

NIOEC-SP-70-08(2)							
DOCUMENT CODE						NO. OF PAGES: 58	
PLAN/PRJ/SUB	UNIT	PHASE	DISCIPLIN E	DOCUMENT TYPE	SERIAL NO.	REV. NO.	DATE
NIOEC	000	EG	IN	SP	7008	A0	APRIL, 2007



NATIONAL IRANIAN OIL REFINING & DISTRIBUTION COMPANY
NATIONAL IRANIAN OIL ENGINEERING
& CONSTRUCTION COMPANY

NIOEC SP

NIOEC SPECIFICATION
FOR
PROCESS CONTROL SYSTEM
(PCS)

SECOND EDITION

APRIL , 2007

THIS STANDARD IS THE PROPERTY OF NATIONAL IRANIAN OIL ENGINEERING & CONSTRUCTION COMPANY. IT IS CONFIDENTIAL AND ALL RIGHTS RESERVED TO THE OWNER. NEITHER WHOLE NOR ANY PART OF THIS DOCUMENT MAY BE DISCLOSED TO ANY THIRD PARTY, REPRODUCED, STORED IN ANY RETRIEVAL SYSTEM OR TRANSMITTED IN ANY FORM OR BY ANY MEANS WITHOUT THE PRIOR WRITTEN CONSENT OF THE NATIONAL IRANIAN OIL ENGINEERING & CONSTRUCTION COMPANY

IN THE NAME OF GOD**FOREWORD**

By their very nature, technical standard specifications are continuously subject to modifications and revisions. To strengthen their merit and usefulness, continuous improvements, addendum, deletion of disparate information and consequently provision of updated revisions are to be made in order to ascertain that such standard specifications meet the current requirements, inclusive of Iranian Petroleum Standards (IPS) and the recognized and acceptable national and international standards, as well as the optimal codes and practices based on the accumulated in-house know-how and plant knowledge and experiences.

However, in reality, due to several reasons, not to mention the complexity of the matter, the ultimate goal of continuous direct embedment of the required changes on the relevant standard specifications may be far reaching. Therefore, in the interim periods between the officially issued revisions, the required changes will appear in other documents related to the engineering and design work of the on going projects.

In response to the initiative of the Design Division of the Engineering and Construction Directorate, and considering that the task of the execution of several important and mega projects for the realization of the new oil refineries, pipelines and oil terminals as well as improvements of the existing facilities, has been assigned to NIOEC, it was decided to update the NIOEC Specifications and to issue new official revisions.

The Design Division of the Engineering and Construction Directorate was itself entrusted to carry out this important task, and as such by forming several special technical committees, working in close co-operation and cohesion and sharing their expertise and knowledge, the updated and revised NIOEC Specifications were successfully prepared and complied.

These Specifications are intended to be used for Oil Refineries, Distribution Depots, Oil Terminals, Pipelines and Pump Stations within NIOEC's projects, and have been proven to be of high value for such purposes. It must however be appreciated that these Specifications represent the minimum requirements and should in no way be interpreted as a restriction on the use of better procedures, engineering and design practices or materials.

We encourage and highly appreciate the users and other clear sighted and experts to send their comments on the Specifications to the Design Deputy of the Engineering and Construction Director of NIOEC for evaluation and consideration.

S. R. KASAEIZADEH


EXECUTIVE DIRECTOR

REVISION INDEX

REV. PAGE	1	2	3	4	5	REV. PAGE	1	2	3	4	5	REV. PAGE	1	2	3	4	5	REV. PAGE	1	2	3	4	5
1						26						51						76					
2						27						52						77					
3						28						53						78					
4						29						54						79					
5						30						55						80					
6						31						56						81					
7						32						57						82					
8						33						58						83					
9						34						59						84					
10						35						60						85					
11						36						61						86					
12						37						62						87					
13						38						63						88					
14						39						64						89					
15						40						65						90					
16						41						66						91					
17						42						67						92					
18						43						68						93					
19						44						69						94					
20						45						70						95					
21						46						71						96					
22						47						72						97					
23						48						73						98					
24						49						74						99					
25						50						75						100					

NOTES:

- 1) THIS SHEET IS A RECORD OF ALL REVISIONS TO THIS SPECIFICATION.
- 2) REMARKS RELATED TO EACH REVISION SHOW A BRIEF DESCRIPTION. THESE REMARKS SHALL BE INTERPRETED IN CONJUNCTION WITH THE REVISED TEXT MARKED BY REVISION NUMBERS.
- 3) WHEN APPROVED EACH REVISION SHALL BE CONSIDERED AS A PART OF THE ORIGINAL DOCUMENT.
- 4) NUMBER OF PAGES EXCLUDES THIS SHEET AND THE COVER SHEET.

5					
4					
3					
2					
1					
0	APRIL, 2007	ASHRAF NIA	ORDOOBADI	FARZAM	SAJEDI
REV.	DATE	PREPARED	CHECKED	APPROVED	AUTHORIZED



Documents

Document Sharing Hub

CONTENTS:	PAGE NO.
1. SCOPE.....	4
2. REFERENCES	4
3. UNITS.....	6
4. DEFINITIONS AND TERMINOLOGY	6
5. ABBREVIATIONS	8
6. PRODUCT HISTORY.....	8
7. CERTIFICATION AND APPROVALS	8
8. GENERAL SYSTEM REQUIREMENTS.....	9
8.1 Electrical Power.....	9
8.2 Environmental Data.....	9
8.3 Ingress Protection and Hazardous Area Classification	9
8.4 Electromagnetic Interference.....	9
9. SYSTEM DESCRIPTION.....	9
9.1 Configuration.....	9
9.2 PCS Architecture.....	10
9.2.1 Automation System	10
9.2.2 Use of Standard Products.....	10
9.2.3 Software Revision	10
9.2.4 Integrity of PCS	11
9.2.5 Reliability of PCS	11
9.2.6 Availability of PCS	11
9.2.7 PCS Redundancy	12
9.2.8 PCS Diagnostics.....	12
9.2.9 Scalability of PCS	13
9.2.10 PCS System Backup	13
9.2.11 PCS Battery back-up	14
9.2.12 PCS Connectivity.....	14
9.2.13 PCS Interface With Third Party Subsystems.....	14
9.2.14 PCS Spare Capacity	14
9.2.15 PCS Performance and Sizing	14
9.3 System Cabinets Mechanical and Electrical Design	17
9.3.1 Mechanical Design.....	17
9.3.2 Marshalling Cabinets.....	17
9.3.3 Electrical Design.....	18
9.3.4 Power Distribution Cabinet.....	20
9.3.5 System Electronic Modules Design and Construction	20
9.3.6 Cabinet and Station Grounding.....	21
9.3.7 Cabinet Smoke Detectors.....	21
9.3.8 Physical Installation of Foundation Fieldbus Devices	21
9.3.9 Power Supply Requirements	21
9.4 Equipment Maintenance.....	21
9.5 Inputs and Outputs	22
9.5.1 Traditional Input and Output.....	22
9.5.3 Manual Input.....	22
9.5.4 HART I/O.....	22
9.6 System Communication	22
9.7 Control and Data Handling.....	22
9.7.1 Calculations.....	22
9.7.2 Regulatory Control	22

9.7.3 Algorithms.....	23
9.7.4 Input Scanning.....	23
9.7.5 Control Loop Execution Frequency	23
9.7.6 Output Functions.....	23
9.7.7 Setpoint Clamps.....	23
9.7.8 Windup protection	23
9.7.9 Sequential Control.....	24
9.7.10 Sequence Language	24
9.7.11 Auto-tuning	24
9.7.12 Fuzzy Logic Control & Algorithms	24
9.7.13 Control Execution Monitoring.....	24
9.7.14 Predictive Maintenance Diagnostics.....	24
9.7.15 Loop Performance Monitoring	25
9.7.16 Process Simulation	25
9.8 Configuration and Database	25
9.8.1 Configuration.....	25
9.8.2 Configuration Tool.....	25
9.8.3 Tag Parameters	26
9.8.4 Engineering Units.....	26
9.8.5 Data Base, Reporting and Modification Utilities.....	26
9.8.6 System Access	27
9.9 Operator and Engineering Stations.....	27
9.9.1 General	27
9.9.2 Operator Stations	27
9.9.3 Engineering Stations	27
9.9.4 Monitors	28
9.9.5 Display Hardcopy	28
9.9.6 Printers.....	28
9.10 Displays and Graphics	28
9.10.1 Updating Capability	28
9.10.2 Displays and Graphics Access.....	28
9.10.3 Hierarchical Displays.....	28
9.10.4 Paging	28
9.10.5 Invalid Values	28
9.10.6 Faceplates.....	29
9.10.7 System and Diagnostic Displays.....	29
9.10.8 Graphics.....	30
9.11 Alarm and Message Handling.....	31
9.11.1 Categorizing Messages.....	31
9.11.2 Operator Actions	32
9.11.3 Engineer Actions	32
9.11.4 Process Alarm Initiation.....	32
9.11.5 System Alarm Initiation.....	33
9.11.6 Process and System Alarms History Retention	33
9.11.7 Process and System Alarms Audible Annunciation.....	33
9.11.8 Process and System Alarms Visible Annunciation.....	33
9.12 Diagnostics	33
9.13 Data Historization	34
9.14 Trend Displays.....	35
9.15 Reports	36
9.16 Availability.....	36
9.17 External Interface	37

9.17.1 Serial Interface - Subsystems	37
9.17.2 OPC Interface	37
9.18 Engineering Tools.....	37
9.19 Embedded Advanced Control Tools.....	37
9.20 Management Information System	38
9.21 Maintenance Planning and Scheduling System.....	38
9.22 Plant Start Up and Shutdown Monitoring System	38
9.23 Automatic Start-up Sequence System	38
9.24 Auto Tuner	39
9.25 Special Requirements.....	39
9.25.1 Multi-variable Constrained Model Predictive Control (MPC).....	39
9.25.2 Virtual Sensors and Quality Estimation	40
9.25.3 Control Simulation	40
10. NAMEPLATES	40
11. PAINTING AND RUST PREVENTION	41
11.1 Paint Specification.....	41
11.2 Paint Colour	41
11.3 Special Requirements.....	41
11.4 Surface Treatment.....	41
12. DOCUMENTATION	41
12.1 General	41
12.2 Design Documents	41
12.3 On line Documentation	41
13. INSPECTIONS AND TESTING	41
13.1 General	41
13.2 Factory Acceptance Test (FAT)	42
13.3 Test Completion.....	42
14. INSTALLATION, START UP AND COMMISSIONING	43
14.1 Installation	43
14.2 Checks	43
14.3 Power up.....	43
14.4 SAT	43
14.5 Commissioning	43
14.6 Test Equipment	43
14.7 Documents.....	43
15. SPARES PARTS SUPPLY	44
15.1 Construction, Pre-commissioning and Commissioning Spare Parts.....	44
15.2 Spare Parts for Two Years of Operation	44
15.3 Maintenance Tools	44
16. TRAINING	44
17. GUARANTEES	44
APPENDIX I.....	46
MAINTENANCE PLANNING AND SCHEDULING SYSTEM.....	46
APPENDIX II	55
PLANT START UP AND SHUTDOWN MONITORING SYSTEM	55
APPENDIX III.....	57
VENDOR'S DOCUMENT SUPPLY (VDC)	57

1. SCOPE

This specification defines NIOEC's minimum requirements for the design, manufacture, test and inspection of Process Control System (PCS).

Deviations from this specification will only be permitted on obtaining written approval from NIOEC.

2. REFERENCES

Throughout this specification the following dated and undated standards and codes are referred to. These referenced documents shall, to the extent specified herein, form a part of this specification.

For undated references, the latest edition of the referenced document (including any supplements and amendments) applies. For dated references, the edition cited applies.

The applicability of changes in the dated references that occur after the cited date shall be mutually agreed upon by NIOEC and the vendor /contractor.

BASEEFA	(BRITISH APPROVALS SERVICE FOR ELECTRICAL EQUIPMENT FOR FLAMMABLE ATMOSPHERES)	
CENELEC	(COMITÉ EUROPÉEN DE NORMALISATION ELECTROTECHNIQUE)	
EEC	(EUROPEAN ECONOMIC COMMUNITY)	
	EMC- Directive 89/336/EEC	"Electromagnetic Compatibility"
EN	(EUROPEAN STANDARDS)	
	EN 55022	"Specification For Limits And Measurement Of Radio Interference Characteristics Of Information Technology Equipment"
FM	(FACTORY MUTUAL)	
IEEE	(INSTITUTE OF ELECTRICAL & ELECTRONICS ENGINEERS)	
IEEE C37.90.1:	IEEE C37.90.1:	"Surge Withstand Capability (SWC) Tests"
IEC	(INTERNATIONAL ELECTRO-TECHNICAL COMMISSION)	
	IEC 60751	"Industrial Platinum Resistance Thermometer Sensors"
	IEC 61000-4-2, IEC 61000-4-3, IEC 61000-4-4	"Electromagnetic Compatibility (EMC)"
	IEC 61499-1, IEC 61499-2	"Function Blocks For Industrial Process Measurement And Control Systems"

	IEC 61158-2	"Foundation Fieldbus Standard For Use In Industrial Control Systems - Physical Layer Specification And Service Definition"
	IEC 61131-3	"Sequential Function Charts"
	IEC 60332	"Test On Electric Cables Under Fire Conditions"
	IEC 60529	"Classification Of Degree Of Protection Provided By Enclosures"
	IEC 60068	"Basic Environmental Testing Procedures"
	IEC-1000-4:	"Electromagnetic Compatibility For Industrial Process Measurement And Control Equipment"
	IEC-60-605:	"Equipment Reliability Testing"
ISO	(INTERNATIONAL STANDARD ORGANISATION)	
	ISO 9000	"Quality Systems"
ISA	(INSTRUMENTATION, SYSTEM, AUTOMATION SOCIETY OF AMERICA)	
ISA - S 5.1:	ISA - S 5.1:	"Instrument Symbols And Identifications"
ISA - S 5.2:	ISA - S 5.2:	"Binary Logic Diagrams For Process Operations"
ISA - S 5.3:	ISA - S 5.3:	"Graphic Symbols For Distributed Control/Shared Display Instrumentation, Logic And Computer Systems"
ISA - S 5.4:	ISA - S 5.4:	"Instrument Loop Diagrams"
ISA RP 55-1:	ISA RP 55-1:	"Hardware Testing Of Digital Process Computers"
ISA- S18.1:	ISA- S18.1:	"Annunciator Sequences And Specification"
ISA- S50.1	ISA- S50.1	"Compatibility Of Analogue Signals For Electronic Industrial Process Instruments"
LCIE	(LABORATORIE CENTRAL DES INDUSTRIES ELECTRICQUES)	
NFPA	(NATIONAL FIRE PROTECTION ASSOCIATION)	
	NFPA 70	"National Electrical Code"

NIOEC SP		(NIOEC SPECIFICATIONS)	
		NIOEC -SP-70-01	“Specification For Instrumentation”
		NIOEC-SP-00-10	“Specification For Units”
PTB		(PHYSIKALISCH TECHNISCHE BUNDESANSTALT)	
TIA		(TELECOMMUNICATION INDUSTRY ASSOCIATION)	
		TIA/EIA-485	“Electrical Characteristics Of Generators And Receivers For Use In Balanced Digital Multipoint Systems”
U.S. Military HNBK		U.S. MILITARY HANDBOOK	
U.S. Military Handbook -217	U.S. Military Handbook -217		“Reliability Prediction Of Electronic Equipment”
U.S. Military Handbook -472	U.S. Military Handbook -472		“Maintainability Prediction”
UL		(UNDERWRITERS’ LABORATORIES)	

3. UNITS

International System of Units (SI) shall be used in accordance with [NIOEC-SP-00-10](#), unless otherwise specified.

4. DEFINITIONS AND TERMINOLOGY

This section contains definitions for the terms as they are used in this document.

Advanced Control: Multi-variable, constraint and optimizing controls will be labelled advanced controls. Controls that fall into this category will be those that are supervisory in nature, i.e., they normally, but not always, output to the set points of other control loops rather than to the valves directly.

Auto Sense: Capability by the system to automatically detect and recognize any hardware upon addition to or removal from the system without user intervention.

Auxiliary System: A control and/or monitoring system that is stand-alone, performs a specialized task, and communicates with the automation system.

Call Up Time: The time between when the operator initially enters a display request and when all objects, lines, values (good or invalid), trends and other parts of the display have been fully presented to the operator.

Configurable: The capability to select and connect standard hardware modules to create a system; or the capability to change functionality or sizing of software functions by changing parameters without having to modify or regenerate software.

Configuration: The physical installation of hardware modules to satisfy system requirements; or the selection of software options to satisfy system requirements.

Cycle: The scanning of inputs, execution of algorithms and transmission of output values to devices.

Dead band: The range through which an input signal may be varied without initiating an action or observable change in output signal.

Discrete Control: Control where inputs, algorithms, and, outputs are based on logical (yes or no) values.

Equipment or System: Process Control System (hardware/software)

Faceplate: A graphic element that mimics the front panel of an analogue controller instrument, hardwired push-button or switch. The same is true for the graphical representation on the Operator Interface

Factory Acceptance Test (FAT): The final test at the vendor's facility of the integrated system being purchased.

Fieldbus Foundation: An independent, non-profit organization established to support standardization of the ISA/IEC Foundation Fieldbus standard.

Foundation Fieldbus: A Fieldbus that conforms to all Fieldbus Foundation specifications.

Foundation Fieldbus Segment: Grouping of Foundation Fieldbus devices connected to the automation system through an H1 interface module.

Foundation Fieldbus Trunk: Main path of a Foundation Fieldbus. The trunk line connects the system H1 module to power supply / power conditioning assembly.

Foundation Fieldbus Spur: A spur branches off the Foundation Fieldbus trunk.

Function Block Application Process: Fieldbus Foundation specification defining the plant or factory applications that perform one or more automatic monitoring and control functions.

H1: Wiring which connects Foundation Fieldbus devices used for control applications such as temperature, level, and flow control. Devices can be powered directly from the Foundation Fieldbus and will operate on existing wiring that was previously used for 4-20 mA devices.

Invalid Value: The state of a tag value which indicates that the quantity being measured or calculated is out-of-range, not measurable or calculable.

Logs: Files or printouts of information in chronological order.

Mode: Control block operational condition, such as manual, automatic, or cascade.

Module: An assembly of interconnected components that constitute an identifiable device, instrument, or piece of equipment. A module can be disconnected, removed as a unit, and replaced with a spare. It has definable performance characteristics that permit it to be tested as a unit.

OPC (Object Linking and Embedding for Process Control): Software application which allows bi-directional real time data flow between two separate applications. These applications may be running on the same or on separate servers.

Operational Data: The statistical data such as alarm limits, tuning parameters, and clamping values, as opposed to process data such as input values, output values and setpoints.

Operator Station: A station used by an operator to perform the functions required to monitor and control his assigned units.

Plant Area: The designated points (inputs, outputs, and calculated values) that belong to a geographic or functional section of a plant.

Plug and Play: The ability of hardware equipment to automatically identify itself to the system. When the equipment is powered up it is automatically assigned a unique identity without the need to set any dip switches.

Point: A process variable derived from an input signal or calculated in a process calculation.

Profibus: Open bus system, standardized in the German DIN 19 245.

Purchaser: In cases where this specification is part of a direct order, Purchaser shall mean the National Iranian Oil Engineering and Construction Company. Where this specification forms part of contract documents, Purchaser shall mean the Contractor. In references to inspection by Purchaser, when this

specification forms part of contract documents, this shall be construed to mean that NIOEC shall also have the right of inspection.

Redundant Configuration: A system/subsystem configuration that provides automatic switchover, in the event of a failure, without loss of a system function.

Regulatory Control: The functions of process measurement, control algorithm execution, and final control device manipulation that provide closed loop control of a plant process.

Reliability: The probability that the system or component will perform its intended function for a specified period of time.

Self-Diagnostic: The capability of an electronic device to monitor its own status and indicate faults that occur within the device.

Supervisory Control: Higher level control functions that interface with regulatory controllers and other automation system equipment to provide for integrated control.

System Access Restriction: Access control by key lock, password or other equivalent method.

System Alarm: Alarm that occurs as a result of an automation system hardware or software fault.

System Operating Software: The vendor's standard software that performs the basic functions of the system.

Tag: A collection of attributes that specify either a control loop or a process variable, or a measured input, or a calculated value, or some combination of these, and all associated control and output algorithms. Each tag is unique.

Tag ID: The unique alphanumeric code assigned to inputs, outputs, equipment items, and control blocks. The tag ID might include the plant area identifier.

Station: A set of electronic equipment including, at a minimum, one PC, one monitor and one keyboard.

5. ABBREVIATIONS

EMI: Electromagnetic Interference

ESD: Emergency Shut Down

FAT: Factory Acceptance Test

FSD: Functional Specification Document

ILD: Instrument Loop Diagram

MOV: Motor Operated Valve

MTBF: Mean Time Between Failures

PC: Personal Computer

PCS: Process Control System

RFI: Radio Frequency Interference

SAT: Site Acceptance Test

SOE: Sequence of Events

UPS: Un-interruptible Power Supply

6. PRODUCT HISTORY

Equipment shall be of the same model and design as used in similar plants and operating/ambient conditions with at least three (3) years of satisfactory operational history.

7. CERTIFICATION AND APPROVALS

The equipment shall bear CE marking in accordance with EMC- Directive 89/336/EEC, and the conformity certificates shall be provided.

The VENDOR shall also submit certificates/records of type test approval of the system, based on recognised national or international standards, which for CENLEC regulations shall be LCIE, TUV, PTB, BASEEFA and for NEC regulations shall be FM or UL.

8. GENERAL SYSTEM REQUIREMENTS

8.1 Electrical Power

The equipment will be powered from dual redundant Un-interruptible Power Supplies (UPS). The UPS will provide 230 VAC $\pm$ 2%, 50 Hz $\pm$ 1%. However all system modules shall be capable of operating during voltage variations up to $\pm$ 10% and frequency variations up to $\pm$ 5%.

The battery back up will be capable of sustaining all components of the system for a period of at least 30 minutes in the event of total power loss.

8.2 Environmental Data

Indoor temperature and humidity (RH) will be 22 °C $\pm$ 4°C and 40% to 70% respectively and shipping and storage conditions will be considered as -20 °C to 85 °C and 0% to 100%.

However, as a minimum the following operating conditions shall not degrade the continuous operation of the system:

- o Min/max temperature: 5°C to 40 °C
- o Min/max humidity: 20% to 90% RH non-condensing
- o Suspended Solids are dust and sand.

Allowable indoor noise level shall be 55 dBA, measured at one meter from equipment in question.

8.3 Ingress Protection and Hazardous Area Classification

Control and rack rooms shall be considered as non-hazardous areas. Both control and rack rooms will be air-conditioned and pressurized.

Indoor stations and system cabinets shall conform to IEC-60529, IP 42, as a minimum.

Electrical accessories, cabling and junction boxes in hazardous areas will normally be of intrinsically safe construction and execution suitable for NEC Class I, Division I, and Group C (IEC Zone I, Group II B) locations. Where intrinsically safety equipment is not available, suitable explosion-proof equipment to suit the Area Classification shall be employed.

8.4 Electromagnetic Interference

Equipment shall meet all electromagnetic compatibility requirements of the IEC 61000-4-2, 61000-4-3, and 61000-4-4 standards.

Each element of the PCS must function without introducing intolerable electromagnetic disturbances to other items or being susceptible to electromagnetic influences from other systems.

Emission limits generally comply with the relevant requirements of BS-6527 for Class B equipment, and Susceptibility performance shall generally comply with the relevant requirements of IEC 1000-4. All equipment comprising the PCS shall be designed in such a way as to ensure immunity to interference from VHF and UHF hand portable transceivers operating in the range 150 MHz to 470 MHz with a power output of 1 Watt (RMS) held at 300 mm from any equipment forming part of the PCS.

9. SYSTEM DESCRIPTION

9.1 Configuration

Configuration of the system and the specifics quantities of hardware will be specified in the specific project documents.

9.2 PCS Architecture

9.2.1 Automation System

Although NIOEC encourages the use and application of modern technologies in its projects, however such approach to the new findings and technologies must be based on a sound and safe engineering and design practice. As such, taking into account the unsatisfactory performance of fieldbus technology on control loops, especially critical loops and those requiring fast response times, the automation system architecture shall be based on a hybrid of fieldbus technology and the conventional DCS, whereby generally the control loops shall be handled by the DCS and the monitoring loops shall be performed via the fieldbus equipment. The system shall make use of OLE/OPC for interconnectivity of multiple systems from different suppliers, compact packaging with flexible DIN rail mounting, field or rack room mountable control and I/O subsystem.

The system shall be based on an integrated, hierarchical distributed architecture with shared displays such that in combining operator interfaces, process controllers and input/output modules it shall provide an operating integrated system effective at the loop, unit and plant control levels.

Information hierarchy shall be incorporated in fixed, variable and customized format displays. The communication shall be such that any bit of information in any part of the plant, connected to the system, shall be available on any operator station. Each station shall be capable of taking over the function of a failed station.

The PCS shall have the capability for the operator to assume manual control of any or all of the control loops.

The operation of the PCS shall include, but not be limited, to the following:

- Control Configuration.
- Database.
- Hierarchical Displays.
- Historisation.
- Real time and Historical Trending.
- Automatic Diagnostics and Fault Reporting.
- Documentation.

Configuration of the system shall be carried out through Engineering Stations to facilitate on- line system configuration and debugging capability. The Engineering functions shall include system configuration, data base management, graphic display generation, report generation management and utility program access. The functions shall be soft/hard lock protected.

Real time dual redundant LAN and associated communication hardware shall be used to transfer data between various PCS components. TCP/IP shall be provided to link the PCS to the hierarchy of management suite.

9.2.2 Use of Standard Products

The system shall consist of manufacturer's standard hardware, field proven systems software, and firmware that can be configured to meet the stated requirements. Vendor's standard system operating software shall not be modified to meet any of the Purchaser's requirements.

9.2.3 Software Revision

All software, exclusive of application software, shall be the most recent revision that is applicable to the system hardware at the time of the hardware freeze date as defined in the contract or purchase order.

Software design shall be such that future revisions or updates of the system operating software will not affect the successful operation of the system.

The system shall allow for upgrading of system operating software on all redundant modules of the system without the necessity of shutting down the process, without losing the operator interface, and without the loss of access to any control function.

Application software shall not require modifications in order to be able to run under new releases of the system operating software. Any new release of system software shall be backward compatible with files created using the previous software releases.

9.2.4 Integrity of PCS

The PCS shall maintain a high availability figure with a high level of integrity. This shall be achieved by:

- The use of high reliability components,
- The use of hardware redundancy where specified,
- Provision of routine and/or automatic testing and diagnostics,
- Simple fault indication and module replacement repairs.

9.2.5 Reliability of PCS

The supplied equipment must be designed for the maximum reliability and the minimal downtime. The system shall have a high degree of tolerance to hardware malfunctions, software and operator miss-keying. Any fault, which develops, shall have its effect localised from that part of the system.

The required reliability shall be achieved through a fault tolerant design, advanced diagnostics and state of the art redundancy schemes. The system shall be designed such that all key elements of the system, including storage devices, communication modules, interfaces and media, power supplies and other major system elements are provided in automatic dual redundant configurations.

Automatic switch over between the redundant modules/cards/components shall be incorporated into the system design. Switch over between redundancies shall be transparent to the system, however it shall be reported to the operator stations. Status of data network, node and modules shall be displayed on the station monitors. Failure of either of the networks or associated communication modules shall not interfere with the closed loop control functions.

It shall be possible to replace the malfunctioning redundant parts without system disruption or power off.

9.2.6 Availability of PCS

The availability of the equipment shall be in excess of 99.5 % and shall include all equipment as supplied by the VENDOR. For calculation purposes the equipment supplied by others shall be assumed to have an availability of 100%.

The VENDOR shall supply availability calculations based on MIL-HDBK-217E based on a minimum configuration of the following items:

- All controllers associated with process monitoring and control is operational with no more than a single I/O module failure.
- All control functions available.
- At least one VDU and one functional keyboard operational per operator station.
- At least one printer operational.

Mean time between failures shall be applied as required to ensure that the entire control cell (excluding field equipment) is a minimum of 99.5% available, based on a MTTR of 4 hours. The MTBF and coefficient of availability rating is inclusive of both hardware and software functions as a system. The PCS supplier shall supply documentation describing the method and identifying the data used in calculating the MTBF and coefficient of availability.

The VENDOR shall detail the MTBF for the total PCS and the method used to achieve the MTTR.

Any module with an MTBF of less than 10,000.0 hours shall be clearly identified by the VENDOR.

9.2.7 PCS Redundancy

In order to meet the required system availability, redundant and/or fault tolerant technology shall be incorporated.

The following equipment shall be redundant as a minimum:

1) Controllers and associated I/O modules

Complete one to one redundancy is required with full duplication of control modules and I/O modules in control loops. If requested, the fully duplicated equipment must allow mounting in separate cabinets to minimise common cause failures. It shall also be possible to have redundant control modules that share a single set of I/O. Identical, standard hardware must be used for all redundancy schemes.

Redundant control modules shall simultaneously and synchronously execute a control scheme. The modules shall continuously monitor the health of each other. When the need for a switchover is established by the redundancy software the redundant controller must immediately become active with no software transfer necessary at the time of control transfer to re-establish control. The switchover time from the main to the standby module shall be less than 10 msec. Process control shall continue to be executed in the non-failed unit.

When a module is replaced the new module must automatically initialise, receive the current database from the primary module and pick up in synchronous execution as a secondary module in the redundant relationship. This shall take place without user action for any of the steps.

2) Communication Network

The network, including fiber optic cabling shall be dual redundant. On line redundant real time LAN and the redundant associated communication hardware shall have switchover time from the main to the standby of less than 100 msec.

3) Power supply

All internal system 24 VDC power supplies shall be dual redundant.

4) Mass Storage Devices

5) H1 Cards

The following equipment shall be provided in “mutually backed-up” configuration on an operational group basis.

1) Operator Station

Identical stations shall be provided with one-for-one backup, independently communicating with the control system. Operator stations need to be supplied such that the failure of one network card or connection does not cause the station to lose communication with the network.

2) System Data Base

9.2.8 PCS Diagnostics

a) General

The system shall continuously check itself and report any malfunction, hardware or software, in any part of the system. Clear diagnostic messages and alarming shall be available on the station displays indicating tag address, nature and severity of the defect and time and date.

All system electronic modules shall have built in status indicators to facilitate rapid fault detection and maintenance work.

The activation of any back up module to maintain the system operation integrity shall be completely transparent to the operator. However diagnostic messages shall be sent to the operators via station displays.

b) On-line Diagnostics

The system must include comprehensive on-line diagnostics with the following minimum features:

Redundant Control Module processors shall perform calculations in parallel and synchronised manner, so that switching from main processor to backup cause no interruption to analogue or digital output signal and without any data loss.

The built-in diagnostics shall include a mechanism to validate the calculation results of redundant processors before sending the calculation results to field devices. Validation shall incorporate a function to check for any difference in the calculation results of the redundant processors. If such error occurs, the built-in diagnostic function shall determine which calculation was invalid and select the processor output with the correct calculation. Vendor shall clearly describe how his system architecture supports this requirement.

Control Module processors shall utilize Error Correction Code (ECC) on the main memory to reduce errors that may be caused by main memory (RAM).

Real-time network shall utilize CRC and frame length check as minimum precaution for securing real-time data transfer.

System alarms initiated by the self-diagnostics functions must alert the operator at the Operator Station within 3 seconds. System alarms and diagnostic displays must be available for all operator stations.

The on-line diagnostic program shall consist of a malfunctions check program that will alert the operator upon the detection of a fault. This shall be a unique and separate system from plant alarms. The self-diagnostics shall, as a minimum, detect a fault or malfunction in the following:

- Real-time network diagnostics which shall include, as minimum, errors due to wrong address, wrong frame length, and response wait time-over, other side busy, and receive data check sum error, network configuration error, and communication timer error. Real-time LAN shall include error counters;
- Power supplies and fans;
- All PCS cards (controllers. Processors, hardwired analogue and digital I/Os, etc.);
- Printers;
- Control Module CPU ROM Sum Check Error;
- Control Module algorithm execution error;
- Calculation function execution error;
- On-line/offline downloads error;
- Recovery Message;
- Third party system communication error, and link failure;
- Redundant Control Module database difference among processors;
- Instantaneous AC power supply failure/recovery to the Control Module;
- Diagnostics shall cover hardware, software and firmware of the PCS.

9.2.9 Scalability of PCS

The PCS shall be modular such that an easy expansion from a small system to a large system can be made if necessary. The VENDOR shall describe the future expansion philosophy of the installed system in terms of limits of capability and ease of implementation. The description shall include the expansion aspects of control, man-machine interfaces, system database, applications, operating system, hardware and communications.

9.2.10 PCS System Backup

The entire control software shall be backed up; this includes vendor software, control database, user-built programs, source code, data files, schematics and so forth.

Back up must be possible on commercially available media. To recover from an outage, any component of the system must be able to be re-loaded from bulk memory (hard disks).

All the system-related software including engineering tools, application programs, standard and optional packages that are included in the scope of supply shall be delivered with the system on magnetic or optical media.

9.2.11 PCS Battery back-up

All volatile memory devices within the system shall be provided with memory power supply battery back-up. The battery back up shall have a minimum capacity of 72 hours and shall be independent of the PCS UPS system at the UPS downtime. The PCS shall monitor the status of the its dc power distribution system in order to alert the operator of the malfunctions.

Power failure to a control module for less than 72 hours shall not require the down load of the control module.

Each Operator stations shall be loaded from its own bulk memory automatically when power is recovered.

9.2.12 PCS Connectivity

The PCS shall be able to be connected with upper level computers and networks using Ethernet with TCP/IP protocol.

9.2.13 PCS Interface With Third Party Subsystems

Dedicated control and monitoring systems for third party subsystems such as PLCs, Tank Gauging etc., shall be interfaced to the PCS, and will be controlled and monitored by the operators.

Sub-systems shall be interfaced via serial link RS-232/422/485 using MODBUS RTU protocol/Ethernet Interface/OPC. The vendor shall have interface ports that support serial links/Ethernet link at the Control Module level and shall provide the driver software.

The PCS shall perform memory mapping of the sub-system, and achieve seamless integration between the PCS database and sub-system.

9.2.14 PCS Spare Capacity

The spare capacity shall allow on site development and modification without major changes to the hardware, software and system configuration.

No more than 70% of the available memory and 70% of the available storage disc shall be utilised during normal PCS operation.

Each system shall be supplied with 10% spare for all elements of the system configuration, including application software, graphics, history, reports, and trends. Fitted and wired spare of 10% for each I/O type and control capability in the base system shall be installed. The base system is defined as the quantity of hardware and software needed to meet the project requirements.

Communication networks within the automation system shall include a ten percent (10%) fitted and wired spare hardware and unused node addresses. System expansion requirements shall be in accordance with the project procurement documents. System expansion shall be achievable without shutting down the regulatory controllers not directly involved with the expansion.

The communication network shall utilize automatic network self-addressing technology (plug-and-play), which automatically assigns unique new controller addressing when a new device is connected to the control network.

9.2.15 PCS Performance and Sizing**a) General**

The control response period shall be used as the measure of PCS performance. The control system can perform proportional, integral, derivative (PID) control using any combination of hardware and software. Functions (e.g. signal selectors, summers, calculation blocks, etc.) associated with controllers shall not increase the control response period.

In case of licensed process units, the maximum allowable control response period shall basically follow the process licensors operational requirements. However following figures are the minimum requirements if no special requirements are specified by the licensors.

Process Category	Maximum control response period (msec)
Flow, PRESSURE, DIFFERENTIAL PRESSURE	300
Temperature	1000
Level	1000
Designated Fast Process Control Loops	150
All Others (Analysis, Density, pH, Etc)	1000
* Shorter control response periods may be required for certain control services (e.g. compressor anti-surge, reactor temperature, etc.). Multi-variable advanced process control may be implemented with longer control response periods. In general, the shorter the control response period, the better the control performance. Control response periods longer than those listed above may degrade performance and affect unit operability.	

NOTES: 1- The criteria shown in the above table are typical requirements if there are no requirements on such special requirement where applicable. The maximum allowable control response period shall basically follow to the process licensors operational requirements.

b) PID Equation Form

The PID controller equation should be of the form in which the derivative action is only based on the change in process variable. Those forms of the PID equation in which the derivative action is based on the change in error (and derivative is used) cause the controller output to spike when the operator changes the set point.

c) Controller Set point Tracking

Controller set point should track their respective process variables while in manual mode. For cascade loops, the output of each primary controller should track the set point of its respective secondary controller when the secondary controller is not in cascade mode. All primary controllers should also revert to manual mode when their associated secondary controllers are not in cascade mode. This allows the controller output tracking to take effect, thereby facilitating bumpless transfer when cascade is re-established. Proper configuration of tracking allows operators to change the mode of any controller from manual to automatic or from local automatic to cascade without causing a process disturbance.

d) Controller Central Processing Unit Capacity

The control system Central Processing Unit(s) (CPU) shall include sufficient capacity to permit 50% of the slowest controllers at 1000 ms to be changed to 300 ms. Changes to the execution/acquisition rate may be required during process unit operation.

This requirement is in addition to other provision for spare capacity in the control system. The system shall have a standard feature to give the user the freedom to select some control and sequencing functions to be executed at system's fastest execution rates.

e) Indicator performance

Indicator data acquisition rate shall be used as a measure of performance. Indicator data acquisition rate is defined as the total time the control system takes to read the process data from the input processor and conditions it for visual display.

For initial system sizing and configuration, an acquisition rate of 2 seconds shall be used. Where indicated data is used in control scheme, the acquisition rate shall follow the controller execution rate listed elsewhere in this Specification.

f) Scanning

The PCS shall scan all data-points at least once every second. All calculated points associated with a scanned data-point shall be computed at that data-points scan rate. No pulses shall be lost to totalisers between scans.

g) Alarm/Event Handling

All alarms and events shall be guaranteed to be displayed and printed at the relevant control room within 2 seconds of occurring at the field equipment. Alarm/event acceptance shall be complete within 1 second of acceptance action by the operator.

The PCS shall be capable of handling up to 100 alarm and events per second without affecting alarm event or display handling.

Each PCS cabinet equipment shall be capable of buffering one event per data-point up to a maximum of 100 per equipment when all changes cannot be transmitted completely or a communications failure occurs to the control room operator stations.

h) Displays

Call up time to bring full display with all information of a standard operation display shall be within two seconds. All dynamic data including historical trends embedded in graphic displays shall be presented on the monitor within the call up time.

All operational displays and customised graphics shall have a data refresh rate of 1 second and all other facilities shall have an initiation response time within 2 seconds of the request being made i.e. reports and logs.

i) PCS System Boot Up After Power Failure

All nodes on the real-time network shall boot up from self-contained database without dependence on other nodes.

Control Modules shall detect power failure/recovery and perform immediate power fail/recover processing and set the control algorithm status to certain defined conditions.

All Control Modules and nodes connected on the real time process LAN network shall boot up automatically upon power source recovery. Each Control Module or node on the network shall have its own database stored inside it, which will enable it to boot up independently without loading the database from other nodes or servers on the network.

Operator stations and historisation platform shall boot up automatically to the level where all its functions are in operation. User log in and password shall not be required during the boot up process. Boot up shall take place automatically upon switching on the power source.

j) PCS Loading

The equipment shall be designed so that under full load conditions, the loading of Processing shall be less than 80%, and that of the Memory shall fall below 70%.

Network load in normal operating condition shall not exceed 50%. This load shall be calculated based on the conditions of "No alarm status" and "All operator displays are continuously updated at one-second cycle with 50 dynamic data per display" occurring simultaneously.

k) PCS Performance Guarantee