HOT-SWAP OF I/O				
4.5.6	MODULE DIAGNOSTIC				
4.5.7	INPUT VALIDATION				
4.5.8	READ-BACK FUNCTION				
4.5.9	FORCED OUTPUT				
4.5.10	SPECIAL INPUTS				

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**INPUT/OUTPUT SPECIFICATION**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
	- ENCODER				
	- INTERRUPT				
	- FAST COUNTER				
	- TEMPERATURE				
	- OTHER – SPECIFY				
4.5.11	INTRINSICALLY SAFE I/OS				
4.5.12	MONITORING FUNCTIONS				
	SPECIAL REQUIREMENTS				
4.5.A					
4.5.B					

Annex F
(informative)

Table for “Software requirements”

The following table contains guidance suggestions, which should be expanded and adapted as required. The table should not be used without reference to the documented clauses of this Guideline. The table may not address every possible PCS technical specification requirement.

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**SOFTWARE REQUIREMENTS**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
4.6.1	SYSTEM DATABASE REQUIREMENTS				
	- PHYSICAL LAYOUT OF DATABASE				
	- COMPATIBILITY WITH EXTERNAL DATABASE				
	- TYPE OF SOFTWARE				
4.6.2	CYBER SECURITY				
4.6.2.2	SECURITY SOFTWARE REQUIREMENTS				
	- ANTIVIRUS				
	- FIREWALL				
	- PROTECTION WITH SSL AND IIS				
	- DIGITAL CERTIFICATES				
4.6.2.3	ACCESS MANAGEMENT				
	- NUMBER OF ADMITTED ACCOUNTS				
	- NUMBER OF DEFINED USER GROUPS				

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**SOFTWARE REQUIREMENTS**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
	- APPLICATIONS AND FUNCTIONS ACCESSIBLE FOR EACH USER GROUP				
4.6.2.4	LOGIN AND PASSWORD SECURITY				
	- ACCOUNT RESTRICTION				
	- PASSWORD RESTRICTIONS				
4.6.3	SOFTWARE SIMULATOR				
	- SIMULATOR OF THE CONTROL LOGIC				
	- ON-LINE DEBUGGING				
	- SIMULATOR OF THE I/O				
4.6.4	REMOTE SUPERVISORY FUNCTIONS				
4.6.5	ON-LINE DOCUMENTATION				
	SPECIAL REQUIREMENTS				
4.6.A					
4.6.B					

Annex G
(informative)

Table for “Human Machine Interface (HMI)”

The following table contains guidance suggestions, which should be expanded and adapted as required. The table should not be used without reference to the documented clauses of this Guideline. The table may not address every possible PCS technical specification requirement.

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**HUMAN MACHINE INTERFACE (HMI)S**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
4.7.2	CONTROL ROOM HMI HARDWARE – ARCHITECTURE				
	- NUMBER OF INSTALLED MACHINE				
	- NUMBER OF MONITORS				
	- FUNCTIONALITIES OF EACH MACHINE				
	- SPECIAL DISPLAY				
4.7.3	CONTROL ROOM HMI HARDWARE – OPERATOR STATIONS				
	- PROCESSOR TYPE				
	- MEMORY RAM				
	- TYPE AND SIZE HARD DISK				
	- OPERATING SYSTEM				
	- COMMUNICATION PORTS				
	- EXTERNAL DATA STORAGE				
4.7.4	CONTROL ROOM HMI HARDWARE – MONITORS				

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**HUMAN MACHINE INTERFACE (HMI)S**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
	- SCREEN TECHNOLOGY				
	- SCREEN SIZE				
	- SCREEN RESOLUTION				
	- NUMBER OF MULTIPLE MONITORS				
	- SUPPORTED COLOURS				
4.7.5	CONTROL ROOM HMI HARDWARE – SPECIAL DISPLAYS				
4.7.6	SOFTWARE SPECIFICATIONS				
	- TECHNOLOGY				
	- ARCHITECTURE				
	- FEATURES NAVIGATION AND DISPLAYING				
4.7.7	LOCAL OPERATOR INTERFACE				
	- PANEL TECHNOLOGY				
	- SPECIAL KEYBOARDS				
	- SCREEN SIZE				
	- SCREEN RESOLUTION				
	- SUPPORTED OPERATING SYSTEM				
	- SUPPORTED COMMUNICATION PORTS				
4.7.8	ALARM MANAGEMENT				
	- TYPES OF ALARMS				
	- ALARM SEVERITY				

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**HUMAN MACHINE INTERFACE (HMI)S**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
	- ALARM PRIORITY LEVELS				
	- ALARM GROUP				
	- ALARM ACKNOWLEDGMENT				
	- "SMART" ALARMING/ALARM HIDING				
	- ALARM ANNUNCIATION				
	- ALARM SUMMARY DISPLAY LISTS				
4.7.9	EVENTS MANAGEMENT				
	- SEQUENCE OF EVENTS (SOE)				
	- INTEGRATION OF SOE WITH THIRD PARTIES SYSTEM				
	- TYPES OF EVENTS				
4.7.10	HISTORICAL ARCHIVING				
	- ARCHIVING METHOD				
	- BACK-UP FOR THE ARCHIVES				
4.7.11	TREND AND STATISTICS MANAGEMENT				
	- FEATURES OF THE TREND				
	- ANALOG VALUES TRENDING				
	- DISCRETE VALUE TRENDING				
	-TREND NAVIGATION REQUIREMENTS				
	SPECIAL REQUIREMENTS				
4.7.A					

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**HUMAN MACHINE INTERFACE (HMI)S**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
4.7.B					

Annex H
(informative)

Table for “Communication requirements”

The following table contains guidance suggestions, which should be expanded and adapted as required. The table should not be used without reference to the documented clauses of this Guideline. The table may not address every possible PCS technical specification requirement.

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**COMMUNICATION REQUIREMENTS**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
4.8.2	FIELD EQUIPMENT SERIAL COMMUNICATION				
	- PHYSICAL LAYER				
	- COMMUNICATION PROFILES				
	- NUMBER OF CONNECTED DEVICES				
	- INSTALLATION IN HAZARDOUS AREAS				
	- REDUNDANCY OF THE COMMUNICATION MEDIUM				
	- MAXIMUM DISTANCE				
4.8.3	CONTROLLER NETWORK				
	- TYPE OF PROTOCOL USED				
	- PHYSICAL LAYER				
	- INSTALLATION IN HAZARDOUS AREAS				
	- REDUNDANCY OF THE				

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**COMMUNICATION REQUIREMENTS**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
	COMMUNICATION MEDIUM				
	- MAXIMUM DISTANCE				
4.8.4	CONTROL ROOM NETWORK				
	- TYPE OF PROTOCOL USED				
	- PHYSICAL LAYER				
	- REDUNDANCY OF THE COMMUNICATION MEDIUM				
	- MAXIMUM DISTANCE				
4.8.5	EXTERNAL LINK				
	- NETWORKS TO BE CONNECTED				
	- SECURITY LEVEL				
	- NEED OF FIREWALL				
	- NEED OF ANTIVIRUS				
4.8.6	COMMUNICATION INTERFACES				
	- COMMUNICATION PROTOCOLS OF THE CONNECTED NETWORKS				
	- QUANTITY OF EXCHANGED DATA				
	- REFRESH TIME				
	- PHYSICAL MEDIUM				
	- SECURITY LEVEL				
4.8.7	COMMUNICATION WITH ERP SYSTEM				
	- DIRECT INTEGRATION				
	- DATABASE INTEFGRATION				

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**COMMUNICATION REQUIREMENTS**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
	- EATM				
	- STANDARD PROTOCOLS				
4.8.8	COMMUNICATION WITH MANUFACTURING EXECUTION SYSTEM (MES)				
	- DIRECT INTEGRATION				
	- DATABASE INTEFGRATION				
	- STANDARD PROTOCOLS				
	SPECIAL REQUIREMENTS				
4.8.A					
4.8.B					

Annex I
(informative)

Table for “Required performances”

The following table contains guidance suggestions, which should be expanded and adapted as required. The table should not be used without reference to the documented clauses of this Guideline. The table may not address every possible PCS technical specification requirement

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		REQUIRED PERFORMANCES			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
4.9.2	TIME PERFORMANCES OF THE PCS				
4.9.2.1	ABSOLUTE TIME SYNCHRONIZATION				
	- NUMBER OF TIME MASTERS				
	- NUMBER OF TIME SLAVES				
	- TIME DISPLAYED IN LOCAL TIME				
4.9.2.2	TIME STAMP REQUIREMENTS				
	- DISCRIMINATION CAPACITY				
	- TIME RESOLUTION				
	- SUPPRESSION TIME				
	- ACQUISITION TIME				
4.9.2.3	OVERALL RESPONSE TIME OF THE PCS				
4.9.2.4	SWITCH-OVER TIME FOR REDUNDANT CPUS				
4.9.3	CONTROLLER PERFORMANCES				
	- REAL-TIME CONSTRAINTS FOR				

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**REQUIRED PERFORMANCES**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
	CONTROL FUNCTIONS				
	- CONTROLLER CYCLIC TIME				
4.9.4	HMI PERFORMANCES				
	- TIME CONSTRAINTS FO DISPLAY				
	- CALL-UP TIME				
	- VIDEO SCREEN PAGE REFRESH TIME				
4.9.5	PLANT ASSET MANAGEMENT				
	- GENERATION OF MAINTENANCE REQUESTS				
	- LIST OF ASSET ALARMS				
	-DEFINITION OF THE SYSTEM BENCHMARK				
	- DEFINITION OF THE KPI				
	- DEFINITION OF THE OEE INDEX				
	SPECIAL REQUIREMENTS				
4.9.A					
4.9.B					

Annex J
(informative)

Table for "Life Cycle Support"

The following table contains guidance suggestions, which should be expanded and adapted as required. The table should not be used without reference to the documented clauses of this Guideline. The table may not address every possible PCS technical specification requirement.

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**TECHNICAL AND COMMERCIAL SUPPORT**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
4.10.2	TRAINING OF THE PERSONNEL				
	- REQUIRED LEVEL OF TRAINING				
	- NUMBER OF PERSON/HOUR NEEDED				
	- PLACE OF TRAINING				
4.10.3	TECHNICAL SUPPORT FOR OPERATION				
4.10.4	WARRANTY				
4.10.5	SOFTWARE UPGRADE				
4.10.6	REFERENCES OF THE SUPPLIER				
	- CORE COMPETENCIES				
	- APPLICATION EXPERIENCE				
	- REFERENCES FOR SIMILAR APPLICATIONS				
	SPECIAL REQUIREMENTS				
4.10.A					

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**TECHNICAL AND COMMERCIAL SUPPORT**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
4.10.B					

Annex K
(informative)

Table for “FAT specifications”

The following table contains guidance suggestions, which should be expanded and adapted as required. The table should not be used without reference to the documented clauses of this Guideline. The table may not address every possible PCS technical specification requirement.

CUSTOMER					
PROJECT				PROJECT NO.	
PLANT/UNIT					
GROUP		**FAT SPECIFICATIONS**			
POS.	DESCRIPTION	REQUIREMENTS	W	VOTE	NOTES
4.11.2	FAT FOR HARDWARE SUPPLY				
	- CHECK OF THE SCOPE OF THE SUPPLY				
	- CHECK OF THE DEVICE OPERATION				
4.11.3	FAT FOR APPLICATION SOFTWARE				
	- LEVEL 1				
	- LEVEL 2				
	- LEVEL 3				
	- LEVEL 4				
	- LEVEL 5				
	SPECIAL REQUIREMENTS				
4.11.A					
4.11.B					

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™