

NIOEC-SP-70-09(2)							
DOCUMENT CODE						NO. OF PAGES: 34	
PLAN/PRJ/SUB	UNIT	PHASE	DISCIPLIN E	DOCUMENT TYPE	SERIAL NO.	REV. NO.	DATE
NIOEC	000	EG	IN	SP	7009	A0	APRIL, 2007



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

NIOEC SP

NIOEC SPECIFICATION
FOR
SAFEGUARDING SYSTEMS

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	ORDOOBADI	ORDOOBADI	FARZAM	SAJEDI
REV.	DATE	PREPARED	CHECKED	APPROVED	AUTHORIZED



Documents

Document Sharing Hub

CONTENTS:**PAGE NO.**

1. SCOPE	2
2. REFERENCES	2
3. UNITS	5
4. DEFINITIONS AND TERMINOLOGY	5
5. ABBREVIATIONS	5
6. PRODUCT HISTORY	5
7. CERTIFICATION AND APPROVALS	5
8. UTILITY AND ENVIRONMENTAL REQUIREMENTS	6
9. DESIGN REQUIREMENTS.....	7
10. SAFETY INSTRUMENTED SYSTEM SPECIFICATION.....	12
11. OPERATOR AND ENGINEERING STATIONS	17
12. ANNUNCIATOR CONSOLES	18
13. ALARMS AND SEQUENCE OF EVENT RECORDING (SER)	19
14. SYSTEM CABINETS DESIGN	21
15. NAMEPLATES	25
16. PAINTING AND RUST PREVENTION	25
17. DOCUMENTATION	26
18. INSPECTIONS AND TESTING	26
19. INSTALLATIONS, START UP AND COMMISSIONING	29
20. SPARES PARTS SUPPLY	30
21. TRAINING.....	31
22. GUARANTEES.....	31
ATTACHMENT I	32
VENDOR DOCUMENT SCHEDULE VDS	32

1. SCOPE

This specification defines NIOEC's minimum requirements for the design, procurement and installation of Programmable Logic Control based Safeguarding Systems which will be used to protect personnel, environment, the process and the associated equipment.

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: Safeguarding 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
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.

Where "TUV-approved" or "TUV-certified" is specified, this shall be in accordance with DIN V VDE 0801 and DIN V 19250. The required AK class shall be indicated in the requisition.

The system hardware and system software shall be certified by TUV.

All input and output cards shall be TUV-approved.

All input and output cards shall be fail safe except those driving alarm lamps.

Vendor shall report any disagreements between this specification and the constraints of the TUV approval reports.

TUV certification shall include the serial communication with the PCS, SER and maintenance and engineering network, and communication. The system shall be unresponsive to faults in the PCS, SER and maintenance and engineering workstation.

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 General

The system shall in general be designed in accordance with the requirements of ISA S 84.01.

During the engineering phase, a Safety Integrity Level (SIL) shall be specified and prepared based on a quantitative risk assessment methodology, assumed values for the PFD of all components of the SGS, and an assumed fatal accident rate of 1 per 10⁴ years. System shall be based on proven and reliable technology satisfying TUV requirements and approvals for the stated SIL class according to IEC-61511. SIL rated instruments shall be utilised in this connection.

The System shall have programming languages as per IEC 61131-3.

The Safety Instrumented System logic solver shall be designed for use in safety applications with high availability of greater than 99.99% and shall be a fault tolerant, redundant Programmable Logic Controller, with self diagnostic coverage. Diagnostics shall include the Input/Output (I/O) interfaces.

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

The Process Safety Time shall be determined prior to the final design of the Logic System to insure a suitable logic solver configuration is utilized. Contractors shall advise vendor of the final requirements. Unless otherwise specified, 500 milliseconds can be used for the maximum program cycle time.

The system shall be normally energized except for lamp status, and shall de-energize output(s) when the logic detects an unsafe condition. A "1" logic signal is considered to be the normal state, and "0" logic signals the abnormal (trip or failure) state. Output signals shall go to a state of "0" on power failure or on component failure.

For commissioning purposes it shall be possible to force I/O signals to certain states via the engineering workstation. This forcing feature shall be under key-lock, and forcing shall be ineffective when the key is removed.

Loss of data communication with the PCS or in the SER and maintenance and engineering network shall not result in trips or status changes of the system communication points.

Recovery of communication shall be automatic. The Supplier shall indicate the type of output (hardwired) that can be made available to permit (back-up) annunciation of communication failure at the PCS operator workstation.

The operator shall be continuously informed of the system status by means of system and utility alarms transmitted to the PCS. As these are Supplier-specific, they may not be included in the I/O listing provided by the owner, but shall be included in the scope.

As a minimum a common cabinet utility alarm and a common system alarm shall be transmitted to the PCS for the attention of the operator.

For system alarms and utility alarms, extra (or all) diagnostic information may be transmitted from the system to the PCS in addition to the common alarms. This shall be indicated in the requisition.

A hard wired alarm shall be provided for total system failure.

The Supplier shall provide a list of those parameters that may cause a trip if not properly set.

9.2 Integrity of the System

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

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

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 Redundancy