



Project No.	5232
Specification No.	13450

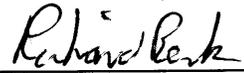
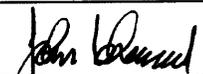
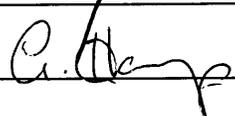
Advanced Mixed Waste Treatment Plant

**CONTROL SYSTEM USER REQUIREMENT
SPECIFICATION**

(Original document reference DD/K0105C/SYST/00007_02)

BNFL Inc.

Status: Final Design Issue (for approval)	Revision No. 0	Date: 1/9/01
Q - Listed: No		

Originator: Nicholas Doyle		Date	1/24/01
Checker: Richard Beck		Date	1/24/01
Verifier (Q-Listed only): N/A		Date	
Lead Discipline Engineer: Richard Beck		Date	1/24/01
Department Manager: John Isherwood		Date	1/29/01
Operations Manager: Martin Wheeler		Date	1/30/01
Project Manager: Grenville Harrop		Date	1/30/01

Circulation list

Purpose of issue: 1 For comment
 2 For action
 3 For information

Name	Location	No of copies	Remarks	Purpose of issue
C. Davis	BEL	1		3
M.Houghton	BEL	1		3
P Atkinson	BEL	1		3
G. Harrop	BNFL Inc.	1		3
J.Isherwood	BNFL Inc.	1		3
J. Reed	BNFL Inc.	1		3
G. Daniels	BNFL Inc.	1		3
R.Beck	BNFL Inc.	1		3
H. Neal	MK	1		2
T. Dallas	MK	1		2
M. Wheeler	Idaho Falls	1		3
I.Milgate	Idaho Falls	1		3
A. Exley	Idaho Falls	1		3
P.Young	Idaho Falls	1		3



History sheet

Rev	Date	Reason for revision	Revised by
00	December 2000	Further comments from issues 01 & 02 incorporated. Document ownership transferred from BEL to BNFL Inc.	N.S.Doyle

Notes on Revision 00

The document was created by BEL as document DD/K0105C/SYST/00007_C and has now been allocated a new BNFL Inc Specification number (starting at Rev 00). The Specification does not follow the format laid out in the PQP 6.10 Section 4.2.1.1 as this format is not appropriate for a software system.

Contents

Item	Page
Circulation list	2
History sheet.....	3
Contents.....	4
1 Introduction, Objectives and Scope.....	10
1.1 Introduction	10
1.2 Objectives.....	10
1.3 Scope	10
2 References	11
3 Definitions	12
4 Process & Control System Overview.....	13
4.1 Process Overview	13
4.2 Control System Overview	14
4.3 Major System Features.....	17
4.4 Control System Architecture	17
4.4.1.1 Layer 1: Front End Control.....	18
4.4.1.2 Layer 2: Supervisory Control (SCADA)	19
4.4.1.3 Layer 3: Data Management System Layer*.....	19
4.4.2 Central Control.....	19
4.4.3 Local Control	20
4.4.3.1 Use of local control to facilitate operations requiring direct viewing.....	20
4.4.3.2 Operational Facilities to be provided by local control.....	20
5 Systems Objectives.....	22
5.1 Safety.....	22
5.1.1 Emergency Stop	22
5.1.2 Glovebox Protection Switches	22
5.1.3 Power Failure.....	22
5.1.4 Control Processor Failure.....	23
5.1.5 Fire.....	23
5.1.6 Criticality	23
5.1.7 Ventilation Failure.....	23
5.2 Access and Security.....	24
5.2.1 Configurable Access Constraints	24
5.2.2 View Only	24
5.2.3 Operator	24
5.2.4 Team Leader.....	25
5.2.5 Engineer	25
5.2.6 System Administrator.....	25
5.3 Virus Scanning	26

5.4	Diagnostics	26
5.4.1	Control System Hardware Diagnostics	26
5.4.2	Software Diagnostics - Sequences	26
5.4.3	Software Diagnostics - Devices	27
5.5	Alarms	28
5.5.1	System Alarms	29
5.5.2	Plant Alarms.....	29
5.5.2.1	<i>Plant Alarm Types</i>	29
5.5.2.2	<i>Distribution of Alarms</i>	30
5.5.3	Alarm Priorities.....	30
5.5.4	Alarm Thresholds.....	31
5.6	Start Up and Shut Down Functions	31
5.7	Control Functions	32
5.8	Degraded Operation and Failure Modes.....	32
5.9	Data Management.....	32
5.9.1	Real Time Process & Plant Status Data.....	33
5.9.2	Data Retrieval and Analysis Requirements	33
5.10	Trending	34
5.11	Prompt Messages.....	34
5.12	Event Messages	34
5.13	Tracking Data Handling	34
5.14	Data Management System Data Handling.....	34
5.15	Equipment	35
5.15.1	Workstations	35
5.15.1.1	<i>Central Control Room and Back-up Monitoring Room Workstations</i>	35
5.15.1.2	<i>Fixed Workstations</i>	35
5.15.1.3	<i>Portable Workstations</i>	36
5.15.1.4	<i>General Considerations</i>	36
5.15.2	Printers	36
5.15.3	Power	37
6	Functions And Facilities.....	38
6.1	SCADA Functions.....	38
6.1.1	SCADA Displays.(i.e. SCADA generated displays).....	38
6.1.1.1	<i>Plant Displays</i>	38
6.1.1.2	<i>Forms and Reports</i>	40
6.1.1.3	<i>Trends</i>	41
6.1.1.4	<i>Utilities</i>	41
6.1.2	SCADA Display Standards	42
6.1.2.1	<i>Screen Layout</i>	42
6.1.2.2	<i>Toolbar Area</i>	42
6.1.2.3	<i>Alarm Area</i>	42
6.1.2.4	<i>Screen Area</i>	43
6.1.2.5	<i>Operator Message Display Facility</i>	43
6.1.2.6	<i>Dialog Area</i>	43
6.1.2.7	<i>Color Standards</i>	43

6.1.2.8	Numeric Displays.....	43
6.1.2.9	Analogue Alarm Limit Display/Edit.....	43
6.1.2.10	Movement of Mechanical Plant.....	44
6.1.2.11	Pop-up Windows.....	44
6.1.2.12	Fonts.....	44
6.1.2.13	Device Animation.....	44
6.1.3	Device Control Faceplates.....	45
6.1.3.1	The Device Control Faceplate (Level 4.5).....	45
6.1.3.2	Diagnostics Faceplate (Level 5).....	47
6.1.4	Sequence Selection & Control.....	48
6.1.4.1	General Requirements.....	48
6.1.4.2	Selection of (Scheduler)Sequences.....	48
6.1.4.3	'Sequence Control Faceplate'.....	48
6.1.5	Alarms.....	51
6.1.5.1	Alarm Banner.....	51
6.1.5.2	Alarm Summary List.....	52
6.1.5.3	Historical Alarms.....	52
6.1.6	User Access.....	53
6.1.7	Mode Selection.....	54
6.1.8	Event Logging.....	54
6.1.9	Sequence Messages and Prompts.....	55
	Message summary list.....	55
6.1.10	Context Sensitive Forms.....	55
6.1.11	Printing Facilities.....	55
6.1.11.1	Screen Printing.....	55
6.1.11.2	Reports.....	56
6.1.12	Development Facilities.....	56
6.1.13	Algorithms.....	56
6.2	PLC Functions.....	56
6.2.1	Automatic Sequences - Description.....	56
6.2.1.1	Sequence Control.....	57
6.2.1.2	Sequence Failure and Recovery actions.....	58
	Recovery.....	59
6.2.2	Devices.....	61
6.2.2.1	Device Failure and Recovery actions.....	61
6.2.2.2	Device Controller Specification.....	62
6.2.3	Interlocks.....	62
6.2.4	Control Modes.....	62
6.2.4.1	PLC Fault Mode.....	62
6.2.4.2	Update Mode.....	63
6.2.4.3	Manual Mode.....	64
6.2.4.4	Auto Mode.....	64
6.2.4.5	Auto Mode with 'Step' function enabled.....	64
6.2.4.6	Stand-By Mode.....	65
6.2.5	Generic Functions.....	65

6.2.6	Serial Links	66
6.2.7	Development Facilities.....	66
7	System Interfaces	67
7.1	Operator Interfaces.....	67
7.1.1	Workstations	67
7.1.2	Stand-by Control Panels.....	68
7.1.3	Operator Control Consoles.....	68
7.1.4	Visual Information Displays	68
7.1.5	Hard Copy Output	68
7.1.6	Audible Annunciation	69
7.2	Plant interfaces	69
7.2.1	Digital Inputs	69
7.2.2	Digital Outputs.....	69
7.2.3	Analog Inputs.....	70
7.2.4	Analog Outputs.....	71
7.3	Inter-system Interfaces	72
7.4	Communications Networks	73
8	System Environment	74
8.1	Plant Layout	74
8.2	Environmental Conditions.....	74
8.2.1	Site Conditions.....	74
9	System Attributes	75
9.1	System Performance.....	75
9.1.1	System Start-up.....	75
9.1.2	System Shutdown.....	75
9.1.3	PLC Response.....	75
9.1.4	Digital State Update	76
9.1.5	Display Update.....	76
9.1.6	Alarm Display.....	76
9.1.7	Alarm Burst.....	76
9.1.8	Alarm Loss.....	76
9.1.9	Processor Loading.....	76
9.2	Data Criteria	77
9.2.1	Natural Language.....	77
9.2.2	Data Capacity.....	77
9.2.3	Data Retention.....	77
9.2.4	Data Format.....	77
9.2.5	Data Validation	77
9.2.6	Archiving Requirements	77
9.3	Availability.....	78
9.4	Reliability.....	78
9.4.1	Hardware and Software failure.....	79
9.4.2	System Recovery.....	79
9.5	Maintainability	79
9.5.1	Lifespan.....	79

9.5.2	Maintenance requirements	79
9.5.3	Diagnostics.....	79
9.5.4	Support.....	80
9.6	Adaptability	80
9.7	Expansion.....	80
10	Training.....	81
10.1	Engineer Training Course	81
10.2	Operator Training Course.....	81
11	Documentation.....	82
11.1	Documentation to be provided by Supplier to BNFL Inc.	82
11.2	Documentation Standards.....	82
12	Testing.....	84
12.1	Sources of Test Documentation.....	84
12.2	Simulation Equipment.....	84
12.3	Testing Phases.....	85
12.3.1	Device Template Testing.....	85
12.3.2	Device Template CAT.....	85
12.3.3	Module Testing.....	85
12.3.4	Mimic Approval.....	86
12.3.5	Pre CAT System Testing (Using Plant Simulation).....	86
12.3.6	CAT System Testing (Using Plant Simulation).....	86
12.3.7	Pre-CAT Integration Testing (Using Simulators).....	86
12.3.8	Integration CAT (Using Simulators) – without DMS.....	87
12.3.9	ICS - DMS Integration CAT (Using Simulators) – with DMS.....	87
12.3.10	SAT Testing.....	87
12.3.11	Commissioning SPD's.....	87
13	Installation and Commissioning.....	89
14	Commercial Considerations	90
14.1	Project Milestones.....	90
14.2	Scope Of Supply.....	90
14.3	Exclusions From The Scope Of Supply.....	90
14.4	Preferred Equipment.....	91
14.4.1	Software.....	91
14.4.2	Hardware.....	91
14.5	Deliverables.....	92
14.6	Methods & Approaches.....	92
14.6.1	Use of CONCISE - General.....	92
14.6.3	Prototyping.....	92
14.7	Compliance With Specification.....	92
14.8	Implementation Techniques	93
Appendix 1 - Building Layout Drawings		1
Appendix 2 – Ergonomics Requirements and Guidelines for VDU-Based Operator Interfaces.....		1
1	Introduction	4
2	Scope.....	5
3	Definitions.....	6

Appendix 3 –AMWTP Control System Architecture (Indicative)	1
Appendix 4 – SCREEN LAYOUT EXAMPLES.....	1
Appendix 5 – System Size.....	1
Estimate of total I/O	1
Estimate of number of Plug in points	3
End of Document	4

1 Introduction, Objectives and Scope.

1.1 Introduction

This document defines requirements for the Integrated Control System (ICS) for the Advanced Mixed Waste Treatment Project (AMWTP) at the Idaho National Engineering and Environmental Laboratory (INEEL) Radioactive Waste Management Complex (RWMC).

The document is structured to provide an overview and also to detail specific system requirements and performance criteria for the Integrated Control System (ICS). The ergonomic requirements and hardware requirements are detailed in the appendices.

1.2 Objectives

The purpose of this document is to define the requirements for the ICS. These consist of:-

- Main functional requirements
- Detailed design and documentation requirements
- Required Standards to be used

1.3 Scope

The scope covers the analysis, design, procurement, build, test and setting to work of the ICS, applied across the whole of the defined AMWTP facility systems outlined in tables 1 & 2 of section 4.2 and Appendix V (see also section 14.3 for exclusions).

Note. Throughout this document the word **shall** indicates a mandatory requirement to be fulfilled by the system integrator/supplier.

2 References

No	TITLE / DESCRIPTION	DOC. REFERENCE No.	REV
Main System Descriptions			
1	Project Design Criteria	BNFL-5232-PDC-01	2
2	Control Philosophy	DD/K0105C/SYST/00004	05
3	Systemization Philosophy	DD/K0105C/SYST/00001	02B
Detail Specifications			
4	General Specification for Cubicles, Panels and Junction boxes	SP_K0105C_SYST_00004	02
5	Programmable Electronic System Based Instrumentation & Control	NF 0069/3	Issue 2.
6	Tagname Structures For Mechanical Handling Systems	DD/K0105C/SYST/00025	00
7	Preparation of System C.E & I Maintenance Manuals	SP_K0105C_MK_PROJ_00006	00
8	Preparation of System Operation Manuals	SP_K0105C_PROJ_00004	01
9	Quality Assurance Requirements FOR Non-Q listed Equipment	SP_K0105C_MK_PROJ_00011	03
10	General Specification for Emergency Stop Systems	SP_K0105C_SYST_00007	03
11	Preparation of Recommended Spares Schedules	SP_K0105C_PROJ_00007	00
12	Data Sheet for DMS Workstations in SCW Areas	BNFL Inc No. 440-1-04	01
13	Consistent approach to the use of the CONCISE specification tool	70G009	A

3 Definitions

ALLMW	Alpha Low Level Mixed Waste
AMWTP	Advanced Mixed Waste Treatment Project
AMWTF	Advanced Mixed Waste Treatment Facility
BEL	British Nuclear Fuels Engineering Limited
BMR	Back-up Monitoring Room
CAT	Customer Acceptance Test
CCR	Central Control Room
CCTV	Closed Circuit Television
DMS	Data Management System
EDMS	Electronic Document Management System
GUI	Graphic User Interface
GSSS	Global System Software Specification
ICS	Integrated Control System
IEC	International Electrotechnical Commission
ILW	Intermediate Level Waste
INEEL	Idaho National Engineering and Environmental Laboratory
LLW	Low Level radioactive Waste
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
PC	Personal Computer
PES	Programmable Electronic System
PLC	Programmable Logic Controller
POS	Plant Optimization System
PSU	Power Supply Unit
PVCS	Polytron Version Control System
RWMC	Radioactive Waste Management Complex
SAT	Site Acceptance Test
SCADA	Supervisory Computer System
SCW	Special Case Waste
SDD	System Definition Document
SPD	System Performance Demonstration
SRN	Snag Rectification Note
TBD	To Be Determined
TSA-RE	Transuranic Storage Area Retrieval Enclosure
TQ	Technical Query
UPS	Uninterruptible Power Supplies
URS	User Requirement Specification
VDU	Visual Display Unit
WIPP	Waste Isolation Pilot Plant
WTS	Waste Tracking System

4 Process & Control System Overview.

4.1 Process Overview.

The purpose of the Advanced Mixed Waste Treatment Project is to treat alpha low level mixed waste (ALLMW) and Transuranic Waste, currently stored in drums and boxes in the Transuranic Storage Area (TSA-RE) at Radioactive Waste Management Complex, to a standard suitable for final disposal. The facility shall have the capability to treat specified INEEL waste streams, with the flexibility to treat other potential INEEL and U.S. Department of Energy regional and national waste streams. The waste product is to meet the applicable Waste Isolation Pilot Plant (WIPP) waste acceptance criteria and thus be suitable for disposal at WIPP.

The process involves retrieval of the waste from the storage area, characterization in the Type I module, storage in the Type II modules, pre-treatment (sorting) and treatment (supercompaction).

Pre-treatment and treatment facilities are provided within the new AMWTF building. AMWTF will accept retrieved waste in drums and boxes, manually sort and repackage the waste in drums using remote handling equipment and then supercompact or incinerate or directly export the sorted waste and finally export the waste in 55 or 83 gallon product drums. Throughout the process, drums and boxes shall be tracked and product quality records providing a complete record of the waste in each drum, box or product drum shall be maintained.

See AMWTF Facility Description BEL, RP/K0105C/PROC/00012 for detailed descriptions.

The concepts of process 'areas' and process 'systems' are used throughout this specification. For definitions of these, reference should be made to document 'Systemization Philosophy', ref. no. DD/K0105C/SYST/00001.

4.2 Control System Overview

The control system shall provide functional control for the systems* listed in table 1 below -

[*N.B. where 'systems' are defined in document 'Systemization Philosophy' - ref. 4]

<u>Process System* No.</u>	<u>Process System* Description</u>
210	Characterization
310	Clean Drum and Waste Box Import
320	Box Import
330	North Box Sort Line
335	North Box Line Conveying
340	South Box Sort Line
345	South Box Line Conveying
350	Box Size Reduction
370	Central Drum Conveying & Marshaling
390	In Plant Drum Assay
410	Supercompaction
420	Puck Handling
422	Drum Import / Export
423	Waste Import to Supercompaction and Sort
440	Special Case Waste
600	Utilities /Miscellaneous
720	Zone 1 Supply/Extract East
740	Zone 2 Supply/Extract East
760	Zone 3/Glovebox Extract East

Table 1

In addition, the control system will interface for status with the systems listed in table 2 below: -

<u>Process System No.</u>	<u>Process System Description</u>	<u>Interface</u>
630	Fire Protection	Status main alarm signals from these service systems to be connected to the ICS for alarm indication and logging purposes. Estimated approximately 60 signals will be required. Utilities will have its own PLC located on the area 700 server.
632	Fire Sprinkler System	
633	Fire Sprinkler System –Water	
634	Fire Suppression-Gas	
640	Process Cooling Water	
650	Steam and Condensate for HVAC and Process	
660	HVAC Heating & Cooling	
661	HVAC Chilled Water	
662	HVAC Hot Water	
670	Compressed Air and Vacuum	
671	Plant Air	
672	Instrument Air	
673	Breathing Air	
674	Vacuum	
680	Gases	
681	Nitrogen	
682	Propane	
690	Non-Process Area HVAC	
805	138KV Overhead Line & Substation	
810	Main Power Distribution	
812	Standby Power	
813	Emergency Power	
814	UPS Power	
811	Lighting & Convenience power	No direct ICS interface
820	Lighting & Surge Protection	
840	Data Management System	System 840 interface to be defined by BE Ltd. Interfaces to be through the PLC SCADA – no wired signals other than network cabling will be required
841	Waste Tracking System	No direct ICS interface
842	Information Acquisition system	
843	Management Information System	
844	Process Optimization System	
845	Electronic Data Management System	

846	Fissile Tracking System	FTS initiated interlocks will be detected by ICS to inform plant operators
850	Communications	Independent system -no ICS interface
860	CCTV	Independent system -no ICS interface
870	Access Control	Independent system -no ICS interface. Hold cell access may need to interface to ICS. Approaches to be confirmed and principles to be developed.
875	Fire Detection & Alarm	Independent system. Fire dampers status (open or closed)will input into ICS. Hardwired emergency stop systems can be utilized to stop equipment if required.
880	Building Evacuation	Independent system -no ICS interface. Separate alarm indications in CCR & BMR
890	Radiological Surveillance System	Independent system -no ICS interface. Separate alarm indications in CCR & BMR
891	Criticality Incident Detection	Independent system -no ICS interface. Separate alarm indications in CCR & BMR
892	Stack Monitoring	Stack Monitoring instrumentation signals are to be connected to the ICS via the Utilities/Misc. PLC. Project requires this information to allow reporting of aerial discharges.
893	Change Room Equipment	Status Alarms to be connected to ICS for alarm indication and logging purposes. Interface via Utilities/Misc. PLC

Table 2

4.3 Major System Features.

The ICS/DMS network provides the following main area's of functionality:

ICS	DMS
Supervisory functions	Plant wide Waste Tracking
Mode selection	Quality Control and Quality Assurance Data
Plant mimics	Process Data
Alarms	WIPP shipping data
Data Communications	Data Storage (Archive /Retrieval)
Interfacing with the DMS and other Programmable Electronic Systems	
Front end PES logic control	
Local tracking (limited capability only)	

The overall control system **shall** contain the following key features:

1. PLC's, allocated to control specific plant or process areas, to provide plant systemization and autonomy during a fault situation in another area.
2. A unified Operator Interface via the use of area CCR workstations, fixed local workstations or portable workstations, each workstation **shall** have the same design and functionality to provide an operator interface that has the same 'look and feel' plant wide.
3. A robust, proven communication network to support the control system infrastructure.
4. Plant and system diagnostic facilities to identify the source of plant failures and effectively reduce plant downtime and repair costs.
5. Ability to launch an Electronic Documentation Management System (EDMS) application for the storage/retrieval of plant manuals (operator, maintenance and emergency instructions) and live plant and product documentation.
6. Overview information to supplier/customer plants and other external computer systems.
7. On-line configuration / software programming facilities and debugging tools.
8. Limited function local tracking system .

4.4 Control System Architecture

The requirements stated above can be split into two functional layers that constitute the Integrated Control System (ICS) which interfaces to external systems in layer 3. This is depicted in Figure 1.

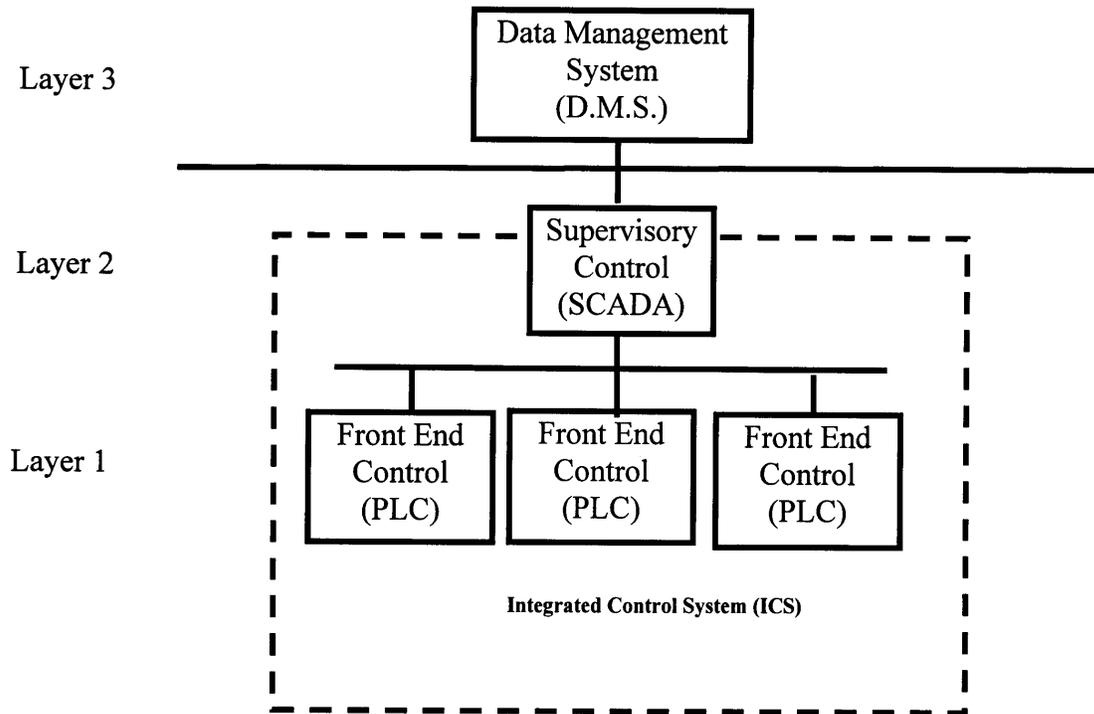


Figure 1. Hierarchy of Control System on AMWTP.

4.4.1.1 *Layer 1: Front End Control*

This layer provides the front end control and co-ordination of each system's production equipment. The PLC's shall be located along with the system's electrical and instrument plant room equipment which shall be as close as possible to the mechanical equipment for each system. Its purpose shall be to provide sequential logic operations and software interlocks required to operate the plant. In addition it shall interface with front end instrumentation for acquisition and validation of data as required for the functions performed by layers 2 and 3 described below. Local operator workstations shall be provided where required and shall be located close to the plant equipment. The basis for the front end control shall be a number of scheduler* and group* operations in each system which shall be enabled by the operator as required and may require operator involvement at specified points until its conclusion. [*A more complete description of scheduler and group operations is provided in section 6 of Control Philosophy document – ref 2.]

The schedulers and groups shall be required to take logical 'decisions' dependent on:

- data supplied from layer 2
- operator decisions input via workstations

- programmed process decisions based on data derived from plant instrumentation

It is intended that sufficient data should be supplied to the scheduler from the layer 2 initially to allow the scheduler to complete without the requirement for further transfers. The reasons for this are:

- more efficient use of data links i.e. small number of transfers of large amounts of data
- once the scheduler commences control of mechanical equipment there shall be no need to wait for a response from the layer 2 (except for designed pauses for operator responses)
- if required by a particular system the scheduler can complete without layer 2

4.4.1.2 *Layer 2: Supervisory Control (SCADA)*

The hardware associated with this function shall be located in the AMWTF Computer Room. It's purpose shall be to act as the main Operator Interface to the plant, and all external programmable systems via the Data Management System.

4.4.1.3 *Layer 3: Data Management System Layer**

[*Note : Layer 3 (DMS) is OUTSIDE the scope of this document but description included here for completeness and clarification]

This layer provides a direct interface to on-line operational data for the management and operations staff. Facilities provided include a database of all waste within the process, long term data archiving and a gateway to other computer systems. The hardware associated with this function shall be located in the AMWTF computer room.

4.4.2 Central Control

A Central Control Room **shall** provide facility for control of areas / systems as detailed in section 4.2., Control System Overview.

Process Ventilation **shall** have limited, hard-wired control and indication facilities available for operation of this equipment independently from the ICS under 'Standby' mode (see section 6.2.4.6), as described within 'Control Philosophy' document (ref.2). These facilities **shall** be provided on the Central Control Room Stand-by control panel and also on the Back-up Monitoring Room Stand-by control panel.

4.4.3 Local Control

4.4.3.1 *Use of local control to facilitate operations requiring direct viewing*

The philosophy is that where an operation requires direct operator viewing, control **shall** be effected from *either* fixed local control workstations *or* portable workstations local to the equipment. Either type of local workstation may also be supported by Closed Circuit Television viewing if required.

Direct viewing, and therefore local control, would routinely be required under the following circumstances:

- Where the normal operations at a station are dependent upon operator interaction, for example drum swabbing, power manipulator & master slave manipulator operations.
- Where direct viewing of equipment is required for maintenance operations e.g. for 'inching' control on individual drives after maintenance on, say, a turntable.

4.4.3.2 *Operational Facilities to be provided by local control*

Local control workstations*(see note 2 below) **shall** provide the operational facilities listed below, subject to appropriate user configuration (refer to Note 1 below and sections 5.2, 6.1.1.4 and 6.1.6 :-

- The use of a single local workstation to log onto and then **control** or **view** any one of a number of machines / systems.
- **Control** of a single machine / system from a number of different workstations, where for each separate workstation, its particular user is logged onto the system for the machine / system being controlled.
- Access for local **viewing** of Operations & Maintenance documentation.

[Note 1 - Facilities **shall** be provided to enable 'limitations to functionality' to be applied by means of user / workstation / system **configuration**. For example, Operator 'A' at local workstation in North Box Line may not be permitted to control Drum Line. Such restrictions shall be implemented, and subsequently amended if required, on a case-by-case basis by the system administrator]

*Note 2 : the local operator workstations fall into two categories: fixed and portable.
Fixed -

All local positions that regularly require operator control functions **shall** be provided with a fixed local workstation. This **shall** be a Personal Computer (PC) based workstation, which is capable of providing similar functionality as available on the central control room workstations.

Portable -

Portable workstations **shall** be used at operating windows that only **occasionally** require control functions, e.g. for maintenance. Plug-in points for portable workstations **shall** be provided at all plant windows that do not have a fixed local workstation and at other designated points as required. For each network plug-in point, the control system **shall**, by configuration, facilitate control access restriction to nominated user(s) and systems to be applicable to that point, regardless of whether or not a portable workstation is plugged into it.

Portable workstations shall also have the same functionality as the fixed workstations.

Where the local operator workstation requires the use of industrially hardened PC's, then the operator interface **shall** also be able to provide the operator with on-line plant diagnostics and Operations & Maintenance manuals via access to the Data Management System facilities.

All central control room, fixed and portable operator workstations **shall** have the same 'look and feel'.

5 Systems Objectives

5.1 Safety.

The design of the control system **shall** incorporate statutory safety facilities, (non 'Q'-listed¹), including the following:

5.1.1 Emergency Stop

Each machine or system **shall** be provided with hard-wired emergency stops whose primary function are independent of software or electronic logic. The location of such stops local to the equipment shall obviously depend on the machine's physical and operational characteristics. Activation of an emergency stop **shall** safely stop* the equipment in the area (room). System emergency stops and associated displays **shall** be provided in the Central Control Room and Back-up Monitoring Room. For diagnostic purposes, the status of all emergency stop circuits **shall** be monitored by the PLC.
[* Note - see section 5.1.8]

The emergency stops will be of the 'push to latch', 'twist to release' type and can therefore be reset locally. Affected equipment **shall** not automatically restart but **shall** have to be re-started by the operator either locally, from the Central Control Room or Back-up Monitoring Room as appropriate.

All emergency stops **shall** be designated priority 1 alarms (see section 5.5). The emergency stop loop label **shall** identify its approximate location.

5.1.2 Glovebox Protection Switches

Gloveboxes containing moving machinery will be fitted with isolation switches. These will interrupt power to the machinery inside the glovebox when an operator moves his hand inside. The switches **shall** be designated priority 1 alarms. The glovebox protection switch loop shall identify its approximate location.

5.1.3 Power Failure.

On re-establishment of power the plant **shall** not automatically restart.

¹ Q listed items are defined as those items identified as having the potential for significant off-site or on-site consequences, based on safety class designation.

5.1.4 Control Processor Failure.

Front end PES control processors **shall** be monitored by external hard-wired watchdog devices that shall constantly monitor processor 'heartbeats'. Failure of a processor heartbeat **shall** cause all outputs to be disconnected from plant devices except for the watchdog output and status indicating outputs. This is subject to the following caveat:- In 'process' areas such as Ventilation, the reaction to processor failure shall be to effect these outputs to their **safest** state (i.e. Off or Current) as appropriate with regard to safety. The 'safest state' can vary from system to system. For mechanical systems this means interrupting the power to the device while HVAC systems need to be kept running. The relevant definition of 'safest state' will be given in each individual CONCISE package on an item by item basis.

Watchdog relay status **shall** be displayed locally using an indicating lamp, and reset **shall** only be possible via a local key-switch.

The supervisory system **shall** also monitor PLC control processors by the use of software watchdogs, the status of which **shall** be displayed along with the hard-wired watchdog status on an appropriate mimic/s.

5.1.5 Fire.

The system will not react automatically to fire alarms. Plant operator procedures will determine what is the appropriate course of action in any given situation.

5.1.6 Criticality.

The system will not react automatically to criticality alarms. Plant operator procedures will determine what is the appropriate course of action in any given situation.

5.1.7 Ventilation Failure.

The ICS system will not react automatically to ventilation failure. Plant operator procedures will determine what is the appropriate course of action in any given situation. Some plant equipment may have intrinsic safety requirements. The impact on the ICS of plant area's that have potentially explosive atmospheres has yet to be determined.

5.2 Access and Security.

All plant area's are potentially accessible from any workstation, this access will be restricted via the use of access level and access port restrictions. These access levels will be defined by the administrator as required. This will be allocated via a battleship diagram defining the user, location and controllable systems. This diagram will be developed in the GSSS and SDD.

The design of the control system **shall** incorporate five levels of Control System access, comprising a 'view only' facility and four restricted control access levels to afford security. These are listed below:-

1. View Only)
2. Operator)
3. Team Leader) Access to all levels
4. Engineer) **shall** be via a password system.
5. System Administrator)

Entry access to any operating level **shall** be logged to the DMS

5.2.1 Configurable Access Constraints

Details of user access facility utilization and constraints are provided in section 6.1.6., subject to the following specific objective:

A configurable facility shall be provided – available under the 'Edit System Access Control' option in 'Utilities' menu as described under section 6.1.1.4. - to limit access to a specific process system(s), and / or sequences therein as appropriate, to:

- Nominated user(s),
- Nominated CCR console or workstation(s)

Each level of access **shall** allow (or restrict) facilities listed in the following sections. The facilities attributable to each access level shall be configurable by the system administrator, but indicative examples are set out below: -

5.2.2 View Only

The 'View Only' access level with no control functions **shall** be provided when none of the other operating levels are selected, subject to location. This shall allow view only access to all displays

5.2.3 Operator

The 'Operator' will be allowed access to all functions of 'view only' access plus the following :

- Assignment of trends and sample rates

- Acceptance of alarms (subject to constraints listed in section 5.6)
- Change of control modes*
- Control of plant operations in Automatic and Manual mode. *

[NB! * 'Changing modes' and 'control of plant operations in automatic mode' by operator shall exclude the ability to abort process system sequences.]

5.2.4 Team Leader

The Team Leader access level, allowing all functions available to the Operator plus:

- Aborting 'Process System' sequences, e.g. Process Ventilation system 710.
- Changing of process alarm level values
- Changing of limit parameters (set points & value limits)
- Update tracking system

Note: While the ICS will track 'Device Manual Mode' steps forward, it cannot track steps back. Therefore if the 'Step back' option in manual mode is used or if plant operators force I/O via laptop/terminal then, upon completion, they will need to update the Waste Tracking Systems records.

5.2.5 Engineer

The Engineer access level, allowing all functions available to the Team Leader plus:

- Changing of date and time
- Changing of system alarm level values
- Access to system diagnostics
- Access to Plus.
- Configuration of displays
- Bespoke Software.

5.2.6 System Administrator

The System administrator access level, allowing all functions available to the Engineer plus:

- System management and database administration functions
- User and Access Management
- Configuration of system

5.3 Virus Scanning

A dedicated Personal Computer **shall** be provided for the sole purpose of scanning electronic media. This Personal Computer **shall** be located in the Computer Room. The Personal Computer **shall** not be connected to the network nor be fitted with a network card. The Personal Computer **shall** be fitted with 3½" Floppy Disk and CD-Rom Drives. Virus scanning software **shall** be installed on the PC.

In addition, rigorous virus protection **shall** be provided across the whole system. This will consist of virus protection software being installed in all workstations, servers and portable P.C.s. Where practicable this should run automatically on connection/boot up.

5.4 Diagnostics

5.4.1 Control System Hardware Diagnostics

These diagnostics **shall** provide comprehensive facilities to detect faults down to module level and **shall** provide information on at least the following:

- Processor units (PLC's, Servers, Workstations).
- Hard disk devices
- Peripherals
- Communications highway, network hub modules and interfaces
- Control and I/O modules (Local, Distributed and Remote)
- Power supplies, where appropriate
- Data communication errors

The diagnostic routines **shall**, where necessary, provide for preservation of system data with automatic transition to back up systems in the event of system failures or errors. In the event of a catastrophic failure, all operational plant **shall** be safely halted.

The System Supplier **shall** provide details of the extent of checking by the diagnostics.

Upon detection of a failure, a system alarm **shall** be raised.

5.4.2 Software Diagnostics - Sequences

Facilities **shall** be provided to monitor the sequence status including:

- i). Sequence Prechecks

At sequence initiation ALL prechecks **shall** be tested and a plant alarm **shall** be generated for EACH ONE that is not healthy. The alarm message **shall** include SYSTEM No., and the alarm description as stated in CONCISE.

ii). Sequence Step Fails

A plant alarm **shall** be raised for any Step Fail. The alarm message **shall** include SYSTEM No., and the alarm description as stated in CONCISE.

iii). Sequence Runchecks

A plant alarm **shall** be raised for any Runcheck Fail. The alarm message **shall** include SYSTEM No. and the alarm description as stated in CONCISE.

iv). General

For any sequence, the Control System **shall** be able to display, via appropriate mimics, the following status / condition information:

Mode (Consecutive or Step)

Current State (e.g. Running / Complete / idle / chk. Flt / on-hold / timeout / step-on)

Current Step No.

5.4.3 Software Diagnostics - Devices

i). Device Mode

The current mode / status of the device **shall** be displayed on the Device Diagnostic Mimic and the Process Mimics; e.g.

Automatic mode

Manual mode

Maintenance* status [Note* that this is not a mode, but an operator designated, notional⁺ status applied to mimics showing devices, depicting that equipment is unavailable due to maintenance. Maintenance status **shall** be indicated by ‘graying’ out of the relevant device(s) on mimics. ⁺Application / removal by admin procedure only.]

ii). Device States

Both the Current state and the Previous State of the device **shall** be displayed on the Diagnostic Mimic; e.g. Previous OPENING or Previous OPENING
 Current OPEN Current FAULT

iii). Device Faults

Device fault status information **shall** be displayed on the Diagnostic Mimic; e.g. Invalid State (e.g. ‘Open’ and ‘Closed’ limit switch inputs active).

State Time-out (all Transient Device States such as OPENING, RETRACTING **shall** have a time limit). During simulation testing, appropriate values for state time-outs shall be determined, implemented in the application software and documented in SSS.

Invalid State Change (e.g. A Valve Closing without a command from the PLC)

This information **shall** be used to raise alarms having appropriate messages on the appropriate page(s) for any instance of a device.

iv). Device Interlocks

All Device Interlocks (DESCRIPTION and STATUS) **shall** be displayed on the Diagnostic Mimic. The mimic **shall** show which interlocks are applicable to which command (open, close, etc.), and to mode changes.

v). Device Real I/O

All Real I/O (TAG, DESCRIPTION and STATUS) associated with the device **shall** be displayed on the Diagnostic Mimic or on a Mimic easily accessible from the Diagnostic Mimic.

vi). Device Reset

After a device fault, the operator will attempt a device reset from the appropriate Mimic. This **shall** result in either the device state changing from fault to a healthy state appropriate to the device real I/O or the device remaining in the fault state. (e.g. Due to Both open and closed limit switch inputs active or Overload trip active)

5.5 Alarms

Comprehensive alarm handling systems **shall** be provided within the Advanced Mixed Waste Treatment Facility to facilitate alarm presentation and management. There shall be three alarm categories, System alarms; Hard-wired alarms and Plant alarms. System alarms relate to problems with the control system itself. Hard-wired alarms are connected to the ICS solely for indication and logging purposes. Plant alarms relate to the actual plant and equipment in the facility and the control sequences that control it.

For 'Plant' and 'System' alarm categories, when an alarm occurs it shall be allocated a 'High', 'Medium Priority' or 'Low Priority' classification in order to assist in prioritizing attention required by the operator.

In general, alarms should be prioritized for attention in the following order, starting with the most important.

Category	Priority
Hard-wired	H
Plant	M
System	L

5.5.1 System Alarms.

The system alarms **shall** be processed through the Integrated Control System (ICS), with the alarms presented at the appropriate* workstation for acknowledgement. [*for details determining the ‘appropriate workstation’ in this context, see Distribution of Alarms, section 5.5.2.2]

The purpose of System alarms is to annunciate faults with the control system itself. As a minimum, these **shall** be provided as described under section 5.4, Diagnostics.

5.5.2 Plant Alarms.

Plant alarms annunciate faults with the plant equipment/processes and **shall** be processed through the Integrated Control System with the alarms presented at the appropriate* workstation for acknowledgement. [*For details determining the ‘appropriate workstation’ in this context, see Distribution of Alarms, section 5.5.2.2.]

5.5.2.1 Plant Alarm Types.

There **shall** be a number of different plant alarm types, which **shall** require to be presented to the Operators via the Integrated Control System:

1. **Process Variable** alarms derived from PLC alarm thresholds placed on plant analog measurement (e.g. High, Low) and digital inputs (e.g. Pressure/Level Switches) which are transmitted directly to Integrated Control System and not via *Device* logic. Note. There **shall** be a configurable) alarm hysteresis provision to prevent multiple alarms, (e.g. from lapping fluids in tanks close to high level). Therefore, Alarm Conditions **shall** not clear until the alarm is acknowledged and the measurements drop below the Alarm Threshold.
2. **Bad Measure** alarms in response to faulty I/O; e.g. Analog inputs moving outside the 4-20 mA range. (e.g. loss of signal, etc.) Note. There **shall** be a configurable out of range deadband (typically 3%) to prevent spurious bad measure alarms, (e.g. from

level sensors on empty vessels). Therefore, Bad Measure alarms are raised for readings below 3.5 mA and above 20.5 mA.

3. **Device Alarms** These **shall** be presented at the Device Diagnostic Display and the relevant mimic and alarm summary display. The System Integrator **shall** develop device diagnostic displays for each device template:
 - **Device Diagnostic** alarms derived from *Device* diagnostic logic using PLC analog and digital inputs e.g. open/close limit switch inputs in fault state (open and close true at same time), or device operation time-out;
 - **Device Discrepancy** alarms derived from *Device* discrepancy logic detecting discrepancy between command and current state; e.g. Valve Closing whilst commanded to remain open; or a discrepancy between two sensors that should agree.
 - **Device Interlock** alarms derived from the device interlock logic.
4. **PLC Sequence/Operation** alarms, e.g. Pre-check, Run check, Scheduler, Group faults;

5.5.2.2 *Distribution of Alarms.*

A given user may log onto an area at any one of a number of systems at a workstation configured for his use. Each local workstation (fixed or portable connection point) **shall** offer access only to a (configurable) predetermined list of systems relevant to its physical location.

Local users on plant **shall** only receive those Alarms that relate to the area that they are currently logged onto.

A user logging onto a system on plant **shall** also cause any alarms relating to that area to be displayed at that local workstation.

5.5.3 Alarm Priorities.

The 'SCADA' Alarm Handling System **shall** present alarms according to an Alarm Priority order. The assignment of an Alarm Priority to each alarm within an Alarm Group aids fault diagnosis by enabling the operator to concentrate on identifying the cause of the alarm, without having to choose the action order.

There **shall** be three Alarm Priorities applied to each Alarm Group:

- High Priority
- Medium Priority
- Low Priority

The '**High Priority**' classification **shall** be allocated to alarms that are safety related or of major plant and equipment significance and require a rapid operator response. For example, ventilation fan motor overloads, cooling water vessel Low Low limit alarm, etc. '**High Priority**' classification alarms are presented to the Operator first.

The '**Medium Priority**' classification **shall** be allocated to alarms that are of secondary importance such as Sequence/Operation Pre-check, Run-Check, Aborted status alarms. (Sequence/Operation status information **shall** be available through means other than alarm displays and thus do not require to be given a 'High Priority' priority status). Other types of '**Medium Priority**' classification' alarms would be approach to trip alarms e.g. Low/High alarms, where there is a related ultimate Low Low/High High. These would be defined as '**Medium Priority**' classification. '**Medium Priority**' classification alarms are presented to the Operator after '**High Priority**' classification alarms, when both are present at the same time.

The '**Low Priority**' alarm classification **shall** be allocated to alarms that are of minor significance, such as System file access (read) errors and performance related problems. Alarms which relate to System software process malfunctions which do not cause failures and where the function would be repeated automatically by the System **shall** be classified as '**Low Priority**' classification. e.g. database access errors.

5.5.4 Alarm Thresholds.

Alarm thresholds **shall** be located within the PLCs. This **shall** enable the PLC software to perform the required alarm control action directly without communicating with SCADA system. The SCADA package **shall** enable PLC alarm thresholds to be modified via SCADA data entry windows under access control. It **shall** be possible to define and modify the alarm threshold in a simple, interactive manner and these modifications **shall** be logged.

5.6 Start Up and Shut Down Functions.

No co-ordinated plant start-up and shutdown procedures are envisaged other than for the start-up of process building ventilation systems.

The system integrator **shall** specify the order and method of a partial and a complete control system power down.

The system integrator **shall** specify the order and method of a partial and a complete control system power up.

Controlled or uncontrolled shutdowns of the Integrated Control System in whole or in part **shall not** cause a state change of any area 700 (Process Ventilation) system. The Process Ventilation systems **shall** continue to run in their current state.

5.7 Control Functions.

Control functions **shall** be provided to allow for the selection of sequences which may then be started, stopped or have current status viewed in detail. Control functions, together with facilities to be provided to effect these, are described in detail within section 6 of this document.

Facility to view and change the current operating modes* of equipment or systems **shall** be provided on an individual basis. [N.B. * Note - for details of Control Mode selection, refer to Control Philosophy doc't ref. DD/K0105C/SYST/00004]

The method of display **shall** enable the user to determine both the current and possible operating modes for each piece of equipment.

Control functions **shall** be provided to allow for the starting and stopping of equipment which is selected to device manual mode. This **shall** be provided on an individual equipment basis.

5.8 Degraded Operation and Failure Modes.

Following failure of equipment or control system elements, sequences may continue until the failed equipment is required. Safety systems are by definition required at all times; as such, failure of a safety-instrumented system shall immediately effect the shut down of process equipment in the most safe manner.

Initiation of sequences that at any step require equipment that is currently in Manual mode or a failed state **shall not** be possible.

Failure of the SCADA shall allow any sequence already in progress to continue to completion or until input from the SCADA is required.

Initiation of sequences **shall not** be possible while the SCADA is in a failed state.

Upon failure of the SCADA, any equipment being run in **Manual** shall have all command signals turned off by the watchdog.

The design of the control system, electrical, electro-pneumatic and electro-hydraulic systems shall be such that systems shall be stable following loss of command signals; e.g. conveyors **shall** stop; gripping devices **shall** not change state (a closed gripper shall remain closed and an open gripper shall remain open).

5.9 Data Management

Several classes of data **shall** be managed by the Control System. The data **shall** be used for a variety of purposes including the monitoring and control of the process. Each use

of the data calls for different characteristics in the detail, duration, and method of storage. The following breakdown identifies the different types and uses of data.

5.9.1 Real Time Process & Plant Status Data.

Process Data

Consists of continuous and discrete signal measurements of plant parameters, results of calculations performed on plant parameters, the state of items of plant which can only be in one of a finite number of discrete states, or the result of logic control schemes implemented in the control system.

Occurrences of continuous (analogue) signals being subject to changes / deviation of approximately 5% from current values **shall** be logged to the DMS as Historical Data.

Continuous and discrete signal data **shall** be continuously logged to DMS (Data Management System) for long term storage, retrieval and analysis when required.

Plant Status

The status of each item of production equipment controlled by the Control System is to be presented to the Operator in the form of mimics.

Alarms are to be time/date stamped on initiated, acknowledgement and reset and logged to Data Management System.

5.9.2 Data Retrieval and Analysis Requirements.

Data retrieval and analysis facilities are required for the following:

- Plant control

To assist the plant operators in their routine and non-routine tasks by viewing the operation of the plant; e.g. trends and reports.

- Detailed Investigation

To provide the plant operators with a tool that can be directed when required to generate data of a fidelity and extent necessary to analyze and monitor specific problems; e.g. Overlay and compare trend data from a selection of analog signals. It **shall** be possible to perform this level of investigation on any one of a group of up to 50 signals.

- Historic Record

To provide a historic record of operation of the plant to allow investigation of plant operation over the long term.

The Control System **shall** log all messages and alarms (and any associated data or operator decision) to the DMS for archiving. This data shall be retrievable by the ICS for subsequent analysis and interrogation at a later date if required..

5.10 Trending.

Historical data storage of certain process measurements for a minimum of 2 years shall provide display and reports of value trends of these measurements. The

5.11 Prompt Messages.

These shall be derived from the PLC and displayed to the operator in text form, along with their time and date stamp in order to prompt the operator to perform an operation or to provide confirmation to the control system.

5.12 Event Messages.

These shall be derived from the PLC's and displayed to the operator in text form along with their time and date stamp in order to provide:

- Indication of the failure of an operation and the reason for failure (this does not cover cases where immediate action is required to prevent mechanical damage or loss of product quality as these would be alarms)
- Information on the state of process operations

5.13 Tracking Data Handling.

Plant mapping **shall** be implemented within the control system. Workstation displays **shall** typically provide the following status/mapping functions:

- Mapping displays and reports for puck, drum, box, part filled product drum status, conveyor loading, etc.
- Raw material inventories

5.14 Data Management System Data Handling.

Specific data collected from front-end instrumentation by layers 1 and 2 shall be routed to the Data Management System (layer 3) as required for the facilities of that layer. In the event of a failure of the communications to Data Management System or a failure of Data Management System itself, the front end instrumentation data should be stored on line at layer 2 as it accumulates over seven days.

5.15.1.3 *Portable Workstations*

These **shall** consist of:

1. Color Screen and US keyboard both integrated in system case.
2. Integrated pointing device
3. Total weight less than 10 Kg

The portable workstation displays **shall** be low radiation, high refresh type. Portable workstations **shall** be easily connected and removed at any time. Workstation procurement selection criteria should consider use by gloved and / or suited operators.

5.15.1.4 *General Considerations*

All workstations **shall** be capable of supporting the SCADA Interface, including access to the Data Management System.

The Central Control Room and Computer Room equipment **shall** be mounted on consoles* which shall be supplied by others. [*See also item 7.1.3]

The System Supplier **shall** advise BNFL Inc. of all heat output ratings for equipment (in Watts) within the SDD.

5.15.2 *Printers*

There **shall** be four 'Report Printers' which **shall** be letter paper compatible printer type, located in the Central Control Room for printing reports, operator action logs, events logs and alarm logs. In addition, there **shall** be one Report Printer located in the Back –up Monitoring Room.

There **shall** be two 'Graphics Printers' which **shall** be letter paper compatible color plotter or color printers located in the Central Control Room for the printing of mimic displays and trends from any of the workstations in the Central Control Room.

This printer device is to be of suitable quality to give an accurate representation of the display mimics.

There **shall** be two 'General Printers' which **shall** be of letter paper compatible printer type, with one located in the Central Control Room and one located in the Computer Room.

Printers **shall** be located to provide tidy paper handling and be supplied with adequate paper feed and collection trays.

5.15.3 Power.

For portable workstations, a power supply* socket outlet **shall** be installed in the immediate vicinity of each network connection plug in point, so as to avoid tripping hazards arising from extended leads that would otherwise be incurred.

In addition, portable workstation use would be facilitated by a local (foldaway) shelf to be fitted adjacent to each network connection plug in point, sized to accommodate a portable workstation.

All fixed workstations, portable workstations and cubicles (except the network hub) **shall** each be fed by a single **110 V ac** 60 Hz single phase supply of appropriate power rating.

The control network hub **shall** include dual redundant PSU's each capable of supporting 100% of the functionality of the hub. Each PSU **shall** be fed by a single **110 V ac** single phase UPS supply of appropriate power rating. Details of the Control Hubs location and system architecture will be more fully developed in the SDD.

Each item of Central Control Room and Computer Room Equipment (including Servers, Workstations and printers) **shall** be fed by a single **110 V ac** single phase supply of appropriate power rating.

Servers **shall** be fed by UPS supplies.

The System Supplier **shall** advise BNFL Inc. of all power requirements within his System Definition Document (SDD).

6 Functions And Facilities.

This section describes the functions and facilities that shall be available from the control system.

6.1 SCADA Functions.

6.1.1 SCADA Displays.(i.e. SCADA generated displays)

The SCADA displays fall into the following categories:

- Plant Displays
- Forms and Reports
- Trends
- Utilities

The displays provided within each category are described in the following sections.

6.1.1.1 *Plant Displays*

The plant displays shall show dynamically updated pictures of the plant. The displays shall be grouped into a hierarchy of up to five levels, which are identified below.

Level 0	-	AMWTP plant overview
Level 1	-	Area overview
Level 2	-	System overview
Levels 3 & 4	-	Detailed plant mimics

N.B. Further level displays are provided, levels 4.5 and 5 for device control, these are detailed in section 6.1.3.

6.1.1.1.1 Level 0 - AMWTP Plant Overview Display

The plant overview display, an illustrative example of which is shown in Appendix 4 Fig.1, shall be the initial screen the user sees and shall provide the mechanism for his logging onto the control system. It shall show all plant areas in a block form, together with indication of any outstanding alarms within each plant area by means of a highlighted alarm text block.

Each user shall be able to log onto a selected area from any workstation, subject to the prevailing “user / workstation / system” configuration constraints described in section 6.1.6, ‘User Access’.

Note that the standard screen layout defined in subsequent sections covering levels 1 to 4 does not apply to this level 0 display, i.e. no alarm banner or toolbar area shall be shown on this level 0 display.

Target areas shall be defined over each 'plant area' block; selection of an area shall initiate the log-on mechanism. Following a successful log-on, the level 1 mimic (area overview) corresponding to the area logged-onto shall be displayed and this is described in the following section.

6.1.1.1.2 Level 1 - Area Overview

A level 1 mimic shall be produced for each area. This shall provide an overview display of all systems within that plant area, together with an indication for each system of both its mode and whether or not an alarm is outstanding.

The system blocks shall each provide a target selection area for accessing the level 2 mimics for that system.

6.1.1.1.3 Level 2 - System Overview

Level 2 mimics provide a basic overview picture of the selected system.

Navigation routes shall be provided to access the detailed level 3 and 4 mimics for appropriate sections of the system. Access to systems shall be subject to constraints, configurable for each user, workstation and system.

6.1.1.1.4 Levels 3 & 4 - Detailed Plant Mimics

Each plant system shall have a number of level 3 and 4 mimics, these show the detailed plant mimics of equipment and the individual devices within the system.

The toolbar section of the SCADA screen shall contain a 'Sequence' button. This allows access to sequence control faceplates, described in section 6.1.4. Each level 3&4 mimic shall have a scheduler sequence associated with it. Selection of the sequence button from a particular plant mimic shall invoke for that scheduler (via a selection faceplate if more than one) the sequence control faceplate.

All devices shown at level 3 & 4 mimics shall have additional device control facilities available, as described in section 6.1.3, and accessed by clicking on the required device symbol on the mimic.

Facilities shall be provided for user to assign any device depicted on level 3 or 4 screens to 'Maintenance' status in order to show that such device(s) are not available for automatic operation due to being under maintenance. This assignment shall be effected, and indicated as such, using the

Maintenance Status facility described in the final clause of section 6.1.3.1, ‘device control faceplate’. The application (and removal) of ‘maintenance’ to any device shall be under ‘operational procedure’ only, except that any device in maintenance status shall inhibit that **device** from automatic mode.

6.1.1.1.5 Navigation

The navigation between plant mimics shall be achieved by the user clicking the screen pointer within appropriate target selection areas within the mimic display. The target area shall be identified by the mimic number within a selection box.

When the screen pointer is positioned over the target area, a ToolTip giving a description of the mimic shall appear. Selecting the area shall display the new mimic.

The top area of the screen (the screen layout is defined in section 6.1.2.) shall provide a toolbar area that shall provide the following additional navigation aids:

- Go back 1 level
- Display previous screen
- Bookmark facility allows screens to be marked for return

Following selection of a plant area from the AMWTP plant overview mimic and subsequent logging on to that area, navigation is restricted to that area. To gain access to another plant area, the user shall have to log off and log-on to the new area from the AMWTP plant overview mimic.

6.1.1.1.6 Perspective Views

Where plant can be **specifically** controlled from different local workstations, the plant mimics shall be produced to provide mimics that display the information in the correct orientation in relation to the view the operator has. In some cases, this shall require development of different perspective views of the same mimic, depending on where the workstations are with respect to the plant equipment being controlled. When the mimic for that equipment is then called up from one of these specific workstations, the system shall automatically display the correct perspective view of the equipment relevant to that user / workstation.

6.1.1.2 Forms and Reports

The following forms and reports shall be provided under this menu option, this being selectable from the main toolbar area:

- List of tracking forms
- Alarm history
- Plant event, operator actions and messages

Further details of the above requirements are provided under section 5.9 to 5.14 of this document.

6.1.1.3 Trends

Trend displays shall be accessible by selecting the 'Trend' option provided within the toolbar area of the screen. Two types of displays shall be provided: **real time trends** and a number of pre-configured **historic trends**.

6.1.1.3.1 Real Time

All analogue inputs shall be trendable in real time. A pick list of all analogue inputs within the area currently logged onto shall be provided. The user shall select the required inputs from the list to trend.

6.1.1.3.2 Historic

A number of historic trend displays shall be provided.

All data shall be logged to, and retrieved directly from, the DMS database.

The trend displays provided shall contain standard pan and zoom facilities allowing more detailed investigation of the data.

6.1.1.4 Utilities

The utilities menu shall include the following options:

- System status and diagnostics display
- Edit alarm limits
- Edit system access control
- EDMS

Details are set out below:-

System status and diagnostics display

This shall provide an overview display of all major network system components. Various diagnostic information shall be available where accessible.

Edit Alarm Limits

All alarm setpoint levels are held within each PLC for relevant analogue inputs associated with that PLC. A 'SCADA' screen shall be configured to enable the user to edit the values of the alarm setpoints. All edits shall be recorded in the Operator Actions log.

Edit System Access Control

The control of each system is restricted to defined users and workstations, determined by configuration, as described in sections 5.2. and 6.1.6. This display provides the system administrator with a display by which he may edit: -

- Control access configurations of users, workstations, systems and schedulers
- Facilities applicable to each access level
- User Privileges i.e. access level attributable to each user
- User Passwords

EDMS

EDMS will be started by desk top application and be able to be launched from a desk top icon on the ICS display mimics. The EDMS will be an additional operational window over the Factorylink system.

6.1.2 SCADA Display Standards

Screen Layout

All SCADA displays (except level 0) shall have a standard screen layout that shall include features as described below and similar to those depicted in the relevant examples contained within Appendix 4

6.1.2.1 Toolbar Area

The top area of each screen shall be reserved for standard toolbars allowing menu navigation. The following options shall be provided within the toolbar area:

- Display previous level within plant mimic hierarchy
- Display previous mimic
- Bookmark function allowing access to any screen
- 'Sequence' button on all plant mimics allowing access to sequence control facilities
- Utilities menu option
- Trend options
- Forms menu option
- Log-out function
- Print screen option

6.1.2.2 Alarm Area

Each screen shall display an alarm area; this shall consist of 3 lines which shall display the latest, un-acknowledged alarms outstanding within the **area** under view from the workstation.

6.1.2.3 Screen Area

The main area of the screen is reserved for the mimic display.

6.1.2.4 Operator Message Display Facility

Each screen shall display an operator message area; this shall consist of one line, which shall display the latest operator message or prompt generated by active sequence(s) within the **system** under view from the workstation. Refer to section 6.1.9 for further details.

6.1.2.5 Dialog Area

The bottom area of the screen shall display the following information:

Username - this displays the username of current logged-on user.

Time and date - US format

Mode of control - this displays the current mode of the system under display

Oracle Connection Status - displays current DMS status

Alarm Logging Status - status of alarm logging

6.1.2.6 Color Standards

Mimics shall be drawn to a standardized color system to be approved by BNFL Inc during detail design. Reference should be made to Appendix 2, section 9 of this document.

6.1.2.7 Numeric Displays

Analogue inputs shall be displayed in a standardized display box showing loop reference, alarm condition, current value and engineering units.

This shall be positioned in close proximity to the location of the measuring device on the display.

6.1.2.8 Analogue Alarm Limit Display/Edit

Each numeric display shall have a popup window configured, this shall display all alarms derived from that input and shall allow user editing (typically Team Leader, by configuration) of alarm limits.

This editing facility shall be in addition to 'Edit Alarm Limits' facility described under 'Utilities' section 6.1.1.4

6.1.2.9 Movement of Mechanical Plant

Provision shall be made, using symbols, to indicate the movement of mechanical plant. At no stage shall more than one image of the plant symbol be drawn. During transient locations, the plant symbol shall not disappear completely.

Wherever practical, the movement depicted should be based on data derived from real plant sensors that are regularly updated, so as to minimize the extent of inferred position with its inherent potential for error with respect to actual position.

6.1.2.10 Pop-up Windows

Certain facilities provided by the SCADA system shall be implemented via the use of pop-up windows, e.g. device faceplates and sequence faceplates. Where pop-up windows are used, these shall be displayed overlaying the main screen area and positioned such as to avoid obstructing important information, e.g. alarm banner. These windows shall be movable but not resizable. Focus shall be retained to the pop-up display until the window is closed via an EXIT button; the focus shall then be returned to the main display.

6.1.2.11 Fonts

All text shall be displayed in bold using the Helvetica font with a recommended minimum size of 15pt, but when necessary smaller font size may be acceptable subject to satisfactory legibility.

6.1.2.12 Device Animation

All plant devices shall be animated with the following standard:

The PLC's shall derive a status code for each device e.g. for a valve this would be open, closed, opening, closing or faulted. The SCADA shall use this state to animate the device status.

On level 4 mimics, additional text display of the device status shall be provided. This shall consist of the device tag and corresponding device status text that shall be dynamically updated. These shall be positioned in close proximity to the device symbol.

The device status box shall also be the target selection area for gaining access to the device control faceplate described in the following section.

6.1.3 Device Control Faceplates.

All level 4 plant mimics shall provide a device control faceplate (level 4.5) and diagnostics information (level 5) for each plant device shown on the mimic. The device control faceplate shall be selected by clicking in the device status box described in the previous section.

6.1.3.1 *The Device Control Faceplate (Level 4.5)*

This **shall** be a pop-up style window; see App.4, fig.5 for illustrative example. It shall provide the facilities to manually control the device and also to reset a device fault when in Automatic modes. These facilities are described below:

- **Current Status**

This field shall be dynamically updated to show the current device status, e.g. 'lowered'.

- **Command Buttons (e.g. Raise/Lower)**

Command buttons allow the device commands to be selected when the device is in manual mode. When the device is in a non-manual mode, these buttons shall be grayed out and not selectable. When a manual device operation is required, the required command button must be first selected e.g. Raise. The command shall only be initiated on selecting the 'Execute' button.

When in Automatic mode, the commands shall be automatically selected via the sequence operation.

Note that the example shown in App.4 is for a device which moves up and down, other devices may have different commands e.g. Open, Close etc.; see relevant Concise for specific definition.

- **Execute**

The 'Execute' button has two functions, one to execute the selected command in manual mode and secondly allowing a device fault to be **reset** in any mode.

When operating a device in manual mode, the required command must first be selected, as described above. The Execute button shall initiate the command, releasing the command buttons.

When in Auto or Step Modes, the command buttons shall already be selected; operation of the Execute shall reinitiate the command.

- **Interlocks**

The Interlocks field shall dynamically indicate the status of the device operation interlocks. These shall be displayed in either red or green, green indicating interlocks are healthy.

- **Diagnostics**

The diagnostics button shall provide a method of accessing to the Device Diagnostics Faceplate. Details concerning the Device Diagnostics Faceplate requirements are provided in section 6.1.3.2.

- **Device Manual Mode Select / De-select facility**

The system integrator shall provide a 'Device Manual Mode Select / De-select' facility, as a means:

- (i) for the user to put the selected device into manual when the system mode is automatic
- (ii) for user to return the selected device to automatic mode, provided the system mode is automatic.

This facility shall only be available when the system is in Auto Mode at all other the Device Manual Mode Select / De-select facility shall be 'grayed out'.

The facility shall clearly indicate whether the current **device** state is 'auto' or 'manual', by reference to the color of the device description text. The design of this facility shall be consistent with the other facilities on this faceplate and to the approval of BNFL inc.

- **Maintenance Status facility**

A 'maintenance status' facility shall be provided as a means for the user to assign the status of the selected device to 'maintenance'. This facility shall only be available when the device is in manual; selection / re-selection of automatic mode shall be precluded whilst maintenance is selected.

Typically, this facility should be along the following lines:

- The device control faceplate shall incorporate a 'maintenance status' checkbox, in addition to the controls depicted in App.4 fig 5.
- When the device is not in manual mode, the 'maintenance status' checkbox shall be unavailable and indicated as such by being grayed out. On subsequently selecting manual mode (either for the complete system or for just the one device), the 'maintenance status' checkbox shall then become available.
- When the device is not in maintenance status, then this box shall be un-checked.
- On subsequently clicking on this box, this device shall adopt **maintenance status** and the box becomes checked.
- If the user elects to exit from the device control faceplate then that device's symbol shall be 'grayed out' on the main plant mimic to reflect its maintenance status. However, the device may still be re-selected [by clicking in the device status box described at clause 6.1.3] in order to return to the device control faceplate display.
- Further clicking on the 'maintenance status' checkbox shall cause the device to exit maintenance status and the box to become unchecked. The graying out of the devices' symbol on the main mimic shall cease.

As this is a procedural facility only, there is no required change to functionality during maintenance status, except that it shall not be possible to run equipment (i.e. a scheduler) in automatic, where that equipment / scheduler contains devices in maintenance status. This functionality shall be achieved as a consequence of device manual mode being a pre-requisite of maintenance status.

- **Exit**

The exit button shall close the window and return focus to the main plant mimic.

6.1.3.2 *Diagnostics Faceplate (Level 5)*

Operation of the diagnostics button on the device control faceplate shall cause the Device Diagnostics Faceplate to be displayed; see App.4, fig.6 for illustrative example. The device control faceplate shall be closed in consequence. The Diagnostics faceplate shall, as a subordinate mimic to the device control faceplate, provide all the facilities that are available on the control faceplate and additionally, more detailed device status and diagnostics information. This additional information is described in the following clauses:

- **Previous State**

Dynamically displays the previous device state as read from the PLC.

- **Fault Details**

This shall show a device fault message identifying why the device has failed. This shall provide information additional to that given by the alarm, e.g. Failed to Achieve Position.

- **Interlocks**

All device interlocks and their status shall be shown within a scrolling window. Healthy interlocks in green text, failed interlocks in red text. A separate window within the same faceplate display shall be provided for each operation of the device; in this example, 'Raise Interlocks' and 'Lower Interlocks'. Where more than 2 operations exist, radio buttons shall be used to select those operations interlocks to be displayed.

- **Plant Inputs and Outputs**

The status of all plant inputs and outputs relating to the device status shall be displayed in a scrolling window. Inputs and outputs in the ON state shall be displayed in green, those OFF shown in red. A tooltip shall be provided for each input and output to provide the user with a description of the input / output and its sense i.e. N/O or N/C.

- **Exit - Shall** delete the window and return the display to the plant mimic.

6.1.4 Sequence Selection & Control

6.1.4.1 General Requirements

Each plant mimic associated with a system shall have at least one scheduler sequence associated with it. In turn, each such main scheduler may have sub-ordinate schedulers or merely sub-ordinate group sequences.

Sequences shall only be controlled whilst displaying a plant mimic showing the appropriate information

The operation of scheduler sequences and / or group sequences that are associated with the selected system shall be controlled via a 'Sequence Control Faceplate' display.

One Sequence Control faceplate shall be created for each main scheduler; see App.4, figs 7B & 9 for illustrative examples.

6.1.4.2 Selection of (Scheduler)Sequences

Since: -

- any given plant mimic may have more than one scheduler sequence associated with it and
 - one 'Sequence Control faceplate' shall be created for each main scheduler;
- then a facility for selecting a single scheduler for control is required.

A 'Scheduler Selection faceplate' shall effect this function.

The 'Scheduler Selection Faceplate' shall provide a 'pick list' of all of the main schedulers associated with that system. However, at any one time, it shall only allow selection of **any one** scheduler that is associated with the currently displayed mimic. Schedulers not associated with the currently displayed mimic shall be grayed out to indicate their non-availability

The 'Scheduler Selection Faceplate' shall be a 'pop-up style' window, which shall be called up by clicking on the 'Sequence' button on the toolbar of the (levels 2, 3 or 4) plant mimic, as referred to in sections 6.1.1.1.4. & 6.1.2.2. See Appendix 2 fig.7A for an illustrative example.

When the 'Scheduler Selection Faceplate' has been displayed, clicking on the required (available) scheduler shall call up the 'Sequence Control Faceplate' for the selected scheduler; for details see sect 6.1.4.3 below.

6.1.4.3 'Sequence Control Faceplate'

The 'Sequence Control Faceplate' shall also be a 'pop-up style' window, which shall be called up via the 'Scheduler Selection Faceplate' described above. The facilities that shall be provided by the control faceplate are described in the following subsections.

6.1.4.3.1 Indication of Sequence status

The ‘Sequence Control Faceplate’ shall list all sequences (i.e. sub-ordinate schedulers and groups therein) within the main scheduler, together with dynamically updated fields to display the step number and state of each of those sequences. Possible states shall include:

- Idle
- Running
- Retry
- Chk Flt
- Step On
- Timeout
- WTS Hold
- Complete

‘**Idle**’ displayed against a sequence indicates that the sequence is **not** running and is not active

‘**Running**’ displayed against a sequence indicates that the sequence **is** currently in the process of executing the actions (tasks) specified in its steps.

‘**Retry**’ shall be displayed against a failed sequence whose fail action is to abort and whose initiator remains ON. This shall be to prevent continuously re-iterative automatic restart attempts.

‘**Chk Flt**’ displayed indicates that the sequence is currently stopped due to it being faulted

‘**Step On**’ shall be displayed whenever the system is operating in ‘AUTO’ mode with ‘STEP’ function enabled and is waiting to be stepped onto the next sequence step.

‘**Timeout**’ displayed against a sequence indicates that the sequence has stopped running owing to excessive time taken attempting to complete.

‘**WTS Hold**’ shall be displayed against (all) sequences associated with that system, which were active but have become suspended owing to the Waste Tracking System having failed or requiring updating.

'Complete' displayed against a sequence indicates that the sequence has completed all of its allotted tasks successfully and is currently waiting reset of its initiator as the final event prior to the sequence becoming inactive (idle).

6.1.4.3.2 Controlling a Sequence

To control a sequence, the following conditions must apply:-

Nominated **user**(s) must be logged in to the appropriate system via one of a number of designated **workstation**(s), with the relevant **system** selected (via the level 1 mimic) and the required **scheduler sequence** selected via the pertinent level 2, 3 or 4 mimic.

[Note that the items in **bold** represent the configurable access constraints defined in section 5.2.1]

The faceplate shall provide the control sequence facilities as described below: -

- **Selecting a sequence**

Selection of a sequence is a necessary pre-requisite for several of the specific functions detailed below. A sequence shall be selected by clicking on the required sequence from those listed on the faceplate and subsequently operating the **Select** pushbutton, thus highlighting the selection.

- **Starting a Sequence**

A sequence shall be started by selecting that scheduler or group, then operating the '**Start**' and '**Execute**' buttons successively.

[Note that if the sequence subsequently enters the 'Fault' or 'Timeout' states then, after any necessary manipulation of individual devices using 'device manual mode', the Start button shall enable the recommencement of the sequence. Similarly, if sequences become suspended under 'WTS Hold', then after appropriate recovery action to regain Auto mode, the Start button shall enable the recommencement of the sequences from the point at which they were suspended.]

- **Aborting a Sequence**

An '**abort**' button shall become available once a master scheduler is running and, regardless of faults, shall abort all sequences listed on that faceplate. The abort action shall be implemented when the '**Execute**' button is pressed following selection of **Abort**.

If the sequence relates to a process system (as against a mechanical handling system), then 'team leader' access rights as a minimum shall be required in order to abort this type of sequence.

- **'Stepping On' a Scheduler / Group**

When in '**Auto**' mode with '**Step**' function enabled, each scheduler / group shall hold at the end of each step. The '**Step On**' button shall allow one scheduler or group to be advanced by one step. After selecting (one) required sequence that has step-on enabled, then operating the '**Step-On**' and '**Execute**' buttons successively, the selected sequence shall execute the next step.

- **Stopping a sequence**

An active sequence can be stopped by selecting that scheduler or group and then operating the **Stop** and **Execute** pushbuttons successively. A stopped sequence shall become idle.

- **Diagnostics**

A ‘diagnostics’ option shall display a window listing the status of all pre-checks (including separately identified tracking pre-checks) and running checks for a selected sequence. A sequence may be selected by ‘clicking’ on the required sequence description. Subsequently operating the ‘**diagnostics**’ button shall then initiate the display of a diagnostics window for the selected sequence; see App.4, fig.8 for illustrative example.

- **Exit - Shall** delete the window and return the display to the plant mimic.

6.1.5 Alarms.

This section describes the general philosophy of alarms within the SCADA system and how alarms are presented to the user.

The user shall only see prevailing alarms within the area currently logged onto – see clause 5.5.2.2. for details of alarm distribution. These alarms shall be viewable through the alarm banner and the alarm summary list defined below.

Alarm acknowledgement **shall** only be possible from a workstation that is in logged onto that area.

The AMWTP plant overview mimic shall also provide indication that outstanding alarm(s) do exist within each area, but no detailed information need be provided without the user being logged into that area.

6.1.5.1 Alarm Banner

Each workstation display shall have a three line alarm banner at the top of every screen, the exception to this being the Plant Overview Display.

The alarm banner shall display alarms that originate only from the **area** that the workstation is logged onto. These shall be displayed in the order of the latest, unacknowledged alarm at the top of the list. They are then listed in time order, the unacknowledged alarms being displayed first.

The format of the text in the banner shall be as follows:

MM / DD / YY	HH:MM:SS	410A211	Lid NOT Detected R/Check Fail
date	time	tag (12 chars max)	text (43 chars max)

The alarm text shall be as defined in the alarm table in Concise. The color of the alarm shall relate to the priority and shall be as Appendix 2, table 5.

When an alarm is raised, the text shall flash. When the alarm is acknowledged, the text shall stop flashing and become steady. If the alarm goes to the 'off' state before it has been acknowledged, the alarm shall be displayed in green.

When an alarm has been acknowledged and has been reset, the entry shall be automatically removed from the alarm banner.

6.1.5.2 Alarm Summary List

Purpose / Objective

The alarm summary list shall display all outstanding alarms within the **area** that the workstation is currently logged onto. It also provides a mechanism to acknowledge alarms in addition to acknowledgement from the detail mimic display.

Method of calling up alarm summary list

The alarm summary list shall be selected from the alarm banner area by clicking on a standard symbol adjacent to the banner.

Alarm Format

The format of alarm entries within alarm summary list shall be identical to the alarm banner.

User options

Options shall be provided to allow the user to change: -

- the selection criteria - to display individual systems and
- the sort criteria - to be *either* 'time only' *or* 'time and priority'

Acknowledgement of alarms in the summary list.

The display shall be provided with buttons offering either selective acknowledgement of individual alarms, or a global acknowledgement of all alarms, in the summary list.

Acknowledging an alarm shall result in the alarm text going to the "none-flashing" state. If the alarm has already cleared, the entry shall be removed from the list.

Note that a user shall only be allowed to acknowledge an alarm providing the workstation is currently logged into the relevant area and the access constraints are appropriate; see section 5.2.1

6.1.5.3 Historical Alarms

All alarms are logged historically to the DMS database. These are viewable through the Historical Alarm Display under the Utilities menu.

The user shall be requested to enter 'start' and 'end' times, 'date' and a 'system number' or 'area number'. The system shall then display all alarms logged from the entered start time.

The format of the displayed text for each alarm shall contain the following:

- Alarm on time
- Alarm off time
- Alarm acknowledgement time and operator* name . (* i.e. acknowledging user)
- Alarm tag
- Alarm text

Options shall be provided to print the retrieved data as a report to one of the printers configured onto the system.

6.1.6 User Access.

Before the SCADA system can be used, the user must first 'log-on' to the control system at the workstation appropriate to that system. Log-on is achieved through the AMWTP 'Level 0' plant overview mimic, described at section 6.1.1.1.1, by selecting a plant area. Multiple log-ons to different terminals is only permitted for terminals that cover the same plant area and are located together e.g. in the CCR. There is to be no automatic log off facility.

The system shall then prompt the user to enter a username and password, to meet the system security requirements of the access levels referred to in section 5.2.

The facilities that each level of user can access shall be configurable, also described in section 5.2. System access control arrangements (passwords, privileges, user / workstation / system configurations etc) shall be editable through a separate SCADA screen, available via the 'Utilities' menu after log-on. This screen shall itself be configured for system administrator access only

Applicable user(s), workstation(s) and control of sequences shall all be configurable for each system. Thus, the control system shall allow more than one user to be logged onto a particular area with the same system selected at any one time (albeit from different workstations), if so configured. All 'log-on's shall be recorded in the 'plant event / operator actions and messages' log.

Following a successful log-on, the selected Area overview mimic shall be displayed. The name of the user logged in at that workstation shall now be displayed in the bottom left corner of that screen.

User access to a system shall be achieved by selection from the Area overview mimic (level 1) subject to the 'user / workstation / system' access constraints. Note that user access to that system may be shared if it is already accessed from another user workstation.

Each user may then view plant mimics for the selected system and access the additional facilities (e.g. sequence faceplates etc.) for which they have the access privileges required (by configuration). Mimics within a different plant area can only be accessed (if wanting to use that same workstation) by firstly logging off, and then re-logging on to the appropriate area.

Facilities that the user is not authorized to use shall be grayed out.

A log-off button shall be provided within the toolbar area of each screen, selection of this shall log-out the user and return the display to the AMWTP plant overview screen.

6.1.7 Mode Selection.

Mode selection shall be both system and device based, the system mode being selectable from the level 1 mimic.

The following system modes are available:

- **Fault**
- **Update**
- **Manual**
- **Auto** (NB Auto also has a Step function available on each sequence – see section 6.2.1.1 for details)
- **Standby** (this is a key-switch activated function)

The functionality within each system mode is described within section 6.2.4. The mode that is currently selected for the system on display is shown in the bottom area of the mimic screen (levels 2,3 or 4).

The level 1 mimic allows selection of Manual and Auto modes for each system.

If Manual mode is being selected from Update mode *or*, alternatively, if Auto mode is being selected from Manual mode, then the user shall be prompted to confirm that the database is correct. If it is not correct, then the database shall be updated by using a manual update form, as referred to at section 6.1.1.2. This shall ensure that all database updates undertaken while in those modes are correctly tracked.

On Process systems (e.g. Ventilation), mode changes shall only be achieved by a user with a higher access privilege than ‘operator’, typically Team Leader or higher.

All mode changes shall be logged to the Operator Action log.

6.1.8 Event Logging.

Events to be logged historically shall include the following items:-

- Sequence scheduler starts/stops by operator
- Mode changes
- Alarm limit changes
- Sequence messages (as defined in the Concise Message Schedule)
- Confirmation of database by user
- Logon and Logoff
- Device state changes in manual mode

All the above items are to be logged to the DMS database for historical records. A display shall exist under the Utilities menu to display and print these entries as a report. The user shall be prompted to enter a start and end date and time and an optional plant area. All logged entries shall then be retrieved and displayed on the screen between the entered dates.

6.1.9 Sequence Messages and Prompts.

The bottom area of all plant mimic displays shall contain one line reserved for the display of 'sequence messages' or 'prompts'. Messages and prompts shall be displayed on the workstation(s) mimics addressing the sequence(s) to which the messages/prompts relate. The messages shall be removed from the area when the PLC resets the appropriate message.

Some messages shall require an operator response. When this type of message is raised, the status goes to the 'Prompt' state. Clicking on "PMT" button shall enable the user to answer the prompt. A confirmation pop-up box shall be displayed. A prompt message shall not be removed from the message area until the prompt has been answered.

Message summary list

A Message & Prompt summary page shall be provided to list all of the active messages and prompts for the related scheduler

The message summary shall be accessed via a symbolic feature (typically a button or icon) located local to the message line on the mimic

The message summary shall not be accessible whilst a prompt confirmation pop-up bow is displayed awaiting confirmation

6.1.10 Context Sensitive Forms

Certain stages of the process shall require data to be entered via tracking forms. Where this is required, the appropriate SCADA displays shall be programmed to display the form when the waste item is selected. The resulting form shall be automatically populated with the item number of the tracked item.

6.1.11 Printing Facilities.

6.1.11.1 Screen Printing

A facility shall be provided to capture the contents of the SCADA screen and output the image to any one of the color inkjet printers.

6.1.11.2 Reports

All tracking forms, historical alarms, 'Plant Events / Operator Actions and Message' log facilities shall include an option to print the contents of the form to a selectable printer.

6.1.12 Development Facilities.

Each SCADA server shall be supplied with a development license. This shall allow a single user development on each area server.

The appropriate tools for software development will be identified in the SDD/SSS.

6.1.13 Algorithms

Algorithms typically used to determine / optimize process operating variables, such as 'Drum Selection' for supercompaction will generally be effected as part of the DMS functionality.

6.2 PLC Functions.

Each PLC (PES) shall be programmed using Modicon CONCEPT IEC1131 compliant programming software.

Common software architecture shall be applied to each PLC, with regards to the layout of code and modules of code within the PLC and their interaction with other modules and systems.

The following sections specify the principle functions to be provided by the PLC systems together with their requirements.

6.2.1 Automatic Sequences - Description.

The plant control system shall be designed such that once operations have been initiated by the operator, they shall automatically run to completion as far as possible. Operator intervention shall only be required where this is unavoidable; for example for operator verification or a manual action being necessary for the safe and secure operation of the plant.

To achieve this, an Automatic mode of operation shall be available. Auto mode of operation is provided by 'Auto' mode and 'Auto' mode with 'Step' function enabled. The requirements for these are discussed later.

Automatic sequences shall be specified by means of the 'Concise' documentation package produced for each system. Concise shall specify all sequences by means of "Operations" which specify each step of a sequence by means of its actions and transition conditions. Each step shall be given a step number. This information shall be displayed on the SCADA mimic screen (with 'sequence control faceplate' selected, ref section 6.1.4. for details) to indicate the current sequence status. The step number shall equate to the step number given in CONCISE and therefore a direct relationship can

be drawn between the CONCISE documentation and the SCADA sequence status screen as an aid to maintenance.

A typical sequence shall sequentially command a number of plant devices to move in a particular order to achieve plant automation.

Sequencers shall include 'Pre-checks' and 'Run-checks'. Pre-checks are a set of conditions, which must be satisfied before the sequence may be started. Once started, the pre-checks are ignored.

Run-checks are a set of conditions which shall be initially monitored as prechecks and then shall continue to be monitored whilst the sequence is in operation. If any run-check fails, then the sequence shall take the most appropriate action as stated in Concise. However, the general rule is that: -

- for 'mechanical handling' systems, the scheduler* / group shall **halt** upon run-check failure.
- for 'process based' systems, schedulers / groups shall normally **shut down** the process upon run-check failure.

[*N.B. for definition of scheduler / groups, see following section.]

6.2.1.1 *Sequence Control*

There shall be two types of sequences, Schedulers and Groups. The schedulers are master sequences, which shall be initiated via the SCADA. The schedulers shall be responsible for controlling all of the groups below them in the sequence hierarchy.

Control of the Scheduler group shall be effected via the SCADA workstation 'sequence control faceplates'. The status of the schedulers and groups shall be displayed on these faceplates.

Schedulers / groups shall run in 'Auto' mode or 'Auto' mode with 'Step' function enabled. **When in Auto**, the schedulers / groups shall run through their Auto operation automatically. Operator interaction may be required by the process being controlled; this shall generally be achieved via prompt messages which shall be displayed on the message banner line on the relevant the workstation. The sequence shall wait until the operator has responded to the prompt and then take the necessary action.

'Auto' mode with 'Step' function enabled shall allow the scheduler / groups to 'step through' one step at a time. The 'Step' function, if required by the user, shall be applied at (main) scheduler level via the 'Step' function select facility on the 'sequence control faceplate'. By doing this, the 'Step' function shall be selected for **all** sequences shown on that faceplate, including subordinate schedulers (if any) and subgroups. The 'Step-On' button on the faceplate may then be used when required to step the selected scheduler / group onto its next step.

The system shall permit only one sequence to be 'stepped-on' at one time. In the case of concurrent groups (i.e. two or more groups which run simultaneously in parallel), then each of the groups must be selected and stepped-on individually when required.

This means that if a scheduler starts two or more parallel groups, then the scheduler shall not continue until all those groups started at that scheduler step have been successfully single stepped to completion.

6.2.1.2 *Sequence Failure and Recovery actions*

This section details the type of faults and recovery actions that shall be provided when the system is running sequences.

Pre-check faults

When a sequence is requested to start, then all the pre-checks are initially checked, prior to the sequence actually starting. If a pre-check fails then an alarm for that specific pre-check shall be produced and the sequence shall **not** start..

Where a scheduler calls several sequences, the pre-checks for the scheduler shall generally be constrained to those directly applicable to the scheduler and not duplicate pre-checks related to the sequences that it calls. This objective of this requirement is to reduce the extent of excessive pre-checks.

Failed prechecks in a group shall behave in the same way as a runcheck failure.

Recovery from a scheduler pre-check failure shall be achieved by firstly clearing the initial fault condition and then re-initiating the scheduler via the sequence faceplate. Alternatively, if it is a group failure then the action of resuming the scheduler shall attempt to restart the group.

Run check faults

When a scheduler / group **run check** fails, then an alarm for that specific run check shall be produced; further response shall be dependent on the type of system -

- for mechanical type systems, the scheduler / group shall hold its current step
- for process type systems, the Concise specified response to a Run-Check failure may be to Abort or terminate to a safe condition.

For mechanical systems, if the group was commanding a device when a run-check failure occurred then, providing that the devices interlocks remain healthy, the group command shall remain 'on', allowing the device to complete.

The 'sequence control faceplate' shall provide a means to continue the scheduler / group by selecting START followed by EXECUTE.

- for mechanical type systems, if the run-check has cleared, then the scheduler / group shall continue and the run-check alarm shall be cleared. If the run-check condition is still failed, then continuing the scheduler / group from the faceplate shall have no effect and the scheduler / group shall remain.

- for process type systems, ‘**Retry**’ shall be displayed against a failed sequence whose ‘fail action’ is to abort and whose initiator remains ON. If the run-check has cleared, then the scheduler / group shall continue and the run-check alarm shall be cleared. If the run-check condition is still failed, then continuing the scheduler / group from the faceplate shall have no effect and the scheduler / group shall remain “held” showing Re-try.

If a device is being commanded from a group and a run-check fails then

- for mechanical type systems, the device shall be allowed to continue, but
- for process type systems, it may be vital that some recovery controlling action is taken by the control system. For instance, failure of a pump may require a standby pump to be started and routing valves opened/closed. Where these actions are required, they shall be defined in the CONCISE run-check action on failure field. For these types of groups then the group shall not hold but take the action defined by the CONCISE failure field, usually the group is aborted and its devices commanded to the datum state, e.g. closed or stopped.

Loss of the tracking system shall not affect any ‘process’ system, only mechanical systems that contain Waste Tracking Locations. For affected systems, WTS failure shall initiate a mode change from Auto Mode to Fault Mode. An alarm shall be raised notifying the user that WTS has failed. Before the system can be recovered to ‘Auto’ operations WTS must be healthy and the operator prompted to confirm that tracking is correct; if the operator response is negative then the PLC shall first have to go through update mode (update mode detailed in section 6.2.4.2).

User defined run-checks and associated alarms shall be defined in CONCISE. Appropriate additional runchecks shall be defined by system supplier during implementation.

Time-out faults

Scheduler / group time-out faults shall be produced when an *operation* step takes longer than a pre-defined amount of time. These sequence timeout faults shall occur if a device commanded by the operation fails to achieve its commanded position within a preset time. The sequence timeout fault shall be in addition to the associated device fault generated at device level. Where a scheduler step initiates a group, then step time-outs shall **not** be used on the scheduler step, since failure of the group to complete shall have generated an alarm where the fault has occurred. This technique shall be used to reduce the number of alarms produced when a lower level group fails. (i.e. unnecessary time-out alarms shall be avoided) .

Scheduler or group steps that wait for the Operator to respond with an action shall not normally be timed.

Recovery

When a device fails at a group step, the group shall hold, as defined by Concise. An attempt to clear the device fault by simply attempting a retry can then be achieved by selecting the device faceplate and selecting the EXECUTE button. Since the device commands remain on from the

sequence (which is now held), the device shall move to its commanded state. The sequence can then be resumed by using the sequence control faceplate.

As an alternative to merely retrying the prevailing device command, the device faceplate can also be used to put that **device** into Manual and then to exercise the device in any direction in a further attempt to clear the fault. Once the device fault has been cleared, the **device** can be returned to Auto mode and then the group sequence continued. **Note** that on completion of the recovery method described in this paragraph, involving selection of device manual mode during (system) auto operations, a confirmatory prompt shall be presented to the user requesting confirmation that tracking is correct. Resumption of Auto operations shall be dependent on an affirmative response.

If the problem is more difficult to solve than by either of the above two methods, then **any** of the devices associated with the failed sequence can be put into device 'Manual' mode, provided that none of those devices are associated with an active scheduler. Having the facility to manipulate **any** devices associated with the plant operation that is stalled without being limited to the originally failed device shall provide the flexibility to resolve the problem without having to abort the sequence. Once the problem has been cleared and all **devices** have been returned to 'Auto' mode, the group sequence may be continued. **Note** that on completion of the recovery method described in this paragraph, involving selection of device manual mode during (system) auto operations, a confirmatory prompt shall be presented to the user requesting confirmation that tracking is correct for each device restored to device 'Auto' mode. Resumption of Auto operations shall be dependent on an affirmative response in all cases.

Note. Since the devices can be operated in both Manual and Auto modes, the device interlocks shall be defined so as to maintain plant integrity, asset protection and safe operation for that area of plant in all modes.

To cater for fault occurrences involving a problem too serious to be corrected by exercising the device(s), but actually requiring the machine/plant to be taken out of service, repaired and the possible removal of any active material, it shall be possible for the auto sequence to be aborted. An abort button shall be available from the sequence control faceplate, which shall reset the sequence back to step 0. Following a scenario like this, the machine/plant shall need to be manually 'datumed' to its starting position by the Operator. Until the machine has been datumed, the scheduler prechecks shall not be satisfied and therefore shall be unable to start up again.

No specific assistance in datuming the machine/plant shall be provided by the ICS system, although it should be noted that the associated sequence pre-checks status display will provide the information necessary to successfully run the relevant sequence; refer to section 6.1.4, para 'Diagnostics'.

For 'process' type systems, the current Auto operation must be stopped prior to change of system mode. Change of system mode for process systems shall only be permitted for users with sufficient access privilege. i.e. Team Leader, since changing to manual mode on process systems shall cause all schedulers to abort.

6.2.2 Devices

A device is defined as a controllable item of plant, such as a motor or valve.

In order to control each device, it will be necessary for a device control program to be implemented within the PLC. Generally, a device controller shall have plant digital outputs such as 'open/close' and associated plant digital inputs such as 'opened/closed'. In addition, the device shall have a number of control and status signals that shall be sent out and received from other software modules within the ICS. Device movements shall be controlled by commands which shall be sent (providing interlocks are healthy) from either sequences or device control faceplate mimics generated via the SCADA. The status of the device shall be read by the SCADA. This device status shall be in the form of a number indicating the device state. In addition, status numbers shall be used to indicate the device's last state and fault state. Every device controller shall produce a device fault alarm when it enters its fault state.

All devices shall be categorized into types and their specifications shall be included in a (Generic Device Library (GDL)) document that shall be produced during the detailed design phase of the project. A specific device controller shall be developed by the system supplier to match the specified functionality of each device type.

CONCISE system 000 shall define all the device types that shall be used on the AMWTP project.

Devices shall be further categorized into base types and template types. The base type shall state the basic device type that the controller is intended to control, i.e. a valve, or a motor. Within a base type, there shall be many variants where the functionality of the device controller is identical, but the names given to the command signals and the names given to the device states shall differ according to the actual application of the controller, e.g. Motor which raises/lowers an assembly, as opposed to a motor which extends/retracts an assembly.

6.2.2.1 *Device Failure and Recovery actions*

Whenever a device fails it shall enter its fault state. The device

The failure of a device shall send an alarm to the SCADA, there shall be one alarm per device. In addition to the alarm there shall be a fault status code which shall be sent to the SCADA, this status code shall be displayed on the device's diagnostic faceplate. The status code shall be translated into a meaningful text message by the diagnostic faceplate. For example, typical device fault status messages shall be "Failed to energize", "Failed to move", "Failed to achieve position", "Illegal I/O", "Overload trip" and "Command lost" etc.

When a device has faulted and it is in its fault state, then recovery from the fault state shall be achieved by commanding the device to move to a valid position or by pressing EXECUTE to recover the device to a valid steady state. If, on receiving the command the device cannot achieve a valid state, then it shall stay in the fault state.

6.2.2.2 *Device Controller Specification*

Detailed specifications for each base device type controller shall be produced. These shall be included in the Generic Function Library document, which shall be maintained throughout the project lifecycle. All derivative template types shall also be documented.

The Device specification shall be suitably detailed to clearly convey the functionality of the device such that no ambiguity remains, whilst detailed enough such that the code can be written from it.

6.2.3 Interlocks.

Interlocks relate to conditions that must be satisfied in order for a device to be commanded to move or continue to move. The interlocks shall be defined in the CONCISE device interlocks tables. In general, interlocks shall only be monitored when the device's command is present. Application of a interlock must cause the device to enter its fault state & terminate the command.

When interlocks need to be monitored after a device has completed its operation, then this interlock shall be identified as 'monitor on completion' in the CONCISE device interlocks table. For example, consider a pump, which is required to fill a vessel. The relevant group sequence 'Fill Vessel' commands device 'Pump A' to start. A relevant interlock during starting would be 'High level in vessel', to prevent overfilling. Completion of the device is achieved when the pump has started. However, even though the device has completed, the interlock remains relevant (because the pump remains running), so that if the high level is subsequently incurred, the interlock will be applied to reset the pumps' output (i.e. stop the pump). Thus, because the interlock is needed after device completion, it is defined as 'monitor on completion'.

6.2.4 Control Modes.

Mode selection shall be included of on a 'system-by-system' basis rather than on 'PLC' basis, so that it shall be possible for a PLC to contain several systems, with each system being in a different mode. Generally there will only be one system per PLC. The control system shall have the following modes of control.

6.2.4.1 *PLC Fault Mode*

This mode is entered whenever a PLC fault condition is detected. The Faulted PLC shall be identified to the SCADA via an alarm or, in the case where the PLC has totally failed, a SCADA to PLC watchdog shall detect the failure. Such fault conditions shall include: -

- Power up of the PLC
- Detection of a internal PLC processor fault, i.e. Memory Checksum failure, execution of an illegal instruction.
- Operation of an E/STOP (note this shall reset all sequences, turn off all outputs, and disable all PLC devices for the system in the PLC)

- PLC Rack faults and Card faults

Whenever PLC fault mode is entered, all PLC outputs shall be either left as is for process systems or turned off for mechanical systems. The PLC program will immediately exit the sequence which will then reset. Once the PLC has left Fault Mode the plant operators will need to reset the plant prior to the resumption of automatic operation.

6.2.4.1.1 PLC Response to Internal Hardware failures

Process Systems

Single channel, PLC I/O card or TIO card failures shall be tolerated. The system shall continue to run in 'Auto' mode, but affected devices shall fail. If a complete remote I/O chassis fails (10 slot chassis) then this should be treated as a system abort i.e. the PLC is put into Fault Mode with all devices outputs off and all schedulers reset.

Mechanical Systems

Single channel failures shall be tolerated. PLC I/O card failures or complete remote I/O chassis failures (10 slot chassis) shall invoke a mode change to Fault mode and affected devices shall fail. The command to a device currently applied on that step / SFC state shall be removed, i.e. the device shall be forced to a fault state, depending on the template type. In either case, the device outputs shall be de-energized, causing motion to stop. It shall then be possible to recover using manual operations.

Analogue out of range (data quality bad).

In this case, all systems shall continue in Auto mode & 'an analogue out of range' alarm shall be produced. System diagnostics can then be used to provide details on the card & channel affected.

6.2.4.2 *Update Mode*

Update mode is only applicable for systems that contain tracking information i.e. mechanical handling systems. The HVAC & Utilities system are not affected by Update mode.

Subject to the proviso that the PLC is healthy, 'Update Mode' is entered on PLC power-up. PLC update mode is used to allow the Waste Tracking System's location information to be checked against the PLC's internal tracking data. Operator input shall be required via DMS (using a form which shall be launched on the workstation) to confirm that the information held within the Waste Tracking System is correct. Once this has been confirmed by the operator, the Tracking information shall be downloaded to the PLC, and the PLC allowed to proceed to Manual Mode. No device control or sequence control shall be possible whilst in Update mode.

Update mode shall also be entered if the operator replies ‘no’ to the confirmation prompt displayed upon selecting system Auto mode from Manual or device Auto mode from Manual.

6.2.4.3 *Manual Mode*

System ‘Manual’ mode shall be entered via the transition from ‘Update’ mode, or it may be entered from ‘Auto’ mode after all sequences are idle. When a system is in ‘Manual’ mode, individual devices shall be controllable via device faceplates provided by the SCADA mimics. Only one device per system shall be controlled at any one time via faceplates; once that faceplate has been closed then a further device faceplate can be selected. When in ‘Auto’ mode, ‘Manual’ mode can be selected after any active sequences have been aborted or completed to idle.

Note: When the system switches from Auto to Manual mode the device modes change to Manual as well.

6.2.4.4 *Auto Mode*

‘Auto’ mode allows the operation of automatic sequences to be performed. This mode shall allow the automatic control of devices via sequences. ‘Auto’ mode shall be entered via ‘Manual’ mode.

The selection of ‘Auto’ mode from ‘Manual’ mode shall only be possible when the Operator has confirmed that the Tracking information is accurate. The Operator shall be prompted to confirm this each time he attempts to change from ‘Manual’ mode to ‘Auto’ mode.

If the Operator decides that the tracking information is no longer accurate (possibly due to something having been moved whilst the system has been in ‘Manual’ mode), then he shall answer ‘no’ to the prompt. This shall force the system into ‘Update’ Mode (see above) and also launch a Waste Tracking System form. This form shall be used to rectify the tracking information.

Following the above reconciliation of the tracking information, the Operator can then take the system out of ‘Update’ mode and, through ‘Manual’ mode, into ‘Auto’ mode.

Note: When the system switches from Manual to Auto mode the device modes change to Auto as well (unless they have been placed in Maintenance Status).

6.2.4.5 *Auto Mode with ‘Step’ function enabled*

‘Auto’ mode with ‘Step’ function enabled allows the single stepping of automatic sequences to be performed. A step of an automatic sequence corresponds to a sequence step in CONCISE. ‘Step’ function shall be enabled by selecting the ‘Step’ facility (i.e. button or checkbox, as proposed by

system integrator) within the sequence control faceplate, prior to initiating the scheduler. Further details are provided within sections 6.1.4.3.2. and 6.2.1.1.

6.2.4.6 *Stand-By Mode*

The principal function of Standby mode defined by document ref 2. is the provision of short term, limited control and indication facilities for critical plant equipment, which shall be implemented by hard wired circuits independent of the ICS.

Transfer of control from the ICS to the 'Standby system' shall be selected by keyswitch, operation of which shall additionally isolate all PLC outputs from that system via electrical means (i.e. independently of software). Additionally, the keyswitch shall provide an input to the PLC confirming 'Standby mode selected'. Receipt of this input shall concurrently select 'Standby' mode within that PLC system wherever possible, i.e. in such cases where the transfer to 'Standby' control was not due to PLC failure.

Under 'Standby' mode within the system, the PLC shall continue to support monitoring, indication and alarm facilities, but no device control or sequence control shall be possible

On de-selecting 'Standby' mode – by returning the Standby keyswitch to the 'ICS control' position – the PLC shall leave 'Standby' and go into Auto mode.

6.2.5 Generic Functions.

This section describes the PLC functions that shall exist within PLC systems where appropriate.

Generic functions shall be provided for: -

- PLC Startup
- PLC Diagnostics and Fault Mode detection
- Mode Control
- Device Interlocks and control logic
- Sequence design and control logic
- Analogues
- Alarm Handling
- Condition Monitoring
- Event Handling
- Tracking Events and Update Handling
- Product Quality Events

6.2.6 Serial Links.

Specifications of protocols for hardware and software, together with details of data packets sent & received, shall assure full compatibility between independent P.E.S.'s or instruments and PLC's.

The only serial links identified so far for the ICS are:

- 1) Bar code readers (BCRs)
- 2) Laser Positioning Sensors (LPSs) on drum bogies
- 3) Some of the encoders for cranes and manipulators
- 4) Possibly some of the Utilities/Miscellaneous signals to the PLC.

For estimated numbers of BCRs and LPSs see Appendix 5

6.2.7 Development Facilities.

Facilities shall be provided by the supplier for development of application code within the PLC's. Access to the PLC's for this purpose shall be either through serial ports at the front of the PLC CPU's or via the workstations, subject to the constraints described elsewhere within this URS.

Development shall be possible either 'on' or 'off' line, and shall utilize approved programming software.

Code for ICS components (PLC's, SCADA etc) shall be managed, developed and multiple hard copies securely stored externally under an approved configuration management system.

Note: The provision of an operator training facility lies outside the scope of this document

7 System Interfaces

7.1 Operator Interfaces.

7.1.1 Workstations

The ergonomic requirements for Operator Interfaces are described further in Appendix 2. All workstations shall provide mimics, sequence start facilities, alarms, messages and system fault diagnostics such that plant operations can be achieved remotely from or local to the production equipment.

The following services are required at all control system workstations:

- Full SCADA functionality
- Access to all DMS functions.
- Ability to launch Electronic Document Management System

The workstations **shall** be based on easily configurable software, which shall provide as standard, facilities such as:

- Mimic displays
- Monitoring and trends on particular points and selective data archiving (e.g. compaction profiles).
- Ad-hoc selection, display and printout of data with report formatting facilities (e.g. to log box sort cell throughput).
- Alarm handling facilities.
- Elapsed time monitoring.
- Data logs - plant events, alarms, operator action etc.

To provide a flexible and consistent operator interface across the plant, three main types of operator station **shall** be provided :

1. Consoles within the Central Control Room **shall** feature large screen workstations providing detailed process mimics, plant maps, management reports, diagnostic information and interaction with the DMS Electronic Document Management System facilities.
2. Local, fixed control workstations installed on the plant, positioned to facilitate viewing by the operator of the process / operation to which it relates. These fixed local workstations **shall** have the same functionality as the central control room workstations.

3. Portable control workstations **shall**, when connected to the plant control system communication network, be capable of providing the same functionality as the fixed local control workstations. Connection would be via data plug into a network socket provided locally to the plant viewing / operating position or, in some instances, other designated points.

All types of operator workstation communicate via the plant control system communications network.

7.1.2 Stand-by Control Panels

‘Standby’ mode is an operational provision for certain items of equipment to be operated independently of the ICS under abnormal conditions, as described within ‘Control Philosophy’ document (ref.2). Since Stand-by mode operations are to be totally independent of the PES, hard-wired push-buttons, lamps or control pendants shall be provided for the items of equipment concerned. They shall be positioned either locally or centrally as appropriate.

7.1.3 Operator Control Consoles.

Operator control consoles **shall** be of ergonomic design such that adequate comfort is provided to the operator.

7.1.4 Visual Information Displays.

In addition to the workstation displays in the Central Control Room, there may also be hard-wired alarm annunciators, which are not within the scope of this document.

7.1.5 Hard Copy Output.

Facilities **shall** be provided for persons having appropriate access level (configurable), to select, generate and print plant performance reports on the report printer.

On an ‘all systems’ or ‘specified system’ basis, logged in users **shall** be able to select operator actions, plant events or alarms and then choose a time and date range to apply to the selection and print the results on a report's printer.

Logged in users **shall** be able to select trend* and mimic* displays for printing on the graphics printer. *For this application, it will be necessary to utilize ‘screen dump’ facilities to facilitate printing.

In the event of a printer being unavailable a logged in user can re-direct printouts to an available device.

7.1.6 Audible Annunciation.

Audible annunciation of alarms shall be provided on workstations in accordance with the requirements of Appendix 2.

7.2 Plant interfaces

7.2.1 Digital Inputs.

Digital inputs **shall** comply with NF69/3 with the following specific requirements.

All digital inputs **shall** be Tag referenced in accordance with:

- **DD/K0105C/SYST/00025** “Tagname Structures For Mechanical Handling Systems” or
- **dwg no 53-0001**, which specifies tagname structure for Process based systems, as appropriate

All digital inputs **shall** have a textual description that describes the condition that the signal indicates in a **HIGH** state.

All digital inputs **shall** have a category description describing the signal primary purpose which **shall** be one off the following:

Primary Purpose	Significance	Example
Safety.	1	Emergency Stop; Ventilation.
Protection.	2	High High Level; Overload; Ultimate Limit
Command.	3	Start; Stop; Local Manual.
Alarm.	4	High Level.
Status.	5	Running; Open.

Where a signal has multiple purpose then the primary purpose with the highest significance **shall** be used.

All PLC inputs **shall** be 24v dc.

(Note: The PLCs remote I/O in the MCC shall be 120v ac source type)

Pulse inputs that may have a frequency higher than that which is reliably detectable by the PLC **shall** be connected using suitable pulse or high speed input modules to ensure that no pulses go undetected by the system.

7.2.2 Digital Outputs.

All digital outputs **shall** be Tag referenced in accordance with:

- **DD/K0105C/SYST/00025** “Tagname Structures For Mechanical Handling Systems” or
- **dwg no 53-0001**, which specifies tagname structure for Process based systems, as appropriate

All digital outputs **shall** have a textual description that describes the function of the signal in a **HIGH** state.

All digital outputs **shall** be configured to fail to the **LOW** state, i.e. off.

All digital outputs **shall** have a category description describing the signal primary purpose that **shall** be one off the following:

Primary Purpose	Significance	Example
Safety.	1	Watchdog Pulse.
Protection.	2	Weight Within Limits
Command.	3	Start; Close; Run.
Alarm.	4	SCADA Link Failed.
Indication.	5	Park Position Lamp.

All outputs **shall** be 24v dc isolated type, except where special circumstances dictate otherwise.

All digital outputs from a given PLC **shall** be disconnected from plant devices on failure of that PLC’s processor when detected by its hard-wired watchdog device, except for watchdog outputs and status indicating digital outputs.

7.2.3 Analog Inputs.

All analog inputs **shall** be Tag referenced in accordance with:

- **DD/K0105C/SYST/00025** “Tagname Structures For Mechanical Handling Systems” or
- **dwg no 53-0001**, which specifies tagname structure for Process based systems, as appropriate.

All analog inputs **shall** have a textual description that describes the measurement.

All analog inputs **shall** have a category description describing the signal primary purpose which **shall** be one off the following:

Primary Purpose	Significance	Example
-----------------	--------------	---------

Safety.	1	
Protection.	2	Weight Within Limits.
Control.	3	Speed.
Alarm.	4	High Temperature.

Where a signal has multiple purpose then the primary purpose with the highest significance **shall** be used.

All analog inputs **shall** have a category description describing the signal measurement type; e.g. Position; Speed; Temperature.

All analog inputs **shall** have a units description describing the engineering units the signal represents; e.g. Pounds; Feet/Second; Degrees Fahrenheit.

All analog inputs **shall** have a range description describing the signals engineering units range; e.g. 10.00 to 800.00; 0 to 32000.

Where appropriate analog inputs are to be scaled to provide a resolution to two decimal places across the engineering units range.

All analog inputs **shall** have a scale description describing the signal's measurement scale as either Linear or Logarithmic.

All analog inputs **shall** be 4 - 20 mA loop type powered by the PLC.

7.2.4 Analog Outputs.

All analog outputs **shall** be Tag referenced in accordance with:

- **DD/K0105C/SYST/00005** “Tagname Structures For Mechanical Handling Systems” or
- **dwg no 53-0001**, which specifies tagname structure for Process based systems, as appropriate

All analog outputs **shall** have a textual description that describes the function of the signal.

All analog outputs **shall** have a category description describing the signal primary purpose which **shall** be one off the following:

Primary Purpose	Significance	Example
Safety.	1	
Protection.	2	
Command.	3	Valve Position

Alarm.	4	
Indication.	5	Fan Speed

Where a signal has multiple purpose then the primary purpose with the highest significance **shall** be used.

All analog outputs **shall** have a units description describing the engineering units the signal represents; e.g. Pounds; Feet/Second;

All analog outputs **shall** have a range description describing the signals engineering units range; e.g. 10.00 to 800.00; 0 to 32000.

Where appropriate analog outputs are to be un-scaled from engineering units that provide a resolution to two decimal places across the engineering units range.

All analog outputs **shall** have a scale description describing the signal's measurement scale as either Linear or Logarithmic.

All analog outputs **shall** be 4 - 20 mA sourced from the output module in the PLC hardware.

All analog outputs **shall** be disconnected from plant devices on watchdog failure except for status indicating analog outputs.

7.3 Inter-system Interfaces

Data

In addition to interfaces with the operators and plant as referred to above, intersystem interfaces shall be provided between :-

- (i) PLC - PLC;
conveying permissive / inhibit / interlock messages, typically associated with the transfer of product from one process system to another (adjacent) system.
- (ii) PLC - SCADA
 - SCADA to PLC for conveying operators' commands to plant [via PLCs] and
 - PLC to SCADA for conveying plant data (typically process variables, alarms etc). up to SCADA workstations for operator presentation.
- (iv) SCADA - Data Management System (DMS)
These classes of data are discussed in more detail at sections 5.10 to 5.15 inc.

Protocols

Inter-system communications **shall** use internationally recognized interface standards and utilize internationally recognized standard or proprietary protocols.

Information detailing the interface standard, protocol, configuration and connection details of each interface **shall** be provided by BNFL Inc. to the supplier/integrator.

The control system supplier shall then take the lead in ensuring that all external systems are interfaced to and integrated with the ICS to the satisfaction of BNFL Inc.

7.4 Communications Networks

The transmission media shall be selected to provide immunity to electrical interference and a capability for high speed communications. The supplier should consider the use of 'Ethernet' for communications networks.

Communications networks shall include the following features :-

- Be capable of continued operation in the event of failure or removal of any node from the network
- Accommodation variable size message handling
- Provision of communications between a number of devices from different manufacturers without the need for custom interfacing
- Allow peripherals to be connected at various points on the network for programming, down loading / verification of software and data access of all network nodes
- Provision of facilities for monitoring network performance and down loading.

Utilization of the Electronic Document Management System (EDMS), typically for example, during retrieval and viewing of plant documents from a local workstation, shall not cause a significant effect on control system operational response times as a consequence of network loading.

8 System Environment.

8.1 Plant Layout.

The 'Advanced Mixed Waste Treatment Facility' building is located between the Transuranic Storage Area Retrieval Enclosure and the Type II storage modules. Building layout drawings are provided in Appendix 1 to show the locations of rooms and the size of the building which is split into first floor (ground level), second floor interstitial level and penthouse.

Integrated Control System equipment is distributed around the building. The PLC's shall be located in dedicated equipment rooms and located adjacent to their associated termination bays and other electrical and instrument cubicles associated with their system.

The system supplier shall ensure that the ICS hardware is suitably located in the AMWTP facility. The following factors should be taken into account:

- Each item of equipment supplied with the Integrated Control System shall have a unique plant item number by which it can be identified. Plant item numbers will be available from BNFL Inc.
- Operator interfaces identified explicitly with a system in the document refer to local operator interfaces.
- The AMWTF central control room operator workstations shall be used for both automatic and manual operations. These have not been allocated with plant item numbers individually as they are integrated into common consoles. These shall be assigned with a sub number of Integrated Control System equipment, as shall all generic Integrated Control System equipment (i.e. equipment not directly associated with a single system).

8.2 Environmental Conditions.

8.2.1 Site Conditions

Details of site location and environmental conditions, together with the required conditions internal to the facility, are defined in specification - doc. Ref 4.

9 System Attributes

9.1 System Performance

The control system performance **shall** conform to the performance criteria defined in spec. NF 69/3

The system architecture **shall** allow each system to operate independently of all other systems as far as reasonably practicable. Some degree of redundancy **shall** be applied to the control network and system hardware to allow Central Control Room and local fixed workstations to control and monitor more than one system if a failure occurs.

The fixed and portable control workstations **shall** have the same functionality as the Central Control Room workstations.

The system supplier **shall** state the means and impact of improving all performance figures specified in this section should they prove unacceptable in practice.

9.1.1 System Start-up

The system design and configuration shall be such that the time taken to fully start-up the control system from a 'power off' state to full functional availability condition is minimized.

9.1.2 System Shutdown

System design and configuration shall be such that the time taken to perform a controlled shutdown of the control system from a full functional availability condition to a power off state is minimized.

9.1.3 PLC Response.

The PLC's response rates to I/O servicing should not exceed 250 milliseconds.

The PLC's response rates to communications servicing for equipment connected by serial communications links should not exceed 250 milliseconds per end of line device. This includes polling, reading device status and writing command/control parameters.

9.1.4 Digital State Update.

The SCADA **shall** communicate with the PLC's such that any discrete state changes communicated to the PLC should be received and actioned by the controller in less than 3 seconds of the event or request.

The PLC's **shall** communicate with the SCADA such that any discrete plant state changes communicated to the SCADA should be received and actioned by the SCADA in less than 3 seconds of the event or request.

9.1.5 Display Update.

The time taken to draw the static aspects of a full screen display mimic or a display window (including faceplates) **shall** not exceed 3 seconds from the start of the draw with the dynamic aspects updated within 3 seconds from the start of the draw.

9.1.6 Alarm Display.

The system **shall** be capable of displaying at least 700 concurrent alarms.

9.1.7 Alarm Burst.

The system **shall** be capable of logging bursts of at least 700 simultaneous alarms without loss of any alarm data.

The system **shall** be capable of displaying within 10 seconds all alarms from a burst of at least 700 simultaneous alarms.

9.1.8 Alarm Loss.

Alarms **shall not** be lost due to a network break or during periods of heavy network loading.

9.1.9 Processor Loading.

Maximum loading of processors should not exceed 75% of the manufacturers quoted capacity (calculated on a rolling average basis)

9.2 Data Criteria

9.2.1 Natural Language.

The natural language to be used throughout the control system is English (United States).

9.2.2 Data Capacity.

The SCADA **shall** have capacity to store operator actions; plant events; alarms etc. for a minimum of a period of 24 hours.

9.2.3 Data Retention.

In order to provide protection from data storage equipment failure, the SCADA **shall** utilize data mirroring on a separate hard disk for all data, such as operator actions; plant events; alarms; (and any associated computational results/data).

Hard disk storage utilization **shall** not exceed 75%.

On a continuous basis, plant event data **shall** be transmitted to the DMS for archiving. It **shall** be possible for the system to queue this activity for a minimum period of 24 hours.

9.2.4 Data Format.

Data **shall** be entered into the system via bar code readers where bar codes represent an alphanumeric code or via a standard United States keyboard.

Keyboard data entry **shall** be verified using data and type validation relative to the data entry field; e.g. that a valid date of the correct format is entered into a date field and that a numeric value is entered into a numeric field. Valid range checking shall also be included for numerical fields.

9.2.5 Data Validation.

Where practical, data entered by an operator should be validated in order to minimize the possibility of operator error.

9.2.6 Archiving Requirements.

Archiving **shall** be performed by the data management system.

9.3 Availability

The Control System **shall** be capable of supporting a plant that operates 24 hours a day for 365 days a year.

The **availability of the AMWTF** called for by the Control Philosophy document to meet the plant throughput requirements stated therein (based on 330 days per year) is “70% or higher”.

The PES availability is defined within NF0069/3 as $MTBF / (MTBF + MDT^*)$
*Within this URS, Mean Down Time (MDT) is referred to as MTTR - see below.
On the basis of the MTBF and MTTR values specified below, the required availability shall be **99.98 %**

9.4 Reliability.

The required **reliability of the PES control system**⁺, (as a contribution towards meeting the required plant availability) shall have a ‘Mean Time Between Failures’ of at least 17,500 hrs. This is equivalent to 0.5 failures per year.

[⁺ The scope of the PES control system for the purposes of the above reliability definition shall be that equipment listed within the ‘Scope of Supply’ (section 14.2) and excluding ad listed in ‘Exclusions’ (sect.14.3) typically field devices, transducers, actuators etc.]

The system Mean Time To Repair **shall** be 4 hours or less.

The Control Network Hub **shall** withstand any single component failure without loss of more than 25% functionality. A single component failure could lose communications within a whole Area, (e.g. Area 200).

25% of the Control System Network Hub functionality is defined as 25% of the required connections between the nodes of the Network. Note that there is a requirement for many nodes to connect to SCADA Servers and Application / Db Servers; there is a requirement for few nodes to connect to each workstation. Therefore a SCADA node, an Application Server node or a Db Server node represents a far greater percentage of the network hub functionality than a workstation node. The design of the redundant features of the hub **shall** reflect this.

The System Supplier **shall** state his recommendations on the effect on the control system of the following:

1. A single node failure.
2. A Workstation failure.

3. Loss of communications between nodes.

9.4.1 Hardware and Software failure.

Failure of any hardware component **shall** be reported to or by the SCADA as appropriate.

Each system component that communicates to other system components **shall** be capable of alarming or otherwise indicating to users any failure in the system to system communications.

Any software function that fails **shall** alarm or otherwise indicate to users the nature of the failure.

9.4.2 System Recovery.

The Systems Supplier **shall** advise BNFL Inc. of methods and time duration's for recovering the system following failures. This shall be defined in the SDD.

9.5 Maintainability.

9.5.1 Lifespan.

Advanced Mixed Waste Treatment Facility shall be in operation for 15 years and the plant must be maintainable for at least this period.

9.5.2 Maintenance requirements

The system supplier shall submit his maintenance recommendations to enable the availability and reliability requirements [defined at sections 9.3 and 9.4] to be met for the lifespan of the Advanced Mixed Waste Treatment Facility defined at section 9.5.1 . These recommendations shall include :

- any preferred diagnostic methods
- maintenance support
- maximum maintenance time
- mean and maximum time to locate and repair a fault.

9.5.3 Diagnostics.

System diagnostic utilities shall be provided, as described elsewhere in this document, to enable the system condition and performance to be monitored. These shall include CPU, RAM and hard disk storage usage, communications network performance and request response times.

9.5.4 Support.

The system supplier shall provide technical support during the commissioning period (on a 24 hours / day basis) up to completion and handover of the system to operations. The population of the support team shall be to the approval of BNFL Inc.

The supplier shall also make provision for immediate 'back-up' or temporary replacement of equipment becoming unserviceable during commissioning; details to be provided by the supplier in the SDD.

The supplier shall be required to provide assistance in the event of future expansion; details to be included in the SDD

9.6 Adaptability

The supplier shall provide, as far as possible, any anticipated enhancements or additional functional, data volume or performance extensions, where this would affect the spares requirements requested

9.7 Expansion

The system requirements for expansion are specified in NF69/3. In addition to these requirements, provision should be made to allow for up to 50% expansion in the number of plug in points and the serial I/O.

10 Training.

The system supplier shall satisfy the training requirements as identified in NF69/3 Section 14

The system supplier shall, at tender stage, identify training requirements for project team members. The system integrator shall include with the tender response their training plan.

The system supplier shall. include in the SDD a list of recommended training courses.

The system supplier shall include in the SDD a strategy for long-term support of the control system post handover to BNFL Inc.

10.1 Engineer Training Course

This shall describe the detailed engineering aspects of the system. The aim of the course is to train people to test, commission, maintain and develop the system during it's working life. The course shall detail:

- Hardware and Software configuration
- Fault diagnosis and repair
- Methods of implementing changes
- Special precautions

10.2 Operator Training Course

This shall describe the detailed operational aspects of the system. The aim of the course is to train people to operate the system during it's working life. The course shall utilize the operations manual.

11 Documentation.

11.1 Documentation to be provided by Supplier to BNFL Inc.

The system supplier shall meet the requirements for documentation defined by section ten of specification NF0069/3, in terms of the provision, content and format.

Typically, this will include, but not necessarily be limited to, the following :-

- Quality Plan
- Development Plan
- Test Plan
- System Definition Document
- Global System Specification
- Software System Specification
- System Maintenance Manual
- Operator Manual
- Test Specifications*

In addition, for **specific** requirements for :-

- Operation manuals, refer to doc SP_K0105C_PROJ_00004
- C.E. & I. maintenance manuals, refer to doc SP_K0105C_MK_PROJ_00006
- Spares schedules, refer to doc SP_K0105C_PROJ_00007

*Note that relevant source documents shall be supplied by BNFL Inc for validation by system supplier of certain test specifications, as described in section 12.1 para. 3.

These source documents provided thus shall include :-

1. MSD's (mechanical sequence diagrams),
2. MFD's (mechanical flow diagrams)
3. VFD's (ventilation flow diagrams)
4. MHD's (mechanical handling diagrams)

11.2 Documentation Standards

Computer generated documents shall be of the following type:-

1. Word Processor Documents - Microsoft Word
2. Drawings - AutoCad release
3. Spreadsheets - Microsoft Excel
4. Implementation Databases - Microsoft Access

Documentation should use the same versions as currently in use by the System Supplier.

The System Supplier **shall** provide copies (as files) of all documentation prepared using the appropriate BNFL Inc. Standard Computer Package on IBM Personal Computer CD-R media with the final Issue of each Document. If the system supplier is unable to

meet this requirement then any alternative /compatible formats **shall** be advised to and agreed with BNFL Inc. Drawings **shall** be drawn on the BNFL Inc. Engineering Standard Sheet that **shall** be supplied in AutoCad Format by BNFL Inc. BNFL Inc. **shall** issue Drawing Numbers for each Drawing.

The System Supplier is required to provide BNFL Inc. with 'system build information'; e.g. word and bit references; plug and socket details. This information is required to be 'related' to the Control System database CONCISE which has been developed by BNFL Inc. using the Personal Computer based Microsoft Access package and DMS. The CONCISE database has been used to generate the detailed specification documentation such as Operation Schedules, I/O and Alarm Schedules for the Control System.

A Build Information Database linked to CONCISE **shall** be developed by the system integrator to include all relevant system build information (such as PLC Addresses, Termination Details) as agreed with BNFL Inc. and the System Supplier. This database **shall** then be delivered to BNFL Inc. with the system build information incorporated.

12 Testing

The supplier **shall** produce a detailed test plan defining the total scope of testing and system test specifications which detail the functional testing for CAT and SAT. The test plan shall meet the requirements of NF0069/3 Section nine, chapter 45.

Further considerations for testing the ICS (control system layers 1 and 2) are described below.

12.1 Sources of Test Documentation

- Concise

The operational functionality requirements of the PLC's and SCADA are reflected in the CONCISE database. CONCISE includes interlocking, sequencing, alarm and message handling of the system, and references to mimic documents, detailing the operator displays and dynamic attributes of those displays.

The preparation of the control system software shall involve the implementation of CONCISE and thus, inherently, the user functional requirements.

Since the CONCISE database has the facility to automatically generate test documentation, then this shall be used as the principal source of test documentation against which the final software **shall** be tested for functionality wherever possible.

- SSS

The System Software Specification (SSS) shall be produced by the system integrator during the course of software preparation to specify the details of his implementation, including structure, addressing and aspects of function over and above the scope of defined user requirements.

The SSS shall be used in conjunction with the CONCISE documents for system testing both during CAT and at site

- SPD's / Other

For systems integration testing, commissioning, etc, where the objective is to confirm performance, specific, manually derived system performance demonstration test documents (e.g. SPD's) shall be used in each case to confirm the relevant objective. These test doc's shall be independently validated by MSD's, MFD's, VFD's and MHD's etc. as appropriate to each system and supplied by BNFL Inc.

12.2 Simulation Equipment

Simulation equipment used to carry out the tests described in some of the following sections will be supplied by the system implementers. Simulators for training the plant operators lie outside the scope of this Specification (see 14.2)

12.3 Testing Phases.

There are eleven distinctly different phases of Software testing, as listed below, each with associated responsible personnel for carrying out the tests and documenting the results.

1. Device Template Testing
2. Device Template CAT
3. Module Testing
4. Mimic Approval
5. Pre-CAT System Testing (Using Simulators)
6. System CAT (Using Simulators)
7. Pre-CAT Integration Testing (Using Simulators)
8. Integration CAT (Using Simulators) – without DMS
9. ICS - DMS Integration CAT (Using Simulators) – with DMS
10. SAT Test
11. Commissioning SPD's

12.3.1 Device Template Testing.

The first set of tests, referred to as 'device template testing', normally takes place at the system suppliers premises, as the device template and the associated mimic device faceplate* is produced. [* SCADA Device / Diagnostic Display]

However, since use is being made of BNFL's generic device library which has previously been tested, this phase shall be limited to any instances of new device types not already in the library.

Each such new device shall be tested against its definitive specification, after approval. Though undertaken internally, such tests must be documented and signed as complete and available for BNFL Inc. inspection prior to Device Template Customer Acceptance Testing (CAT).

12.3.2 Device Template CAT.

As the device templates shall be delivered in advance of the rest of the control system, any new device templates shall be CAT tested separately.

12.3.3 Module Testing.

The third set of tests take place at the system suppliers premises, as larger sections of code (modules) are developed. Typical modules may be generic e.g. comms modules, signal conditioning modules etc.

This is known as module testing and takes place as each separate logical part of the code is produced to verify correct operation. Though undertaken by the supplier

internally, these tests must be documented and signed as complete and available for BNFL Inc. inspection prior to Customer Acceptance Testing (CAT).

12.3.4 Mimic Approval

The system supplier must submit his implementation of mimic screens, and have had these approved for layout, ergonomics and features prior to commencing system testing - see 12.3.5. - during which mimic functionality will be checked.

Although not a test phase as such, it is considered thus here for ease of description.

12.3.5 Pre CAT System Testing (Using Plant Simulation).

The fifth set of tests [known as Pre- CAT testing] is carried out on the code for a complete system. The tests are conducted at the system suppliers premises, and takes place once all modules in a given system have been successfully tested.

Though undertaken internally, these tests must be documented and signed as complete and available for BNFL Inc. inspection prior to Customer Acceptance Testing (CAT).

For PLC Systems these tests **shall** be :-

- based on the CONCISE based test documentation, support documents and mimics
- carried out against a plant simulator

12.3.6 CAT System Testing (Using Plant Simulation).

The sixth phase is CAT where BNFL Inc. engineers witness the testing of all the tested modules that form a given process system. This testing phase **shall** be carried out to BNFL Inc. source documentation, including CONCISE based documentation.

BNFL Inc. **shall** also ensure that the SSS produced by the system Supplier reflects the software undergoing test.

For PLC Systems, these tests **shall** be based on the CONCISE SPD documentation and **shall** be carried out using an approved software simulation package.

12.3.7 Pre-CAT Integration Testing (Using Simulators).

The seventh phase of testing **shall** involve large groups of PLC systems plus SCADA and either use the appropriate elements of the DMS or simulate their interface(s).

Systems at the interface between two plant areas **shall** be included in the Integration Tests that cover each of those areas.

The PLC's **shall** be connected to Plant Simulators.

Test documentation **shall** be written to ensure that data is stored in the locations specified.

13 Installation and Commissioning

The requirements of spec. NF69/3 shall be met.

Each process viewing position (window) on plant **shall** have either a local fixed workstation or a plug-in point for a portable workstation . In addition, area operator workstations **shall** be available within the Central Control Room, these workstations **shall** be available during commissioning for such duties as:

1. Control functions/displays for System Performance Demonstrations.
2. Access to Programmable Electronic System (PES) programming software for system debugging (as well as locally).

The systemization philosophy covered in DD/K0105C/SYST/00001 “Systemization Philosophy” shall ensure that phased delivery and installation of mechanical equipment can proceed in tandem with control system setting to work and commissioning.

14 Commercial Considerations

14.1 Project Milestones.

For relevant project milestones, reference should be made to the 'Project Schedule'.

14.2 Scope Of Supply.

The Control System **shall** be supplied under one contract. The Control System **shall** include but not be limited to:

- Computers, and Equipment detailed elsewhere in this document.
- PLC's and Cubicles.
- Communications Network equipment and Cubicles
- All Interface modules and connectors for the plant networks.
- All programming workstations and service tools (Hardware and Software) required to commission and maintain the system including the Code Management System (see section [14.8 Implementation Techniques)
- All proprietary software packages and licenses necessary to support system operation diagnostics and maintenance.
- All configuration tools and compilers necessary to reconfigure the system.
- All cables with plugs/sockets required to connect all items of equipment supplied under this contract.
- All system software and supporting design.
- Documents and test requirements as detailed in BNFL Inc. specification NF69/3.
- Final delivery to site.
- Setting to work on site - (Installation and commissioning **shall** be done by BNFL Inc. with support from the System Supplier)

14.3 Exclusions From The Scope Of Supply.

Exclusions from the scope of supply are:

1. All field devices such as switches, solenoid valves, motors and actuators
2. All plant cabling.
3. All electrical Motor Control Centers and drive cabinets.
4. All plant devices such as weighers and bar code readers.

Plant simulation software for training operators shall be supplied by others

The final system architecture **shall** be agreed with BNFL Inc. before any equipment is ordered by the system integrator.

Hardware **shall** be chosen to provide commonality and reduce spares holding. System supplier **shall** submit a schedule of drawings to be produced. BNFL Inc. shall issue drawing numbers for these.

Instem have been selected by BNFL Inc. to assist in the implementation of this contract. Subcontracting of any work to companies other than Instem **shall** only be permitted with the express agreement of BNFL Inc.

All system integration both Software and Hardware **shall** be at the system supplier's premises.

14.4 Preferred Equipment.

14.4.1 Software

The Control System Software used for the Advanced Mixed Waste Treatment Facility **shall** be

1. PLC Programming tool - Groupe Schneider Automation ConCept, version 2.0 (or higher)
2. Operating System for SCADA Servers and all Workstations :- Microsoft Windows 2000
3. SCADA Server & Client application :- US Data FactoryLink version 7 Webclient for MS-WIN NT4.0.

The System Integrator **shall** inform BNFL Inc. of release dates for imminent higher versions of the above products.

The System Integrator **shall** ensure that at CAT test stage, the system only utilizes the latest version of the above products except where a concession to do otherwise has been expressed by BNFL Inc.

Plant simulation software for testing shall utilize PICS software package and **shall** be developed by the Supplier.

14.4.2 Hardware

The following control system hardware for the Advanced Mixed Waste Treatment Facility **shall** be utilized:

1. PLC's - Modicon TSX Quantum Range & Momentum I/O

2. Network Equipment - 3Com

An initial proposal for AMWTP Control System Architecture is shown in Appendix 3.

14.5 Deliverables

The design is to be in accordance with BNFL Inc. Standard NF69/3. All aspects are within the scope including:

1. Detail design
2. Hardware supply
3. Software design and implementation
4. Testing
5. Full integration

Technical Queries, Memos, Agendas and Minutes of meetings and draft copies of any reports or specifications including SSS and SDD, may be sent via e-mail with a hardcopy to back it up. X400 and Internet Addresses shall be supplied for all BNFL Inc. Contacts. Approved Reports, and Specifications **shall** be posted or handed over at progress / technical meetings - see contract interface document and project schedule for detailed procedures.

14.6 Methods & Approaches

14.6.1 Use of CONCISE - General

Specific design requirements for control of the plant **shall** be defined using the 'CONCISE' specification tool. Details governing the use of using the 'CONCISE' specification tool are mandated in document ref.13.

14.6.2 Prototyping

The control system supplier should complete a prototyping exercise, the results of which when agreed by all parties, shall form the basis of development for the remainder of the systems.

14.7 Compliance With Specification

The following B.E.Ltd specifications **shall** apply. System supplier **shall** state his compliance to these specifications:

1. NF69/3 - Programmable systems - Engineering Specification
2. SP_K0105C_SYST_00004- General Specification for Panels & Junction Boxes.
3. This URS

Compliance with section four of NF69/3 is NOT required. Comply instead to SP_K0105C_SYST_00004 General Specification for Cubicles, Panels and Junction boxes.

The related documents specified within NF69/3 **shall** apply with the exception of :

1. Project Quality Procedures: Control and registration of drawings
2. NF 0129/1 - Electrical Interference.
3. British & Other Standards- These should be replaced by the most appropriate US standards.

14.8 Implementation Techniques

All Source Code **shall** be written in accordance with the current version of the ILW Coding Standards.

The System Integrator **shall** revise the coding standards if required in light of the experience gained during this contract.

All PLC code for Device Templates **shall** be implemented using only the IEC 1131/3 library of function blocks.

The integrator **shall** seek acceptance from BNFL Inc. before using any PLC functions or modules that are not IEC 1131/3 compliant.

Any revisions to the Coding Standards **shall** be submitted to BNFL Inc. for approval. BNFL Inc. retains ownership of the Coding Standards and may issue them to other companies tendering for or in contract to supply PES systems.

The system integrator **shall** avoid duplication of code and instead develop generic solutions (such as code modules that can be called with parameters). The System Integrator **shall** identify any duplication within the CONCISE system specifications and develop generic solutions.

The system integrator **shall** hold all source code in a Code Management System. Configuration management tools for PLC / SCADA are PVCS.

Modules **shall** be under strict version control once submitted for testing. All Changes **shall** be referenced to an initiating document either:

- | | | |
|------------------------------------|---|------------|
| 1. A TQ Response |) | See |
| 2. A Contract Variation |) | Project |
| 3. A SRN (Snag Rectification Note) |) | Procedures |

The Code Management System **shall** be frequently backed up.) ditto

All Software released for test shall be archived at that version.) ditto

The Code Management System, associated hardware (including backup device) and all software (inc. archived versions) shall be delivered to INEEL immediately after control system handover to BNFL Inc.

Appendix 1 - Building Layout Drawings.

51-0002	TREATMENT FACILITY FIRST FLOOR PLAN GENERAL ARRANGEMENT
51-0003	TREATMENT FACILITY SECOND FLOOR PLAN GENERAL ARRANGEMENT
51-0004	TREATMENT FACILITY INTERSTITIAL PLAN GENERAL ARRANGEMENT
51-0005	TREATMENT FACILITY PENTHOUSE & ROOF PLAN GENERAL ARRANGEMENT
51-0006	TREATMENT FACILITY BUILDING ELEVATIONS
51-0007	TREATMENT FACILITY BUILDING ELEVATIONS
51-0008	TREATMENT FACILITY BUILDING SECTIONS
51-0009	TREATMENT FACILITY BUILDING SECTIONS

COPIES OF ABOVE DRWGS AT CURRENT REVISIONS TO FOLLOW

Appendix 2 – Ergonomics Requirements and Guidelines for VDU-Based Operator Interfaces

CONTENTS

1	Introduction	4
2	Scope	5
3	Definitions.....	6
4	Related Documents	7
5	Visual Display Units (VDUs).....	8
5.1.1	General.....	8
5.1.2	Fixed VDUs.....	9
5.1.3	Portable VDUs.....	9
5.1.4	Connection of VDU's to the Network.....	12
6	Operator Interaction	13
6.1.1	General.....	13
6.1.2	Distribution of Operator Control	15
6.1.3	Level of Automation	16
6.1.4	Data Entry	17
6.1.5	Event Log.....	18
6.1.6	Interaction Devices.....	18
6.1.7	System Access/Security.....	20
7	Information Presentation.....	21
7.1.1	General.....	21
7.1.2	Ergonomic Principles.....	22
7.1.3	Display Organization and Structure	23
7.1.4	Navigation.....	24
7.1.5	Display Selection	25
7.1.6	Animation	26
7.1.7	Mimic Displays.....	27
7.1.8	Process Lines	30
7.1.9	On-Screen Control and Display Equipment	31
7.1.10	Trend and Charting Facilities.....	32
7.1.11	Operator Messages.....	33
7.1.12	Tables and Lists.....	34
7.1.13	Titles, Labels and Tags.....	35
7.1.14	Display of Sequence Information.....	36
8	Alarms.....	37

8.1.1	General.....	37
8.1.2	Alarm Presentation.....	38
8.1.3	Auditory Alarm Signals.....	39
8.1.4	Alarm Banner.....	40
8.1.5	Mimic Displays.....	41
8.1.6	Alarm Summary Lists.....	41
8.1.7	Alarm History List.....	42
9	Color.....	43
9.1.1	General.....	43
9.1.2	Color Coding.....	43
9.1.3	Combinations.....	49
10	Text Attributes.....	50
10.1.1	Font/Case.....	50
10.1.2	Size.....	50
10.1.3	Spacing.....	51

1 Introduction

Ergonomics and human factors are concerned with the design of systems so that the human operator and the equipment can work together safely, effectively and efficiently.

Within AMWTP, the majority of plant systems will be controlled, monitored and supervised via interfaces on visual display units (VDUs). VDU-based operator²-interfaces form the main human operator-control system interface via the plant's Supervisory Control and Data Acquisition (SCADA) system – or Integrated Control System (ICS), as on AMWTP. In addition, interaction with other systems as diverse as the Data Management System (DMS), Electronic Document Management (EDMS), Closed Circuit Television (CCTV), Access Security and Radiological Surveillance System (RSS) will be via VDU-based operator interfaces, possibly on a number of different display units. These later systems will remain separate and will not be integrated into a single interface.

The human operator within the process plant will use a number of these systems (e.g. ICS, DMS, EDMS and CCTV) simultaneously to complete any particular task. The operator will need to integrate the available information in order to complete tasks safely, efficiently and effectively. Inconsistencies in the manner in which information is displayed will adversely effect the operator's ability to integrate information. By designing interfaces in accordance with the requirements and guidelines presented in this document a standardized approach to information presentation of VDU-based operator interfaces will be produced. The existing systems at the INEEL Site systems must also be considered if they are to interact with the AMWTP computer-based systems and involve operator interaction.

There may be a number of difficulties in satisfying every ergonomics criterion. Therefore, the application of ergonomics principles must inevitably result in compromise. Steps such as identifying points as either mandatory or advisory guidelines aims to aid this process³. Additionally, by prioritizing the criteria and undertaking evaluation exercises, it is possible to develop an operator interface, which would meet the criteria of an ergonomics audit and enhance safety and operability. Finally, system prototyping of systems will be completed to ensure all parties (e.g. Operations/Client groups, design engineers, human factors specialists, etc) are content with the interface.

This document supports the “AMWTP Control System User Requirements Specification” (- or URS). This document provides the detailed requirements for the operator-interface aspects of the ICS. The main principles are included in the URS.

² Operator refers to anyone who directly operates the plant processes and equipment. This includes operator-maintainers, team leaders and shift managers, as appropriate.

³ A human factors specialist should be consulted to aid the evaluation of any trade-offs / compromises.

2 Scope

The purpose of this document is to provide ergonomic guidelines for engineers during the design and build stages of the VDU-based operator interfaces for AMWTP. The guidelines are intended to be used directly by design personnel and the control systems integrator to ensure good human factors and consistency of interface design throughout AMWTP. The guidelines also briefly cover issues regarding hardware and the positioning of VDUs on the plant. The requirements have been classified as either mandatory or advisory guidelines.

The guidelines are applicable for all VDU-based operator interfaces. This includes the ICS, DMS, EDMS, RSS, CCTV, Security systems, etc. This document provides designers with the information that will encourage good design and consistency. Specific supplementary guidance for the design of the DMS will be provided at a later date to ensure that all of the specific design aspects of the DMS operator-interface (e.g. format and presentation of forms, reports, etc) are fully addressed.

A number of additional documents cover human factors/ergonomic issues outside the scope of the present document. Ergonomics guidance for process plants concerning the design of conventional control and display equipment for use both in the CCR and locally on plant can be found in “Ergonomic guidelines for the design of control desks, panels and gloveboxes”. Detailed ergonomics guidance concerning the design of areas where remote handling tasks will be completed can be found in “Robotics and Remote Handling: Ergonomics Design Manual”.

3 Definitions

The following abbreviations and definitions are utilized in this Appendix:

- Shall** Indicates a guideline that is a *mandatory* requirement.
- Should** Indicates a more general recommendation considered to be good design practice, and *should* be implemented, if possible.

The requirements and recommendations contained within each sub-section are not prioritized.

4 Related Documents

The following documents are directly related to these guidelines:

Generic Specifications:

13490/01	Ergonomics Requirements and Guidelines for the Design of Control Desks, Panels and Gloveboxes
13490/02	Ergonomics Requirements and Guidelines for VDU-Based Operator-Interfaces
BNFL CDDC (99) P361	Robotics and Remote Handling: Ergonomics Design Manual.

5 Visual Display Units (VDUs)

General⁴

Mandatory Requirements

1. Within process plants, operators will utilize a number of different display units to access the same systems (i.e. different VDU types and different VDU sizes). A single operator interface display design **shall** be utilized on all the different types of hardware. The design of the user interface **shall** be completed on the hardware with the poorest performance (i.e. the slowest, lowest resolution, smallest screen). This will ensure consistency and ensure that operators at all locations can readily utilize the operator-interface.
2. CRT, LCD and TFT display technologies may be utilized. Each of these display technologies has different strengths and weaknesses that must be understood to develop a suitable interface. Each different type and/or size of display unit to be utilized on the plant **shall** be evaluated. This will ensure that an appropriate user interface is developed for operators at all operating locations. Each type of display **shall** be checked to evaluate and verify key aspects such as color consistency, color contrast and discrimination, etc.
3. Each workstation or console **shall** contain enough VDU's to simultaneously display all the relevant information required for an operational decision.
4. There **shall** be no perceptible flicker on screen.
5. Brightness levels **shall** be adjustable.
6. Tilt-able CCTV monitors (up, down, left and right) **shall** be provided to allow the operator to view monitors directly rather than at an oblique angle.
7. The center of all VDU monitors **shall** be located below eye height, i.e. 3'8" on a seated console and 5'0" on a sit-stand console or vertical panel.
8. Space at local plant workstations to accommodate and operate all appropriate fixed and portable control and display units **shall** be provided at each workstation.
9. The system **shall** be flexible to accommodate future hardware and software expansion.
10. Well-designed maintenance instructions and facilities **shall** be provided.
11. A screen saver function **shall** be provided on all systems/VDUs to ensure images can not be burnt onto CRTs.

Recommendations

1. If a dot matrix character generation is used, a 7 x 9 pixels, or higher resolution, matrix **should** be utilized.
2. If using raster lines, there **should** be a resolution of 10 raster lines per character height, with a minimum of 1.3 per mm.

⁴ Guidance concerning interaction devices (including keyboards, trackballs, etc.) is given in Section 6.

3. The total overall number of monitors (CCTV or VDU) **should** be limited to four per operator to avoid overloading the operator with information from diverse systems. If more than a total of four CCTV and VDU monitors are necessary, the number of operators **should** be increased and/or the division of information be reorganized between pages and screens to enable operators to work at the console. Large banks of screens **should** be avoided.
4. In local plant areas, additional space **should** be provided where permanent monitors are situated to allow additional VDU-based equipment to be used when necessary, e.g. additional CCTV monitors for the completion of maintenance tasks. The space requirements for additional equipment, such as printers, **should** also be considered.
5. The consoles or workstations **should** have a sufficiently large, low reflectance surface. They **should** allow the flexible arrangement of the VDUs, keyboards, documents, communication facilities and related equipment.

Fixed VDUs

Mandatory Requirements

1. All desk/console mounted VDUs **shall** be adjustable. Rotation around both the x and y axis's **shall** be provided.
2. All local plant mounted fixed VDUs **shall** be mounted on brackets that allow adjustment in the x and y axes and allow rotation around the y axis.
3. All units that have TFT or LCD screens **shall** undergo assessment to ensure that they are capable of displaying all the necessary information and colors effectively from a range of operating positions, e.g. from directly in front and to the side of the display unit.

Recommendations

1. To reduce the requirements for operators to transport equipment around the process plants, the positioning of VDU's permanently at workstations **should** be provided, where appropriate. In particular, this **should** be considered at remote locations, operating positions that are reached via stairs, and any operating positions inside controlled (Zone 3) areas, etc.

Portable VDUs

Mandatory Requirements

1. Portable control and display equipment **shall** be truly portable (i.e. they should be light, easy to carry, etc). Operators will be required to carry such equipment over relatively long distances, up and down stairs and lift the device over a vertical distance of up to 6'0".
2. Portable units **shall** be secure when set-down at the operating position (i.e. it should be difficult to knock any unit off a control station or accidentally disconnect it from the network).
3. The display screens of portable VDU's **shall** be adjustable. This will allow potential problems of glare and reflection to be overcome and also aid operator comfort whilst using this equipment.

4. Where laptop devices are utilized, they **shall** allow the operator to tilt the screen.
5. Where a single solid unit is utilized, the VDU **shall** be mounted on a bracket that allows adjustment in the x and y axis's and allow rotation around the y axis.
6. During transit, portable units **shall not** constitute a hazard that may lead to injury to the operator or damage to the equipment. Where the climbing of stairs can not be avoided, the portable unit **shall not** increase the hazard of traversing stairs (ie. by obstructing the operators' view of stairs, occupying both hands to prevent usage of handrails, etc). Solutions such as an 'over-the-shoulder' carry strap **shall** be considered.
7. All removable/portable units **shall** have some form of handle provision.
8. Handles **shall not** interfere with equipment operations or maintenance.
9. The handle position **shall** allow the unit to be withdrawn from racking/housing, and carried without interfering with walking.

Recommendations

1. Simple instructions concerning the operation and maintenance of the portable VDU **should** be clearly printed on the portable unit.
2. Where possible, trolleys, or other equipment, **should** be utilized for the transportation of portable control and display equipment.
3. Operators **should not** be required to climb stairs whilst carrying portable control and display equipment. This increases the risk of injury and damage.
4. General guidance for manual handling operations **should** be followed. These state that manual handling operations **should** be avoided as far as is reasonably practicable (by redesigning the task to avoid moving the load, automating or mechanizing the process). A suitable and sufficient assessment **should** be completed for any hazardous manual handling operations that can not be avoided. The risk of injury from the task **should** be reduced so far as it is reasonably practicable. In particular consideration **should** be given to the provision of mechanical assistance. Where this is not reasonably practicable, then other improvements to the task, the load and the working environment **should** be explored.
5. Manual handling guidance does not set specific weight limits. An ergonomics assessment of the relevant factors (e.g. weight, size and shape of object to be lifted, distance to be carried, etc.) **should** be carried out. In general, operators **should not** be required to lift weights in excess of those shown in Table One. The table represents limits for static lifting tasks, limits for carrying loads will be lower than these.

Table One: Recommended Combinations of Height and Weight Limits for Lifting

Weight (lbs)	Height to be Lifted					
	0 – 1’	1’ – 2’	2’ – 3’	3’ – 4’	4’ – 5’	5’ – 6’
0 – 15	1	1	1	1	1	1
15 – 20	1	1	1	1	1	2
20 – 25	1	1	1	1	2	2
25 – 30	1	1	1	2	2	2
30 – 35	1	1	1	2	2	MLD
35 – 40	1	1	2	2	2	MLD
40 – 45	1	1	2	2	2	MLD
45 - 90	2	2	2	2	MLD	MLD

Key: 1 = Suitable for one person lift
 2 = Suitable for two person lift (label as such and provide additional hand-holes/handles)
 MLD = Use a mechanical lifting device (again items should be labelled)

6. Where a single handle is provided, it **should** be placed over the center of gravity. If two or more handles are provided they **should** be equidistant from the center of gravity of the object to be carried.
7. The clearance distances for a one handed bar or recessed type handle **should** exceed 2” between the inside of the handle and the item to be carried, 4.5” inside the handle to accommodate the width of the hand, and 2” either side of the handle to allow the handle to be easily grasped. These recommendations are for bare hands, a gloved hand will require greater clearance⁵.
8. The use of handles as locking devices to secure components in place **should** be considered.
9. The relative positions of the operator(s) and the unit at the start and finish of the lift/carry **should** be considered. This will assist in determining the correct shape and location of handles.

⁵ For a gloved hand the measurements should exceed 2.5” between the inside of the handle and the item to be carried, and 5” inside the handle and 2” either side. If the operator is wearing arctic mitts (ie. big gloves) the measurements should exceed 4” between the handle/item, and 5.5” to accommodate the width of the hand and 4” either side of the handle.

Connection of VDU's to the Network

Mandatory Requirements

1. A simple connection/disconnection system **shall** be utilized for both power and communication cables.
2. All portable control/display units **shall** connect to the control network via a light, robust and easy to orient device (eg. the connection plug should fit in one hand).
3. Connections **shall** be secure and **shall** ensure that an item can not become disconnected during use (eg. by the use of a plug that can be secured with screws).
4. A suitable connection cable (in terms of quality and length) **shall** be provided.
5. Excessive cabling **shall** be avoided. Any cabling that is used to connect equipment will not constitute a trip hazard. An integral cable store **shall** be considered within equipment/furniture.
6. All portable control and display equipment **shall** include instructions concerning connecting equipment to the main network.
7. The operator **shall** be provided with information at the operating location to ensure that the portable workstations can be logged on to the system accurately (ie. signs to show the operating location, connection point ID, orientation information, etc).

Recommendations

1. Storage space within portable control/display equipment **should** be provided to accommodate and secure the connection equipment and associated cabling.

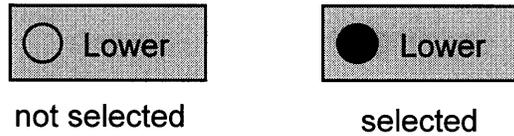
6 Operator Interaction

General

Mandatory Requirements

1. Control and display design and operation philosophies **shall** be applied consistently throughout the plant.
2. Control and display arrangements **shall** be consistent at all operating locations.
3. Opportunities for operator interaction that are available from each VDU-based interface **shall** be clearly indicated and distinguishable from other areas of the screen (eg. easily distinguishable target areas, three dimensional buttons, greying of non-available functions, items do not suddenly appear and disappear from the interface without interaction, etc). Only two levels of coding **shall** be used ie. options are either greyed or not greyed. ‘Greying’ is superior to making them invisible.
4. When the system is operating in Automatic mode, the text on control selection keys for individual items of equipment **shall** appear ‘greyed’.
5. All control movement **shall** be provided with adequate feedback to the operator to indicate that the control has been actuated. For example, use a response ‘click’ or other tactile/audible control and visual feedback, such as response message, symbol change, color change, etc.
6. Control actions that change the plant conditions **shall** require more than one keystroke, with the option to cancel after the first.
7. Where control actions require confirmation (i.e. selecting a sequence and then initiating it), separate actions **shall** be performed. The operator selects the sequence with one ‘click’ of the select button on the interaction device and initiates the sequence by moving the cursor over another target (located elsewhere on the screen eg. an “Execute” button) and ‘clicking’ again.
8. In the event of the requirement for the operator to update the Waste Tracking System (WTS) database (eg. following operator intervention or when changing from Manual to Automatic mode), the system **shall** prompt the operator to verify the accuracy of the WTS database. This may not necessarily be required for each item of information in the database except for the plant systems/areas where operations were undertaken.
9. To reduce the risk of accidental activation, ‘double clicking’ on a single target area **shall not** be used as a confirmation step.
10. The feedback to indicate that a selection has been executed **shall** be **identical** in both automatic and manual mode.
11. When options are selected, the on-screen buttons **shall** appear ‘depressed’. If this is not an obvious change of status (ie. the depression is too subtle), then in-fill indicators **shall** be added to the appropriate keys. See Figure One. The button **shall** remain depressed until the action has been completed. On-screen buttons that actually initiate the control action (eg. ‘Execute’ and ‘Exit’ keys), **shall not** be given these indicators.

Figure One: On-Screen Control Selection Buttons



12. The system **shall** prevent the re-selection of current commands or additional selections until the current command is complete.
13. Unavailable and disabled control actions (eg. sequence initiations and mode of control changes) **shall** be ‘greyed out’.
14. A single tone, followed by visual feedback, **shall** accompany an error (or ‘illegal’ entry) made by the operator during data input or control actions
15. Visual feedback from the system **shall** inform the operator not only that the control has been operated, but that the action it is controlling has been effected. The visual signal the operator receives means, for example that, the valve has closed successfully, and not merely that the control has moved, or that the signal has been sent, or even that the signal has reached the actuator.
16. Clear and concise information regarding operations being inhibited by trips, interlocks, sequences, other operators, etc, **shall** be provided.
17. The operator **shall** be able to recover from an input error easily.
18. An operator confirmation step **shall** be provided wherever there may be a high operational or safety penalty. The confirmation prompt messages **shall** emphasize the potential operational or safety penalty.

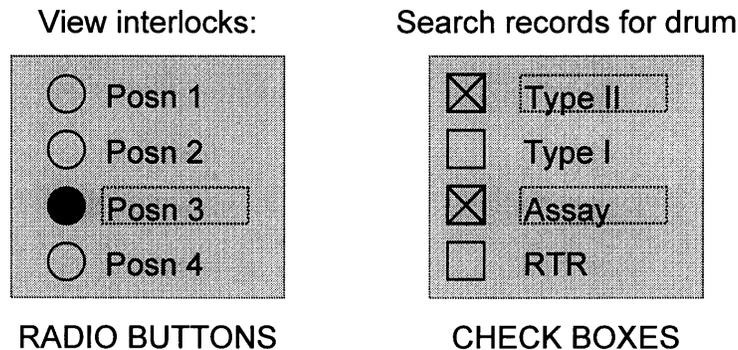
Recommendations

1. The majority of operator interaction with VDU-based interfaces **should** be via a point and click method with a trackball. The operator **should** be required to position a cursor over a visible ‘hot-spot’ on the GUI and press the selection button on the trackball.
2. The operators **should** be given as much direct feedback as possible, and not indirect feedback. This may lead to a delay in response feedback (eg. if a valve takes thirty seconds to close). However, this is preferable to misleading information. The optimal design is that when the operator initiates a control action, a signal occurs indicating the control has been sent. A second signal is given when the action has been effected This **should** be achieved by an item on the display flashing to show the action is in progress and then going steady when the action is complete.
3. The operator **should** be provided with information concerning the progress of lengthy operations or other actions in progress (eg. the use of indications such as “% Complete”, progression of line/bar, etc).
4. If the application response time is longer than three seconds, a delay message **should** be presented to the operator, by the application software.
5. Re-set functions **should** be provided. For example, functions such as ‘Return to Main Menu’, step backwards, previous pages, or return to a default setting etc, **should** be included.

6. An on-line help system **should** be provided. This system **should** be consistent (but not necessarily identical in format, presentation, etc) with any other VDU system or paper based manuals that are provided.
7. When the system is operating in Manual mode, prior to a control selection being made, the 'Execute' key **should** be 'greyed'. Following a control selection being made, the 'Execute' key should be shown in its normal state (ie. not 'greyed') to highlight that the control action can be executed.
8. Control keys **should** occupy standardized locations.
9. Radio buttons should be utilized for exclusive/or options and check boxes **should** be utilized for multiple/and selections. See Figure Two.

Do not use radio buttons if the operator is able to initiate a control action via a single 'click', or the system requires a default selection. Use an on-screen target button for control actions. Radio buttons and check boxes **should** be used for non-control actions, such as formulating searches, display information request, etc

Figure Two: Examples of Radio Buttons and Check Boxes



Distribution of Operator Control

Mandatory Requirements

1. It **shall** only possible to initiate control actions and sequences whilst displaying a screen providing all the necessary information for making the particular decision that the control action is correct ie. the associated mimic display.
2. In Manual mode, only one local workstation **shall** be able to control a parameter or device, although more than one workstation may view the parameter/item simultaneously. In Automatic mode, control may be available from more than one local workstation, as appropriate.
3. In the CCR, only one console (comprising a number of VDU workstations) **shall** be able to control a parameter, process item or sequence, although more than one console may view the parameter/item simultaneously.

4. In the CCR, on each individual console, all of the VDU workstations **shall** be able to control a parameter, process item or sequence for the plant area(s) to be controlled and monitored at that particular console. ie. the distribution of control is between the consoles and not the individual workstations on the console. This requirement also applies to the BMR.
5. Certain VDU's, or a sub-set of the displays, **shall** be configured for information-only/monitoring purposes. These displays **shall** present all the information that is needed for monitoring purposes, but it **shall not** allow any control actions to be completed. These VDUs and/or displays **shall** be utilized for the Team Leader, Shift Manager and other managerial or support personnel.

Recommendations

1. In Manual mode, the first operator to access a system **should** retain control over the device until he/she gives permission otherwise.
2. Changing between manual and automatic modes of control **should** be able to occur on a system-by-system or scheduler basis (ie. when manual is selected, all drives within that system or scheduler will be put into manual mode). All system scheduler or groups must be idle before a change from automatic to manual mode is permitted.
3. Changing between manual and automatic modes of control **should** be an available function undertaken near the top of the display hierarchy eg Level 2. With some systems it may be appropriate to place individual items in manual mode while the rest of the system remains in automatic mode. Where this is the case, the auto/manual change over **should** be carried out at a lower level in the hierarchy eg. Level 5. See also Section 7.4 Navigation.
4. Information on the changes resulting from a auto/manual change over (eg. which devices will or will not go into manual mode, which sequences will stop, etc) **should** be displayed to the operator prior to the change over being completed.

Level of Automation

Mandatory Requirements

1. The level and type of operator interaction with the system **shall** ensure that the operator maintains an up-to-date awareness of the status of the equipment and processes. Possessing a comprehensive mental model of the process and equipment is essential for dealing with novel fault conditions and achieving production targets. An intermediary level of automation **shall** be provided (ie. human-centered automation).
2. The operator **shall not** be required to solely undertake passive monitoring.
3. The system **shall** require operator interaction in operations that are significant/related to safety or are important to product quality, throughput and equipment availability.
4. Key decision (eg. determining the drum route, specifying when to initiate an important stage in the process, etc) **shall** incorporate some level of operator involvement or consultation.

Recommendations

1. The system **should** require the operator to interact with the whole of the plant area or system that they currently have access to. There **should** be a greater level of interaction with the main sub-systems or areas which may be subject to important alarms, than areas of lesser importance. Areas **should not** be neglected entirely.
2. The form of operator interaction **should** take the following:-
 - requirement to check the status of an item of equipment
 - requirement to check that a variable is within a specified range
 - selection of a sequence
 - initiation of a sequence
 - entering data – possibly from another system or received from another operator
 - initiation of the continuation of a sequence
 - an authorization

A combination of two or more of the above is often appropriate. The preference is to involve the operator in selection tasks, rather than implementation.

3. For key parts of the process or operations, a series or group of operator tasks **should** be provided that form a meaningful objective (rather than single isolated interventions). This **should** aim to make the operator utilize more than one system and integrate the information (eg. from the CCTV system, ICS, communication, DMS) or different parts of the same system.
4. A subset of the operator tasks **should** require the operator to utilize their knowledge of the plant, processes and control systems (eg. an assessment of a situation, evaluate alternative actions, make decisions, schedule sequences, etc).
5. As a general rule, batch process **should** require the operator to be involved at notable events (eg. at the beginning and end of a sequence), and continuous processes **should** require the operator to actively monitor the process/sequence at suitable predetermined intervals (- depending on the importance of the sequence, etc).
6. The level of automation **should** take into account the need to avoid workload peaks and troughs.

Data Entry

Mandatory Requirements

1. The system **shall** provide prompts for the operator as to when data entry is required.
2. Any erroneous entry **shall** remain displayed until corrective action has been under taken (ie. it does not disappear when the error message appears).

Recommendations

1. To aid data entry, the format and quantity of data that is required **should** be explicitly stated.
2. Prompts to the operator **should** clearly state the required action.

3. Underscores and cues **should** be used to indicate the length and type of data required, e.g. “Enter data here ____”; “Enter the value for alarm limit ____ E+ __ Gv”, etc.
4. Error messages **should** be prescriptive, informative of the problem and indicate possible remedial actions (eg. “Code format not recognized, enter two letters and then three digits” rather than messages such as “Invalid Input”).

Event Log

Mandatory Requirements

No mandatory requirements are made in this section.

Recommendations

1. The event log **should** record all events on a plant wide basis.
2. The event log **should** record all operator messages.
3. Filtering/search facilities **should** be available.

Interaction Devices

Mandatory Requirements

1. All GUIs **shall** be designed to support the relative strengths and weaknesses of the interaction device. For example, if function keys are utilized, the GUI **shall** represent the physical layout of the keys. The GUI for trackballs can be more flexible since it is easy to navigate the cursor around the screen.
2. Pointing devices **shall** be of the trackball type. This is for both the local plant and in the CCR. Trackball devices require less desk space and are more robust than other pointing devices.
3. Interaction devices **shall** provide adequate feedback to the operator. A response ‘click’ or other tactile/audible feedback **shall** be provided.
4. Where personal protective equipment (gloves, body suits, respirators, etc), is required to be worn, control and display equipment **shall** be designed to overcome the disabling effects (eg. reduced vision, tactile feedback, hearing).
5. System response time **shall not** exceed 0.1 seconds, e.g. for keyboard depression, parameter entry.
6. System response time **shall not** exceed 2 seconds for indicating a response to a request.
7. Keyboards **shall** be movable/adjustable and not fixed down.
8. All keyboards **shall** be QWERTY keyboards. Alphanumeric keyboards **shall not** be used.

Recommendations

1. The force required to operate controls (eg. key depression, trackball button) **should** be high enough to avoid inadvertent/accidental activation, but low enough not to cause operational problems.

2. The inclusion of a ‘hold-to-run’ push button/facility **should** be considered – particularly for operations in manual mode. At the CCR consoles, a keyboard key to activate the hold-to-run function is recommended. At local plant workstations, a traditional push button is recommended rather than an on-screen device or a keyboard key due to the ease of use and increased level of tactile feedback. The precise function of the push button/key could be defined by the GUI. If the operation is lengthy (eg. in excess of 30 seconds), an alternative to a ‘hold-to-run’ strategy **should** be considered.
3. Keyboards **should** have a matt surface to avoid reflective glare.
4. All number pads **should** be laid out in a standardized manner. Number pads **should** be of the calculator type. The only exception to this is telephones, which utilize their own traditional layout. See Figure Three.

Figure Three: Recommended Layouts for Number Pads



5. The use of “function keys” **should** be avoided on control screens.
6. Permanently dedicated keyboard function keys **should** be utilized for frequently used, time consuming, repetitive and/or particularly important or critical control actions. They **should** also be used for ‘confirm functions’ in conjunction with permanent on-screen target areas (eg, Alarm Page, Home, Last Page, Menu, Alarm Accept).
7. The labeling of “function keys” on-screen **should** represent the layout of the physical keys on the control device, where appropriate.
8. Touch sensitive interaction devices **should not** be used. These devices (eg. touch-screens, membrane keypads) **should** only be utilized where the operator is required to input very short strings of data on an infrequent basis.
9. Touch screens or membrane keyboards **should** only be utilized on vertical panels.
10. For positioning purposes, a touch screen **should** be considered as a VDU display, rather than a control device.
11. Where interaction devices can not be located close to the VDU monitor, or the interaction devices are infrequently used, housing the interaction device in a pull-out tray **should** be considered. This is only applicable to local plant workstations.

System Access/Security

Mandatory Requirements

1. Restrictions **shall** be placed on system access. There **shall** be at least three levels of access. The system **shall** be flexible and have the capability to extend the number of levels.
2. The different levels of access **shall** allow different potential operations, e.g. for operators, team leaders or engineers. An example is shown in Table Two.

Table Two: Example Levels of Access to VDU-Based Systems

Level	Name	Operation/Description
0	View	View only. Access to displays, trends and reports.
1	Operator Level	As above, plus, initiating of sequences, control devices and acceptance of alarms. Request printed reports/screen printouts.
2	Team Leader Level	As above, plus changing of control values, adjustment of log frequencies, changing system time/date, enable/disable scanning of I/O points and authorizations (eg. for transfer operations).
3	Engineer Level	As above, plus configuration of displays, database and trends/reports, modification of application software, setting of alarm priorities/levels, access to system diagnostics, re-allocation of passwords, copy system media manual and modification of individual I/O values.

3. In the CCR, ‘logging-on’ **shall** result in the access to all the VDU workstations on that console ie. in effect, the operator logs on to the console and not individual workstations.
4. In local plant, ‘logging-on’ **shall** result in the operator accessing only that particular workstation.

Recommendations

1. Password, key or card swipes **should** be considered as a means of implementing restricted access.

7 Information Presentation

General

Mandatory Requirements

1. It is estimated that the hardware with the poorest performance will be equivalent to a 14” SVGA monitor (diagonal measurement). Therefore the VDU-based interfaces **shall** be designed using the example templates shown in Appendix 4. Larger VDUs will be utilized in the CCR, but these units will access the same software and utilize the same interface. If the interface/monitor is radically different, individual templates may be required for different types of units. The template/display **shall** include all major interface components (e.g. toolbars, banners, etc), and the mimic will be designed to fit the remaining available space.
2. A number of similar systems will be found in a number of different plant areas (eg. cranes, transporters, shield doors, transfer bogies, personnel access, etc). In order to ensure consistency, the operator interface design for the control and display of these pieces of equipment **shall** be standardized.
3. The most effective operator interface is often the simplest. The use of ‘state-of-the-art’ three dimensional graphics, animation, etc, **shall** only be considered when it provides the operator with additional information that will enable them to make more effective decisions. Three dimensional graphics, animations, etc, **shall not** be added to the user interface solely because these display options are available. Do not unnecessarily over complicate or clutter the display. The display will show the necessary information in a clear and structured manner to avoid risk of operator confusion/inaccuracy.
4. The operator **shall not** be presented with information that requires transposing, computing, interpolation or mental translation.
5. Where activities are viewed directly (via a cell face window) or indirectly (via CCTV) and controlled via a GUI, the information from all sources **shall** be consistent, representative and compatible. The display on the VDU-based system **shall** be consistent and representative with what the operator views via direct or indirect means.
6. The general layout of VDU-based interfaces **shall** be consistent with associated panel controls and displays utilized to control the equipment, where applicable.
7. Flash **shall** only be used to gain the operator’s attention to important information.
8. All flashing of screen components **shall** be synchronized.
9. Analogue and digital data updates **shall** become evident on a screen, including when the screen is in use, without having to page out of the screen and back in again.
10. Time information **shall** be presented in 24 hour clock format (hh:mm:ss) and not with a.m./p.m. indications.
11. The format for date information **shall** be standardized across all operator-interfaces. Use mm/dd/yy.
12. Items of equipment that are undergoing maintenance or are inhibited **shall** be flagged or coded in a clear and consistent manner. This can be a tag on the device faceplate entered and removed by the operator

13. The current mode of control **shall** be permanently displayed. This could be part of a toolbar.

Recommendations

1. VDU-based interfaces **should not** merely display an electronic representation of a conventional control and display equipment (that it replaces).
2. VDU-based interfaces offer the opportunity to integrate a larger amount of information onto a single display than conventional control and display equipment. The operators information requirements **should** be assessed to ensure that information is integrated in a manner that will facilitate task performance.
3. Inverse video **should** only be used to highlight a word or alphanumeric code.
4. Information that is not required for normal operator/maintainer activities (eg. specialist maintenance, technical support) **should** be located elsewhere. Do not integrate this information into the displays that the operator will utilize. For example, specialist maintenance pages, detailed diagnostic displays, etc.
5. Overview displays, showing key items of information and omitting detailed data, **should** be provided. This information may be appropriate for the team leaders and shift managers' VDU systems. No control actions will be available from these screens.
6. The need for an operator to continually switch between screens in order to perform a task **should** be avoided. If all the relevant task information can not be displayed on a single screen, the operator **should** be provided with an additional VDU.
7. All quantitative data that must be scanned and compared by human operators **should** be presented in either tabular or graphical format.
8. A 'Maintenance Summary Page' **should** be provided that lists the items currently in maintenance, the time they were placed in maintenance, and an area where the operator can enter descriptive text. A 'Maintenance History' function **should** also be provided.

Ergonomic Principles

Mandatory Requirements

1. The **significance** principle **shall** be applied. The more important an item is to the operator in enabling the system to operate safely, effectively or to protect the plant, the more the item should be placed centrally on the screen.
2. The **frequency** principle **shall** be applied. The more frequently an item is used, the more the item should be placed centrally on the screen.
3. The **grouping** principle **shall** be applied. Items, which are functionally related in terms of safety, operating or protecting the system, should be grouped together.
4. The **sequence of use** principle **shall** be applied. If certain items are generally used in a particular sequence or pattern, then these items should be laid out in this sequence.

5. No single principle can be applied across all situations to define the display layout. Where the principles are not compatible, either with each other or operator expectations, trade-offs will have to be made. The trade-offs and alternatives **shall** be fully considered before decisions are made. Generally, the principles are applied in the above order (ie. the significance principle is the most important, and the sequence-of use principle is the least), and the significance and frequency principle are used to define the general layout and the grouping and sequence-of-use principles are used to more specifically locate items.

Display Organization and Structure

Mandatory Requirements

1. The overall screen display system **shall** be hierarchical in nature to facilitate understanding of the process.
2. The hierarchy **shall** be logical to the operator. The structure of the display system **shall** be simple and unambiguous.
3. The hierarchy **shall** be broad rather than deep.
4. The hierarchy **shall not** exceed five levels in depth.
5. At each level of the hierarchy, a particular title format **shall** be used so that the operator knows where he/she resides in the hierarchy system. Additional coding, such as background color can also be used to assist in identifying where the operator is.
6. An overview display **shall** be the first screen the operator views after logging-on. It **shall** provide a rapid links to the system areas that the operator will need to access from that particular operating location.
7. Windows **shall** never overlay important information. This includes alarm messages/banners, display page title, important status information and operator messages.
8. In some systems, crucial components of the display (eg. the alarm banner) are separate windows. These areas **shall** be protected to prevent them from being covered.
NOTE: If it is not possible to prevent the Alarm Banner from being covered by a window, then the system **shall** be designed so that windows (eg. faceplates) appear in the center of the mimic part of the display (ie. not obscuring the Alarm Banner). The window will be moveable by the operator, and not fixed.
9. Where there are a large number of options, a hierarchical system of sub-menus **shall** be utilized. If hierarchical “pop-up/pull-down” menus are used, there **shall** be a maximum of three levels in the hierarchy.
10. Menu items that link to sub-menus **shall** be clearly distinguishable from those that initiate actions. For example, the menu option is followed by a symbol “➡” and as the cursor passes over the menu option the sub-menu appears next to the parent menu.

Recommendations

1. The fixing of pop-up window positions, and the removal of functions such as window re-sizing, **should** be applied in order to prevent important areas of the display being covered.

2. In order to prevent the cluttering of the display, the use of additional screens which contain detailed information **should** be considered as an alternative to “pop-up” windows (i.e. use a more detailed level in the hierarchy).
3. Menu options **should** be grouped in a logical (to the operators) order. This is typically by sequence and frequency of use.
4. The operator **should** only be able to open a maximum of three windows at any one time.
5. A title bar **should** be provided at the top of each pop-up menu. This **should** display the title and, where possible, provide a “Close” icon or similar facility.
6. Where long lists are shown in pop-up menus, a scroll bar **should** be provided.

Navigation

Mandatory Requirements

1. The navigation techniques **shall** be applied consistently throughout a system
2. The operator **shall** be provided with a simple means to follow process information from page to page. This **shall** be done by showing the target areas on the ends of all process lines or mechanical transfer equipment at the edge of mimic screens.
3. A box around a target item (or other appropriate size, symbol or color coding mechanism) **shall** depict the target areas on the screen.
4. The characteristics of the cursor **shall** change whenever it moves over an area that can be selected for example, the normal arrow symbol “↖” is replaced with a target “⊕” or a hand “☞”.
5. The operator **shall** be provided with a simple means to go back up a level of the hierarchy. This is typically achieved by the operator selecting a ‘move up the hierarchy’ icon from the tool bar.
6. A bookmark function **shall** be provided to allow rapid navigation as defined by the operator.
7. A last page facility **shall** be provided.

Recommendations

1. The operator **should** be provided with information that helps identification of the quickest route to access a desired display.
2. The associated displays available from the current display **should** be accessible by a number of different access methods. These methods **should** include built-in target areas in mimic symbols, arrows on the ends of process lines, inputting the number of the new display or selecting a hierarchical page link icon in the tool bar.
3. The operator **should** be given simple navigation tools. For example, use **↑ ↓ ← →** keys positioned consistently in the tool bar on each screen. These symbols **should** display to the operator what navigation choices are available (by being visible when a link is available and ‘greyed out’ when no link is available).
4. If a ‘tool tip’ function is available, there **should** be a means for the operator to activate and de-activate the function. In addition, there **should** be a short lag between the positioning of the cursor and the appearance of the tool tip.

Display Selection

Mandatory Requirements

No mandatory requirements are made under this heading.

Recommendations

1. Symbols/tags for similar parameters **should** be of the same type and format, and not vary from system to system or from plant to plant.
2. Display selection **should** be in accordance with Table Three.

Table Three: Recommendations for VDU Screen Design

Display Function	Appropriate Display Type	Description and Comments
Discrete status representation for binary changes	Symbol Symbol fill Text descriptor	Should physically represent the actual item. Show changes in status by location change, completeness of outline, color or size coding (ie. large vs. small). Use to show open/close or on/off. One word status description of item eg. open, closed.
Precise value presentation	Digital value	Place value in a box located adjacent to a set-point value.
Variable status information (qualitative)	Vertical bar graph Horizontal bar graph Continuous symbol fill Continuous color graduation Analogue indicator	Show increases and decreases. Including set-points and alarm conditions. Ideal for check readings. If appropriate, include range of limits, output requirement, alarm positions, etc Character should represent plant item. Appropriate for vessel levels or power output. Use for temperature representation. Color changes from blue (cold) to red (hot), or move through saturation (but not both). Good for showing rates of change or tracking. Use a set-point for particular parameters.

Display Function	Appropriate Display Type	Description and Comments
Variable status with precise value (qualitative and quantitative)	Digital scale with pointer Scaled bar graph Scaled analogue indicator	Include range limits, set-points and alarm positions. Level of accuracy is determined by scale. As for digital scale with pointer. Do not use if scale has to go further than one rotation of the face.
Status comparisons over time	'Deviation only' chart Dynamic graph Scaled trend	Use for sampled status to show parameter in relation to a set-point. Cuts down redundant clutter and 'drifting' easily spotted. Ideal for normally stable parameters. Good for showing current value in relation to set-points and limits, as well as historical information. Design the update mechanism to provide smooth changes rather than large step changes. Include a digital display for precise information. 'Time' should be displayed along the horizontal axis and the measured parameter on the vertical axis.
Plant/group overviews and comparisons (representational)	Graphical deviation display Deviation displays (vertical bars) Mimics	Allows easy recognition of problem parameters. All acceptable states should be in the same relative position. Short row of vertical bars allowing the comparison between control loops. Use for showing overall changes in plant/state/configuration, particularly if associated with sequence operations. Do not use as background for complex process dynamics.
Auditory signals	Eg. speech synthesis, tones, bleeps	Use for alarm information to gain the operators' attention. Use only if visual displays are overloaded or if the operator has more than one workstation/workplace. Do not use if background noise may interfere.

Animation

Mandatory Requirements

1. Animation **shall** only be used where it provides a significant benefit to the display in terms of improving the representation of equipment on the mimic or as an effective means to provide information to the operator. The requirements for animation require

identification and specification before the mimics are designed. Animation **shall not** be used solely because it is an available feature.

Recommendations

1. Large amounts of animation **should** be avoided. Use animation selectively so that its impact is maintained.
2. Area overview displays **should** only utilize a minimal amount of animation.
3. Substantial amounts of animation **should** only be used on the more detailed levels of the display hierarchy.
4. Complex animation, to show device/plant states **should** be avoided, as it is likely to cause operation confusion. Dynamic banners, which utilize simple text descriptions, **should** be utilized instead.
5. Animation of dynamic symbols **should** be representative of the real plant/equipment.

Mimic Displays

Mandatory Requirements

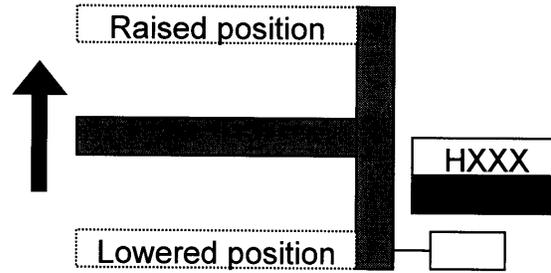
1. The number of parameters displayed on a single mimic **shall** be limited to ensure that the display is readable and is not cluttered. The appropriate number of parameters will depend on screen size and display characteristics.
2. Where the mimic represents equipment that can be seen (directly or via the CCTV system), the mimic **shall** be drawn so that it is compatible with the observed equipment. For example, equipment is in the appropriate position relative to other equipment, equipment travels in the same direction, information does not require mental rotation, etc.
3. The equipment and operations within the cells can be viewed either directly (via the windows) or indirectly (via the CCTV) from a number of orientations. The orientation of mimics **shall** consider the location of the operator in relation to the items of equipment on the plant. Where operation may be from a number of locations, different mimics **shall** be provided for each operating location at different orientations.
4. Mechanical equipment or items (eg. drums and boxes) that move between a number of set positions **shall** be shown at the position. An intermediate position **shall** be displayed between each of the set positions where possible. An arrow (colored cyan) will indicate the direction of movement. At no time will the item/equipment 'disappear' from the display. An item **shall** only be displayed at one position at a time.
5. Irrelevant digital detail **shall** be avoided.
6. Size, centrality and labeling **shall** be used to show the importance of items.
7. An agreed set of standardized process symbols **shall** be utilized in all interfaces. These symbols **shall** be meaningful to the operators who will operate the plant.
8. The symbols for mechanical equipment **shall** represent the physical shape of the item and retain the correct orientation. Ensure the items are immediately recognizable to the operator as specific plant items. Note that they do not have to be photo-realistic representations. If the representation is complex it can detract the operators' attention

- from the rest of the mimic, slow down the update rate and can occupy a large amount of space. A trade-off is required between realism and usability of symbols.
9. Where items are repeatedly displayed on several screens, they **shall** maintain their relative positions.
 10. Significant process states such as “Compacted”, “Encapsulated” or “Monitored” **shall** be displayed using dynamic text directly adjacent to the plant item to which the state refers.
 11. Measurements such as level, temperature, pressure, etc, **shall** be positioned and tagged to an item at the same position as which they occur in reality. For example, the reading is displayed where the actual reading is taken on a specific item of equipment).
 12. If different sizes of symbols are used for coding purposes, a maximum of three levels of size **shall** be utilized.

Recommendations

1. Mimics **should** be drawn in the most appropriate orientation for the particular information they display. As a rule, overview mimics **should** always be shown as plan views. As default, detailed mimics **should** also be shown in plan view. The exception to this is if the mimic depicts a significant amount of vertical movement, where the mimic **should** be drawn from an elevation view.
2. Where the equipment can not be viewed via direct or indirect means (eg. incineration, off-gas, ventilation, etc), a schematic approach to mimic design **should** be used. Mimics **should** be drawn to highlight the tasks required, processes involved and important relationships between different items of equipment. The spatial relationships between equipment items, whilst still maintained, can be simplified to avoid clutter, if appropriate.
3. In a trade-off between completeness of a screen and too high a density of information, the designer **should** err towards completeness of screen. The mimic **should** attempt to illustrate a complete picture (ie. an identifiable sub-group of items that have a related function).
4. As a general guideline, VDU-screens **should** be formatted so that preferably 50-70% of the available screen area is utilized. Never more than 80% of the available screen **should** be used.
5. Where useful, any major or significant items of plant and equipment that are not available for control by the computerized system **should** be included and displayed on the mimics to provide the operator with contextual information. (eg. some of the plant utility supplies). A graphical representation of all devices **should** be shown on the most detailed mimics.
6. The orientation of symbols **should** remain consistent across mimics.
7. Vertical height on the screen **should** represent vertical height in chemical processes, so that flows downwards may be gravity flows, whereas ones upwards are pumped/airlifted.
8. If a visible ‘touch frame’ is utilized (ie. a visible box that surrounds an object to signify a hot-spot), It **should** be an integral part of the design of each mimic object.
9. Reference points for moving items of equipment **should** be provided. For example, if a box moves up an elevator, the elevator denotes the box positions. See Figure Four.

Figure Four: Example of Simple Representation of Raising an Elevator



10. The drum and box symbols displayed on mimic diagrams **should** be provided with a simple coding system to give key information for that drum or box. A suggested coding mechanism is described in Tables Four and Five, and outlined as follows:-

- Symbol shape used to denote the type of box / drum (ie. 55 gal, puck drum, wooden box, metal box, overpacked, etc).
- Lid symbol to indicate whether the drum or box is lidded or not.
- Display the weight of the drum or box.
- Use labeling to denote the contents of the drum / box.
- Color coding should be kept to a minimum.
- Labels (ie. 3 and 4 above) should be contained within the drum / box symbol.

Table Four: Suggested Coding for Drums

Drum Type	Coding – Color, Letter, Shape, Size
Empty (55 gal or Puck Drum)	Black outline, grey infill., label “Empty”
Puck/Product Drum	Use different symbol size i.e. wider shorter drum
Debris (sort)	Label “Debris Sort”
Debris (sorted)	Label “Debris”
Direct Feed	Label “Direct”
Inorganic Homogeneous Solids	Label “IHS”
Organic Homogeneous Solids	Label “OHS”
Reject	Red, label “Reject”
Prohibited	Yellow, label “Prohibited”
Unknown	Yellow, label “Unknown”
Calibration Drum	Pink, label “Calibration”
Lid or unlidded drum	Lid symbol – present or absent
Overpacked drum	Dark brown drum
Special Case Waste	Yellow, label “SCW”

Table Five: Suggested Coding for Boxes

Box Type	Coding – Color, Letter, Shape, Size
FRP/Wooden Box	Mid brown box symbol
Metal Box	Black box
Overpacked Box	Dark brown box
Non-Standard Box	Grey box symbol
SWB or LLW export box (?)	Dark grey symbol
Metal Debris	Label “Metal Debris”
Inorganic Debris (eg. filters)	Label “Inorganic Debris”
Paper, Rags, Plastic, Rubber (PRPR)	Label “PRPR”
Calibration	Pink
Problem / Reject	Red
Unknown	Yellow, label “Unknown”

Process Lines

Mandatory Requirements

1. The crossing of process lines (- including mechanical transfer routes) **shall** be avoided. Where this is unavoidable, precedence **shall** be given to the vertical line (ie. the horizontal line will break either side of the cross over).
2. All process flows and mechanical transfer routes **shall** be labeled at entry/exit of the screen.
3. Arrows **shall** be used to indicate process flows and mechanical transfer route directions. Arrows **shall** be present as a line enters a symbol, or joins or leaves the screen. Sufficient arrows **shall** be provided to clearly depict the flow or direction.

Recommendations

1. Process flows **should** travel from left to right, or top to bottom, with the main process line in any particular screen mimic occupying the central part of the screen.
2. The main process line on a mimic display **should** have a width of between 1.0-1.5mm. All other process and utility lines **should** have a width of between 0.5-1.0mm.

3. The use of different types of process lines, to represent types of materials, **should** be avoided. If different types of process lines are used, a maximum of three different types **should** be used (eg. continuous lines, dots and dashes). Also see Section 9 Color.

On-Screen Control and Display Equipment

Mandatory Requirements

1. Control/display arrangements **shall** be applied consistently across different operator-interfaces and workstations such that to operate a system at one location requires similar actions to operate a similar system in another location.
2. A “pop-up” window displayed when clicking on a device status box **shall** provide detailed status information that summarizes the device state.
3. Mirror imaging of control/display layouts **shall** be avoided.
4. Functionally related items **shall** be grouped together in a consistent manner.
5. The control actions, and the corresponding display response, **shall** be consistent, predictable and compatible with the operators’ expectations.
6. Feedback **shall** be provided for all control actions. Where applicable, display the position of moving items of equipment.
7. Simulated controls and displays **shall** conform to the arrangements shown in Table Six.

Table Six: Mandatory Requirements for Position of Simulated Controls/Displays on VDU-Based Operator-Interfaces.

Top or left	Bottom or right
* Raise	Lower
Engage	Disengage/Release
Lock	Unlock
Advance/Extend	Retract
Open	Close
Slow	Fast
Anti-clockwise rotation	Clockwise rotation
Movement away from operator	Movement towards operator
Movement to the left	Movement to the right

Note: An exception is for on/start/increase and off/stop/decrease. If they are arranged horizontally, the off/stop/decrease **should** be on the left, and on/start increase **should** be on the right. If arrange vertically, on/start increase **should** be on the top.

8. On-screen toggle switches **shall not** be used.

9. The pointing ends of simulated knobs **shall** be clearly marked/visible (e.g. a white line on the pointing end of the knob or rotary selector switch, etc).
10. Simulated multiple selector controls **shall not** be capable of being put into unused positions.
11. VDU-based emergency stop controls **shall not** be used.
12. Simulated mechanical counters **shall not** be utilized. Digital counters **shall** be used instead.
13. Digital numeric values **shall** change sufficiently slow for the operator to read the display, ie. change slower than once every two seconds.
14. Pointers on simulated dials **shall not** obscure the scale numbers/marks.
15. The scaling of simulated displays **shall** follow the requirements and recommendations set out for physical items in 13490/01 'Ergonomic Requirements and Guidelines for the Design of Control Desks, Panels and Gloveboxes'.

Recommendations

1. On-screen control and display equipment **should** follow the requirements and recommendations set out for physical items in 13490/01 'Ergonomic Requirements and Guidelines for the design of Control Desks, Panels and Gloveboxes'.
2. A control action forward, to the right, or clockwise **should** result in an increasing value or starting up.
3. Where the option exists, multiple displays **should** be arranged to facilitate the detection of abnormal values.
4. The number of digits in a display **should** be kept to a minimum and all readings are displayed to a pre-specified and appropriate number of decimal places.
5. If size is used for discrimination between controls, then no more than three discriminable sizes **should** be used.
6. Pop-up windows showing detailed device status information **should** be connected to the device symbol by a 'dog-tag' line.
7. If the operator requires further detailed information on a device, a full screen **should** be available. This can be accessed via a "Diag" key within the pop-up box.

Trend and Charting Facilities

Mandatory Requirements

1. Trend displays **shall** be utilized to display plant status data in a graphical manner.
2. The system **shall** allow multiple trends to be displayed on a single display to facilitate easy comparison on the same scale. No more than four trends **shall** be displayed on a single graph.
3. It **shall** be possible to use the displayed information directly without the need for calculation or interpolation.
4. The trend name, description and engineering/measurement units **shall** be clearly shown for each trend line.

5. The scale marks **shall** allow the display to be read to the required level of accuracy ie. at appropriate intervals and suitable values are displayed.

Recommendations

1. Trend displays **should not** be overcrowded. Preferably no more than three different variables **should** be displayed on a single chart.
2. A trend history display **should** be provided.
3. Variables **should** be color-coded based on standardized colors. See Section 9 Color. The use of dotted or dashed lines **should** be avoided.
4. The current real time value for an analogue signal **should** be displayed to the right of the displayed chart.
5. Scales with normal and stable values within a limited part of the scale, **should** be given color coding to show the limits for normal and abnormal values. For example, abnormally high and low ends of the scale are color-coded red. Alternatively, set-points be **should** be shown as lines across graphs.
6. Linear scales **should** be used in preference to non-linear (eg. logarithmic) scales wherever possible (- unless there is a specific identified need otherwise).
7. Time **should** always be displayed on the horizontal axis.
8. The time scales of trend information **should** allow expansion and compression as defined by the operator. Time span, start and end time **should** all be easily configurable by the operator.
9. It **should** be possible to review a trend over a long period of time, eg. several days.
10. Mini trend displays **should** be produced for integration into mimic displays or as “pop-up” windows on larger trend displays. These **should** be designed carefully to ensure the necessary information can be ascertained from the small display area.
11. Scale markings **should** be separated by 2mm (min) and represent the smallest numerical value to which the scale is to be read.

Operator Messages

Mandatory Requirements

1. Operator messages **shall** be provided on each display screen to inform the operator of any specific conditions or specific points being reached in the process.
2. The latest message **shall** be presented in a banner that is displayed on all mimics.
3. Operator messages **shall** be date and time stamped. Use the format mm/dd/yy - hh/mm/ss).
4. Operator messages **shall** be clearly distinguishable from alarm messages. They **shall** be colored white.
5. Operator messages **shall** only be received by those local workstations or CCR consoles that currently have access to the particular system.

Recommendations

1. The operator message **should** directly correspond with the sequence of events and **should** be informative to the operator.

2. A message summary display **should** be provided. This **should** list all the current messages associated with any particular workstation, system or area in chronological order, with the most recent at the top of the list.
3. Operator messages **should not** require acknowledgement.
4. Messages **should** be self-canceling ie. they will always be replaced by more recently received messages. If the message requires the operator to confirm the status of an item of equipment or intervene in an operation, the messages will be stacked until the operator has carried out the action, and then the message is automatically deleted.
5. Messages **should** use active affirmative sentences. Negative sentences **should** only be used for warnings/prohibitions.
6. Individual sentences **should** refer to a sequential step and remain as simple in structure as possible. Messages **should** maintain a standard grammatical structure and use short, meaningful, common words (eg. 'enter code' rather than 'the code should now be entered').
7. Text messages **should** be brief, concise and unambiguous, e.g. "Product Drum T6502 overfill" rather than 'contents of T6502 exceed operational requirements'.
8. Operator messages **should** be presented in a similar format to alarm messages. See Section 8.2 for details.
9. Operator messages **should not** be 'stacked'. For example:-

Avoid: Box Import Sequence 1235:
 Running

Use: Box Import Sequence 1235: Running

10. Unacknowledged operator messages **should** flash. Use a flash rate of 2-3Hz, synchronized with other flashing displays. Once acknowledged, the message **should** revert to a steady state.
11. Specific messages which require the operator to perform an action, effect a decision or to input data to enable the process to continue, **should** be accompanied by an auditory tone whilst they are unacknowledged. The tone **should** reset following acknowledgement, and **should** be easily distinguishable from the auditory alarm signal.

Tables and Lists

Mandatory Requirements

1. Column labels **shall** remain visible throughout any scrolling action.
2. Where a table or list extends over a number of pages, scrolling throughout the entire table/list **shall** be allowed. This is via a scroll bar with up and down functions. Rows and pages **shall** be numbered (eg. in the format of 'page of pages') so that the operator knows where they are in the list at all times.

Recommendations

1. In dense tables, a blank row or line **should** be used to aid horizontal scanning. These **should** be at approximately 5 row intervals.
2. There **should** be at least 3 spaces between groups of data fields.
3. There **should** be at least five spaces between each column.
4. Labels such as “continued” (to signify the list is continued on another screen) “page of pages” and “end of list” **should** be included in standardized positions.

Titles, Labels and Tags**Mandatory Requirements**

1. Consistent abbreviations **shall** be used, with no punctuation. An approved list of abbreviations **shall** be developed and used across the plant. This **shall** also be consistently applied to other control/display equipment, plant signs and documentation.
2. An agreed list of concise, descriptive and standardized text descriptions **shall** be utilized in all interfaces.
3. Each screen **shall** have a unique and distinctive title.
4. Display pages **shall** be consistent such that menus and titles are in the same place on each page.
5. Functionally related items **shall** be grouped together with labeling at the top of the demarcated area, with the label breaking the demarcation line.
6. All displays, devices, symbols and controls **shall** be labeled.
7. All devices, etc, displayed on the most detailed level of the mimic hierarchy, **shall** be accompanied by a current status indication in text.
8. All labels **shall** describe the item/condition/action completely, correctly, and unambiguously.
9. Superfluous and unnecessarily long labels **shall** be avoided.
10. All labels **shall** be simple, easy to read and conform to the operators’ expectations. Labels that require interpretation **shall** be avoided (e.g. Conveyor 12 position 1 is referred to as “Conveyor 12 Position 1” and not “C1201”).
11. Each label **shall** be closer to the item it identifies than any other, so that there can be no possible confusion as to which item the label refers.
12. All characters **shall** be vertical/upright.
13. Italics **shall not** be used.
14. Ambiguities and similarities between adjacent labels **shall** be avoided. Information or characters that distinguishes between similar labels **shall** be highlighted, e.g. by underlining, bolder characters, etc.
15. Annunciator nomenclature, symbols and abbreviations **shall** be compatible with other controls and displays.

Recommendations

1. The title of the screen **should** be informative and, where possible, provide reference to the location of the mimic in the hierarchy, e.g. “Incinerator In-Feed: Level 3”.
2. Each mimic **should** be numbered uniquely. The numbering **should** be hierarchical to allow operators to understand the position of any particular screen within the hierarchy. Eg. 1. for the overview; 1.1 and 1.2 for the next level; 1.1.1, 1.1.2, and so on.
3. Labels **should** be consistently placed above the items that they refer to. If the label can not be placed above the item, it **should** be located directly to the left.
4. Dog-leg tag lines to link labels to items **should** be utilized to connect instrument readings to the actual place the reading was taken. Tag lines are not required for linking devices and device status boxes.
5. If more than five alphanumeric characters are used in a code or label, they **should** be split into groups of 3-4 to reduce errors caused by short term memory demands. Each block **should** be separated by one blank character space.

Display of Sequence Information

Mandatory Requirements

1. The detailed sequence displays **shall** show the current status of the sequence. Provide a text description to indicate that the sequence is ready, running, idle, completed or failed, etc. This should be supplemented by color coding. Color should only be applied to those states that require operator intervention. (See Section 9, Color).
2. The detailed sequence display **shall** show the pre-checks and run-checks, plus the current status. This should be supplemented by color coding. (See Section 9, Color).
3. Closing the detailed sequence display **shall** return the operator to the detailed scheduler display.
4. Closing the scheduler display **shall** return the operator to the previously displayed mimic.

Recommendations

1. An icon **should** be provided in the toolbar, that when accessed, displays a list of all the available schedulers. ‘Clicking on’ a scheduler **should** produce a pop-up window that details all the individual sequences that comprise that scheduler.
2. The sequences **should** be displayed in hierarchical order, with parent/child relationships being shown by indentation and/or line spacing.
3. If control buttons on sequence display windows (ie. “start”, “stop”, “abort”) refer to a scheduler that automatically selects the appropriate sequences, the buttons **should** be displayed above the sequence information.
4. On the sequence menu, associated sequences that are not available **should** be listed, but ‘greyed out’.

8 Alarms

General

Mandatory Requirements

1. Alarm signals **shall** only be used to inform the operator of a significant plant state that requires the operators' attention. Other plant information **shall** be transferred via other means. eg. mimic displays, symbol changes, operator messages, etc.
2. The design of all alarm displays **shall** be considered together (e.g. alarms on VDU's, hardwired panels, printers etc) to ensure consistency across the plant.
3. Alarm priority levels **shall** be assigned according to the severity of failing to respond to an alarm and the time available for the operator to carry out compensatory action. High priority alarms **shall** be dedicated to potentially safety-related fault conditions. Alarms **shall** be displayed in a number of levels, as follows:

Level 1	High Priority
Level 2	Medium Priority
Level 3	Standard Priority

- Effective alarm prioritization is essential for good alarm handling. Assign high priority alarms with care in order to avoid multiple high priority alarm situations.
4. High priority alarms **shall** be duplicated on appropriate hardwired alarm panels at both central and local operating positions. The duplication may be soft or independently hardwired, as appropriate.
 5. It **shall** only be possible to acknowledge an alarm from a page giving appropriate details of the alarm state. This **shall** be either the relevant detailed mimic display or the Alarm List display. It **shall not** be possible to acknowledge the alarm from the alarm banner.
 6. When specific plant areas or systems are shut down and potentially numerous spurious alarms may be generated or standing alarms present. A facility **shall** be provided to prevent the display of the associated standing alarms or to display that the alarms are a result of the area being shutdown.
 7. Logging facilities, both to printers and hard disk, **shall** be provided for purposes of historically recording and interrogation. Automatic logging **shall** be configurable, and turned on/off by persons with the appropriate access.
 8. It **shall** be possible to call up an alarm listing giving all alarm information, in chronological order with the most recent at the top of the list. In a multi-screen system (as provided on the CCR consoles), it **shall** be possible to dedicate one screen to the display of alarms.
 9. It **shall** only be possible to acknowledge an alarm from the console or workstation that currently has control of the system. Alarms will only need to be accepted once. It will not require further acceptance on other consoles or workstations where it is displayed.

Recommendations

1. Alarms **should** be prioritized so that there are fewer alarms within each of the higher priority groups.
2. Oscillating process variables **should not** generate repeated alarms.
3. Where there are a large number of possible alarm signals, alarms **should** be grouped. The grouping of alarms **should** be meaningful to the operator eg. grouped by geographical areas within the plant, related systems, etc. A facility to show all alarms **should** be maintained (eg. for use in the CCR and BMR).

Alarm Presentation**Mandatory Requirements**

1. The alarm message **shall** clearly indicate the time, location, priority and type of alarm.
2. Alarm priority **shall** be represented by the color of the priority level. See Section 9 Color, for details.
3. Every screen **shall** display the presence of an unacknowledged alarm state.
4. Unacknowledged alarms **shall** flash at a frequency of 2 - 3 Hz.
5. All alarms and messages **shall** flash in synchronism.
6. An alarm message **shall** only become steady once it has been acknowledged.
7. If an alarm state clears, but the alarm has not been acknowledged, the alarm **shall** continue to flash until it has been acknowledged.
8. Once an alarm state has been acknowledged and cleared, the alarm **shall** automatically reset and clear from all displays except the most detailed alarm list.
9. It **shall not** be possible to clear an alarm message if the fault still exists.
10. Alarm messages **shall** be displayed at all appropriate interfaces (both local, cell face, CCR and BMR).
11. It **shall** only be possible to accept an alarm from the interface or console that currently has control.
12. Where an abnormal value is displayed, it **shall** be accompanied by a description of the abnormal condition, e.g. 95% HH, 90% H, 10% L, 5% LL, etc.
13. Alarms within the list **shall** be listed in chronological order with the most recent at the top (and then priority order, with the highest first, if more than one alarm occurs at the same time).
14. Alarm messages **shall** be date and time stamped (format mm/dd/yy - hh/mm/ss).
15. Alarm messages **shall** display information about the type, location and priority of the alarm condition. If space is limited, the message **shall** only present information that is relevant to the operator and provide it in a concise manner that will be easily understood by the operator.

Recommendations

1. Alarm presentation **should not** include the unique alarm reference number. This takes up space and does not provide the operator with valuable information.

2. Alarm presentation in the Alarm Banner, Summary and History Lists **should not** display the current analogue value within the message. The operator will obtain this information from the detailed status displays and mimic displays.
3. Alarm messages **should** be unambiguous, explicit and contain all the necessary information. The message **should** either contain information as to how the problem can be resolved or identify where further information is available. Sequence related alarms **should** state which scheduler or sequence they are related to.

Examples:

Sequence related alarms:-

410_xxx Step description – Compactor lowered – Precheck failure

370_xxx Step description – Drum transfer from position AA to BB – Runcheck failure

410_xxx Step description – Puck Handler to park position – Group failure

Other alarm messages:-

FxxxB Device name – Supercompactor Area Sump – Level high

Hxxx Device name – MSM not at park position – Interlock failure

From/to system 440 – Communications fault

FxxxA Device name – Incineration feed system – Trip initiated

Auditory Alarm Signals

Mandatory Requirements

1. Auditory signals **shall** only be used when action is required of the operator, or to attract the operator to a significant change of state needing urgent attention.
2. Unacknowledged alarms **shall** be accompanied by an audible tone. This signal **shall** be modulating or intermittent, and not a continuous tone. The signal **shall** be discriminable from other audible (non-alarm) signals. This tone **shall** be between 500 and 4500 Hz.
3. Auditory tones **shall** be activated at both central and local operating positions, as appropriate.
4. The auditory tone **shall** be produced via an internal sound-card or external device (eg. bells, klaxons, etc).
5. The alarm sounder **shall not** be placed behind the facia or other objects as this may baffle, distort or cause reverberation of the signal.
6. Each console in the CCR, cell face VDU workstation or other local operating panel **shall** have its own sound source so each operator knows when his/her area/console/workstation is in alarm.
7. The auditory signal **shall** be distinct from other background sounds in the operating environment (eg. data input error signal from the ICS/DMS system, ‘paper out’ warnings on printers, etc).
8. Once the alarm has been acknowledged, the auditory tone **shall** reset - assuming there are no other unacknowledged alarms active at the time.

9. There **shall** be an audible alarm signal test facility. This **shall be** easily accessible by the operator.

Recommendation

1. Where there are a relatively large number of consoles or workstations in the same area/room, two or three discriminable auditory signals **should** be used. Alternate the different signals between cell workstations or CCR consoles. No more than six different clearly discriminable alarm signals **should** be used. Three to four are recommended.
2. No more than six different clearly discriminable alarm signals **should** be used. Three to four are recommended.
3. Audible alarm signals **should** be approximately 10 dB above normal ambient noise conditions for that particular area. It is especially important to consider this when designing portable control units as ambient noise levels may be significantly different in the various operating locations.
4. Audible alarm signals **should not** exceed 15 dBA above the normal ambient noise level to avoid startling personnel and affecting speech communication.

Alarm Banner

Mandatory Requirements

1. An alarm banner **shall** be included in the same position on every screen.
2. The banner **shall** display the three latest unacknowledged, highest priority, alarms and/or messages for the entire plant area(s) controlled and/or monitored from that particular CCR console, cell-face workstation or other local plant workstation. (Note that if the banner occupies too much of the available screen area, the number of alarms can be reduced to two).
3. Once an alarm has been acknowledged, it **shall** stop flashing, and remain steady. The acknowledged alarm **shall** only remain on the banner when there are no newer, higher priority or unacknowledged alarm detected by the system.
4. Once an alarm state has been cleared, the alarm **shall** be automatically removed from the banner.
5. Operators **shall not** be able to acknowledge an alarm from the alarm banner.
6. The alarm banner **shall** display information in the format shown in Figure Six. Each message will be color coded to denote the alarm priority.

Figure Five: Sample Format for Alarm Banner and Alarm Lists.

DATE	TIME	ALARM	MESSAGE
Mm/dd/yy	hh:mm:ss	Sequence	Cause and type of problem
Mm/dd/yy	hh:mm:ss	Device	
Mm/dd/yy	hh:mm:ss		

Recommendations

1. In order to maximize the amount of information per line, the alarm banner **should** occupy the entire width of the screen. Keep borders to a minimum.

Mimic Displays

Mandatory Requirements

1. Alarm information **shall** be embedded in the mimic screens.
2. The operator **shall** be provided with a simple way of immediately getting to the correct area in the VDU mimic hierarchy for dealing with an alarm (eg. one or two keystrokes, “Fetch Alarm” target area or dedicated function key).
This can be relatively easy or difficult to achieve depending on the design of mimic displays. Where devices (ie. individual pumps, conveyors, valves, motors, etc) have only been included on one detailed mimic, any alarms relating directly to a device can be directly associated with the most detailed mimic that shows that particular device. However, with VDU operator-interface system designed in this way it is not so easy to determine which is the ‘correct’ display with sequence related alarms (ie. there is potentially more than one ‘correct’ display).
Furthermore, if the operator-interface design applies the design approach of using the most detailed mimics to illustrate particular sequences, this results in individual devices being repeated across a number of detailed mimics. While this means that sequence related alarms are more easily dealt with, the association of device related alarms to a particular detailed mimic is not so easy to specify.
3. The acknowledgement of an alarm on any of the mimic display **shall** acknowledge the alarm on all other relevant pages.
4. The re-setting and/or clearing of the alarm **shall** cause the dynamic alarm symbol to go to the non-fault state. The appropriate dynamic text **shall** continue to flash unless the alarm has been acknowledged.
5. The operator **shall** be able to acknowledge all the alarms associated with the equipment displayed on the particular detailed mimic via a simple method (e.g. a icon on the toolbar, a dedicated function key on the keyboard, etc.).

Recommendations

1. For moving mechanical equipment that go into a fault condition, the equipment symbol **should** be shown at its last known state/position (and not in a transitory position).

Alarm Summary Lists

Mandatory Requirements

1. On large systems, it **shall** be possible to show alarm information by functional groups of alarms, and/or plant area.

2. An alarm summary list **shall** be available which contains detailed information concerning current and previous alarm conditions.
3. The alarm list **shall** display information in the format shown in Figure Five. Include an additional column entitled “Priority” (as alarms will be colored green once they have returned to normal).

Recommendations

1. It **should** be possible for the operator to view alarm lists relating to each individual group of alarms. For example, where a group alarm has been triggered, the operator will be able to request a list of all the alarms in that particular area/system).
2. The ability to acknowledge all the alarms within a particular group, from the appropriate group alarm on the summary list display, **should** be considered.

Alarm History List

Mandatory Requirements

1. The list **shall** be capable of displaying the maximum number of alarms eg. in excess of 200 (maximum of 700).
2. The alarm history list **shall** display all the individual alarms that have been received across the whole plant.
3. Alarms **shall** remain in the history list, even if the condition has been cleared and the alarm has been acknowledged.
4. The history list **shall** catalogue alarms over a suitable period of time eg. seven days.
5. The alarm history list **shall** display information in the format shown in Figure Five. Include an additional column entitled “Priority” (as alarms will be colored green once they have returned to normal).

Recommendations

1. ‘Find’, ‘sort’, ‘go to’, and ‘bookmark’ functions **should** be available for analysis and trending, eg. priority, time window, system, etc.
2. The provision of additional useful information (as compared to Figure Five) **should** be considered in the alarm history list. The provision of information concerning the time of acknowledgement, remedial action, time alarm condition cleared, operator comments, etc, **should** be considered with regard to operator information requirements.

9 Color

General

Mandatory Requirements

1. All GUIs **shall** be displayed on color VDUs. Mono-chrome VDUs **shall** only be utilized for simple alpha-numeric displays.
2. Each potential color **shall** be checked for consistency on each type of interface (i.e. CRT, TFT, LCD, etc.) under the various potential operating conditions prior to operation to check for clarity and color consistency.

Recommendations

No recommendations are made in this section.

Color Coding

Mandatory Requirements

1. Color coding of all VDU-based interfaces **shall** be as shown in Table Seven. This will ensure that meanings associated with color match operator's expectations, eg. red for danger, yellow for caution.
2. The meaning of colors **shall** be unambiguous, not contradictory, and consistently applied across all interfaces.
3. Color coding **shall not** be utilized as the sole method of coding or sole means of identification. Color plus another form of coding **shall** be used.
4. When assigning colors to process lines, if more than one type of process material exists in a category, an additional form of coding **shall** be adopted (e.g. dashed process lines).

Recommendations

1. The use of orange and amber **should** generally be avoided since they can easily be visually confused with red or yellow. Orange may be used sparingly for static equipment symbols on mimics for mechanical areas.
2. Color **should** be used to improve the clarity of display information. For example, color may be used as an identification code, to highlight key items of information, to group items by background color or as a means of reducing clutter from background graphics. If color is utilized in this way, a clear philosophy **should** be developed that will ensure that color is applied consistently and effectively.
3. Color characters **should** not be used to display quantitative values.

(NO PAGE 44)



Table Seven: Mandatory Requirements for VDU Operator-Interface Color Coding System.

Color	Generic Meaning	Process Material Identification	Current Status of Equipment or Item	Alarm Information Abnormality
White	Information only Safe status	Utilities and process water Device steady states Inactive condensate Fire water Domestic water Chilled water	Locking bolt engaged Machine parked Equipment available Shield door closed Authorization to proceed Equipment in Automatic mode Use white on a black background for dynamic text to indicate that the system or sequence is in a normal/safe state	-
Yellow	Warning/caution	Gaseous reagent feed (excluding process and instrument air) High and Low pressure steam Off-gas	Cautionary or potentially unsafe state that the operator or system has intentionally put the equipment into At or approaching operating limits for function such as travel, hoist movement or potential collision zones Shield door open Sequence running Do not use for static equipment symbols for mechanical plant	2 nd priority level alarm Alarm condition (HH and LL) Abnormal states/items Use yellow on a black background for dynamic text to indicate that the system or sequence is in a fault state Instrument failure Failed Timeout Overrun, overspeed, overtravel, overload Torque limit exceeded

Color		Generic Meaning	Process Material Identification	Current Status of Equipment or Item	Alarm Information Abnormality
Magenta (purple)	-		Aqueous reagent feeds:- Alkaline (dark) Acidic (light)	Calibration drum or box Equipment in Manual mode	Monitor inhibited Bad or questionable values or measurements Under maintenance or calibration Abnormal state/items Radiation alarms
Orange	-		Solvent Water glycol	-	-
Cyan (light blue)	Moving		-	Symbol used for equipment that physically moves Only use on the actual part of the machinery that is moving. Eg. section of conveyor currently moving.	Alarm condition (H and L) Acceptable alarm condition Low priority alarm 3 rd level priority alarm Abnormality notification
Red	Emergency Danger Used sparingly to maintain 'attention grabbing' properties		-	In chemical processes <u>only</u> , use equipment symbol shape and outline with a red infill for the following <u>equipment states</u> :- <ul style="list-style-type: none"> • Stopped • Closed • Off Do not use for static equipment symbols for mechanical plant I/O value falling Pre/run check failure/false message	Emergency / safety-related high priority alarm 1 st level priority alarm Major control system fault Interlock or trip failure/activated Emergency stop activated Power supply fault Reject



Color	Generic Meaning	Process Material Identification	Current Status of Equipment or Item	Alarm Information Abnormality
Green	Safe	Aqueous Effluent Active steam Active drains Clean (light) Dirty (dark)	In chemical processes <u>only</u> , use equipment symbol shape and outline with green infill for the following <u>equipment states</u> :- <ul style="list-style-type: none"> • Running • Open • On Do not use for static equipment symbols for mechanical plant Normal operation / healthy System healthy Pre/run check 'true' I/O value rising/on	An unacknowledged alarm state that has returned to normal (flashing only)
Blue	Live Information only Non-essential information, eg:- <ul style="list-style-type: none"> • Tags • Labels • Functional grouping (use sparingly) 	Ventilation and air supplies. Use a darker blue for contaminated or lower quality ventilation or air supply. Use light blue for breathing, process and instrument air.	Power on/energized Control available Standby equipment	-



Color	Generic Meaning	Process Material Identification	Current Status of Equipment or Item	Alarm Information Abnormality
Grey (slate)	Target, eg:- <ul style="list-style-type: none"> • Page links • Control points eg. start/hold/stop operation 	-	-	-
Black Grey	Backgrounds <ul style="list-style-type: none"> • Black – dynamic text • Grey – mimic background 	-	-	-

NOTE FOR INFORMATION: The AMWTP system is largely a mechanical process plant, therefore, the column entitled “Current Status of Equipment” will be the prevailing coding system. Ventilation and Utilities will follow the process material identification coding specification

Combinations

Mandatory Requirements

No mandatory requirements are made in this section

Recommendations

1. Color combinations **should** provide good contrast. The foreground information **should** be distinct against the chosen background color. Additionally, the background color **should not** interfere with the color coding.
2. A single, non-distracting, color **should** be used for all display backgrounds. Black is the preferred color, but light grey is a good alternative. Check that a high contrast is maintained between foreground colors and the background, particularly for colors such as white, yellow and cyan. If necessary, techniques such as black outlines **should** be considered.
3. Avoid using red and blue for fine detail. Green or white **should** be used.
4. Color combinations **should** be as shown in Table Six.

Table Eight: Recommendations for Color Combinations

Background	Foreground	Avoid Using
White	Black	Red/Orange
Dark Blue	Yellow or White	Blue/Green
Green	White	Red/Blue
Light Grey	Black	Red/Black
Dark gray	White	Green/Yellow
Red	White	Blue/Orange
Yellow	Black	Green/Red
	Dark Blue	Red/Green
		Orange/Black
		Orange/White
		Yellow/White
		Red/Magenta
		White/Magenta

10 Text Attributes

Font/Case

Mandatory Requirements

1. A standard font **shall** be utilized across all VDU-based operator-interfaces.
2. Bold text **shall** only be used where necessary and in a selective manner. If bold text is utilized, use a larger font.
3. Character fonts **shall** be such that it is easy to discriminate between similar alphanumeric characters (eg. I and L, B and 8, Z and 2, etc.). Fonts such as arial, helvetica and sans serif are probably the most acceptable.

Recommendations

1. Titles and mixed alphanumerics **should** be in UPPER CASE.
2. Mixed text **should** be used for all other text since it reduces the risk of operators making reading errors, i.e. “Plant Item” rather than “PLANT ITEM” or “plant item”. Mixed text **should** be used for all lengthy pieces of text information (eg. alarm and operator messages, sequence descriptions, etc). UPPER CASE text **should** be restricted to short items of text (eg. mimic and window titles, device status, etc)

Size

Mandatory Requirements

1. Text **shall** have a minimum font size of 9 pt for SVGA displays (a character height of approximately 2mm) when displayed at 100% zoom.
2. The adequacy of the font size **shall** be verified as soon as appropriate hardware is available. Check legibility in the typical operating conditions (ie. the lighting system) and the likely positions of the operator in relation to the monitor/screen. Use a number of people in order to account for differences in eyesight.
3. Character width to height ratio **shall** be between 0.7:1 to 1:1.
4. The numerical width to height ratio **shall** be 3:5.

Recommendations

1. Text **should** be of a minimum font size for high resolution displays of 3.5 mm. Note that a font size of 12 pt is usually recommended, but since different size screens will be used, the actual displayed height is stated.
2. A smaller font **should** only be utilized where a larger font adversely affects the completeness of text descriptions.
3. The character stroke width to height ratio **should** be in the range of 1:6 to 1:10.

Spacing**Mandatory Requirements**

No mandatory requirements are made under this section.

Recommendations

1. No more than 40-60 characters **should** be presented on one continuous line of text. A double column of 30-35 characters is acceptable.
2. Columns **should** be separated by five blank character spaces.
3. There **should** be one stroke width between characters.
4. There **should** be one character width between words.
5. Spacing between lines **should** be 50 - 150% of the character height.
6. Where indents are used, a minimum distance **should** be 3 character spaces from the start of the heading.
7. If in excess of five characters are used to make up an alphanumeric code, the code **should** be divided into groups of 3-4 characters. Each block be **should** separated by one blank character space

END OF APPENDIX 2



Appendix 3 –AMWTP Control System Architecture (Indicative).

See drawing ref: 54-5624

AMWTP Proposed Control System Architecture

Appendix 4 – SCREEN LAYOUT EXAMPLES

Note that the following examples are for illustrative purposes only and are derived from project(s) other than AMWTP.
As such, nomenclature and references should be ignored.

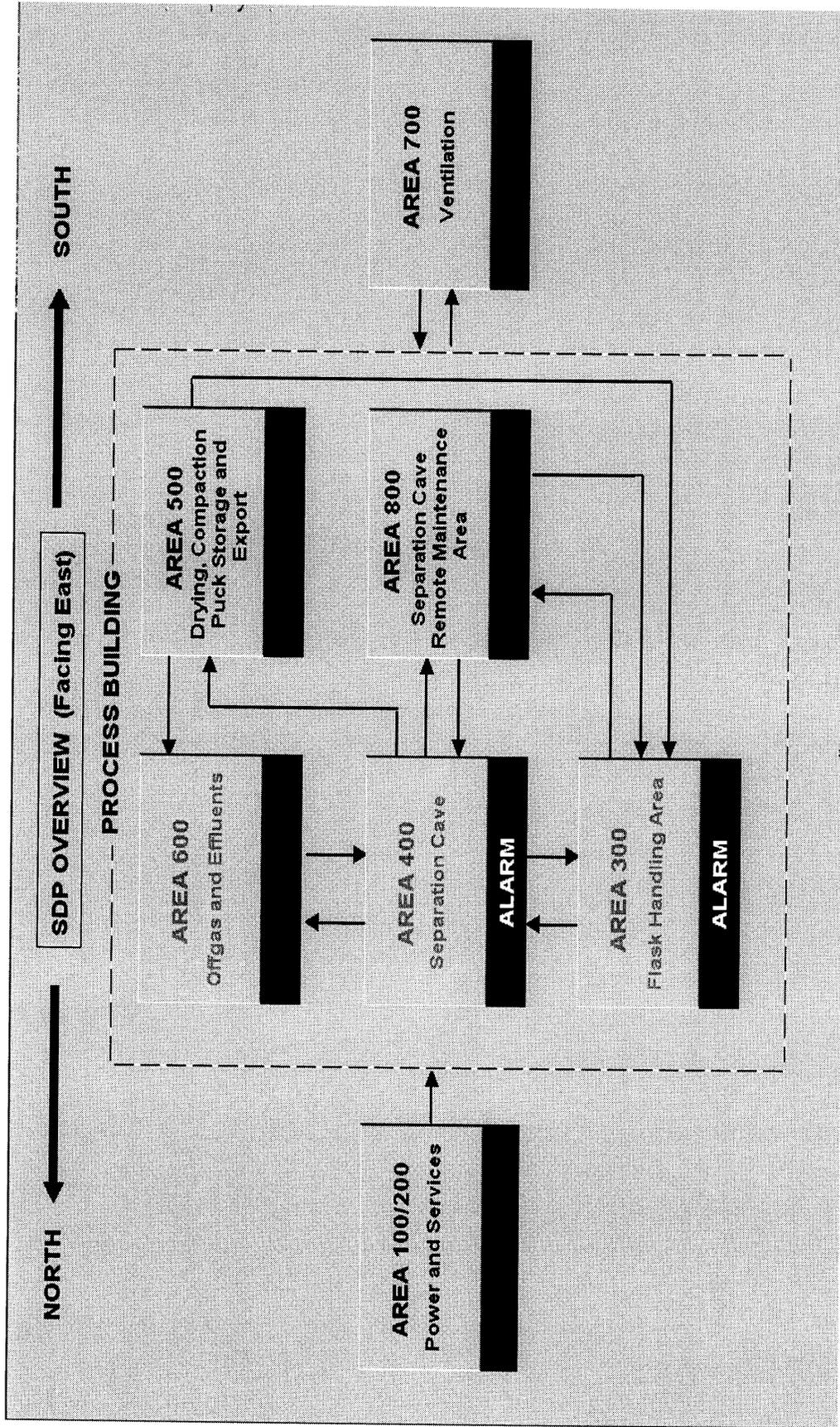


Fig 1 – Level 0 – Plant Overview display

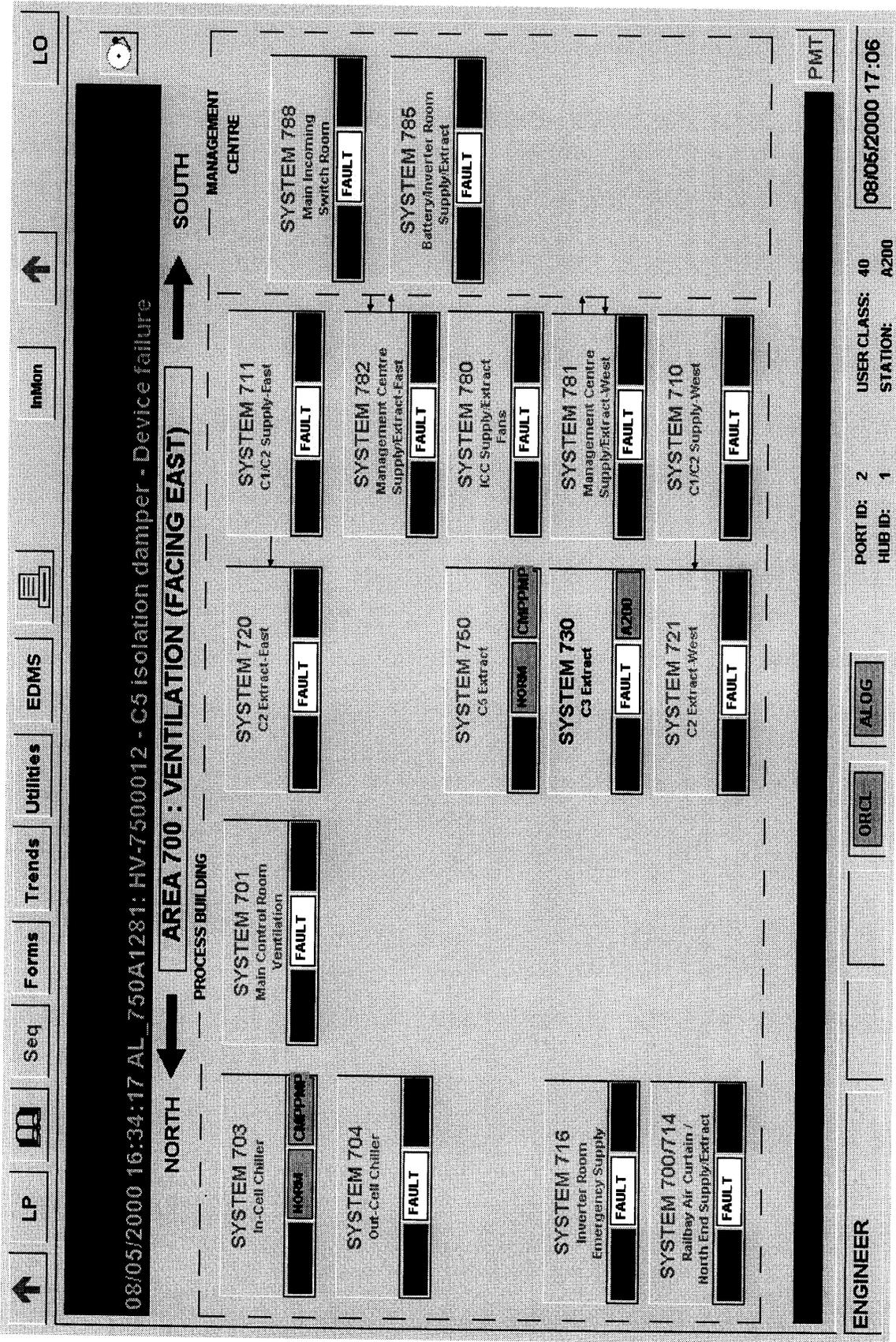


Fig. 1A Typical Level 1 Mimic - Area Overview display

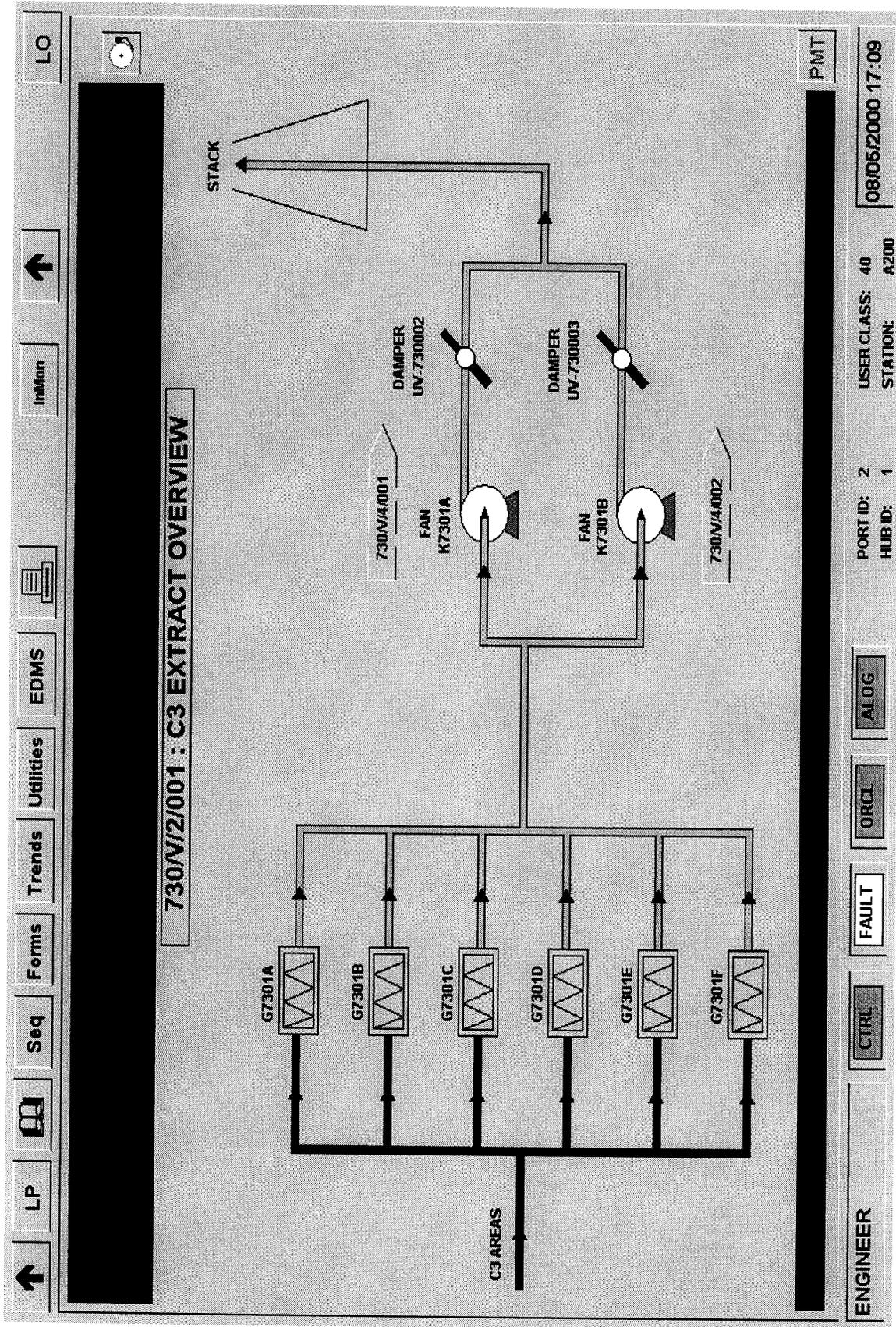


Fig. 1B Typical Level 2 Mimic-System Overview display

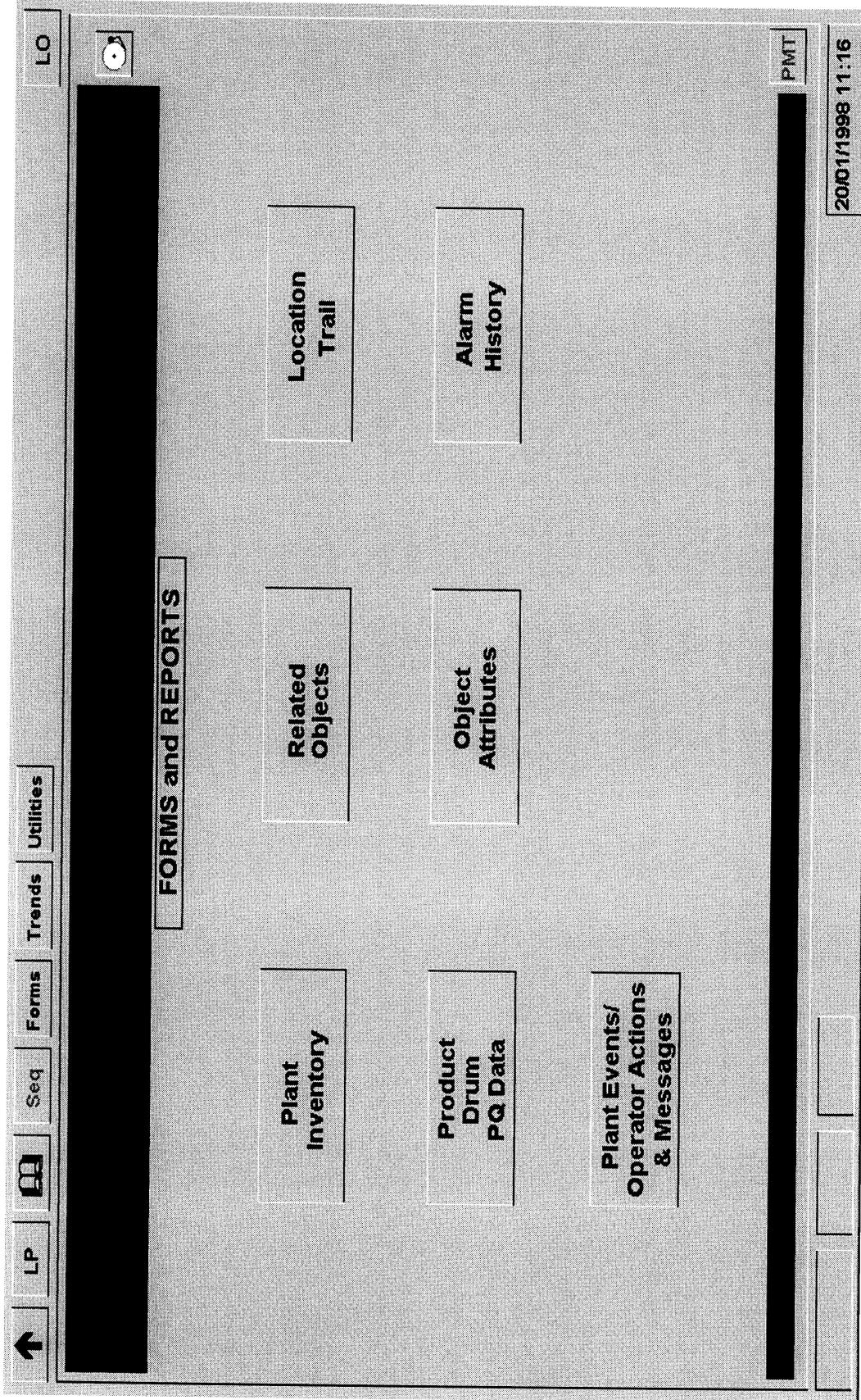


Fig 2 – Forms and Reports Screen

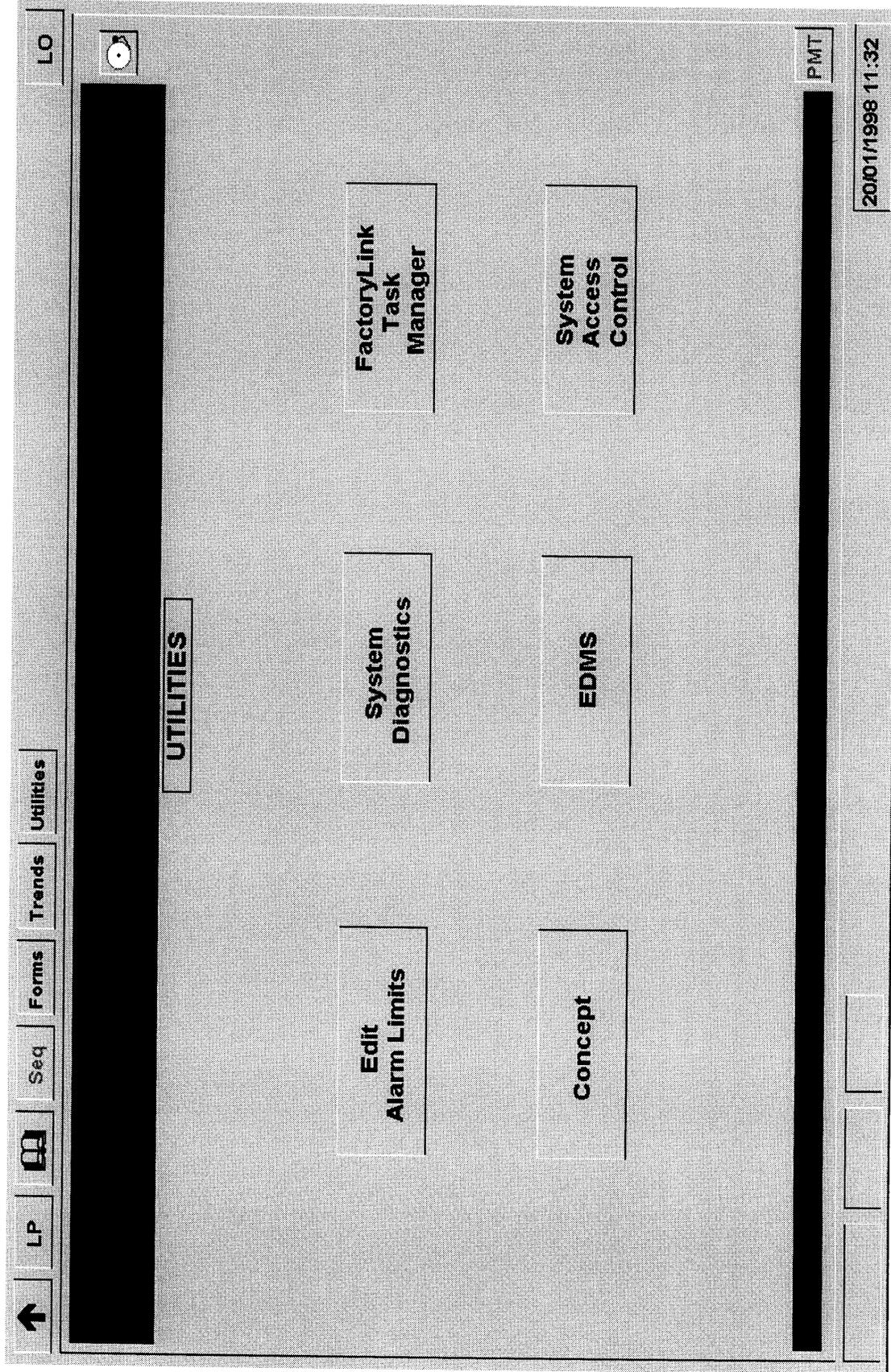


Fig 3 – Utilities Screen

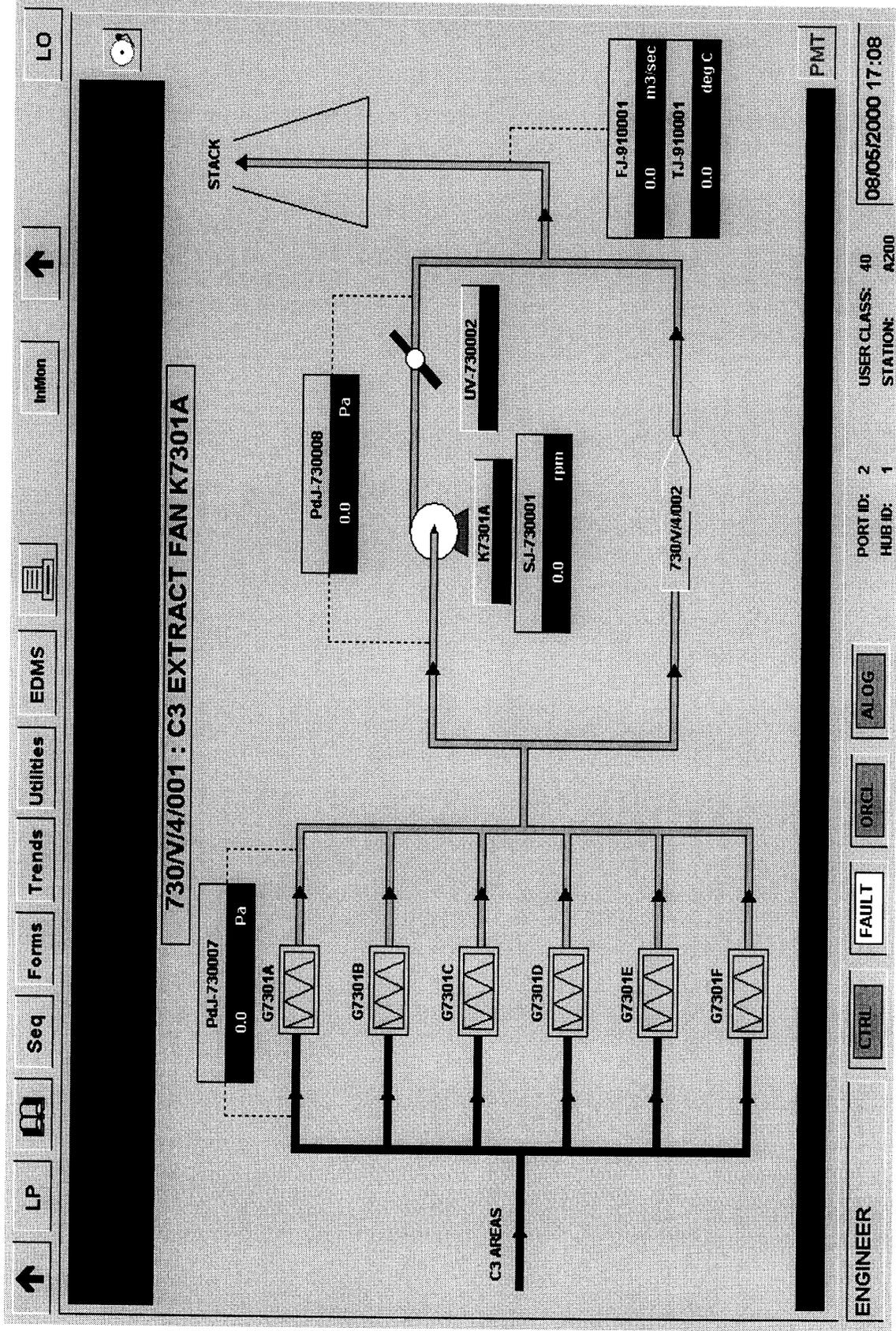


Fig 4A – Typical Layout for Mimic Screens Levels 1, 2, 3 or 4 (Level 4 in above example)

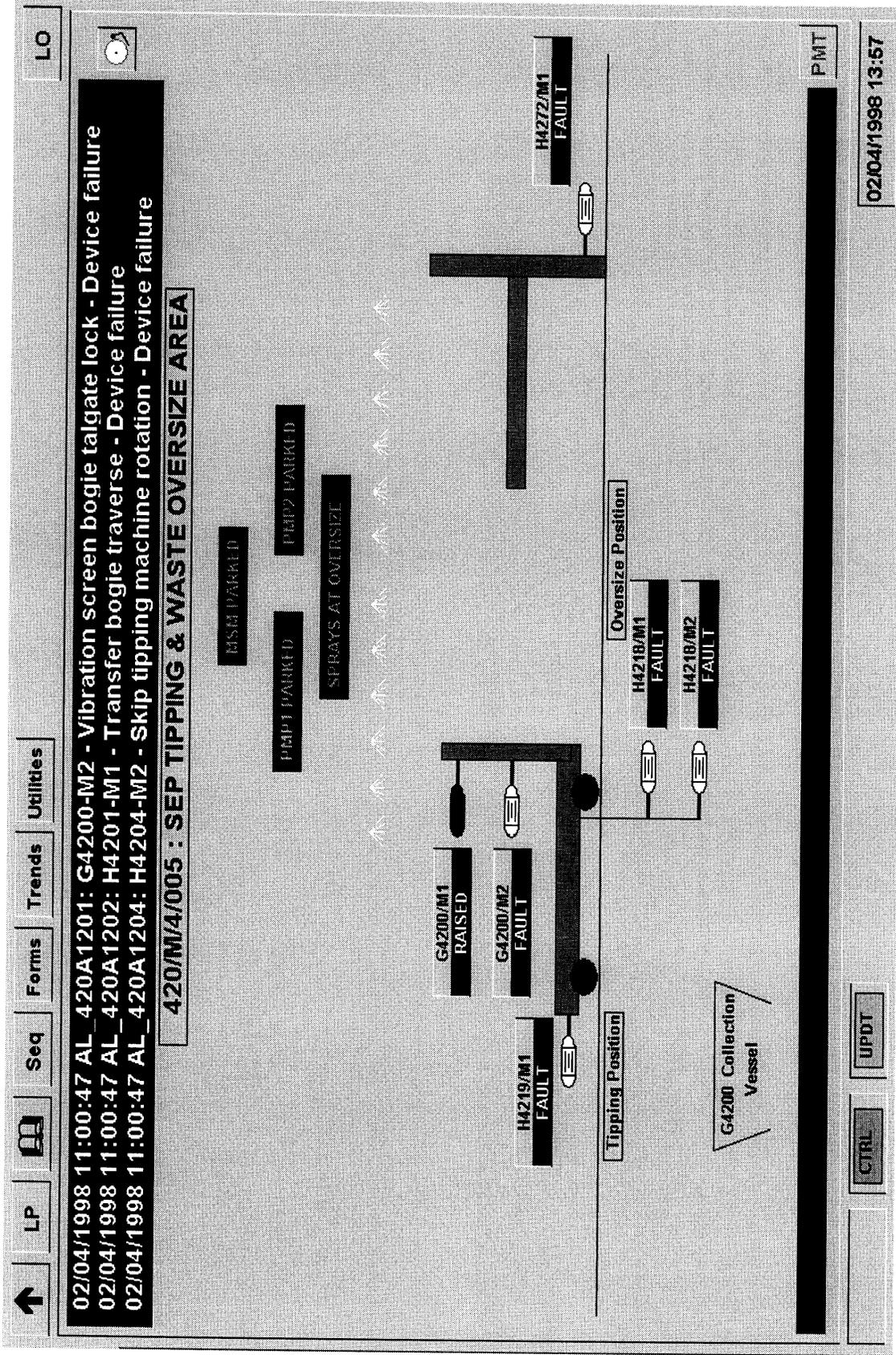


Fig 4B – Typical Level 4 Detailed Plant Mimic

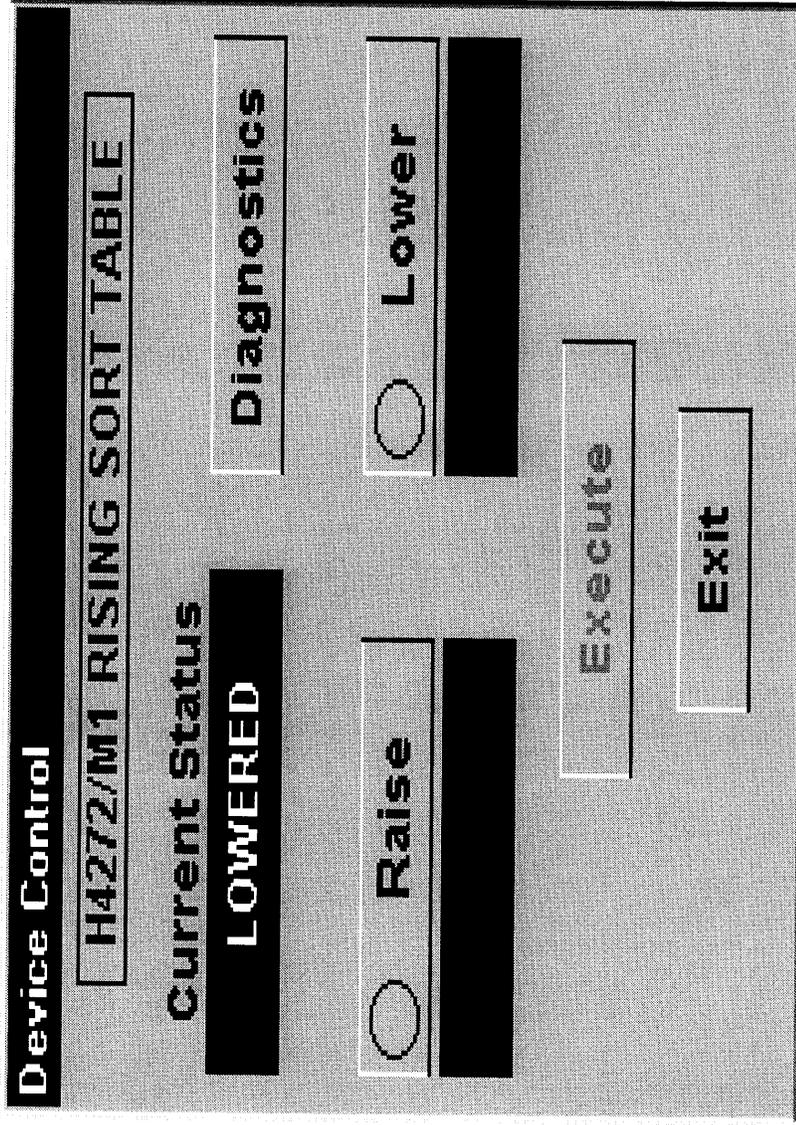


Fig 5 – Example of Device Control Faceplate

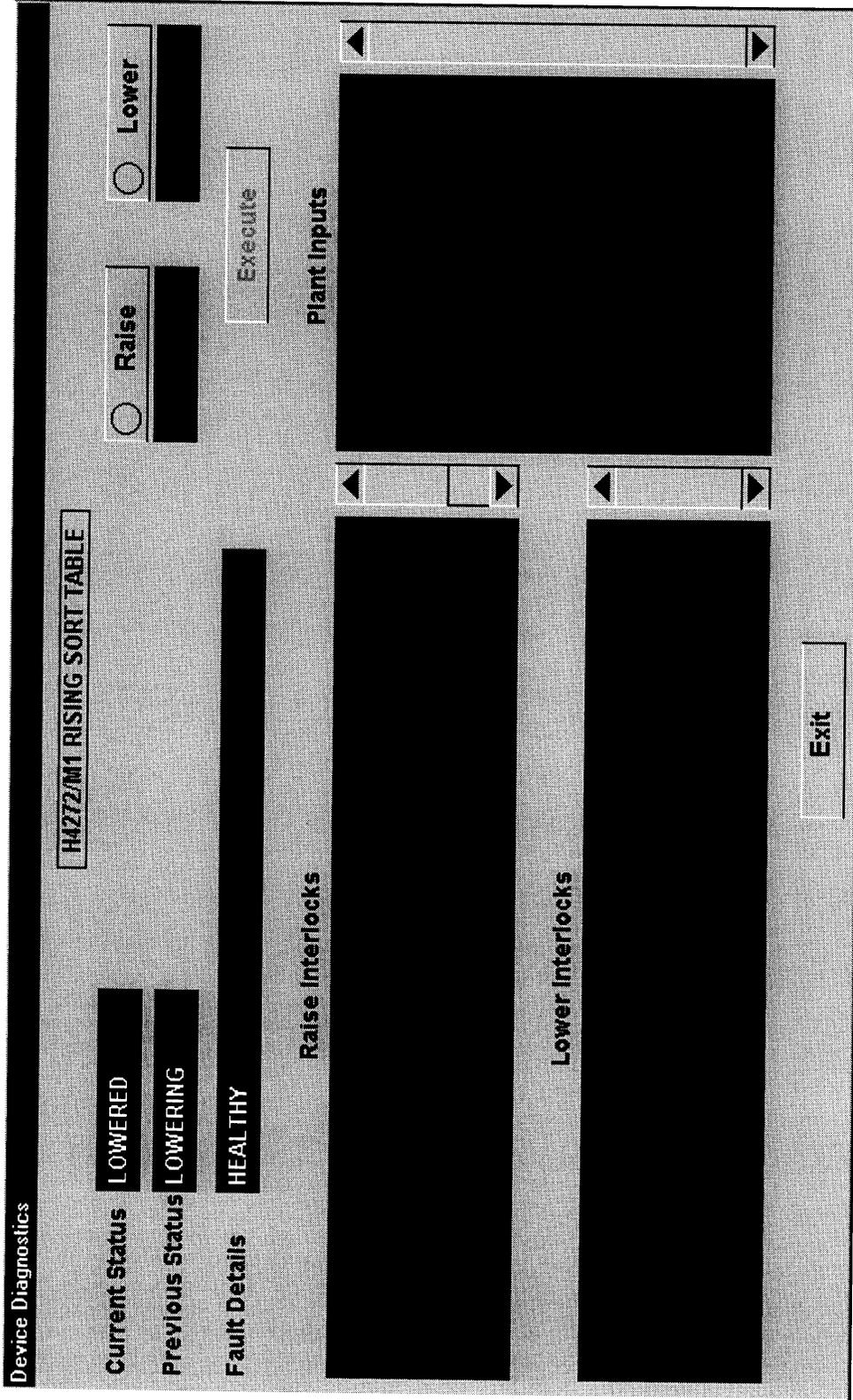


Fig 6 – Example of Device Diagnostics Faceplate

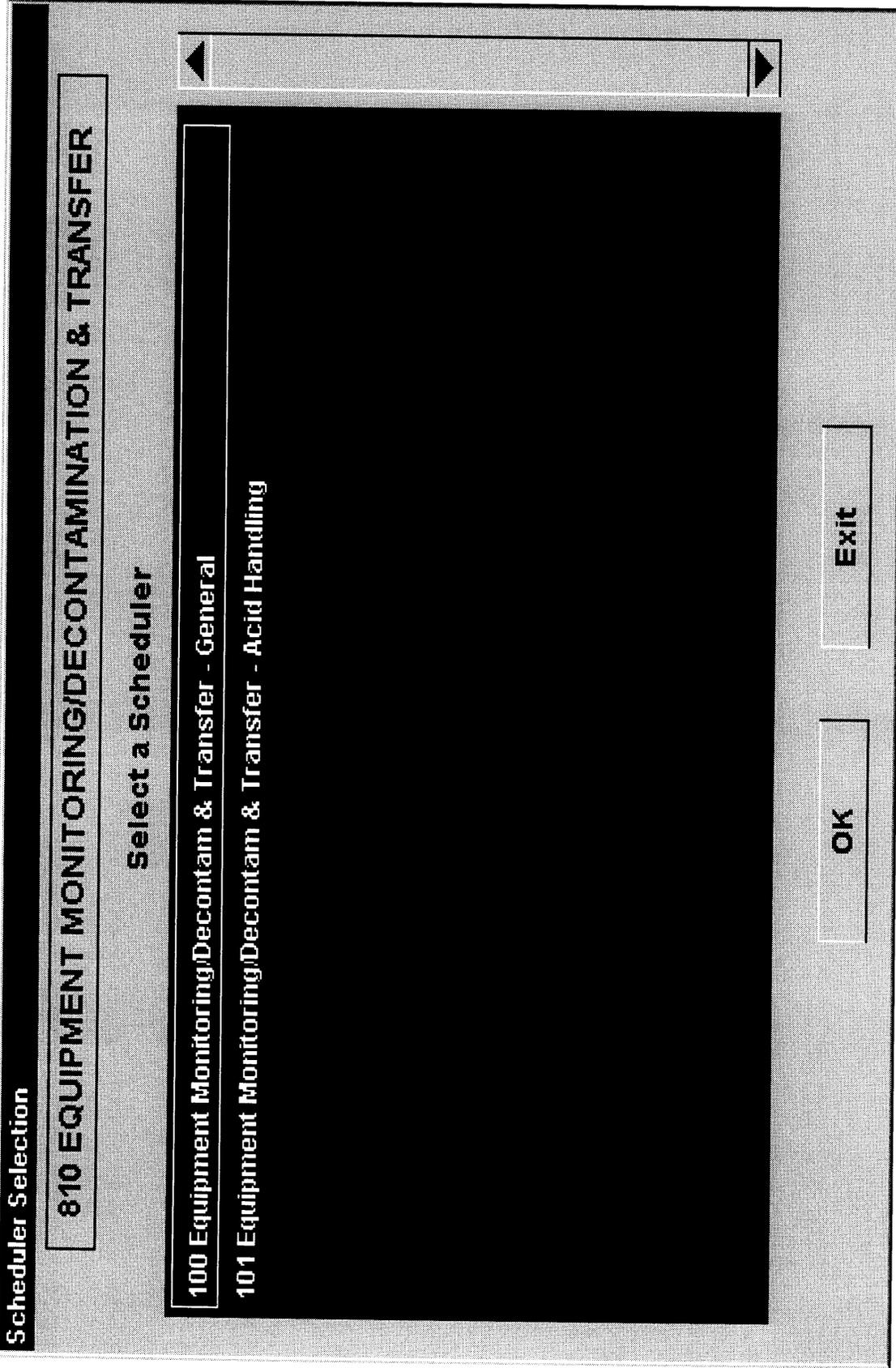


Fig. 7A - Example of Scheduler Selection Faceplate

Sequence Control

730 C3 EXTRACT

Group / Scheduler

100 C3 EXTRACT FAN OPERATION

200 Extract Fan K7301A run

201 Extract Fan K7301B run

Step	State
0	IDLE
0	IDLE
0	IDLE

Start
 Abort
 Stop
 Step On
 Select

Fig. 7B - Example of Sequence Control Faceplate

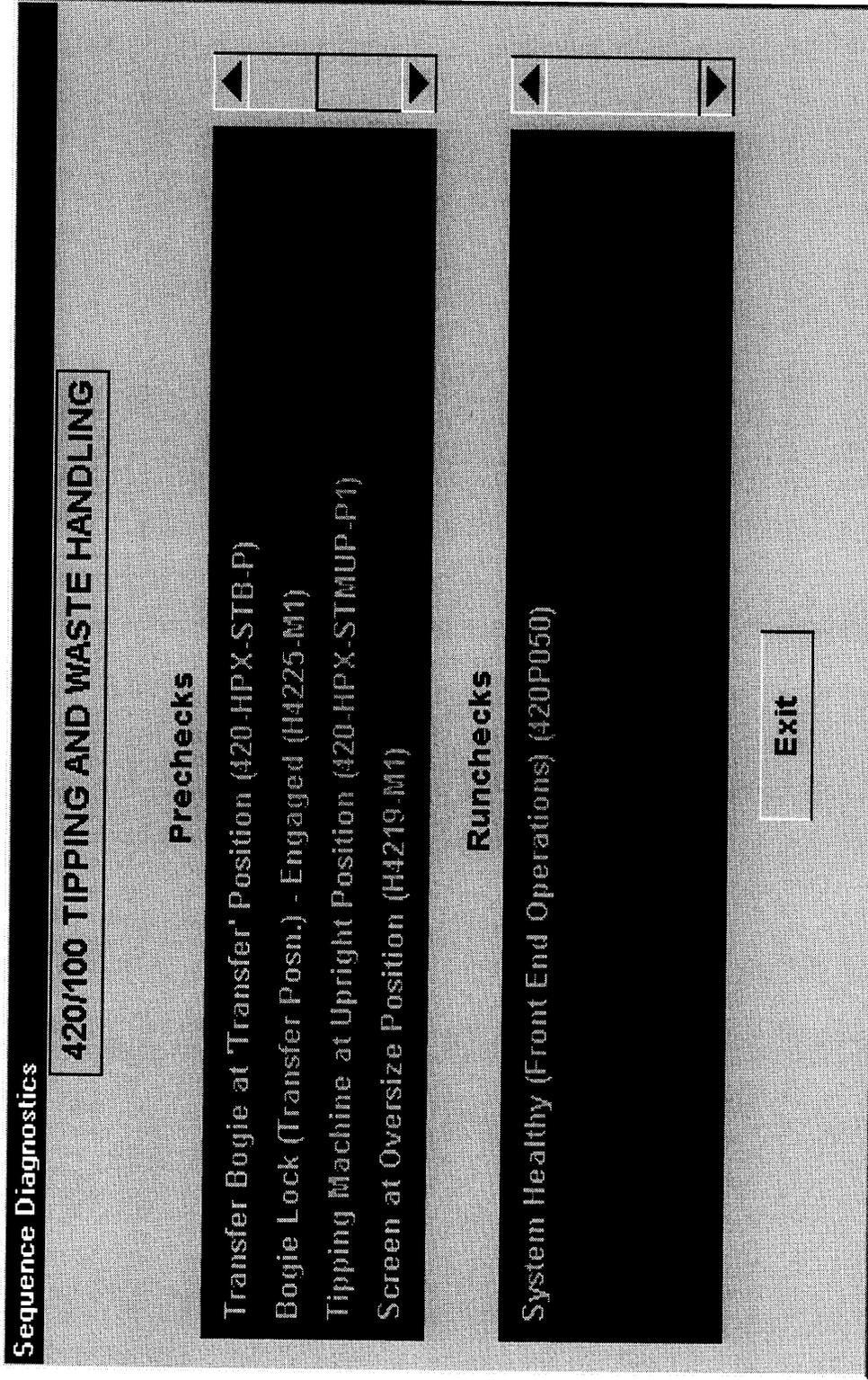


Fig. 8 - Example of Sequence Diagnostic Faceplate

Sequence Control

810 EQUIPMENT MONITORING/DECONTAMINATION & TRANSFER - GENERAL

Group / Scheduler	Step	State
100 Equipment Monitoring/Decontam & Transfer - General	0	IDLE
215 F8200 Sump Emptying	0	IDLE
218 F8100 Sump Sentencing	0	IDLE
219 F8100 Sump Emptying - Ejector W8100A	0	IDLE
220 F8100 Sump Emptying - Ejector W8100B	0	IDLE
224 F8107 Sump Emptying	0	IDLE
225 T8105 Citric Acid Recirculation	0	IDLE
226 T8107 Citric Acid Recirculation	0	IDLE
209 H8162 In-cell Spray/MSM Operated Wash Lance	0	IDLE
210 H8139 Equipment Wash Tank	0	IDLE
211 F8105 Bund Area Washdown	0	IDLE
216 H8237 Hand Spray - C3 Workshop	0	IDLE

Start
 Abort
 Stop
 Step On
 Select

Fig. 9 - Example of Sequence Control Faceplate for a Process based System

Appendix 5 – System Size

The overall size of the ICS is still not fully defined. However current estimates suggest it will be as follows:

Estimate of total I/O

System No	Description	Server No.	DI	DO	AI	AO	LPS No.s	BCR No.s	Total I/O
210	Characterization	200	157	88	0	0	0	13	245
310	Waste Rec'r & Stage	300B	175	66	3	0	2	8	244
320	Box Import	300A	204	72	9	0	0	3	285
330	North Sort Box Line	300A	115	46	0	0	0	0	161
335	N Box Line Conveying	300B	270	95	1	0	2	6	366
340	South Box Sort Line	300A	98	6	5	0	0	0	109
345	S Box Line Conveying	300B	264	108	6	0	2	4	378
350	Box Size Reduction	300A	13	4	1	0	0	0	18
352	Clean Box Impr/LLW Expt	300A	110	34	1	0	0	4	145
370	Central Drum Conveying	300B	375	174	0	0	2	5	549
390	In Plant Drum Assay	300B	113	43	0	0	1	2	156
410	Supercompaction	400	172	68	5	0	0	2	245
420	Macroencapsulation	400	222	81	2	0	0	5	305
422	Macro. Drum Imp/Exp	400	134	48	0	0	0	4	182
423	S/C & SCW Import	400	186	54	4	0	0	TBD	244
440	Special Case Waste	400	233	64	0	0	0	TBD	297
600	Utilities	700	TBD	TBD	TBD	TBD	0	0	TBD
710	Ventilation	700	212	38	46	9	0	0	305
730	Ventilation	700	331	59	72	13	0	0	475
750	Ventilation	700	195	35	42	8	0	0	280
Totals			3579	1183	197	30	9	56	4989

Note: Expansion capacity must be provided as specified in section 9.7

Servers have been allocated to systems so as to minimize the amount of plant interaction across server boundaries.

Estimate of required numbers of ICS Schedulers, groups and mimics

System No	Description	Groups	Schedulers	Mimics
210	Characterization	20	3	6
310	Waste Rec'r & Stage	34	1	7
320	Box Import	28	3	9
330	North Sort Box Line	26	1	8
335	N Box Line Conveying	15	1	6
340	South Box Sort Line	26	1	8
345	S Box Line Conveying	15	1	6
350	Box Size Reduction	3	1	2
352	Clean Box Imprt/LLW Expt	20	1	2
370	Central Drum Conveying	TBD	TBD	10
390	In Plant Drum Assay	31	5	9
410	Supercompaction	19	1	4
420	Macroencapsulation	30	1	4
422	Macro. Drum Imp/Exp	55	1	11
423	S/C & SCW Import	TBD	TBD	6
440	Special Case Waste	TBD	TBD	3
600	Utilities	TBD	TBD	2
720	Ventilation	TBD	TBD	5
740	Ventilation	TBD	TBD	5
760	Ventilation	TBD	TBD	5
Totals				

These size estimates will be refined as the plant design is developed.

Estimate of number of Plug in points

The estimated numbers of plug in points is as follows:

<u>Process System* No.</u>	<u>Server</u>	<u>Local Workst ation</u>	<u>Plug in Points</u>	<u>Zone</u>
210	200	1	5	
310	300B	2	9	1
320	300A	1	2	
330	300A	3	4	3
335	300B	1	5	3
340	300A	3	4	3
345	300B	1	8	3
350	300A	1	2	3
352	300A	1	2	1
370	300B	4	4	3
390	300B	2	3	
410	400	4	4	
420	400	1	2	2
422	400	1	2	1
423	400	6	2	clean
440	400		5	
600	700		TBD	
720	700	0	2	
740	700	0	2	
760	700		2	
Total			69	

It is anticipated that operational constraints will make it difficult to remove a lap top PC from a higher contamination zone to a lower one.

End of Document

The tests **shall** include common functions such as alarm handling, diagnostics, ergonomics, mode control, generic SCADA items, etc.

The tests **shall** also focus on System Interfaces, including

- PLC to PLC,
- SCADA to DMS facilities.

The tests shall demonstrate satisfactory operation of process run through, e.g. tracking, assay as determined by the SPD test documentation.

12.3.8 Integration CAT (Using Simulators) – without DMS

This **shall** be a repeat of the Pre-CAT Integration Test, witnessed by BNFL Inc.

12.3.9 ICS - DMS Integration CAT (Using Simulators) – with DMS

This **shall** be a repeat of the Integration CAT Test, including DMS elements to demonstrate operability of the ICS – DMS interface.

12.3.10 SAT Testing.

This phase of testing, involving the System Integrator, is the Site Acceptance Test (SAT) which **shall** take place once the System Supplier and BNFL Inc. have installed the equipment at INEEL and set it to work. This shall consist of a sub-set of the Integration CAT Test and shall demonstrate no impairment resulting from transport, setting to work or site environment.

At the successful completion of SAT Testing BNFL Inc. shall issue a certificate of acceptance.

12.3.11 Commissioning SPD's.

Commissioning System Performance Demonstration lies outside the scope of this document.

A written document **shall** be produced detailing all of the necessary fields and their associated parameters for each of the sets of data required for both Product Quality and Waste Tracking data.

The document **shall** also specify where in the Control System architecture this data is to be stored and what format, together with at what point it **shall** be removed.