

NIOEC-SP-70-21(1)							
DOCUMENT CODE							NO. OF PAGES: 43
PLAN/PRJ/SUB	UNIT	PHASE	DISCIPLINE	DOCUMENT TYPE	SERIAL NO.	REV. NO.	DATE
NIOEC	000	EG	IN	SP	7009	A0	APRIL 07



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

NIOEC SP

NIOEC SPECIFICATION FOR PROGRAMMABLE LOGIC CONTROLLERS (PLC)

FIRST 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,

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					
0	APRIL 2007-04-14	ORDOOBADI	ORDOOBADI	FARZAM	SAJEDI
REV.	DATE	PREPARED	CHECKED	APPROVED	AUTHORIZED

CONTENTS:	PAGE NO.
1. SCOPE	2
2. REFERENCES.....	2
3. UNITS	5
4. DEFINITIONS AND TERMINOLOGY	5
5. ABBREVIATIONS.....	5
6. PRODUCT HISTORY	6
7. CERTIFICATION AND APPROVALS.....	6
8. UTILITY AND ENVIRONMENTAL REQUIREMENTS	6
9. DESIGN REQUIREMENTS	7
10. INTERLOCK SYSTEMS SPECIFICATION.....	11
11. LOGIC CONTROL SYSTEMS SPECIFICATION	15
12. OPERATOR AND ENGINEERING STATIONS.....	26
13. ANNUNCIATOR CONSOLES.....	29
14. SYSTEM CABINETS DESIGN	30
15. NAMEPLATES	34
16. PAINTING AND RUST PREVENTION	34
17. DOCUMENTATION.....	35
18. INSPECTIONS AND TESTING	35
19. INSTALLATIONS, START UP AND COMMISSIONING	38
20. SPARES PARTS SUPPLY	39
21. TRAINING.....	40
22. GUARANTEES	40
ATTACHMENT I.....	41
VENDOR DOCUMENT SCHEDULE VDS.....	41

1. SCOPE

This specification defines NIOEC's minimum requirements for the design and installation of Logic Systems, which will be based on Programmable Logic Control.

Logic Systems addresses in this document are classified as follows:

1.1 Systems, which will be used to perform interlocks and will be referred to as "Interlock System". In plants, where Process Control System is employed, this function is normally incorporated within the PCS. However, in plants with Single Loop Digital Controller, conventional electronic controllers, or pneumatic controller technology, such a function is usually implemented via relay logic. In the latter cases, the Interlock System is specified herein as a substitute to the conventional relay logic technology.

1.2 Systems which will be used to perform repetitive, batch type sequencing of valves and controllers and provide process control and automation in plants where other process control systems are not employed due to small size of plant and the economies involved, and will be referred to as "Logic Control System".

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	“Surge Withstand Capability (SWC) Tests”
	IEEE 802.3	"Local Area Network carrier Sense Multiple access with Collision Detecting (CSMA/CD) Access Method and Physical Layer Specification"
	IEEE 802.4	"Token Passing Bus Access Method and Physical Layer Specification"
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 61151	"Functional safety - Safety instrumented systems for the process industry sector"
	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”
ISA	(INSTRUMENTATION, SYSTEM, AUTOMATION SOCIETY OF AMERICA)	
	ISA - S 5.1	“Instrument Symbols And Identifications”
	ISA - S 5.2:	“Binary Logic Diagrams For Process Operations”
	ISA - S 5.3:	“Graphic Symbols For Distributed Control/Shared Display Instrumentation, Logic And Computer Systems”
	ISA - S 5.4:	“Instrument Loop Diagrams”
	ISA RP 55-1:	“Hardware Testing Of Digital Process Computers”
	ISA- S18.1:	“Annunciator Sequences And Specification”
	ISA- S50.1	“Compatibility Of Analogue Signals For Electronic Industrial Process Instruments”
	ISA- S84	"Application of Safety Instrumented Systems (SIS) for the Process Industry"
ISO	(INTERNATIONAL STANDARD ORGANISATION)	
	ISO 9000	Quality Systems”
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”
	TIA/EIA-310 C	“ 19 inch Rack standard”
U.S. MILITARY	(U.S. MILITARY HANDBOOK)	
	U.S. Military Handbook -217	“Reliability Prediction Of Electronic Equipment”
	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.

Equipment or System: Logic Systems (hardware/software)

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.

5. ABBREVIATIONS

EMI: Electromagnetic Interference
ESD: Emergency Shut Down
FAT: Factory Acceptance Test
IS: Interlock Systems
LCS: Logic Control System
MOV: Motor Operated Valve
MTBF: Mean Time Between Failures
PC: Personal Computer
PCS: Process Control System
PFD: Probability of Failure on Demand
RFI: Radio Frequency Interference

SAT: Site Acceptance Test

SGS: Safeguarding System

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

CE marking shall be required 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 or HSE and for NEC regulations shall be FM or UL.

8. UTILITY AND ENVIRONMENTAL REQUIREMENTS

8.1 Electrical Power

The equipment will be normally 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:

- Min/max temperature: 5°C to 40 °C
- Min/max humidity: 20% to 90% RH non-condensing
- 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 shall 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.

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 SYSTEM provided to meet the requirements of this Requisition 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 SYSTEM 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 SYSTEM.

9. DESIGN REQUIREMENTS

9.1 Applications

9.1.2 Interlock Systems (IS)

Interlock Systems are employed to perform interlocks.

The Interlock System logic solver shall have suitably high availability as determined by the economic impact if the System fails to operate on demand.

The logic solver shall be a fault tolerant, redundant programmable logic controller, with self diagnostic coverage. Diagnostics shall include the I/O interfaces.

Unless otherwise specified, 500 milliseconds can be used for the maximum program cycle time.

The logic solver shall be separate from the Process Control System (PCS).

9.1.3 Logic Control Systems (LCS)

Systems which will be used to perform repetitive, batch type sequencing of valves and controllers and provide process control and automation in plants where other process control systems are not employed due to small size of plant and the economies involved.

Process economics will dictate the required level of availability.

The logic solver may be a Programmable Logic Controller, or sequential logic functions within a PCS.

The system shall incorporate the following continuous and discrete control strategies:

For batch control, the system shall contain control strategies for both continuous loops and discrete devices, to perform the continuous control of the required batch operations.

The continuous control loop strategies shall range from simple regulatory PID control to advanced user defined algorithm controls.

The continuous and discrete control strategies shall be capable to be configured by means of the operator interface terminals.

The number of controller loops available in the system shall be equal to the numbers defined in the project data sheets plus 50% more control loops for future expansion and trimming of the control system.

9.2 Integrity of Logic Systems

The SYSTEM 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 appropriate.

Provision of routine and/or automatic testing and **diagnostics**.

Simple **fault indication** and module **replacement repairs**.

9.2.1 Reliability of SYSTEM

The SYSTEM must be designed for the maximum reliability and the minimal downtime. The System shall have a high degree of tolerance to malfunctions of hardware, 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. 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 consoles. Status of data network, node and modules shall be displayed on the console 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.

9.2.2 Availability of SYSTEM

The availability of the equipment shall be in accordance with the requirements of Section 3 of this document.

Availability calculations shall be based on MIL-HDBK 217E based on a minimum configuration of the following items:

All controllers, associated with process monitoring and control, are operational with no more than a single I/O module failure.

All control functions available.

At least one monitor and one functional keyboard operational per operator station.

At least one printer operational.

Any module with an MTBF of less than 10,000 hours shall be clearly identified by the VENDOR.

9.2.3 System Redundancy

The System shall be designed such that all controllers and associated input/output modules, storage devices, communication modules, interfaces and media, power supplies and other major System elements are provided in automatic redundant configurations.

a) Controller and I/O Redundancy

Complete redundancy is required with full duplication of control modules and I/O modules in control loops.

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 milli-seconds. 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.

b) 2- Out of- 3 System

When specified, The System shall employ 2 out of 3 voting technique as follows:

- i) Triple automatic redundant and independent processors. Each processor shall execute its individual application program simultaneously and independently (executing logic instructions, control calculations and clock and voter/synchronisation).
- ii) Triple automatic redundant input cards. Each detector signal shall be separated into three isolated paths and input to three input cards, compared and voted in a 2-out-of-3 arrangement and then sent via three separate paths to processors, where 2-out-of-3 voting is again performed on the data.
- iii) Triple automatic redundant output cards. Processors outputs shall be sent via redundant paths to output cards where they shall be voted again (2-out-of-3) to ensure integrity.

c) Communication Redundancy

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 milli-seconds.

d) Power supply Redundancy

All internal DC power supplies shall be provided in dual redundancy.

9.2.4 System 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 console 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 console 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 utilise Error Correction Code (ECC) on the main memory to reduce errors that may be caused by main memory (RAM).

Real-time network shall utilise 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 Console within 3 seconds. System alarms and diagnostic displays must be available for all operator consoles.

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:

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

9.3 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.

9.4 Battery back-up

- a) 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 48 hours.
- b) The System will be powered from battery backed UPS at 230 V AC, consequently the internal dc power Systems shall not be provided with their own battery back- up facilities.

9.5 Spare Capacity

- a) The spare capacity shall allow on site development and modification without major changes to the hardware, software and System configuration. The spare I/O capacity shall be distributed evenly by I/O type per System Cabinet. The Vendor shall define this during the functional design phase.
- b) No more than 70% of the available memory and 70% of the available storage disc shall be utilised during normal SYSTEM operation.

c) The following spare capacity shall be provided in the design of the System unless otherwise stated elsewhere in this specification:

i) Controllers and I/O cards

Each System cabinet shall have 20 % spare fitted and wired controllers, I/O cards and other associated facilities to render 20 % future control and monitoring expansion facility.

In addition 30 % spare space shall be provided for each of the above mentioned categories.

ii) Other cabinets

All other System cabinets shall have 20 % spare equipment plus 30 % spare terminals.

9.6 Scalability

The SYSTEM 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.

9.7 System Loading

System's processing and memory loading under full load conditions shall be less than 70% of the maximum capability.

9.8 Testing

All logic solvers shall have internal and/or external methods to allow functional testing of the total System, including field devices, to detect covert faults that prevent the System from operating in the desired manner.

The testing interval(s) of the components that make up the total System must be taken into account when designing the System. Logic System designer shall provide adequate testing procedures including automation features available and verification report capabilities.

Safety Instrumented Systems are normally designed with the following maximum test intervals:

Field sensors - 1 year interval

Logic solvers - 1 year interval

Solenoid valves - 1 year interval

Shutdown valves - 4 year interval

9.9 Communication with Third Party Systems

All Logic Solvers specified herein shall provide secure digital communication to other Systems for annunciation, logging of alarms and events and retransmission of process variable data. Logic solver shall be capable (as a minimum) of updating all process variable data every two seconds. The communication shall be based on serial link RS-232/422/485 using MODBUS RTU protocol/Ethernet Interface. The vendor shall have interface ports that support serial links/Ethernet link at the Control Module level.

10. INTERLOCK SYSTEMS SPECIFICATION

10.1 General

This application includes interlocks of single equipment to perform orderly start-up and shutdown in order to prevent it from working under extreme conditions which may damage the equipment.

10.2 General Hardware Requirements

10.2.1 The processor, I/O System, and power supplies shall be of dual hot stand-by type. The dual stand-by processors shall have a common data base, staying fully informed of each other's status at