

NIOEC-SP-70-09(3)							
DOCUMENT CODE							NO. OF PAGES: 40
PLAN/PRJ/SUB	UNIT	PHASE	DISCIPLINE	DOCUMENT TYPE	SERIAL NO.	REV. NO.	DATE
NIOEC	000	EG	IN	SP	7009	A3	SEPTEMBER 2015



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

NIOEC SP

NIOEC SPECIFICATION FOR SAFEGUARDING SYSTEMS

SECOND EDITION

DECEMBER, 2009

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 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 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 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 ongoing projects.

In response to the initiative of the Design and Engineering 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 and Engineering 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 and Engineering Director of NIOEC for evaluation and approval.

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

NOTES:

- 1) THIS SHEET IS A RECORD OF ALL REVISIONS TO THIS SPECIFICATION.
- 2) WHEN APPROVED EACH REVISION SHALL BE CONSIDERED AS A PART OF THE ORIGINAL DOCUMENT.
- 3) NUMBER OF PAGES EXCLUDES THIS SHEET AND THE COVER SHEET.

6					
5					
4					
3	SEPTEMBER, 2015	F. FAZLI	H.SHIRINPOUR	M.ORDOOBADI	A.ARMAN .MOGHADAM
2	DECEMBER, 2009	INST. DISC.	KHATIB	FARZAM	SAJEDI
1	APRIL, 2007	ORDOOBADI	ORDOOBADI	FARZAM	SAJEDI
REV.	DATE	PREPARED	CHECKED	APPROVED	AUTHORIZED

CONTENTS:	PAGE NO.
1. SCOPE	2
2. REFERENCES	2
3. UNITS	6
4. DEFINITIONS AND TERMINOLOGY	6
5. ABBREVIATIONS	6
6. PRODUCT HISTORY	7
7. CERTIFICATION AND APPROVALS	7
8. UTILITY AND ENVIRONMENTAL REQUIREMENTS	7
9. DESIGN REQUIREMENTS	8
10. SAFETY INSTRUMENTED SYSTEM SPECIFICATION	15
11. OPERATOR AND ENGINEERING STATIONS	21
12. ANNUNCIATOR CONSOLES	22
13. ALARMS AND SEQUENCE OF EVENT RECORDING (SER)	24
14. SYSTEM CABINETS DESIGN	27
15. NAMEPLATES	32
16. PAINTING AND RUST PREVENTION	33
17. DOCUMENTATION	33
18. INSPECTIONS AND TESTING	33
19. INSTALLATIONS, START UP AND COMMISSIONING	36
20. SPARE PARTS SUPPLY	37
21. TRAINING	38
22. GUARANTEES AND WARRANTIES	38
APPENDIX I	39

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. On certain occasions, where due to the limited number of signals, using microprocessor type SGS cannot be justified, relay based ESD system may be used upon written approval from NIOEC.

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

Resolution on cases not explicitly stipulated in this Specification, or on cases where conflicts may arise among the requirements of the referenced/relevant IPS and the international standards, shall be made through written consent and approval of NIOEC.

2. REFERENCES

The following standards, codes, and specifications, to the extent specified hereinafter, shall constitute a part of this NIOEC Specification. Latest edition of the undated referenced documents and the cited edition of the dated references shall apply. The applicability of changes made to the dated references, after the cited date shall be mutually agreed upon between NIOEC and the Vendor/Contractor.

BASIEFA	(BRITISH APPROVALS SERVICE FOR ELECTRICAL EQUIPMENT FOR FLAMMABLE ATMOSPHERES)	
CENELEC	(COMITÉ EUROPÉEN DE NORMALISATION ELECTROTECHNIQUE)	
EEC	(EUROPEAN ECONOMIC COMMUNITY)	
	EMC- Directive 89/336/EEC 1989	“Council Directive on the Approximation of the Laws of the member states Relating to Electromagnetic Compatibility”
EN	(EUROPEAN STANDARDS)	
	BS/EN 55022	“Information technology Equipment- Radio Disturbance Characteristics-Limits And Methods Of Measurement”
FM	(FACTORY MUTUAL)	
IEC	(INTERNATIONAL ELECTRO-TECHNICAL COMMISSION)	
	IEC 60068	“Environmental Testing”
	IEC 60332	“Tests on Electric and Optical Fibre Cables under Fire Conditions”

IEC 60529	“Degree Of Protection Provided By Enclosures (IP Code)”
IEC-60605:	“Equipment Reliability Testing”
IEC 60751	“Industrial Platinum Resistance Thermometers and platinum temperature Sensors”
IEC 61000-4-2, IEC 61000-4-3, IEC 61000-4-4	“Electromagnetic Compatibility (EMC)”
IEC 61131-3	“Programmable controllers – Part 3: Programming languages”
IEC 61158-2	"Industrial communication networks – Fieldbus specifications - Physical Layer Specification And Service Definition”
IEC 61499-1, IEC 61499-2	“Function Blocks”
IEC 61508	“Functional Safety of Electrical/Electronic/Program mable Electronic Safety- Related Systems”
IEC 61511	"Functional safety - Safety instrumented systems for the process industry sector"
IEEE	(INSTITUTE OF ELECTRICAL & ELECTRONICS ENGINEERS)
IEEE C37.90.1	“Surge Withstand Capability (SWC) Tests for Relays and Relay Systems Associated with Electric Power Apparatus”
IEEE 802.3	"Information technology— Telecommunications and information exchange between systems—Local and metropolitan area networks— Specific requirements Part 3:

		Carrier Sense Multiple access with Collision Detecting (CSMA/CD) Access Method and Physical Layer Specification"
	IEEE 802.4	"Information Processing Systems- Local area Networks- Part 4:Token Passing Bus Access Method and Physical Layer Specification"
ISA	(INSTRUMENTATION, SYSTEM, AUTOMATION SOCIETY OF AMERICA)	
	ANSI/ISA-5.1	"Instrumentation Symbols And Identifications"
	ISA-5.2	"Binary Logic Diagrams For Process Operations"
	ISA-5.3	"Graphic Symbols For Distributed Control/Shared Display Instrumentation, Logic And Computer Systems"
	ISA-5.4	"Instrument Loop Diagrams"
	ISA RP 55-1	"Hardware Testing Of Digital Process Computers"
	ISA-18.1	"Annunciator Sequences And Specifications"
	ANSI/ISA-50.00.01	"Compatibility Of Analogue Signals For Electronic Industrial Process Instruments"
	ANSI/ISA-84.00.01	"Functional Safety: Safety Instrumented Systems for the Process Industry Sector"
ISO	(INTERNATIONAL STANDARD ORGANISATION)	
	ISO 9000	"Quality Management Systems - Fundamentals and Vocabulary"

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-70-05	“Specification For Instrumentation Control Cables, Cable Trays, Conduits, Junction Boxes and cable Glands”
	NIOEC-SP-00-10	“Specification For Units”
NIOEC SIP	(NIOEC SHOP INSPECTION PROCEDURE)	
	NIOEC-SIP-70-01	“Shop Inspection procedure for Instruments”
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”
UL	(UNDERWRITERS’ LABORATORIES)	
	UL 508	“Standard for Industrial Control Equipment”
U.S. MIL HNBK	(U.S. MILITARY HANDBOOK)	
	MIL-HDBK-217	“Reliability Prediction of Electronic Equipment”
	MIL-HDBK-472	“Maintainability Prediction”

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

CRC: Cyclic Redundancy Check

ECC: Error Correction Code

EMI: Electromagnetic Interference

ESD: Emergency Shut Down

FAT: Factory Acceptance Test

IS: Interlock Systems

MCC: Motor Control Centers

MOS: Maintenance Override Switch

MTBF: Mean Time Between Failures

OOS: Operational Override Switch

OTC: Operator Training Console

PC: Personal Computer

PCB: Printed Circuit Board

PCS: Process Control System

PFD: Probability of Failure on Demand

SAT: Site Acceptance Test

SER: Sequence of Events Recording

SIL: Safety Integrity Level

SGS: Safeguarding System

UPS: Un-interruptible Power Supply

VDS: Vendor Document Schedule

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 recognized national or international standards, which for CENELEC regulations shall be LCIE, TUV, PTB, BASEEFA or HSE and for NEC regulations shall be FM or UL.

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 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 $\pm$ 2°C and 30% to 65% 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: 0°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 according to hazardous area classification.

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 ite

ms or being susceptible to electromagnetic influences from other Systems.

Emission limits generally comply with the relevant requirements of BS EN 55022 for Class B equipment, and Susceptibility performance shall generally comply with the relevant requirements of IEC 61000-4. 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 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 84.00.01 or IEC 61508.

9.1.1. 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 10^4 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 utilized in this connection.

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

9.1.3. 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.

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

9.1.5. 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.

9.1.6. 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.

- 9.1.7. Loss of data communication with the PCS or SER shall not result in trips or status changes of the system communication points.
- 9.1.8. 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.
- 9.1.9. 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.
- 9.1.10. 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.
- 9.1.11. 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.
- 9.1.12. A hard wired alarm shall be provided for total system failure.
- 9.1.13. The Supplier shall provide a list of those parameters that may cause a trip if not properly set.
- 9.1.14. Emergency shutdown shall be performed by SGS, which shall provide the next layer of safety. SGS shall operate independently from the PCS and the intervention by the operator shall be only possible by pre-defined maintenance and operator overrides.
- 9.1.15. SGS shall be designed to be fail-safe; to this end the following considerations shall apply:
- 9.1.15.1. Contact sensors shall be normally closed (energised) if the measured variable is within the normal operating range and will open if the measured values exceed the safe thresholds.
 - 9.1.15.2. Analogue transmitters shall be configured in combination with the SGS, to cause a shutdown action if the transmitter fails and when an open or short circuit is detected by the SGS.
 - 9.1.15.3. Solenoid valves on ESD valves shall be energised in the normal operating mode. On demand, the solenoid valves shall be de-energised, causing the ESD valve to travel (by spring force) to the safe position.
 - 9.1.15.4. Digital communication between field sensors and SGS shall be prohibited (e.g. "smart" transmitters may only be used in the analogue 4-20 mA DC communication mode).
 - 9.1.15.5. Intelligent/smart transmitters, used within the SGS shall be write-protected to prevent inadvertent modifications and digital communication with remote systems and hand-held communicators.
- 9.1.16. To prevent a common cause fault, which inhibits correct operation of the PCS, from affecting the safety integrity of the SGS, the following philosophy shall be followed throughout the design of the plant:
- 9.1.16.1. Sensors applied for PCS shall not be shared for ESD functions except if three sensors are provided which are to be connected to both the PCS for midpoint selection and to the SGS for 2 out of 3 voting.

- 9.1.16.2. In case 2 out of 3 voting and midpoint selection are provided, the signals will be powered from the SGS and duplication of signals will be part of the SGS interface. Duplication may be via high quality passive components (e.g. resistors), provided both the SGS and the PCS have galvanically isolated inputs.
- 9.1.16.3. Sensors applied for ESD functions shall not share the same process connections with sensors used for control. However, each of the sensors in a "2 out of 3" configuration shall have independent process connections, etc. In case of orifice meters, the same orifice plate and flange set may be used for all transmitters (control and ESD functions), however, each sensor shall have its own pressure tapping, isolation valve, impulse lines and, if applicable, heat tracing. Signals from the 3 transmitters may be connected to the same junction box and may share the same multi-core cable.
- 9.1.16.4. Level instruments, used for safeguarding, shall not share the same standpipe with instruments for control and/or pre-alarms.
- 9.1.16.5. Level instruments, used for "2 out of 3" voting and/or midpoint selection, shall not share the same standpipe and shall be directly connected to vessel wherever applicable. However, level gauges may share the standpipe with any of the level transmitters
- 9.1.16.6. PCS software or data highway between PCS and SGS shall not be used to initiate an emergency shutdown.
- 9.1.17. Configuration and programming of the PCS and SGS-PLC shall strictly follow the requirements of the P&IDs, control narratives, functional block diagrams, safeguarding narratives, logic diagrams, alarm and trip-setting list and (if available) the cause and effect diagram. Only released for engineering issues shall be used.

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.