



Document No.	GP 30-80
Applicability	Group
Date	6 May 2003

Guidance on Practice for Safety Instrumented Systems (SIS) - Implementation of the Process Requirements Specification

GP 30-80

**BP GROUP
ENGINEERING TECHNICAL PRACTICES**

Foreword

This is the first issue of Engineering Technical Practice (ETP) BP GP 30-80. This Guidance on Practice (GP) is based on part of the heritage documents as follows:

BP

RP 30-5 Instrumentation and Control – Selection and Use of Equipment for Instrument Protection Systems.

The portions of the heritage document RP 30-5 that relate to competency, management, verification, and functional safety assessment have been replaced by GP 30-75 (Safety Instrumented Systems – Management of the Safety Lifecycle). The remaining material from the heritage document RP 30-5 is in this GP.

This GP reflects experience gained in implementing safety instrumented systems (SIS) since the publication of RP 30-5. Significant differences exist between RP 30-5 and this GP, which is based on IEC 61511 (Safety Instrumented Systems for the Process Sector).

Copyright © 2003, BP Group. All rights reserved. The information contained in this document is subject to the terms and conditions of the agreement or contract under which the document was supplied to the recipient's organization. None of the information contained in this document shall be disclosed outside the recipient's own organization without the prior written permission of Manager, Standards, BP Group, unless the terms of such agreement or contract expressly allow.



Table of Contents

	Page
Foreword	2
Introduction	3
1. Scope.....	3
2. Normative references	3
3. Terms and definitions	3
4. Symbols and abbreviations	3
5. General	3
6. Safety lifecycle – Implementation of Process Requirements Specification.....	3
7. Procedures	3
8. Selection of equipment for subsystems	3
9. Selection of SIS architecture	3
10. Reliability analysis of the proposed system	3
11. Development of SIS Full Requirements Specification	3
12. Design of SIS subsystems	3
12.1. General.....	3
12.2. Maintenance facilities.....	3
12.3. Operations facilities	3
12.4. Sensors	3
12.5. Logic systems.....	3
12.6. Actuation.....	3
12.7. Power supplies and cabling between subsystems	3
13. SIS Plans	3
13.1. Development of the installation plan.....	3
13.2. Development of the validation plan.....	3
13.3. Development of the commissioning plan.....	3
13.4. Development of operations and maintenance plans	3
14. Installation.....	3
15. Validation	3
16. Commissioning	3
17. Verification	3
18. SIS documentation	3
18.1. General.....	3
18.2. Design dossier for safety and environmental integrity	3
18.3. Design dossier for commercial integrity.....	3
19. Independent functional safety assessment.....	3
Annex A (Informative) Choice of equipment or logic subsystems	3



A.1. General	3
A.2. Types of logic subsystem	3
A.3. Compliance assessed equipment	3
Annex B (Informative) Typical subsystem architectures	3
B.1. Introduction	3
B.2. Architectures	3
B.3. IL 1 configuration	3
B.4. IL 2 configuration	3
B.5. IL 3 configuration	3
B.6. IL 4 configuration	3
Annex C (Informative) System design for robustness.....	3
C.1. Introduction	3
C.2. Evaluation of cost of spurious trips	3
C.3. Evaluation of the cost of additional equipment for robustness.....	3
C.4. Criteria for robustness	3
C.5. Example.....	3
Annex D (Informative) Example of the development of an architecture for a SIS.....	3
D.1. General	3
D.2. Process and background.....	3
D.3. Process Requirements Specification	3
D.4. Selection of equipment for subsystems	3
D.5. Selection of SIS architecture.....	3
D.6. Reliability analysis of the proposed architecture.....	3
D.7. Architecture adopted	3
Bibliography	3

List of Tables

Table 1 – SIS ETP objective, scope, input, and output.....	3
Table 2 – GP 30-80 Safety lifecycle objectives, scope, inputs, and outputs.....	3
Table D.1 – Robustness considerations.....	3
Table D.2 – PFD calculation	3

List of Figures

Figure 1 – Relationship between SIS ETPs	3
Figure 2 – SIS implementation lifecycle	3
Figure B.1 – Architecture for IL 1 subject to conditions	3
Figure B.2 – Architecture for IL 1 (no conditions).....	3
Figure B.3 – Architecture for IL 2 for specified conditions	3



Figure B.4 – Architecture for IL 3 for specified conditions	3
Figure B.5 – Architecture for IL 3 (no conditions).....	3
Figure D.1 – Process plant and SIS	3
Figure D.2 – SIS system architecture.....	3

Uncontrolled Copy



Introduction

Safety instrumented systems (SIS) have been used for many years within the process sector. The original approach was prescriptive with standards (for example, API RP 14C in the offshore sector) stating the specific equipment to use for a particular process application. In recent years, the increased complexity of new applications and the complexity of new equipment becoming available for use have made the prescriptive approach insufficient. This is particularly the case where programmable equipment with complex failure modes is used for safety applications. Some years ago, the international community recognised the need for new standards, and the International Electrotechnical Commission (IEC) developed a new generic standard that adopted a risk-based approach.

The new standard IEC 61508 (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems) was published in seven parts between 1997 and 2000. Before IEC 61508 was published, a need was recognised for a process sector standard and work commenced on IEC 61511 (Safety Instrumented Systems for the Process Sector). IEC 61511 applies the generic standard IEC 61508 to process industries. It also incorporates experience from national and industry standards, such as ISA S84.01. Since publication of IEC 61508, the process sector has had significant experience in the application of the risk-based approach.

The risk-based approach tailors equipment to the needs of the application and has significant safety and economic benefits. This approach does, however, demand more management, competency, planning, and technical judgement during all stages of realisation, from initial hazard and risk analysis through to operation, maintenance, and modification.

The objective of this GP is to provide requirements and guidance on how to specify and implement an SIS starting from the Process Requirements Specification through installation, validation, and commissioning of the system. This GP relates to GIS 30-801, which addresses the specification and procurement of the SIS logic solver subsystem.

As with all updated BP and industry standards, new facilities and modifications to existing facilities should use the latest standards. While the new standards are not normally applied retrospectively, facilities may wish to undertake a gap analysis against the new standard and address any deficiencies.



1. Scope

- a. This GP provides guidance on implementation, installation, validation, and commissioning of safety instrumented systems (SIS) used to reduce the following risks to tolerable levels:
 1. Process safety risk.
 2. Environmental risk.
 3. Commercial risk, including rebuild cost and cost of lost production.
- b. This GP addresses SISs that are based on the use of electrical and electronic instrumentation for logic solvers.
- c. The same basic principles of this GP shall apply to SIS logic solvers that are based entirely on other technologies (pneumatic or hydraulic).
- d. This GP relates to GIS 30-801 that addresses the specification and procurement of the SIS logic solver subsystem.
- e. This GP shall be used in conjunction with GP 30-75 Management of the Safety Lifecycle that applies to all lifecycle phases.
- f. This GP shall also be used in conjunction with the ETPs that apply to the other phases of the safety lifecycle:
 1. Development of the Process Requirements Specification (GP 30-76).
 2. SIS Operations and Maintenance (GP 30-81).
- g. Compliance with this GP requires:
 1. All "shall" statements are complied with.
 2. All "should" statements are considered and complied with unless alternate measures are more appropriate in the context of the specific application.

2. Normative references

The following normative documents contain requirements that, through reference in this text, constitute requirements of this technical practice. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this technical practice are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies.

BP

GP 30-75	Guidance on Practice for Safety Instrumented Systems (SIS) – Management of the Safety Lifecycle.
GP 30-76	Guidance on Practice for Safety Instrumented Systems (SIS) – Development of the Process Requirements Specification.
GP 30-81	Guidance on Practice for Safety Instrumented Systems (SIS) – Operations and Maintenance.
GIS 30-801	Guidance on Industry Standard for Safety Instrumented Systems (SIS) – Design and Engineering of Logic Solvers.

International Standards Organization (ISO)

ISO 10418	Petroleum and natural gas industries – Offshore production installations – Analysis, design, installation and testing of basic surface safety systems.
-----------	--



Instrumentation, Systems, and Automation Society, The (ISA)

ISA 84.01 Application of Safety Instrumented Systems for the Process Industries.

International Electrotechnical Commission (IEC)

IEC 60085 Thermal evaluation and classification of electrical insulation.

IEC 61508-1-4, &6 Functional safety of electrical/electronic/programmable electronic safety-related systems (parts 1 through 4 and part 6).

Part 1: General Requirements.

Part 2: Requirements for Electrical/Electronic/Programmable Electronic Safety-related Systems.

Part 3: Software Requirements.

Part 4: Definitions and Abbreviations.

Part 6: Guidelines on the Application of IEC 61508-2 and IEC 61508-3.

IEC 61511-1 Functional safety: Safety Instrumented Systems for the process industry sector (part 1).

Part 1: Framework, definitions, system, hardware and software requirements.

3. Terms and definitions

Terms and definitions for this GP are provided in BP GP 30-75 and the Normative industry standards.

4. Symbols and abbreviations

For the purpose of this GP, the following symbols and abbreviations apply:

CAE	Cost of additional equipment.
CASS	Conformity Assessment of Safety-related Systems.
CIL	Commercial integrity level.
CST	Cost of spurious trips per year.
CVP	Capital value process.
DCS	Distributed control system.
EIL	Environmental integrity level.
EMC	Electromagnetic compatibility.
EMF	Electromotive force (voltage)
ESD	Emergency shutdown.
ESDV	ESD valve.
F&G	Fire and gas.
FAT	Factory acceptance test.



FMEA	Failure modes and effects analysis.
HSE	Health, safety, and environment.
IL	Integrity level (general).
INERIS	National Institute for Industrial Environment and Risks (France).
OREDA	Offshore reliability data.
OVP	Operations value process.
P&ID	Piping and instrumentation diagram.
PAS	Process automation system.
PFD	Probability of failure on demand.
PIP	Process industry practices (USA).
PLC	Programmable logic controller.
PT	Pressure transmitter.
QA	Quality assurance.
SIL	Safety integrity level.
SIS	Safety instrumented system.
SOV	Solenoid-operated valve.
UKOOA	United Kingdom Offshore Operators Association.
UPS	Uninterruptible power supply.

5. General

- a. The approach to developing SIS requirements shall be in two stages:
 1. The first stage shall be development of the SIS Process Requirements Specification (covered by GP 30-76).
 2. The second stage shall be implementation of the SIS Process Requirements Specification (covered by this GP), including development of the SIS Full Requirements Specification.
- b. The following shall be in accordance with GP 30-75:
 1. Safety lifecycle phases defined in this GP.
 2. Management of the safety lifecycle.
 3. Integration of the safety lifecycle into the project lifecycle.
 4. SIS tasks with a specified integrity level (IL).

Such tasks may be performed by designers, vendors, installation contractors, etc.



- c. Because compliance with the ISO 9000 family of standards may not be sufficient for SIS, organisations that have been compliance assessed as meeting the requirements of the ISO 9000 family of standards should have an assessment to determine if the procedures developed to comply with the ISO 9000 family of standards give sufficient assurance that the risk of functional failure has been reduced to appropriate levels. In making such judgements, account should be taken of the complexity of the task and the required integrity levels.
- d. Relationships between relevant SIS ETPs in the safety lifecycle (shown in Figure 1) shall be considered along with objectives, input, and output for each SIS ETP (shown in Table 1).

Figure 1 – Relationship between SIS ETPs

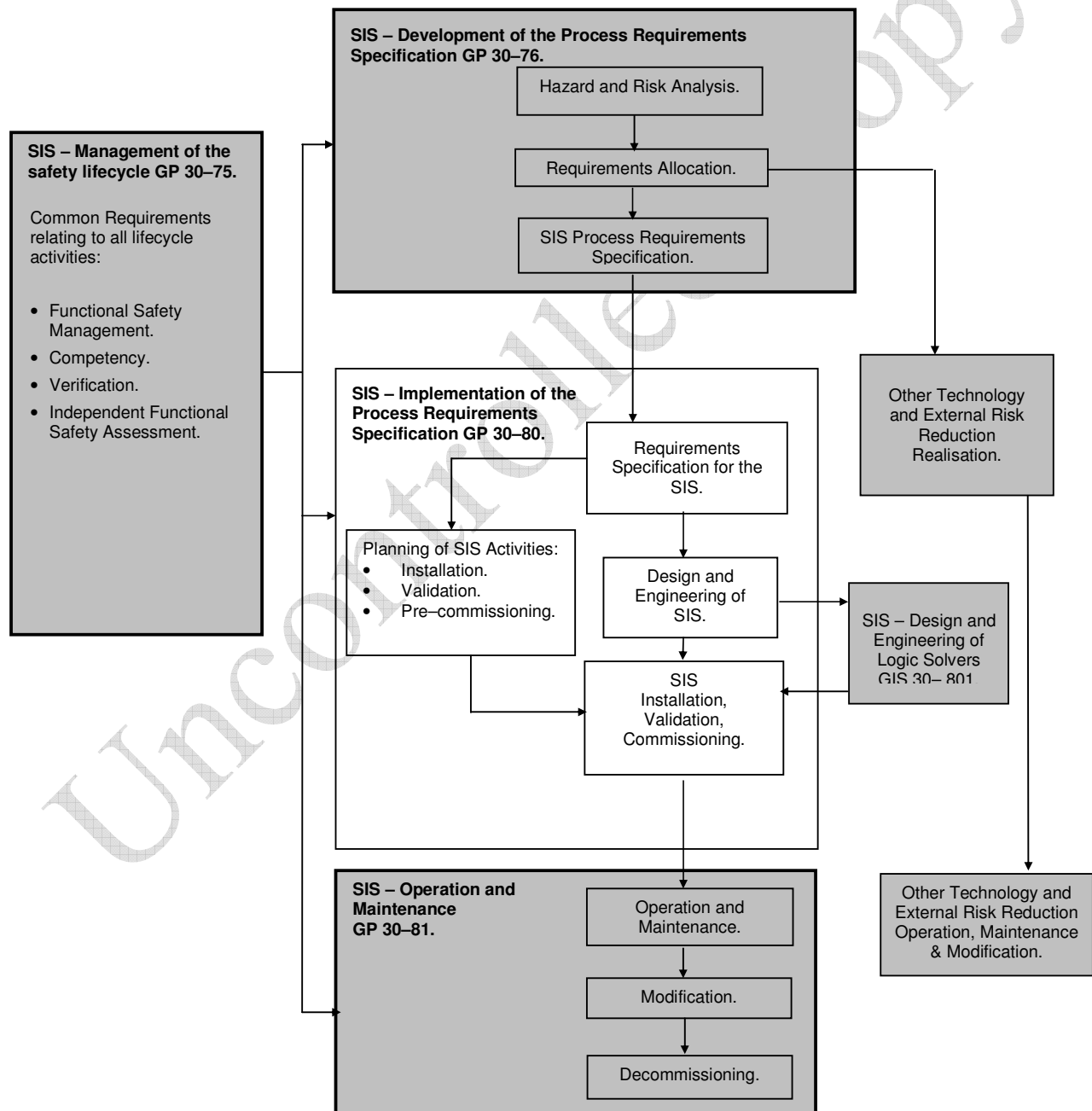


Table 1 – SIS ETP objective, scope, input, and output

ETP & safety lifecycle phase	Objective	Scope	Input	Output
GP 30-75 Guidance on Practice for Safety Instrumented Systems (SIS) – Management of the Safety Lifecycle.	Specify overall framework and requirements applied to all safety lifecycle phases.	Risks from functional failures leading to safety, environmental, and asset consequences.	2. HSE policy. 3. CVP process. 4. OVP process.	1. Overall safety lifecycle and plan. 2. Functional safety management requirements for competency, verification, and independent functional safety assessment.
GP 30-76 Guidance on Practice for Safety Instrumented Systems (SIS) – Development of the Process Requirements Specification.	Specify requirements of safety layers to reduce risks to tolerable levels.	Risks from functional failures leading to safety, environmental, and asset consequences.	1. Process design. 2. Manning levels. 3. Environment factors. 4. Business impacts of loss of production.	1. Hazard list caused by functional failures. 2. SIS Process Requirements Specification, including function and performance characteristics of safety layers required to reduce risks to tolerable levels.
GP 30-80 Guidance on Practice for Safety Instrumented Systems (SIS) – Implementation of the Process Requirements Specification.	1. Design, procure, install, and pre-commission SIS to achieve performance requirements. 2. Specify operations and maintenance requirements to maintain required integrity during life of asset.	Safety instrumented systems.	SIS Process Requirements Specification. This specification includes function and performance characteristics of SIS safety layers required to reduce risks to tolerable levels.	1. SIS Full Requirements Specification. 2. SIS Activities planning for installation, validation, and precommissioning. 3. SIS is installed according to international standards, validated against functional and performance requirement specification. 3. Operations and maintenance procedures to maintain performance levels over life of asset. 4. Architectures supporting high availability, tolerable risk, and low maintenance cost.
GP 30-81 Guidance on Practice for Safety Instrumented Systems (SIS) – Operations and Maintenance.	Manage risk of functional failure throughout life of asset to maintain tolerable risk.	Safety instrumented systems.	1. SIS Installation – SIS is installed according to international standards, validated against functional and performance requirement specification. 2. Operations and maintenance procedures to maintain necessary performance levels over life of asset.	1. Continuing achievement of tolerable risk level throughout the asset life. 2. Tolerable plant availability and low maintenance cost.
GIS 30-801 Guidance on Industry Standard for Safety Instrumented Systems (SIS) – Design and Engineering of Logic Solvers.	Procure SIS logic solver.	SIS logic solver.	SIS Full Requirements Specification.	SIS logic solver procurement specification.



- e. In the U.S. and Canada, compliance with IEC 61511 may be replaced with a requirement to comply with the equivalent clauses in OSHA, EPA, and ISA standards. (Refer to GP 30-75, Annex B for more detail. This annex maps some major clauses of GP 30-75 to OSHA 29 CFR 1910.119 and ISA 84.01 standards.) In such cases, the following documents apply:
 - 1. ISA 84.01.
 - 2. 29 CFR 1910.119.
 - 3. 40 CFR, Part 68.

6. Safety lifecycle – Implementation of Process Requirements Specification

- a. A detailed safety lifecycle shall be defined for the activities after specification of the process requirements up to final validation.
- b. The SIS implementation lifecycle shall be as shown in Figure 2 and Table 2. A modified lifecycle may be used if justified, but this shall be documented and mapped to the requirements of this GP and IEC 61511-1.

The safety lifecycle shown in this GP differs from the safety lifecycle in IEC 61511-1. The major difference is that determination of the SIS Requirements Specification is in two stages (covered in GP 30-76 and this GP).

- c. Development of plans for installation, validation, commissioning and operations and maintenance shall be carried out during the design phase.
- d. The SIS implementation lifecycle shall be integrated into the project lifecycle as described in GP 30-75.



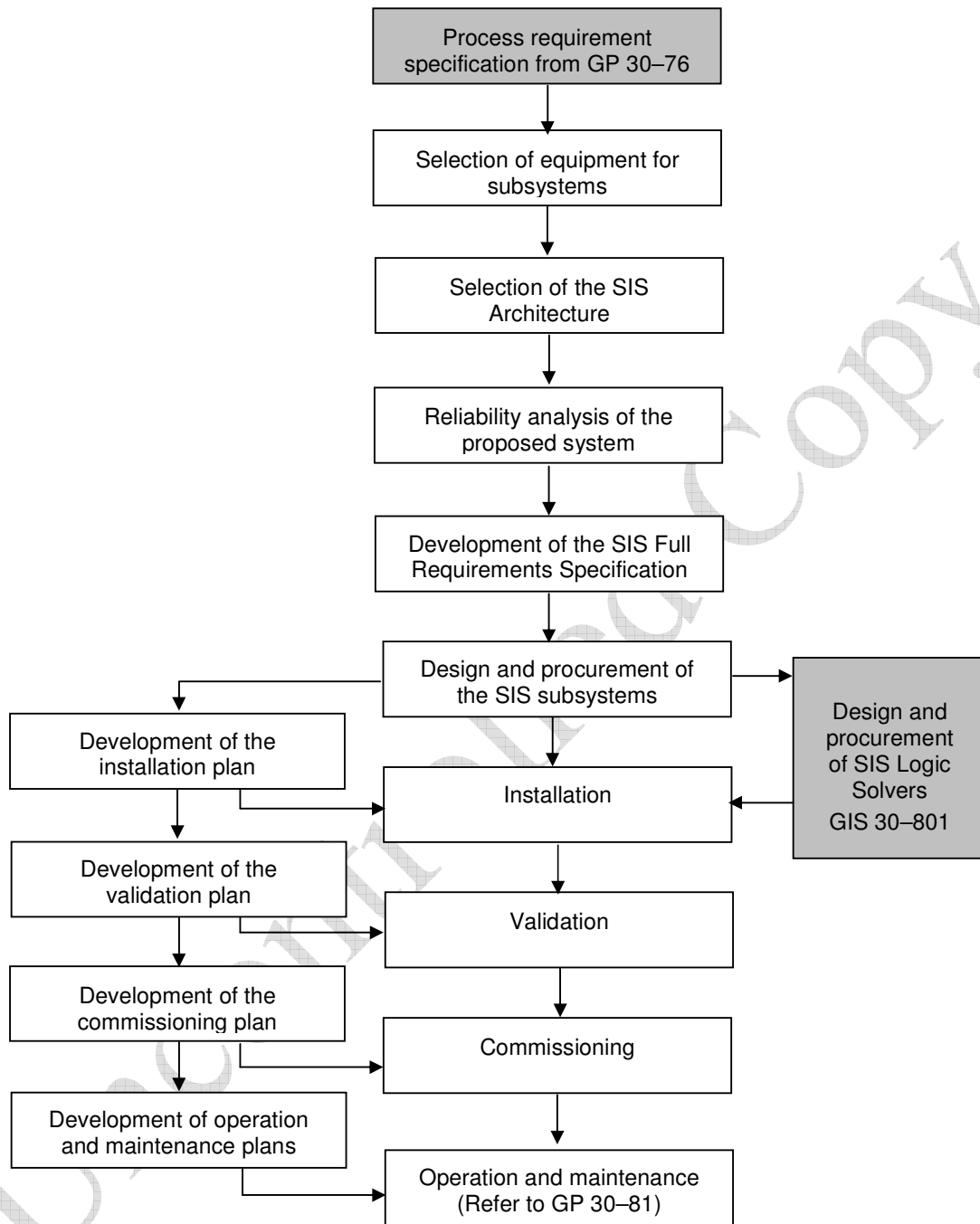
Figure 2 – SIS implementation lifecycle

Table 2 – GP 30-80 Safety lifecycle objectives, scope, inputs, and outputs

Safety lifecycle phase	Objectives	Scope	Inputs	Outputs
Selection of equipment for subsystems.	To select equipment that will meet the needs of the GP.	SIS	Function requirements in SIS Process Requirement Specification.	List of vendors and equipment types approved for use
Selection of SIS architecture.	To select equipment architectures that meet the reliability and fault tolerance requirements.	SIS	Integrity and robustness requirements in SIS Process Requirement Specification.	Minimum architectures for SIS
Reliability analysis of proposed architecture.	To ensure the equipment and architectures meet the PFD associated with the required integrity levels.	SIS	Integrity and robustness requirements in SIS Process Requirement Specification	Confirmed architectures and required proof test intervals
Development of SIS requirements specification.	To develop the final SIS requirements specification.	SIS	SIS Process requirements specification, confirmed architectures	SIS Full Requirements Specification
Design and procurement of the SIS subsystems.	To develop the detailed design of the SIS..	SIS	SIS Full Requirements Specification	1. Detail installation drawings. 2. SIS Procurement specifications.
Development of the installation plan.	To plan the installation of the SIS.	SIS	SIS full specification and installation drawings.	Installation plans and specifications.
Development of the validation plan.	To plan the validation of the SIS.	SIS	SIS full requirements specification.	Validation plans and FAT specification.
Development of the commissioning plan.	To plan the commissioning of the SIS.	SIS	SIS full requirements specification.	Commissioning plans.
Development of the operation and maintenance plan.	To plan the operations and maintenance.	SIS	SIS full requirements specification.	Operation and maintenance plan.
Installation of the SIS	To install the SIS	SIS	SIS installation plan	SIS installed
Validation of the SIS.	To validate the SIS.	SIS	SIS validation plan.	SIS validated.
Commissioning of the SIS.	To commission the SIS.	SIS	SIS commissioning plan.	SIS commissioned.

7. Procedures

- a. The following procedures shall be applied during the safety lifecycle phases of this GP:
 1. General procedures specified in GP 30-75, Clause 11.1.
 2. Configuration management procedures in accordance with IEC 61511-1, Clause 5.2.7.1.1.
- b. Procedures shall be applied rigorously.
- c. Independent functional safety assessment shall be performed as specified in this GP, Clause 19.

8. Selection of equipment for subsystems

- a. Equipment for implementing SIS functions with an IL requirement of 1 or higher shall either:
 1. Comply with IEC 61508-2 (and IEC 61508-3, if a programmable system is used).
 2. Meet the requirements for the selection of components and subsystems based on prior use specified in IEC 61511-1, Clause 11.5.3.



- b. General purpose industrial PLCs should not be used for implementation of SIL or EIL rated functions.
- c. Guidance provided in Annex A shall be considered in the selection of appropriate technology for logic subsystems.
- d. Preference should be given to equipment that has been assessed by an independent organisation and shown to comply with IEC 61508-2 and IEC 61508-3 for the specified IL. Independent organisations performing assessments should be approved by a national accreditation body.

Considerable caution is needed on vendor's claims to be compliant, unless these are backed by an independent assessment. It is generally less costly and quicker to use equipment that has been compliance assessed by an independent organisation because the assessment process to enable a claim to be made that a previously developed component complies with IEC 61511 is likely to involve significant work.

- e. Logic systems for IL 4 applications shall be nonprogrammable.
- Software has complex failure modes and cannot be comprehensively tested to ensure that unintended system actions will not occur.*

- f. Logic systems for IL 3 applications should be nonprogrammable. Proposed use of programmable logic systems for IL 3 shall be specifically justified.

For relatively small numbers of IL 3 functions, nonprogrammable technology is usually more cost-effective.

- g. The type of logic system selected shall reflect the needs of the application. In selecting the type of logic system, the following factors shall be considered:

1. Skills and experience available within the project and the application site.
2. Number of inputs and outputs, with further consideration of the following:
 - a) Relay systems may be cost-effective for small systems with very limited numbers of inputs and outputs, but are not suitable for large applications.
 - b) Relay systems are difficult to document, test, and change.
3. Guidance included in Annex A, with respect to the choice of system.
4. Complexity of the function to be implemented, with further consideration of the following:
 - a) Limited variability programmable systems may be needed for complex or sequence applications.
 - b) In the case of sequence applications, the system selected should have suitable application languages.
5. IL required, with further consideration of the following:
 - a) Higher ILs require a high level of assurance that the system can always fulfil the required function under all conditions of input and output, and internal states of the system.
 - b) This high level of assurance is difficult to provide with programmable systems because testing all combinations is not practicable.

- h. SIS logic solver shall be specified in accordance with GIS 30-801 and clause 12.5 of this GP 30-80.
- i. Functions that have been designated as "No special safety requirements" may be implemented in general purpose control equipment such as DCS or PLC providing the following conditions apply:

