



RP 30-4

INSTRUMENTATION AND CONTROL

**CONTROL AND DATA ACQUISITION
SYSTEMS - SYSTEM DESIGN AND
CONFIGURATION GUIDELINES**

February 1998

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. RP 30-4		Issue Date	February 1998								
Document Title		Latest Amendment Date									
INSTRUMENT AND CONTROL - CONTROL AND DATA ACQUISITION SYSTEMS - SYSTEM DESIGN AND CONFIGURATION GUIDELINES											
APPLICABILITY Regional Applicability: International											
SCOPE AND PURPOSE This Recommended Practice provides a guide for selection and use of Control and Data Acquisition Systems for the control and monitoring of production and process plant, storage facilities, pipelines and other installations handling flammable gasses, liquids and other materials. Its purpose is to provide design engineers and plant management with:- (a) guidance on the need and applicability of Control and Data Acquisition Systems. (b) a basis for designing, evaluating and selecting and making best use of Control and Data Acquisition Systems for various duties. (c) guidance on health and safety aspects associated with the design, installation and operation of Control and Data Acquisition Systems.											
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 & Electrical Systems											
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	v
1. INTRODUCTION	1
1.1 Scope	1
1.2 Application	1
1.3 <i>Quality Assurance</i>	1
2. SPECIFICATION	2
2.1 DCS Project Organisation and Implementation Strategy	3
2.1.1 Basic Training	5
2.2 Statement of Requirements and Control Philosophy	6
2.3 Front End Engineering Design (FEED).....	8
2.3.1 Functional Specification	8
2.3.2 FDS System Sizing	9
2.3.3 Ancillary Areas	15
2.4 Performance.....	16
2.4.1 Safety Requirements	16
2.4.2 Reliability and Availability	19
2.4.3 System Response Times.....	21
3. SYSTEM SELECTION AND PURCHASE.....	22
3.1 Pre-qualification of Vendors	22
3.2 Enquiry and Vendor Selection.....	23
3.2.1 Invitation To Tender	23
3.2.2 Secrecy Agreements.....	23
3.2.3 The Tender	23
3.2.4 Bid Evaluation and Vendor Selection.....	24
3.3 Purchase	25
3.3.1 Negotiation.....	25
3.3.2 Purchase Specification	25
3.3.3 Delivery Schedule	25
3.3.4 Warranty and Vendor Support	25
3.3.5 Payment Terms	26
3.3.6 Training.....	26
4. DETAILED SYSTEM DESIGN	27
4.1 Project Management	27
4.1.1 System Design Specification	27
4.1.2 Management of Data	28
4.1.3 Documentation.....	28
4.1.4 Software	30



4.1.5 System Configuration	30
4.1.6 CONSOP.....	30
4.2 System Infrastructure.....	31
4.2.1 Control Room Design	31
4.2.2 Equipment Location and Accommodation	39
4.2.3 Spare Capacity and Upgrades	39
4.2.4 Power Supplies.....	40
4.3 System Functionality	40
4.3.1 Interfaces.....	42
4.3.2 Maintenance and Diagnostics	44
4.3.3 Control and Data Acquisition	44
5. SYSTEM CONFIGURATION.....	46
5.1 Man Machine Interface.....	46
5.2 Security	47
5.3 Information Display.....	48
5.3.1 User Requirements.....	48
5.3.2 Providing the Functionality.....	49
5.3.3 The Display Hierarchy	50
5.3.4 Access/Navigation	51
5.3.5 Custom Replacement of Standard Displays.....	52
5.3.6 Data Access/Change Facilities.....	52
5.3.7 The Use of Colour.....	53
5.3.8 Display of Fixed Information.....	55
5.3.9 Display of Variable Information	56
5.4 Data Entry	57
5.4.1 Physical Devices	57
5.4.2 Functional Aspects.....	59
5.5 Alarm Systems.....	60
5.5.1 Alarm Definition.....	61
5.5.2 Alarm Detection.....	62
5.5.3 Alarm Prioritisation	63
5.5.4 Association of Alarms with Plant Areas or Process Units.....	64
5.5.5 Audible Warning.....	64
5.5.6 Alarm Identification and Situation Assessment.....	65
5.5.7 Corrective Action.....	66
5.5.8 Alarm and Event History Reporting	69
5.5.9 Alarm System Management.....	69
5.5.10 Point Processing/ Alarm Conditioning	70
5.6 Trending and History Configuration.....	74
5.6.1 Historical Data to Collect.....	74
5.6.2 Time and Magnitude Resolution of Historical Data	75
5.6.3 Archiving	76
5.6.4 Trends	76
5.6.5 SQL Reports.....	78



5.7 Controller Configuration Guidelines	78
5.8 Batch and Sequence Control.....	80
5.9 Advanced Control/ Optimisation.....	84
5.9.6 Other Kinds of Advanced Control Scheme.....	90
6. ACCEPTANCE AND INSTALLATION	91
6.1 Factory Acceptance Testing (FAT)	91
6.2 Delivery and Installation.....	93
6.3 Site Acceptance Test (SAT)	94
6.3.1 Site Testing Principles	94
6.3.2 Hardware Testing.....	95
6.3.3 Software Testing	95
6.4 Pre-commissioning and Loop Testing	96
6.4.3 Operator Familiarisation and Training.....	97
6.5 Commissioning.....	98
6.5.1 Loop Tuning Starting Values	98
6.5.2 Re-instrumentation - Hot Changeover	99
6.5.3 Advanced Control Commissioning.....	100
7. OPERATIONAL MANAGEMENT	101
7.1 Operation and Development	101
7.2 Change Procedures	101
7.3 Housekeeping	102
7.4 Maintenance and Spares	103
7.5 Refresher Training.....	103
APPENDIX A.....	104
DEFINITIONS AND ABBREVIATIONS	104
APPENDIX B.....	106
LIST OF REFERENCED DOCUMENTS	106
APPENDIX C.....	107
GUIDANCE CHECKLISTS	107
C.1 DCS Specification Contents	107
C.2 Instructions To Tenderer.....	110
C.3 Front-End Engineering.....	111
C.4 Enquiry	112
C.5 Purchase	112
C.6 Delivery Schedule.....	113
C.7 Man-Machine Interface Philosophy and Specification	114
C.8 Detailed Design.....	115
C.9 FAT	116
C.9.1 FAT Specification.....	116



C.9.2 FAT - Hardware Testing	117
C.9.3 FAT - Software Testing	118
C.10 Delivery and Installation	119
C.11 SAT	119
C.12 Precommissioning and Loop Testing.....	120
C.13 Commissioning	120
APPENDIX D.....	121
ABRIDGED AMHAZ METHODOLOGY	121
APPENDIX E	125
SOFTWARE CHANGE REQUEST FORM.....	125

SUBSEA CONTROL SYSTEMS:

The old Section 4, Subsea Control Systems, has been removed from this latest (February 1998) issue with the intention of producing a separate document covering Subsea Control Systems or a new Subsea document with a section within it covering Subsea Control Systems.



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 Recommended Practice

This document gives the basis for the Specification, Selection, Design, Configuration and Use of Control and Data Acquisition Systems. It has been developed from cross-Business experience gained during capital project developments, operations and maintenance; and from equipment developments and evaluations.

This document gives guidance on Control and Data Acquisition system strategy, equipment selection and project development which is not available from industry, national or international codes. Where such codes exist for established elements of the technology, the document guides the user as to their correct application.

General

This document specifies all BP's general requirements for Control and Data Acquisition Systems that are within its stated scope.

This document previously contained sections for Telecommunications and Subsea Control Systems, which now appear under separate issue. This document has been updated to reflect the current industry wide appreciation of Control and Data Acquisition Systems. This document therefore contains abridged sections from those previously released, as well as some additional sections and sub-sections (see Contents).

Principal Changes from Previous Edition

Principal changes to Sections Issued from October 1994:-

- (a) Sections 3 (Telecommunications) and 4 (Subsea Control Systems) have been removed.
- (b) The sections have been updated to include references to new standards and reflect changes in operating practices.
- (c) Section numbering has been amended to suit the applicable part.



Application

Text in italics is Commentary. Commentary provides background information which supports the requirements of the Recommended Practice, and may discuss alternative options. It also gives guidance on the implementation of any 'Specification' or 'Approval' actions; specific actions are indicated by an asterisk (*) preceding a paragraph number.

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.

Feedback and Further Information

The document covers the rapidly developing field of digital technology, it is therefore intended to review and update this document at regular intervals. The value of this document will be significantly enhanced by contributions to its improvement and updating. Users are urged to inform the BP custodian of their experience which could improve its application.

Users are invited to feed back any comments and to detail experiences in the application of BP RPSEs, 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 Recommended Practice provides a guide to the Specification, Selection, Design, Configuration and Use of Control and Data Acquisition Systems.

The successful design of digital systems is a challenge. This challenge stems from detailed design after purchase order placement, rather than before as with most other equipment.

The document is structured to reflect phases of project execution, and sections can be used/ adapted for free-standing issue.

Other related Practices to BP Group RP 30-4 specify BP requirements for specific equipment, i.e. Instrumentation and Control Design and Practice, Measurement, Valves and Actuators and Protective systems.

1.2 Application

To apply this Practice, it shall be necessary to make reference to other BP Group RPSEs and national codes and standards as indicated in the relevant text.

Reference is made to British Standards. These standards are generally being harmonised with other International/European standards and will be allocated ISO/EN reference numbers. In certain countries, national Standards may apply. BP shall approve use of other standards.

1.3 Quality Assurance

Verification of the vendor's quality system is normally part of the pre-qualification procedure, and is therefore not specified here. If this is not the case, clauses should be inserted to require the vendor to operate and demonstrate the quality system to the purchaser. The quality system should ensure that the technical and QA requirements specified in the enquiry and purchase documents are applied to all materials, equipment and services provided by sub-contractors and to any free issue materials.

Further suggestions may be found in the BP Group RPSEs Introductory Volume.



2. SPECIFICATION

This section defines the recommended requirements for the safe, reliable and fit for purpose design and specification of a Distributed Control System (DCS).

The term DCS is synonymous with the family of micro-processor based process control systems that includes Supervisory Control & Data Acquisition (SCADA) and PLCs. The term DCS is used here in this wider context, and recommendations made are equally applicable across this family of system types.

The procedures for each specific project will depend upon its size and nature. Therefore a specific strategy should be determined for each project. The scope of the following activities should be assessed:-

- (a) Generate Statement of Requirements.
- (b) Pre-qualification of Vendors.
- (c) Front End Engineering Design.
- (d) Enquiry.
- (e) Vendor Selection and Purchase.
- (f) Detailed Design and Construction.
- (g) Factory Acceptance Testing.
- (h) Delivery and Installation.
- (i) Site Acceptance Testing.
- (j) Pre-commissioning and Loop Testing.
- (k) Commissioning.
- (l) Operation and Development.

It is important to develop a firm design and implementation framework during the DCS project formative stages. This should be done in association with the Asset management. Sufficient time should be allowed in the pre-project programme for development, discussion and acceptance of this framework.



2.1

DCS Project Organisation and Implementation Strategy

Many aspects of control system interact with other disciplines at various stages of the project. Project organisation should facilitate networking and communication between these disciplines. Key cross discipline links:-

Control Room Layout	Architect, Civils, H&V, Lighting
Hardware Installation	Architect, Civils, Electrical, Fire Protection, Safety Systems
Power Supply	Reliability & Availability
Hardware I/O Control	Process Design, HAZOP
Control Configuration	Process Design, HAZOP, Operating Procedures
MMI; Alarm Handling	Process Design, HAZOP, Operating Procedures
Training Simulator	Process Design, HAZOP, Operating Procedures, Training



The detailed design engineering of DCS differs from almost all other plant equipment because it is carried out after the purchase order, not before.

The detailed engineering is extensive and complex to manage. A number of approaches can be used to manage the detailed engineering phase. The following table lists the more common methods.

DCS IMPLEMENTATION METHODS				
Method	Hardware	Configuration	Application Software	Comments
1	Vendor	Vendor	Vendor	Best suited to grass roots projects with well understood and defined control requirements, e.g. BP licensed and own processes
2	Vendor	Vendor	BP	Best suited to grass roots projects with well understood and defined control requirements, e.g. BPs own processes
3	Vendor	Vendor	Contractor	Not recommended unless the contractor owns the process technology supplied and is DCS experienced and competent
4	Vendor	Vendor	Specialist	Useful where special application software is required e.g. optimisers
5	Vendor	BP	BP	Good for Site projects such as BP led reinstrumentation projects
6	Vendor	BP	Specialist	Good for site projects such as BP led reinstrumentation projects
7	Vendor	Contractor	BP	Needs careful vetting to ensure contractor DCS competence experience and capability. The number of information interfaces detracts.
8	Vendor	Contractor	Specialist	Needs careful vetting to ensure contractor DCS competence, experience and capability. The number of information interfaces detracts.
9	Vendor	Contractor	Contractor	Not recommended unless the contractor owns the process technology supplied and is DCS experienced and competent

On site-based projects such as reinstrumentation projects, BP will be generally managing the project and its resources whether they are wholly BP or integrated with contractor resources. Site personnel familiar with the operation and control requirements of the plant are invariably involved. Implementation methods 5 and 6 are therefore most appropriate.

On grass roots projects, the choice of implementation method is less straightforward and is influenced by the overall project organisation e.g. number of contractors their responsibility and the location and type of project, e.g. wholly-owned or joint venture. Methods 1 and 2 have proved the most successful. Methods 5 and 6 can also be used but they tie up significant BP resources for long periods, which can be difficult to justify. The other methods involving contractors and specialists should only be used following careful vetting and evaluation. Few plant contractors have a significant DCS capability.



In selecting an implementation method, it is good practice to minimise human interfaces, i.e. minimise the numbers of contractors and vendors and generally to avoid split responsibility unless the split is between BP and the vendor.

Whichever implementation method is adopted it is recommended that a DCS task force or team is formed with responsibility for the detailed engineering, from purchase order until at least completion of Site Acceptance. On Site projects, this team should be an integrated team where contract resources are used. On grass roots projects where the contractor typically is managing, the BP resources should be integrated with the Contractors and include a vendor representative. The team should ideally also contain members with responsibility for other control room instrumentation such as ESD to ensure a unified and robust control system design is achieved.

It is recommended that at least one BP DCS Engineer is involved full-time in any project using DCS. On site projects, and where a large DCS (e.g. > 2,500 tags or 250 control loops) is required on grass roots projects, it is recommended that more than one engineer should be involved.

2.1.1 Basic Training

Training in the basics of DCS technology and terminology, the use of keyboards and familiarisation with standard displays should normally be in a specialised training facility.

The following table provides overview guidance of the type, extent and likely timing of such training.

JOB FUNCTION	SUGGESTED TRAINING	TIMING	COMMENTS
Project manager Project engineer Planning engineer	DCS project overview	At start of project	Can be joint BP and vendor overview session
DCS engineer Control engineer	Full vendor training courses	Before detailed DCS design. Preferably before SDS development	
Process engineer Plant management	DCS overview course. Simulator training.	Before detailed DCS design	General overview by vendor
Maintenance technician	Vendor first line maintenance course. Attendance at factory testing	Before FAT	As an alternative on-site training by vendor following delivery can be considered
Operator	"Hands-on" training on DCS operation. Attendance FAT. Simulator training	Before loop testing at site	Generally carried out by BP DCS engineers.



The requirement for a Training Simulator should be determined at the initial stages of a project. If a Training Simulator is required, its schedule, resource and data requirements should be considered as part of the overall project plan.

Delivered, sufficiently early, the simulator will not only train operational staff, but provide valuable checks on plant control system design and operability, and operating procedures. Control schemes and display configuration can be developed in a 'live' environment, and process design problems can be identified and proposed changes validated.

The Pre-commissioning phase of the project is an opportunity for operators to become thoroughly familiar with the whole interface. Walk-through exercises can be used to test the compatibility of DCS displays with plant operating instructions.

Plant operating instructions should be developed interactively with DCS configuration to ensure consistency and compatibility. Training on the delivered system should be spread between instructors from operations, technical and engineering to give a balanced understanding of the capability of the interface and how it meets the operators needs.

2.2 Statement of Requirements and Control Philosophy

2.2.1 A Statement of Requirements (SOR) and Control Philosophy should be developed with the Operating Business to define the use and purpose of the DCS.

The SOR should contain the following information;-

- (a) Location, type and scope of plant to be controlled.
- (b) Scope of field instrumentation and instrument sub-systems to be connected to the DCS; interfaces to other systems.
- (c) Operator requirements (e.g. location and number of operating centres, number and responsibilities of individual operators).
- (d) Operating philosophy, (e.g. continuous or batch processing, start-up, shutdown and operation in normal, unsteady and emergency conditions: the need for operator intervention, what is controlled and monitored, and where).
- (e) Centralised control building and local equipment room requirements.
- (f) Extent and purpose of advanced control, profit optimising controls and management information.
- (g) The type, extent, features and location of associated equipment with a definition of the proposed interface; e.g. ESD & package equipment; to define alarm and display strategy.



- (h) Required control system reliability, availability and maintainability.
- (i) Definition of project responsibilities and third party involvement.
- (j) Changeover and Commissioning Requirements.

2.2.2

The Control Philosophy (CP) for the plant and its DCS is then developed in line with the SOR. The CP functionally describes how the control, monitoring and safe operation of the plant is achieved through the DCS. The CP should address the following:-

- (a) How the control of the plant is to be achieved, (broad functional terms).
- (b) The areas to be controlled and the extent of control, e.g. regulatory, sequential, advanced, optimisation.
- (c) Remote control requirements, (if any).
- (d) Subdivision of the plant into control 'Areas' and 'Units'.
- (e) The form and extent of the operator interface, e.g. number of consoles.
- (f) Number and types of displays and reports required.
- (g) Safety and protective system display, monitoring and interface requirements; e.g. philosophy and means for applying overrides.
- (h) Alarm Philosophy.
- (i) Operator console additional facilities (e.g. communications equipment, closed circuit TV).
- (j) Other user interfaces, (e.g.. shift supervisors, engineers, development engineers, disturbance, and plant management).
- (k) Interfaces to packaged equipment.
- (l) Interfaces to other instrument systems, e.g.. ESD, Fire and Gas, Metering, Analysers, Sub-sea, Anti-surge controllers etc.
- (m) How motors are to be interfaced and controlled.
- (n) Functional outline of software applications and any advanced control or optimisation required.
- (o) The extent of historical information recording and trending requirements.
- (p) The need and extent of computing facilities required for Management Information and higher level applications.
- (q) Hazardous Area Classification of field mounted equipment.
- (r) Field equipment interfacing, signal and transmitter types, e.g. smart.
- (s) Requirements for future expansion or plant integration.
- (t) Cabling and termination philosophy, i.e. overhead or underground, armoured cable or conduit, close coupled or segregated field terminations.
- (u) Power supply (UPS) and distribution requirements.



- (v) Fire and smoke detection and protection e.g. VESDA.
- (w) Environmental requirements of the control and equipment rooms e.g. HVAC, lighting, noise.
- (x) Established operating sites may include their requirements for DCS maintenance and support.

2.3 Front End Engineering Design (FEED)

A Front End Engineering Design is required to develop strategies for later stages of the project and to establish a robust Class III estimate to enable full project sanction to be sought.

During FEED the DCS design should be developed sufficiently so that the following will be produced:-

- (a) An approved Functional Specification for the system.
- (b) A cost estimate based on a firm quotation from the potential system vendor.
- (c) A definition of project strategy and cost estimate for detailed design, installation and commissioning phases of the project.
- (d) On projects associated with operating plant an implementation strategy for system installation and commissioning with due regard to operational safety and potential production losses, particularly where 'on-the-run' loop changeover is envisaged.
- (e) The outline Man Machine Interface philosophy.
- (f) Training requirements for operators, system engineers and maintenance technicians. Engineers and operators involved in the design will require training early in the project if they are to be effective.

2.3.1 Functional Specification

The Functional Specification should be based on the SOR and the CP documents and should describe the required system functionality. The Functional Specification (FS) should detail the vendor's scope of supply. It should:-

- (a) be written purely in functional terms
- (b) concentrate on application requirements, and not repeat vendor standard specification material.
- (c) include the extent of hardware needed and the requirements for overall project management of the system.
- (d) include sufficient information to permit sizing of the DCS.
- (e) an outline block diagram showing the inter-relationship between the major components of the DCS.



The block diagram clarifies the design intent and assists in ensuring that a unified and robust design is produced.

- (f) Include specific rules for implementing the design of displays.

The FS on a single vendor project will typically be developed in association with the vendor and include more specific design details, e.g. network topology, outline console design and layout, powering arrangements, and equipment packaging. Generally, the FS can be developed into the System Design Specification (SDS), with very little further work. This is an obvious advantage of the single vendor route. Where several vendors are being asked to bid, it may be necessary to write different FS documents for each vendor so as to make best use of each make of equipment, or to write the FS in more general terms so as not to prejudice the vendor selection.

2.3.2 FDS System Sizing

Accurate sizing of a DCS at the front-end of a project can be difficult. This is particularly the case on processes that are new and unfamiliar. DCS sizing can also be difficult on Reinstrumentation projects if drawings are out of date, etc.

Sizing of is predominantly a function of:-

- (a) Physical Input/ Output (I/O).
- (b) Number of control areas, consoles, screens and process operators.
- (c) The extent and complexity of the process to be controlled.
- (d) The number of users other than the operator.
- (e) The reliability & availability of control & monitoring required and hence the use of redundancy.
- (f) The extent of historical information recording.
- (g) The extent of subsystem interfacing.
- (h) he extent of advanced control.
- (i) The extent of interlocking.
- (j) The extent of event monitoring.
- (k) The application software processing requirements.
- (l) Numbers and types of control functions.
- (m) Power supply philosophy or arrangements.
- (n) Spares allowance viz. installed spare capacity and system expandability.



2.3.2.1 Physical I/O Requirements

The physical I/O required will depend on the extent of field equipment to be monitored and controlled plus any (non serial link) repeats from other systems such as the ESD system.

On new plant projects, the I/O count is best established from the P&IDs, or using data from a similar plant. For bought-in processes, the licensor can generally advise.

Machinery packages with condition monitoring, can be especially difficult to assess at FEED. The following guidance is therefore provided, n.b. figures are typical averages based on casings containing two radial, and one axial bearing:-

MACHINE	TYPICAL SIGNAL NUMBERS								
	Speed		Lube Oil Systems		Vibration & Displacement per Casing		Temperature per Casing		Status
	4-20mA	DI	4-20mA	DI	4-20mA	DI	T/C	DI	DI
Compressor			6	4	6	4	8		3
Turbine	2	1	4	8	6	4	6		2
Turboexpander	1			6	2		2		2
Hi-Speed Pump					4	4		3	3

2.3.2.2 Number of Consoles, Screens and Operators

The number of control areas and the number of process operators required will dictate the number of consoles and screens needed.

Plant complexity will ultimately have an impact on the design of the console(s), i.e. number of consoles, number of operators, and number of screens per operator. A Plant Complexity Assessment will assist in determining these requirements. Pertinent issues in this assessment will be the size of plant, degree of unit interaction, amount of advanced control schemes, etc.

(a) Control Loops (Valves) per Operator

An assessment of the operator workload can be broadly determined on the basis of the number of final control elements (control valves) that the operator must manipulate.

The number of control valves per operator is influenced by factors including plant complexity, additional tasks that the operator is required to perform, the degree of plant upset that may be experienced, etc.

Good practice within BP typically calls for between 100 and 200 control valves per operator, and reported good refinery practice indicates that the optimal number of control valves per operator is approximately 160, or 195 with advanced controls.

(b) Screens per Operator

Screens per operator depends on factors including plant complexity and the number of control valves allocated per operator.

Good practice within BP calls for 3 or 4 screens per operator. Consideration should be given to the 3 keyboard-6 screen (3+3 stacked) console on large units. Process plants with a high degree of complexity or high speed of response would need an increase above the figures given.

As technology changes and a move is made towards 'windows' based displays it will be possible to display additional data on one screen and it may be possible to reduce the number of screens per operator.

Poor display design can lead to demands for a greater number of screens per operator. Should an operator need two or more displays to monitor one task, improved design should be sought to provide this data more concisely.

(c) Screen for users other than the process operators

The number of users other than the operator requiring system access, i.e. engineers, plant superintendents, should be established, and dedicated screens in dedicated rooms are generally preferred.

On some DCSs two screens are required for effective DCS engineering work.

2.3.2.3 I/O Modules and Spares Allowance

Physical segregation of control areas and software maintenance requirements should be considered as there is always the need to develop software whilst the plant is running. Sizing in whole hardware modules per plant area or per reactor, etc. is generally the most practical and effective approach.



The chosen installed spares allowance significantly impacts DCS size and cost. The temptation to minimise on spares should be resisted as the cost and delay potential of running out of I/O far outweigh the hardware costs in spares. Spare capacity should be considered for both installed modules and rack-space. Installed modules can be added at small incremental cost, but adding rack-space can have a major impact on the project. The table is provided for guidance:-

PROCESS ATTRIBUTES	INSTALLED SPARES I/O ALLOWANCE		COMMENT
	MODULES	RACK SPACE	
Well Known	10%	20%	Min ^m recommended
Established (not well known)	15% to 25%	25% to 35%	Normal range
New and untried	30%	40%	Max ^m recommended

I/O spares allowance should be evenly distributed as far as practicable.

“Hot-spares” have the advantage that the equipment is guaranteed to work when it is needed, and in some cases can be used without physical interference. “Hot-spares” can also provide a development environment if appropriately configured. It should be ensured that when installed spares are removed from a live system there is no potential adverse affects on the adjacent live equipment.

2.3.2.4 Reliability and Availability

The reliability and availability of control and monitoring required as defined in the SOR, dictates the extent of redundancy required on shared processors, such as multiloop controllers, shared display processors, multiplexors and gateways. As a starting point the following design criteria can be applied:-

- (a) All control redundant. This applies to any shared control processor, power supplies and associated input/output cards, and may include the field loop equipment.
- (b) All monitoring non-redundant. Exceptions would be large capacity shared processing, (more than 16 analogue signals or 32 digital or temperature signals), or signals used for high value control schemes.

A CONSOP should be performed for high value control schemes

- (c) No single fault in the display system should cause a complete loss of process vision or ability of the operator to control the plant.



This means on systems with a single display processor driving several display screens, the display processor and screens would be redundant. Whilst on a single display processor per screen system, sufficient screens should be provided for a single display failure to be tolerated.

The availability/reliability requirements can then be established to match the process needs.

If the critical control loops on the process can be established and agreement reached that only these are redundant, a more cost effective design can be achieved. On demand corrective cover is an alternative consideration, and alternatives should be assessed on the maxim that the cost of plant downtime is generally large compared to the cost of DCS hardware to provide redundancy or other remedial alternatives.

On some systems the processing speed of control is user selectable. However faster control will be at the expense of a greater number of controller modules. Where variable processing speed is available, a 1 second processing interval satisfies analogue control loops with outputs to pneumatic control valves. Faster rates may exceptionally be required for interlocks or control of high-speed rotating machinery.

Beyond the basic three term control and process variable monitoring requirements, the following will normally demand additional processing capacity:-

- (a) Cascade control.
- (b) Mass flow conversions.
- (c) Selectors, e.g. hi-lo selects, etc.
- (d) Derived variable calculations, e.g. partial pressure, heat load.
- (e) Accumulations, e.g. flow or time integration.
- (f) Dynamic compensations, e.g. lead-lags, time delays.
- (g) Ramping.
- (h) Logic processing, e.g. for interlocks, etc.
- (i) Simple sequencing.
- (j) Custom algorithms, e.g. dual transmitter handling.

2.3.2.5 Extent of Historical Information/ Trending

The extent of historical information recording will have direct and significant impact on hard disc capacities. Advanced control and optimisation schemes will often require the historical collection of additional parameters to the PV, e.g. SP, OP. Without the use of data compression techniques, 50 kilobytes of hard disc capacity will typically be required to store 1 process variable at 1 minute intervals for 1 week.

Beyond the immediate needs of operations, (typically 2 to 4 weeks of history), plant data should be kept in a computer database, e.g. PI, Oracle on a DEC VAX. This allows data to be more easily and cost effectively managed, whilst facilitating wider access to the data.



All real time and historical data should be available for use in displays, trends, reports, calculations and application programs. As well as spot values the system should be capable of producing hourly, 4 hour, shift, daily, weekly and monthly averages of any selected analogue point for use in trends, reports and calculations.

Trend displays should be both real time and historic. It should be possible to assign all analogue input variables, any displayed, calculated or manually input variables and all controller setpoints and outputs.

It should be possible to trend multiple variables on the same screen for comparison of variables.

Trending should be selectable over discrete time intervals ranging typically from 1 minute to a minimum of 4 days. For historical trends it should be possible for the operator to scroll backwards through the last 4 days of 1 minute spot values of any selected point.

The system should allow the operator to re-scale the Y-axis of any trend or temporarily change the range of a point that is being trended for better observation of the trend.

2.3.2.6 Extent of Subsystem Interfacing

The extent of subsystem interfacing will dictate the number of interface modules or gateways required. In the case of PLC controlled packaged plant, typical I/O figures can usually be obtained from the vendor or the licensor. As these data are typically acquired via serial link the DCS tag number count, i.e. database size is affected rather than the physical I/O count.

2.3.2.7 Extent of Advanced Control

Additional controllers or modules may be needed for advanced control schemes and models, and for plants with significant amounts of batch control and recipe management. The sizing of these requirements is particularly difficult at FEED unless the application is well known or understood. It is recommended that an assessment is made of the number and likely size of programs required by:-

- (a) Comparison with similar applications
- (b) Consultation and advice from vendors
- (c) BP Group experience
- (d) Program number and size estimates



2.3.2.8 Power Supply Arrangements

The power supply arrangements for the DCS will affect physical sizing and cost.

On the process I/O, the choice needs to be made whether to power from redundant battery/charger sets within the DCS, or from an external high integrity (bulk DC or inverter) supply. The battery/charger set solution is generally cheaper and provides good diversity but does result in batteries in the DCS cabinets rather than in the switch room or elsewhere. The maintenance management of a distributed battery back-up system needs to cater for un-revealed battery failures, and for batteries failing at different times.

The operator interface is typically powered from an inverter fed mains supply.

2.3.3 Ancillary Areas

The DCS will impact a number of ancillary areas, in particular on the following:

- (a) Control and Equipment Room size.
- (b) Power supply requirements.
- (c) Heating, Ventilating, and Air Conditioning Requirements (HVAC).
- (d) Control Room Lighting.

Vendors can readily supply the physical dimensions, weights, power consumption etc. of DCS equipment. Good estimates can be made of system power consumption including inrush, and of system heat output. These can be used in the preliminary sizing for power and HVAC requirements.

Vendors often provide guidance on lighting. The lighting arrangements in the control room, and especially around the MMI should be subject to specialist advice from consultant specialists in ergonomic design.

The numbers of equipment and termination cabinets and consoles should be established in a vendor's budgetary estimate. Using this information, the DCS equipment in the control and equipment rooms can be laid out and the space requirements estimated. It is prudent to make some unallocated floor space allowance for future requirements.

As cabinets are often mounted on sub-frames, consideration should be given to the installation of sub-frames and cabinets to accommodate future expansion. Where a false floor is provided this should be integrated into the sub-frame to provide stability.



Cabinet spacing in equipment rooms should allow sufficient clearance for cabinet doors and access for maintenance. Inter-cabinet spacing of no less than 1 metre is recommended.

2.4 Performance

2.4.1 Safety Requirements

Reliable control systems are essential for safe operation of process plant. Unreliable systems place extra demands on safety devices such as relief valves and high integrity instrument systems. The performance of control systems is limited by equipment and application design and the normal errors made during operation, maintenance and modification. Where control system failure would lead to consequences such as risk to life, the environment or significant asset loss, separate devices such as relief valves or protective instrument systems should normally be provided to reduce the risks to tolerable levels.

All systems with protection functions with claimed average probability of failure on demand less than 0.1 shall be designed in accordance with [IEC61508](#) Functional Safety - Safety Related Systems (Reference RP 30-6).

2.4.1.1 Control systems where failures would lead to safety consequences or demands on safety systems or protective instrument systems shall also be implemented in accordance with [IEC61508](#) unless the following can be established:-

- (a) The safety systems is independent. It should be established that control system failures will not lead to a failure of the safety system to act on demand.
- (b) The safety system is separate. It should be established that the safety system is physically separate from the control system such that external influences such as environmental change or maintenance activities are unlikely to cause a failure of both systems simultaneously.
- (c) The safety system is designed for all reasonably foreseeable failures of the control system. With DCS's a single failure may cause all outputs on a single output card to fail to the high output state at the same time and it will need to be established that equipment such as relief systems have been designed accordingly. The same hazard could occur where complex



software schemes are used to control multiple valves on heating/cooling applications.

- (d) The safety system is designed for the likely failure rate of the control system. The likely failure rate can be established from either field experience, calculation using industry standard methods or industry databases on generic failure rates. The claimed failure rate should not be less than 0.1 per year.

2.4.1.2 Control systems can be used to reduce the demand rate on safety systems or protective instrument systems subject to the following restrictions:-

- (a) There shall be sufficient time for the operator to take action between when an alarm is indicated and when the process conditions exceed required levels.
- (b) The claimed reduction in demand rate shall not be more than a factor of 5.

2.4.1.3 Control systems which have not been implemented according to [IEC61508](#) can be used to diagnose failures of the protection system by comparing control system and protective system sensor readings. The diagnostic coverage can be taken into account in determining the average probability of demand of protection systems subject to the following restrictions:-

- (a) Alarms are automatically generated in a permanently manned control room when a difference in control and protective system sensors are detected.
- (b) The claimed diagnostic coverage for the sensor shall not be more than 60%.

2.4.1.4 Where control systems are used to diagnose failures of the protection system sensor(s) and the claimed diagnostic coverage is greater than 60% then the control system shall be implemented according to [IEC61508](#).

Where a failure of a control system would lead directly to a hazard and no independent protection is provided then the control system shall be implemented according to [IEC61508](#) but in addition the following will apply.

- (a) The process dynamics should be considered such that it can be established that the process conditions will remain within the



safe region after all reasonably foreseeable failures of process equipment and utilities.

- (b) A quantitative reliability analysis shall be carried out to confirm that the hazard rate is tolerable.

2.4.1.5 Certain control system vendors claim that their systems have been designed in accordance with [IEC61508](#). The advantages of using such systems include the following:-

- (a) The claimed demand rate on protection systems may be reduced leading to a reduction in the required safety integrity level of safety instrumented protection systems.
- (b) The number of shutdowns due to failures of the control system can be reduced.

2.4.1.6 Where credit is taken for the system being designed according to [IEC61508](#) the following shall apply:-

- (a) An independent assessment shall be carried out to verify that the control system is in accordance with the requirements of [IEC61508](#). Independent organisations capable of carrying out such assessments include TÜV, FM, Ineris, ERA.
- (b) Application software shall be designed, verified, validated, assessed, and modified according to the requirements in [IEC61508](#).
- (c) Where the same control system is used for non safety applications then the complete arrangement of hardware and software shall be designed and maintained in accordance with [IEC61508](#) unless it is demonstrated by independent assessment that the security arrangements are adequate to prevent design errors or unintended modifications causing failures of the safety functions.

2.4.1.7 System Safety Review

The consequences of equipment failure and its potential impact on plant protection systems should be considered. In particular, the failure modes of analogue output cards should be established, e.g. common mode failure causing multiple outputs to fail high simultaneously. Such failures may lead to a demand on the plant protection systems and should be addressed by techniques such as loop allocation, card de-population, equipment redundancy etc.



The DCS design should be subject to a formal (project) independent Instrumentation Technical Safety review. The Safety Review is a two part process.

- Part 1 Performed soon after the Process OHSE Stage 2 review
- Part 2 Performed soon after the Process OHSE Stage 3 review.

Typical Review Subject Categories	Documentation Required
Part 1	
Software variability of the system. Alarm Systems Control and Monitoring Operator Interface Occupational Health aspects Power Supplies Equipment location and environment Failure definitions Vendor choice and record	Control Philosophy Document Man-Machine Interface Design Document DCS Design Topology Drawing Power Supplies Single Line Diagrams SDS (dealing with part 1 review topics) Vendor Overview - summarising functionality P&I Diagrams

Typical Review Subject Categories	Documentation Required
Part 2	
Reliability Assessment Design implementation and progress Training	Vendor Reliability calculations Screen Display Layouts Control Room Layout Drawing Equipment Room Layout Drawing DCS Console Layout Drawing DCS Testing Strategy and Procedures Typical Loop Drawings Details of Advanced Control Schemes DCS Network Cable Routing Drawings DCS Training Strategy Later revisions of Documents reviewed at Part 1

2.4.2 Reliability and Availability

In addition to section 2.3.2.4, To achieve a practical design that meets the Business requirements in terms of reliability and availability the following approach is recommended. Establish the Business or operating plants requirements (or expectations) for:-

- (a) DCS failure definition. This will depend upon the type of plant and the nature of the process, e.g.

Minor	effecting loss of information/status data
Significant	effecting loss of a single control
Major	effecting loss of multiple control or vision
Total	effecting loss of the whole system



Unless otherwise specified by BP, major system failure criteria should be considered to be:-

- (i) Total loss of Operator screens for a process area.
 - (ii) A failure which causes two or more controller outputs to fail to a non safe position simultaneously.
 - (iii) A failure that causes the operator to be unable to adjust the output of two or more controller outputs.
- (b) Acceptable Mean Time Between Failure (e.g. MTBF > 10 years), or downtimes in hrs/yr, for each class of failure. This requires a knowledge of the technology, its capability and cost implications. Over specification should be avoided.
- (c) Acceptable equipment repair times for each class of failure.
- (d) terms (b) & (c) will enable the reliability and availabilities to be calculated for the DCS, its power supply and communications systems.

The vendor should define the calculation method and any assumptions made particularly those relating to failure modes and periods for individual cards or circuit boards. As well as random failures, common mode or systematic failures should not be overlooked. The design should be adjusted if necessary and the calculations repeated until acceptable results are obtained.

In the absence of specific Business requirements for reliability and availability it is recommended that section 2.3.2.4 is used.

All communication networks at the control level should be redundant.

In applications involving a hierarchy of control, the design should ensure that failures at an upper supervisory level do not affect the integrity or operability at the plant control level.

The integrity of critical control loops and redundant process equipment, e.g. duty/standby pumps, should be maximised where possible. Consideration should be given to allocating points to different I/O cards and controller files to minimise the impact of common cause control system hardware failures.

Where redundant arrangements are installed, the health of the duty and back-up devices should be continually monitored and any failure of the



duty equipment on control applications requiring uninterruptible service should effect an instantaneous switch to the back-up device.

It is recommended that failure identification and system recovery procedures are developed for the DCS. These should be written for and made available to the operators to inform them what immediate action, if any, to take in the event of a failure. Detailed recovery procedures should also be prepared by the Systems Engineer for all foreseeable failures.

The procedures and any fast load facilities should be tested at the site acceptance test. Very often this is the only time when the full system will be available for testing since in future there may always be some portion of the system in service.

2.4.3 System Response Times

Special requirements with respect to system response may be specified in project or tender documents. The following maximum response times should be met:-

All Graphic Displays	2 seconds
Alarm Annunciation	2 seconds
Operator Display Dynamic Data Update	5 seconds (normal)
	2 seconds (selectable)
Alarm and Event Resolution	1 second
Sequence of Events Resolution	1 millisecond
Response to Keyboard	immediate

Most plants are operated by means of Operator Graphic Displays in preference to Standard Displays, and emphasis should consequently be placed on the performance of these.



3. SYSTEM SELECTION AND PURCHASE

3.1 Pre-qualification of Vendors

A pre-qualification enquiry document should be produced which defines the functional requirements in broad terms without attempting to show how these requirements must be met. The document should also request vendor responses to various technical and commercial screening criteria.

There is a recommended 'move' to pre-qualify vendors for the Business(es) as a whole to avoid every project having to repeat this activity. The benefits of a uniform control system strategy across the Business(es) cannot be underestimated.

There is a need to prequalify and provisionally select (short-list) DCS vendors at an early stage. On a reinstrumentation project this must be done before the FEED, as significant differences in vendors equipment will influence many of the strategy decisions and the associated costs estimated.

Typical screening criteria for potential vendors should include:-

- (a) Size and resources of company
- (b) Recent experience and track record
- (c) An established Quality Assurance system
- (d) Long term commitment to product support, and the ability to provide on-site maintenance and application support.
- (e) Ability to provide and support application software
- (f) Communications capability
- (g) Adequacy of operator interface
- (h) Whole of life ownership cost, including integration with any existing support structure, site knowledge base and spares holding
- (i) Weight and space requirements
- (j) System constraints
- (k) System performance, e.g. display call-up times.
- (l) Ability to accommodate advanced control and higher level applications.
- (m) Integrated ESD and Fire and Gas system capability.

A qualitative evaluation should be carried out on the vendor responses to the pre-qualification enquiry document, by considering the functional aspects of the systems and assigning scores and weighting to these aspects.

The DCS evaluation should also take account of relevant in-house company experience where a system is well established and its technical strengths and weaknesses are known. Where systems are less well known, these systems may have



been in-house benchmarked. Account should also be taken of external technical evaluations, typically by SIRA or TNO.

3.2 Enquiry and Vendor Selection

3.2.1 Invitation To Tender

It is recommended that all commercial requirements associated with an enquiry are separated from the Functional Specification (FS) and are presented in an Invitation To Tender (ITT) document. The FS together with the ITT documents forms the Enquiry Specification.

The ITT should define the relative responsibilities of vendor and purchaser to meet the requirements of the functional specification along with the commercial terms and conditions of purchase. It should be drawn up by a procurements and contracts engineer familiar with digital systems.

3.2.2 Secrecy Agreements

On some BP processes, there is a requirement to implement a process specific control package in the DCS. These packages invariably contain process know-how which is proprietary to BP. In these cases, a secrecy agreement shall be drawn up and signed with the vendor or contractor before any information is released for design and implementation. This agreement shall preclude release of information to any sub-contractors. These shall be covered by separate agreements where necessary.

3.2.3 The Tender

Tenderers should be required to supply their project programme covering the period from contract award to site acceptance testing. Key Dates and Milestones should be defined.

A statement of compliance should be completed by tenderers to confirm the level of compliance or non-compliance against each paragraph of the ITT and FS.

Tenderers should provide a breakdown of costs, including the following key areas:-

- (a) System Hardware.
- (b) Licensed and applications software.
- (c) System configuration.
- (d) Contract documentation.
- (e) Project management costs.
- (f) System testing, delivery and site installation.
- (g) System support options.
- (h) Training options.
- (i) Schedule of rates for reimbursable services.



(j) Basis of charging for contract variations.

Attention should be paid to whole of life system costs. Tenderers should therefore supply a list of recommended spare parts together with software and hardware support costs and call-out support costs.

Tenderers should propose their project organisation and implementation policy. A project organigram should be requested to clearly define the proposed reporting structures within the various departments of the vendor's organisation and with any proposed sub-contractor. Details should also be supplied of design information flow and communication routes. They should nominate a project manager and any lead discipline engineers, declaring their previous experience with the specified system.

Tenderers should provide details of perceived and actual work load projections for the proposed contract period.

Tenderers should detail standard documentation, both hard copy and firmware based, and define in detail any project special documentation required.

Vendor responsibilities covering delivery, site installation and site acceptance tests should be defined. Site manning level estimates and organisation should be provided. All site works should be performed using site approved contractors.

Recommendations for training courses for engineering, technical and operations staff should be requested; both vendor based and site based. The provision of such courses should be negotiated at the same time as the main supply contract.

Tenderers should provide their preliminary Quality Plan and QA Procedures.

3.2.4 Bid Evaluation and Vendor Selection

A technical and commercial qualitative assessment should be carried out taking account of whole life cost of ownership to select the most cost effective and fit for purpose system.

Received bids should be checked for accuracy, i.e. do the numbers add up and match requirements. The bids should be checked for over and under specification errors. Both can be expensive, and sometimes impossible to correct later.

Allowances for services and support, e.g. project management should be carefully vetted.

Application software and configuration man-hour estimates should be assessed against the scope of work requested.



Compliance with the FS and ITT should be checked against the vendors compliance statements. Bids should be reconciled so that a 'like for like' comparison is made. A 'Clarification' meeting may be held to confirm and finalise the scope of individual tenders.

3.3 Purchase

3.3.1 Negotiation

On competitive bids post tender negotiation may be sanctioned. Negotiation will generally commence towards the end of the enquiry phase once all bids have been evaluated and reconciled.

The negotiator should be assisted and supported by a DCS Engineer fully familiar with the bid and the system to be purchased.

3.3.2 Purchase Specification

The Purchase Specification should be an updated version of the Functional Specification. The update should endeavour to include the following:-

- (a) Elimination of all non-compliance
- (b) Incorporation of all clarification issues
- (c) Incorporation of all changes agreed during the enquiry, clarification and negotiation phases.

The above can be conveniently presented as an addendum to the original Functional Specification.

3.3.3 Delivery Schedule

During negotiation, the delivery schedule for the system, services, and information to be supplied should be agreed. All significant dates should be clearly identified and tabulated in a schedule of dates. This should include Project Milestones which are associated with a contract payment, other key dates related to project schedule, and information due dates, to allow work to proceed smoothly.

3.3.4 Warranty and Vendor Support

It is recommended that warranty support is discussed with the vendor during the contract development phase to ensure that the extent and duration of warranty cover for hardware and software failures matches the project requirements.

The warranty period should commence from the date of factory acceptance, delivery, or site acceptance, as applicable. Where the interval between completion of acceptance testing and plant start-up is expected to be longer than the vendor's normal warrantee period, it is recommended that an extension to the warranty is negotiated, as some problems may only manifest themselves once the plant is operational.

System warranties should, as a minimum, cover the repair or replacement of faulty hardware/software by the vendor, including the costs of carrying out such repair or replacement at the point of use. The level of support that may be expected under the warranty (e.g. engineer availability, delivery and response times) should be established.

Maintenance support following the warranty should be explored at this stage to establish the range of options available and their likely cost. Although support following warranty will be the responsibility of the operational site, there is generally significant advantage in negotiating for, or actually purchasing hardware spares at project prices.

3.3.5 Payment Terms

The payment terms need to be appropriate for local conditions and to minimise BP's risk and exposure. Stage payments against agreed Milestones are generally used on European Projects but other arrangements are prevalent elsewhere.

The following payment terms are typical of European projects and are provided for guidance:-

(a)	Receipt and approval of the SDS	5%	Total	System Price
(b)	Confirmed delivery of all hardware into staging	15%	Total	System Price
(c)	Completion of system assembly	20%	Total	System Price
(d)	Completion of Factory Acceptance Test	35%	Total	System Price
(e)	Completion of Site Acceptance Test	25%	Total	System Price

Payments (a) to (c) are generally covered by bank guarantees valid until delivery to site. Payment (e) by a bank guarantee valid until the end of the warranty period.

3.3.6 Training

It is recommended that consideration be given at an early stage of the project towards the training requirements of staff on the DCS. Where a contractor is involved, his engineering staff will also need training early in the project if they are to be effective. The provision of training courses by the vendor on the DCS should form part of the DCS contract rather than a separate training contract.

The purchase phase is a good time to secure training courses for technical and other staff. Often an element of vendor training can be negotiated into the contract at little or no extra cost.



4. DETAILED SYSTEM DESIGN

4.1 Project Management

4.1.1 System Design Specification

It is strongly recommended that following the issue of the purchase order the vendor be required to develop a detailed system hardware and software specification of the system. This specification is called the System Design Specification (SDS).

The objective of the SDS is to allow the detailed system design to be more fully developed in functional terms and to verify that the vendor fully understands the requirements and his scope of work. It further allows BP to more fully understand the vendor's system functionality and supply. Development of the SDS should be led by the vendor with full involvement of BP and the contractor where appropriate.

As a minimum the SDS should develop from the Purchase Specification the following aspects:-

- (a) Control Room and Equipment Room Layout drawings.
- (b) Equipment general arrangement drawings.
- (c) Signal interconnection diagram.
- (d) DCS Console design layout.
- (e) The allocation, partitioning and numbering of hardware including installed spare equipment.
- (f) Principles to be adopted to minimise the effects of failures, (e.g. redundancy levels, slot allocation rules).
- (g) Unit and Tag numbering rules.
- (h) Field cable termination cabinet general layout drawings.
- (i) Control system cabinet general layout drawings.
- (j) Definition of earthing schemes and external and internal power supply arrangements.
- (k) Finalised functional specifications of all special project application software.
- (l) Finalised details (including scope and security details) of serial link or network architecture interfaces to other systems.
- (m) Finalised Man Machine Interface (MMI) philosophy, i.e. display hierarchy and design rules.
- (n) Alarm prioritisation, presentation and handling philosophy.
- (o) The definition of historical data storage (i.e. trending and archiving).



4.1.2 Management of Data

A significant task when engineering DCSs is the control and management of the design data.

It is recommended that the means of data management and flow to the vendor is discussed and agreed early before any significant amounts of design data are generated. It is recommended that computer based systems and electronic data transfer is used rather than paper forms.

Most DCS vendors can now provide PC based configuration packages for their systems. Alternatively, projects have previously developed instrument databases.

4.1.3 Documentation

The provision of documentation of the right level and at the right time is an essential requirement of DCS projects.

The overall documentation requirements should be clearly identified in a documentation index. This generally forms part of the vendor's contractual scope of supply.

The following documentation should be provided as a minimum. In many cases this could be provided within a self documenting system, e.g. configuration database, and this need only exist on the system and backup disks:-

- (a) Hardware Layout and General Arrangement.
- (b) Full Set of Vendor Hardware, Software and Configuration manuals.
- (c) Details to assist the specification of linked equipment, e.g. HVAC, UPS.
- (d) System Design Specification.
- (e) System Block Diagram and Interface Schematic.
- (f) Operator Manuals.
- (g) Termination Index and Input/ Output Listing.
- (h) Configuration Database.
- (i) Advanced Control Schematics.
- (j) Logic Diagrams.
- (k) Sequence Flowcharts.
- (l) Man-Machine Interface Design Document.
- (m) Power Supply, Distribution and Earthing Drawings.
- (n) Reliability Report.
- (o) Installation Planning Manuals.
- (p) Acceptance Test Procedures.
- (q) Application Software Manuals.
- (r) IS Certification Dossiers where appropriate.
- (s) System Maintenance Manuals.
- (t) "As built" design documents.



The following table gives guidance in assessing the main documentation requirements and their timing of issue:-

ACTIVITIES	DOCUMENTS	TIMING	COMMENTS
DCS Engineer Support	Full set of vendor specifications and configuration manuals. System Design Specification (SDS)	Within 1 month of contract award Within 2 months of contract award	Usually subject to BP approval
Other discipline support	Operator manuals Design Specification Man-Machine Interface	Within 1 month of contract award Within 2 months of contract award	
DCS Installation	Installation planning manuals	Within 1 month of contract award	
Specification of ancillary equipment	Heat dissipation calculations. Power consumption and distribution details. Earthing details	Within 1 month of hardware freeze or earlier.	Usually subject to BP approval
Definition of detailed design	DCS and equipment drawings. DCS configuration details. Cable, wiring and termination schedules. Application software functional design specifications.	Live documents subject to revisions until design is frozen Prior to any software coding.	Usually subject to BP approval
Definition of test procedures	Acceptance test procedures	1 month prior to any testing or earlier.	Usually subject to BP approval
Operator Training	Operator manuals "As built" display and configuration details.	Prior to any operator training	Where a training simulator is used details of the DCS displays and configuration will be required to build the simulator.
Definition of the detailed design. Loop testing Pre-commissioning Commissioning "First-line" maintenance Support over plant lifetime.	Full set of vendor specifications, configuration and operating manuals. "As built" configuration details, drawings, and schedules. Application software manuals IS Certification dossiers where appropriate. Maintenance manuals	Factory acceptance test for review and approval. Final issue at or close to Site acceptance.	Subject to BP approval. This documentation will comprise paper and electronic format items.



4.1.4 Software

It is recommended that the vendor produces for approval a Detailed Functional Specification of all application software to be written.

Before placing any equipment order, the vendor should clarify the standard system software release that will be supplied and his expected software updates in the coming three years. The migration path for future software upgrades should be clearly specified by the vendor.

Application software is expensive to develop and maintain compared to the use of standard vendor algorithms. Therefore application software coding should be minimised with maximum use being made of the DCS vendor's standard algorithms.

For straightforward supervisory control and monitoring applications where coding is necessary, the DCS vendor's control language and applications/control processor will generally be the most cost effective and appropriate choice. For more complex applications, e.g. optimisers and real time databases, industry standard high level languages such as FORTRAN 90, PASCAL or C running in a plant computer should be considered.

4.1.5 System Configuration

The system should be provided with an engineer's console capable of allowing the complete system configuration and program development. The engineer's console should as a minimum be able to perform the following tasks:-

- (a) Configure the system and point database (both on-line and off-line.
- (b) Build all operator displays.
- (c) Save and load all configuration data.

It should also be possible to save and load configuration data from the Operator's workstation.

The system should be capable of self documenting configuration data in clear English format onto a printer. Additionally, it should be capable of saving configuration data on portable digital media for safe storage.

Bulk system configuration should be performed on a PC or Workstation rather than on the system itself.

4.1.6 CONSOP

The CONSOP (**CON**trol Safety and **OP**erability) review methodology provides a structured and systematic framework and approach to review the controllability, safety and operability issues surrounding the implementation of complex advanced control applications.



CONSOP was developed as a result of some early and adverse operational experiences with proprietary multivariable predictive controller (MVPC) applications. CONSOP is complementary to existing HAZOP and PHSER reviews, utilising many of their principles but, importantly, addresses areas not covered by them. Other techniques, such as FMEA and CHAZOP concentrate on the security and integrity of system hardware and software, rather than the adverse operability consequences of MVPC mal-operation.

CONSOP is implemented by a multidiscipline review team that apply a checklist of questions covering all aspects of application implementation, operation and interface handling.

Provision of the CONSOP methodology as part of the bid documentation to a vendor serves the purpose of acting as a design guide and, consequentially, results in more appropriate and better quality bids and quality assurance during project implementation.

CONSOP is used by BP Oil sites and has also been taken up by third parties.

CONSOP methodology details are given in report No: 1995-224022. Guidance is given on how to run a review, its documentation, team composition, timing and deliverable requirements. The deliverable is a short CONSOP report, with defined supporting documentation. An audit trail of what was reviewed is thus provided, including review Findings and Recommendations and a register for recording subsequent actions. Extensive background notes to preferred solutions are provided for the checklist questions as well as techniques for analysing the complex and interactive nature of MVPC applications.

4.2 System Infrastructure

4.2.1 Control Room Design

4.2.1.1 Console Design

The Operator Console typically consists of a combination of the following:-

- (a) Operator Stations (display screen and keyboard sets).
- (b) An auxiliary console area for hardwired equipment (e.g. for ESD buttons, PA system).
- (c) Communications equipment (e.g. telephones, radio).

In addition, space should be provided for operators documentation along with a suitable writing area.

The Operator Console should comply with the HSE Display Screen Equipment Regulations 1992 (EEC directive [89/391/EEC](#)). These requirements include:-

- (d) display screen with stable image, adjustable brightness and free of glare.



- (e) minimisation of reflection, noise, heat and radiation.
- (f) adequate lighting and humidity.
- (g) work chair with leg room and clearances for postural changes.

Examples given by the HSE where compliance can be argued as being unnecessary include:-

- (d) use of detachable keyboard - inappropriate where the operator has to locate and operate emergency controls.
- (c) requirement for tilting and swiveling screens - undesirable as screens may need to be aligned in a console.

The HSE also state that more detailed and process industry specific standards such as the draft [ISO 11064](#) standard on the general ergonomic design of control rooms should be applied.

An operator console should be provided for each section of the plant normally under the control of an individual operator, or operating team (where all members are responsible for operating the same process units).

Each console should be furnished with facilities to provide alarm logging and report production. Typically, 2 printers are provided. One printer should be used exclusively to log alarms and events. Alternatively, where there is no statutory or operational requirement for a printer, consideration should be given to installing a separate computer based alarm and event logging system. The other printer should be used for other services such as printing of reports.

The printers should have a maximum noise level of 48 dBA. The level may be achieved by the use of acoustic hoods.

Alternatively, consideration should be given to the installation of printers in a separate printer room.

A video copier should be made available near the operator consoles for taking colour prints of the displays.

The most efficient operator screen pointing device should be selected. Considerations should include that Touch screens may not be the preferred device, especially in a Windows environment, due to lack of precision, poor resolution, arm-reach fatigue, errors when cleaning etc. A preferred alternative may be the mouse (except for robustness) or tracker-ball.

The extent of hardwired equipment mounted on consoles should be minimised to that required for safe operation of the plant. Hardwired annunciators, pen recorders and back-up controllers are not normally required.



Trip alarm panels may be installed in the console and if so should be placed in a position where the operator can comfortably access the controls (e.g. reset/defeat/accept).

Console layout should be reviewed and agreed with the plant operations team.

A curved console layout is generally preferred since it improves the operators overview.

Consoles for users other than operators (plant management, engineers, etc.) should be positioned away from the main control area.

A 'Supervisor Monitoring Console' may be provided which is set apart but close to the operator consoles. This will provide an overview of all plant areas and is intended for use during plant incidents. Process shift supervisors would typically use it during normal operations.

Data from other information sources (e.g. management information, lab data, etc.) required by the operator for process operations should be displayed within the console, preferably on DCS screens. The introduction of 'windows' based displays can remove the need to integrate 'non DCS' screens into the console layout.

The operators DCS console is a collection of DCS workstations, peripherals, telecommunications and ancillary equipment.

The ultimate console layout must be reviewed and agreed with the plant operations team. This is essential to avoid re-design post commissioning.

4.2.1.1.1 Layout of Console

The layout of the operating consoles must be agreed and accepted by the operations team. Allowing operators to visit vendors facilities or to sites where the equipment is installed helps to establish preferred layout very early in a project. This practice also engenders ownership.

The layout requirement of other types of equipment needs to be included e.g. radios, telephones, CCTV controls, etc.

A number of different layouts are generally used throughout the industry ranging from a single tier approach (i.e. a number of screens side by side) to a two tier design (screens side by side and on top of each other). The design also dictates the number of keyboards and hence the maximum number of operators that may use the console at any one time. A concave curved console layout is generally preferred.

A console design with upper and lower screens above keyboards would give a single operator easy access. However in an upset if two operators were required access would be difficult. Similarly a console design with a number of screens side by side would give a single operator difficult access to all screens. To this effect the ergonomics of the design against the physical measures of the operator must be



considered. It should also be noted that on certain systems upper screens have limited functionality.

Other consoles may be required for other users e.g. maintenance personnel, disturbance monitoring, operations management, DCS engineers, etc. These should be positioned away from the main control area, but preferably within visual range.

A prototype console in the form of a cardboard mock-up should be considered at an early stage in a project. This allows different configurations to be tried out ensuring the best design is achieved. This exercise may take the form of a complete cardboard replica or simply pictorial representation of the screens, ancillary equipment, etc., pasted to a wall to give the operating team a look and feel of the final design.

Adequate space should also be made available for any associated documentation and a writing area for the operator during his normal work tasks.

4.2.1.1.2 Other 'Control' Equipment

Trip alarm panels may be installed in the console and if so should be placed in a position where the operator can access the controls (i.e. reset/defeat/accept).

Any secondary information systems (i.e. management systems required by the operator) should be fed via the DCS console screens. If this is not possible then secondary information screens may be integrated into the operators console.

Communications equipment (radios, telephones, etc.) will also need to be located within the console. This should be positioned to allow easy access and to particularly avoid having trailing leads running across screens (and possibly interfering with touchscreen mechanisms).

4.2.1.1.3 Disturbance facilities

Where a control-room contains two or more teams of operators having different areas of responsibility, their activities may be co-ordinated, during a major upset, from a single disturbance centre manned by a process supervisor. The following issues should be considered:-

- (a) The consoles may be read-only with no control actions permitted.
- (b) Special displays should be provided covering the whole plant or site controlled from that control room.

Enables the supervisor quickly to assess the overall context in which actions are being taken.

- (c) Access to all of the displays used by all of the operating teams



Enables the supervisor to refer to the same information that the operators are using.

- (d) The supervisor needs rapid access to emergency operating procedures.

Where these are provided in electronic form, the disturbance centre must include access to these.

- (e) Appropriate communication equipment should be provided: radio, telephones, hot-lines to shift management and emergency services.

The overall disturbance centre design and its position relative to the other operator consoles, is an important aspect of the plant definition or site emergency procedures. It is essential that these are done as a co-ordinated activity during a project.

The disturbance centre may also be used in quiescent times for the benefit of engineers, managers or others needing to access process information.

4.2.1.2 Control Room Layout

The following issues should be considered in determining the control-room layout:-

- (a) The console or operating desk should be laid out in a concave curve.

This facilitates easier viewing across a number of screens.

- (b) Where there are several operating teams, an inward facing horse-shoe, oval or circular arrangement of consoles is recommended. The split and size of the consoles needs to reflect the operating strategy.

Walk-through gaps in the console delimit areas of responsibility, whilst facilitating communication between different operating teams.

- (c) ESD, F&G , and CCTV operating facilities are normally incorporated into the console. The monitors for these systems may be console mounted, (windowed into DCS screens), or remote mounted (ceiling suspended or wall mounted).

Such systems must be clearly visible at all times to the operators, and the same system may need to be seen by several teams of operators.

- (d) Large back-projected wall-mounted screens displaying plant or site over-view information may be used.



The audience for this feature should be carefully considered. Display resolution may be insufficient for the normal control room occupants, however plant and site over-view information can be useful for control-room visitors.

- (e) Communications equipment, (telephone and radio), should be readily accessible on the operating desk without moving from the normal operating position.

Vertical console mounting is often preferred as it leaves valuable desk-space free.

- (f) Process documentation, (logs, night-order books, operating instructions, P&I diagrams, emergency procedures, &c.), should be readily accessible from close to the operating position, and there should be a convenient table or desk to spread out and use the documents and drawings.
- (g) Consideration should be given to segregating the control-room from other parts of the building by a windowed corridor.
- (h) A desk may be positioned away from the operating position for issuing work permits etc. This desk may also be used for interactions with tradesmen, visitors and other external issues.

This keeps non-operational personnel away from the operating area.

- (i) DCS Engineering should be performed in an adjacent room, separated from the control-room by clear glass partitions. The screens should be positioned where the operators can see them in use.

This enables the operators to see who is working on the system without the intrusion of non-operational personnel in the control-room.

4.2.1.3 Control Room Access Control

The following issues should be considered in controlling control-room access:-

- (a) Access doors should be positioned to discourage the use of the control-room as a corridor to other parts of the building.
The control applications group may have a dedicated entrance.
- (b) Visitors should be able to see the control room without intruding by means of a windowed corridor (or other barrier, e.g. desk).
- (c) permits etc. should be dealt with from a desk close to the access door or through a hatch.
- (d) Other means of restricting access to the operating area may be considered, such as floor demarcation lines or illuminated signs.



It is important that only those essential for plant operation have access to the operating area, especially when dealing with a critical disturbance when distraction by unwanted personnel can degrade operator performance.

4.2.1.4 Control-Room Lighting

It is recommended that a lighting consultant is appointed to design the control room lighting. Consideration should be given to:-

- (a) Closely focused and shielded down-lighting, different zones being individually adjustable for brightness.
- (b) Operating screens should be hooded or provided with anti-reflection masks.
- (c) Individual lights, adjustable for position, direction and brightness, may be provided for reading documentation or drawings.

There are two conflicting requirements on control room lighting:-

It is essential to avoid glare into the operators' eyes and reflections from the operating screens; these are both distracting and tiring.

and

There must be sufficient light to allow documentation to be clearly and easily read, to avoid a depressing atmosphere and to help night-shift operators to stay alert.

Research has shown that night-shift operators remain more alert if close attention is paid to lighting quality. The spectrum should match that of natural sunlight, and it should be comparable in brightness. It is not necessary, however, that it floods the entire room, but it may be contained in a non-distracting position to one side of the operators' normal range of view.

4.2.1.5 Control Room Noise

Recommendations are to provide:-

- (a) Good external and internal insulation.
- (b) Acoustic ceiling-tiles.
- (c) Carpets, carpet tiles or soft vinyl flooring in preference to hard surfaces.
- (d) Shrouding console equipment cooling fans.
- (e) Key-boards that minimise key-rattle.
- (f) Printers located in a separate printer room, or substituted by PC based printer replacement system.

It is highly desirable that control-room noise-levels are minimised. All noise is distracting and tiring. It also interferes with communication



between operators, between operating teams and with supervision in a disturbance. Noise also tends to raise anxiety and tension in a disturbance tending towards emotional instead of logical decisions and actions.

4.2.1.6 Control Room Interior Decoration

Careful consideration should be given to the visual features of the environment.

- (a) Bright shiny highlights should be avoided.

They cause glare and reflections from the screens.

- (b) A series of different and distinctive features should be provided.

A typical control room may have a selection of mural paintings/ large photographs and groups of large potted plants. This allows the eyes and mind to restfully exercise and relax.

Where control rooms feature an expanse of bare plain walls, operators feel a sense of disorientation and depression. The lack of external windows also causes a sense of time-disorientation leading to fatigue and lack of concentration. This can be reduced with dummy windows opening onto a large landscape photograph, with programmed lighting, (direction, spectrum & intensity), to follow a natural day cycle.

4.2.1.7 Control Room Furniture

In general, the control-room furniture should be robust but comfortable. Colours should be chosen to blend with the rest of the decor, but should avoid shiny surfaces or bright highlights as these can cause glare or reflections from the screens. The following issues should also be considered:-

- (a) Operating screens and keyboards may be console mounted, but should preferably be located on desks specifically designed for the purpose.
- (b) Sufficient clear desk area should be available for the documentation that the operator needs to consult in performing his task.
- (c) The desk should include sufficient clear knee-space and foot-rests to allow a variety of comfortable operating positions.
- (d) Chairs should be able to swivel 360°, and ride on castors. They should have a shoulder-high back with a fully adjustable lumbar support, seat-height and seat-tilt adjustments and may be provided with arm-rests. Arm-rests, if provided, should be chosen so mutual damage is not caused with the console where they come into contact.

The operator console chairs are in constant use, 24 hours a day, and get extremely heavy wear. They should be designed to be robust and hard-wearing as well as comfortable. They should be replaced promptly if they become dilapidated.

- (e) Documentation tables should be large enough to spread out the largest drawings the operators need to consult; they may include drawing and documentation storage facilities in the base.
- (f) Furniture for efficient storage and rapid retrieval of bound documentation, such as operating instructions, should be provided.

4.2.2 Equipment Location and Accommodation

The control equipment should be installed in areas where the environmental conditions will not violate the vendors specification for temperature and humidity. The need to protect against ingress of dust particles and corrosive chemicals should be considered. Environmental control via HVAC is usually required for most applications.

Heat load and temperature rise calculations should be carried out and input into the HVAC design.

Digital equipment installed close to or within plant areas should be installed in housings which meet the required environmental conditions. Wherever practicable, local equipment rooms should be located in safe areas.

Fire detection and protection should be provided for computer/electronic equipment rooms.

Computer equipment supporting higher level control schemes and information systems should be located in a secure equipment room where access can be controlled.

4.2.3 Spare Capacity and Upgrades

Further to the guidance in section 2.3.2.3. Spare capacity should be provided for future site development and modification. Capacity for future development should be agreed with the client Business. The extent of spare capacity shall be specified by the user in tender or project documents and are job specific.

As the design develops and better definition is obtained it may be possible to reduce the spare capacity defined at FEED. It should however be remembered that the difficult areas to expand easily are equipment racks, power supplies and pre-wired controller and circuit board files. Priority should be given to retaining sufficient space in these areas. Slotting additional circuit boards into pre-wired files is relatively easy and boards can often be secured relatively quickly.



The spare capacity should normally be evenly distributed throughout the system unless it is known that there is more potential growth in one area rather than another.

An examination should also be made of system capacity with regard to processor and communications loading.

Typically, the average loading should not exceed 50% at placement of order. The loading limits may vary depending on the system and should be discussed with the vendor.

As a minimum the spare capacity for the following items should be specified:-

- (a) I/O points.
- (b) Control processor capacity.
- (c) Point database.
- (d) Display database (particularly Graphics.
- (e) Historical database.
- (f) Communications network loading.
- (g) Communications Gateway or interface units.

In addition to the specified spare capacity the system should be capable of future expansion without major changes to the existing hardware/software.

4.2.4 Power Supplies

Electrical Power supplied to the DCS should be uninterruptible and plant operation must not be affected by short term supply variations.

Careful consideration of power supply configuration is recommended to ensure optimum DCS availability. It is recommended that:-

- (a) DCS power should be derived from two independent secure supplies.
- (b) Power should be supplied to and distributed within the DCS in accord with the requirements for system reliability and the effect of failure on plant operation and availability.

4.3 System Functionality

Detailed design of the hardware involves confirming and freezing the quantities and the arrangement of equipment. The frozen design should recognise the needs of all the system users and should encompass the requirements for system availability and ease of maintenance.



The design should provide a reliable, well proven system in the simplest and most standard form to meet the project requirements.

Equipment should be provided to cover all operational needs during both normal and abnormal plants conditions.

Control functions should be allocated within the system hardware with due regard to plant integrity, common mode failure, cable marshaling, efficient use of equipment and segregation for maintenance.

When allocating functions to non-redundant equipment the effects of on-line maintenance and reconfiguration should be considered.

Typical activities during hardware detailed design are:-

- (a) Confirmation and freezing of DCS size in terms of controllers, I/O points, consoles, screens etc.
- (b) Confirmation and freezing of DCS cabinet and console layouts and sizes.
- (c) Design and layout of field termination cabinets (FTCs).
- (d) Allocation of field cables to FTCs. Draughting of termination and cable schedules and loop diagrams. Design of cable entries and routings.
- (e) Allocation of cables and cores ex DCS. Design and draughting of DCS-FTC and internal DCS cabling.
- (f) Calculation of heat load and its distribution for input into HVAC design.
- (g) Confirmation of power supply sizes and arrangement, catering for in-rush current requirements. Specification and procurement of non DCS vendor supplies, e.g. UPS. Design and draughting of distribution and fusing.
- (h) Design and draughting of DCS earthing arrangements including any plant computer.
- (i) Design and draughting of inter-system cabling and electrical isolation requirements. Typically for DCS-ESD, DCS-Machinery Monitor, DCS interfaced packaged units, ESD interfaced packaged units, DCS-Plant computer.
- (j) Design of ESD system operator plaques and integration into DCS consoles if required.
- (k) Design of miscellaneous and telecommunication systems and their integration into DCS consoles.
- (l) Design and layout of control room, equipment room, and any outstation rooms.



Where a DCS needs to interface with other systems such as computers, PLCs, analysers, anti surge equipment, metering systems, plant protective systems etc., it is recommended that secure and field proven data links are used.

As a minimum suppliers of DCSs should demonstrate well proven interface units to the following items of equipment:-

- (a) Windows NT based PC's
- (b) PLCs and other equipment using serial links with industry standard protocols.
- (c) DEC VAX and UNIX range of computer equipment.

The preferred digital transmission protocols at the control network level should be deterministic. Therefore in general [IEEE 802.4](#) Broadband Token passing hiway communications (deterministic) are advocated in preference to [IEEE 802.3](#) Baseband type communication (non deterministic).

Non-deterministic protocols (e.g. [IEEE 802.3](#), Ethernet, DECnet etc.) are considered acceptable for communication at the plant/management information level.

LANs are usually designed so that the ratio of propagation delay to the packet transmission time is small. As this ratio increases the efficiency of LANs using CSMA/CD, i.e. [IEEE 802.3](#) degrade, the problem manifesting itself when the ratio exceeds 20% and where at over 50% access to the network deteriorates dramatically. Arranging for CSMA/CD networks to run at high speeds with a high number of users is difficult as collisions become a major problem and throughput is seriously affected. [IEEE 802.3](#) is non-deterministic and frames are not prioritised making it ill-suited for real-time applications.

Deterministic protocols allow estimation of the worst case access time to the communication network (i.e. they are predictable, where as non deterministic protocols may be unpredictable). [IEEE 802.4](#) is deterministic and can handle short minimum frames. Token bus supports priorities and can be configured to provide a guaranteed fraction of the bandwidth to high-priority traffic. It also has a high level throughput and efficiency at high loads.

Where maximum percentage loading is kept below 30%, baseband networks behave as if they were deterministic due to the low traffic loading coupled with retransmission checking on message sends and receives. This network configuration can offer advantages over [IEEE 802.4](#) as the network may not be constrained by the token travelling time with messages being sent as capacity is available. Modified non-deterministic protocols may be acceptable where response times are not critical. Modified non-deterministic protocols usually limit the size of file that any node may transmit and utilise a re-try algorithm which changes the delay between re-tries.

The interface to PLC's and instrumentation sub-systems such as compressor antisurge equipment, should be by means of standard industry, e.g. Modbus B, Allen Bradley Data Hiway+. Likewise

standards communication links e.g. RS422 or RS485 should be used in preference to RS-232C link, as many vendors use the RS -232C standard differently.

TCP/IP is frequently used for the information connection layer (and to printers), and is becoming an industry standard connection level. TCP/IP and Ethernet interfaces are well suited to information hand off and X-Windowing into package PC's.

Several DCSs now have databases that support SQL queries (e.g. Oracle), this allows the equipment to be connected to the information network (TCP/IP) to directly query the external package databases. This has the advantage of openness and no data tables.

In the event that a proven implementation does not exist for linking the required sub-system to the DCS, the following topics are recommended to assist in determining the suitability of the proposed linkage:-

- (a) *Type of link, unidirectional, bi-directional, etc.*
- (b) *The security of data transmission. Parity checks, checksums, cyclic redundancy checks, etc.*
- (c) *The length of transmission circuits. What are the limitations?*
- (d) *What signals and pins are to be used. This can be shown later on a pin connection diagram.*
- (e) *The type of cable and connectors required.*
- (f) *Electrical isolation requirements and earthing.*
- (g) *Data loading and transmission rates*
- (h) *Maintenance, fault diagnosis and test facilities.*
- (i) *The definition of logic levels.*
- (j) *Power supply requirements and their location.*
- (k) *Handshaking and clearance of signals. Timing, i.e. who does what and when? This can be shown later on a timing diagram.*
- (l) *Protocols and the extent of protocol use. Are some protocol functions not supported?*
- (m) *Initialisation and recovery from failure.*

Interfaces to Protective Instrument Systems shall be designed to ensure that the integrity of the Protective System is not compromised by any fault in the plant control and display system.

Where Protective System defeats can be applied by software action within the DCS, (single points or groups), a hard wired key should be used as a defeat permissive. The key provides security control against accidental or deliberate operation of the DCS soft defeat. Soft defeat links should be avoided where the protective logic is classified as safety critical.

Soft defeat systems are very cost effective as compared to hard wired key defeat systems, and provide functionality to improve measurement diagnostics and log operator and system events. The security and safety implications of connecting the protection system to the DCS must be considered in detail.

Signals used as part of the protection system should not be serially communicated to the DCS for control purposes. The requirement to



segregate control and protection should be recognised and carefully considered.

Traditionally the protection system has been totally isolated from the DCS to avoid any common mode failure risk. DCS measurement diagnostic functionality provides accurate and high signal availability to challenge these traditional practices. Where dual signal usage is required, the signals can be wired to the two systems independently, (not by serial communication link, which would be a common mode failure point).

Interfaces to other connected digital devices shall be designed to ensure that the control system is fully protected from corruption and invalid commands emanating from any such connected system.

The control system should support communication with smart transmitters in analogue (4 -20 mA) and digital communication modes.

4.3.2 Maintenance and Diagnostics

The equipment should be provided with self diagnostic routines that allow continuous on-line monitoring of the software and hardware. The diagnostic functions shall run continuously and shall be capable of detecting a fault before system integrity is lost. It shall inform the operator of a failure and indicate the type of fault and the device unit or card to be replaced

It should be possible to monitor and operate back-up facilities from the operators console, i.e.:-

- (a) To initiate manual changeover from duty to standby.
- (b) To monitor correct operation of automatic change-over.
- (c) To monitor the status of both duty and standby equipment.

Where individual operating units are shutdown for overall, the hardware and power distribution, should be designed for the associated control and monitoring equipment to be isolated from the remainder of the operating equipment.

The arrangements for maintenance access to equipment should be considered, including arrangements for equipment segregation, powering and fusing of I/O circuits.

4.3.3 Control and Data Acquisition

Control and data acquisition hardware should be provided to allow the plant to operate in a secure, safe and efficient manner. Control and data acquisition functions should operate in an integrated manner such that a process signal is terminated only once regardless of the number of uses within the system.

Where I/Output cards are mounted separately from the processor, secure redundant communications should be installed for all control applications.



High speed precision time tagging may be essential to identify a sequence of events which caused a plant emergency or shutdown (e.g. for post incident analysis). Some DCSs offer integrated sequence of event modules which may be used in preference to a separate 'sequence of events' facility interfaced to the DCS. Such systems should be limited to monitoring only the most critical field inputs and outputs.

PLC systems should generally be used where there is a need for significant amounts of sequence control, batch logic or interlock logic or where there is a requirement to monitor and control a large amount of digital I/O. Some DCSs have fully integrated PLC modules removing the need to configure gateways to third party PLCs.

Control and sequence processors should be capable of communicating directly with each other digitally over the system communications network.



5. SYSTEM CONFIGURATION

5.1 Man Machine Interface

The DCS is the mechanism to view and control the process. The DCS is also the means to perform Advanced Control, Optimisation, Sequencing and Shut Down. DCSs should enhance an operators performance. Enhancement by performing the tasks that he does less well, e.g. routine and frequent monitoring, checking for bad data and then taking preconceived actions. This allows the operator to handle unexpected and unpredictable events.

The Man-Machine Interface (MMI) is a key factor in the ultimate acceptance of the DCS by operators. The MMI can adversely affect the reliability of the plant if poorly designed. The Man-Machine Interface (MMI) must therefore be carefully designed.

It is recommended that early in the detailed design a philosophy/specification document for the MMI is developed in association with operations staff and vendors specialists. Emphasis should be on operability rather than over complex or colourful graphics.

The MMI specification should detail requirements for:-

- (a) Usage and layout.
consoles and screens
- (b) System Navigation.
display hierarchy, touch screen target areas & point selection, navigation between displays
- (c) Display Philosophy.
use of colours, flashing, reverse video, intensity, display of bad values or off scan points, equipment symbols, dynamic features
- (d) Data Presentation.
descriptions, controller parameters (SP, PV, OP, mode, alarms), number format, tag numbering convention, display of equipment status, engineering units
- (e) Alarm handling and prioritisation.
- (f) Parameter selection and data entry.
- (g) Security.
access levels (view, operator, supervisor, engineer)
- (h) Display types.
overviews, specials e.g. ancillary equipment

The operator interface is the means by which the operator performs his tasks. It should be designed such that it simplifies rather than complicates the operator's task. The characteristics of a well designed operator interface are as follows:-



- (i) Consistent commands, rules, syntax and responses throughout the system
- (j) Minimum number of commands, syntax and rules which the user is required to memorise.
- (k) Minimum number of mental transformations to be performed on the data.
- (l) Data, messages and prompts presented in a directly useable form.
- (m) Minimum data entry. Ensure maximum use made of information available to the system.
- (n) Provide effectively structured dialogues and/or selection lists.
- (o) On-line aids such as help, summary displays, diagnostic aids.
- (p) Computer algorithms for pre-processing of complex data before presentation to simplify decision making.

Mental processing operations which should be avoided by good design include:-

- (q) Complex commands and syntax.
- (r) Commands, rules or syntax that are specific to a particular display, sub-system or software package.
- (s) Memorising abbreviations and codes.
- (t) Translating data into different units.

The latest BP Group experience on DCS MMI should always be sought when developing the MMI. On systems widely used by BP, existing configured display software, e.g. display symbols, trend facilities should be utilised.

5.2 Security

A security strategy for the DCS including access to controllers and control configuration must be developed at an early stage to ensure subsequent safe and reliable operation.

Means must be provided of controlling access to the various facilities in a secure manner (e.g. by key lock, badge reader or password).

The badge reader or password is preferable for individual engineers to enable an audit trail of changes to the system to be recorded.

Instant log-in of operators must be available with ideally a facility for individual identification.

A minimum of three levels of access should be provided:-

Level 1	Operator	For normal operation of the plant
Level 2	Supervisor	Access to alarm settings, point processing, tuning parameters.
Level 3	Engineer	Unrestricted access to the database.



The DCS should also be split into process areas, which are attachable by configuration to Operator stations. Changes to functions within an area are then from stations configured to it and are 'view only' from all other stations. Monitoring of process performance from remote stations should be limited to view only access.

Potential risks to DCS security arising from connections to plant computers and through them to wider area computer networks should not be overlooked.

Remote user access to a control system network should go through some form of firewall. This approach is widespread in the IT world, and can be a physical hardware device on the control network (e.g. Honeywell CM50), or it could be via a client/ server software product (e.g. @aGlance or PI). In both cases the user is not logged into the control system and has restricted access dictated by the firewall.

Many DCSs have inherent security by using a proprietary network protocol (e.g. Honeywell LCN/UCN, ABB DCN, etc.). As control system products move to standard hardware and operating systems, particularly Windows-NT, they become more vulnerable to unauthorised access ("hackers"). This is a potential drawback to "open systems", however it does not present a problem if addressed carefully.

The weak links in external security are the connections to the outside world (modems, bridges, LAN/WAN connections, etc.). All remote access over open telecommunications systems, for example modems, should only employ dial-back facilities and should have a means of intelligently recognising the client system. The simplest form of security is keyboard password protection, however it is also the easiest to overcome. A growing range of high security systems are now available, and consideration should be given to the use of these systems e.g. photographic recognition, electronic ID tags, voice recognition.

Engineer changes should have a full audit trail with individual identification against each system change.

5.3 Information Display

5.3.1 User Requirements

The DCS operator's needs are paramount in the design of the displays. The DCS operator is required to perform:-

- (a) Process monitoring and control
- (b) Diagnosis of abnormal conditions
- (c) Responses to alarm conditions
- (d) Planned changes in operation.



Achieving this functionality from a VDU based system has some inherent difficulties, due to the restrictions on information presentation on a single screen, which increases the difficulty of a rapid overview and pinpointing a problem.

Inspecting and modifying system hardware and software should all be provided by standard system displays. Systems provided to communicate additional information to the operator should be integrated into the operator displays.

5.3.2 Providing the Functionality

The functionality required of the operator station is generally met by the provision of the following classes of displays/features:-

- (a) **Overview displays for steady-state monitoring.**
The provision of overview displays, to enable the key process variables to be monitored, is an attempt to overcome the restricted process window. Experience has shown that standard vendor offerings are of limited use, and are often replaced by custom displays. Even these tailored solutions, however, are not commonly used by experienced operators
- (b) **Customised Graphic.**
In addition to operating schematics, customised graphics provide useful status, summary and information displays.
- (c) **Clear Identification of Abnormal Conditions (Alarm Displays).**
Effective alarm summary displays and the linking of process operating graphics to the alarm system is a major step in providing an effective operator plant interface.
- (d) **Help Displays for Unusual Conditions.**
A Windows-based system offers the opportunity for help information to be dynamically altered to match the plant conditions.
- (e) **Task Oriented Displays**
'Task oriented' displays offer advantages over the conventional process graphic. These displays should be structured to guide the operator through a particular task and should minimise the number of screens required to carry out the task by careful selection of the relevant data, and by the judicious use of windows or sub-pictures.
- (f) **Detail Point Displays.**
Database point configurations are accessible showing all point parameters and attributes e.g. tuning constants and alarm settings.
- (g) **Controller Face-Plate Displays.**
These provide an easy conversion route for operators familiar with panel-based instruments.. Where these are grouped in displays, they should be configured show the relationship between linked controllers, and allow quick access to parameter trending.
- (h) **Trend Displays.**
The ability to display recent history for a selection of parameters is a valuable aid to process problem diagnosis and solution. Displays for related variables showing process variable, setpoint and output both digitally and in bar graph form is also a very useful feature. The ability to trend the PV, SP and OP aids control performance monitoring.

It is recommended that the plant be controlled via custom built operating schematics. Where grouped displays are used, they should generally correspond to the operating schematics, and should be selected by targets on the operating display.

Easy access to point detail displays is needed from operating schematics to carry out point parameter modifications. A convenient method of implementing this link is to provide a detail target which is brought up when a point is selected on the display.

5.3.3 The Display Hierarchy

The display hierarchy should assist the operator to scan the process he is controlling, and to rapidly identify a process disturbance. The operator needs to be able to 'walk through' the process he is controlling and to rapidly pin point any process disturbance. The display hierarchy must reflect these needs.

The structure of the hierarchy will be dependent on the size, process complexity and the split of responsibilities between operators. The DCS database structure must also reflect the link between operator stations and plant areas. This is generally achieved by the concept of plant areas and units. A plant area is associated with a console, which limits alarm annunciation and control access to the designated area. Hence the custom graphics must follow the same structure. At any console, however, a total plant view is a desirable feature. The inter-linking of process areas needs to be considered in the display design, possibly by repeating plant data from adjacent areas.

Typically four levels are generally needed in the hierarchy for all except the simplest plants. The hierarchy should be accessible from any level. Typically the levels can be classified as follows:-

Level 1: Plant/ Site Over-View	<i>Plant over-view schematics; site-wide utility and network schematics; interface to plant-wide control systems e.g. economic optimiser.</i>
Level 2: Process Area	<i>Over-view of one plant area, that requires several unit schematics for operation. Includes the interface to multi-variable or other advanced controls that affect the whole of that plant area. Interface to F&G, ESD, control sub-systems covering that area.</i>
Level 3: Process Unit	<i>Level at which all individual measurements and PID controllers are displayed on process unit schematics. Any area may be divided into typically from three to fifteen units, (e.g. a distillation column may be divided into feed; base/ reboiler; overheads; column profile). Interfaces to small-scale advanced controls specific to that unit may be provided at this level. Trend displays are typically accessed at</i>

Level 4: Detailed Displays *this level.
Focus on a single controller, measurement,
interlock, subsystem, etc.*

An additional level of detail may be required on some items of equipment such as furnaces, complex columns, rotating machinery. Links from selected points on a process graphic to the point detail are required for point parameter updates. Operator actions will usually be carried out from unit control level, or below.

The displays need to be linked both vertically - giving more detail as one moves down the hierarchy - and horizontally, so that the operator can move through the plant at the overview or control level.

The Area Overview display consists of a process block diagram for that part of the plant showing the main units within that area with targets to the Unit Overviews. It may also include some key process parameters and alarm indications and include important parameters that are related to each unit. It is at this level that the operator would interact with plant optimisers, and set targets, however it should not be possible to control the plant directly from this level. Production rates and key plant performance indices may also be included.

The Unit Overview consists of a display showing main vessels and equipment within that unit with targets to the operating schematics. It may also display key process parameters and alarm indications.

There are three types of targets: display navigation, which brings up a different display; display further detail, normally on the same display, operator interaction with the process. Targets should be clearly identifiable, either overtly, or if covertly, the so called 'invisible' targets, they should be recognisable by some distinct feature, e.g. a vessel detail may be accessed by its equipment label forming a target which is identifiable by being displayed in reverse video

The allocation of loops within a group display should show any relationships between master and slave cascade loops. A loop may appear in more than one group display. Group displays should be configured for different operating tasks e.g. unit start-up, catalyst regeneration. It should be possible to page through group displays in parallel with task procedures. It should be possible for the operator to configure a set of group displays for temporary use.

Help displays and task oriented displays (e.g. for non-routine tasks such as plant start-up, shutdown, optimisation, etc.). are normally configured at the unit level of the hierarchy.

5.3.4 Access/Navigation

Experienced operators require fast access to the unit control displays. Inexperienced or infrequent users require a means to move through the hierarchy in a structured manner, which is clear and consistent.

The needs of the operating task must be reflected in the linking of displays, and the data selected for a given screen. The design should



address the need to minimise the number of display screens the operator must access to carry out a task, balanced against not overloading the screens with information. Screen overlays or windows can be incorporated to minimise screen switching.

Multiple methods of display call-up should be provided. Typical facilities provided are:-

- (a) Direct access from user configured keys on the keyboard.
- (b) Touch screen targets.
- (c) Manual Data Entry.
- (d) Dedicated Function Keys e.g. Alarm Summary.
- (e) Mobility Keys e.g. Prior Display, Page or Display Forward/Backward.
- (f) Smart Targets - logic behind a target makes a decision on the display to be called, e.g. the active equipment in a duty/standby configuration.

On process schematics, the feed, utility, and product labels can serve as the display targets for moving through the process. Alternatively, a section on the display can be reserved for the display targets.. When moving down through the hierarchy, targets may be provided within the graphic representations of sub-units or equipment.

To simplify navigation through the hierarchy, the level on view at any time should either be explicitly indicated, or clear from the display title or layout. A "Help" display showing the hierarchy should be provided.

Multi-page listings of information, should be associated by a page linking mechanism, (indicating page x of y).

Direct access should be provided for commonly used displays, by the use of configured function keys/buttons.

5.3.5 Custom Replacement of Standard Displays

The use of custom displays to replace standard displays is not generally recommended, as the mechanisms to provide the functionality required can often prove complex, and difficult to maintain.

Replacing vendor displays with custom displays should only be considered when the vendor displays are not fit for purpose, and a more effective interface can be provided, examples are generally restricted to Alarm Overviews, Process Area Overviews, and Trend Displays.

If custom displays are developed to replace vendor standard displays, then access to the superfluous displays should NOT be possible.

5.3.6 Data Access/Change Facilities

The process of entering a value into the system consists of three steps:-



(a) Point Selection

The selectable data on screens should be clearly identified, either explicitly e.g. by a target box, or by following a simple convention, e.g. all variables are selectable.

Selectable data entry fields should be sufficiently spaced to make "pointing" to the field an error free task. When this is not possible, for example when lists of data are presented, the fields should be laid out so that tabbing keys can be used to avoid selection mistakes.

Whilst a point is selected, it should be highlighted on the main screen.

(b) Parameter Selection

Following point selection, an overlay (e.g. Change Zone), or window should appear on the screen which displays the parameters the operator is most likely to change. Selection of the parameter to change may then be provided by targets (in the change zone), or by special function keys which are only active when a point is selected.

(c) Data Entry

The format of entered information should be consistent with the form in which it is displayed. The format of specific data types should be consistent throughout the system. For entry of numerical values the operator should be able to view the new value alongside the old value before pressing "ENTER" to complete the transaction. It is essential that no change to the process can be made by a single unconfirmed operator action.

5.3.7 The Use of Colour

The effective use of colour can enhance visual clarity, and convey information in a succinct form. It can draw attention to screen areas and serve to highlight items of significance. Poor use of colour, such as insufficient contrast between foreground and background colours, or excessive use of bright colours can actually diminish the visual clarity of displays. The key factors to the effective use of colour are:-

- (a) Use conservatively - avoid making the screen too "busy".
- (b) Use as an aid to code data or in structuring a screen.
- (c) Make use consistent with traditional expectations.



- (d) Use colour coding in a consistent manner on all screens.
- (e) Use colours with high contrast to draw operator attention.
- (f) Use bright colours on a dark background, or vice versa.

The human eye has a sensitivity to colour which is not uniform in the visible spectrum.

The apparent "brightness" of colours is shown in the following table, which may be used to aid the selection of foreground/background colour combinations, to ensure sufficient contrast.

White	10.0	
Yellow	7.6	
Cyan	7.4	
Green	7.1	
Red	4.7	(Reference - <i>The Effective Use of Color: Physiological Principles</i> , by Gerald Murch, Tektronics Inc.)
Magenta	3.7	
Blue	2.7	

A consistent design philosophy for the use of colour must be established. The preferred technique for operating schematics is to use "cool" colours for less important information and "warm" colours for items of importance. To provide sufficient contrast, black has traditionally been used as the background colour, however, Microsoft led/ compatible applications use low intensity white (grey) for a background colour. The choice of the main screen background colour will determine the colour combinations that are easy to read and work well at getting the operator's attention.

The windows environment also permits a great deal of flexibility in display design. It is possible to include photographic images or simulated 3-D representations of pipes and vessels. It is important to avoid cluttering the schematic with detail that would detract from the operator's primary task of quickly identifying and correcting disturbances to the process.

Because the Windows environment low intensity white back-ground lowers the relative contrast with other colours, (compared to the traditional DCS black back-ground), more attention has to be given to the issue of drawing the operator's attention to important abnormal data in the display. Icon use, for example allows a single object to be displayed that contains a high contrast, and in this case a black border around a red or yellow symbol gives a stronger visible impact than the same red or yellow directly against the low intensity white back-ground.

The use of warm and hot colours (e.g. yellow, red) in a high-contrast situation should be reserved for alarms and indications of abnormal conditions. The design of back-grounds and fixed information should be subdued and not conflict with the usage for alarms and abnormal conditions. Variable but normal information, (analogue values, digital states, messages), should be clearly distinguishable from fixed information, using cool colours (e.g. green, cyan) against a back-ground chosen for ease of readability.



A typical use of colour is as follows:-

Main Process Lines/ Equipment	Cyan
Subsidiary Process Lines	Cyan (low intensity)
Utilities	White (low intensity)
Process Variables: Normal	Cyan
Low priority alarm	Yellow
High priority alarm	Red
Emergency	Red
Faulty	Magenta

5.3.8 Display of Fixed Information

Displays should be headed by an informative title, which always appears in the same position and the same colour.

It is useful to display the system file name as part of the picture

Information density and the use of colour/intensity must ensure that the screen is not cluttered and important information is easily distinguishable.

The fixed (static) information should be displayed in a subdued manner, so that it does not distract from the variable data fields.

The format for labels should be consistent and equipment labels should be adjacent to or within the equipment symbol.

The engineering unit descriptors should be as concise as possible without incurring ambiguity.

Care must be taken on identical units that the unit identity is clearly visible - by the use of colour or highlighting - so that there is no danger of the operator mistakenly making changes on the wrong unit.

Process representation should be adequate for operating needs, and not be cluttered by too much P&ID detail.

Operating Schematics should normally be broken down such that they contain typically no more than thirty indicators or control points.

Standard equipment symbols should be used conforming to PFD/P&ID practice.

Duplicated equipment such as exchanger shells need not be represented. One symbol will suffice.

Measurement locations should be indicated. Controller connections should be shown by lines which are differentiated from process lines.

Displays should follow the process flow from left to right and/or top to bottom.

The use of arrows should be kept to a minimum.



Incoming feeds and outgoing products should be labeled.

Visual clarity is aided if the major process flows are distinguished from the rest by intensity or line width.

Tag names and descriptors should be easily accessible, but not permanently on display.

It should be ensured that the requirements of advanced control and optimisation are considered, and properly integrated with the plant control displays, and should be seen by the operator as a seamless extension to regulatory control.

5.3.9 Display of Variable Information

The value format for a point should be to the resolution needed by the operator and consistent wherever it is displayed.

A clear convention should be adopted for displaying values which are off scan or bad.

Colour is recommended as the means of conveying the status of the process variable.

The recommended convention is:-

Colour	Status
Cyan	Normal
Red	Emergency/ High Priority Alarm
Yellow	Low Priority Alarm
Magenta	Faulty Unavailable

5.3.9.1 Controller Display

The four variables commonly displayed for any regulatory controller are: setpoint, process variable, controller output and mode. These values may be grouped together in a controller box.

The mode of a controller may be represented by colour and/or text. Abnormal modes of operation, e.g. when a cascade control is broken, should be highlighted.

The controller output can be represented by a horizontal bar graph, colour coded to highlight if the output is saturated.

5.3.9.2 Valves with Associated Position Indications

Use a solid symbol for a closed valve and a hollow symbol for an open valve as per the P&ID convention. Colour is then used to denote normal/abnormal states, e.g. cyan for normal and red for abnormal. The colour of the abnormal state should correspond with the alarm priority colour. Magenta should be used to indicate faulty inputs, and



blinking colours to indicate valve in motion where such feedback is available.

It is important that the operator has a reminder on the display for valves which are linked to a trip output. This may be done by the choice of symbol and additionally by the use of the text 'FO' or 'FC' to indicate fail open or fail closed.

For Motor Operated Valves with remote control facilities and limit switches the display must show the valve status: open, closed, moving and any abnormal condition. During a transition, an alarm should be given if the expected position is not achieved in the given time period. Valves in transit should be displayed flashing.

Valve status can also be used to selectively highlight current pipework routing

5.3.9.3 Equipment Status

Use a hollow symbol for running and a solid symbol for stopped. Colour may then be used to denote whether this is a normal or abnormal state.

Although spared equipment need not be explicitly shown on the graphic, dynamic labels should be used to indicate which item is in use.

5.3.9.4 Control Switches

Control schemes which incorporate switches require a dynamic indication of the switch position.

5.4 Data Entry

5.4.1 Physical Devices

The data entry interface to the DCS should consist of the following :-

Keyboard

and

Screen Pointer - e.g. mouse, tracker ball, touch screen, light pen

(a) Keyboard

The Keyboard should contain the following functionality/keys:-
Standard computer QWERTY keyboard.

Programmable operator function keys, which provide easy access to frequently used operating graphics. A facility to allow



easy modification of the Function Key legends should be available, preferably electronically.

Engineering function keys - for housekeeping, configuration tasks, etc.

Standard operator function keys - these would include commonly employed operator actions such as raise/lower buttons, mode selection keys, alarm acknowledgement, etc.

Where possible the keyboard should be adjustable/tiltable and separate from the screen to allow the operator to find a comfortable working position. Additionally the keyboard should have a matt surface to avoid reflective glare.

Where possible keys should be full travel (rather than membrane) with some form of protective covering against dirt and liquids.

Combined operating and engineering keyboards should be utilised if possible. If however the number of keys specific to configuration and housekeeping are numerous two separate keyboards should be used. Easily removable covers are then required to protect the engineering keyboard whilst the operating station is in use.

Where configurable annunciator lamps (e.g. LEDs) are used in conjunction with operator function keys there should be at least two levels of alarm priority. These lamps should also be clearly visible under all normal lighting levels.

(b) Screen Pointers

The most widely favoured types of pointer device suitable for DCS are:-

- | | |
|------------------|--|
| (i) Touch Screen | Touch-screens can be slow, have coarse resolution, poor accuracy and be error-prone. They also cause fatigue in the arm if used for long periods.
They require a facility for automatic alignment. A switch to disable the screen for cleaning purposes is desirable. |
| (ii) Mouse | The mouse is a quick device, it has good resolution and is accurate. Its lack |



- | | | |
|-------|--------------|---|
| (iii) | Tracker Ball | of robustness is offset by its low price
The tracker-ball is as accurate as the mouse and has the same resolution, but it takes substantially longer for the operator to reach a specific screen location. It is more robust than the mouse. |
|-------|--------------|---|

For consistency the cursor associated with a pointer device should appear in the same initial position on displays to enable the user to quickly locate it. There is also a requirement for the cursor to be easily seen yet not obscure characters underneath. Studies indicate that users are particularly receptive to a blink frequency of around 3 Hz.

5.4.2 Functional Aspects

The method of entering information needs to be consistent, in particular:-

- (a) The format in which the operator enters information.
- (b) The same keys should be used for the same functions throughout the system.
- (c) The use of shift keys should be avoided.
- (d) Procedures (i.e. keystrokes) for carrying out similar or related operations

All operations (e.g. input, cursor movements) should provide immediate feedback to the operator. The preference is for visual (e.g. target changes colour) rather than audible feedback.

The system should be designed to minimise data entry requirements, to reduce the likelihood of error. This can be achieved by structuring dialogues effectively and by using display options, rather than having to memorise strings of commands.

The system should further minimise the possibility of operator errors through facilities for detecting (e.g. data validation) and handling them. This is achieved by communicating the error through meaningful messages, highlighting the fields in error and prompting for corrections.

Examples of data validation for error prevention include:-

The use of standard system features such as absolute setpoint and output limits.

and

Limiting the magnitude of operator entered setpoint and output changes. This feature may not be offered as standard and may require specific software to be written.



There should be a minimum of one verification step if the operator is about to execute an action from which it may be difficult to recover. Screen pointer devices should be used to move around displays, with operator actions of consequence (i.e. irreversible changes e.g. initiating a shutdown) shall require confirmation by use of an appropriate key (e.g. enter) to commit the change.

For operator transactions that do not impact on plant (e.g. screen navigation) a dedicated key that would immediately reverse the last command is advantageous.

5.5 Alarm Systems

The objective of alarm handling is to give the operator as much early warning as possible of a process problem which requires action from him. To achieve this, a DCS should offer:-

- (a) clear and unambiguous information as soon as possible
- (b) a fast route to the corrective actions required
- (c) the least possible opportunity for mistakes.

For every plant an overall alarm strategy should be defined at an early stage of design in full consultation with plant operations personnel. This should be maintained, and adhered to throughout the life of the plant.

A clear policy of alarm presentation is required. This should consider how alarms and information from other systems such as Shutdown, machinery monitoring and laboratory relate to the operators tasks and how they will be presented.

To control the number of alarms defined on the P&I Diagrams the purpose and priority of each alarm should be recorded, in an Alarm Response Manual.

The alarm handling process can be classified into a number of distinct and separate functional areas:

- (d) Alarm Definition.
- (e) Alarm Detection Mechanisms.
- (f) Alarm Prioritisation.
- (g) Association of Alarms with Plant Areas or Process Units.
- (h) Audible Warning, the first indication of a problem.
- (i) Alarm Identification or situation assessment.
- (j) Corrective Action: minimising the consequences and restoring normal operation.
- (k) Alarm and Event History Reporting.
- (l) Alarm System Management and Engineering Utilities.
- (m) Point Processing.
- (n) Alarm Reduction Mechanisms.



5.5.1 Alarm Definition

An alarm is a warning to the operator that immediate action from him is required.

If an alarm exists on the system for which no immediate operator action is appropriate, it should not be an alarm. Its presence on the system distracts the operator from his main task in an upset; the presence of many such alarms is a potential safety hazard because important alarms may thus be hidden from the operator.

An alarm is to be distinguished from other plant status indications, discrete value information, sequence messages, and batch reports. Whilst the operator must have ready access to such information through his displays, he generally does not require to take any immediate action, and thus does not require it to be drawn to his attention through the alarm mechanism.

5.5.1.1 Operating Instructions

During a process upset, the DCS Operator's task is primarily one of responding to alarms. The Operating Instructions must be compiled in close association with the alarm definition to ensure that for each alarm there is a clear corrective action. Where no clear action can be identified, there should not be an alarm.

5.5.1.2 Process Design Considerations

Process design, Safety and Operability Studies, AMHAZ, and post disturbance enquiries should consider:-

- (a) Total quantity of alarms which may occur following a given disturbance.
- (b) Rate at which the new alarms can occur.
- (c) Time taken to perform the corrective actions required following each alarm.

This will clearly identify whether the demands being placed on the operator are realistic.

Where an alarm reduction mechanism is included in the system, an AMHAZ study should be performed.

5.5.1.3 Alarm Response Manual

Each plant should possess a properly maintained Alarm Response Manual containing a list of alarm definitions, including:-

- (a) Tag number and duty description.

(e.g. vessel, location, sensor type)



- (b) Type,
(e.g. deviation, rate of change, high absolute)
- (c) DCS configuration parameters.
(e.g. threshold, deadband, priority, process unit, message text)
- (d) Justification.
(why it is there, reference to safety studies, incident reports etc.)
- (e) Required operator response to alarm.

Management should ensure that process design and HAZOP engineers have sufficient understanding of the capabilities and limitations of DCS alarm handling to make appropriate design decisions. The ARM should embellish the need to reduce the number of alarms to those needed to inform the operator to them take action to avert an upset condition.

5.5.2 Alarm Detection

The objective of alarm detection should be to give as much early warning as possible that there is a problem whilst minimising unnecessary or nuisance alarms. To achieve this the most appropriate alarm detection mechanism should be chosen for each parameter.

The following detection mechanisms should be used as and where appropriate:-

Absolute	Absolute alarms should be used only where there is an absolute value of a parameter which must be avoided e.g.:- Safety valve setting, Trip threshold, Tank or vessel over-flow, Low vessel level on pump suction. Their unrestricted use in other places can give rise to an unnecessary quantity of nuisance alarms.
Deviation	Deviation alarms are useful for parameters which are directly associated with a control loop, especially cascade slaves.
Rate-of-Change	Rate-of-change alarms are useful for parameters which have a wide range of “normal” values but which do not normally move very rapidly.
Statistical	Where the DCS is running a statistical process control package, a variety of statistical alarms are available which are noted for their ability to give early warning of real problems whilst minimising nuisance alarms.

Recipe Driven	Recipe driven alarms are useful for multi-product processes, or for processes with multiple operating modes. Most DCSs have some sort of recipe facility for sequential control and batch processes these can generally be adapted to modify alarm parameters according to logical combinations of plant data. The recipe should permit all alarm parameters to be changed in response to a change in the operating mode of the unit, including:- - Thresholds, - Priorities, - Dead-bands, - Trigger and reset delay times. The recipe or other standard features can be used as a means of alarm suppression on units which are shut-down or undergoing regeneration.
---------------	--

5.5.3 Alarm Prioritisation

The objective of alarm prioritisation is to define the order in which an operator should take corrective action when a number of alarms are present. The priority of an alarm thus defines the degree of urgency associated with it, and typically is dependent on a number of factors, including:-

- (a) The severity of the consequences, (in safety, environmental and economic terms), of failing to take the corrective action associated with the alarm.
- (b) The time available and required for the corrective action to be performed and to have its desired effect.
- (c) The state of the rest of the plant, and in particular, what other alarms are active.

None of these factors are fixed, and they can vary in subtle and complex ways with the state of the plant. Therefore determining the correct alarm prioritisation requires a great deal of thought and effort at the process design stage.

Every plant should have a clearly defined strategy on alarm prioritisation so that later additions or modifications retain consistency. The objective is to reduce, as far as possible, the burden on the operator in deciding which high priority alarms he must attend to first in the early stages of a process disturbance.

An alarm which annunciates that equipment has tripped should always be given a lower priority than the pre-alarm which warns that the trip is imminent but can be avoided with corrective action.



If insufficient time exists for corrective action between pre-alarm and trip, the need and design of the pre-alarm should be reconsidered.

The following prioritisation guidelines are suggested.

Alarm Priority	Method of Assigning
Emergency	Immediate operator action required to resolve an imminent loss/plant shutdown condition
High	Rapid operator action required to resolve a probable loss condition
Low	Prompt operator action required to resolve a possible loss condition - Default Setting
Journal	Condition Historised - for record purposes
No Action	Alarm not required

5.5.4 Association of Alarms with Plant Areas or Process Units

Each alarm should be associated with the process unit where the operator must take action when the alarm occurs.

In some cases, especially utilities, a disturbance may have repercussions in several areas, so an alarm must be associated with several process units.

In many DCSs this may mean replicating the alarm detection algorithm. The alarms may have different consequences and requires different corrective actions on each unit, it may therefore require different thresholds and priorities on each unit.

5.5.5 Audible Warning

The audible warning should convey as much information as possible about the nature of the alarm, its priority and the plant area affected.

Discrimination of Priority Low volume sounds with a slow pulsation frequency should be used for low priority alarms and higher volume sounds with a rapid pulsation frequency to denote higher priorities.

In some circumstances it may be appropriate to only visually and not audibly alarm low priority alarms.

Discrimination of Plant, Area or Unit Consideration should be given to distinguishing plant areas by using sounds with clearly distinguishable characteristics.

It is not advisable to use different pitches; few people have perfect pitch and in isolation they can be misinterpreted.



Tones of the same fundamental pitch, can have quite different characteristics which are easily discriminated both together and in isolation.

Operators can rapidly learn to identify the particular sound which represents his area of responsibility, and to ignore others.

Achieving Audible Discrimination	Most current DCSs provide a set of relay contacts, which can be programmed to respond to different alarm priorities. By connecting these to sounders provided with interrupter circuits of different pulsation frequency, the bleep frequency can be made to vary according to the priority.
--	--

Sounders can be purchased with different tone qualities to distinguish different plants or plant areas. Alternatively, by mounting the sounders on bases with different resonant characteristics, clearly distinguishable noises can be produced.

5.5.6 Alarm Identification and Situation Assessment

The way in which alarms are presented is of utmost importance in determining how effectively the operator can take the appropriate corrective action in a process upset.

When more than one alarm is present, the system should allow the operator to identify quickly and easily which alarm he must respond to first. It should also allow him to assess the situation on the plant as a whole since this may affect his actions.

Human factors research clearly indicates that the best means to assess a multiple alarm situation is through a pattern recognition display system;

(a) Pattern Recognition Based on Rectangular Grid

Traditional annunciator panels are often cited as the reference against which DCS alarm handling should be judged. Some DCSs provide a basically similar grid-array of alarms. On other systems, it is possible to use the graphics to configure one. The limitation of the rectangular grid is that it contains no process data, and so other displays must be consulted to allow the operator to assess the situation on the whole plant and make appropriate decisions on the corrective actions.

(b) Pattern Recognition Based on Plant Over-view Schematic

An alternative to the rectangular grid is to use differently shaped icons or symbols to represent the different units of a process. These can be linked forming a schematic overview of the process also containing the values of



key plant parameters. The icons can be configured to change colour and blink to represent the status, acknowledgement, priority and location of the active alarms. Where appropriate the sequence of occurrence may also be indicated. This helps the operator assess the situation by giving him a large amount of information which can be rapidly assimilated.

5.5.7 Corrective Action

When a new alarm occurs, having identified the alarm and assessed the situation on the plant, the operator must be able to access the relevant schematic display and perform the appropriate corrective action quickly.

There should also be an easily accessible reminder of the action appropriate to that particular alarm. This is particularly important for events which occur infrequently, and for inexperienced operators.

There should be a mechanism to remind the operator of which alarms are still waiting for attention. When several alarms are present, it may be difficult to identify which have already been dealt with and which are still awaiting attention. This is especially important at a shift change, but may also be important in a complex upset situation or when two or more operators are involved in the corrective action process.

5.5.7.1 Display Considerations

Alarms of all types should blink when triggered, and remain blinking until acknowledged by the operator, then remain steady until the parameter returns to normal.

The use of colour for alarm states must be consistent across the plant, and should conform to common expectations. Colour may be used to denote priority, and types of alarm, (e.g. reserving magenta for instrument or system faults). Alarm colours should be chosen to be readily distinguishable from the remainder of the schematic display.

Systems which allow varying blink frequency may use this to denote priority, a fast blink indicating a high priority.

Parameters in alarm should be denoted by changing the displayed value (back-ground or both) to a brighter (hotter) colour. Where appropriate, a single character to distinguish the type of alarm, (High, Low, Deviation, Rate, Fault), can be displayed.

Alarms associated with parameters which are not available as analogue values in the DCS should be displayed either by brief and unambiguous identifying text or by an icon or symbol. These are normally invisible and become visible when the alarm is present, or they may change shape or colour or both, a key or touch-target should be provided to make invisible items temporarily visible for diagnostic and system management purposes.

5.5.7.2 Annunciator Buttons and Display Navigation

Once the operator is aware of, and assessed the upset plant condition, the display where corrective action is taken should be accessible as quickly as possible.

Some systems have an “associated display” parameter linked to each alarm. A single operator action (pressing the “associated display” button) will call the display where the operator actions relating to that alarm can be performed.

Most DCSs provide annunciator buttons with LED's which can be configured to respond to alarms, and which call the appropriate schematic display when pressed. There are rarely enough of these buttons to satisfy the requirements of larger plants, so some further display navigation is required. The system should be configured to make this as direct and efficient as possible.

Corrective action across a number of displays can be inefficient. Appropriate task-specific displays should be considered which can expedite corrective action.

5.5.7.3 Alarm Acknowledgement

Ideally the operator should only be able to acknowledge an alarm from the display on which he must take the associated corrective action.

The current practice on alarm acknowledgement is for the operator to acknowledge the alarm as soon as he has identified it. It is preferable to use the alarm acknowledge status as a reminder of which alarms have been dealt with and which still require attention. Therefore operators should be trained to leave each alarm unacknowledged until the associated corrective action has been performed.

Most DCSs can display a list of unacknowledged alarms as a check on what actions are outstanding after an upset.

It is important that operators know the differentiation between the Alarm Acknowledge function and the Horn Silence function.

Some DCSs provide alarm acceptance mechanisms which cause all of the active alarms on a schematic or in a process area to be acknowledged at a single key-stroke; the use of this mechanism should be avoided if possible.

5.5.7.4 Links to Operating Procedures

It is possible to use some current DCSs to display a reminder of the corrective action procedure. Some DCSs provide functionality for ‘Help’ or ‘Associated’ displays which can be customised for this purpose, others allow hidden text to be displayed on schematics in response to logical conditions. These facilities should be used when available.

5.5.7.5 First-Up Indication

For some operations it is desirable for the operator to know in what order a series of associated alarms occurred. Whilst the current alarm summary provides this information, it is not accessible at a glance, since the alarms associated with the group of interest may be scattered amongst a number of others, and the mechanism depends on reading and interpreting text. An extra flag or highlight on the schematic display against the oldest unacknowledged alarm would satisfy this requirement.



5.5.7.6 System Alarms

Every DCS has a number of alarms associated with its own internal self-checking. These also require operator actions which may vary from putting control valves onto by-pass, to telephoning for call-out assistance or even shutting the whole plant down.

Virtually all DCS Manufacturers provide an entirely separate and different mechanism for handling system alarms, and do not provide facilities for incorporating the alarm states into schematics or linking to operating instructions. This can lead to confusion and incorrect operator response.

Until DCSs provide more flexibility in this area, the systems must be supported by clear operator guide-lines and effective training.

5.5.8 Alarm and Event History Reporting

DCS alarm and discrete event history is held in a database from which enquiries can be made and reports generated. Process and System Engineers will make use of this data for post-event analysis, alarm utilisation audits, operator response monitoring and process trouble-shooting. It is advantageous to export the raw data to other systems (PCs) to provide adequate analysis.

For operator use, a number of pre-defined report structures should be available which are readily accessible from a DCS screen menu. Most DCSs provide this as a standard facility, others have an applications programming capability which can be used to provide this.

5.5.9 Alarm System Management

The objectives of DCS alarm management are:-

- (a) Safe and efficient operation of the plant.
- (b) Rapid recovery from upsets.
- (c) Facilitate the operator's task at all times.

There must be procedures and facilities for:-

- (d) Change recording.
- (e) Auditing.
- (f) Alarm database management.
- (g) Monitoring and Reporting, e.g. suppressed or inhibited alarms.



5.5.10 Point Processing/ Alarm Conditioning

5.5.10.1 Process Variable Filtering

Analogue input processing points should have the facility to filter the incoming field signal. By generic type some field signals are more prone to noise than others. This noise if not dealt with can provide an operator nuisance alarm problem in addition to providing a burden on further system processing including:-

- (a) communications overloading which degrades system performance.
- (b) quicker data loss on system logs and/or history files
- (c) inferior performance of calculated data which uses the noisy data

A certain degree of filtering is therefore considered prudent. For controllers the degree of filtering should be individually set during loop tuning. For non controller points the filtering is recommended according to the following list:-

Point Type	Filter Constant
Flow	0.04 mins
Level	0.04 mins
Pressure	0.02 mins
Temperature	0.00 mins

5.5.10.2 Analogue Point Alarm Deadbands/ Digital Point Alarm Delay Time

Alarm Deadbands are recommended for use in reducing the degree of unnecessary dynamic cycling of alarms on analogue points. Dynamic alarm cycling will be reduced with the prudent selection of signal filtering and the selection of alarm thresholds. There is still scope for the alarm information presented to the operator to be improved by the application of alarm deadbands. Alarm deadbands should be set according to the expected dynamics and criticality of the process application. The table below provides general guidance and recommendations for default deadband settings.

Point Type	Deadband
Flow	5%
Level	5%
Pressure	2%
Temperature	1%



The minimum duration for which a Digital point is in alarm can normally be set in order to prevent oscillating contacts from inundating the operator with an alarm. The digital alarm delay time should be set according to the expected dynamics of the process application. The table below provides general guidance and recommendations for default delay time settings. Critical applications, or applications presenting specific problems will require individual consideration.

Point Type	Delay Time
Flow	15 secs
Level	60 secs
Pressure	15 secs
Temperature	60 secs
Others	05 secs

Critical applications, or applications presenting specific problems will require individual consideration.

Points which reside in DCS modules without normal full functionality may be confined with a fixed deadband/ delay-time. This may be the case for devices which obtain signals relayed from another high level device, e.g. a third party PLC. When such devices are used, it is recommended that the non DCS device is configured to suitably condition the signals sent to the DCS. Signal conditioning should comprise signal filtering, or the separate transfer of an alarm signal.

5.5.10.3 Bad Process Variable Handling

Bad Process Variables, as determined by a transmitted signal going out of range, can generally be alarmed to indicate that an instrument requires corrective maintenance.

It is recommended that only controllers and critical values used in calculations for advanced control algorithms should be actively alarmed for this condition. All other points should report the Bad PV condition to the system journals. The DCS Support Engineer should regularly interrogate the system journals for Bad PV alarms.

5.5.10.4 Extended Ranges

The use of extended ranges on Analogue Input signals minimises the frequency of Bad PV alarms by providing a tolerance against:-

- (a) field conditions transgressing slightly beyond instrument calibration.
- (b) signals which are slightly out of calibration.

The Extended Range values used need to be chosen in order to assist the operator whilst not disguising the need for calibration maintenance of a signal.

Initial settings for the Extended Range parameter are recommended to be globally set to a default value of 10% of Range. This default value can then be modified should this figure prove unsuitable for a particular application.

5.5.10.5 PV Clamping

Bad PVs can be removed from points which are not appropriate for extended PV ranges by application of a PV clamping option. Caution should be exercised in the application of PV clamping if misinterpretation can result from a clamped value. Applications of merit can be in the background processing of points associated with some advanced control applications which would otherwise experience discontinuity of control if Bad PVs were encountered.

5.5.10.6 Background Processing Points

Various points on the DCS are intended to be processed "invisible" to the operator. Such signals include feed forward and analyser dead time calculations for advanced control loops. There is no requirement to annunciate alarms on such calculation points, as the operator is not expected to take action specifically on these points.

5.5.10.7 Equipment Status

The position of on/off valves, or the run status of pumps are often set by the operator. The operator should not therefore require an alarm to indicate the status of such equipment. The operator is informed of equipment status by means of the status condition point in the DCS driving colour coded mimics on the graphics.

Operator control points for valves and pumps should therefore be configured to alarm a disagreement of its current status against its commanded state.

5.5.11 Alarm Reduction Mechanisms

Some useful alarm reduction mechanisms do exist on many current DCSs:-

Alarm suppression or alarm cut-out can be used to reduce the problems of:-

- (a) *Alarm flood following a trip.*
- (b) *Standing alarms.*
- (c) *Nuisance alarms.*
- (d) *The mechanism for suppression or 'cut-out' may take one of several forms, depending on the possibilities and limitations of the DCS:-*
 - (i) *Inhibit alarm detection, possibly by taking the alarm detection algorithm off scan.*
 - (ii) *Automatic alarm acknowledgement.*
 - (iii) *Alarm priority reduced, perhaps to 'journal only'.*



- (iv) Alarm detection thresholds altered to reflect the state of the plant, possibly by using an Automatic recipe system.

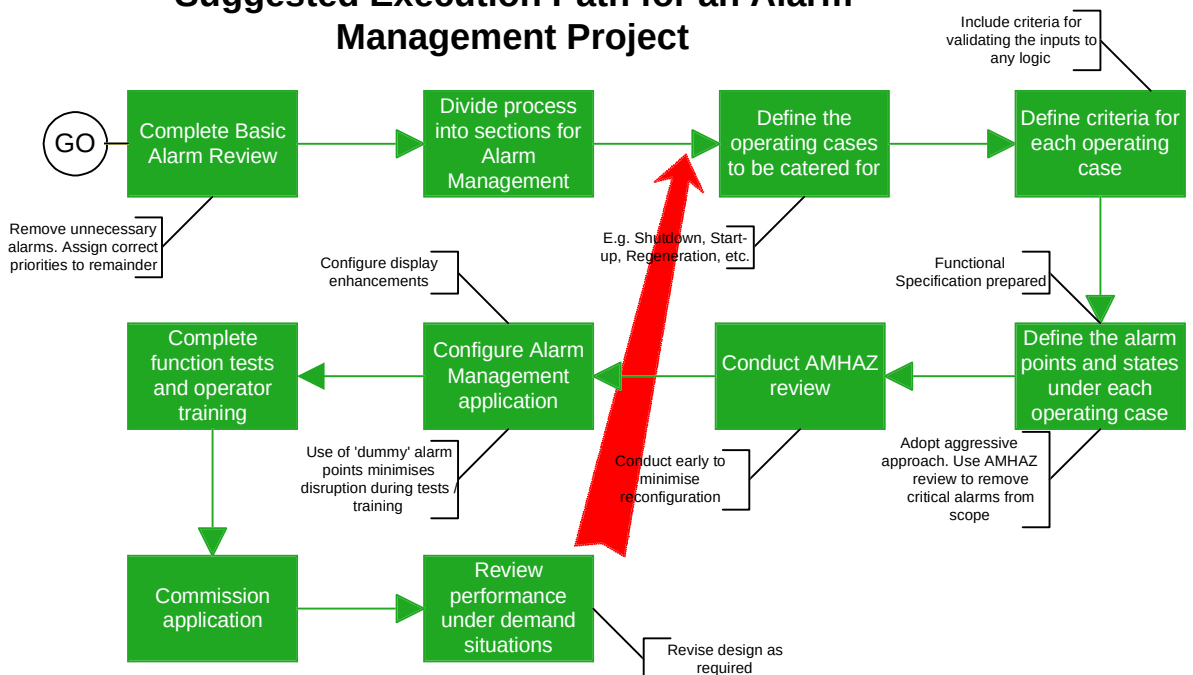
5.5.11.1 Alarm Handling Packages (AHPs)

It is vital to prevent/ minimise alarm floods on the DCS. Alarm floods result in important alarms being missed amongst the mass of inconsequential alarm information during a process upset.

Alarm Handling Packages (AHPs) to prevent alarm floods should work by disabling alarm annunciation (audible/ visual on alarm summary displays under certain prescribed operating conditions. The alarms will still be visible to the control operator on the process graphics and will be recorded on the system journal. The operating conditions are identified automatically (can be selected manually) by the software according to a set of criteria based on measured operating parameters. The alarms selected to be disabled should be those which are of no consequence to the situation being dealt with at the time, e.g. during unit feed stoppage there will be no value in identifying that a product rundown flow is low.

Process alarms are an inherent element in ensuring safe plant operation. Therefore an AHP which will disable alarms should be examined to ensure that no unnecessary hazards to continuing safe operation are introduced by disabling the alarms.

Suggested Execution Path for an Alarm Management Project



5.5.11.2 Alarm Management Hazard Assessment (AMHAZ) Study Methodology

Dynamically altering an alarm priority can, on some systems, have unexpected and unwanted interactions with alarm display and reporting mechanisms, since these may not be handled separately.

AMHAZ is a methodology to identify, and provide recommendations to prevent potential hazards created by disabling alarms in an AHP. AMHAZ provides the end-user with assurance that the AHP can be safely put into service.

The AMHAZ process considers the operator function to best resolve a process upset condition. The dynamics of the process upset and the operator need to be considered, i.e. likely cascading of process upsets, rate of new/ repeated alarms, and the time to achieve corrective action (if any).

The AMHAZ study methodology assesses the safety and operability implications of disabling process alarms under certain prescribed operating conditions. AMHAZ is a rigorous assessment tool, but it does not replace other safety and operability studies/reviews, e.g.. HAZOP, PHSER, CONSOP, which should also be performed. AMHAZ complements other studies by very specifically addressing the impact of the application of alarm management which would not be addressed by any of the other studies or reviews. Abridged details are given in Appendix D, with full details available in report [No. 1996-225211](#).

5.6 Trending and History Configuration

5.6.1 Historical Data to Collect

The following data should be included in the continuous history:-

- (a) all analogue measurements.
- (b) all calculated or dynamically modified parameters used as controller measurements.
- (c) all controller outputs.
- (d) all cascade slave or other dynamically calculated controller set-points.
- (e) other controller parameters subject to continuous change, e.g. adaptive gains, calculated or dynamically compensated feed-forward parameters.
- (f) analogue values communicated from instrument subsystems, PLCs, ESD, F&G, etc.



The following data may either be included in the continuous history or logged and time-stamped in an event-log:-

- (g) all operator analogue actions: controller set-point adjustments, manual modulating valve movements, sequence control analogue settings, (e.g. ramp-rates, targets).

The following data should be logged and time-stamped in an event-log:-

- (h) all discrete operator actions: controller mode changes, discrete valve movements, motor start or stop, sequence control initiation, option selection or interruption.
- (i) discrete control output actions from sequence controls.
- (j) all alarms.
- (k) ESD, F&G and other subsystem actions.

It is preferable that the following data should also be logged and time-stamped in an event-log:-

- (l) all DCS configuration changes, especially alarm settings.

An important use of the history system is for post-event diagnostics. It is impossible to know in advance what parameters will be required in post-event analysis, so it is strongly advised to collect all available data, noting that data storage media are very cheap compared with the cost of an incorrectly analysed process incident.

5.6.2 Time and Magnitude Resolution of Historical Data

The following should be considered:-

- (a) Ideally, all plant data should be recorded on the finest possible magnitude resolution and for the longest available period.
- (b) The typical time resolution used for most data is 1 minute. Some fast moving parameters may require a faster collection interval to prevent aliasing.

Network loading may be a constraint on time resolution.

- (c) The data collected should be saved for a minimum of five days before archiving.

To allow for post-event analysis after a long public holiday, (e.g. Easter)

Complex data compression was once in vogue to save disk space at the expense of retrieval speed and resolution; multi-gigabyte disks are now cheaply available that this is unnecessary; (e.g. 1 gigabyte holds 6 byte analogue values for 23,000 tags at one minute resolution for five days without any data compression).



5.6.3 Archiving

The following should be provided:-

- (a) Data history archiving should be to optical disk or other high resolution storable media, and should be performed automatically, (e.g. as a scheduled back-ground activity), except for media replacement.
- (b) Archive data retrieval should use the same trend and reporting facilities as the on-line history.
- (c) A mechanism for off-line data retrieval, (e.g. via a PC), should be provided.

5.6.4 Trends

5.6.4.1 There are three main uses of the trend facility:-

- (a) Predictive monitoring of the plant. The critical factors here are:-
 - (i) real-time updating and scrolling.
 - (ii) fine resolution of the magnitude of the process parameter.
 - (iii) the ability to scale the individual traces separately on a multiple trend.
 - (iv) the ability to retrieve a trend previously defined by the operator without having to redefine parameter selection, time-base or scaling.

Here the trend is used to monitor conditions whilst vessels are being filled or emptied, units being brought up to temperature or pressure, batch processes nearing a point requiring operator intervention, reaction or separation processes nearing specification as they are brought on stream. The operator watches a number of key parameters relating to the process, (typically up to eight), so that he can correctly anticipate and time his next action.

- (b) Post-event analysis of disturbances. The important considerations here are:-
 - (i) fine time resolution, (to distinguish cause from effect).
 - (ii) facilities for zoom and pan in the time dimension.
 - (iii) the ability to bring a succession of different parameters onto the same trend graph quickly and easily.
 - (iv) It is also desirable to be able to identify discrete events and operator actions on trends.



When an unexpected event has occurred, trends are used to identify the original cause and to trace the propagation of the event. The operator typically trends the parameter which he first noticed as having a problem, and brings onto the same graph the possible causative parameters. Having found an immediate cause, he may well seek further initiating or predisposing events by a similar process.

- (c) Loop tuning. This may be achieved by a custom graphic, however a standard graphic is preferable, and the important features to include are:-
 - (i) Ability to load all necessary parameters (MV, SP, OP) by entering the loop tag name.
 - (ii) the ability to leave the page and return to it without repeating the definition or losing data, so as to be able to tune very slow loops.
 - (iii) fine time resolution so as to be able to tune the fastest loops.
 - (iv) real-time updating.
 - (v) fast configuration: a single tag-name definition generates trends for set-point, measurement and output.
 - (vi) Ability to change tuning parameters, (gain, integral action time, derivative action time-constant, filter time-constant), as well as set-point, output and controller mode, from the same page.

Typically, it is necessary to trend the set-point, measurement and output, together with parameters which are known to disturb or influence the loop, (e.g. feed-forward value, cascade controller measured value).

5.6.4.2 In all cases, the following apply:-

- (a) The trends should distinguish parameters by line-colour.
- (b) The display should show, for each parameter: the tag-name, description, measured value, units, upper and lower trend-display limits.
- (c) The upper and lower trend display limit for each parameter should be capable of individual definition and on-screen modification.
- (d) It should be possible to zoom and pan along the time axis, or to specify start and end times.
- (e) The time axis should indicate the exact time and date represented by each grid-line.
- (f) A “hair-line cursor” facility should allow the numerical read-out of the trended values at the time specified by the cursor position.



- (g) Where the trend end-time is “now”, the trend display should update in real-time, no matter what the time-span is.
- (h) Real-time updating trends may update the trended parameters at the display time-resolution, no matter what the history collection interval.

5.6.5 SQL Reports

Interrogative access to history data should be possible:-

- (a) On-line SQL-type search and reporting of data from both the continuous and event histories, (with appropriate merging of the results)
- (b) It should be possible to display the SQL reports on a system screen or to print them on the standard system printers
- (c) It also should be possible to transfer the SQL report to spreadsheets or other software packages in PCs or other network-linked machines

5.7 Controller Configuration Guidelines

All process inputs should be checked for measurement range validity. An out of range condition should generate an operator workstation message, and on controllers the loop mode should change to manual. For low level temperature inputs the equivalent of up-scale (down-scale) burnout protection should be provided. Where an out of range condition exists the system should allow configuration of whether the point continues to process on last good value or not. Process outputs should be checked for 4-20 mA range validity.

All control loops should be arranged to fail safe, e.g. by shedding master or supervisory loops onto basic regulatory control and holding current set point or valve position. Controller algorithms should always reside at the lowest practicable level of the control system hierarchy.

Control output to valves should be configured on all operator displays as:-

0% Output	=	Valve Closed
100% Output	=	Valve Open

Loop initialisation with measured value tracking should be provided for multi-loop control schemes to ensure bumpless switching between control modes.

It should never be necessary for the operator to perform a manual initialisation or controller balancing process.



Multi-loop control schemes should be configured within a single control processor wherever possible thus ensuring inter processor communications are minimised.

Control loops typically have a 1 second controller cycle time. Where significantly faster processing is required, (e.g. compressor anti-surge control), DCSs are generally too slow and separate dedicated controllers should be used interfaced to the DCS via serial links for remote monitoring.

Controllers which connect directly to valves in the field should not in general be configured to restore the controller mode following power failure or controller failure, i.e. loops should (in general) restart in manual.

Some specific loops may need individual consideration, this should be achieved through safety and operability studies (e.g. CONSOP).

On failure of a non-redundant controller or a controller and its back-up, the action of the output should be to fail fixed at its last good value, or to the power failure mode.

The failure mode would normally be specified as frozen at the last good value unless there is an overriding process reason to do otherwise.

Following complete power failure, outputs should be restored at 0 %.

The settings for bad measured value detection should be defined, e.g.:-

- 3 %	=	Low Bad Value
+ 103 %	=	High Bad Value

Vendor's standard control algorithms and functions should be used where possible in preference to user defined and programmed algorithms.

Similar control schemes that are used in several locations on a plant should be configured in the same manner e.g. algorithm usage, display and initialisation.

Advanced control and applications running in higher level computers, e.g. VAX, should not directly manipulate valve outputs. They should reset DCS controller setpoints.

Supervisory Control is the term used where controllers are manipulated through set point changes. Supervisory Control should be used in preference to Direct Digital Control, (where the control valve position is manipulated). This ensures that basic level control functions are maintained should the communication or control links fail. Likewise, Supervisory computer outputs to DCS controllers should be subject to validity checks at the DCS for security of plant control.



Max/min and rate of change limits should be configured on base controllers used in advanced control, optimisation and higher level application programs to ensure that software faults in these programs do not drive the base controller to an unsafe state.

Advanced control schemes should be easy to use and the operator should have a quick and convenient method of turning them on and off. Operators and plant managers should be trained in the objectives and use of the advanced control schemes.

Consideration should be given to the provision of special operator help displays to assist the operator in all but the simplest schemes.

Configuration details should be checked for appropriate and consistent application by means of the CONSOP process.

5.8 Batch and Sequence Control

In addition to the recommended practices for all DCS requirements, batch and sequence control presents some extra considerations. The main features of batch and sequential controls are their time dependency and the use of alternative routing or equipment. Operator action is more frequently in the form of an interactive dialogue and therefore clear understanding, consistent responses and confirmation feedback are very important.

5.8.1 Operating Philosophy

A form of operational or task analysis is required to identify the essential order of interactions, (review of the display format is insufficient), for example analysis is required to:-

- (a) Determine what information is required in the selection or initiation of sequence controls.
- (b) Co-ordinate actions by outside operators such as starting machinery or resetting trip devices.
- (c) Ensure that safety interlocks are not required to be defeated in normal operation.

The analysis should also determine:-

- (d) The diagnostic information on faults in equipment or sequence operation needed by the operator.
- (e) Stable hold conditions such that sequences can be temporarily stopped.
- (f) Means to restart, proceed manually or abandon the current step.
- (g) The effects of an emergency or general plant shutdown on any active sequence.



5.8.2 Summary of Displays

The display hierarchy is generally flatter and navigation between the different types is greater than with continuous plant operations. In addition to the customary displays the operator requires:-

(a) Sequence Summary Display

A summary of all sequences and their status, unacknowledged alarms or messages.

(b) Individual Sequence or Batch Overview

Detailing the process, the current stage of the sequence, the main equipment selected, key parameter current and target values, elapsed time, alarms, messages active interlocks.

(c) Sequence or Batch Set Up Displays

Simple sequences, routing or transfers can be set up from a Unit display, using menu or dedicated key selection.

More complex sequences should be set up from a custom display. Menu's can be used to enter pre-set recipes or routings. Additional automatic checks of manually entered data are recommended, (e.g. equipment availability, validity of line routing etc.)

(d) Control Detail Displays

Items of equipment in an inaccessible state, due to an overriding sequence, interlock or external trip should be highlighted on the display. Status data should still be available.

(e) Message and Interlock Summaries

Sequence and batch programs should generate messages to:-

- (i) Initiate operator action.
- (ii) Confirm status of equipment not monitored by the DCS.
- (iii) Advise why operator actions have been inhibited (interlocked).

No operator action should be inhibited without explanation



5.8.3 Recipe/ Route Selection

Pre-set recipes and routings should be held in tabular format for ease of selection. Options to modify individual components should be provided. Authorisation to make changes may be required and all changes must be recorded.

5.8.4 Alarms and Interlocks

Batch operation may be affected by the interaction between sequences and fixed interlocks. The operator should be able to easily distinguish between external 'trips', sequence interlocks and other 'holds' by means of effective alarm displays and messages.

External alarms, from shutdown and safety interlocks, should be displayed on the graphics as for continuous plant. Sequence interlocks should be shown as a status flag and annunciated, as a message, only when activated; that is when an automatic control or operator action is prevented.

5.8.5 Message Handling

Messages are issued to inform the operator of an expected event. They will normally, but not necessarily, require a response or action from the operator. They are displayed and annunciated on either a custom overview or the sequence summary listing. Messages should appear directly and in full on a sequence control graphic.

Simplicity and consistency are essential, for example, held, paused, stopped, aborted, waiting, off, are all similar but have different meanings in the context of sequence operation.

Progress through a sequence can be monitored by archiving messages as they are displayed to the operator. In simple cases custom operator displays showing the details of the current sequence step can be provided using flowchart concepts or a high level 'pseudo' code.

5.8.6 Navigation

Effective navigation is vital. In addition to plant overviews and alarm summaries batch applications can include high level sequence overviews and message summaries. This is compounded when the use of alternative routing means there is no fixed relationship between sequences and equipment.

The use of proprietary batch or sequence software may provide all the necessary facilities. The alternate is to balance the simplicity of operator navigation against the complexity of software. When practicable dynamic linking should be used to move directly from the alarm acknowledgement to the control display.



Sequential control schemes typically have a number of distinct steps of which only a small number is active at any one time. Progress to the next step may be dependent on elapsed time or on certain process conditions being satisfied. There may be selection steps, where the next step may be one of several, depending on the states or values of some parameters. Some steps may require operator actions, in which case an advisory message is generated.

The detailed advanced sequencing display typically contains the following features:-

- (a) A schematic diagram, (flow-chart), of the principal steps including the selection steps and operator intervention points.
- (b) The currently active steps are highlighted, and the actions being taken by the step are indicated.
- (c) The target and measurement for the condition that moves the scheme to the next step are displayed.
- (d) If operator intervention is required, data entry points for the relevant actions are included together with help text to prompt the correct action.
- (e) A recent history is provided giving the values of previously manipulated parameters, elapsed times for previous steps, selection parameter values and other relevant information. A scrollable window is preferable for this feature since the entire history can then be interrogated.
- (f) A trend may be included of key measurements associated with the scheme.
- (g) “Start/abort” and “pause/continue” targets or buttons should be provided where appropriate.

5.9

Advanced Control/ Optimisation

Advanced Control can deliver substantial pay-back to raise profitability. Operator acceptance is crucial to ensure continual good utilisation of schemes. It is therefore vital to have a well designed interface for the operation of advanced control and optimisation systems.

Advanced Control is a technology which is advancing quickly, and it is as well to define terms in current use:-

Regulatory Control	Control applications that are shown in detail on the Unit control display.
Algorithmic Advanced Control	Higher levels of control that are implemented using control algorithms available in the DCS, (aka Traditional Advanced Control)
Sequential Control	Where there are a number of distinct steps or stages of control in which different control actions take place.
Multi-Variable Predictive Control (MVPC)	Where a multi-variable system identification provides a matrix process response model which is inverted to provide a multi-variable controller. Widely used MVPC packages include DMC and RMPCT
Optimisation	A layer above the control system that provides targets to the control system, and can take the forms:- Advisory Optimisation (aka Open-Loop Optimisation) and Closed-Loop Optimisation

5.9.1

General

General principles that apply to all advanced control and optimisation schemes are:-

- (a) Information relating to the advanced control or optimisation system should follow the general principles used throughout the DCS.
- (b) The operator interface to the scheme should be at the appropriate point in the display hierarchy.

thus a scheme that affects the whole of a plant area or process unit should have its primary interface at the area or unit level of the hierarchy. All advanced control scheme points of interaction with regulatory controls should be shown on the relevant operational graphic displays.

- (c) The operator interface should provide a means of identifying the mode of operation, (on/ off control), and the principal indications of correct function, (e.g. a target value and



measurement). A means of changing the status and target value may be provided at this point, or in the detailed advanced control display.

hexagon symbol is often used to denote an advanced control scheme, and can be used as a target for calling the detailed advanced control display.

- (d) The detailed advanced control display should enable the operator to understand what the scheme is for, what it is doing, how and why. It should provide sufficient information that the operator can be confident he knows the full effect of any operational changes he is proposing to make. It should inform him of any measurement validity problems or process constraint violations that he needs to take into account when commissioning or decommissioning any part of the scheme, or when modifying any settings.
- (e) Schemes are often part of a control hierarchy, with higher levels of control providing inputs, (e.g. optimiser feeding into algorithmic control set-points or MVPC targets). The detailed display should include a means to connect or disconnect the higher level of control, and a target to move to the detailed display for that control.
- (f) Where the scheme executes infrequently, it may be desirable to indicate the last and next expected execution times.

perhaps with a suitable graphical indication of progress through the execution cycle.
- (g) The control scheme should be configured to take the appropriate degradation or fall-back action when a bad measurement, inappropriate regulatory control mode or unsuitable process situation occurs. The operator interface should clearly identify to the operator what has happened and why.
- (h) Operator interface design should be optimised for:-
 - (i) Routine operations. The operator should not feel restricted or influenced in his action by the control system itself. Common actions and display navigation should be fast, intuitive and should use a minimum of key strokes or screen interactions.

- (ii) Non-routine operations. The experienced operator should be given guidance by the system, both unprompted and operator requested help should be considered.
- (iii) New or inexperienced operators. There should be guidance available about all aspects of the control system, the control application and the expected human actions. This may take the form of brief notes, (which may be context-specific), on the advanced control detailed display. Additional pages of more detailed information may be provided. Hypertext may be used to advantage, here.
- (i) A performance monitoring and reporting system should be provided, together with a suitable display. The statistics gathered may include, as appropriate: on-line time or service factor; frequency of successful or unsuccessful runs; and some indication of performance, in terms of economic benefit, production rate or process efficiency.

The configuration and programming details for Advanced Control and Optimisation schemes should be checked for appropriate and consistent application of the principles outlined above by means of the CONSOP process.

5.9.2 Algorithmic Control Scheme

Algorithmic control schemes typically have a number of process measurements providing feed-forward, calculation, dynamic compensation or constraint control to single- or multi-layer cascade or ratio control systems. Blocks containing program code may be included in the scheme for complex calculations, interlocks or initialisation sequences.

The detailed advanced control display will typically include the following features:-

- (a) The principle feature may be a schematic block-diagram of the control scheme giving the points at which the operator can make mode or setting changes, and any switch or selection actions that the scheme performs.
- (b) The control connections between algorithm blocks should be shown, with arrows giving the direction of signal flow. Where there are switch or selection actions, the active path may be indicated by making these connections brighter than the inactive paths.



- (c) Measurement and calculated values should be displayed at appropriate points so that the operator has a clear understanding of what is happening.
- (d) small trend display of the key variables may be included so that the operator can identify what has recently happened after a disturbance within the control scheme.
- (e) A single button or target may be provided that will commission or decommission the whole scheme, or a major section of it.

5.9.3

Multi-variable Predictive Control Schemes

MVPC schemes vary in complexity from simple two input, one output (2x1) schemes, to complex schemes covering a large section of plant. In principle, a dynamic model relating the controller output(s) to the inputs is used for control. The external parameters generally consist of:-

- (a) Manipulated variable MV - An independent variable manipulated by the controller i.e. the controller output.
- (b) Controlled Variable CV - A dependent variable (i.e. affected by the MVs). The targets and constraints of the controller.
- (c) Disturbance or Feedforward Variable DV - An independent variable which the controller has no influence over.

The detailed advanced control display typically contains the following features:-

- (d) For large schemes, the parameters are broken down into small manageable groups consisting of those variables that are closely associated in influencing terms. Some variables may appear on several display pages if they influence several areas of the plant. There may be a top-level display with key plant over-view parameters and the scheme on/ off/ initialise controls, with links to subordinate displays.
- (e) Colours or highlighting may be used to indicate constrained variables, out-of-limits variables or those currently not meeting target objectives.
- (f) Displays are generally tabular in form and the target and constraint set-point values may function as operator data entry fields. Steady-state prediction values and status for each controlled variable should be provided.
- (g) The output signals are provided with auto/manual or cascade/local mode-change facilities and provision for manual entry of the value to allow for manual intervention on a particular output.
- (h) An indication should be provided of the output move directions, sizes and ramping, preferably by graphical means.

- (i) Fall-back for the MVPC consists generally of simple, cascade or ratio PID controllers plus some manual loading stations. A target on each advanced control detailed display should allow rapid navigation to the fall-back control display. Consideration should be given to automatic commissioning of fall-back controllers to minimise the operator's work-load in the disturbance following mal-operation of the MVPC.
- (j) The MVPC detailed display often contains a trend graph of the key variables for that area, (usually the controlled and constrained measurements). This should plot both the predicted and actual values of the parameters, and include forward predictions.

5.9.4

Advisory Optimisation

Advisory optimisation systems calculate optimum plant operating conditions and the operator has to respond to this information. These systems generally operate in final value form, i.e. take no account of plant dynamics nor how long it will take the plant to settle at the optimum value.. Often such systems operate on a significant change basis, advising the operator by way of messages of a new optimum when a significant change has occurred to the plant, (e.g. feed-stock quality).

- (a) The detailed optimiser display is generally tabular in form, with actual measurement, current set-point and optimiser target values for each of the manipulated variables. The table should also contain an evaluation of lost profit calculated from deviation of each actual process measurement from target; a bar-graph indicating this deviation for each parameter allows the operator to scan the optimiser displays quickly to identify his action priorities.

For large optimisers, this table may spread over several pages.

- (b) The operator needs to be able to inform the optimiser which of the set-points he does not want to be manipulated, or which are unavailable for optimisation for any reason, as this will affect the optimum.
- (c) A mechanism may be provided for down-loading the optimiser targets, either one at a time or as a group, into the controller set-points.
- (d) Further pages of display may be provided for the process constraints. The current actual process measurement is listed with the optimiser upper and lower constraint boundaries. Calculated "constraint approach values" are displayed showing



the operator the economic effect of changing the currently active constraint boundaries.

5.9.5 Closed-loop Optimisation

Closed-loop optimisers generally operate in incremental form, moving the plant conditions only by the amount that the plant can respond during the next optimiser cycle. To provide bump-free commissioning, increments rather than whole values are passed to the control system set-points, and are often enacted through a set-point ramping feature to minimise disturbances.

- (a) In addition to a tabular display for target values and constraints, there is generally an over-view display that provides status monitoring of the optimiser and provides the operator with switches to select closed-loop or open-loop operating modes. This display includes monitoring of protection features such as a watch-dog on data communication to the control system from the optimiser computer.
- (b) Closed loop optimisers will often have a stand-by mode where all cascade links are established, but no action is propagated to the underlying controls. This state is useful for commissioning, maintenance and transient handling. Switching to the fully operational state should be with a single operation located on the optimiser summary page. Optimisers should only be left in the stand-by mode for short periods of time, this being enforced by a timer automatic link break.
- (c) Control loops whose set-point can be set by the optimiser require a cascade/local mode select switch. The mode selector should appear on the individual advanced control detailed display, with status repeated on the optimiser target-value display.

An optimiser watch-dog or off-line signal should set all mode selector to local. Cascade commissioning requires individual action on each control scheme. In some cases local clusters of a few cascades may be grouped together into one control scheme.

- (d) It is essential that the operator can identify what the optimiser is doing to the plant. As changes should occur slowly, this is often not obvious from the direction or magnitude of the increments. It is desirable that the optimiser has an intelligent means of informing the operator the strategy it is following.

Operator messages should be generated in the optimiser host computer and down-loaded to the control system.



- (e) Operators should be able to set constraint limits and controller set-points. Since constraints affect operation of the whole optimiser, access will usually be through constraint summary pages.
- (f) The operator should be made aware when constraints become active, however constraint status should be restricted to passive indication, as a closed loop optimiser will generally be running to one or more active constraints in normal operation, which does not require alarming.

5.9.6

Other Kinds of Advanced Control Scheme

There are many specific circumstances where programs are provided for particular complex plant control functions, which do not fit the above categories, e.g.:-

- (a) routing logic for tank-farms or silos.
- (b) ship or road-tanker transfer schemes.
- (c) recipe management schemes for batch processes.
- (d) grade-transition schemes for multi-grade continuous processes.
- (e) batch-blending systems.
- (f) fuzzy-logic control and optimisation systems.

The nature and function of such schemes is so diffuse that only general principles for the operator interface design are provided:-

- (g) The operator must be able fully to understand the function and action of the control scheme. As far as possible this should be apparent from graphical or schematic presentation of information; help text should be supplementary rather than a primary essential.
- (h) The operator must have sufficient confidence that the control scheme will do what he expects it to do, from the information on the display, that he feels able to put it into commission.
- (i) The operator must know how to tell when the control scheme is not doing what it is supposed to do, and what to do when that happens.
- (j) The operator's interactions with the control scheme must match his expectations.



6. ACCEPTANCE AND INSTALLATION

6.1 Factory Acceptance Testing (FAT)

The objective of the DCS FAT is to ensure and confirm the following:-

- (a) All deliverable items, i.e. hardware, software, documentation, media etc. are present and acceptable.
- (b) The correct functioning of the DCS in accordance with the SDS, including all interfaces to other equipment and sub-systems.
- (c) The system operates under simulated load conditions over the test period at or better than design availability.
- (d) The system can tolerate failure of individual modules and sub-systems and be recovered to full function following repair and re- instatement of such items.
- (e) That no untoward control actions can occur.
- (f) That the operator interface is accurate, safe and operable with respect to the presentation of data and alarms and the implementation of control.

The FAT should be carried out at the vendors works by the vendor's personnel, witnessed by Project representatives. The tests should be carried out in accordance with an FAT procedure specification prepared by the system vendor and agreed in advance of test commencement.

Prior to this test, the vendor should have completed all his in-house validation testing and quality checks to ensure that the system fully complies with the SDS and all application software specifications.

Experience has shown that faults found at site will take significantly longer - often more than twice as long - to rectify than faults found at the vendor's factory. This is especially the case for new sites, or new equipment on established sites. Where there is an established site infrastructure to support the project equipment, on-site repairs may not incur such disadvantage, and the FAT may be less rigorous accordingly. Bearing this in mind, it is recommended that the extent and scope of the FAT should be established against the risks involved in leaving some testing to site.

Effort should be tailored in accordance with risk, e.g. statistical methods such as 10% checks on I/O should be considered to reduce testing effort on well established items.



An agreed period should be set up at the end of the FAT for conducting any additional or repeat testing that may be required.

The vendor should provide documented evidence of all faults identified and their subsequent correction.

The scope of the FAT should include:-

- (g) Inventory Checks.
- (h) Labeling and Presentation Checks.
- (i) Hardware Testing.
 - Module Testing, e.g. - Diagnostic Routines.
 - Redundancy Testing.
 - Failure and recovery Testing.
 - Field Termination Testing.
 - Power, Fusing and Earthing Checks.
 - Interfaces to other systems and Sub-systems.
- (j) Configuration Testing.
 - System Configuration Checks.
 - I/O Database Configuration Checks.
 - MMI Configuration Checks - Displays, Alarms etc.
 - Control Loop Functionality Testing.
- (k) Software Testing.
 - Application Program Testing against Functional Specification.
- (l) Integrated System Tests.
 - Overall System Tests.
 - Operability Testing - system response times.
 - Failure and Recovery of System.

FAT Test details are covered in the appendix C.

Complex software with non-trivial logic, control sequences, mass flow accounting packages, supervisory control packages, etc. should be tested by the "walk through" test approach. Simple simulator boxes comprising switches and potentiometers or the equivalent in simple software points should be used to drive the "walk through" test. Control loops can be simulated by feeding the output back into the input.

The objective of the "walk through" test is to ensure each line or section of code is exercised at least once and its correct operation. The flowcharts and listings of the software can form part of the test script. As the "walk through" test proceeds, paths through the code can be marked off on the flowchart as they are checked and confirmed. Operator interfaces to application software should be checked at the same time, preferably with operations staff present.

It is recommended that application software is tested by a two person team, one being the program author, the other being the client's witness tester.



Delivery and Installation

It is important to thoroughly plan delivery and installation of a DCS in conjunction with the vendor and the receiving site or Project. In particular, Civil, Electrical and Instrumentation work at the receiving location should be as complete as possible. If work has to be completed following delivery of the DCS equipment suitable partitioning or screening should be erected to protect against the ingress of dust or dirt.

The following points should be checked prior to delivery:-

- (a) Access adequate for delivery vehicle?
- (b) Access adequate for equipment siting?
- (c) All partitioning complete?
- (d) All painting complete?
- (e) Sub-floor clean and suitably sealed?
- (f) False floor complete?
- (g) HVAC installed, tested and commissioned?
- (h) Lighting installation complete?
- (i) The earthing system complete?
- (j) The UPS power supply and distribution complete?
- (k) Field cable pulling and glanding complete?
- (l) Have procedures been developed to prevent ingress of dust and dirt following DCS installation?
- (m) Have fire precautions been addressed, i.e.. extinguishers, smoke detectors etc?

A delivery and installation plan should be developed in association with the vendor, the project contractor or site, and the vendor's haulage contractor. This plan should be circulated and discussed with all interested parties prior to delivery. It is recommended that this plan includes the following aspects:-

- (n) A programme bar chart showing all activities, duration's, and dates including phasing if the delivery is phased.
- (o) A description/listing of all activities, i.e. work scope
- (p) A clear definition of responsibilities for all parties
- (q) An equipment list
- (r) Detailed power supply requirements, i.e. which distribution boards will be needed, etc.
- (s) Details of the size and weight of delivery vehicles
- (t) Detailed means of moving equipment from delivery vehicle to point of installation

6.3 Site Acceptance Test (SAT)

6.3.1 Site Testing Principles

Following delivery and installation, it is recommended that a Site Acceptance Test (SAT) is carried out. This test should be based on a subset of the Factory Acceptance Test (FAT) supplemented by tests which can be carried out only at Site, for location or logistical reasons.

The SAT test specification should reflect the structure and the phasing of the testing starting with inventory checks and hardware tests through software testing to final testing of a fully integrated system of hardware and software. Test scripts should be produced to cover all testing.

An SAT test specification should be developed to cover all testing to be carried out. The specification should state clearly the objectives of testing and contain test pre-requisites, test scripts, programme, procedures for fault rectification and the means for documenting the tests.

The purpose of the SAT is to establish that the DCS equipment has been shipped without damage, has been correctly installed and operates reliably to specification in its final environment.

For guidance, the following typical DCS SAT Objectives list is provided:-

To ensure and confirm the following :-

- (a) All deliverable items, i.e. hardware, software, documentation, media, etc. are present and acceptable.
- (b) The correct functioning of the Distributed Control System (DCS) in accordance with the SDS, including all interfaces to other equipment and sub-systems on the final power supply and earthing system.
- (c) The system operates under loaded conditions over the test period at or better than design availability.
- (d) The system can tolerate failure of individual modules and subsystems and be recovered to full function following repair and re-instatement of such items.
- (e) All remedial work agreed at FAT has been satisfactorily completed by the vendor and the system meets its design specification in full.
- (f) The Operator Interface is both safe and operable with respect to the presentation of data and alarms and the implementation of control.



It is also good practice at this time to check that all environmental conditions in the control and equipment rooms meet design specifications, and operational needs e.g.:-

- (g) HVAC.
- (h) Lighting and glare.
- (i) Noise levels.

6.3.2 Hardware Testing

Correct assembly of redundant equipment items should be established by forced failure and recovery testing. This testing should extend to network communication cables, power distributions, and any connected instrument subsystems.

Any equipment replaced or added since FAT should be thoroughly tested.

The following supplementary hardware testing is recommended to be carried out at SAT:-

- (a) Power distribution, fusing, segregation and earthing checks.
- (b) DCS/UPS tests including in-rush, mains failure, static switch failure, battery discharge, voltage and frequency variation.
- (c) Check for interference from ancillary equipment, e.g. HVAC thermostats, lighting dimmers, radios, etc.
- (d) Check noise levels versus specification.
- (e) Check operator interface for glare, reflections, etc.
- (f) Check operation and acceptability of alarm annunciators, lamps and contacts.
- (g) Check operation of all connected subsystems. In particular, those not previously tested, e.g. links to remote systems by communications link, etc.

6.3.3 Software Testing

Any software which has been subject to remedial work since FAT should be thoroughly re-tested including any potential impacts on unmodified software. Similarly any software added since FAT should be fully tested.

6.3.4 Integrated Testing

To conclude the SAT, it is recommended that a test of the fully integrated DCS, i.e. hardware, software, instrument sub-systems, communications links should be carried out. If such a test was previously carried out during FAT at the vendor's premises, the duration of the SAT test may be reduced. The integrated testing of equipment not available at FAT, e.g. sub-systems and communications links, should be performed.



6.4 Pre-commissioning and Loop Testing

It is recommended that the planning of pre-commissioning and loop testing activities is carried out as early as possible during the DCS detailed design phase, e.g. on availability of approved for construction P&I diagrams. Planning should be carried out in conjunction with construction and plant commissioning staff and reflect the program of mechanical completion and phasing of process commissioning.

6.4.1 Loop Testing Organisation and Schedule

In discussion with construction and commissioning staff, the number of loops to be tested and the dates by which they are required should be established. From this data, the average, number of loops to be tested per day can be established for all phases of pre-commissioning, and hence the number of test teams required and the resource profile against time. For guidance in this area the following information is provided:-

- (a) Loop test teams of two instrument technicians are typically used. Any corrective or remedial work is best carried out by teams dedicated to that task, i.e. not by test teams. Test teams can often be beneficially supported at the control room end of loops i.e. at the DCS screen, by plant operators.
- (b) On recent DCS projects, the productivity of loop test teams has averaged between 4 and 8 loops per day. This rate is obviously dependent on the loop complexity and availability and the higher figure is more likely where there is a lot of simple loops, e.g. plants with high number of digital inputs.

On reinstrumentation jobs the productivity rate is very dependent on the level and commitment of the operations/ process support available.

- (c) In drawing up any schedule or resourcing plan, equipment access and availability should be checked. This applies particularly to DCS screens where the phasing of pre-commissioning and DCS engineering support work may cause access bottlenecks. In such cases, it may be possible to loan or hire extra DCS screens from the vendor for the commissioning period.

6.4.2 Loop Testing Procedures

Formal procedures detailing method and responsibilities should be written for loop testing. Each loop should have a documentation dossier raised prior to testing for use by testers. Loop tests should be witnessed. On satisfactory completion of a test, a test certificate should be produced. This should be endorsed by the witness. Any



documentation errors encountered in the test should be marked up and corrected.

The following outline DCS loop testing procedure is provided for general guidance:-

- (a) Issue test schedule.
- (b) Raise inspection and test documentation dossier
- (c) Check field cabling for short circuits and earth faults.
- (d) Check loop voltage and polarity.
- (e) Power up loop.
- (f) Test loop.

For analogue inputs, simulate at 0-50-100-50-0 % of input at transmitter process side. Check for correct reading at DCS Screen.

For field switches, simulate input signal at switch process side. Check for correct reading at DCS screen.

For control valves, check stroking by adjusting at DCS in manual at 0-50-100-50-0 % output. Check for correspondence between field valve position in field and DCS screen value. Check operation of any ancillary devices. e.g. limit switches, boosters, lock up devices etc.

Analysers will need special attention but wiring from the field junction box through to DCS can be tested by simple signal injection.

Software functionality should also be tested by means of integrated loop testing. This should include loops incorporating logic signals and calculations.

For full operation tests, a fully integrated functional test may be required, e.g. interlocks and safety systems requiring a functional integration of the DCS with PLC sub-systems, mechanical devices etc.

- (h) Obtain witness endorsement of test and certificate.
- (i) Mark up and correct any discrepancies in documentation and drawings.

6.4.3 Operator Familiarisation and Training

Operators are involved at the DCS screen to assist in loop testing wherever possible. This has the benefit of providing early DCS familiarity on the actual equipment and allows them to learn DCS operating procedures, display content and structure before commissioning starts.

6.4.4 Precommissioning: Plant Trials and Test Runs

Where the process characteristics allow, water test runs can be used to pre-commission process equipment. In these cases, every opportunity should be taken to set up and carry out tuning of control loops and schemes even though the process conditions may differ from design



figures. Water tests should also be used to further check and set-up control sequences and logic. Inevitable mismatches between plant equipment and sequence logic can be beneficially resolved at this stage without the risks of spoiling actual process material.

Every opportunity should be taken during pre-commissioning to set-up and confirm the operation of advanced control schemes. Use should be made of any plant test or water trials to set up limits and constraints. Test runs afford good training opportunities to familiarise plant management and operators with the advanced control design, objectives and operation. Operator interface and reporting aspects can also be re-checked and confirmed directly with the user.

6.5 Commissioning

DCS commissioning and loop tuning activities should be closely coordinated with plant commissioning and with the process operators. It is useful to use a two week look ahead of plant commissioning activities to plan and resource activities on DCS.

Process operators should be provided with full DCS support during commissioning. This support should reinforce training, and quickly clarify any misunderstandings. This is in addition to resolving any problems with DCS control and configuration. At start up, shift working by DCS engineers may be required to provide the right level of support.

6.5.1 Loop Tuning Starting Values

It is recommended that all PID controllers are loaded with safe starting values for the three term control constants. This will greatly assist commissioning loops, for which the following tuning constant starting values are provided for guidance:-

LOOP TUNING SUGGESTED STARTING VALUES				
LOOP TYPE	APPLICATION	GAIN	INTEGRAL (MINS/RPT)	DERIVATIVE (MINS)
Flow	Simple Control	0.3	0.05	0.0
Flow	Cascade Slave	0.3	0.05	0.0
Pressure - Liquid	Simple Control	0.3	0.05	0.0
Pressure - Gas	Simple Control	3.0	2.0	0.0
Temperature	Simple Control	1.0	10	later
Temperature	Cascade Master	1.0	10	later
Level - Tight	Simple Control	4.0	10	0.08
Level - Averaging	Simple Control	1.0	5.0	0.0
Level	Cascade Master	1.0	5.0	0.0

On re-instrumentation projects, changeover to the new DCS instrumentation can be made with the process equipment shut-down, i.e. cold or with the process equipment live 'loop by loop', i.e. hot. Cold changeover is generally used where equipment can be conveniently shut-down or where the re-instrumentation project is set-up to coincide with a planned plant maintenance shut-down period. It is arguable which changeover method involves the least risk and disruption to the plant. Commercial considerations favour hot changeover as the plant continues to operate. Furthermore, as loops are transferred one by one rather than en-block, more control can be exercised over the rate of loop transfer and any faults are picked up immediately rather than all at once during plant start-up.

Hot changeover has procedural similarities with conventional plant instrumentation maintenance. In devising changeover procedures, it is therefore recommended that the use of existing procedures for instrument maintenance are maximised. This has the benefit of employing well proven and understood techniques to minimise changeover risk. Proven procedures will normally exist for:-

- (a) Electrical isolation.
- (b) Prevention of upsets during instrument maintenance, e.g. by use of valve hand wheels, by-passes etc.

Changeover procedure documentation packs should be produced for all loops. Loops involving control valves should be surveyed to establish an appropriate means of changeover and any potential interaction problems, e.g. the valve may be part of a safety system or be slave of a cascade loop. Changeover documentation should include:-

- (c) Overall checklist.
- (d) Operational requirements.
- (e) Step by step changeover procedure.
- (f) Instrument loop diagram.
- (g) P&ID extract.
- (h) Termination details.
- (i) Permit (prior to changeover).

Changeover rates are normally in the range of 10-15 controller loops per day. This rate is limited by the rate at which operations staff can safely accept and feel comfortable with the changed over loops, rather than the rate loops can physically be progressed by instrument technicians. On previous re-instrumentation projects, deliberate breaks

have been built into the project programme to allow operations staff 'breathing space' to get used to DCS controls.

Particular attention should be paid to the training and support of the operator. As the plant is changed over, operators will have to work with the new and the old interfaces at the same time. This temporarily increases operator loading and stress. Training programmes should address these issues and the provision of operator support staff should be considered.

6.5.3 Advanced Control Commissioning

Advanced control commissioning should be carefully planned in association with plant management and operators. Prior to attempting to commission any scheme, it is recommended that the following steps are taken:-

The scheme should be set-up with appropriate safe starting parameter values and maximum use should be made of any available constraints and limits, i.e. take all practical measures to avoid upsetting or shutting down the plant.

- (a) Operators and plant management should be trained on the objectives and operation of the scheme.
- (b) Full descriptions of how to operate the scheme should be available to operations staff. In particular, how to put in and out of service and what to do if something goes wrong.
- (c) A means of monitoring and recording the performance and usage of the scheme should be available.
- (d) Operators should be directly involved in the commissioning and be fully supported during the initial phases of operation.



7. OPERATIONAL MANAGEMENT

7.1 Operation and Development

It is essential that the procedures developed during DCS pre-commissioning and commissioning phases for controlling changes and housekeeping are maintained for the life of the plant. This will ensure that all changes and development are checked for safety and operability and are auditable and fully documented.

DCSs should not be commissioned and then left technically unsupported. Every effort should be made to maximise the use of the DCS facilities for the economic benefit of the plant. Effort should not just be concentrated on improved or advanced control schemes, but also on operability issues such as alarms and displays.

7.2 Change Procedures

On completion of the FAT, any further software changes made on the DCS should be documented and approved on a Software Change Control Procedure. This procedure should be set up and agreed prior to the FAT.

The vendor and the project should have developed change control and housekeeping procedures in implementing the DCS. These procedures should be reviewed and used as the starting point for developing suitable change control and housekeeping strategies for the running plant situation.

A well developed Software Change Request (SCR) form is presented in Appendix E. The SCR form incorporates a checklist which assists in providing a well engineered control system change.

It is recommended that the developed procedures incorporate the following points:-

- (a) All changes that impact plant control, operability or safety should be subject to review and approval via a DCS Change Procedure and fully documented. Changes should be reviewed for safety and operability implications and approved by a panel of suitably experienced and qualified staff. Typically this would entail approval of the plant process engineer, plant instrument engineer and the DCS engineer.
- (b) The impact of a change on other systems. e.g. ESD should be fully considered.
- (c) All changes must be furnished with a clear audit trail of documentation, both in paper form and via magnetic media.
- (d) Changes should only be made by suitably qualified, experienced and trained personnel.



- (e) Plant management and operators should be fully informed and briefed on all changes both before and after the change.
- (f) Training should be given where the change impacts existing plant control or procedures.
- (g) What constitutes a minor change should be clearly defined.

7.3 Housekeeping

Housekeeping procedures should always be reviewed following changes to system hardware or system software to ensure they remain up-to-date and appropriate.

Recommendations for efficient housekeeping include:-

- (a) Compiling, and working by a set of DCS Operating Procedures. These procedures should include a DCS Permit to Work System, a Software Change Control Procedure, Back-Up Procedures, and a Disaster Recovery Procedure. All procedures should outline responsibilities for DCS support.
- (b) The Disaster Recovery Procedure should include diagnosing failures, assessing their impact, and agreed remedial actions. Failure areas to be covered include loss of operator window, module and card failures, network failures, with remedial actions including reload procedures.
- (c) The Back-Up Procedure should include:-
 - (i) Regular back-ups should be made of all configuration and program files. The frequency of back-ups should be determined by the extent and rate of system change and the risk of data loss, e.g. in periods of intensive development daily back-ups may be required.; once the system settles down and the development pace reduces weekly or even monthly back-ups may be sufficient.
 - (ii) A minimum of two copies of the current back-up should be kept off-system on magnetic media. These copies should be kept in separate locations, e.g. one copy at the plant; one copy off the plant. Storage in a fire-proof safe should be considered for at least one copy.
 - (iii) Keeping a previous generation back-up system,

these copies are generally referred to as 'Present Generation'/'Father Copy'/'Grandfather Copy'.



- (iv) Full use should be made of any on-line DCS back-up system. This should include full re-installable back-ups, as well as configuration file re-load back-ups.
- (v) A master set of current up-to-date DCS configuration and software documentation should be maintained on paper or electronically.

7.4 Maintenance and Spares

Maintenance contracts and spares holdings should be geared to plant requirements. A continuous plant may require significant on-site spares and a 4 hour call out response for the vendor's maintenance engineer, whereas a batch plant might only require minimal on-site spares with a 24 hour response. Remote plant locations are likely to require larger on-site spares holdings. Spares holdings and maintenance contracts should be optimised across sites where several systems from the same vendor are installed. Potential to optimise across the Group should not be overlooked. Existing agreements within the Group should be consulted to ensure best value for money is obtained on any new arrangements.

Arrangements where the vendor manages on-site DCS spares holding can be attractive. This arrangement has clear responsibilities should a spare be unserviceable, and the spares are then kept up-to-date at the correct revision levels.

7.5 Refresher Training

Refresher training of plant operators on DCS should be carried out periodically. This has a number of advantages:-

- (a) It enables less frequently used operating procedures to be revisited.
- (b) It enables updated procedures to be incorporated.
- (c) It enables bad operating habits to be eliminated.
- (d) It reinforces best practice.



DEFINITIONS AND ABBREVIATIONS

Definitions

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

The following general definitions are applicable to all Parts of this Code of Practice:-

Abbreviations

AHP	Alarm Handling Package
AMHAZ	Alarm Management Hazard Assessment
CCTV	Close Circuit Television
CHAZOP	Computer Hazard & Operability (Study)
MVPC	Multivariable Predictive Controller
CONOP	Control Safety and Operability
CP	Control Philosophy
CSMA/CD	Carrier Sense Multiple Access/Collision Detect
CV	Controlled Variable
DCN	Distributed Control Network
DCS	Distributed Control System
DMC	Dynamic Matrix Control
DV	Drive Value
ERA	Electrical Research Authority
ESD	Emergency Shutdown
F & G	Fire & Gas
FAT	Factory Acceptance Test
FC	Fail Closed
FEED	Front End Engineering Design
FMEA	Failure Mode and Effect Analysis
FO	Fail Open
FS	Functional Specification
H & V	Heating and Ventilation
HAZOP	Hazard and Operability (Study)
HVAC	Heating, Ventilation and Air Conditioning
I/O	Input/Output
ID	Identification
IS	Intrinsically Safe
ITT	Invitation to Tender
LAN	Local Area Network
LCN	Local Control Network



MMI	Man-Machine Interface
MTBF	Meantime Between Failures
MV	Measured Variable
MVPC	Multivariable Predictive Control
OHSE	Occupational Health, Safety and Environment
OP	Output
P&ID	Piping and Instrumentation Diagram
PA	Public Address
PFD	Process Flow Diagram
PHSER	Project Health Safety and Environmental Review
PID	Proportional Integral Derivative
PLC	Programmable Logic Controller
PV	Process Variable
RMPCT	Robust Multivariable Predictive Control Technology
SAT	Site Acceptance Test
SCADA	Supervisory Control and Data Acquisition
SCR	Software Change Request
SDS	System Design Specification
SIRA	Scientific Instrument Research Association
SOR	Statement of Requirements
SP	Set Point
SQL	Standard Query Language
FM	Factory Mutual
UCN	Universal Control Network
UPS	Uninterruptable Power Supply
VDU	Visual Display Unit
VESDA	Very Early Smoke Detection
WAN	Wide Areas Network



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.

International Standards

IEC 61508	Functional Safety - Safety Related System
ISO 11064	Ergonomic Design of Control Centres
IEEE 802.4	Broadband Token Business Standard
IEEE 802.3	Baseband/Ethernet Standard

Group Standards

RP 30 series	(Control and Instrumentation)
------------------------------	-------------------------------

Others

1975-224022	CONSOP Report
89/391/EEC	EEC directive - Display Screen Equipment
Report 1996 - 225211	AMHAZ Report



GUIDANCE CHECKLISTS

C.1 DCS Specification Contents

Guidance checklist for the contents of a Functional Specification.

The list given is for a single vendor approach. On a competitive project some of the more specific detail would be omitted.

INTRODUCTION

Background
Purpose of Specification
Vendor Specific Clauses
Instructions to Tenderer Document
Use of Language

DESCRIPTION OF PLANT

Geographical Layout
Remote Operator Station
Control Building
Environmental Conditions in Buildings

OVERALL OPERATIONAL PHILOSOPHY

DCS Design Philosophy Overview
Allocation of Operational Areas

VENDOR RESPONSIBILITIES AND SCOPE OF SUPPLY

Hardware
Software
Services
Failure Modes and Availability Analysis
Long Term System Support

BP /CONTRACTOR RESPONSIBILITIES

SYSTEM DESIGN PHILOSOPHY

Controller and Plant Interface Redundancy
Worst Tolerable Controller Failures
Redundancy of Operator Station
Data Communications
Change, Repair and Test On-line

SYSTEM SIZING

Controller Module Sizing
Input/ Output Processor Count
Sizing and Arrangement of Controller Cabinets
Hot Spare Capacity
Consoles
Peripherals
Data Storage Modules
Application Processors
Computer Interface
Serial Interfaces
Cable Lengths



OFF-LINE DEVELOPMENT SYSTEMS

SYSTEM FUNCTIONALITY

Regulatory Control
Advanced Control
Computing Facilities
Internal Data Communications
Interfaces to Intelligent Instrumentation
Communications to/from Associated Computer
Consoles and Displays
Historical Storage and Trending
Alarm Presentation
Reporting
Engineering Facilities
Pre and Post Trip Recording Facility

HARDWARE

System Design
Interfaces
Analogue Inputs
Analogue Outputs
Digital Inputs
Digital Outputs
Smart Transmitter Interfaces
Power Supplies
Operator Interface
Disc Units
Printers
Screen Copy Device
Earthing
Cabinets and System Packaging
Interconnecting Cables
Associated Computer
Electrical Standards
Labelling and Cable Identification

SOFTWARE

Controller Functionality
Execution Speed and Timing
Programming Facilities
Sequence of Event Recording
Control Package for Plant
Internal Data Communications
External Data Communications
Display Facilities
Display Attributes
Alarm Presentation
Trends
Data Storage
Internal Security
Access Security
Utilities
Start-up, Back-up and Recovery
System Clocks
On-Line Modifications

SYSTEM PERFORMANCE

Execution Speeds
Display Response
Display Refresh



Feed-back
Loading
Alarm Floods
Availability/Reliability

QUALITY ASSURANCE

SYSTEM TESTING, SHIPPING AND INSTALLATION

Factory Acceptance Test
Foreign Device Interfaces
Packing and Shipment
Installation
Site Acceptance Testing

DOCUMENTATION

Specifications
Drawings
Test Procedures
Operating and Maintenance Manuals
Software Documentation
Configuration Manuals
Documentation for Approval

SPARES

Extent of Spares
Firmware Revisions

CONSUMABLES

Vendor Supply
Supply During Factory Test

MAINTENANCE SUPPORT

Vendor Support
Maintenance Agreements
Special Maintenance Equipment
Software Maintenance

TRAINING

Configuration Training
Maintenance Training
Operator Training
Inspector Training

APPENDICES & DRAWINGS

APPENDIX I	SCHEMATIC & REPORT EXAMPLES
APPENDIX II	INPUT/OUTPUT COUNTS AND PID CONTROLLERS
APPENDIX III	DETAILS OF SERIAL INTERFACES TO EXTERNAL PROGRAMMABLE
SYSTEMS	
APPENDIX IV	CONTROL PACKAGE DOCUMENTATION MANUAL
APPENDIX V	DOCUMENTATION INDEX (EXAMPLE)
DRAWING I	PLANT - PROPOSED PLOT PLAN
DRAWING II	PLANT - PROPOSED CONTROL ROOM LAYOUT
DRAWING III	PLANT - DCS PROJECT PROGRAMME
DRAWING IV	PLANT - PROPOSED DCS TOPOLOGY DIAGRAM
DRAWING V	PLANT - PROPOSED DCS ELECTRICAL ONE LINE DIAGRAM
DRAWING VI	PLANT - PROPOSED DCS BLOCK DIAGRAM
DRAWING VII	PLANT - PROPOSED CONSOLE LAYOUT



C.2 Instructions To Tenderer

Guidance checklist for ITT contents for an installed contract.

More detailed information on ITTs can be supplied by the BP Procurement and Contracts Group.

	Comment
INTRODUCTION	
SCOPE OF PROPOSED CONTRACT	
PROJECT PROGRAMME	<i>As list of key dates</i>
SUBMISSION OF TENDER	<i>Copies required, form, etc.</i>
INFORMATION REQUIRED WITH TENDER	<i>TS Paragraph compliance</i>
DCS SELECTION	
SYSTEMS COSTS	
DCS Pricing Schedule	<i>Presentation of prices</i>
Documentation	
Project Costs	
System Testing, Delivery and Site Installation	
System Support	
Training Facilities	
SITE UTILITIES	<i>Power, Off-loading</i>
PROGRAMME OF WORKS	<i>Schedule with milestones</i>
PAYMENT	
GUARANTEES	
Parent Company Guarantee	
Bank Guarantee	
System Warranty	
TERMS AND CONDITIONS	
PROJECT MANAGEMENT AND ENGINEERING SUPPORT	
Project Manager	
Lead Hardware Engineer	
Lead Application Engineer	
Use of Agency Staff	
PROJECT IMPLEMENTATION AND ORGANISATION	
Contract Organisation	
Project Planning	
Planning Information	
Project Reporting	
Minutes of Meetings	
Implementation Plan/Method Statement	
Vendor Support Facilities	
Procurement and Material Control	
OTHER COMMITMENTS	
QUALITY ASSURANCE/QUALITY CONTROL	
TENDER DOCUMENTS TO BE CONFIDENTIAL	
FINANCIAL STATUS	
LANGUAGE	
ENQUIRIES CONCERNING THE TENDER	
APPENDIX I - DCS PRICING SCHEDULE	<i>Completed by Vendor</i>



C.3 Front-End Engineering

Guidance checklist of the activities and deliverables during FEED:-.

Activities

- Develop Control Philosophy
- Develop DCS Outline Design
- Estimate DCS Size
- Enquire of Budgetary Costs
- Estimate DCS Costs
- Develop DCS Procurement Strategy
- Evaluate Systems
- Select Vendor
- Obtain Endorsement/ Approval of Choice
- Develop DCS Project Organisation and Implementation Strategy
- Develop DCS Technical Specification
- Develop MMI Philosophy
- Develop Training Philosophy

Documents

- Statement of Requirements
- Feasibility Study Report [Reinstrumentation]
- Engineering Basis and Design Data [Grass Roots Projects]
- Control Philosophy
- User Requirements Specification
- Budgetary Enquiry
- Cost Estimate
- Procurement Strategy
- Vendor Evaluation and Selection Report
- DCS Technical Specification
- DCS Project Organisation and Implementation Strategy
- MMI Philosophy

Drawings

- DCS Block Diagram
- Proposed Control Room Layout
- Proposed DCS Project programme
- Proposed DCS Network Topology
- Proposed DCS Electrical One Line Diagram
- Proposed DCS Console Layout



C.4 Enquiry

Guidance checklist for the activities and deliverables during the Enquiry phase:-

Activities

- Develop Invitation to Tender (ITT)
- Develop Supplementary Conditions of Purchase
- Raise Secrecy Agreement where appropriate
- Reconcile Bids
- Hold Clarification Meetings with Vendors and Clarify Bids
- Assess Bids Technically
- Assess Bids Commercially
- Choose Vendor
- Obtain Endorsement/Approval of Vendor Choice
- Issue Letter of Intent.

Documents

- Invitation to Tender (ITT)
- Conditions of Purchase/Service
- Supplementary Conditions of Purchase
- Secrecy Agreement
- Technical Bid Analysis and Assessment
- Commercial Bid Analysis and Assessment
- Recommendation for Purchase
- Letter of Intent

C.5 Purchase

Guidance checklist for the activities and deliverables during the Purchase phase:-

Activities

- Negotiation with Vendor(s)
- Develop Purchase Specification
- Develop Contract/Purchase Order
- Agree Contract Terms and Conditions
- Contract/Purchase Order Issue and Signature

Documents

- Purchase Specification
- Purchase Order
- Contract
- Delivery Schedule

C.6 Delivery Schedule

During negotiation the system delivery schedule should be agreed, and this should include services and information that is to be supplied. The delivery schedule should be drawn up as a network diagram or Gantt chart. All significant project dates should be clearly identified, and tabulated in a schedule of dates, (identified as either a Milestone or Key Date).

Milestones are generally associated with a contract payment

Key Dates are related to project schedule and not usually associated with a contract payment.

Significant information due dates should also be tabulated in a schedule of information.

The following guidance example is provided:-

Significant Project Dates

		By
<i>Milestone 1</i>	- Approval of System Design Specification (SDS) and Hardware Drawings sufficient to define system hardware. - Reliability analysis. - Information on total power requirements	
<i>Milestone 2</i>	- Delivery of all Hardware into Staging. - Confirmation of all cable lengths	
<i>Milestone 3</i>	- Completion of System Assembly	
<i>Milestone 4</i>	- Completion of Factory Acceptance	
<i>Milestone 5</i>	- Completion of Site Acceptance	
<i>Key Date 1</i>	- Freeze Date for Hardware	
<i>Key Date 2</i>	- Freeze Date for Software/Configuration	
<i>Key Date 3</i>	- Field Termination Cabinets Available for Delivery	

Significant Information Due Dates

Hardware

	By
Console Layout Drawing approval	
Field Termination Cabinets (FTC) internal layout approval	
Field Termination Cabinets (FTC) cross wiring approval	
Control Room Layout	
System Cable Lengths	

Software

	By
Network Design	
I/O Tag Design	
Applications Software Program Design	
Faceplate Group Design	
Historical and Real Time Trend Design	
Display Static Template Design	
Display Dynamic Design	
Report Design	



C.7 Man-Machine Interface Philosophy and Specification

Guidance MMI specification contents:-

Introduction

Objective

General

Responsibilities

Interface Hardware

Manning

Database Structuring for Alarm and Display

DCS Security

ESD Security

DCS INTERFACE

DCS Displays

Display Philosophy

Hierarchy

Operator Change Access

Screen Usage

Configuration

Layout

Touch Screen Target Areas

Level of Detail

Symbols

Descriptions

Colour Codes

Lines

Normal Conditions

Decimal Places

Abbreviations

Engineering Units

Feedback

Date/Time Format

Use of Colour and Attributes

General

Colours

Visibility

Intensity

Reverse Video

Flashing

Fill Level

Selection

Bad Data

Use of Standard Library Pictures and Symbols

General

Controllers

Equipment

ESD Trip Valves

Operator Access Areas

Flow Direction

Source/Destination Indicators

Area Displays

Unit Displays

Group Displays

Detail Displays

Trend Displays

Other Displays

Alarm Handling

Help Displays

Allocation of Display References

Use of Operator Keyboard

Use of Hard Copy Devices

Use of Historisation Facilities

ESD INTERFACE



C.8 Detailed Design

Guidance checklist for the activities and deliverables during the Detailed Design phase:-

Activities

- Agree System Design Specification (SDS)
- Agree methodology for DCS design data management
- Develop Man-Machine Interface Design Specification
- Develop and agree interfaces to other systems
- Obtain design information for ancillary areas, i.e. earthing, UPS, HVAC.
- Obtain reliability analysis of system
- Develop and freeze DCS hardware requirements
- Develop and agree application software requirements
- Develop "ground rules" for configuration and control scheme design
- Design and configure system
- Hold Safety Reviews of system
- Review DCS security

Documents

- System Design Specification (SDS)
- Man-Machine Interface Design Specification
- Vendor specifications
- Vendor configuration manuals
- Vendor operating manual
- Vendor installation planning manual
- Application Software Functional Design Specifications
- Vendor reliability analysis
- Acceptance test procedures
- Application software manuals
- Vendor maintenance manuals
- Hazardous area certification dossiers
- Configuration listings
- Screen dumps

Drawings and Schedules

- Console design and arrangement drawings
- Cabinet arrangement drawings
- Termination cabinet drawings
- Earthing drawings
- Power distribution single line drawings
- Wiring and system interconnection drawings
- Cable schedules
- Termination schedules

C.9 FAT

Guidance checklist for the activities and deliverables during the FAT:-

Activities

- Develop and agree FAT specification in conjunction with the vendor
- Develop and agree FAT schedule and resourcing
- Arrange availability of third party sub-systems and computers where appropriate and feasible
- Carry out paper checks of configuration prior to FAT
- Carry out inventory and bill of material checks
- Carry out hardware testing
- Carry out software testing
- Carry out integrated testing

Documents

- FAT specification
- FAT programme and resourcing plan
- Test scripts for FAT
- Bill of materials - must be latest
- Configuration printouts
- Colour screen dumps
- Application software flowcharts and listings

C.9.1 FAT Specification

The FAT test specification should reflect the structure and phasing of the testing, and will depend on the vendor's scope, for guidance a contents list for a total system supply is given:-

- INTRODUCTION
- OBJECTIVES
- PRE-REQUISITES
- PREPARATION
- TEST PROCEDURE & RECORDING OF RESULTS
- INVENTORY CHECKS
- LABELLING & PRESENTATION CHECKS
- HARDWARE TESTING
 - MODULE TESTING
 - I/O TESTING
 - FIELD TERMINATIONS TESTING
 - POWER, FUSING & EARTHING CHECKS
 - ENVIRONMENTAL TESTS - RFI, Heat, etc.
 - INTERFACES TO OTHER SYSTEMS AND SUBSYSTEMS
 - COMPUTER TESTING
- CONFIGURATION TESTING
 - SYSTEM CONFIGURATION CHECKS
 - I/O DATABASE CONFIGURATION CHECKS
 - MMI CONFIGURATION CHECKS - Displays, Alarms, Trends, etc.
 - CONTROL LOOP FUNCTIONALITY TESTING
- SOFTWARE TESTING
 - INFORMATION & CALCULATION PROGRAM TESTING
 - CONTROL PROGRAM TESTING
 - PLANT COMPUTER PROGRAM TESTING
- INTEGRATED SYSTEM TESTS
 - OVERALL SYSTEM TESTING
 - OPERABILITY TESTING - System response times, etc.
 - SUBSYSTEM TESTING
 - CONTROL SCHEME SIMULATION & TESTING
 - ALARM FLOOD SIMULATION & TESTING
 - FAILURE AND RECOVERY OF REDUNDANT MODULES
 - FAILURE AND RECOVERY OF SINGLE MODULES
 - FAILURE AND RECOVERY OF PLANT COMPUTER
 - FAILURE AND RECOVERY OF SYSTEM
- PROGRAMME
- APPENDICES
 - PRE-REQUISITE CHECKLIST, PREPARATION CHECKLIST, TEST SCRIPTS



C.9.2 FAT - Hardware Testing

Inspection Tests

- labelling and presentation checks
- cabling checks
- correspondence with general arrangement drawings

Module Testing

- hardware test programs
- module failure and recovery testing
- redundancy testing

I/O Testing - consider statistical check here

- correct operation of I/O points at 3 positions on scale
- correspondence of field I/O with configured points

Field Termination Testing

- correspondence with design drawings
- correspondence of field I/O and vendor terminations
- checks on converters and isolators

Power, Fusing & Earthing Checks

- Distribution and feeder checks
- Power consumption checks
- Segregation and Isolation checks
- Insulation & Fusing checks
- Earthing checks

Environmental Testing

- RFI/EMI tolerance tests

System Testing

- Network cable failure tests
- Power Failure tests
- System clock changes

Interfaces to Other Systems and Sub-systems

- Configuration data checks, baud rate, parity, address maps, etc.
- Start-up, shut-down, failure and recovery testing
- Correct correspondence between sub-system and DCS data

Computer Testing

- hardware test programs
- Start-up, shut-down, failure and recovery testing.
- Correct correspondence between computer and DCS data



C.9.3 FAT - Software Testing

System Configuration

- Full off-line paper checks versus approved design information (Pre-FAT)
- Full check comparing the online system with approved design information.

I/O Database (Tags)

- Full off-line paper checks versus approved design information (Pre-FAT)
- Statistical check comparing the online screen version with approved design information. Increase coverage if fault incidence high.

Operator Function Database (Faceplates, Trends, Function Keys, etc.)

- Full off-line paper checks versus approved design information (Pre-FAT)
- Statistical check comparing the online screen version with approved design information. Increase coverage if fault incidence high.

Custom Schematics

- Spot check a selection of colour screen dumps of the built schematics against approved design information. This checks static elements of the schematic and typically picks up errors in the following:-

- Line detail - colour, shape, thickness, intensity, etc.

- Titles

- Display number

- Tag number static aspects

- Target static aspects

- General presentation

- Check schematics on system to ensure the dynamic aspects of the schematic had been correctly built and applied. This typically picks up errors in the following:-

- Tag correctness and updating

- Target vectoring

- Information status presentations, e.g. alarms

Reports/Logs

- Check print-outs for conformity to design and format including:-

- Titles

- Report/Log no

- Tag number correctness

- Dynamic variables

Complete Loop Functionality (For complexities beyond simple cascade)

- Check initialisation, mode changes and correct operation by simulation, e.g.. feeding controller output into the measured variable for all slave loops.
- Check resilience to transmitter failure and general operability.

Interlocks

- Check logic for conformity to design.
- Check operability and presentation to the operator



C.10 Delivery and Installation

Guidance checklist for the activities and deliverables during the Delivery and Installation phase:-

Activities

- Arrange for vendor inspection of DCS equipment and control rooms
 - Check for completions of all ancillary Civil, Electrical, and Instrumentation works necessary for delivery
- Develop and agree delivery and installation plan
 - Develop procedures to prevent ingress of dust and dirt into DCS equipment where necessary
- Review fire precautions for DCS equipment and control rooms

Documents

- Delivery and Installation Plan

C.11 SAT

Guidance checklist for the activities and deliverables during the SAT:-

Activities

- Develop and agree SAT specification in conjunction with the vendor
- Develop and agree SAT schedule and resourcing
- Carry out inventory checks against bill of material and shipping list
- Carry out documentation, drawings, and media checks
- Carry out hardware testing
- Carry out software testing
- Carry out integrated testing

Documents

- SAT specification
- SAT programme and resourcing plan
- Test scripts for SAT
- Shipping List
- Bill of materials - must be latest
- Full system documentation - manuals, drawings, media



C.12 Precommissioning and Loop Testing

Guidance checklist for the activities & deliverables during precommissioning and loop testing:-

Activities

- Plan pre-commissioning and loop test activities with construction and commissioning staff.
- Establish loop testing resourcing, organisation and schedule.
- Develop loop test procedures.
- Generate loop test dossiers.
- Mobilise test teams and familiarise them with test procedures and DCS operation.
- Carry out loop testing.
- Use pre-commissioning test runs to check out & set-up advanced control and sequencing.
- Develop system change control and housekeeping procedures.

Documents

- Loop testing organisation and schedule
- Loop testing procedures
- Loop test dossiers
- System change control and housekeeping procedure.

C.13 Commissioning

Guidance checklist for the activities and deliverables during the commissioning:-

Activities

- Plan and resource DCS commissioning activities in association with operations staff.
- Set up DCS starting parameters for commissioning.
- Prepare documentation packs for Hot loop changeovers (Re-instrumentation).
- Train and prepare operations staff for advanced control loop commissioning.
- Prepare advance control loop operating procedures and write-ups

Documents

- DCS commissioning plan and schedule.
- Hot loop changeover documentation packs. (Re-instrumentation)
- Advanced control loop descriptions and operating procedures.



ABRIDGED AMHAZ METHODOLOGY

AMHAZ is a methodology to identify, and provide recommendations to prevent potential hazards created by disabling alarms in an Alarm Handling Package (AHP). AMHAZ provides the end-user with assurance that the AHP can be safely put into service.

Study Timing	Items to be available:- - functional specification for the alarm management software - operating scenarios in which alarm disablement will be effected together with the process parameters to be to trigger those scenarios - list of alarms to be disabled for each operating scenario <i>(Experience may lead to the situation in which AMHAZ can be applied at the same time as the selection of operating scenarios and selection of alarms to be disabled, i.e. at the initial design stage. This may be both cost and schedule effective by utilising the team making the selections as the core of the AMHAZ team and saving any potential delay to implementation of the system due to changes resulting from the AMHAZ study.)</i>
Team Composition	<u>Core team</u> Chairman <i>experienced in AHMAZ; capable of leading the team; familiarity with the process of the plant to be studied would be beneficial but is not essential</i> CR Operator <i>experienced with the plant to which the AHMAZ relates</i> Process Eng. <i>familiar with the plant to be studied</i> <u>Additional team members</u> Engineer from alarm management system vendor Site Control/ Systems Engineer Site Safety Engineer
Documents Required	Functional Design Specification for the alarm management system which includes details of the operating scenarios for disablement, the operating parameters selected to identify the scenarios and the lists of alarms to be disabled. Up-to-date Process and Instrumentation Drawings (P&IDs) for the plant Cause and Effect charts for the plant HAZOP and / or CONSOP study of the plant



Getting Started	Familiarisation with the process and control details of the plant from drawings and documentation. Presentation by someone closely involved in the design on the specific proposals Chairman should then describe the AMHAZ methodology and the manner in which the study will be conducted
Perform Study	Operating scenarios:- Taking each operating scenario in turn, discuss the operating parameters selected to identify each scenario in the AHP. Agree if the proposed operating parameters uniquely identify the scenario or if other operating conditions would also be identified. The scenarios addressed should include the 'default' or 'fallback' scenario (which, in most cases, would be expected to enable all alarms) and discuss all the conditions under which that scenario would be selected. e.g. normal operation of the plant, failure or false signals on the input to the alarm management system, failure of the alarm management system itself. The alarms to be disabled - Led by the chairman the team decide on which operating scenario to address first, e.g. start-up, heat-off, feed trip, etc..<i>(There is likely to be more than one operating scenario to be addressed in the study and to focus the concentration of the team, it is recommended that if there are more than two scenarios then all the alarms are studied for one operating scenario before moving on to the next scenario. If there are only two scenarios it may be possible to consider each alarm for both scenarios before moving on to the next alarm. If in doubt, one scenario at a time should be the rule.)</i> - The chairman selects the first alarm to be studied and the team identify it on P&IDs and agree on its basic purpose(s), e.g. it is a high temperature alarm to warn that a product rundown temperature is getting too high and could cause a problem in the storage tank - The HAZOP and / or CONSOP report for the plant is checked for any specific requirements for this alarm. - The team then consider the effect of the alarm being disabled under the operating conditions pertaining to the scenario being studied. The chairman should lead the team considerations by structuring a series of questions to the team as well as allowing free-ranging team discussion of the impact of disabling the alarm. The structured questions to the team should include:-

- For the selected operating scenario, is the loss of the agreed basic purpose of the alarm likely to create a hazard or lead to an operational difficulty?
 - Is the alarm used for a purpose other than the agreed basic purpose, i.e. is it used to infer a problem elsewhere, and, if so, does loss of the alarm for the inferred purpose create a potential hazard or operational difficulty?
 - Is there another alarm which will provide similar information, e.g. a pump stopped alarm and a pump discharge low flow alarm could, in many circumstances, provide the same information to the control operator, and, if so should one, other or both be disabled?
 - Is there any other potential hazard or operability problem created by disabling this alarm?
- (e) If any potential hazards or operability problems are identified a record is made on the AMHAZ log sheet to identify the potential hazard or operability problem and to make a recommendation for change.
- (f) The chairman then leads the team through steps b) to e) for the other alarms proposed to be disabled in the selected operating scenario.
- (g) When the first operating scenario has been completed, steps a) to f) are repeated for each remaining operating scenario.

Reporting

The main study reporting will be on report sheets. As a minimum, the report sheet should include:-

- alarm tag identification
- function of the alarm
- operating scenario considered
- implication on the plant if the alarm is disabled (relating to the operating scenario being considered)
- any additional function which is inferred from the alarm
- any other alarm from which the function of the alarm being considered can be inferred
- any potential hazard or operability problem identified
- any recommendation or comment

In addition to the report sheets, the AMHAZ report should include the following:-

- brief details of the application including identification of the plant and the application vendor/ system name
- a list of the team members and any advisers, the documents



used, the timing and location of meetings

- a statement of the recommendations and conclusions of the study team including a statement that, subject to satisfactory resolution of the recommendations contained in the report, the application can be put into service safely.

(It is anticipated that the text element of the report will be quite brief and the main information will be contained in the report sheets.)





BP SITE / ASSET

SOFTWARE CHANGE REQUEST FORM

Change Request Serial Number

1. DESCRIPTION OF CHANGE REQUESTED (All relevant drawings must be attached)

2. ORIGINATED BY:DATE:

3. IMPACT OF CHANGE ON DCS / OTHER SYSTEMS:

4. SAFETY CHECKS

Encircle as Appropriate

HAZOP Required?	YES	NO
PMP Required?	YES	NO
Alarm Handling Impact?	YES	NO
Change Permanent? (if No specify in section 3)	YES	NO

5. RELEVANT DOCUMENTATION UPDATED

Sign

Alarm & Trip Schedule	I	
Register of Safety Related Devices	P	
P+IDs	P	
Loop Diagrams	I/S	
Operating Procedures	O	

6. Approved By: (Sign and Date)

Operations Engineer (O)

Process Engineer (P)

Instrument Engineer (I)

Systems Engineer (S)

Above signatures are mandatory and Letter code signifies responsibility for completion of section 5

Systems Control Engineer

Other

7. IMPLEMENTATION COMPLETED

Sign and Date

SYSTEM CONFIGURATION	
SOFTWARE	
WORK BACKED-UP	



**BP SITE/ASSET
SOFTWARE CHANGE REQUEST FORM**

Notes for Completion of Software Change Request Form

Section 1 Originator to complete this section giving a description of the change required.

Section 2 Originator to print his name and date request.

Section 3 Any person who is party to completing the SCR should detail impact on DCS or other systems affected by the requested change.

Section 4 Any person who is party to completing the SCR should note the impact of any safety implications with respect to the requested change. It is then incumbent on the senior signatory authority in the process area of the requested change, as to the requirement for safety checks/audits. Encirclements should be initiated by the Engineer making the comment.

Section 5 This section should be completed by the discipline Engineer identified by the Discipline Letter Code adjacent to the document type that may need updating. It is incumbent on the identified discipline to ensure that the relevant documentation is updated.

Section 6 Approvals should be signed for as appropriate. For simple changes all signatory disciplines may not be needed. In such cases the discipline deeming that another discipline does not need to authorise the change should p/p for that discipline.

Section 7 Record of the completed work should be signed for and dated.

Additional Comment Space

SUBSEA CONTROL SYSTEMS

The old Section 4, Subsea Control Systems, has been removed from this latest (February 1998) issue with the intention of producing a separate document covering Subsea Control Systems or a new Subsea document with a section within it covering Subsea Control Systems.

