Grupa LOTOS S.A.	**TECHNICAL SPECIFICATION**	Spec. N° 3650
	Automatic protection system (Safety Instrumented System)	

Contents

1 Subject of specification 3
2 Scope of validity 3
2.1 Deviations 3
2.2 Exclusions 3
3 Hierarchy of documents 3
4 Definitions and designations 3
5 Description 7
5.1 General issues 8
5.2 Requirements concerning conformity of designing to requirements of standards 8
5.2.1 Analysis and conception – base design 10
5.2.2 Engineering design execution 14
5.2.3 Erection and start-up 16
5.3 Techniques employed in automatic protection systems 16
5.4 Configurations of measuring elements used within SIF functions 17
5.5 Configuration of executing elements 18
5.6 Requirements regarding measuring and executing instruments 19
5.6.1 Documentation for measuring and executing equipment forming part of SIS 21
5.7 Requirements regarding SIS-PLC programmable controller 22
5.7.1 Documentation 24
5.7.2 I/O modules 25
5.7.3 Central processing unit – CPU 25
5.7.4 Software 25
5.7.5 Input/output forcing, MOS signals 26
5.7.6 Connections to DCS and other systems 27

This document is the property of LOTOS Group SA.. Copiyng and giving it to other is forbidden without express written authority by LOTOS Group SA

5.7.7 Sequence of Events Recorder (SOER) 27
5.7.8 Cabinets 27
5.8 Safety of machines 27
5.8.1 Requirements for certificate of conformity 27
5.8.2 Safety of equipment 28
5.8.2.1 Furnaces, boilers 28
5.8.2.2 Other machines 29
5.8.2.3 Comparative criterion of risk assessment 29
6 Relevant documents 29
7 Norms and standards 29
7.1 Directives and Decisions of European Community 29
7.2 Polish legal acts 30
7.3 PN-EN 30
7.4 PN-EN ISO 32
7.5 PN-IEC 33
8 Record of changes 34

1 Subject of specification

This specification used in conjunction with other technical specifications of LOTOS Group S.A., establishes minimal requirements regarding designing and execution of automatic protection system on process plants, on the grounds of PN-EN 61508, PN-EN 61511 norms, as well as directive of European Council 96/82/EC (Seveso II) as amended in M1 … M4.

2 Scope of validity

This specification shall be used when preparing both quotations and Purchase Orders concerning planned LOTOS Group S.A. new investments and modernizations.

It shall also be a base for preparation of other detailed specifications and quotations relevant for package units or other equipment deliveries.

2.1 Deviations

Any deviation from this specification and the relevant specifications, standards and related documents including proposals, which the bidder claims to be economically and / or technically superior solutions, must be submitted in writing for review and approval by Grupa LOTOS SA. Non-approved exceptions are not acceptable by Grupa Lotos S.A.

The supplier must report in writing any ambiguity in this or any other specifications of Grupa LOTOS SA or non-compliance with the referred documents / standards and obtain a written explanation from Grupa Lotos SA.

2.2 Exclusions

The following equipment or works, connected with subject of this specification, are included within scope of design works and deliveries of other branches:

- Identification of hazards and risk assessment – technological study (on base design stage)
- Specification of safety requirements, definition of automatic SIF functions along with determination of Safety Integrity Level (SIL) – technological study (on base design stage)

3 Hierarchy of documents

In case of conflicts existing between this specification and other documents, the following order of precedence shall govern:

- The current Polish legislation
- Terms of purchase order / contract and other requirements agreed in writing with GLSA
- Data Sheets approved by GLSA
- This specification
- Other Specifications
- Drawings and other documents
- Standards

4 Definitions and designations

BELOW LISTED TERMS HAVE BEEN DRAWN DIRECTLY FROM PN-EN 61508-4 NORM. ADDITIONAL REMARKS (FROM OUTSIDE OF THE NORM) ARE GIVEN IN SQUARE BRACKETS [ ]

Safety - lack of unacceptable risk

Functional Safety - part of entire safety relating to EUC and EUC control system, which depends on proper operation of E/E/PE safety related systems, safety related system implemented in another techniques and external risk limiting measures

Safety Function - a function to be implemented through E/E/PE safety related system [SIS], safety related system implemented in another technique or external risk reducing device, which purpose is to reach or maintain of EUC safe condition in relation to specific endangering event

Safety Integrity likelihood that safety related system shall satisfactorily perform required safety function, in all specified conditions and within specified period of time.

Risk combination of loss occurrence likelihood and severity of the loss

Tolerable risk the risk that is acceptable in specified context based on current social values

Mode of operation foreseen way of safety related system operation, referred to frequency of calls [actuation demands], which can be:

- **low demand mode of operation:** when safety related system is called not more frequently, than once a year and not more frequently than twice as periodical test frequency
- **high demand or continuous mode of operation:** when safety related system is called more frequently than once a year and more frequently than twice as periodical tests frequency

Verification confirmation, by completion of tests and presentation of objective evidence, that requirements have been met
[it answers the question: „Am I building the system in proper way?”]

Validation confirmation, by completion of tests and presentation of objective evidence, that requirements regarding specified intended use have been met
[it answers the question: „Has correct system been built?”]

Failure loss of functional unit ability to perform required function

Random hardware failure a failure that happens in random moment and results from at least one possible mechanism resulting in hardware degradation. Intensity of hardware failures can be evaluated to certain accuracy. [This applies to failures which source is hardware defect]

Systematic failure a failure connected in deterministic way with some causes, which can be removed only by modification of design or production process, operating procedures, documentation or other adequate factors. Intensity of such

failures occurrence cannot be evaluated.
[This applies to failures, which source lies in erroneous problem analysis or improper completion of task, and is directly connected with human factor].

Diagnostic coverage relative decrease of likelihood of dangerous hardware damages, resulting from operation of automatic diagnostic tests.
[Not all damages can be detected by diagnostics. Majority of damages can, however, be detected during periodical proofing tests].

Independent person the person that is separated and autonomous from activities performed during life cycle stage: total, E/E/PES or software, being a subject to functional safety assessment or validation, and who is not directly responsible for the activities.

Independent organisation the organisation that is separated and autonomous, by means of management and other resources, from organisations responsible for activities performed during life cycle stage: total E/E/PES or software, being a subject to functional safety assessment or validation.

OTHER TERMS

Independency independency of system or equipment means lack of interference possibility into its action by other systems or equipment. This need not necessarily mean that no connection exist between the independent system or equipment and other systems (DCS in particular); independency in this case is characterised by lack of possibility to change function of the independent unit by external factors.

Access protection consists in use of access restriction mechanism, thanks to which access to systems (equipment) is granted only to persons having adequate authorisation and simultaneously foreseen to operate them. Depending on application, various access levels for various persons can be distinguished.

Redundancy technique of multiplication of elements (or their sub-assemblies) in designed plant, applied in order to minimise likelihood of plant, or even its part downtime in result of single element failure (this applies to e.g. measuring and executing elements of automatic protection system, control CPU, I/O modules, supply, or others). In case of instrumentation equipment, the most frequently used solution is doubling of elements, so that in case of basic device failure the reserve device automatically undertakes any tasks. What is essential, such changeover proceeds imperceptibly for the process, without any influence on functionality performed by the elements. Redundancy implementation methods are not, however, limited only to doubling of elements. There are known solutions with tripled elements, particularly in critical, safety related applications. In such cases voting between mutually redundant elements is additionally employed, consisting in rejecting of the device which action contradicts the two other devices action – it would be outvoted in such case.

ACRONYMS USED:

GLSA	-	Grupa LOTOS S.A.
CPU	-	Central Processing Unit
DCS	-	Distributed Control System
PLC	-	Programmable Logic Controller
ESD	-	system of interlocks used for implementation of functions without defined SIL level (Emergency Shut Down system)
I/O	-	Input/Output
DC	-	Direct Current
AC	-	Alternating Current
UPS	-	Uninterruptible Power Supply
CR	-	operators' room / central control room (Control Room)
TIR	-	Technical Instrument Room for location of system cabinets
ER	-	Engineering Room
SOER	-	Sequence of Events Recorder
EUC	-	Equipment Under Control – the equipment, machines, instruments or systems used in production, **processes**, transport, medicine and other fields of activity
E/E/PE	-	Electrical / Electronic / Programmable Electronic – based on electrical (E) and/or electronic (E) and/or programmable electronic (PE). Automatic protection systems are specified in PN-EN 61508 norm with "E/E/PE safety related systems" term.
SIS	-	automatics system used for implementation of SIF functions (Safety Instrumented System). SIS name in PN-EN 61511 norm depicts automatic protection systems.
SIS-PLC	-	PLC controller, in which SIF functions are implemented
ESD-PLC	-	PLC controller, in which functions without defined SIL level are implemented
SRS	-	Safety Requirements Specification – specification containing all requirements regarding safety function, which should be executed by safety related systems
SIF	-	Safety function with defined SIL level (Safety Instrumented Function)
SIL	-	Safety Integrity Level – discrete level (one out of four possible) for specification of safety functions integrity level requirements, which should be assigned in E/E/PE safety related systems [SIS], while level 4 of safety integrity is the highest one, and level 1 of safety integrity is the lowest one.
PFD_{avg}	-	average in specified time likelihood of incapability to perform consigned function on demand (average Probability of Failure on Demand)
RRF	-	Risk Reduction Factor

SFF - this part of all random hardware failures concerning the device, which results in safe failures or detected unsafe failures (Safe Failure Fraction)

CCF - a failure brought about by common cause (Common Cause Failure) – such failure that results from single event or several events, causing simultaneous failure of two or several separate channels in multi-channel system, leading to system failure. Noted as β. It is used for calculation of redundant systems' reliability.

PTI - Proof Test Interval,

PTC - Degree of failures detectability during periodical proofing tests (Proof Test Coverage)

MTTR - mean time necessary for equipment repair (Mean Time to Restoration)

MTTFS - Acceptable time between unfounded shutdowns (Mean Time To Failure Spurious)

MOS - manually activated signals, overriding interlock signals. Used for maintenance purposes (Maintenance Override Switch)

POS - manually activated signals, overriding interlock signals. Used for process engineering purposes, for example during start-up (Process Override Switch)

FAT - complex of tests performed by buyer of specific equipment at equipment manufacturer's works. It takes place after fabrication of the equipment, but prior to its delivery to destination place (Factory Acceptance Test).

FSA - Functional Safety Assessment – testing based on evidences, undertaken in order to assess functional safety reached by single E/E/PE system (or several E/E/PE systems), related to safety, safety related systems implemented in another techniques and external risk reducing measures. Such assessment is conducted by independent person or organisation (refer also to PN-EN 61508-1, paragraph 8).

5 Description

Safety is one the priorities and orders, which observance during designing, implementation and operation of plant is rigorously required. This specification indicates safety aspects and adequate requirements related to them, to which provisions of international standard PN-EN 61508 and its variation for process sector, PN-EN 61511, are referring.

Consequence of PN-EN 61508 standard implementation is that on each designing, construction and start-up stage, as well as plant, or complex of plants operation and maintenance, planned safety management system must be observed. In this regard one should take particular attention for the following aspects:

- **competences** of persons performing assigned tasks
- **evidencing** of individual stages during all investment phases
- **verification** of assigned tasks completion
- **assessment** of functional safety realisation

More detailed directions in scope of above-mentioned requirements realisation techniques, tasks imposed by provisions of standard, as well as to what degree result of this actions influences requirements imposed on individual Instrumentation instruments related to automatic protection system, are described in the following paragraphs.

5.1 General issues

Safety in depiction of PN-EN 61508 standard is treated in connection with possible hazards and corresponding to them risks connected with plant operation (which does not mean, however, that during standstill or repair such hazards do not occur!). Therefore the requirements, imposed by this standard in scope of safety management have its references to risk level, and tasks put on automatic protection system relate to limitation of this risk to acceptable level. And although risk of incurring of losses, according to the standard, relates mainly persons, proceeding ensuring safety is required in relation to property and environment as well.

In scope of safety related legislation, directive 96/82/WE „on control of serious failures hazard related to dangerous substances" (SEVESO II) should now be called, which aims at „serious failures prevention (…) and limitation of their effects to population and natural environment". Intention of requirement for use of rules included in PN-EN 61508 standard is also to deliver adequate material for creation of „safety report" required by above-mentioned directive, the report, which individual requirements show analogies to PN-EN 61508 standard. Therefore, while referring to basic provisions of GLSA policy on serious failures counteracting, one should treat PN-EN 61508 standard as technical determinant, good engineering practice when preparing adequate input to safety report, with particular attention paid to automatic protection system. Such actions shall always be coordinated with process engineering branch, with consideration of specification GLSA 1170 in subject scope.

When working on the grounds of PN-EN 61508 standard, identification of potential hazards shall be treated as widely meant analysis, transgressing in some points beyond directive SEVESO II scope. Safety shall be referred not only to persons and environment, but also to property. Hazard sources shall be sought and identified in properly defined and conditioned object (with consideration given to, for example, environment), while not restricting dangers only to those, where substances considered dangerous are involved.

It is required that for safety approach principle of risk reduction by preventing (precluding) of dangerous events rising shall be used, and not only by use of measures minimising effects of failure (those are not included within subject of this specification).

5.2 Requirements concerning conformity of designing to requirements of standards

PN-EN 61508 (all parts) and PN-EN 61511 (all parts)

In depiction of PN-EN 61508 and PN-EN 61511 standards, functional safety of plant is achieved by oriented actions on all phases of plant „lifetime", i.e. starting from conception, through base design, technical design, make and operation until final disassembly – liquidation of the plant.

Three phases of plant lifetime can be distinguished:

- Analysis and conception – base design
- Development of technical design
- Erection and commissioning of a plant

Each phase of plant life cycle can be further divided on stages, within which specific works connected with introducing or maintaining of safety are executed.

Work stages characteristic for each phase are shown on diagrams 1, 2 and 3.

Caution:

Below, after description of each work stage, a paragraph Documentation appears. It contains information on documentation (set of documents) required by LOTOS Group S.A., which must be delivered by organisation responsible for specific stage.

Moreover, contractors – organisations responsible for specific stage of works or its part (sub-contractors), must perform additional actions in parallel with these phases, such as:

- Safety management according to directions given in PN-EN 61508-1, paragraphs 6, or PN-EN 61611-1 paragraph 5.
  Documentation
  A report appropriate for particular work stage, confirming fulfilling of requirements given in PN-EN 61508-1 paragraph 6, or in PN-EN 61511-1 paragraph 5, prepared by organisation responsible for specific stage.
- Provision of technique and measures aiming at avoiding and control of systematic failures, adequate for SIL level required, according to directions given in PN-EN 61508-2 Annex A and B.
  Documentation
  A report appropriate for particular work stage, confirming fulfilling of requirements given in PN-EN 61508-2 Annex A and B, prepared by organisation responsible for specific stage.
- Creation of „Safety Plan", determining actions that are necessary to perform, along with assignment of persons – groups responsible for specific task. The plan shall be a document that is constantly updated, and stored through whole lifetime of the plant. Detailed directions can be found in PN-EN 61511-1 paragraph 6 or PN-EN 61508-1 paragraph 7.
  Documentation
  "Safety Plan" according to guidelines included in PN-EN 61511-1 paragraph 6 or PN-EN 61508-1, paragraph 7.
- To organize of regular in-house safety audits, reviews of actions being undertaken and revisions / modifications introduced, during whole lifetime of the plant, starting from base design. Dedicated team of persons of adequate skills and experience, appropriate for specific plant type, shall be appointed for this purpose.
- To comply of Functional Safety Assessment (FSA), performed by external organization or interdependent person, after the following stages:
  - Hazard assessment, allocation of safety functions, creation of Safety Requirements Specification (SRS)
  - After technical design stage
  - Installation of SIS devices and verification of their proper configuration and operation (pre-commissioning)
  - After modifications and prior to SIS disassembly
    Precise direction in subject of „Functional Safety Assessment" can be found in PN-EN 61508-1, paragraph 8.

Documentation:

1. Confirmation of Functional Safety Assessment (FSA) completion (if required for specific work stage)
2. Confirmation of completed internal audits, on GLSA request
3. Confirmation of competences of persons connected with functional safety, on request of GLSA

5.2.1 Analysis and conception – base design

LOTOS Group S.A. verifies assumptions, requirements and restrictions resulting from basic design stage or elaborat done by expert in relation to newly designed plant, such as:

- Definition of loss – i.e. determination if directions of PN-EN 61508 standard shall serve protection of human life, protection of property, or possibly protection of environment. Simultaneous joining of several aspects is also possible.
- For life protection criterion: Number of persons in place of danger, stay duration, means of protections against injuries.
- For property protection criterion: Amount of production losses, amount of equipment losses.
- For environment protection criterion: Type of hazard and its effects.
- Acceptable methods of risk assessment.
- Tolerable risk
- Assumed plant lifetime
- Time for plant operation restoration after shutdown
- Acceptable time between spurious shutdowns (MTTFS)
- For sensors, control system (SIS-PLC) and executing elements – interval between proofing tests (PTI), degree of failures detectability (PTC) and restoration time (MTTR).
  It shall be assumed, that periodical proofing tests shall be performed during plant standstill. In relation to this, time interval between periodical tests for measuring instruments, executing devices and SIS-PLS shall be not shorter than planned interval between plant standstills increased by 50%. In case of SIF and measuring and executing instruments connected with it, for which periodical proofing tests are being performed on-line (without interruption to normal plant operation), time interval between these tests can be shortened after adjustment with GLSA.

All assumptions assumed for calculations shall be always submitted for GLSA acceptance.

When creating safety systems, one shall always follow below given directions:

- One shall model on existing, proper solutions of analogous processes and previous solutions
- PN-EN 61508 / PN-EN 61511 standard do not release from keeping to „good engineering practice"
- It shall be remembered, that safety is achieved not only by establishing of automatic protection systems, but also by proper system of work organization and monitoring of failures.

On basic design stage it is necessary to perform identification of hazards and analysis of existing risk, aiming at:

- recognition of hazards and their effect
- assessment of hazards' likelihood
- assessment of required risk reduction
- evaluation if used process engineering, mechanical and other protections, beside safety functions accomplished by automatics elements are sufficient, and if not then:
  - creation of protecting functions accomplished by E/E/PE systems, reducing risk to level of acceptable risk, and isolation of SIF functions from them
  - definition of requirements within SRS for SIF functions, providing for achieving of tolerable risk.

One shall endeavour for the plant to be safe on its own accord, i.e. that additional protection layers would not be required for it. If this is impossible, then mechanical protections shall be employed, e.g. safety valves (PSV), and if even this is not sufficient, then functions accomplished by E/E/PE systems shall be used.

Recognition of hazards resulting from normally operating plant is insufficient, therefore professionals specialising in safety of specific type plant shall be employed for purposes of this analysis.

Detailed requirements regarding hazard analysis are presented in PN-EN 61511-1, paragraph 8.

Specification of SRS requirements must include, for each function:

- Precise description of each function (input and output definition)
- Definition of measuring values range and threshold values of logics tripping
- Requirements for executing elements, such as Tight Shut-Off
- Definition of logics used in controller and requirements as to software
- Definition of safe condition
- Mode of operation (Low Demand/ High Demand)
- Definition of required safety level SIL and risk reduction factor RRF (or PFD_{avg})
- Intervals of proofing tests for sensors, controller and executing elements.
- Required response time – execution of safety function
- Replacement time of damaged elements (according to assumptions of LOTOS Group S.A.)
- Environmental requirements that can influence operation of functions
- Tripping method of function Energized /De-energized to trip
- Resetting methods – if any.
- Required minimum time between spurious shutdowns (according to assumptions of LOTOS Group S.A.)
- Description of used diagnostics, if any
- Is it possible to trip functions manually?
- MOS, POS usage for functions

- Behaviour of functions on supply failure
- Requirements for operator
- Links to other systems
- Method of operator's action if errors in operation of functions are noticed
- Others, which influence SIF function operation.

Detailed directions for SRS requirements specification are included in PN-EN 61511-1, paragraph 10.3.

Documentation:

- Description of plant operation technology used in basic design, with particular attention paid to safety aspects.
- Full report and results of hazards and risk analyses, along with SIF protecting functions assigned and RRF or PFD_{avg} required from them.
- Specification of SRS requirements

Chart of proper actions for safety and operation conception analysis phase is presented on diagram 1.

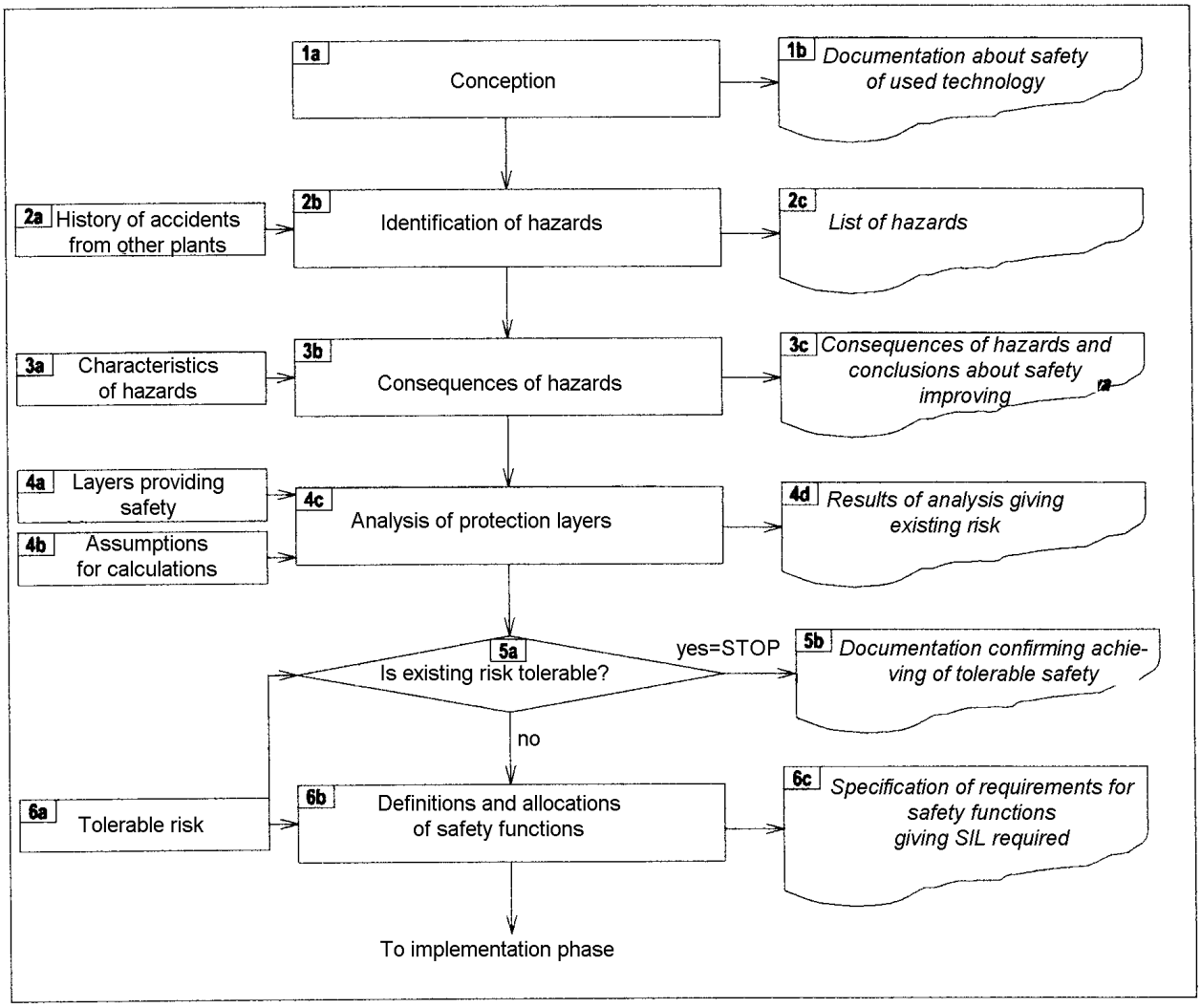

Diagram 1. Analysis and conception phase – basic design

5.2.2 Engineering design execution

Risk reduction factor RRF or PFD_{avg} required from each safety function, must be computed for each safety function.

Such safety functions, for which RRF is greater or equal to 10 „become" SIF functions with defined SIL level, and only them constitute subject of PN-EN 61508 and 61511 standards' requirements. The functions shall be implemented in SIS-PLC system.

The functions, for which calculated RRF is lesser than 10 are functions that do not subject to requirements of PN-EN 61508 and 61511 standards. These functions shall be implemented in ESD-PLC system or left in system destined for SIF functions, taking into account, however, that the same restrictions shall be valid for them as imposed by PN-EN 61508 and 61511 standards for SIF functions.

Reliability of operation for equipment included in SIF safety functions must be tested by manufacturer and confirmed with adequate documents (refer to p. 5.6 and 5.7). Process of SIF functions verification against requirements imposed in SRS and confirmed by LOTOS Group S.A. results in directions as to required type, reliability and architecture of SIF functions elements. Initially set configuration of SIF functions equipment can be changed in such a way, so that SRS requirements would be met (e.g. change of single transducer on two in 1oo2 configuration). This is shown on diagram 2, block 8a.

Verification process must be documented.

Results of verification process can cause changes in several linked documents, for example Cause and Effect Diagram, technical specifications, process engineering diagrams, plant operating instructions and others. It is necessary to ensure that all changes and requirements as to properties of equipment and its further operation would be reflected in adequate documents and would not be oversought.

During engineering design phase process of HAZOP project verification has to be completed as well, because designing according to PN-EN 61508 / PN-EN 61511 directions does not release from usage of expert techniques.

Final documentation shall contain all data on equipment reliability, certificates and other assumption, used for calculations.

Additional documents containing information connected with achieving and maintaining of required safety level shall be created, if required. They can contain requirements regarding assembly and operation, as well as disassembly of SIS equipment.

After completion of designing phase one shall perform validation of design works and commission independent person or organization to perform assessment of functional safety. Precise directions on „Functional Safety Assessment" can be found in PN-EN 61508-1, paragraph 8.

After completion of plant designing phase, general contractor of project shall create a document – guide, which puts in order all documents (also those created by sub-contractors) into one package of plant functional safety documentation.

Above-mentioned leading document shall serve as key to all safety related documents. This means, that requirements for functional safety provision are contained only in it and in documents referred to in it, and in no other place.

Above-mentioned leading document and documents referred to in it, create package documenting conformity of project to requirements of PN-EN 61508 and PN-EN 61511 norms for LOTOS Group S.A.

Documentation:

- Documentation of completed verification
- Placing of safety related information into all relevant documents
- Documentation of assumptions to calculations (certificates, conditions of certificates' validity)
- Documentation of safety related requirements achieving and maintaining
- Creation of leading document for all safety related documents
- Confirmation of completed validation
- Confirmation of assessment completed by independent organization

The phase connected with project execution was illustrated on diagram 2.

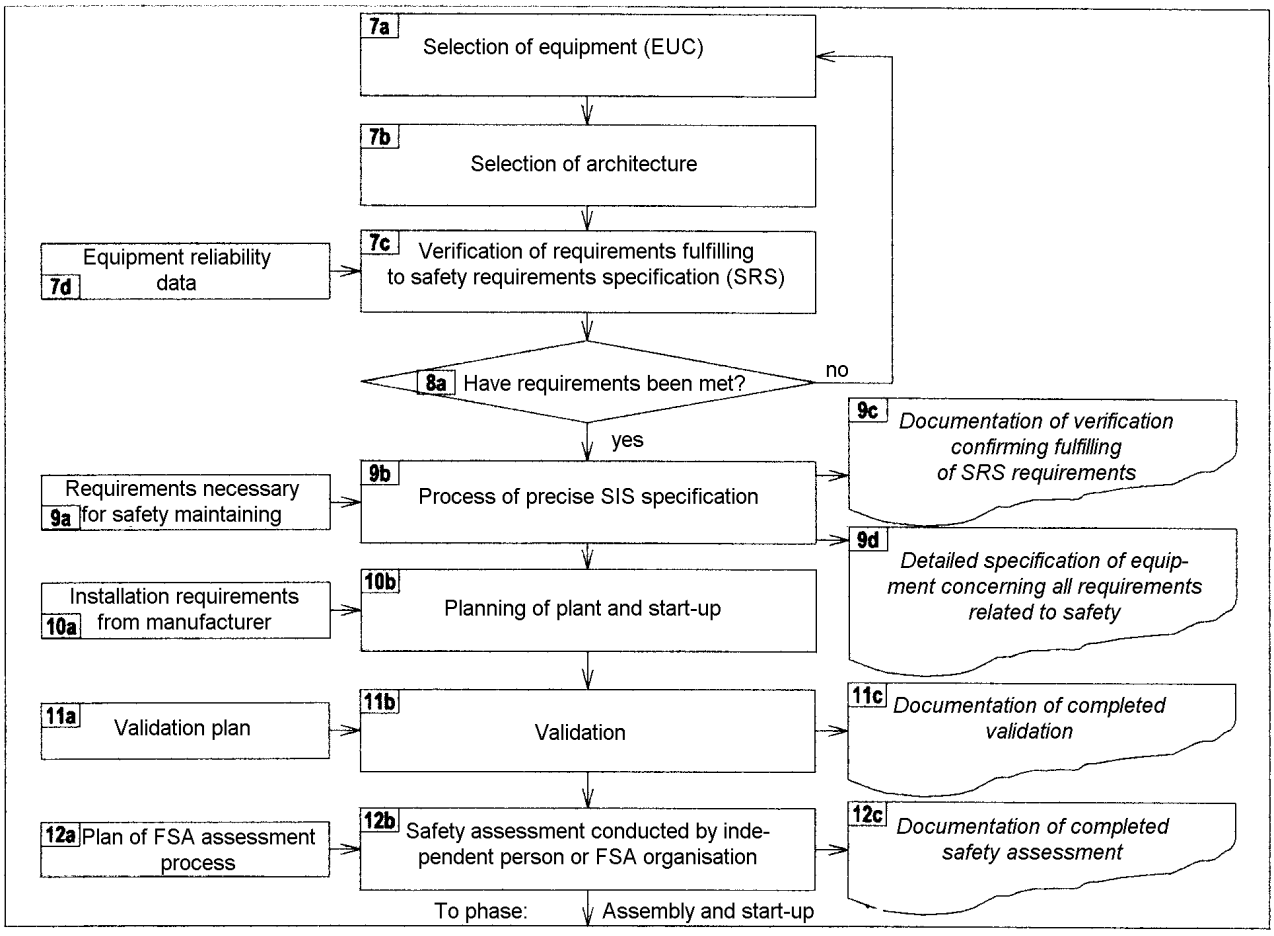

Diagram 2- Phase – execution of engineering design

5.2.3 Erection and start-up

Engineering design shall be ended with FAT tests. Requirements concerning the tests are presented in PN-EN 61511-1 paragraph 13.

After assembly of equipment on the plant and prior to starting it up, independent person or organization (refer to PN-EN 61508-1 paragraph 8, and also PN-EN 61511-1 paragraph 15) has to perform assessment of SIS system. This action consist in among other things verification ,of equipment assembly correctness, their connections, method of marking, values of thresholds tripping SIF functions activation, required operation times of individual SIF functions, correctness of their operation and other requirements included in safety documentation package. Adequate document, confirming completion of verification and assessment, shall be issued.

Passing on to plant starting-up is possible only after positive FSA assessment and elimination of possible discrepancies.

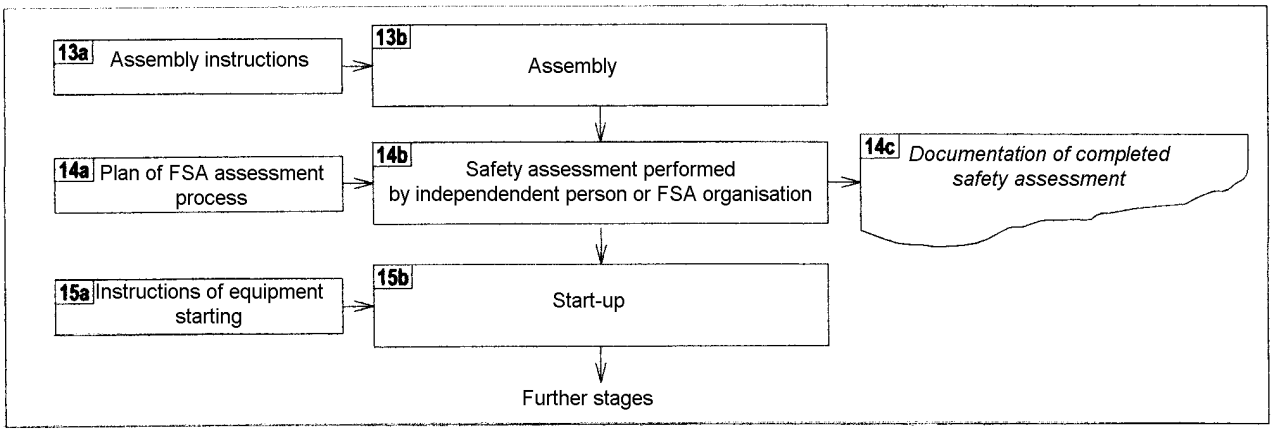

Diagram 3 – Phase –erection and start-up

The residual stages, such as operation, keeping the plant operational, modification of SIF functions and their disassembly do not constitute subject of this specification.

5.3 Techniques employed in automatic protection systems

For individual elements of the system one shall use commonly known and accepted techniques (methods of implementation, equipment properties), which help, and sometime constitute essential requirement for implementation of automatic protection systems. Some of them, which shall be followed when designing, specifying and constructing, are listed below.

FAIL SAFE – this term shall be referred to all Instrumentation devices connected with automatic protection systems both in scope of software and hardware, and consist in transition of specific element – device to proper for particular event safe condition in case of failure. Notion of failure depends on specific case, e.g. for valve it means that in event of lack of supply air or breaking of electrical connections, the valve transits in effect of spring action to defined safe position. For examples refer to p. 5.6 and 5.7.

FAULT TOLERANCE – according to PN-EN 61508 norm, ability of functional system to continue required function (serving consigned tasks), at presence of faults or errors. FAULT TOLERANCE term is connected with known and widely used REDUNDANCY and VOTING techniques. Functional system serving measurement of process parameter with '2oo3' voting can be quoted here as an example. Three REDUNDANT elements with VOTING have been used here (the function is executed if at least two sensors indicate such necessity), while FAULT TOLERANCE of the system amounts to one (the function shall be properly executed when not more than one sensor is damaged).

DIAGNOSTICS – as attribute or mechanism verifying correctness of equipment or software operation, is recommended technique in relation to individual devices, and also the system that they are forming. Diagnostics of equipment and implementation of mechanism detecting faults of functional system, enables realisation of automatic protection systems in more effective and efficient way. Diagnostic signals shall be first of all obtained (read-out, interpreted), and then properly used for intended purpose. Essential parameter in relation to equipment diagnostics is so-called DIAGNOSTIC COVERAGE, giving information about percentage of detected failures. There are some types of diagnostics, e.g. diagnostics performed internally by specific equipment, that is self-diagnostics, diagnostics performed by equipment on demand (e.g. valve test – Partial Stroke Test), or diagnostics at workshop after its disassembly in advance.

DIVERSIFICATION – that is the method used for redundant equipment, consisting in differentiation of measures types in order to achieve the same aim. Two different (mutually INDEPENDENT to large extent) types of transmitters, serving process parameter measurement and operating in 1oo2 voting arrangement can be quoted here as an example. It can be also implemented by use of transmitters manufactured by various producers or based on different measuring methods measuring the same parameter and used within the same safety function. Another, practical differentiation for selection of measures is realization of dual-channel disconnection (e.g. from pushbutton): through ESD-PLC and through independent path, e.g. by means of relays with auxiliary contacts adequately connected into control or supply circuits of any related executing equipment. Application of various types equipment can improve reliability of the whole system by several times.

5.4 Configurations of measuring elements used within SIF functions

Meaning of most frequently used configuration of measuring elements within SIF functions according to PN-EN 61508, is given below.

Voting 1oo1

The architecture contains single channel, where each dangerous failure of the channel (λ_D) results in failure of SIF function execution on reported demand – in such case the functions losses ability to execute consigned task.

Purely formal, any diagnostics (if any) has no influence on system output condition, and its results are only reported. Nevertheless, according to specifics of Instrumentation equipment currently present on market, and broad programming possibilities, effects of equipment diagnostics (even such partial one) can be separated in form of binary signal(s) and properly programmed. In case of such system defects' detection, it is required that the function transits to safe state. It is, however, necessary to assume 1oo1 configuration (and not 1oo1D !) for verifying calculations of systems without separate output to diagnostics results signalling.

Voting 1oo1D

The architecture contains single channel, where part of dangerous failures (λ_{DD}) is detected by diagnostics. It has such advantage over 1oo1 voting, that in case of dangerous failure detection by diagnostics, the system transits to safe state, and therefore system reliability is greater than in case of 1oo1 configuration. Such devices mostly have separate output to signalling of diagnostics results.

Voting 1oo2
The architecture consists of two channels connected in such a way, so that each of them can execute SIF function. Hence the two channels have to be simultaneously damaged for the function execution failure. If any diagnostics exists, then its results are only reported, not influencing output or voting state.

Voting 1oo2D
The architecture contains two channels connected in such a way, so that during normal operation both channels have to demand execution of SIF function, in order for it to be executed. Furthermore, if channel failure is detected in any of the channels, then voting is modified in such a way, so that system output depends only on state of the second, properly working channel. If diagnostics indicate failure in both channels, or such discrepancy between them that cannot be assigned to specific channel, than system output is set in safe state. Discrepancy between channels must be detected with measures that are independent of operation of these channels.

Voting 2oo2
The architecture contains two channels connected in such a way, that both of them must demand execution of the function before it would be executed. If any diagnostics exists, then its results are only reported, not influencing output or voting state.

Voting 2oo3
The architecture contains three channels connected parallel in majority voting between inputs in such a way, so that input signal would not change if only one channel produces signal demanding execution of SIF function, contradicting the two other channels that do not report such demand. For initiate execution of function at least two channels must demand it.If any diagnostics exists, then its results are only reported, not influencing output or voting state.

Voting NooM
The architecture contains M channels connected in such a way, so that N channels have to demand execution of function, before it would be executed. If any diagnostics exists, then its results are only reported, not influencing output or voting state.

5.5 Configuration of executing elements

Meaning of most frequently used configurations of executing elements according to PN-EN 61508, is given below.

Voting 1oo1

The architecture contains single executing element, where any dangerous failure (λ_D) results in lack of SIF function execution.

Voting 1oo2

The architecture contains two executing elements connected in such a manner, that any of them can execute SIF function. Hence, in order for the SIF function to be not executed, both the executing elements must simultaneously fail.

Voting 2oo2

The architecture contains two executing elements connected in such a way, so that both them must properly actuate in order for the SIF function to be executed. Hence, failure of single executing element is sufficient for the function to be not performed.

Voting NooM

The architecture contains M executing elements connected in such a way, so that N elements have to properly actuate in order for the SIF function to be performed.

5.6 Requirements regarding measuring and executing instruments

Scope of Instrumentation equipment for automatic protection system purposes, results directly from detailed SIS design, remaining in conformity to safety requirements imposed in SRS. This means that individual elements of SIS system (as for example pressure transmitters, blocking valves), their number, configuration, as well as detailed requirements as to their required reliability, are known on this stage.

Elements of SIF function shall be particularly resistant to interferences, such as electromagnetic, vibrations and operation specific for installation place. Attention shall be paid so that SIF function elements would not operate at their limit parameters, such as current, voltage and environmental conditions (adequate safety margin shall be kept).

In case of excessive sunlight operation in place of equipment installation, protection roof shall be used, and IP enclosure class shall be selected with safety margin taken into account.

Constructions of measuring and executing elements shall be mechanically tough (accidental knocking against them cannot result in their damage).

Working point of transmitters shall not be located near beginning nor near end of measuring range.

Equipment constituting part of SIF functions cannot be used for execution of any other functions. Use of these elements in SIS system, and for purposes of any functions in another system, is prohibited. It means that also tap connections and impulse lines to transmitter shall be used and dedicated for safety function only.

Each measuring, executing or intermediary (e.g. barrier) element, shall be adapted to required SIL safety level. This adaptation consists in:

1. Application of element of required guaranteed reliability (documentation, refer to p. 5.6.1).
2. Application of equipment redundancy level adequate to SIL, according to PN-EN 61508-2 7.4.3, Table 2 or Table 3, or PN-EN 61511-1 11.4, table 6.
   Recommendation of paragraph 5.7.5 shall be taken into account in relation to equipment redundancy.
3. Application of systematic failures monitoring adequate to required SIL level (refer to p. 5.2).

Application of measuring and executing equipment possessing certificate of conformity according to PN-EN 61508 is preferred.

Non-electrical equipment, such as e.g. pneumatic valve, despite they do not directly subject to restrictions of PN-EN 61508 standard, shall also be certified product (because reliability of defined SIF function, to which the valve belong, depends to large extent on reliability of this valve operation).

Application of transmitters in SIF functions is preferred, considering their higher reliability and wider possibilities of errors' detection by transmitters, as distinguished from signalling devices. This is additionally supported by fact, that transmitters constitute majority of certified measuring instruments (during writing of this specification).

All equipment must operate as FAIL SAFE.

In case of electric energy failure, output signal from transmitter (or signalling device) for measuring elements shall be low, similarly as in case of cabling continuity breakage.

In case of signalling devices, application of proximity signalling devices conforming to PN-EN 60947-5-6 (NAMUR) standard is recommended.

When signalling devices with potential-free contact are used, then devices having certificate of conformity to PN-EN 61508 standard shall be selected.

For executing equipment in case of low level of control signal, or breakage of connections' continuity, executing element shall automatically and without external energy supply, transit to condition safe for the plant – „de-energize to trip". This applies both to electrical energy supply failure and pneumatic or hydraulic supply.

Interfaces of measuring and executing equipment used within SIF functions shall be protected against change of parameters by non-authorized persons. Change of any parameters for these devices shall proceed according to GLSA procedure valid in this respect, and is connected with necessity of SIS modification rules observance, described in PN-EN 61508/61511 standards.

Change of parameters that are of key importance for equipment safety can be done only by persons responsible for functional safety in LOTOS Group S.A., specified in „Safety Plan" document.

Manipulating elements of transmitter (signalling device) valve block shall be removable, or equipped with interlock. The same applies to other valves on path of transmitter (signalling device) process connections.

The purpose of this protection is to protect against disturbance of measuring elements operation. The protection would be possible to remove or unblock only by persons responsible for functional safety in LOTOS Group S.A.

Separate I/O modules shall serve elements of redundant systems.

It is particularly recommended to use devices of various types (of different operating principle or of different make, refer to Diversification p. 4.3) in redundant configurations, as well as in systems of different protection layers but connected with single, specified hazard (e.g. the first transmitter in DCS regulation system, and the second, of different type, in SIS safety system).

In order to trip operation of SIS system executing elements, it is necessary to provide pushbuttons (manual means) independent from SIS-PLC, unless otherwise ordered by safety requirements specifications.

Equipment having certificate of conformity to PN-EN 61508 standard are preferred, as distinguished from Proven in Use or Prior Use documentation.

In case when many measuring and/or executing devices of SIS system exists in nearby location, they shall be connected to dedicated junction boxes, to which equipment operating in SIS system shall exclusively be connected. Moreover, it is recommended to connect equipment forming redundant system to different (separate) junction boxes.

In cases where SIF function circuits and other circuits are present in single box, then in relation to connections in junction boxes (separation of signals), records of paragraph „Junction boxes" in specification GLSA 3110 are valid.

Measuring and executing elements constituting part of SIF functions shall be marked in a manner enabling easy identification from among elements that do not constitute parts of SIF functions. Details of marking execution are included in specification 3030, paragraph 5.3.2.1.

5.6.1 Documentation for measuring and executing equipment forming part of SIS

Documentation required by LOTOS Group S.A. for measuring and executing equipment constituting part of SIF functions is presented below.

If device possesses certificate of conformity to PN-EN 61508 standard, then the following documentation is required:

a) In case when method of specific device operation is complex or may not be obvious, e.g. a valve with complex control system, then description of operating principle of the device shall be presented, with detailed representation of issues influencing operating reliability

b) Reliability factors of the device, specifying failures detected by internal diagnostics of the device - λ_{DD}, λ_{SD}

c) Reliability factors of the device, specifying failures undetected by internal diagnostics of the device - λ_{DU}, λ_{SU}

d) Environmental requirements (can be included in certificate)

e) Life cycle of the device

f) Suggested frequency of periodical proofing tests and possible proofing tests coverage (PTC)

g) Frequency of internal self-diagnostic tests (performed by the device itself)

h) Proofing tests coverage for internal self-diagnostic tests

i) Directions as to mean time to restoration (MTTR) – device replacement

j) Maximum SIL level (for specific configuration), at which the device can operate

k) Certificate of conformity to PN-EN 61508 standard

l) Documentation of conditions (environmental, operation and other) that must be met in order to preserve validity of certificate

Notes:
1) Points g) and h) are required, if internal tests of the device are taken into account in calculations of reliability.
2) Points from b) to i) are needed for PFD calculation for device
3) Points b), c), g), h) are required if measuring or executing device can be used in redundant architecture. If such situation does not take place, then specification of PFD_{avg} is possible, but directions of f) point shall be given in such case.

If device does not have certificate of conformity to PN-EN 61508, then the following documentation is required:

a) In case when method of specific device operation is complex, e.g. a valve with complex control system, then description of operating principle of the device shall be presented, with detailed representation of issues influencing operating reliability

b) Reliability factors of the device, specifying failures detected by internal diagnostics of the device - λ_{DD}, λ_{SD}

c) Reliability factors of the device, specifying failures undetected by internal diagnostics of the device - λ_{DU}, λ_{SU}

d) Environmental requirements

e) Life cycle of the device

f) Suggested frequency of periodical proofing tests and possible proofing tests coverage (PTC)

g) Frequency of internal self-diagnostic tests (performed by the device itself)

h) Proofing tests coverage for internal self-diagnostic tests

i) Directions as to mean time to restoration (MTTR) – device replacement

j) SFF factor, or data necessary for its calculation

k) FAULT TOLERANCE parameter for the device

l) Documentation Proven in USE according to PN-EN 6508-2 7.4.7, or Prior Use according to PN-EN 61511-1 11.5.3.

Notes:
1) Points g) and h) are required, if internal tests of the device are taken into account in calculations of reliability.
2) Points from b) to i) are needed for PFD calculation for device
3) Points b), c), g) and h) are required if measuring or executing device can be used in redundant architecture. If such situation does not take place, then specification of PFD_{avg} is possible, but directions of f) point shall be given in such case.

5.7 Requirements regarding SIS-PLC programmable controller

SIS-PLC controller, in which SIF functions have been implemented, shall be particularly resistant to interferences, such as: electromagnetic, temperature, humidity, vibration and operation specific to its installation place.

Attention shall be paid so that modules of SIF functions elements would not operate at their limit parameters, such as current, voltage and frequency (adequate safety margin shall be kept).

All detailed requirements come from safety requirements specifications, resulting from cross-sectional study of previously defined SIF functions, and operating reliability requirements imposed on them.

Specific requirements imposed in the following paragraphs in relation to SIS-PLC, constitute complement of basic requirements for PLC controllers, described in specification GLSA 3640. This applies both functionality and installation. Shall any discrepancy arise, directions of this specification would prevail.

SIS-PLC programmable controller can serve measuring and executing equipment constituting part of SIF functions, and in exceptional cases, devices constituting safety functions without defined SIL level.

Functions, for which calculated RRF is less than 10, do not subject to requirements of PN-EN 61508 nor PN-EN 61511 standards. Those functions shall be implemented within ESD-PLC system, or on GLSA approval, within SIS-PLC system intended for SIF functions, taking into account, however, that the same restrictions and requirements as imposed on SIF functions by PN-EN 61508 and 61511 standards, shall be obligatory for them.

It is recommended that ESD-PLC controller shall execute only functions without specified SIL level, and that separate controller (SIS-PLC) shall be provided for SIF functions.

If separate controller is foreseen for SIS system, then it has to be independent from other systems. Similarly, ESD-PLC controller shall be a system independent from other systems.

Operation of SIF functions shall be independent from operation of other safety related functions.

FAULT TOLERANT and FAIL SAFE requirements shall be applied towards SIS-PLC and ESD-PLC controllers.

The controller in which SIF functions are implemented, must fulfil SIL requirements on level equal to at least maximum level from among of SILs for function served by the controller.

SIS-PLC controller must have adequate certificate of conformity to PN-EN 61508 standard, as distinguished from documentation Proven in Use or Prior Use (for requirements, refer to p. 5.7.1). The controller (and its certificate) shall foresee possibility for on-line introduction of changes to software, i.e. without interrupting of operation both the controller and object. Complete SIS-PLC, considering modules such as CPU, I/O and internal communication links and others, required for this purpose, must fulfil requirements imposed in SRS.

Conformity of SIS system controller implementation to PN-EN 61508 standards shall be confirmed by adequate documentation – refer to p. 5.7.1.

Degree of SIS-PLC controller redundancy depends on required SIL level and shall correspond to requirements of PN-EN 6508-2 7.4.3 Table 3, or PN-EN 61511-1 11.4 table 5, but cannot be less than one.

Adequate diagnostics implemented in SIS system shall detect breakage of measuring instruments cabling continuity, and shall perform system reduction or initiate execution of SIF function, depending on their configuration (refer to p. 5.4).

If diagnostics of measuring and executing elements implemented in SIS-PLC system detects element damage, then signalling of this damage shall proceed independently from DCS system operation, or if it takes place by means of DCS system – then subjects to periodical proofing tests similarly as the element which it is linked to.

The following information of key importance for keeping of adequate SIL level for specific SIF shall be available for operator:

- Current operating state of the function
- Signalling of function activation
- Signalling of function operation blockage
- Results of diagnostics and indication of redundant systems' degradation degree (refer to e.g. voting 1oo2D, p. 5.4).

- Condition of measuring and executing elements
- Failures of devices influencing proper execution of SIF, e.g. failure of regulation systems of environmental conditions (heating, cooling, ventilation).

Interface of SIS-PLC station shall enable execution of the following functions, while ensuring adequate protection against unauthorized access for each of them (separate access password).

- SIS operating mode, program, data, measures of alarms' cancelling, tests, forcing of I/O state, maintenance
- SIS diagnostics, voting and handling of errors
- Functions adding and removing, software modification
- Module of program analysis and errors' searching

Access to writing into SIS system memory shall be enabled only from SIS system level and only for persons of adequate authorizations, foreseen by LOTOS Group S.A.

SIS system shall be designed in such a way, so that despite of failure or interference on communication links of this system to other system, SIS-PLC operation would be possible until rectification of communication failure, as well as bringing of SIF function by SIS-PLC to safe state in case of necessity.

SIS-PLC system shall enable testing of SIF function along path starting at measuring element up to executing element.

Required system scanning time Ts (total time required for: inputs read-out, logics execution and processing of output states, storing of outputs), shall be determined with consideration given to safety requirements specification for all defined SIF, and distribution of SIF function response time on its individual elements (measuring instruments, SIS-PLC, executing devices). Scanning time Ts must satisfy inequality: Ts <= (required time of entire SIF function execution) – (time necessary for measuring and executing elements).

Controller implementing SIF functions shall meet requirements regarding systematic failures monitoring imposed by PN-EN 61508-2, table A.16.

5.7.1 Documentation

Documentation required by LOTOS Group S.A for controllers handling SIF functions, is presented below.

Because SIS-PLC controller shall have certificate of conformity to PN-EN 61508, so the following documentation is required for it:

a) Description of controller operation with detailed presentation of issues influencing reliability of operation

b) Equipment reliability factors determining failures detected by internal diagnostics of equipment - λ_{DD}, λ_{SD} for all modules influencing SIF function execution

c) Equipment reliability factors determining failures not detected by internal diagnostics of equipment - λ_{DU}, λ_{SU} for all modules influencing SIF function execution

d) Environmental requirements (can be included in certificate)

e) Life cycle of equipment

f) Suggested frequency of periodical proofing tests and possible proofing tests coverage (PTC)

g) Directions as to mean time to restoration (MTTR) – device replacement

h) Maximum SIL level (for specific configuration), at which the device can operate

i) Certificate of conformity to PN-EN 61508 standard

j) Documentation of conditions (environmental, operation and other) that must be met in order to preserve validity of certificate

5.7.2 I/O modules

Preferred solution for I/O signals in scope of protection against explosive atmosphere is application of intrinsically safe circuits. Exi separators, apart from certificates of conformity to intrinsic safety requirements, have to possess certificate of conformity to PN-EN 61508 standard (documentation according to p. 5.7.1). The following I/O module types are foreseen for purposes of connecting external signals to SIS-PLC:

- INPUTS
  - 4-20mA
  - binary of NAMUR type, for inputs from proximity sensor conforming to PN-EN 60947-5-6
- OUTPUTS (two-state)
  - potential-free contact,
  - 0/24V DC,

Furthermore, binary NAMUR type inputs, shall be adapted to handling signals of potential-free contact type (e.g. for RESET type signals, MOS, certified contact-type equipment purposes).

Maximum number of filled I/O points on single I/O module cannot exceed:

- 8 channels for 4-20 mA inputs and NAMUR
- 8 channels for two-state outputs

When considering protection, within framework of single group of signals, limit of 8 signals maximum for one fuse is valid.

For redundant systems it is recommended to connect redundant measuring and executing elements to different I/O modules. Similarly signals related to redundant process equipment (e.g. stand-by pumps) shall be connected to different I/O modules.

5.7.3 Central processing unit – CPU

Application of redundant modules in form of separate devices is assumed as minimum requirement in scope of CPU redundancy. Above-mentioned FAIL SAFE and FAULT TOLERANT requirements find application here.

5.7.4 Software

In scope of SIS-PLC and ESD-PLC programming languages, requirements of PN-EN 61131-3 are in force. Allowable representations are as follows:

- FBD - functional block diagrams
- LAD - ladder diagram

- SFC – sequential function chart

If common SIS-PLC controller shall be used for implementation of SIF safety functions, as well as functions without specified SIL level, then programs and logics specific for them shall be placed in separate program modules.

Source code shall be simple, legible and comprehensible, as well as shall enable testing and further modifications. Descriptions of states "0" and "1" also of internal variables are mandatory. As far as possible, the designs shall minimize this part of the program, which is related to safety.

FIRST OUT logic shall be implemented in the program, enabling quick identification of initiating event in situations, when partial or whole plant disconnection takes place.

Access to SIS system software shall be protected against access of unauthorized persons. Changes in software can be introduced only by persons responsible for functional safety in LOTOS Group S.A., specified in „Safety Plan" document.

Moreover, as regards programming and „on-line" changes, provisions of certificate and safety manual of SIS-PLC controller shall be stringently adhered to in this respect. Essential modifications or modernizations shall be performed during standstill of plant. Recommendations of all called procedures of PN-EN 61508/61511 standards, regarding modification of systems, shall be each time observed.

Possible firmware replacement require necessity of carrying out full procedure of automatic protection system (SIS) re-commissioning.

5.7.5 Input/output forcing, MOS signals

Forcing of inputs or outputs states in SIS-PLC controller cannot be used as component of:

- application program
- operating procedures (plant process engineering)
- operation upkeeping, with above-mentioned exception

Forcing of SIS-PLC inputs or outputs state prior to SIS stopping (shutdown) is impermissible, unless performed with use of adequate procedures and access protection foreseen by LOTOS Group S.A. Application of forcing must be adequately notified (announced), or an alarm must be activated.

Forcing and MOS usage shall be adequately protected against unauthorized access.

If deblocking has been established for SIF function (MOS, forced I/O state), then alarms and manual measures serving bringing of SIF to safe state cannot be blocked.

MOS signals for non-redundant configuration of measuring and executing elements and SIF function operating in „low demand" mode, can be applied only if:

- The function is brought to safe state in advance
- Application of other measure ensuring safety on level that is at least equal to the level provided by „by-passed" SIF function, for period of MOS signal duration. This period cannot exceed MTTR time assumed for calculations. After expiration of this time, operation of SIF function must be restored in full configuration, and MOS signal have to be automatically removed (deactivated) by SIS-PLC system, or SIF function must achieve safe state.

For safety functions, essential from plant running point of view (e.g. where bringing of SIF to safe state entails production interruptions), application of redundant configurations is recommended (even

if not required for safety reasons), in order to enable application of MOS for individual instrumentation equipment.

MOS signals for redundant configuration of measuring or executing elements and SIF function operating in „low demand" mode, can be used only when:

- The function is brought to safe state in advance
- By-passing of one element for MTTR time is applied. During this period functions of system are maintained by not by-passed elements (active ones). After expiration of this time, operation of SIF function must be restored in full configuration, and MOS signal have to be automatically removed (deactivated) by SIS-PLC system, or SIF function must achieve safe state.

For each MOS adequate operator interface must be provided, informing about its status, MTTR time remaining to use, as well as alarm shall be implemented informing that MTTR time draws to an end.

5.7.6 Connections to DCS and other systems

In scope of communication links, connections of SIS-PLC system to DCS shall correspond to requirements imposed on communication between PLC and DCS in specifications GLSA 3710 and GLSA 3640. Furthermore, redundancy of communication links is required.

The signals that are essential from control strategy of plant technology point of vies, shall be exchanged with DCS (or other systems) by means of connections through I/O cards (hardware ones), excluding links of digital communication.

5.7.7 Sequence of Events Recorder (SOER)

SIS-PLC and ESD-PLC shall be equipped with sequence of events recorder (SOER) together with printer. All events shall be stored together with time tag, which is assigned in CPU.

5.7.8 Cabinets

All technical requirements, equipment and installation in cabinet, as well as matter of electrical supply network and requirements regarding supply distribution, are described in specifications GLSA 3640 and GLSA 3130.

5.8 Safety of machines

This paragraph is devoted to machinery safety matter, from the point of view of directions for automatic protection systems application.

5.8.1 Requirements for certificate of conformity

All technical equipment, discussed in these paragraphs, subject to conformity assessment system prior to approving them for operation. Scope of conformity assessment, that is forming its set of regulations, depends on specific equipment. The following new approach directives mainly find application here:

⇒ 2006/42/EC, Machines (MAD)

⇒ 97/23/EC, Pressure equipment (PED)

⇒ 2009/142/EC, Gas appliances (GAD)

⇒ 2009/104/EC, Working equipment

and adequate norms harmonized with above-mentioned directives.

Conformity assessment system is composed of requirements imposed on equipment being tested, and in particular case all safety related requirements, appropriate for the equipment type.

Positive result of conformity assessment process, confirmed with *certificate of conformity* issued by certifying body, constitutes condition for approving the equipment for operation. One shall bear in mind that both the machine and its manufacturing process subject to certification – also, and maybe first of all, with consideration given to adequate safety aspects.

For time of writing this specification, the only notified, certifying Polish body is Office of Technical Inspection (UDT – CERT). In connection with it, all applications for testing shall be directed just to UDT-CERT, while adhering to recommendations dictated by this Office.

Fulfilling of requirements determined by assessment system, as well as completing of all formalities connected with obtaining of conformity certificate, is included within scope of responsibility of the machine supplier (manufacturer), or in case of equipment modernization – contractor of this modification. In particular cases, also authorised representative of manufacturer can be a mover, on behalf of the manufacturer. In case of modernisation of machines, one shall remember about fulfilling of directive 2009/104/EC requirements in scope of adaptation of machines that do not meet current requirements of appropriate directives and norms.

5.8.2 Safety of equipment

Apart from basic requirements contained in directives, it is necessary, in case of specific equipment (i.e. furnaces, boilers, other machines), to fulfil requirements imposed by adequately selected norms, relating to safety matters. Equivocal results here from equipment diversity from the one hand, and that in relation to some equipment various directives can be applied from the other hand, which treat safety in peculiar manner, referring to various sets of harmonized norms. Manufacturer of equipment is responsible for determination of directives/norms relating to specific equipment (which simultaneously are included in conformity assessment system).

Important aspect that shall be emphasised here, is the matter to what (or whom) safety shall be applied to. The following paragraphs are unequivocally defining this question.

5.8.2.1 Furnaces, boilers

1. When boilers are designed and fabricated according to EN 12952 or EN 12953 norm, then in scope of protections based on electrical devices they subject to rigour of conformity to **EN 50156-1** norm. Requirements imposed on protection systems described in this norm, in its approach to safety matters, indicate on analogies to PN-EN 61508 norm (concerning electrical protection devices as well), that EN 50156-1 norm frequently refers to. Despite the PN-EN 61508 norm basically relates to personal safety, the PN-EN 50156-1 norm specifies requirements for provision of personal, property and environmental safety.
2. Another case exists in situation, when furnace safety requirements are based on records coming from PN-EN 746 norm. When designing safety related control systems, hazard analysis, risk assessment, as well as while selecting risk reducing measures, one shall then follow directions of the following norms:

   - **PN-EN ISO 13849-1**
   - **PN-EN ISO 12100**

   The above-mentioned norms refer also to provisions contained in PN-EN 61508 norm. According to record in PN-EN ISO 12100 concerning evaluation of loss severity, persons, property and environment shall be safeguarded (protected).

It shall be remembered that norms, to which designing process is being subordinated, including safety matters of specific equipment, are to be treated in their entirety and consequently. Fulfilling of individual norms' requirements only selectively, i.e. referring to single norm (e.g. PN-EN 12952) in matter of some aspects, while applying simultaneously another, separate norm (e.g. PN-EN 746) in relation to other issues, is considered improper approach. For issues not defined in subject norm, but identified by manufacturer, e.g. particular type of hazards and risk connected with it, the problem shall be solved by application of adequately documented, proper protections.

5.8.2.2 Other machines

General determinant for machinery safety matters approach is machinery directive and list of adequate harmonized norms. Similarly as in §5.8.2.1/2, PN-EN ISO 13849, PN-EN ISO 12100, EN ISO 12100-1 and EN ISO 12100-2 norms are valid in relation to automatic protection systems matters.

5.8.2.3 Comparative criterion of risk assessment

One shall remember about necessary adjustment with GLSA in scope of parameters determined in §5.2.1, and particularly in relation to tolerable risk.

6 Relevant documents

Any "Technical Specification" issued by GRUPA LOTOS S.A. listed in Contract Files.

7 Norms and standards

Designing, production and erections shall comply with the latest editions of below listed norms and standards.

Mainly norms that are specifically connected with electrical system are listed here. The other norms, related to Instrumentation, are quoted in specification GLSA 3010 – General Requirements.

7.1 Directives and Decisions of European Community

2006/95/EEC	Electrical equipment designed for use within certain voltage limits (LVD)
2004/108/EC	Electromagnetic compatibility and repealing Directive 89/336/EEC Text with EEA relevance
2008/765/EC	Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Text with EEA relevance)
2008/768/EC	Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC
2009/104/EC	Directive 2009/104/EC of the European Parliament and of the Council of 16 September 2009 concerning the minimum safety and

	health requirements for the use of work equipment by workers at work
94/9/EEC	Equipment and protective systems intended for use in potentially explosive atmospheres (ATEX 100A)
99/92/EC	Minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres (ATEX 137)
2006/42/EC	Machinery
97/23/EC	Pressure equipment
2009/142/EC	Directive 2009/142/EC of the European Parliament and of the Council of 30 November 2009 relating to appliances burning gaseous fuels
96/82/EC	Control of major-accident hazards (COMAH, SEVESO II)

7.2 Polish legal acts

The Law of 30 August 2002 on system of conformity assessment (uniform text announced in Official Journal of 2004, No 204, pos. 2087)

The Law of 27 April 2001, The law on environment protection (Official Journal of 2001, No 62, pos. 627, with further amendments)

7.3 PN-EN

PN-EN 746-1	Industrial thermoprocessing equipment. Part 1: Common safety requirements for industrial thermoprocessing equipment.
PN-EN 746-2	Industrial thermoprocessing equipment. Part 2: Safety requirements for combustion and fuel handling systems.
PN-EN 746-3	Industrial thermoprocessing equipment. Part 3: Safety requirements for the generation and use of atmosphere gases.
PN-EN 50156-1	Electrical equipment for furnaces and ancillary equipment - Part 1: Requirements for application design and installation
PN-EN 12952-1	Water tube boilers and auxiliary installations – Part 1 General
PN-EN 12952-2	Water tube boilers and auxiliary installations – Part 2 Material for pressure parts of boilers and accessories
PN-EN 12952-3	Water tube boilers and auxiliary installations – Part 3 Design and calculation for pressure patrs
PN-EN 12952-4	Water tube boilers and auxiliary installations – Part 4 In service boiler life expectancy calculations
PN-EN 12952-5	Water tube boilers and auxiliary installations – Part 5 Workmanship and construction of pressure parts of boiler
PN-EN 12952-6	Water tube boilers and auxiliary installations – Part 6 Inspecting during construction, documentation and marking of pressure parts of the boiler

PN-EN 12952-7	Water tube boilers and auxiliary installations – Part 7 Requirement for equipment for the boiler
PN-EN 12952-8	Water tube boilers and auxiliary installations – Part 8 Requirements for firing system for liquid and gaseous fuels for the boiler
PN-EN 12952-9	Water tube boilers and auxiliary installations – Part 9 Requirements for firing for solid fuels of the boiler
PN-EN 12952-10	Water tube boilers and auxiliary installations – Part 10 Requirements for safeguards against excessive pressure
PN-EN 12952-11	Water tube boilers and auxiliary installations – Part 11 Requirements for limiting devices and safety circuit of the boiler and accessories
PN-EN 12952-12	Water tube boilers and auxiliary installations – Part 12 Requirements for boiler feedwater and boiler water quality
PN-EN 12952-13	Water tube boilers and auxiliary installations – Part 13 Requirements for flue gas cleaning systems
PN-EN 12952-14	Water tube boilers and auxiliary installations – Part 14 Requirements for flue gas DENOX-systems
PN-EN 12952-15	Water tube boilers and auxiliary installations – Part 15 Acceptance tests
PN-EN 12952-16	Water tube boilers and auxiliary installations – Part 16 Requirement for grate and fluidized bed firing systems for solid fuels
PN-EN 12952-17	Water tube boilers and auxiliary installations – Part 17 Guidelines for the involvement of an inspection body independent of the manufacturer
PN-EN 12952-18	Water tube boilers and auxiliary installations – Part 18 Operating instructions
PN EN 12953-1	Shell boilers Part 1 General
PN EN 12953-2	Shell boilers Part 2 Materials for pressure parts of boilers and accessories
PN EN 12953-3	Shell boilers Part 3 Design and calculation for pressure parts
PN EN 12953-4	Shell boilers Part 4 Workmanship and construction of pressure parts of the boiler
PN EN 12953-5	Shell boilers Part 5 Inspection during construction, documentation and marking of pressure parts of the boiler
PN EN 12953-6	Shell boilers Part 6 Requirements for equipment for the boiler
PN EN 12953-7	Shell boilers Part 7 Requirements for firing systems for liquid and gaseous fuels for the boilers
PN EN 12953-8	Shell boilers Part 8 Requirements for safeguards against excessive pressure
PN EN 12953-9	Shell boilers Part 9 Requirements for limiting devices of the boiler and accessories
PN EN 12953-10	Shell boilers Part 10 Requirements for feedwater and boiler water quality
PN-EN 12953-11	Shell boilers Part 11 Acceptance tests

PN EN 12953-12	Shell boilers Part 12 Requirements for grate firing systems for solid fuels for the boiler
PN EN 12953-13	Shell boilers Part 13 Operating instructions
PN-EN 60204-1	Safety of machinery. Electrical equipment of machines – Part 1: General requirements.
PN-EN 61508-1	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements
PN-EN 61508-2	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
PN-EN 61508-3	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements
PN-EN 61508-4	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations
PN-EN 61508-5	Functional safety of electrical/electronic/programmable electronic safety related systems Part 5: Examples of methods for the determination of safety integrity levels
PN-EN 61508-6	Functional safety of electrical/electronic/programmable electronic safety related systems Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
PN-EN 61508-7	Functional safety of electrical/electronic/programmable electronic safety related systems Part 7: Overview of techniques and measures
PN-EN 61511-1	Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and software requirements
PN-EN 61511-2	Functional safety — Safety instrumented systems for the process industry sector — Part 2: Guidelines for the application of IEC 61511-1
PN-EN 61511-3	Functional safety — Safety instrumented systems for the process industry sector — Part 3: Guidance for the determination of the required safety integrity levels
PN-EN 61131-1	Programmable controllers - Part 1: General information
PN-EN 61131-2	Programmable controllers - Part 2: Equipment requirements and tests
PN-EN 61131-3	Programmable controllers – Part 3: Programming languages
PN-EN 61131-5	Programmable controllers – Part 5: Communications
PN-EN 61131-7	Programmable controllers – Part 7: Fuzzy control programming

7.4 PN-EN ISO

PN-EN ISO 12100	Safety of machinery -- General principles for design -- Risk assessment and risk reduction
PN-EN ISO 13849	Safety of machinery. Safety-related parts of control systems. Part 1: General principles for design.

7.5 PN-IEC

PN-IEC 60364 Electrical installations of buildings

8 Record of changes

Date	Description	Introduced by
	This specification entirely replaces the former LOTOS Group S.A. standard No. PR 07 372 with the same title.	M. Domaniewski
30-11-2013 (rev. 1)	Review, update, standardize and changes to the Standard within scope of order No. OK/990/2012	Editorial board coordinated by T.Wróbel
31-08-2015	Korekta nagłówka strony, bez mian w treści dokumentu	T. Wróbel