



GS 130-9

SPECIFICATION FOR THE SUPPLY OF SHUTDOWN SYSTEMS

January 1994

Copyright © The British Petroleum Company p.l.c.

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 organisation. None of the information contained in this document shall be disclosed outside the recipient's own organisation without the prior written permission of Manager, Standards, BP International Limited, unless the terms of such agreement or contract expressly allow.

BP GROUP RECOMMENDED PRACTICES AND SPECIFICATIONS FOR ENGINEERING											
Doc. No. GS 130-9		Issue Date January 1994	Latest Amendment Date								
Document Title SPECIFICATION FOR THE SUPPLY OF SHUTDOWN SYSTEMS											
APPLICABILITY Regional Applicability: International											
SCOPE AND PURPOSE This document specifies the minimum requirements for the design of Shutdown Systems. Its purpose is for the specification of fit-for-purpose Shutdown Systems at minimum cost.											
AMENDMENTS <table border="1"> <thead> <tr> <th>Amd</th> <th>Date</th> <th>Page(s)</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td colspan="4"> </td> </tr> </tbody> </table>				Amd	Date	Page(s)	Description				
Amd	Date	Page(s)	Description								
CUSTODIAN (See Quarterly Status List for Contact) Control & Instrumentation											
Issued by:- Engineering Practices Group, BP International Limited, Research & Engineering Centre Chertsey Road, Sunbury-on-Thames, Middlesex, TW16 7LN, UNITED KINGDOM Tel: +44 1932 76 4067 Fax: +44 1932 76 4077 Telex: 296041											

CONTENTS

Section	Page
FOREWORD	ii
1. INTRODUCTION.....	1
1.1 Scope.....	1
1.2 <i>Functional Specification Guidelines</i>	1
2. SYSTEM REQUIREMENTS.....	1
3. HIGH INTEGRITY SYSTEMS.....	4
4. TESTING	5
5. DOCUMENTATION.....	5
APPENDIX A.....	8
DEFINITIONS AND ABBREVIATIONS.....	8
APPENDIX B.....	9
LIST OF REFERENCED DOCUMENTS	9
APPENDIX C	10
FUNCTIONAL SPECIFICATION DATA SHEETS	10
C1. SYSTEM DESCRIPTION	10
C2. ENVIRONMENT, AREA CLASSIFICATION AND UTILITIES	12
C3. ESD I/O SCHEDULE.....	14



FOREWORD

Introduction to BP Group Recommended Practices and Specifications for Engineering

The Introductory Volume contains a series of documents that provide an introduction to the BP Group Recommended Practices and Specifications for Engineering (RPSEs). In particular, the 'General Foreword' sets out the philosophy of the RPSEs. Other documents in the Introductory Volume provide general guidance on using the RPSEs and background information to Engineering Standards in BP. There are also recommendations for specific definitions and requirements.

Value of this Guidance for Specification

This Guidance for Specification identifies the minimum requirements for the design of Shutdown Systems. The intention is to simplify the purchasing requirements when dealing with a known and mature supplier source.

Application

This Guidance for Specification is intended to guide the purchaser in the use or creation of a fit-for-purpose specification for enquiry or purchasing activity.

Text in *italics* is Commentary. Commentary provides background information which supports the requirements of the Specification, and may discuss alternative options.

This document may refer to certain local, national or international regulations but the responsibility to ensure compliance with legislation and any other statutory requirements lies with the user. The user should adapt or supplement this document to ensure compliance for the specific application.

Specification Ready for Application

A Specification (BP Spec 130-9) is available which may be suitable for enquiry or purchasing without modification. It is derived from this BP Group Guidance for Specification by retaining the technical body unaltered but omitting all commentary, omitting the data page and inserting a modified Foreword.

Feedback and Further Information

Users are invited to feed back any comments and to detail experiences in the application of BP RPSE's, to assist in the process of their continuous improvement.

For feedback and further information, please contact Standards Group, BP International or the Custodian. See Quarterly Status List for contacts.



1. INTRODUCTION

1.1 Scope

This Specification, details the basic minimum requirements for the design of shutdown systems. For system procurement, this specification will need to be supplemented by details of the functional requirements for the specific application.

1.2 *Functional Specification Guidelines*

A functional specification should cover the following areas:-

Introduction

Scope of Supply:-

General

Testing

Documentation

Work by Others

Commissioning

Applicable Codes, Standards and Regulations

Special Requirements

Information Required with Quotation

Price and Delivery

Quality Verification

Appendices:-

System Description (see Appendix C1)

Environment, Area Classification and Utilities (see Appendix C2)

Input/Output Schedule (see Appendix C3)

2. SYSTEM REQUIREMENTS

- 2.1 The Supplier shall submit his proposal for the preferred method of logic operation to enable the functions to be performed with the required system availability/reliability, where specified. The supplier shall give consideration to proposal of alternative arrangements where significant cost savings or reduction in complexity/maintenance burden can be demonstrated with minimal penalty to specified system performance.



It is essential to agree with the Operator during the initial design phase the required operating and maintenance philosophy (including reliability/availability and on line/off-line testing arrangements).

2.2 The design shall meet the requirements necessary to gain approval of any appropriate third party or regulatory authorities, together with any testing requirements.

2.3 Where a programmable system is proposed this shall maximise the use of standard proven software thus minimising the amount of custom programming necessary. An established method for controlling and validating software development and subsequent modification shall be available. All software and associated hardware necessary for programming and modifying system software and configuration shall be included in the supply.

Full variability programmable systems should be avoided. They should only be considered where the complexity of application requires advanced algorithms. Fixed or limited variability programmable systems where the program is fixed and unchangeable and Limited Variability system, typically a PLC, are preferred. Points to be considered in the application of programmable electronic systems include:-

- (i) *Failure and Failure Modes - It is unlikely that the mechanism of failure can be predicted and it is possible that a fault may lie unrevealed. It is therefore necessary to have arrangements to detect failure and take action, usually by forcing plant to a safe state.*
- (ii) *Modifications - It is important to ensure that access to, and modification of, the application software is closely controlled*
- (iii) *Overrides - Where override facilities are provided by application software, indications need to be provided for operations supervision to ensure plant protection is not gradually downgraded.*

2.4 The general principle to be used for shutdown shall be for fail-safe i.e. de-energise/contacts open to trip. Exceptions may be specified where continuity of operation is of greater importance for ensuring safety, e.g. boiler plant.

2.5 Shutdown trip inputs will be mainly from transmitter analogue inputs. The input capability of the system shall be such that it makes use of supplier standard components and results in no degradation of system availability/ reliability or system self test.

Input modules shall have common/series mode interference rejection in range 50 to 500 ms.

The system shall include secure transmitter and digital input and output power supply.



The power supply for field equipment and logic system is an essential component of an ESD system. During design the operating voltage specification of all components should be determined. It should be established by calculation that with the power supply regulation characteristic and cable voltage drops that the required voltage is available at the solenoids/loads. This should include operation on battery only. The loads should also be specified to withstand any temporary, higher system voltage that might be applied during battery boost charging.

- 2.6 Unless otherwise specified by the purchaser, the shutdown system shall communicate with the main installation control system for display of shutdown input alarm, analogue value, system status, sequence of event recording, and this shall be by an established and proven interface. Feedback of shutdown device status (e.g. valve, pump, damper) will be reported to the control system directly and not via the shutdown system.

The overall display response shall be such that rapid indication of hazard and access to detail information is given to the operator.

Small system display requirements may not necessitate this interface, and a simpler hard wired display may be more appropriate, however this would be application specific and requires review during the initial design phase.

The communication can be by serial link or hard wired input. A study should be carried out to examine cost effectiveness of the application to cover overall cost including the control system components, both hardware and software but recognising space constraints.

The time resolution of event recording of some control systems may not be adequate for diagnosis purposes and separate sequence of event recording facilities may need to be considered.

- 2.7 A separate shutdown system overview panel section shall also be provided for incorporating into the main control point operator station. This shall provide manual shutdown and status indication on an area and/or level basis as appropriate to the plant operations. These controls/indications shall be hardwired, independent of the logic and bypass any override. The manual shutdown switches shall be of a type to avoid inadvertent operation.

Where 'red shutdown' is specified (i.e. electrical isolation of all but 'essential' services) this will be a manual shutdown operating on an energise to trip/contacts closed principle with redundant path arrangement and condition monitoring.

- 2.8 Each part of solid state and software driven shutdown systems and associated power supplies, should have test and diagnostic facilities to test both hardware and software, where used, in order to minimise the possibility of unrevealed faults occurring. The fault shall be alarmed



and confirmed to board level. Control action on detection of fault shall be selectable.

There shall be no need for a total system shutdown to repair faults, and the facilities lost during any fault period shall be minimised. First line fault repair shall be possible using 'non-expert' multi-trade technicians.

- 2.9 Key protected inhibit facilities shall be provided, as necessary, to enable routine testing and calibration of the system and inputs/outputs without significant reduction in the available detection/protection. All inhibits shall be reported to the operator and indication shall not be cancelled until the inhibit has been removed. Overrides on inputs shall not inhibit the operation of the associated alarm. Keys shall be retained in the defeat position.

A common key profile is preferred on at least a unit basis, with separate profiles for outputs. The number of keys needs to be strictly controlled to remove the temptation to leaving keys in locks.

It will not normally be necessary to provide defeat switches for protective circuits associated with spare or stand-by equipment or for intermittently operating plant.

- 2.10 The supplier shall provide a detailed assessment of reliability and availability. This shall take into account all system components including field devices and cabling.
- 2.11 The supplier shall carry out a failure modes effects analysis of the system considering the consequences of a component module failure. This shall be used to demonstrate that an unrevealed common mode failure does not occur which could jeopardise the integrity of the system.
- 2.12 The panels and fitted equipment shall be suitable for the environment and due regard shall be taken of mounting vibration and panel noise where appropriate.
- 2.13 For larger systems, where more than one cubicle section is involved, separate termination areas shall be provided for the main logic panel(s) connected via plugs and sockets. This is to allow for the termination of field cables prior to delivery of the main section of the panel.

3. HIGH INTEGRITY SYSTEMS

- 3.1 Where a requirement for 'high integrity' Category 1/2A systems are identified, these shall be implemented by means of independent hardwired or solid state systems and inputs/outputs as appropriate to meet the application required reliability to trip on demand and



availability. Redundant systems shall be provided where necessary to meet these requirements for test purposes.

Programmable systems should not be used. The main problem in using programmable systems for Category 1/2A is establishing the integrity of the software. The only exception to this is where independently assessed equipment, by a recognised body such as TUV, is available. and such equipment is specifically approved for the category of risk involved for the application.

- 3.2 The systems shall be provided with all necessary test facilities to ensure system integrity is maintained during operation. This should not necessitate shutdown of plant or equipment unless this is defined in by the Purchaser as an acceptable situation.

The need for manual override or defeat facilities for testing or start up on high integrity systems should be avoided.

- 3.3 The supplier shall be responsible for full system assessment from detector to actuation device including:-

Probability to trip on demand assessment
Full documented proof of assessment
Provision of independent audit of calculations
Detail of trip frequency requirements and procedures

- 3.4 The systems shall be provided with dossiers including full documentation to ensure life of field system integrity, test and maintenance.

4. TESTING

- 4.1 The supplier shall produce a detailed test procedure which will demonstrate design integrity along with the correct operation of each element of the system. The test procedure shall ensure that on-site testing and remedial work is minimised. All testing shall be recorded and such records shall be retained for inspection for audit purposes.

The control panels shall be demonstrated to be immune to electromagnetic interference using project specific sources for test purposes.

5. DOCUMENTATION

Documentation shall be provided to enable assessment of design. This should be limited to that essential to verify conformance with specified functionality and as necessary to permit installation, operation, calibration and maintenance of the systems.



Requirement should be detailed in the Functional Specification and would consist typically of the following:-

(i) Information Required With Quotation

- *Detailed description of proposed system and any field equipment included in the scope.*
- *Reliability and availability assessment.*
- *List of applicable Codes and Standards and any deviations from these or this specification and associated documentation.*
- *Statement of capabilities and proposals for providing installation supervision (on/offshore) and testing/commissioning (on/offshore).*
- *Programme for construction, testing and delivery.*
- *Proposals for testing and commissioning.*
- *Spares and test equipment proposals together with prices.*

(ii) Documentation Required During Design, Build and Test

Documentation must be limited to the minimum required to design the installation and to operate and maintain the equipment.

It should be recognised that it is the responsibility of the vendors to approve the detailed design drawings and not the design contractor. This is a new approach and will substantially reduce the volume of documentation required.

The specific documentation requirements will need to be defined by the design contractor for each particular application.

The prime objective is to eliminate unnecessary documentation, reformatting and approvals, thereby realising large savings in vendor and contractor costs.

It is suggested that the following is used as a basis for agreeing the documentation requirements:-

8 weeks after confirmation of order

- *Front of panel and matrix layout drawings.*
- *Logic diagrams.*
- *Detailed reliability assessments for any high integrity systems*
- *Panel power and heat load estimates.*
- *Wiring, electrical distribution, earthing and inter-connection drawings.*



- *Installation and terminal point details.*
- *Equipment lists, schedules and data sheets for input to operational maintenance database systems (where specified).*
- *I/O and interface schedules including signal state.*
- *Detailed spares and test equipment listings to cover commissioning and two year's operation.*
- *Functional design specification of any bespoke hardware, software or system configuration.*
- *Failure modes and effects analysis.*

8 weeks prior to Factory Test

- *Detailed procedure, programme and test sheets for system testing at the factory, on site commissioning and for subsequent routine operation and maintenance. These are to include for the system and any sub-vendors or ancillary equipment. Special requirements for high integrity systems shall also be included.*
- *Equipment safety certification dossier (as applicable).*
- *Independent audit report of high integrity system reliability assessment.*
- *Operation and maintenance manuals with all information necessary for continued operation during the life of the installation.*

On delivery

- *As built documentation*
- *Confirmed weight and Centre of Gravity (offshore only or as specified)*

The document approval category requirements for the above will need definition for specific applications. The requirement for approval before continuation of manufacture should be minimised.



DEFINITIONS AND ABBREVIATIONS

Definitions

Standardised definitions may be found in the BP Group RPSEs Introductory Volume.

Abbreviations

PLC Programmable Logic Controller



LIST OF REFERENCED DOCUMENTS

A reference invokes the latest published issue or amendment unless stated otherwise.

Referenced standards may be replaced by equivalent standards that are internationally or otherwise recognised provided that it can be shown to the satisfaction of the purchaser's professional engineer that they meet or exceed the requirements of the referenced standards.

- NONE -



FUNCTIONAL SPECIFICATION DATA SHEETS

C1. SYSTEM DESCRIPTION

C1.1 General

-- HOLD --

(Note: Description of the project, location and application)

C1.2 System Layout

-- HOLD --

(Note: Summary of the system and any particular features/requirements for the application)

C1.3 Shutdown Hierarchy

-- HOLD --

(Note: Summary of shutdown levels e.g. unit, pressurised, de-pressurised, total etc.)

C1.4 System Availability/ Reliability

-- HOLD --

(Note: Agree realistic requirements with the operator.)

C1.5 Display and Operator Interface Arrangement

Vendor to advise optimum solution.

C1.6 Integration with other Systems

-- HOLD --

(Note: Describe functional requirements and request supplier to propose optimum solutions.)



C1.7 Special to Project Maintenance Facilities

-- HOLD --

(Note: Agree any special requirements with the Operator.)

C1.8 High Integrity Trip Systems

-- HOLD --

(Note: Requirements should come from process design and HAZOP.)

Reliability to Trip on Demand (for each application).

-- HOLD --

(Note Requirements should come from risk assessment.)

C1.9 Device and Equipment/Panel Tag Numbering.

-- HOLD --

(Note: Detail to fit project philosophy but with due regard to supplier system capability.)

C1.10 Panel Maximum Noise Levels

Control Room Panels: -- HOLD --

(Note: Consider requirements for continuous manning.)

Equipment Room Panels: -- HOLD --

(Note: Should be less onerous as usually not normally manned.)



C2. ENVIRONMENT, AREA CLASSIFICATION AND UTILITIES

Field equipment

Field equipment will be subjected to a marine environment with a salt laden atmosphere.

<i>Max. ambient temperature</i>	<i>°C</i>
<i>Min. ambient temperature</i>	<i>°C</i>
<i>Max. Rel. Humidity</i>	<i>%</i>
<i>Area Classification</i>	<i>Zone</i>
<i>Gas Group</i>	<i>II</i>
<i>Temperature Class</i>	<i>T</i>

Central control/Field equipment rooms

The control/equipment rooms shall be classified as a safe area and suitable for general purpose equipment such as control panels and printers.

<i>Max. ambient temperature</i>	<i>°C</i>
<i>Min. ambient temperature</i>	<i>°C</i>
<i>Max. Rel. Humidity</i>	<i>%</i>

Utilities and Services

Electrical power

<i>1. Voltage</i>		<i>V AC</i>	<i>V AC</i>
<i>Frequency</i>		<i>Hz</i>	<i>Hz</i>
<i>Regulation</i>	<i>-</i>	<i>VTA</i>	
<i>Harmonic Distortion</i>	<i>-</i>	<i>VTA</i>	
<i>Switching Transients</i>	<i>-</i>	<i>VTA</i>	
<i>2. Voltage</i>		<i>V DC</i>	<i>V DC</i>
<i>Regulation</i>	<i>-</i>	<i>VTA</i>	
<i>Ripple</i>	<i>-</i>	<i>VTA</i>	
<i>Harmonic Distortion</i>	<i>-</i>	<i>VTA</i>	

Instrument Air

<i>Inst. Air Pressure</i>	<i>barg (max.)</i>	<i>barg. (min.)</i>
<i>Dew Point</i>	<i>°C</i>	

VTA - Vendor to advise with submission





C3. ESD I/O SCHEDULE

NOTES

[illegible]