MANUAL

HUMAN-MACHINE INTERFACE IN A CONTROL ROOM

DEP 32.00.00.11-Gen.

July 1997

DESIGN AND ENGINEERING PRACTICE

USED BY

COMPANIES OF THE ROYAL DUTCH/SHELL GROUP

PREFACE

DEP (Design and Engineering Practice) publications reflect the views, at the time of publication, of:

Shell International Oil Products B.V. (SIOP)
and
Shell International Exploration and Production B.V. (SIEP)
and
Shell International Chemicals B.V. (SIC)

The Hague, The Netherlands,

and other Service Companies.

They are based on the experience acquired during their involvement with the design, construction, operation and maintenance of processing units and facilities, and they are supplemented with the experience of Group Operating companies. Where appropriate they are based on, or reference is made to, national and international standards and codes of practice.

The objective is to set the recommended standard for good design and engineering practice applied by Group companies operating an oil refinery, gas handling installation, chemical plant, oil and gas production facility, or any other such facility, and thereby to achieve maximum technical and economic benefit from standardization.

The information set forth in these publications is provided to users for their consideration and decision to implement. This is of particular importance where DEPs may not cover every requirement or diversity of condition at each locality. The system of DEPs is expected to be sufficiently flexible to allow individual operating companies to adapt the information set forth in DEPs to their own environment and requirements.

When Contractors or Manufacturers/Suppliers use DEPs they shall be solely responsible for the quality of work and the attainment of the required design and engineering standards. In particular, for those requirements not specifically covered, the Principal will expect them to follow those design and engineering practices which will achieve the same level of integrity as reflected in the DEPs. If in doubt, the Contractor or Manufacturer/Supplier shall, without detracting from his own responsibility, consult the Principal or its technical advisor.

The right to use DEPs is granted by SIOP, SIEP or SIC, in most cases under Service Agreements primarily with companies of the Royal Dutch/Shell Group and other companies receiving technical advice and services from SIOP, SIEP or SIC. Consequently, three categories of users of DEPs can be distinguished:

1) Operating companies having a Service Agreement with SIOP, SIEP, SIC or other Service Company. The use of DEPs by these Operating companies is subject in all respects to the terms and conditions of the relevant Service Agreement.

2) Other parties who are authorized to use DEPs subject to appropriate contractual arrangements.

3) Contractors/subcontractors and Manufacturers/Suppliers under a contract with users referred to under 1) or 2) which requires that tenders for projects, materials supplied or - generally - work performed on behalf of the said users comply with the relevant standards.

Subject to any particular terms and conditions as may be set forth in specific agreements with users, SIOP, SIEP and SIC disclaim any liability of whatsoever nature for any damage (including injury or death) suffered by any company or person whomsoever as a result of or in connection with the use, application or implementation of any DEP, combination of DEPs or any part thereof. The benefit of this disclaimer shall inure in all respects to SIOP, SIEP, SIC and/or any company affiliated to these companies that may issue DEPs or require the use of DEPs.

Without prejudice to any specific terms in respect of confidentiality under relevant contractual arrangements, DEPs shall not, without the prior written consent of SIOP and SIEP, be disclosed by users to any company or person whomsoever and the DEPs shall be used exclusively for the purpose for which they have been provided to the user. They shall be returned after use, including any copies which shall only be made by users with the express prior written consent of SIOP and SIEP. The copyright of DEPs vests in SIOP and SIEP. Users shall arrange for DEPs to be held in safe custody and SIOP or SIEP may at any time require information satisfactory to them in order to ascertain how users implement this requirement.

All administrative queries should be directed to the DEP Administrator in SIOP.

NOTE: In addition to DEP publications there are Standard Specifications and Draft DEPs for Development (DDDs). DDDs generally introduce new procedures or techniques that will probably need updating as further experience develops during their use. The above requirements for distribution and use of DEPs are also applicable to Standard Specifications and DDDs. Standard Specifications and DDDs will gradually be replaced by DEPs.

TABLE OF CONTENTS

APPENDICES

1. INTRODUCTION

1.1 SCOPE

This is a new DEP which specifies requirements and gives recommendations for the proper design of the Human-Machine Interface (HMI) of the plant monitoring and control systems to reduce human errors in the operation of the plant. It may be used for new projects or to improve the design of an existing HMI.

The DEP contains a starter set of graphic configurations.

1.2 DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS

Unless otherwise authorised by SIOP, the distribution of this specification is confined to companies forming part of the Royal Dutch/Shell Group or managed by a Group company, and to Contractors nominated by them (i.e. the distribution code is "C" as defined in DEP 00.00.05.05-Gen.).

This DEP is intended for use in oil refineries, chemical plants, gas plants, oil and gas production facilities and supply/marketing installations.

If national and/or local regulations exist in which some of the requirements may be more stringent than in this DEP, the Contractor shall determine by careful scrutiny which of the requirements are the more stringent and which combination of requirements will be acceptable as regards safety, environmental, economic and legal aspects. In all cases the Contractor shall inform the Principal of any deviation from the requirements of this DEP which is considered to be necessary in order to comply with national and/or local regulations. The Principal may then negotiate with the Authorities concerned with the object of obtaining agreement to follow this DEP as closely as possible.

1.3 DEFINITIONS AND ABBREVIATIONS

1.3.1 General definitions

The **Contractor** is the party which carries out all or part of the design, engineering, procurement, construction, commissioning or management of a project or operation of a facility. The Principal may undertake all or part of the duties of the Contractor.

The **Manufacturer/Supplier** is the party which manufactures or supplies equipment and services to perform the duties specified by the Contractor.

The **Principal** is the party which initiates the project and ultimately pays for its design and construction. The Principal will generally specify the technical requirements. The Principal may also include an agent or consultant authorised to act for, and on behalf of, the Principal.

The word **shall** indicates a requirement.

The word **should** indicates a recommendation.

1.3.2 Specific definitions

Anthropometry	Deals with the measurement of the dimensions and certain other physical characteristics of the human body which provide information for the design of things people use.
Configuration	The selection process using predefined software of the DCS .
Control room	The section of a control centre containing the essential equipment required to operate the plant optimally and safely.
Display	What is seen on a visual display unit.
Distributed Control System (DCS)	A configurable microprocessor-based control system.

Ergonomics (human factors)	The application of human physical and cognitive sciences in conjunction with the engineering sciences to achieve the optimum human performance and interaction between a human user and a machine.
Ergonomic design	User-entered, task-based design which focuses on developing system requirements based on the capabilities and limitations of humans while executing system tasks.
Human-Machine Interface (HMI)	All the areas where people interact with the system. In this DEP it mostly refers to the DCS operator workstation but it may also be the engineering workstation.
Faceplate	A display pre-configured in the DCS that resembles the display and controls of the equivalent conventional panel instrument. It could be a controller faceplate (allowing SP output and controller mode changes), an indicator faceplate, a switch faceplate (status and output changes), etc.
Instrumented Protective Function (IPF)	A function comprising the Initiator function, Logic Solver function and Final Element function for the purpose of preventing or mitigating Hazardous Situations.
Instrumented Protective System (IPS)	The electromechanical, electronic and/or programmable electronic Logic Solver component of the Instrumented Protective Function, complete with input and output equipment.
Link analysis	A technique to define relationships between people and components of the system. It is also used as a tool which is used to identify the movement of people within a system.
Operator console	A group of equipment comprising VDU screens, keyboards, pointing devices and switches which are allocated to a defined part of the plant (e.g. "console for hydrogen units").
Parameters	The variables associated with a tag or point. For example, AUTO, MAN, CASCADE are parameters of controller points.
Points and tags	The instrument, numeric, timer, flag, Boolean, logical entities within the DCS. Both words are used interchangeably, with "points" often being used when calculated or inner variables of the DCS are being referred to. "Tags" generally refer to data coming from wired or data inputs to the DCS.
Subsystem	A microprocessor-based system configured for specific control and monitoring applications, which can operate in isolation or communicate with a DCS.
System security	Safeguards within the monitoring and control systems to prevent occurrence of conditions which might compromise the integrity of the system and the plant which is being operated.
System access	The way into the various parts of the system. This might involve the temporary bypassing of some of the security parameters.
Task	A set pattern of operations with the intent of achieving a goal.
Task analysis	A method for describing what an operator is required to do, in terms of actions or cognitive processes, to achieve a system goal.
Workstation	User's workplace with an HMI within the control room. A console typically consists of several workstations.
Window	A portion of the screen that contains a display. The display could be graphics, messages, instrument faceplates, trends etc.

1.3.3 Abbreviations

APC	Advanced Process Control
BOD	Basis of Design
BDP	Basic Design Package
BDEP	Basic Design and Engineering Package
CCTV	Closed-Circuit Television
CRT	Cathode Ray Tube
DCS	Distributed Control System
ESD	Emergency Shutdown
FAT	Factory Acceptance and Testing
FGS	Fire, Gas and Smoke detection and protection system
HMI	Human - Machine Interface
IPF	Instrumented Protective Function
IPS	Instrumented Protective System
LED	Light Emitting Diode
MOS	Maintenance Override Switch
ODS	Operational Data Supervision
OOS	Operational Override Switch
PC	Personal Computer
PS	Project Specification
PEFS	Process Engineering Flow Scheme
PV	Process Value (process parameter being measured)
QMI	Quality Measuring instrument
SAT	Site Acceptance and Testing
SER	Sequence of Events Recorder
SP	Set-point
VDU	Video Display Unit

1.4 CROSS-REFERENCES

Where cross-references to other parts of this DEP are made, the referenced section is shown in brackets. Other documents referenced in this DEP are listed in (12).

2. GENERAL

The application of DCS for controlling process plants has substantially changed the task of the operators. Control using the DCS has paved the way to activities which are more supervisory in nature. In addition, demands for safer and more efficient operations have resulted in operators being given more demanding tasks. Design of the HMI can improve or worsen the way in which a plant is operated and maintained. Poor HMI design can cause errors which will endanger integrity, safety and the environment and lead to lower productivity and plant availability.

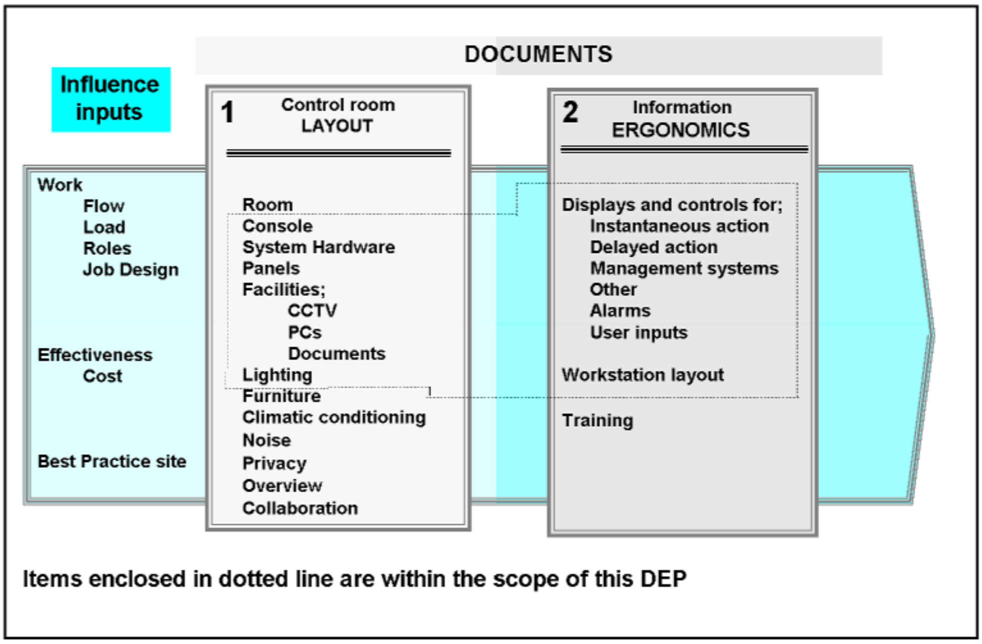
This DEP gives guidance on how the HMI should be designed to assist the operator and to minimise errors in using the system, with respect to:

- DCS Displays;
- ODS Displays;
- Alarm Management;
- HMI Hardware.

Within the context of control room design this DEP currently covers only the information ergonomics of the HMI (see Figure 1). The physical layout of the control room and the organisation of work are outside the scope of this DEP but shall be considered in the overall design of the control room (see ISO/DIS 11064-3 and DEP 34.17.10.30-Gen.).

This DEP is based on the capabilities of recent DCSs which are supported by SIOP.

FIGURE 1 Content design for control rooms



3. HMI DESIGN PHILOSOPHY

3.1 INTRODUCTION

This section deals with the general rules related to the configuration of the DCS and the design of the HMI. It serves as the framework for the detailed design which is covered in later sections of this DEP. The design of the HMI shall be conducted by a team of operators advised by an ergonomist and experts from other disciplines as required.

NOTE: The tasks that the operator must perform and understand, as well as other human factors, should be considered in the HMI design. To support this goal, detailed task analyses are required. Ergonomic advice will be sought to help perform these task analyses.

3.2 OPERATING PHILOSOPHY

The DCS shall be configured so that the operator can work simultaneously in two different modes. These modes are captioned as:

Awareness
This mode requires the proactive role of the operator in controlling the plant. He monitors the status of the plant by paging through displays, watching trends and deviations and taking action when required or prompted. Awareness is improved by a well-designed hierarchical arrangement and a logical and understandable grouping of the DCS displays.

Exception
This reactive mode is triggered by events such as alarms. The operator's attention is demanded and directed by the system to displays where he can see what has happened and can take corrective action. Visualisation of alarms and access to corrective controls depend on the urgency of action required.

3.3 PROCESS SITUATIONS

The HMI shall be configured as follows for all operating conditions:

- Steady state - running normally;
- Perturbed or plant upset (off steady state) - Pump trips, operating situation exceeds constraint, control instability;
- Normal deviations or transients (change of steady state) - Start-up, scheduled shutdowns, feed changes;
- At rest - "plant stopped".

Figure 2 shows the various operating conditions and corresponding control tools that the operator needs.

The work activity, the degree of vigilance, surveillance and reaction time of the operator are different for each operating condition.

The HMI shall be designed to assist the operator and all other users of the DCS in performing their tasks under all the operating conditions. This involves specific displays and alarm handling strategies for the various operating situations. Controls shall be intuitive and images shall be self-explanatory, leading the operator to the corrective actions he has to take to restore the plant to steady state.

NOTE: A task analysis is required in order to understand the various actions the operator must take to restore the system to steady state. The analyst (ergonomist) should focus on the operator's task using the DCS interface.

The DCS and HMI shall be configured according to the urgency of the actions required in the following way.

- For cases in which the actions to be taken depend on the operator's analysis of the context of the situation or if the corrective action must be taken within a specified time, the operator shall be supported by information such as alarms, messages and good diagnostic help screens, together with automation which brings the process to the most manageable state.

- If the corrective action is known (without ambiguity) automation should also be applied and the HMI should prompt the operator with the automation options mentioned in the note below.

NOTES: 1. Execution of automation in the DCS may be AUTO, SEMI-AUTO or MANUAL WITH AUTO-PROMPTING.

2. Examples of automation are schemes to reduce throughput, trip to minimum firing in furnaces, grade switching, etc.

FIGURE 2 Plant operating conditions and corresponding activities of the panel operator

	STEADY STATE	PLANT UPSET	TRANSIENTS	PLANT STOPPED
OPERATOR ACTIVITIES MAIN TASK	SURVEILLANCE Optimise operation	DIAGNOSTIC, Restore to steady state	SEQUENCE OPERATION	SURVEILLANCE
INPUTS FOR CONTROL	(A)PC Automation Trends Displays Analysis tools Alarms On-line optimisation	Alarm mangnt. Fast access to displays/data Control Automation	Alarms Operator messages Automation	Displays Alarms
WORKLOAD	LOW	HIGH DEPENDING ON UPSET SEVERITY	HIGH	LOW

3.4 CENTRALISED HMI

The DCS interface shall be the centralised interface for all control and monitoring systems and subsystems, which they include ODS, optimisation, IPS, FGS, tank gauging systems, machine monitoring system, QMIs and CCTV.

NOTES: 1. The operator requires access to the process and system parameters to carry out his tasks and does not need to know the hardware origin of information displayed on the HMI.

2. For FGS se DEP 32.30.20.11-Gen. for details.

Status of instrument equipment subsystems shall be displayed in the DCS to warn the operator of subsystem malfunctions. Warnings should indicate the severity of malfunction and the course of action to be taken by the operator.

Detailed diagnostics for maintenance personnel may also be displayed in the DCS if convenient and cost effective, otherwise they may use other interfaces.

ODS often have their own HMI, though they also remain accessible on the DCS screens via windowing techniques. ODS manipulates historical data for a long time frame and is of little use for immediate operator actions. Data calculated or scanned by the ODS from another system and which is necessary for the operator to execute his tasks shall be presented on the DCS. Attention shall be paid by the Contractor to detailing business variables that can be cascaded to the operator so that he (or the various control systems) can react by adjusting the plant.

3.5 USERS AND THEIR REQUIREMENTS

The HMI (including ODS facilities) shall meet the requirements of all users:

- Operators (panel and field)
- Shift Supervisor
- Operations Management
- Support Team (e.g. Maintenance Engineers, Technologists)

The list given is generic. Specific requirements for each project or site shall be specified for each particular user application, using task analysis.

3.5.1 Operators

Operators require clear, unambiguous displays and the possibility to take fast and flexible action.

This means that the HMI shall be configured with:

- Displays which show an overview of the overall operating situation of the plant the operator is monitoring. These displays shall incorporate status, alarms and data. These displays shall provide access to all other operator displays.
- Displays that allows the operator to control the plant.
- Effective alarm management which warns and guides the operator when alarms occur.

The HMI should also be configured with:

- Displays which help the operator achieve a safe and environment-minded, optimum economy operation.
- Display summaries and handover reports to enable the clear handover from one operational shift to another.
- Operational reports on plant performance, maintenance activities and operational planning.

3.5.2 Shift supervisor

Shift supervisors need to know what is going on and what has happened during the last shift, so the HMI shall have displays and reports designed to accommodate this. The list of displays below shall be configured. At the start of the shift the HMI shall have pre-printed intelligent, condition-sensitive, reports about the performance of the last shift in comparison to production targets and about the hand-over status.

- A graphic showing the major parameters of the unit, production balances, yields production targets and quality. These displays should include representations of the degree of latitude remaining between a parameter and its operational, economic, environmental or safety constraint. This tells the shift supervisor whether there are opportunities left for him to maximise profitability.
- Graphics showing the status of alarm activation; which alarm points are overridden, inhibited, disabled or otherwise out of operation.
- Graphics showing which controllers are not in their normal mode. This allows the shift supervisor to pinpoint control irregularities and enables investigations for corrective actions to commence.
- Sample result displays showing the time when samples were taken and the results obtained from the laboratory. This tells the shift supervisor whether his operators have any shortfall in information due to samples not being taken on time or results not coming

back from the laboratory promptly.

- Loss displays showing which valves are open to the flare, how much is lost, how much is going to slops, what is being wasted.
- The shift log display. The shift log display shall contain the same information you would find in the conventional control room log book. The shift log display information should be ported to the ODS for access via site networked PCs.

3.5.3 Operations management

Operations management needs information about the plant's overall operation and its performance. This should be given via ODS displays accessible from site networked personal computers.

3.5.4 Support team

These teams are the maintenance engineers, reliability engineers, technologists and project engineers of a site. The sort of information they need may be accessible via the ODS, but at least the following displays shall be configured within the DCS:

- Identifying defective equipment (bad inputs, out of service flags, system alarms),
- Diagnosis of plant upsets (e.g. history file access),
- Maintenance on the system (e.g. system displays),
- Modification of configuration and tuning parameters.

4. DCS DISPLAYS

The specific features and configuration guidelines for the different types of displays in the DCS are given below.

4.1 MANUFACTURERS' STANDARD DISPLAYS

Standard displays are part of the DCS default features, and have a pre-defined format and layout set by the DCS manufacturer. They may take the form of fixed panels or windows which can be called up from graphic displays or from other standard displays. Standard displays shall be configured as supporting displays to graphics, providing detailed information on instrument tags associated with or contained in the graphics. Standard displays often have attributes that are very appealing for the user but contain functionality that cannot be easily configured. At the beginning of the design for the HMI, operations and those who will configure the DCS shall examine these standard displays in order to appreciate what they do and consequently how they shall be contained within the overall philosophy being mapped out for the HMI design.

NOTES: 1. Different DCS manufacturers may have different terminology for standard displays than that which is used in this DEP.

2. The standard displays below are those which are well-known and commonly used in operating the plant. Different DCS manufacturers may have other standard displays which are not included below, i.e. trendpoint display, tuning display, overview panel, system display, configuration panel etc.

Standard displays typically consists of the following:

4.1.1 Control group

The control group displays an array of instrument faceplates for different instrument tags. The instrument faceplates correspond to function blocks in the control station and are visual representations of the status of each of these function blocks in the HMI. This display can be used to simultaneously monitor and manipulate PV, SP, output and modes (auto, manual cascade, etc.) of groups of instruments. The maximum number of faceplates per display varies for different DCS manufacturers, but eight faceplates per display is common. Control group displays are identified by a page number (can be up to 800 pages) and/or a user assignable name.

On an individual page consideration should be given to a logical allocation of instrument tags within the pages, i.e. instruments associated with a particular sub-process unit or equipment should be located together. This will enable faster manipulation of tag parameters or mode changes (e.g. cascaded control loops).

Control groups should be configured as supporting displays to graphics of process units containing these instruments. In some cases more than one control group will be required for a graphic page. These should be accessed by paging from the primary group.

4.1.2 Trend group

The trend group displays trend data of instrument tag parameters (PV, SP, output, etc.) pictorially using multicoloured trend pens. The maximum number of trend pens per display varies for different DCS manufacturers but eight trend pens are common. Trend displays are identified by a page number and/or a user assignable name.

Configuring the trend group display consists of assigning instrument tag parameters to the pre-defined pen numbers within the trend group display.

On an individual trend page consideration should be given to a logical allocation of instrument tag parameters within the pages, i.e. trends associated with a particular sub-process unit or equipment should be located together in the same way as the control group.

Trend groups are categorised based on the sampling period as well as the time during which the trend can be stored (history). High speed trends (sampling period 1-10 seconds) should be reserved for critical monitoring applications requiring high resolution trends for a short duration (e.g. compressor discharge pressure on a CCU wet gas compressor). Medium term trends (sampling period of 1 to 5 minutes) should be reserved for general purpose trending (e.g. distillation column pressure). Long term trends (sampling period of 5 to 10 minutes history of 30 days) should be reserved for information relating to plant performance (e.g. compressor energy consumption).

4.1.3 Alarm summary

The alarm summary displays process alarms in the order and time they are generated, together with the status of each individual alarm tag (acknowledged, unacknowledged, active). It can be configured to display the priority levels associated with each individual alarm or to display only alarm tags assigned with high priority levels.

Acknowledgement for all types of process alarms can be executed at this display.

A total acknowledgement feature within the alarm summary display shall not be used as this could lead to dangerous operation.

4.1.4 Tag detail

The tag detail displays the parameters associated with an instrument tag. It can include alarm settings, tuning parameters for controllers and configuration details. A real time trend which can be used for tuning is available. This display is not used in conjunction with plant operation but is specifically meant for tag parameter setting and controller tuning.

4.1.5 Alarm overview

The alarm overview displays an overview of the active alarms presented in a matrix schematic format, mimicking the classic alarm annunciator panel. If there is an alarm in a functional group of the process, the alarm is indicated in the appropriate box until it is acknowledged. The boxes can be configured as targets which, when selected, can access a graphic page, the alarm summary page or a control group from where the operator can take corrective actions.

4.2 GRAPHIC DISPLAYS

Custom displays are pictorial displays that are built up via a configuration using the graphic builder application programs on the DCS. They are built up using a combination of text, symbols, lines, patterns, graphs, dynamic data etc., where colour and animation (e.g. blinking, inverse video, dynamic process data) can also be used to convey additional information.

They usually take the form of a schematic representation of process units showing details of equipment, process flow and relevant control loops. Dynamic data for process variables, alarms and equipment status are incorporated in the schematics to provide a realistic appreciation of plant operation. In this schematic form, graphics are used to help an operator to visualise the process so as to enable him to perform his task more effectively.

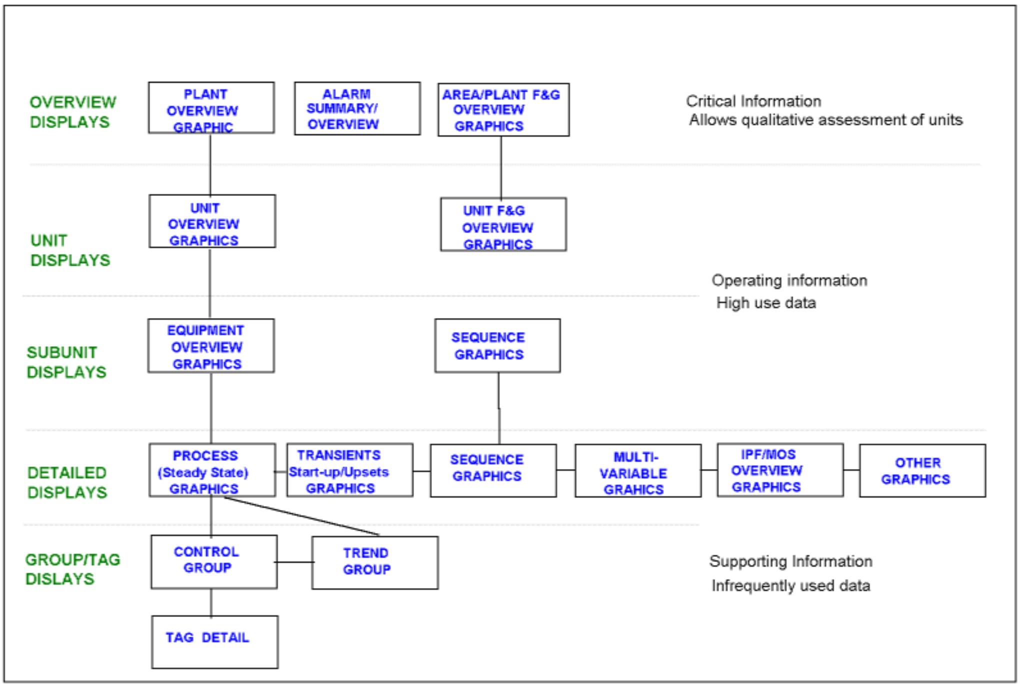
Graphics may also take the form of specific displays such as tables showing switches (UZ, OOS), APC displays, plot plans and sequence displays. In this form they are used to provide reference information to the operator.

Graphic displays are identified by a page number and/or a user assignable name.

Graphic displays shall be designed to take into consideration the different plant operating conditions as shown in Figure 2. Guidance over which type of graphic display is used for each operating condition is discussed below for each display category.

Because a single display cannot present all plant information in its entirety, a structured approach of graphic types shall be applied. The following gives guidance on the different categories and hierarchy of graphics that should be configured in the DCS. See Figure 3 below.

FIGURE 3 Typical DCS display hierarchy



NOTE: The operator should be able to form a mental map of how the displays are organised and know how to move from one display to another. This becomes difficult if there are too many layers in the hierarchy. There should be no more than five layers.

4.2.1 Overview displays

4.2.1.1 Plant overview

Consists of graphical views of all process units controlled from a particular workstation. This may be a collection of process units (e.g. hydrogen plants) or a single complex process unit (e.g. catcracker). They usually take the form of a line-up of units contained within the plant.

They shall provide the operator with the status and mode of the process units by providing dynamic data, possibly in the form of short duration trends, for key process performance parameters (e.g. feeds, rundowns, environmental monitoring etc.)

These displays are meant to be used during steady state plant conditions; details covering equipment or instrument loops shall not be shown in these displays.

Targets shall be configured within the schematics to call up the graphic displays of the process units.

Appendix 1 shows a typical plant overview display.

NOTE: Besides schematic views of plants, other presentation tools such as graphs, spider diagrams, alarm summary windows and process unit matrices may collectively be used as overview displays. They may also be added to the schematic views as information enhancing tools. Appendix 2 shows this style of overview display.

4.2.1.2 FGS area overview

This consists of a simplified plot plan depicting the relevant plants in which the FGS sensors are installed. On detection of a fire, smoke, flammable gas, toxic gas or system fault alarm, the box depicting the plant shall fill red (yellow for revealed failure robust initiators with only one of the initiators in alarm) and flash until the alarm is acknowledged. The boxes shall have symbols to display the type of alarm and shall re-flash once a new alarm is sensed. Wind speed and direction shall be shown in this display.

It should be possible to call up the FGS plant overview displays via targets configured within the boxes depicting the plants.

4.2.1.3 FGS plant overview

Consist of simplified plot plans depicting the relevant units in which the FGS sensors are installed. One plant overview display shall be provided for each plant. On detection of a fire, smoke, flammable gas, toxic gas or system fault alarm, the box depicting the units shall fill red (yellow for revealed failure robust initiators with only one of the initiators in alarm) and flash until the alarm is acknowledged. The boxes shall have symbols to display the type of alarm and shall re-flash once a new alarm is sensed. Wind speed and direction shall also be shown in this display.

It shall be possible to call up the FGS unit overview displays via targets configured within the boxes depicting the units.

Appendix 3 shows a typical FGS plant overview display.

4.2.2 Unit displays

4.2.2.1 Process unit

Provides the operating display for a particular process unit (e.g. crude distiller or hydrotreater) and an interface for the subunit displays of that process unit. One process unit display shall be made available for each of the process units.

These provide the condition of the process unit by providing dynamic data, including short duration trends, for supervising the status of the subunits (e.g. unit feed rate, furnace outlet temperature, rundown flow rates, product quality etc.).

They are mainly used for constraint optimisation and interpretation of alarms within the unit.

The unit displays are mainly used during steady state plant operating conditions. Details covering specifics of equipment or instrument lines shall not be shown in these displays.

Appendix 5 shows a typical unit displays.

4.2.2.2 FGS unit detailed

One unit detailed display shall be available for each of the process units. Where applicable a detailed display for each building, substation, analyser house and one for the FGS utility and UPS fault conditions shall be made available. In case of process units, the displays shall consists of a simplified unit layout showing the approximate physical locations of the individual sensors. For buildings, all fixed fire protection and fire control systems shall be shown on the geographic layout (including fire walls, smoke doors and dampers). When an initiator is in alarm, the symbol shall turn red and flash (see DEP 32.30.20.11-Gen.).

Wind speed and direction shall be shown in the unit display.

Appendix 4 shows a typical FGS unit display.

4.2.3 Subunit displays

4.2.3.1 Process subunit

Consist of schematic graphical views of major process equipment within a subunit, e.g. distillation column together with its auxiliaries (condenser, reboiler, etc.).

These allow control and monitoring of major process variables (e.g. reflux controller on a distillation column). Dynamic process values shall be displayed next to the equipment symbols.

Short duration trends for key control loops should be shown within this display as they provide short term historical data. This is useful during shift change and subunit analysis.

For each subunit (furnace, compressor, column, FG network etc.), the content of the displays should depend upon the prevailing operating conditions of the subunit (see Figure 2).

Appendix 6 shows a typical subunit display.

4.2.3.2 Sequence

Sequence displays are used for batch processes and subunits where sequence control is applied (e.g. catalyst regeneration in a platformer). They consist of a graphical view of the control steps as well as their respective state and an indication of the sequence step within the subunit.

Windows with sequence steps, or guidance messages, should be configured within these displays to assists the operator when problems are encountered. The windows can be accessed by clicking or touching targets configured in the graphics, or automatically displayed.

Appendix 9 shows a typical sequence display.

4.2.4 Detailed displays (steady state)

4.2.4.1 Process

These consist of schematic graphical views of process equipment within a subunit i.e. the top section of the distillation column or a compressor and its luboil system.

These displays shall show details of the equipment together with their auxiliaries and should show process values and control signal lines of instruments associated with the process equipment.

It shall allow control of the process equipment (e.g. discharge controller of the compressor). Dynamic data shall be shown next to the equipment icon.

Short duration trends for major control loops should be shown within this display as they provide short term historical data is useful during shift change and subunit analysis.

Appendix 7 shows a typical detailed process display.

4.2.4.2 Multi-variable control loops

Consist of schematic views of the multi-variable control schemes, containing process variables and tuning parameters required to monitor the system's performance. These displays are typically used by technologists and control engineers for diagnostic purposes.

Appendix 8 shows a typical multi-variable control loops display.

4.2.4.3 Sequence

These consist of a graphical view of the control steps and their respective state for a particular equipment.

Windows with sequence steps, or guidance messages, shall be configured within these displays to assists the operator in case problems are encountered. The windows can be accessed through targets configured in the graphics, or automatically displayed.

4.2.4.4 IPF logic status

This is a schematic representation of the IPF logic (e.g. using "cause and effect" matrix) displaying the status of the individual IPFs and override facilities (e.g. MOS, OOS, automatic overrides) that are grouped for each equipment or process unit.

If feedback signals are available, they shall be used to display the status of IPF outputs (e.g. valve limit switches, motor running contacts, etc). Where feedback signals are not available status flags from the IPS shall be used.

Within these displays first failure alarms shall be displayed, acknowledged and reset.

Acknowledgement of IPF alarms and the resetting of IPFs shall be allowed within this graphic.

These displays may also be used as supporting displays for analysis of trips or for trouble shooting purposes.

NOTE: The displayed logic resides on the IPS and status updates are read by the DCS through the IPS- DCS communication link.

Appendix 10 shows a typical IPF logic status display.

4.2.5 Detailed display (transients)

These displays are based on reconfigured steady state process graphics to cater for specific transients and modes of operation. (e.g. for crude feed change, start-up, process upsets, etc.)

4.2.5.1 Start-up

These displays assist the panel operators to visualise the various phases that equipment undergoes during start-up. This may be achieved by the reconfiguration of the detailed process displays showing the steps in the start-up sequence and/ or IPF status.

Windows with written start-up procedures, or guide messages, should be configured within these displays to assists the operator with problems encountered during start-up. The windows can be accessed through targets configured in the graphics, or automatically displayed.

NOTE: Consideration should be given to implement the "help" files on a separate server in the "non-DCS environment".

4.2.5.2 Plant upset

These displays assist the panel operators to control and monitor the process during plant upsets. This may be achieved by reconfiguration of the detailed process displays to assist the operators in minimising the effects of the upset by masking consequential effects on associated equipment (e.g. minimum firing on furnaces, pump spill-back control). Options that may be considered are automatic alarm setting change, controller set-point changes, controller mode changes, etc.

Windows with written procedures, or guide messages, should be configured within these displays to assists the operator in taking the appropriate actions or allowing operator interaction. The windows should be accessed through targets configured in the graphics, or automatically displayed.

4.2.5.3 Mode changes

Mode change targets are developed within the graphics to assist the operator in making decisions. Typical mode change targets or mode displays are:

- Mode (e.g. crude) selection display;
- Mode displays to present the set-point targets, to activate them and to start/stop an individual ramping to a target set-point;
- Mode displays to compare the active mode and the new mode;
- Mode displays to monitor and control a mode transfer.

4.2.6 Other graphic displays

Displays not included in the above categories which are configured for a particular application, e.g. recipe list, operating targets, major unit parameters, shift log display, etc.

4.3 DISPLAY PAGE ALLOCATION

For each type of display the page allocation shall follow a systematic grouping, where a certain range of page numbers are related to a process unit. At the beginning of the design of the HMI, the operations personnel and the personnel who will configure the DCS shall map out the range of pages to each of the process units, taking into consideration the number of pages needed as well as spares for future display additions. The table below shows a typical allocation of display pages.

Process Unit	**Control Group (CG)**	**Trend Group (TG)**	**Graphics (GR)**
Crude Distiller1	CG 001-099	TG001-099	GR001-099
Platformer	CG100-199	TG100-199	GR100-199
Hydrocracker	CG200-299	TG200-299	GR200-299
Utilities	CC300-399	TG300-399	GR300-399

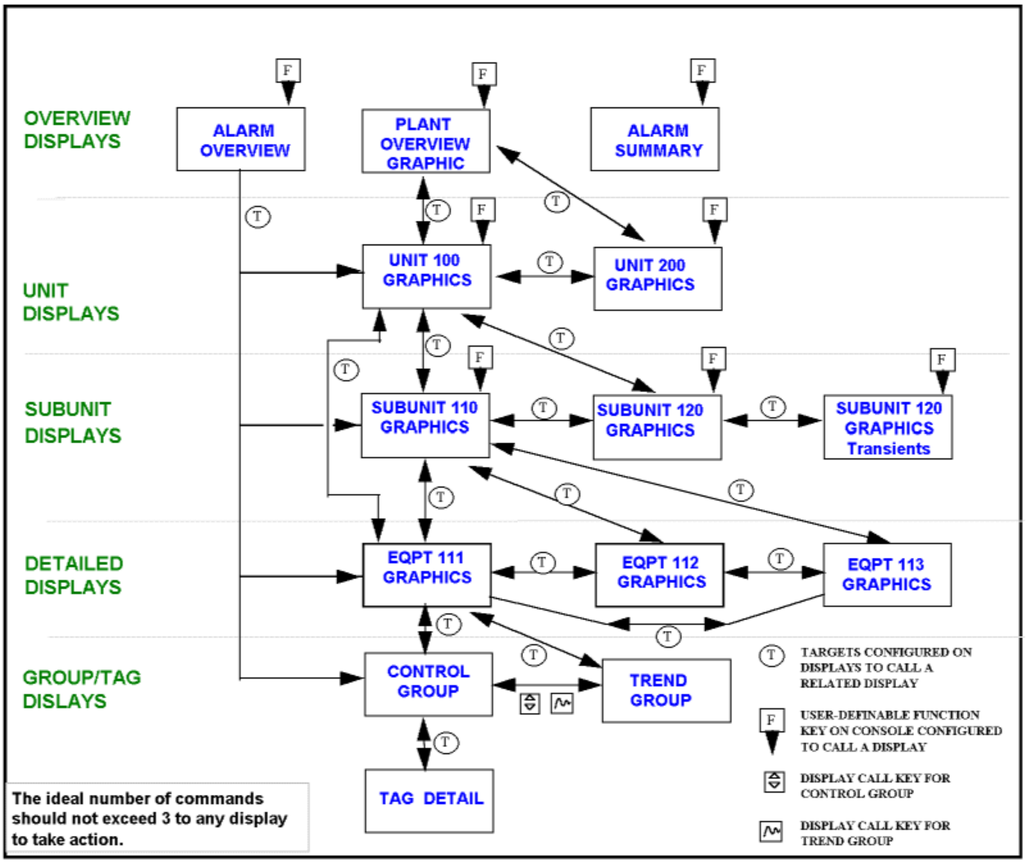
5. DISPLAY NAVIGATION

5.1 GENERAL

Displays in the DCS can be accessed using console keys or through targets configured within the graphics. Navigation through the different displays in order to take action resulting from an alarm should be achieved by a maximum of three commands.

During the design and configuration of displays, clear navigation rules should be developed to ensure that a consistent and structured approach in going from one display to another is adopted. Figure 4 shows a typical display navigation diagram.

FIGURE 4 Typical DCS display navigation scheme



5.2 DISPLAY NAVIGATION AND COMMAND TOOLS

5.2.1 Function keys

Function keys are "one touch" operation keys which can be configured to call up displays, windows and faceplates and to initiate sequences or application programs. They are used to minimise the typing of frequently used commands and requests, thereby minimising time required to access a display or initiate a sequence. They also reduce the memory load of the operator and the risk of typing errors.

Function keys are ideal for fast access to displays. However due to their limited number it is not possible to assign every display to a function key. Careful consideration should be given to their allocation.

Function keys should be arranged in logical and consistent groupings which clearly indicate their purpose.

Secondary confirmation shall be required for initiation of sequences or application programs, etc. in order to prevent inadvertent entries.

Function keys are also equipped with LEDs that can be configured to aid the operator in responding to alarm conditions.

5.2.2 Targets

Targets are areas within a graphic display which can be configured to call up displays, windows and faceplates and to initiate sequences or application programs. They have the same functionality as function keys but have the advantage of being configurable for every graphic display.

To ensure ease of operation the target area should be at least 2 cm^2 on touch targets. Smaller targets may be considered where track-ball or mouse pointing devices are used.

Generic targets should be considered for navigation purposes and consistently positioned in the screen. These may include calling detailed displays, help windows, toggling control lines, trend displays, etc.

6. ODS DISPLAYS

ODS displays could be mission-critical but are rearely time-critical for these displays the aspect of human error reduction is therefore less important.

The guidelines and conventions used for configuring DCS graphic displays (where applicable) should also be used for configuring ODS displays. Where similar displays are available on the DCS and ODS a clear distinction should be made to avoid confusing the operator, especially if they are shown physically next to one another.

NOTE: Task analysis should support which displays should be allocated on the DCS and ODS.

7. GUIDELINES FOR GRAPHIC DISPLAY BUILDING AND CONFIGURATION

7.1 GENERAL

This section is intended to promote a consistent layout and configuration of graphic displays. It gives guidelines on how the graphics should be built as well as how to present information effectively.

7.2 DENSITY OF INFORMATION ON SCREENS

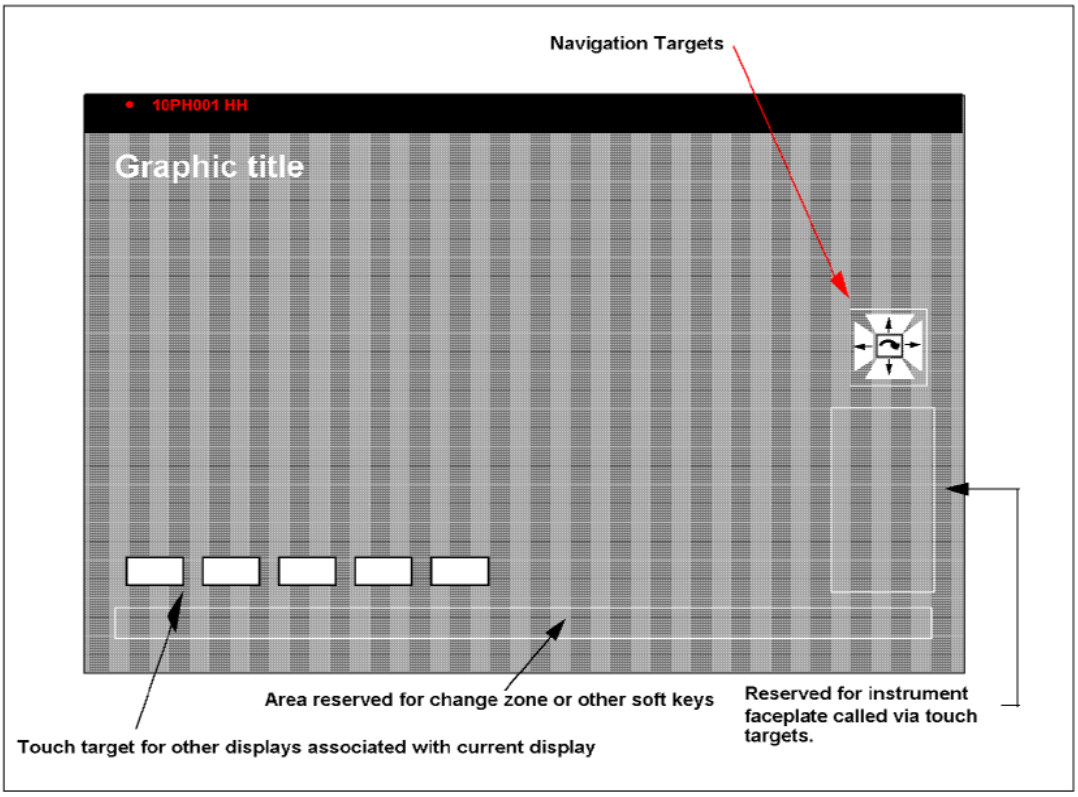
Graphic displays should not be cluttered since excessive information may result in extended search times by the operator and a loss of clear direction.

There should be no more than 40 live data points per display.

7.3 GENERIC GRAPHIC TEMPLATE

Specific areas of the screens should be reserved for certain kinds of information, such as graphic titles, navigation targets and command zones. These areas should be consistent on all displays and should be developed in the generic graphic template, an example of which is given in Figure 5a.

FIGURE 5a Typical generic graphic template



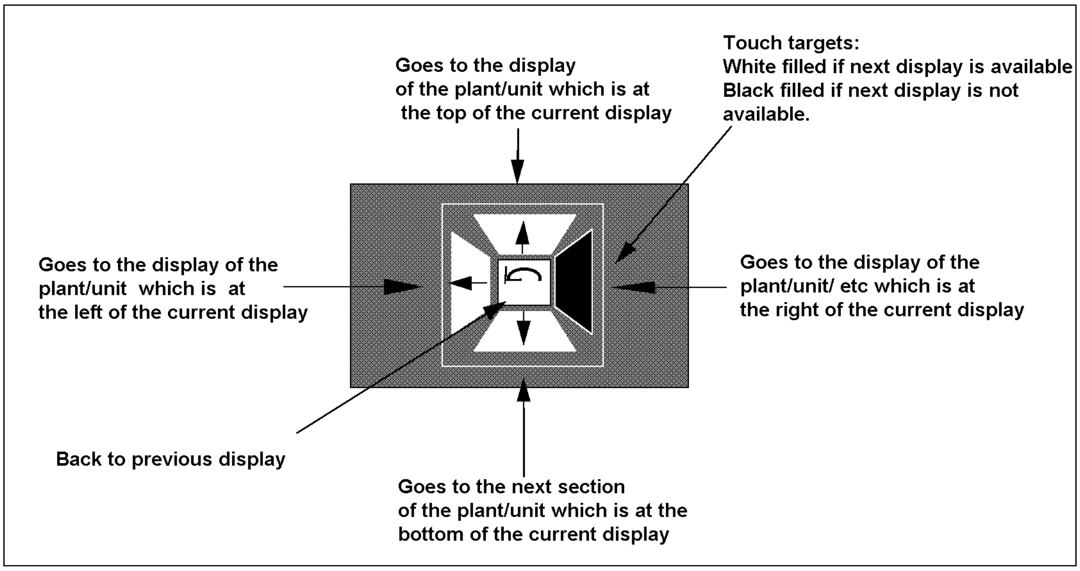
Graphics Title - Specific areas within the screen shall be reserved for the graphic title preferably in the left upper corner area.

Navigation Targets - Specific areas within the screen should be reserved for these targets in such a way that the user can "naturally" go from one screen to another for the continuation of the process. Some sites use these navigation targets, whilst other sites put the targets on the process schemes.

Command Zones - Specific areas within the screen shall be reserved for the command zones which may be used for instrument faceplates/change zones allowing the operator to make control changes.

Information Flow - screens should be organised in such a way that the user can almost "naturally" go from one screen area to another. The flow of information should be from left to right, and from top to bottom.

FIGURE 5b Navigation targets



7.4 LAYOUT FOR PROCESS SCHEME DISPLAYS

Graphics should be logically built up from major pieces of process equipment (vessels, columns, pumps, compressors etc.) and control schemes to meet the panel operators' requirements.

Graphics should be oriented from left to right with pipes or signal lines entering from the left and leaving at the right. Crossing pipes or signal lines and details not needed for the understanding of information should be avoided as much as possible.

Process equipment that cannot be controlled (e.g. isolation and bypass valves) should not be shown unless this information is needed for a proper understanding of the task.

The main criterion for depicting information should be task driven for the major equipment displayed. For example, a graphic for the control of a furnace should contain all control aspects of the coil balancing and combustion control.

The outer edges of the displays may be obscured by the rim of the CRT if the operator is not sitting directly in front of it. Therefore this area should not be used for data display.

7.5 CONFIGURATION STANDARDS

7.5.1 Introduction

It is important to develop standards or conventions for the design and configuration of graphics to discriminate between different classes of items presented on the screen. Standards within the configuration will ensure a consistent approach for all display configurations, allowing the operator to interpret symbols quickly without referring to a key. The following are typical conventions used.

7.5.2 Colours

Colour shall be used conservatively to avoid an appearance of clutter and extra strain on the eyes. The number and usage of colours should be carefully allocated reserving the more prominent colours for urgent/emergency situations.

For search or locate tasks within the displays, colours are better than size or brightness to draw attention to symbols.

To avoid the problems and ambiguities in accepted colour conventions, colour should not be the sole means of distinguishing important plant items and states. As a general rule, colour should be used together with other highlighting features (e.g. redundancy of coding).

The manner in which redundancy is achieved in a display will depend on the significance of the information which is to be conveyed. If the information is important and redundancy should be explicit, it can be achieved by adding an additional feature such as symbols, labels, inverse video, blink, brightness, size or sound.

7.5.2.1 Typical colour conventions

The colours used in the display should be:

foreground colours:	red, yellow, green, cyan, magenta, white
background colours:	light grey and dark grey

The colours given below together with their usage are those which have been commonly used in past projects. This should not limit the site in selecting colours other than the above when building up their colour convention.

COLOUR	USAGE
Red	High priority alarm indication (primary alarms and IPFs class III and higher); alarm text in alarm banner; alarm text in alarm list display; equipment with tripped/alarm status; trend line in trend display.
Yellow	Medium priority alarm indication (secondary alarms); trend line in trend display.
Green	Healthy logic signal; Fire and gas displays - bar graphs showing normal status; trend line in trend display.
Cyan	trend line in trend display.
Magenta	Unreliable data indication in process scheme displays; equipment giving readings known to be faulty; unreliable data point in process scheme; fault status in fire and gas displays; trend line in trend displays.
White	Text, labels, numeric data in normal intensity; process lines and equipment symbols in process scheme displays, electrical distribution lines, signal lines; normal status indication of equipment (open valves, running rotating machinery, circuit breaker in make state); inverse video white for manually entered data; touch target borders, half line thickness; touch target legends; framing lines in bar graph and trend displays, in block diagram displays and in instrument lines background grid in trend displays, half line thickness.
Dark grey	Background colour of the screen for all displays, except for: the background for the trend and bar graph depiction area in trend and bar graph displays; the background of displays windowed into other displays. For these two kinds of background, black should be used.

Colour conventions to be avoided:

Pure blue

Pure blue on a dark background should be avoided for text, thin lines or high-resolution information.

Chromostereopsis

Simultaneous presentation of both pure red and pure blue (or to a lesser extent red and green, or blue and green) on a dark background may result in chromostereopsis (a three-dimensional effect) and should therefore be avoided, unless chromosteriopsis is acceptable or intentional.

Pure red

Dominant wavelengths above pure red should be avoided in displays.

Background colour

Coloured (white or chromatic) information should not be used against a background which is black and has no apparent visual texture. This produces an excessive contrast between the background and the characters so that the latter may have a tendency to appear to float in space and appear at different visual distances. Also, if the background is very light it may be impossible to provide sufficient brightness for the (foreground) information to satisfy contrast requirements. It is better to have a greyish background that remains neutral in colour under the ambient light and looks like a surface on which the information is placed.

7.5.3 Highlighting

Highlighting is a means of emphasising some items in the display, such as label, data item, title or message. It is effective only when used in moderation. Excessive use of highlighting will be self-defeating as "contrast" with the surroundings is reduced. The most commonly used methods of highlighting are discussed below.

NOTE: Underlining, fonts, upper case letters, double-size characters, thin/thick/double rulings should not be used for highlighting purposes because they are not very effective in drawing attention.

7.5.3.1 Blinking

Blinking is used primarily for its powerful "attention-getting" properties. Blinking shall be used judiciously because it is distracting and distorts the structure of the display, and its "attention-getting" effect will be compromised if used indiscriminately. Blinking should be limited to situations where the user must respond quickly (e.g. alarms) and should disappear upon acknowledgement by the user. Blinking should be applied only for symbols and not for text. Blinking should alternate from high intensity to low intensity and not simply be an on-off blink.

7.5.3.2 Brightness

Brightness, or contrast enhancement, can be used to indicate the significance of particular items of information. It enables information to be located more quickly and may be used for indicating:

- which items or sequence steps are "active";
- which route has been selected in a pipe or electrical network.

As a general guideline it is recommended to use brightness differences only as a layout mechanism.

7.5.3.3 Inverse (reverse) video

Inverse video is a technique whereby items are displayed as a negative image, i.e. items normally displayed as light characters on a dark background are displayed as dark characters on a light background, or vice versa. The technique should normally be used for selected items on a display rather than for the whole screen. It is useful for highlighting significant messages, test and data fields.

Inverse video is also used for data entry.

7.5.3.4 Colour

Colour changes can be used in numerous ways to attract the attention of the operator (e.g. normal or healthy condition: green, alarm condition: red).

7.5.4 Symbols

Symbols within graphics can be used to represent specific plant items and thus assist in plant item identification. They can also be used in conjunction with other methods, e.g. colour, to indicate changes of plant item state.

An advantage of symbols is that they give a more concise representation of plant items and their states than the equivalent text labels (e.g. a filled pump symbol indicates that the pump is running and a hollow pump symbol indicates that the pump is off).

7.5.4.1 Symbol usage

Graphic symbols shall be arranged to depict physical relationships, and shall flow in a consistent manner, i.e. from left to right, from top to bottom. Arrows should be used in process lines to indicate direction of flow. Symbols should only be shown if they are important for the understanding of the operations or if they are an integral part of the process depicted. Symbol qualities (e.g. contrast, luminance) shall be used judiciously to avoid any masking of adjacent display targets.

A symbol library should be compiled and used in the process schemes. These symbols should be based on internationally used conventions e.g. ISA or PEFS symbols. They should be developed and stored in the graphic library for generating the HMI graphics. Where applicable, minimum size and associated attributes should be specified (example: closed valve: hollow, open valve: filled).

NOTE: It is useful to set up a graphic of the symbol library which depicts the different states of a symbol for different attribute conditions. Appendix 11 shows a typical symbols graphic library.

7.5.4.2 Symbol size

Given the specifications of the DCS-CRT, symbols may require adjustment if the preferred shape and size cannot be presented (e.g. a small circle changes to a hexagon if the resolution of the screen is insufficient). As a general rule a symbol (considered square or circular) should be at least 5.0 to 6.0 mm in height. This makes the symbol easily distinguishable from a distance of 1 m.

The label identifying the symbol (e.g. C 1024, V 1011) should be positioned in such a way that it is clear which symbol and identifier belong together. There should be consistency in positioning the label location relative to the symbol (e.g. underneath the pump). Vertically oriented labels should be avoided.

7.5.4.3 Typical symbols and behaviour

Valves:

Monitored valves that are shown, will normally be presented in white. A single valve symbol may be used to represent all types of valves.

Open	line colour, filled
Closed	line colour, hollow
Travelling	line colour, inverse video (On/Off Service)
Bad value	Magenta (Fail to travel)

Pumps:

Running	line colour, filled
Off (available)	line colour, hollow
Bad value	perimeter Magenta
Tripped/Alarm	Red, blinking, alternating hollow and filled, tag red until acknowledged

7.5.4.4 Process lines and process equipment

A convention should be developed for the line widths to be used in drawing process lines and process equipment. A typical convention is as follows:

Main process lines:	3-dot width
Minor and utility process lines:	2-dot width
Process equipment:	4-dot width

Crossing lines should be drawn such that the vertical line breaks at the crossing point. This should be used consistently in all graphic displays.

7.5.4.5 Instrument signal lines

Representation of instrument lines is useful at the subunit and detailed display level. Instrument lines shall not be shown at unit and plant level.

Instrument lines should be white dashed lines (1-dot width) to distinguish them from process lines. They are used to support understanding of the control schemes (i.e. showing which valve is controlled by a controller). Switched control lines shall be shown dynamically.

Whenever instrument lines are shown on a graphic, consideration should be given to a target which will toggle these lines on / off, thereby the number of items displayed on the screen. This can be achieved by using the inverse video feature.

7.5.5 Process data representation

7.5.5.1 Numeric data point

Process data should be displayed right justified, using the following typical conventions:

Flow	4 digits and a decimal point (e.g. 1.234, 12.34, 123.4, 1234 t/d, Kt/d)
Pressure	3 or 4 digits and a decimal point (e.g. 123.4, 12.3, 1.23 bar, mbar, bara)
Temperature	4 digits and one decimal point (e.g. 123.4 degC)
Level	3 digits and no decimal point (e.g. 100 %)
Tank level	5 digits and no decimal point (e.g. 12345 mm)
Controller outputs	3 digits and no decimal point (e.g. 100%)

For other process data, such as QMI output, etc., a specific convention can be used.

Tag numbers identifying numeric datapoints are useful at the unit, subunit and detailed display levels but should not be shown at plant overview display levels. Where they are shown in a graphic, consideration should be given to a target which will toggle these tag numbers on / off to reduce the number of items displayed on the screen. This can be achieved by using the inverse video feature.

The following conventions should be applied for controller outputs:

0% controller output means valve closed irrespective of the valve spring action.
100% controller output means valve open.

Colours or shaped borders may be considered to distinguish between different data points e.g. flow, level, pressure, temperature etc.

Typical data point display behaviour

Normal	Green
Alarm	Black text on red or yellow, blinking until acknowledged
Manual entry	Black text on white (inverse video)
Bad value	To the left of the value, black on magenta (inverse video) "U" for unavailable, "L" for last known value, "F" for fault

7.5.5.2 Bar display

This is commonly used to represent the level in a vessel, allowing faster recognition of level than reading a numeric data point. It shall be drawn as a simple bar display in the vessel.

Typical bar display behaviour

Normal	Bar green
Alarm	Bar red or yellow, blinking until acknowledged
Bad value	Bar magenta

7.5.5.3 Bar graph

This is a series of bar displays placed on an x-axis, with each of the bars representing a process parameter or a calculated value. They are ideal for showing relationships between two or more process parameters or deviations against performance targets. A typical example is a graph of the temperature profile from bottom to top of a distillation column.

7.5.5.4 Radar chart/spider diagrams

This is a chart with radial axes, each axis being used to represent a process parameter. A plot in the form of a closed polygon is traced on the basis of the reading for each of the axes. They are ideal for immediately spotting deviations of three or more related parameters. A symmetrical polygon plot indicates that the parameters are more or less reading the same, whereas a distorted polygon indicates deviations in the parameters. A typical application would be a plot under coil balancing control of the temperature profile of the coils of a furnace.

7.5.5.5 Short duration trends

These are small single point trend displays of 10 to 15 minutes duration which are drawn within the schematic graphic displays. In unit and subunit graphics they are preferred over numeric data points as they provide a short term history of the particular process value being monitored, which is more meaningful than instantaneous data value. As a general rule they should only be used for key or critical process parameters and a maximum of four should be used per graphic display. Consideration should be given to toggling the display of these trends on and off, with the default being off when the graphic is called. See Appendix 5.

7.5.6 Controller parameters displayed in graphics

At the plant and unit overview display levels, the measured process values (PVs) are the important operating parameters. Therefore, information displayed with or for a controller at these display levels should be limited to the PVs.

The other parameters such as setpoint (SP), output and modes (e.g. auto, manual, cascade) can be useful at the subunit and detailed display levels. In addition to PVs, these parameters may also be shown together with the controller provided they assist the operator in performing his task.

7.5.7 Labelling

Labelling is placing a descriptive title, phrase or word adjacent to a group of related items of information. Good labels provide quick identification and assist the operator in rapidly scanning for an item of interest, or help to ensure that data is being entered into the proper field.

Labels can be used to identify a single data item (e.g. tag number), a group of items or an entire display. Labels should be unique, meaningful and descriptive.

Each graphic display should be provided with a title in the top left-hand part of the display.

Data labels should be clearly distinguished from the data items themselves. Labels should be placed to the left of single items. For repeating items, the label should be placed above the columns of items. Every item should be clearly labelled. It should not be assumed that the user is able to identify individual items on account of past experience. Context plays an important role.

Where a unit (e.g %, bar) is associated with a particular data field, it should be part of the fixed label instead of having it entered by the user. In crowded data entry displays, auxiliary layout means may be adopted to distinguish labels from data.

7.5.8 Text

Text should be in lower case, with only the first letter of the first word in a sentence in upper case. Text in lower case reads more easily than text in upper case.

Upper case text should only be used to call attention to certain items or statements and for titles, headings and labels.

To bring structure into the text, it should be broken up into sections (e.g. paragraphs). These sections should be separated by blank lines. Text should be left-justified. Full (left and right) justification should not be used since it can affect legibility, especially if there is uneven spacing between words.

If text is presented on a small screen area, there should be a maximum of 50 to 55 characters on each line. On larger screen areas, the text should be broken up into two (or more) columns of 30 to 35 characters per line. The columns should be separated by at least 5 spaces if the text is left-justified, and by 3 or 4 spaces if the text is fully (left and right) justified.

The use of abbreviations should be kept to a minimum.

7.5.9 Tables

Data presented in tabular form should be aligned vertically. Alpha-numeric data should be left-justified, and numeric data should be right-justified. Where numbers contain decimal places, each number should be given the same number of decimal places. Decimal points in columns of numbers should align vertically. Indentation should be used for sub-classification.

If multiple columns are used, columns should be separated horizontally by at least 3 (but preferably 5) character spaces, or the equivalent average number of character spaces in the case of proportional fonts. If columns are not separated by vertical lines, they should be separated by at least 4 mm. In long tables, numbers should be split up into groups by providing a space between groups of 5 mm.

If tables require more space than can reasonably fit on the display screen, the user should be able to scroll the table upwards and downwards, with the column headings remaining at the top of the display screen.

Each column in a table should have a heading which should be easily distinguishable from data in the table (e.g. by case, colour highlighting, underlining etc.). Units of measurement should be given in the caption or heading, or as part of the data item. Columns and sub-headings should be arranged to reflect hierarchies and grouping of the data.

The order in which the information in a table is presented should be logical to the user and may depend on:

- the order in which the user uses the data;
- the importance of the data to the user;
- the frequency with which an item is used;
- time order (newest first or oldest first, as appropriate);
- alphabetical or numerical order.

7.5.10 Windows

Windows are particularly useful when there is a need for extra or detailed information to augment the information contained in the current display without having to use another screen or call up another display.

Typical types of standard windows in the DCSs include:

Alarm Window: Shows a list of the latest 5 alarms which can be invoked from any display through targets configured in the message bar of the screen.

Instrument Window: Shows an instrument faceplate which can be invoked through targets configured within graphics. It eliminates the need to call up the control group display when adjustments have to be made for an instrument while on a graphic display.

Trend Window: Shows the trend of an instrument which can be invoked through targets configured within graphics. It eliminates the need to call up the trend group displays when reviewing trends while on a graphic display.

Message/Help Window: Contains messages which can be used to assist the operator in the performance of his tasks. It can be invoked through configured targets within graphics or can be made to appear automatically once a particular condition is met. It is ideal for providing information for sequence steps or for announcing errors or problems in a sequence.

NOTE: 1. The above types of window can be shown simultaneously from a graphic display as they have a fixed location and a size which does not cover the whole area of the screen.

2. The above windows are those which are commonly known and used; different DCS manufacturers may have other default windows which are not included above.

Other newer generation DCSs have full windowing capabilities which can present all other types of displays as windows (e.g. graphic displays, trend displays, etc.) either individually or simultaneously. The windows can be moved, stretched, minimised, maximised and presented either in tile or overlapping arrangement for multiple open windows.

With more than two windows open, the tiled arrangement rather than the overlapping arrangement should be used. Experience has shown that the user can keep track of his task more effectively when using tiled windows since task components can be viewed on the display simultaneously. In order not to burden the memory load of the operator the maximum number of windows open at any one time shall be limited to four per CRT. This also ensures that the size of the individual windows is not too small to make the information illegible. The DCS shall be configured such that only four windows can be opened at any time.

The tiled window arrangement is ideal in aggregating information on a single screen if properly configured. A policy should therefore be made on how the windows should be arranged within the screen to allow ease of use. This policy should include the allocation of certain parts or regions of the screen for specific types of displays, e.g. graphics in the right hand part, trend displays in the left hand part, control group displays in the bottom part, etc. The DCS should be configured so that when a new window is opened, the type of display it contains dictates where the window should appear on the screen.

8. ALARM MANAGEMENT

8.1 INTRODUCTION

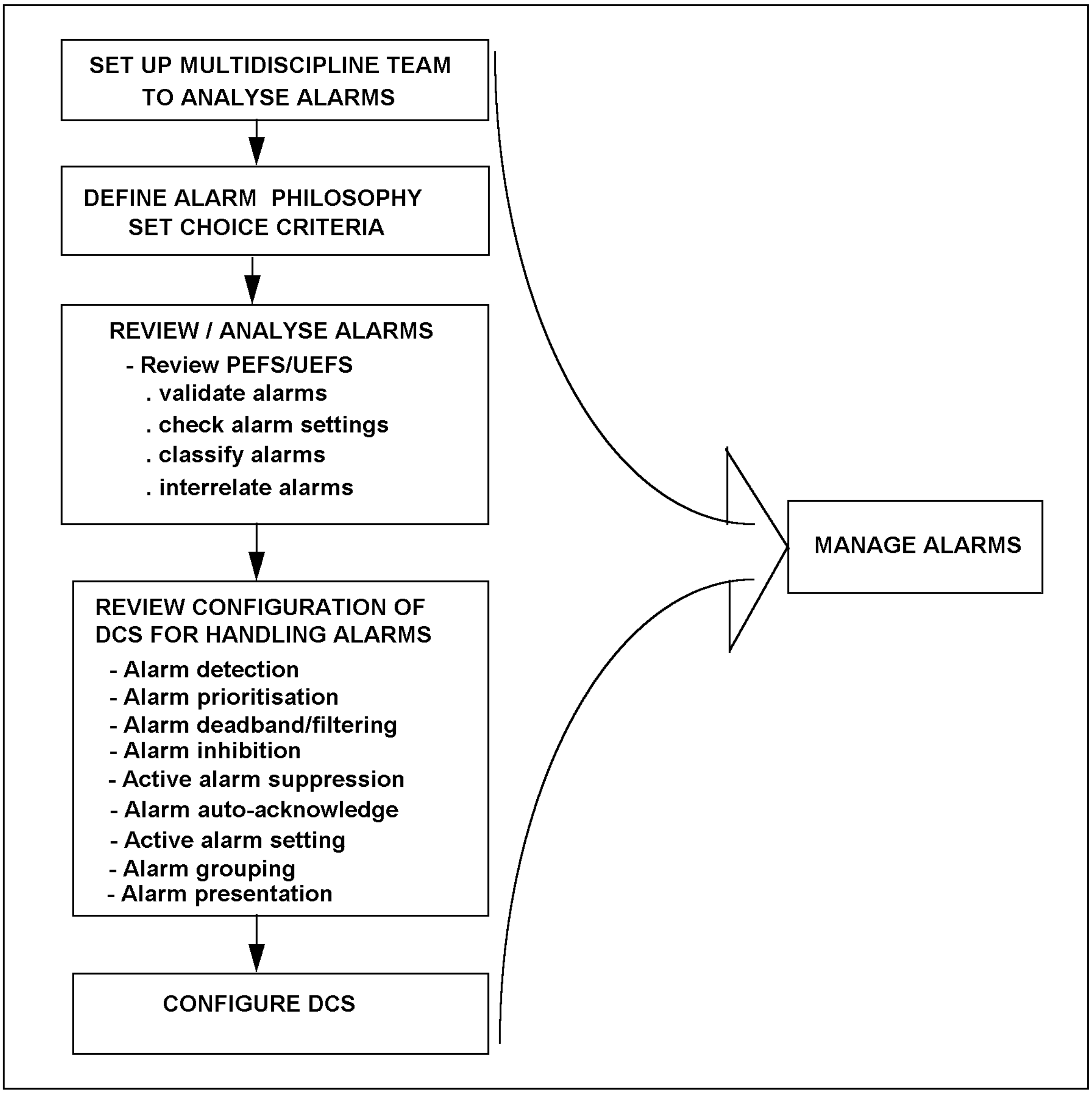
This section describes the methodology in designing alarm management. It assists in setting out an alarm philosophy whilst exploiting the default features and capabilities of the DCS with regards to alarm management.

Advanced alarm management achieved through non-DCS features is not covered in this section.

8.2 APPROACH TO ALARM HANDLING

The flowchart below describes the general approach to design alarm handling. Details of the individual boxes are discussed in the succeeding sections.

FIGURE 6 Alarm handling



8.3 MULTIDISCIPLINE TEAM TO ANALYSE ALARMS

The tasks of the multidiscipline team are:

- Document the alarm philosophy (i.e. purpose and use of alarms and rules for prioritising and presenting alarms);
- Analyse every alarm, establish any grouping or masking to be applied and classify according to the rules defined;
- Implement applicable alarm management features of the DCS.

The multidiscipline team should consist of staff from operations, technology, process safety, instrument engineers etc. as follows:

- Panel Operators with experience (minimum 2 operators from different shifts) to identify the purpose of the alarm and the action to be taken;
- Process Engineer to identify unit response to alarm condition and best reaction for the operator to the situation (e.g. column overhead pressure might be more sensitive to preheat changes than overhead temperature);
- Instrument Engineer to identify potential configuration changes to the system and interpret current configuration. The Instrument Engineer should also act as the Facilitator/Recorder asking questions to the group about each alarm and keep the group moving.

Other resources may be necessary to provide input to specific alarms. These include specialists in rotating equipment, metallurgy and electrical systems.

NOTE: Consideration should be given to combining the alarm analysis and prioritisation exercise with the IPF Classification as the team members are essentially the same. See DEP 32.80.10.10-Gen.

8.4 ALARM PHILOSOPHY

An alarm philosophy provides guidance in establishing the purpose, use and need of alarms, with rules for prioritising and presenting alarms. Below are some points which form the basis of an alarm philosophy.

Alarms are for the purpose of minimising the potential for deviations (abnormal situation) in plant equipment and processes to develop into significant hazards or disturbances. They are used to alert the operator so that he can react in a timely manner by performing the proper corrective actions, and also to provide information whether the deviation is corrected or not (i.e. a trip has occurred). Changes in process variables, transition in operating mode, open/closed position of MOV, etc., which are a normal part of plant operation and do not require action from the operator should not be presented as alarms.

Priorities of alarms are to prompt the operator of the extent of the deviation and are meant to assist him in cases of multiple alarm situations. The priority levels (high, medium, low, recording, no priority) should set distinct criteria for each of the levels in terms of:

- Consequences to the plant systems and processes in case the alarm is not responded to in time (i.e. IPF initiation, operational upsets, off-spec product).
- How quickly the operator must react (immediately, can wait 5 minutes or more, etc.).
- Available functionality in the DCS in terms of alarm processing relative to priority.

Alarms shall be presented to the operator in such a way that they are easy to locate and priorities are readily and distinctly recognised. Using the DCS features, a consistent and unambiguous approach for visualising and locating alarms (e.g. overview displays, function key LEDs, alarm lists etc.) shall be defined and configuration standards set for all parameters associated with an alarm (its deadband, animation/colour before and after operator acknowledgement, filter setting on inputs, hooter tone etc.).

The philosophy discriminates between alarms and messages. The latter comprise textual notes to guide the operator. They often manifest themselves by mechanisms within the DCS that are similar to those for alarms. However, they are intended to provide status information and do not imply an urgent situation that requires action.

Certain plant states (shutdown, start-up etc.) can generate alarms which are temporarily not important, whereas certain alarms when activated result in the generation of consequential alarms. The alarm philosophy defines how and in which situations alarm grouping and masking techniques can be implemented to prevent the generation of consequential alarms.

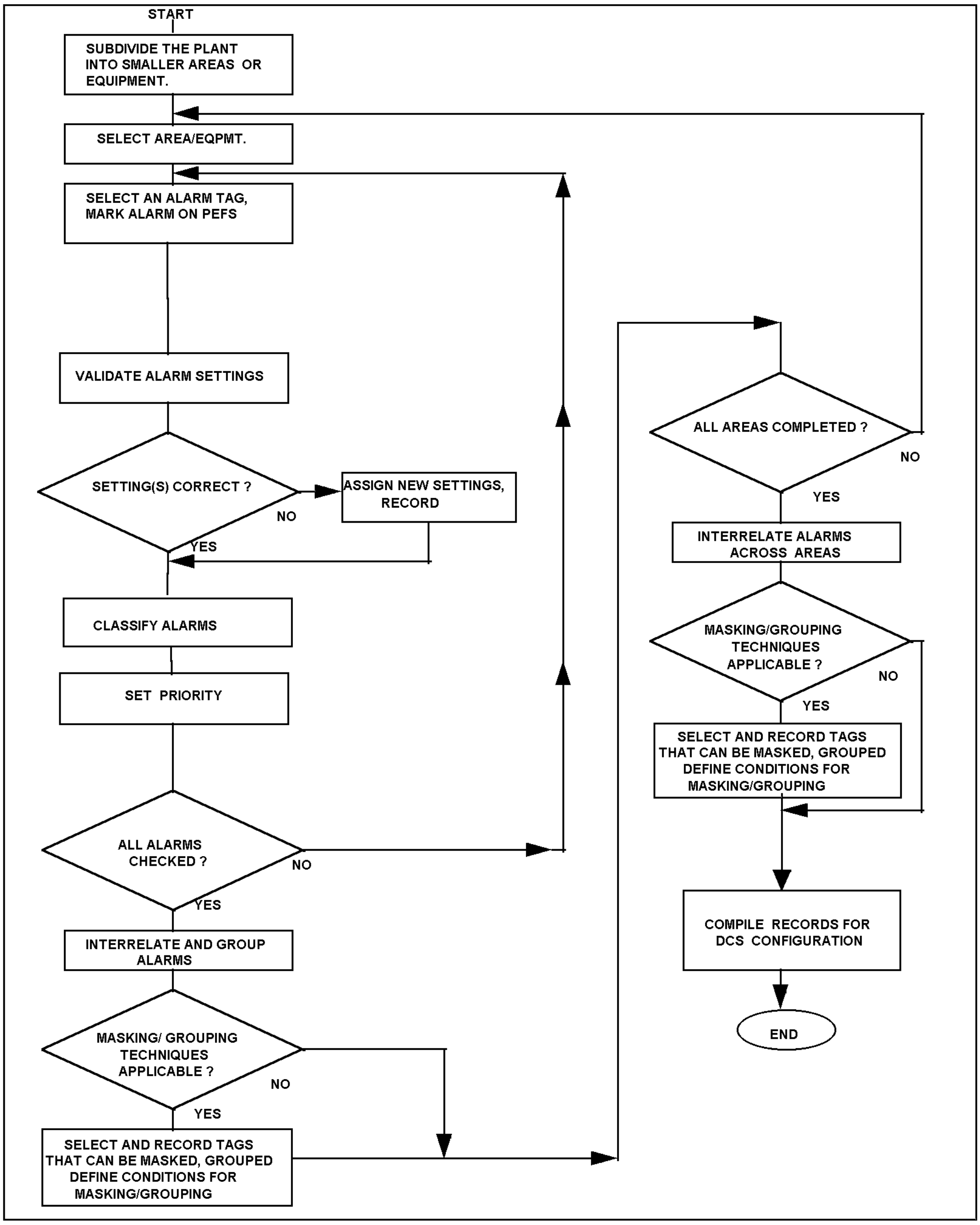
8.5 ALARM ANALYSIS

All alarms should be analysed for the accuracy of their setting and their assigned priority level. Figure 7 provides a systematic approach on the analyses of alarm implementations.

The following materials/documents should be available during the analyses (review) of process alarms:

- List of alarms and their set points (alarm & trip database);
- Several sets of PEFS;
- Control and IPF narratives;
- IPF classification results (if available). See DEP 32.80.10.10-Gen.

FIGURE 7 Alarm analysis



8.5.1 Alarm settings

Alarm settings shall be such that operator has time to react and shall have a deadband to prevent oscillation. In some cases it may be worth considering to modify the alarm set point or priority, based on the modes of operation (normal, regeneration, start up) which shall be defined for process units and equipment. See (7.6.9.).

8.5.2 Classification of alarms

Each alarm should be classified in terms of both urgency of action required and the consequences of not responding to the alarm. Criteria for both should be defined in order to assign the priority for an alarm. Typical criteria are given below.

8.5.2.1 Urgency of action required

Urgency of action can be classified as:

- Operator action within 1 minute to minimise further disturbance.
- Operator action within 5 minutes to minimise the disturbance.
- Information of an abnormal process condition that requires operator attention but does not fall in the above categories.
- Information required for the sequence of events and analysis that will not assist the operator in correcting a disturbance.

Care should be taken in the classification of alarms as missing an alarm/information could lead to:

- Equipment trip (furnace, compressor)
- Process disturbances with possible production of off spec. products
- Environmental impact

8.5.2.2 Consequence

If the operator does not respond to an alarm in time, the consequences can be classified as:

Major:

- trip of major equipment;
- disturbance will cause off-spec. products.

Minor:

- disturbance to process not leading to off spec. products;
- deviation from targets.

The alarm which indicates to the operator that a trip has occurred shall also be classified with respect to any additional actions to be taken.

8.5.2.1 Priority setting

Priorities for the individual alarms should then be assigned based on the urgency of action required and the consequences. The number of priority levels should be consistent with the functionality available in the DCS.

High Priority should be assigned to an alarm if urgent action by the operator will prevent a major consequence.

If the action required shall be carried out in less than one minute, automation should be applied.

Medium Priority should be assigned to an alarm if action is required by the operator to prevent a minor consequence.

Tags with different alarm levels (e.g. H and L) shall be assessed independently.

A clear colour coding shall be assigned to each priority, e.g. red is high priority, yellow is medium priority.

Low Priority should be assigned for abnormal process condition that require operator attention but do not require action within five minutes.

Alarm Classification Sheet

A classification sheet with the format given below, indicating the alarm function, consequences of missing or not responding to the alarm, mode of operation and urgency of corrective action should be used for each alarm. The priority should be entered last after assessing the urgency and consequence criteria.

Typical examples of filled in alarm classification sheets are as follows:

Tag No.: 03LA 001 Alarm: High

Alarm function *Alert operator is needed to prevent the following condition*	**Consequence**	**Urgency**	**Mode** *Steady state Start up, Regen, etc.*	**Priority**	**Comments** *Operator action*
Shutdown	Major	1 min	SS	High	K301 pretrip open LRC x
Process upset					
Efficiency					
Environment					

Tag No.: 01TA014 Alarm: High

Alarm function *Alert operator is needed to prevent the following condition*	**Consequence**	**Urgency**	**Mode** *Steady state Start up, Regen, etc.*	**Priority**	**Comments** *Operator action*
Shutdown	Major	5 min	Regen	High	Reactor pretrip open quench
Process upset					
Efficiency					
Environment					

Tag No.: 02FCA001 Alarm: Low

Alarm function *Alert operator is needed to prevent the following condition*	**Consequence**	**Urgency**	**Mode** *Steady state Start up, Regen, etc.*	**Priority**	**Comments** *Operator action*
Shutdown					
Process upset	Minor	5 min	SS	Medium	Small disturbance increase SP
Efficiency					
Environment					

8.6 ALARM CONFIGURATION

Below are features of the DCS that relate to alarm management which can be applied to individual instruments or groups of instruments. Prior to any configuration work in the DCS an alarm strategy should be developed (e.g. grouping or masking techniques) which takes into consideration the applicability of these features to the various plant operating conditions.

8.6.1 Alarm detection

Alarm detection for instruments is performed by the control stations. The control station has functions for enabling and disabling alarm detection for each instrument which can be configured in the control station builder. These are generally the out of range triggered high/low, high/high, low/low, deviation alarms, velocity alarms, output high/low, etc.

A common oversight made when configuring the DCS is to leave the default alarm detection function enabled for continuous control blocks. This creates a problem during operations as each block can generate out of range alarms when threshold values are reached even though this may not require any action.

Only those tags which are indicated to have alarm functions on the alarm and trip listing (derived from the PEFS) should be configured with the alarm detection function in the enabled mode. Similarly, the alarm should be limited only for the particular alarm function required. E.g. if HH is required, only HH should be configured and the other default alarms H/L, V/H, etc. should be disabled.

8.6.2 Alarm priority

The DCS has default alarm priority levels which can be assigned to individual instruments. These typically range from high priority, medium priority, low priority, recording alarm to no alarm. The way the DCS handles an alarm in terms of display, audible signal and acknowledgement (locking, non-locking, self-acknowledge) differs according to the priority level set.

The assignment of a priority level to an alarm should be consistent with the level defined in Section (7.5).

For most DCSs acknowledgement of alarm is allowed only on specific displays in which the instrument in alarm is contained, e.g. alarm summary, control group and graphics. It is a general rule in DCSs that alarms cannot be acknowledged without the operator seeing what he is acknowledging.

8.6.3 Alarm deadband and signal filtering

The alarm hysteresis deadband of individual instruments can be set via the control station builder. The alarm deadband should be carefully selected for each individual alarm.

- Too narrow a deadband will not suppress oscillating alarms;
- Too wide a deadband keeps the alarm present for too long.

The deadband should be set according to the type of measurement and its application. For measurements with a slow response time (e.g. temperature, viscosity) a narrow deadband should be set, whereas for measurements with a fast response time a wider deadband should be set. The DCSs usually have default deadbands (at around 1% of the range value) and this should be verified or readjusted on a case-by-case basis.

Inputs to the DCS can have a filter assigned. This generally averages the input and thereby smooths it. Careful choice of the filter parameters setting will ease alarm difficulties. If the input is for a PID block, extra care should be taken because the control dynamics are also affected.

8.6.4 Alarm suppression

Alarms of individual instruments can be suppressed (masked) or un-suppressed (demasked) using the alarm disable function, which is done at the DCS-HMI. The alarm detection remains active but the current alarm status information is not passed onto the DCS-HMI and no alarm message or audible tone is generated. Disabling of alarms shall only be done via a security access feature built in the DCS. Care shall be taken when disabling alarms because it can lead to loss of information displayed on the graphics.

8.6.5 Static alarm suppression

Groups of instruments can be set to "alarm disabled" by configuring a software switch which is toggled (from enabled to disabled state) by the operator. This is called static alarm suppression and is usually implemented via sequence blocks. Before static suppression can be performed, permissive states depending on process conditions should be configured within the sequence blocks. Only when these permissive states are satisfied shall static alarm suppression be allowed.

This feature is useful during certain plant states such as shutdown and maintenance or for certain modes of operations when process units or parts thereof are out of operation, e.g. spare equipment not in use. Large numbers of temporary alarms associated with the non-operational equipment are generated, which leads to confusion. They should therefore be disabled.

8.6.6 Active alarm suppression

Alarms of individual instruments or groups of instruments can be automatically disabled depending on a set of predefined process conditions or events. The disabling of these blocks can be configured via a combination of calculation blocks and sequence blocks.

For example, a furnace trip resulting from a number of process signals will have a number of consequential alarms. In the case of Flame Failure the operator would be alerted by the flame failure trip alarm, a low fuel pressure alarm, a low fuel trip alarm, low furnace outlet temperature alarm, air fuel ratio alarm etc. The subsequent alarm conditions can be automatically suppressed once the flame failure has been sensed by the alarm management sequence block. Care shall be taken in the development of these sequence blocks to check that the expected alarm conditions are sensed by the system. If a low fuel trip alarm is not sensed, after the flame failure, an independent high priority alarm shall be generated to alert the operator.

Active alarm suppression shall be configured for a period following the initial trip alarm within the sequence block. The operator shall be able to de-activate (demask) active alarm suppression via the DCS-HMI. To prevent alarm flooding, implementation of automatic acknowledgement should be considered as a part of the active alarm suppression routine before the suppression is lifted.

8.6.7 Alarm auto-acknowledge

Alarms of individual instruments or groups of instruments can be automatically acknowledged via a combination of calculation blocks or sequence blocks, depending on a set of predefined conditions or events (permissive) configured within these blocks. The alarm status of instruments will appear on the graphics and alarm list of the DCS-HMI as acknowledged alarms. No audible sound will be generated.

This feature is useful when it is desirable to automatically acknowledge subsequent expected alarms after a primary alarm has been activated.

Automatic acknowledgement of alarms shall be configured for a limited period of time after the initial trip. The duration can be configured in the sequence blocks. The operator shall be able to deactivate alarm auto-acknowledge via the DCS-HMI.

8.6.8 Alarm grouping/ representative alarming

The DCS has a standard function block which can be configured as a single alarm representing a pre-defined group of alarms (e.g. common alarm) and which can inhibit the individual alarms.

When an alarm occurs within an instrument group, the associated alarm block generates a common alarm. Only after all attached instruments have returned to normal will the representative alarm go back to its normal status. The representative alarm block will not be affected by the disable status of the attached instruments. The alarming of the representative alarm block can also be selected in such a way that it will only generate the first failure alarm for a predetermined time or will alarm whenever an alarm occurs on the individual instruments attached to it.

This technique is useful when it is desirable to group alarms on a per equipment or a per unit basis so as not to confuse the operator with alarm details of individual instrument. It can be used in conjunction with graphic displays in both the overview and unit levels. It is effective in preventing alarm avalanches if priorities are applied, e.g. the representative alarm block is configured with high priority while the attached instruments are configured with recording priority.

8.6.9 Active alarm limit setting

The setting of alarm limits can be dynamically changed to predefined values via the combination of calculation blocks and sequence blocks based on a set of conditions configured on this blocks.

This feature is useful when there is a need to change alarm limits automatically, e.g. start-up sequences, feed switches, various product runs etc., thus necessitating higher or lower alarm limits.

8.6.10 Alarm presentation - graphic configuration

Alarm information is a subset of process information and should be presented to the operator in such a way that it is easy to locate exactly where the problem is so that immediate corrective action can be taken. All alarms shall have a descriptor which is readily understandable.

In designing the graphic display users shall decide how to present the various features of an alarm (red flashing for an unacknowledged alarm, red steady for an acknowledged alarm and so on for all situations). Modifiers such as colour change, blinking, hidden or inverse patterns and pattern replacement can all be combined for an effective, user-friendly presentation of alarms to the operator. The presentation of alarms within the HMI should always depict the status of the alarm condition, e.g. acknowledged, reset, etc.

In order not to divert the operator's attention, representative alarming on a per unit or per equipment basis can be configured in the graphics.

It is advantageous to create dedicated graphic pages illustrating static alarm suppression and dynamic alarm suppression, showing the list of alarms which can be suppressed or auto-acknowledged, trips which will auto-acknowledge or cut out other alarms.

8.6.11 Audible alarm

The DCS HMI can be configured to emit different audible tones corresponding to alarm priority levels for process alarms. In order for process alarms to be easily distinguished, no more than two different auditory tones should be used, as follows:

- a high pitched continous tone for high priority alarms;
- an intermittent tone for medium and low priority alarms.

The tone volume should be adjustable, with the minimum setting above the background noise level in the control room.

NOTES: 1. The DCS usually has a default tone for system alarm which is distinct from those configurable for process alarms.

2. The audible alarm generated by the hardwired display panel of the FGS should be distinguisable from the process alarm tones configured in the DCS.

8.6.12 Alarm handling techniques for plant operating conditions

Applicable alarm handling techniques for the different plant operating conditions are given in the table below.

Operating Condition	Alarm Handling Techniques

Steady State	Alarm Grouping Active Alarm Suppression / Auto acknowledge
Plant Upset	Alarm Grouping Active Alarm Suppression / Auto acknowledge
Transients	Active Alarm Setting Active Alarm Suppression/ Auto acknowledge Alarm Grouping
Plant Stopped (shutdown)	Static Alarm Suppression

9. CONSOLE DESIGN

9.1 OPERATOR INTERFACE

9.1.1 Layout of consoles in the control room

Future expansion should be taken into account when determining the console layout.

The setup of the consoles in the control room should conform to the process path and to local preferences, e.g. from left to right or from right to left.

The consoles should be functionally grouped according to each section in the process.

Setting up consoles next to each other in either a U or C shape depends on the number of operators which will control the console and on the functional link between the processes.

Attention shall be given to coordinating the process flow with the communication flow between the operators and consoles. The link analysis should be utilised to determine the optimum layout of the consoles. For the different console layouts together with their advantages and disadvantages see ISO/DIS 11064-3, ISO/DIS 9241-3 and ISO/DIS 9241-5.

9.1.2 HMI console types

Two types of HMI configuration are available for the DCS: the free-standing console type and the desk top/workstation type.

For the free-standing type, the VDU, keyboard and pointing device are fixed on the chassis of the console cabinets. It offers less HMI arrangement flexibility to suit the needs of the users.

For the desk top type the VDU, keyboard and pointing device are supplied as separate items and are placed on tables to form a console. The desk top type is more adaptable than the free standing type with regards to the arrangement of the keyboard and the VDU (tilt and swivel). The arrangement of the furniture can be customised to the requirements of the users (e.g. two tier or single tier VDU holders). The furniture shall have sufficient writing space. Desk top DCS-HMIs are less expensive than the free standing console types and allow easier maintenance since components can be easily replaced without having to open console cabinets. For both console types, care should be taken in setting up the workplace with respect to general anthropometric requirements.

NOTE: General anthropometric requirements are as follows:

Workplace dimensions in the console should accommodate 90-95% of the user population.

If the furniture is non-adjustable, the critical body dimensions of the smaller individuals (i.e. 5th percentile) should be used to establish reach distances and the critical body dimensions of the larger individuals (i.e. 95th percentile) should be used to establish clearance dimensions.

Adjustable workplaces should be such that they accommodate at least a range from the 5th percentile to the 95th percentile of the (critical body dimensions of the) user population. Adjustment devices shall be easy to use.

Controls should be within reach of the operator working with an erect posture and from the expected work locations at the console.

Controls should not be positioned above the shoulder height of the 5th percentile.

Input devices (e.g. keyboard) and other devices (e.g. telephone) should be freely moveable over the work surface towards and away from the displays.

9.1.3 Number of HMI consoles

A set of continuous process units having between 200 and 400 control valves should have:

- A main console consisting of four VDUs, two keyboards, two pointing devices, a communication panel, a hardwired switch panel and a CCTV panel.
- A secondary console consisting of two VDUs, a keyboard and a pointing device. This console is required during start-up, during certain manoeuvres or during severely disturbed states in one or more units. It may be shared with another set of process

units.

- A supervisory console consisting of one VDU-keyboard-pointing device which may be placed in another room. Only one is needed for more sets of process units. This console serves several functions, as follows:
  - Used by the Technologist, Operations Management for checking plant operability.
  - Used by Engineering for modification of parameters, process control, diagnosis/condition monitoring and system maintenance.
  - Used as an Emergency Control Centre with fire and gas displays, etc.
  - In normal operation this console shall be configured as READ ONLY. The console can be switched to READ/WRITE with the proper authorisation.

For process units having higher numbers of control valves or clear splits in the panel operators' responsibilities, multiples of the above configuration should be considered. The availability of additional secondary (and/or supervisory) consoles should be assessed to minimise capital expenditure.

Possible operation of simple units and subunits remote from the centralised control facility may require additional consoles, e.g.

- Operation of water treatment under normal conditions.
- Product preparation for batch units.
- Data entry (e.g. position of manual valves) for product movements.

In general, during an upset situation an operator can control no more than three adjacent screens (e.g. 1 overview screen, 1 detail screen and 1 alarm display).

9.1.4 Hardwired switch panel

The Main Console HMI shall include a hardwired switch panel in which ESD switches, de-pressuring switches and MOS enable switches are individually labelled and arranged in a logical layout.

Operational Override Switches (OOSs) should be avoided by using automatic timer functions in the IPS.

MOS enable switches shall be in the DCS console (hardwired). The actual MOS itself shall be operated from the DCS screen.

Subsequent to identification of statutory needs, the overall approach should be to limit the switches on the hardwired switch panel to those described above.

For the implementation of the OOS and MOS, see DEP 32.80.10.10-Gen.

9.1.5 Communication panel

The Main Console HMI shall include a panel in which radio, telephone and intercom equipment can be installed. For the radio equipment consideration should be given to installing the voice-activated type or the foot-activated type of headset microphones in order to free up both hands of the Panel Operators and to reduce the overall noise level in the control room.

9.1.6 CCTV panel

Where CCTVs are used, the main console should include a panel in which the controls for the CCTV have been installed (e.g. wiper/wash switch, fan and tilt switch etc.). If space allows, the CCTV switches can be mounted in the communication panel.

The CCTV display may be incorporated as a window on the DCS screen or may be on a dedicated monitor. If a dedicated monitor is used a panel should be provided to mount this monitor within the main console. The monitor may also be mounted on a dedicated console or suspended from the ceiling.

9.1.7 FGS mimic panel

No hardwired Alarm Display Panels (ADPs) should be applied, except for the FGS mimic panel. The FGS mimic panel may be included in the main HMI console or mounted on a dedicated console.

9.1.8 Printers and video copy units

Alarm/event printers and video copy units should be mounted on table tops or dedicated furniture separate from the main HMI console. The number of printers should be minimised by using a shared configuration. Consideration should be given to PC-based alarm archiving to minimise the use of printer paper whilst maximising the ability to interrogate the collected data. These devices should be located away from the main console in order to limit the amount of noise and to avoid distracting the panel operators.

9.2 CONSOLE DIMENSIONS AND SHAPE

The dimensions of the operator console depends on the working population's physical dimensions for sitting height, reaching of controls, ability to see the screen without turning the body and accommodation and space for writing. The work surface height for reading and writing should accommodate both men’s and women’s dimensions. The absolute dimensions should be determined by consulting the anthropometric tables for the working population.

9.3 CONTROL ROOM LIGHTING CONSIDERATIONS

A lighting plan shall be developed based on the layout of the HMI consoles in the control room. The layout of the consoles in the control room shall be designed first and then the lighting shall be designed accordingly.

In places where document reading and report writing as well as VDU-related tasks are performed, the lighting specification should be carefully considered to take into account all tasks performed. The lighting specifications should cover the illumination levels required, the colour scheme, the positioning of lighting fixtures and the luminance of the surrounding surfaces (walls, ceilings, table tops, etc.). Consideration should be given to light intensity adjustment means, such as dimmers.

NOTE: Serious visual problems may easily arise as a result of working at VDUs; and this can cause a lack of visual comfort and reduced working performance. The problems can be reduced by a suitable distribution of luminance in the room and at the workplace. When working with VDU screens with light text on a dark background, the lighting levels in the room shall be kept relatively low. However, it shall not be so low that other visual tasks (reading printed or hand-written text) cannot be done. A suitable compromise is a general lighting level of 200-300 lux with table lighting available which can give a local light level of about 600 lux for reading difficult hand-written text or text in small print.

The control room lights should be positioned so that they do not cause reflections on the VDU screen. Fittings for the lights shall be placed either directly overhead or behind the screens, but not in front of the screens above the operator. Light fittings with a diffuser, mirror grids or reflective shading should also be considered. The light fittings should be positioned relative to the VDUs such that they are outside the Panel Operator’s field of vision.

For desk-top type consoles reflections can also be prevented by adjusting the tilt or swivel of the VDU.

Reflections on the keyboard should be avoided. This can be achieved by leaving a light-free area above the keyboard. The size of this area depends on the height of the light above the table.

NOTE: For existing sites the following strategies can be used to reduce glare in the control room, in the following order of preference:

1. Lighting design:
   a) selecting suitable light fixtures;
   b) changing the position of the lighting;
   c) shielding sources of glare, including large white (light) sources.
2. Location of the displays:
   a) swivelling and/ or tilting of the screen;
   b) adjusting the height;
   c) moving the screen.
3. Equipment design:

a) displaying dark information on a light background;
b) installing glare guarding devices;
c) adding hoods (but take care to avoid shadow areas on the upper half of the screen).

9.4 VDUs AND ASSOCIATED CRITERIA

For displaying graphic symbols, high resolution VDUs should be used which can reproduce at least 1024 x 1024 pixels or 1280 x 1024 pixels.

To avoid flicker, image refresh frequency should be 70 Hz for displays using dark symbols on light backgrounds.

Contrast and brightness should be adjustable.

10. HMI MAINTENANCE

10.1 INTEGRITY

Integrity of HMIs shall be managed as follows:

- For the DCS, authorised personnel shall be appointed to manage the HMI integrity.
- Principles and practices of system management shall be applied.
- HMI hardware modifications shall be carried out in accordance with plant change procedures.
- Software change procedure shall be instituted as described in (9.2.)
- HMI software configuration changes shall be carried out in accordance with the software change procedure.
- Modifications following a software change shall be immediately documented using the self-documentation features of the DCS.
- Temporary modifications, e.g. setting off an alarm shall be separately identified within the software change procedure.
- A focal point for the DCS manufacturer maintenance and support shall be appointed.
- System software revision and upgrades should be avoided. If a revision or upgrade is required, procedures specified by the Manufacturer shall be followed.
- All revisions shall be documented.
- Back-up of system files shall be made whenever changes to the system are implemented following a software change.
- A procedure on how to maintain the back-up media (e.g. number of copies, last date of back-up and storage location) shall be developed.
- System documentation shall be available.
- Security and access rights shall be documented.
- Software copies of graphics shall be available.

10.2 SOFTWARE CHANGE PROCEDURE

Software change refers to the modification of the existing software configuration resident in the DCS. This may involve changing the functionality of control loops, changing parameter settings, deletion or addition of instruments, changing security and access level, modification of graphics, etc. In order to ensure that a proposed software change will not compromise the integrity of the DCS as well as the process plant or equipment being served by the DCS, a procedure shall be instituted to establish a consistent methodology which will involve parties concerned to review/evaluate a proposed software change before implementing it in the DCS.

10.3 SYSTEM SECURITY AND ACCESS

Security features shall be configured in the DCS to minimise occurrence of operational mistakes and/or unauthorised change in settings. These include restrictions in the range of operations and monitoring (display) functions. During the configuration of the DCS, security levels covering parameter changes and access to the HMI should be assigned for individual instruments or groups of instruments. (e.g. Operator level, Supervisor level, Engineering level). Modifications in standard and graphic displays should only be allowed in the Engineering level. Access to security levels shall be controlled via pass codes or key locks. Procedures shall be instituted covering authorised holders of keys or pass codes.

10.4 HARDWARE MAINTENANCE

Time and condition based maintenance schedules such for as de-gaussing of screens, CRT replacement etc., should be followed to ensure the quality of displays in the HMI.

11. HMI IMPLEMENTATION WITHIN A PROJECT

Figures 8 and 9 show the activities and stages involved in the implementation of HMI within a project, as well as areas where this DEP shall be applied.

FIGURE 8 HMI implementation within a project

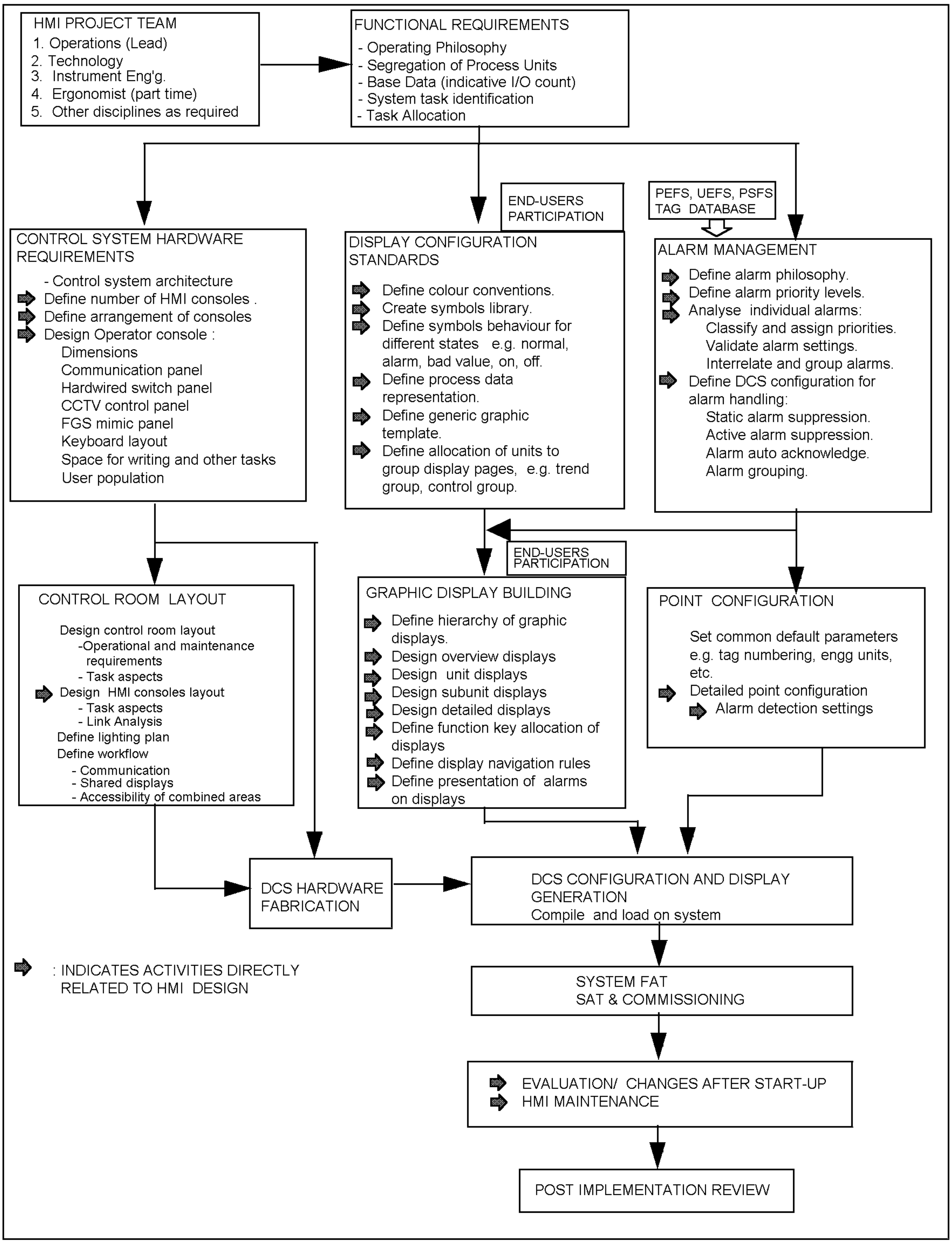
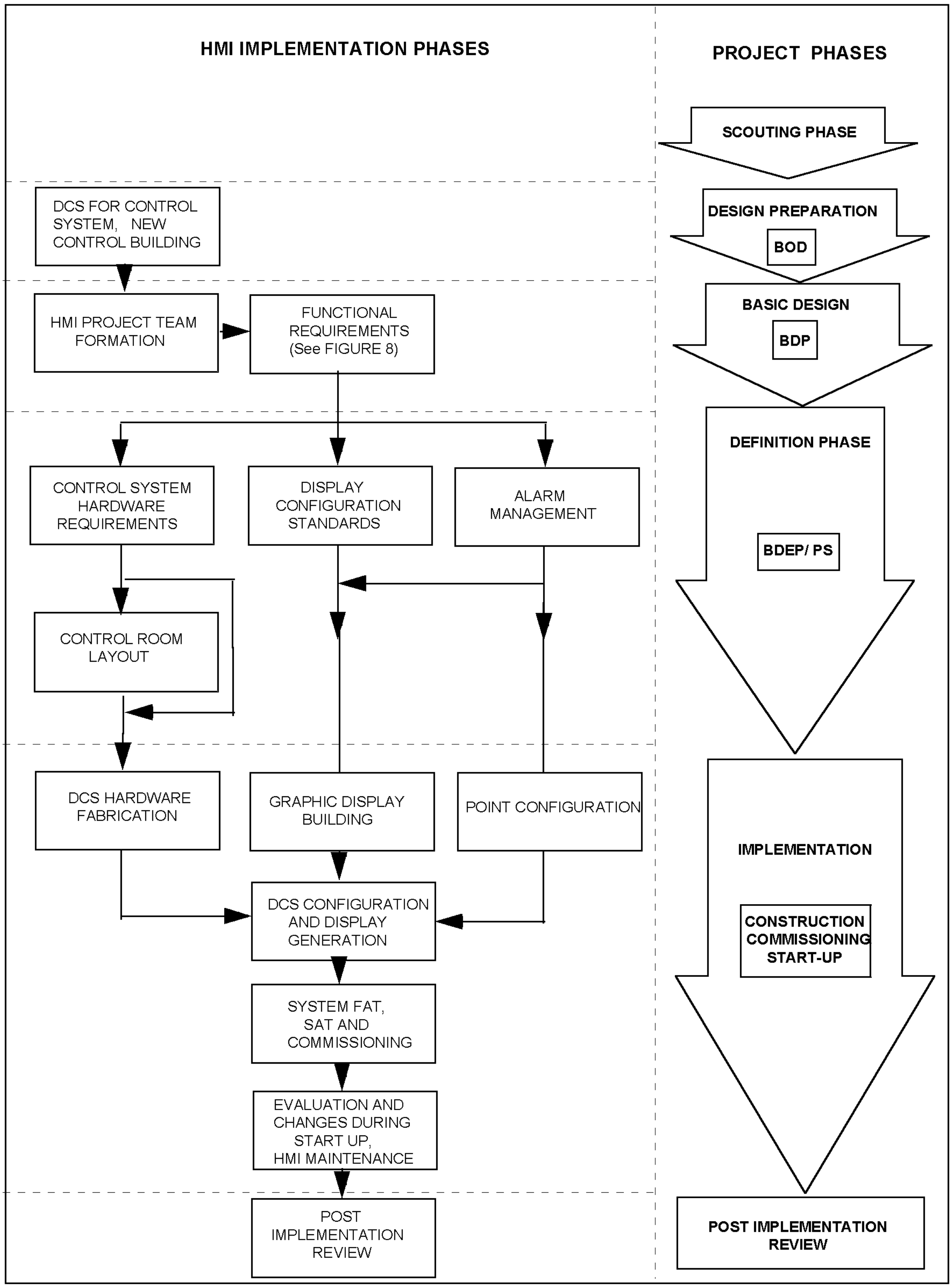


FIGURE 9 HMI implementation phases within a project



12. REFERENCES

In this DEP reference is made to the following publications:

NOTE: Unless specifically designated by date, the latest edition of each publication shall be used, together with any amendments/supplements/revisions thereto.

SHELL STANDARDS

Index to DEP publications and standard specifications	DEP 00.00.05.05-Gen.
Fire, gas and smoke detection systems	DEP 32.30.20.11-Gen.
Classification and implementation of instrumented protective functions	DEP 32.80.10.10-Gen.
Reinforced control buildings/field auxiliary rooms	DEP 34.17.10.30-Gen

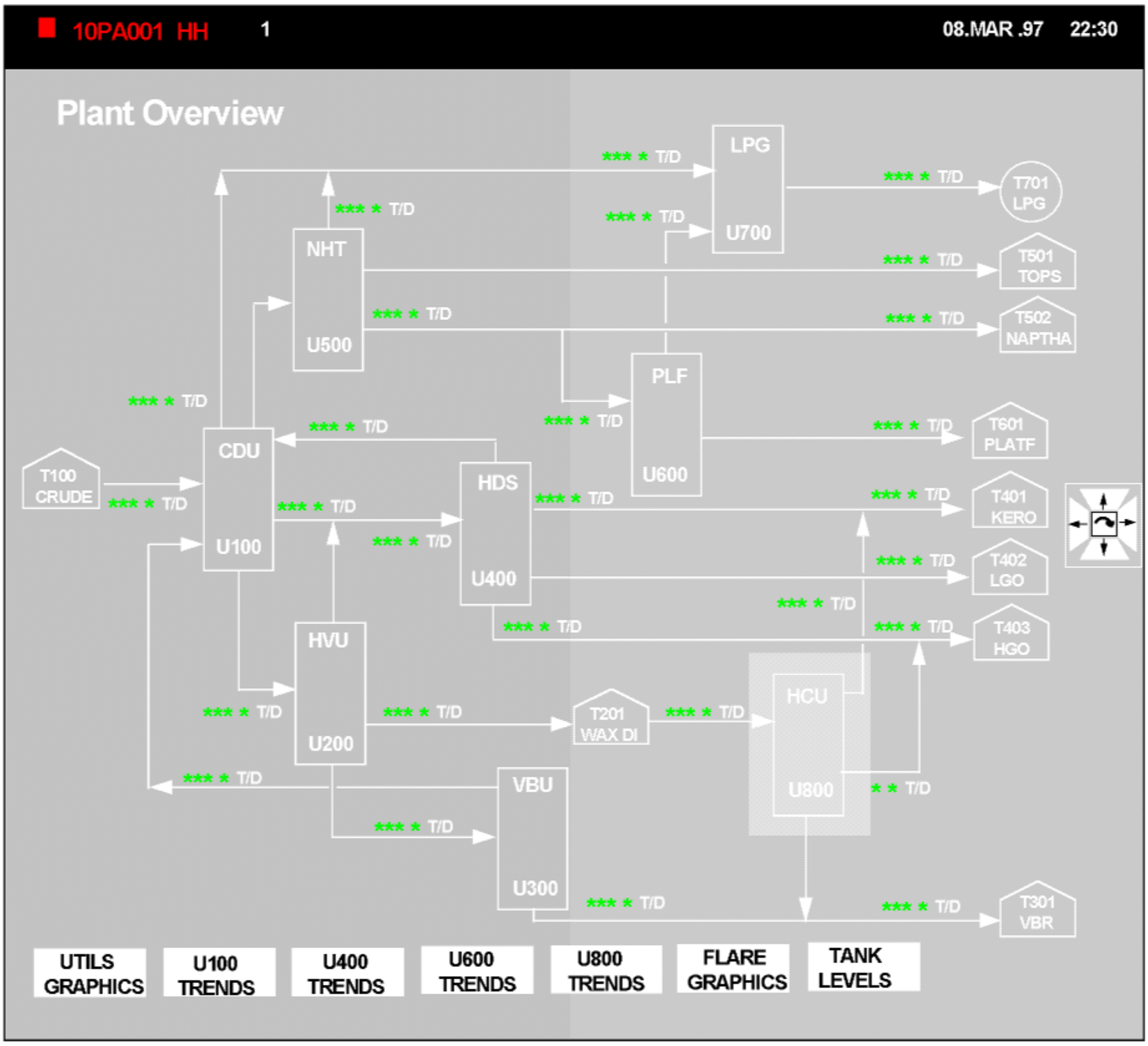
INTERNATIONAL STANDARDS

Ergonomic design of control centres:	
Part 3: Control room layout	ISO/DIS 11064-3
Ergonomic requirements for office work with visual display terminals (VDTs):	
Part 3: Visual display requirements	ISO/DIS 9241-3
Part 5: Workstation layout and postural requirements	ISO/DIS 9241-5

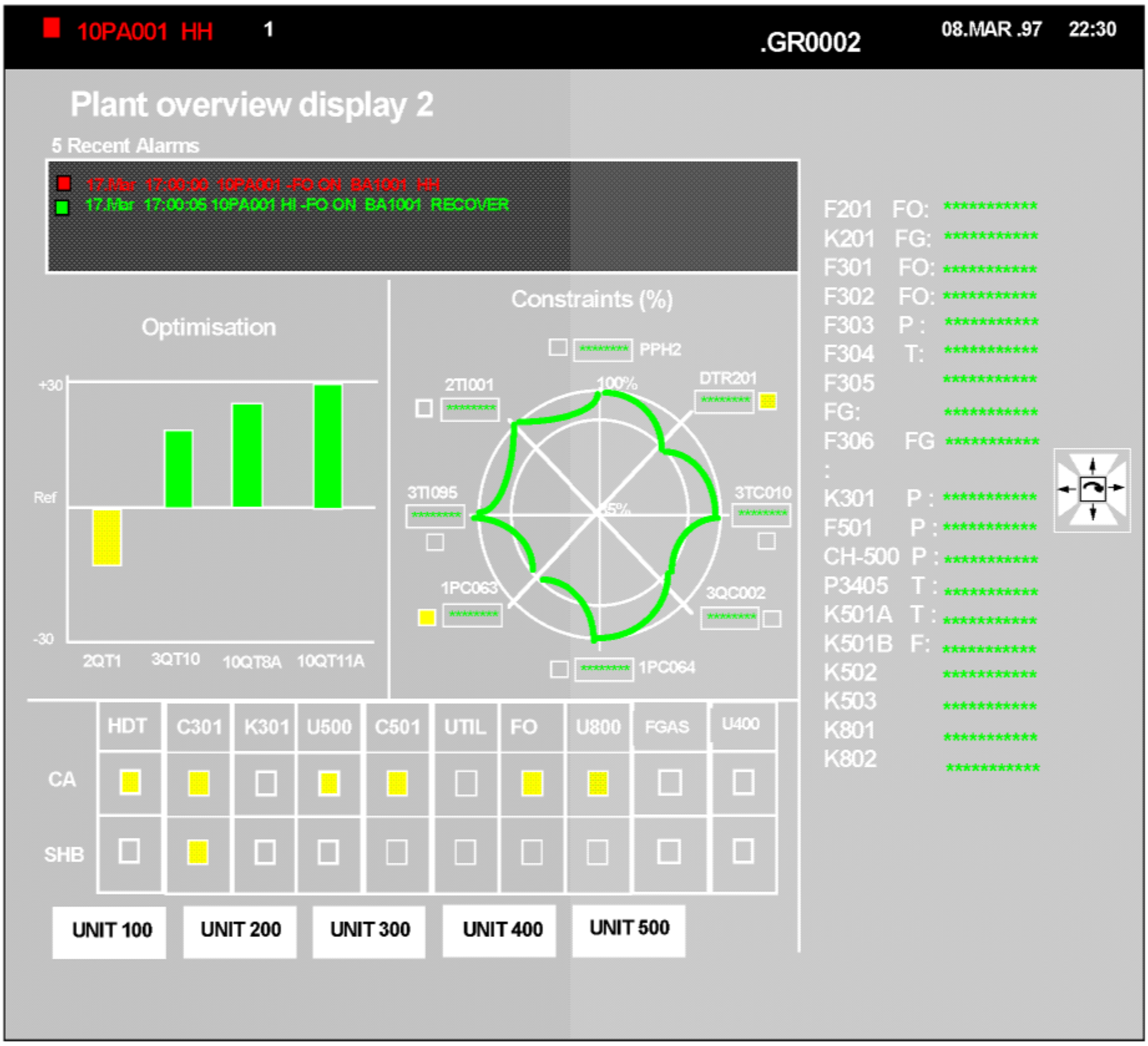
Issued by:
International Organisation for Standardization
1, Rue de Varembé
CH-1211 Geneva 20
Switzerland.

Copies can also be obtained from national standards organizations

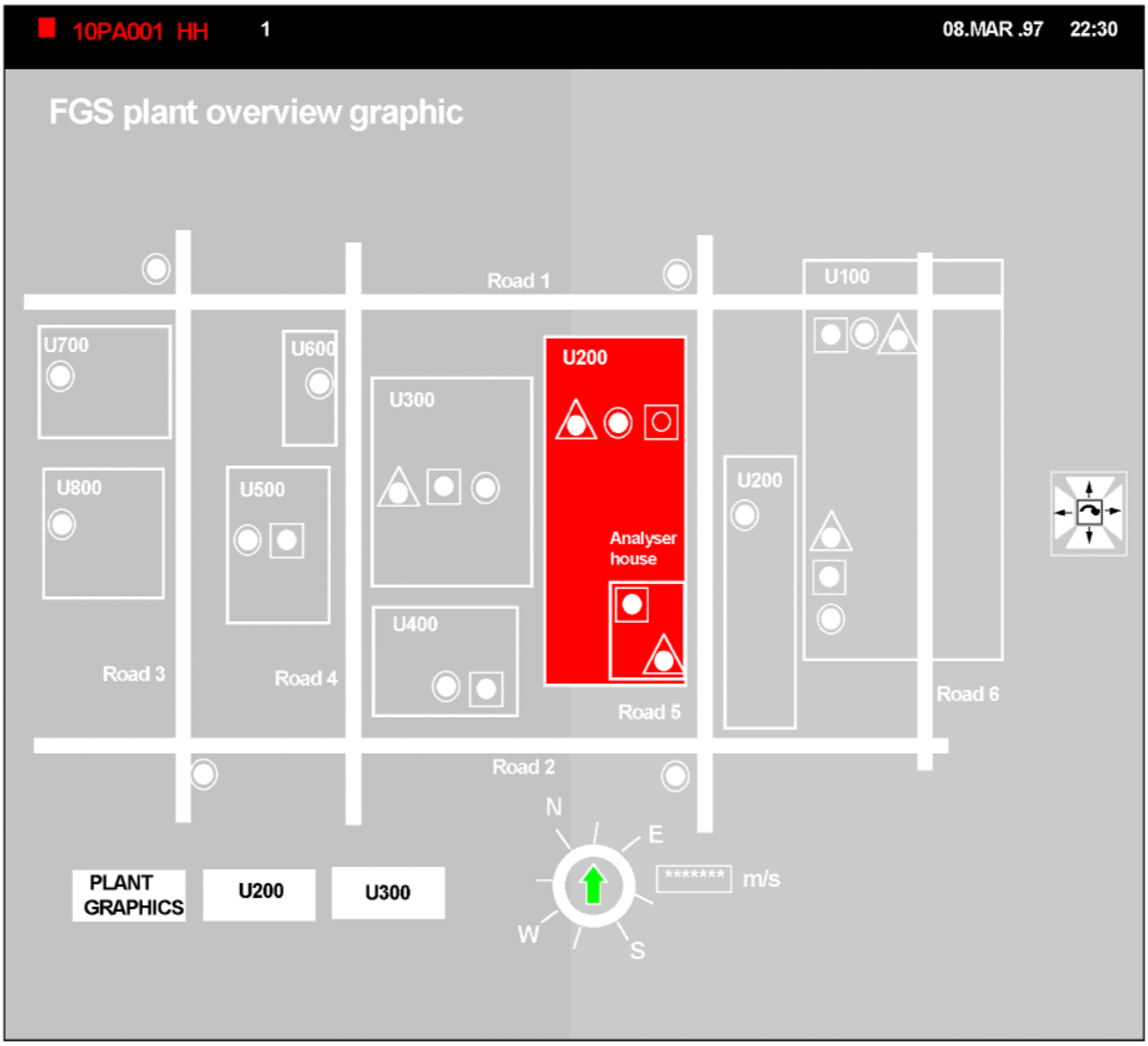
APPENDIX 1 TYPICAL PLANT OVERVIEW DISPLAY (SCHEMATIC REPRESENTATION)



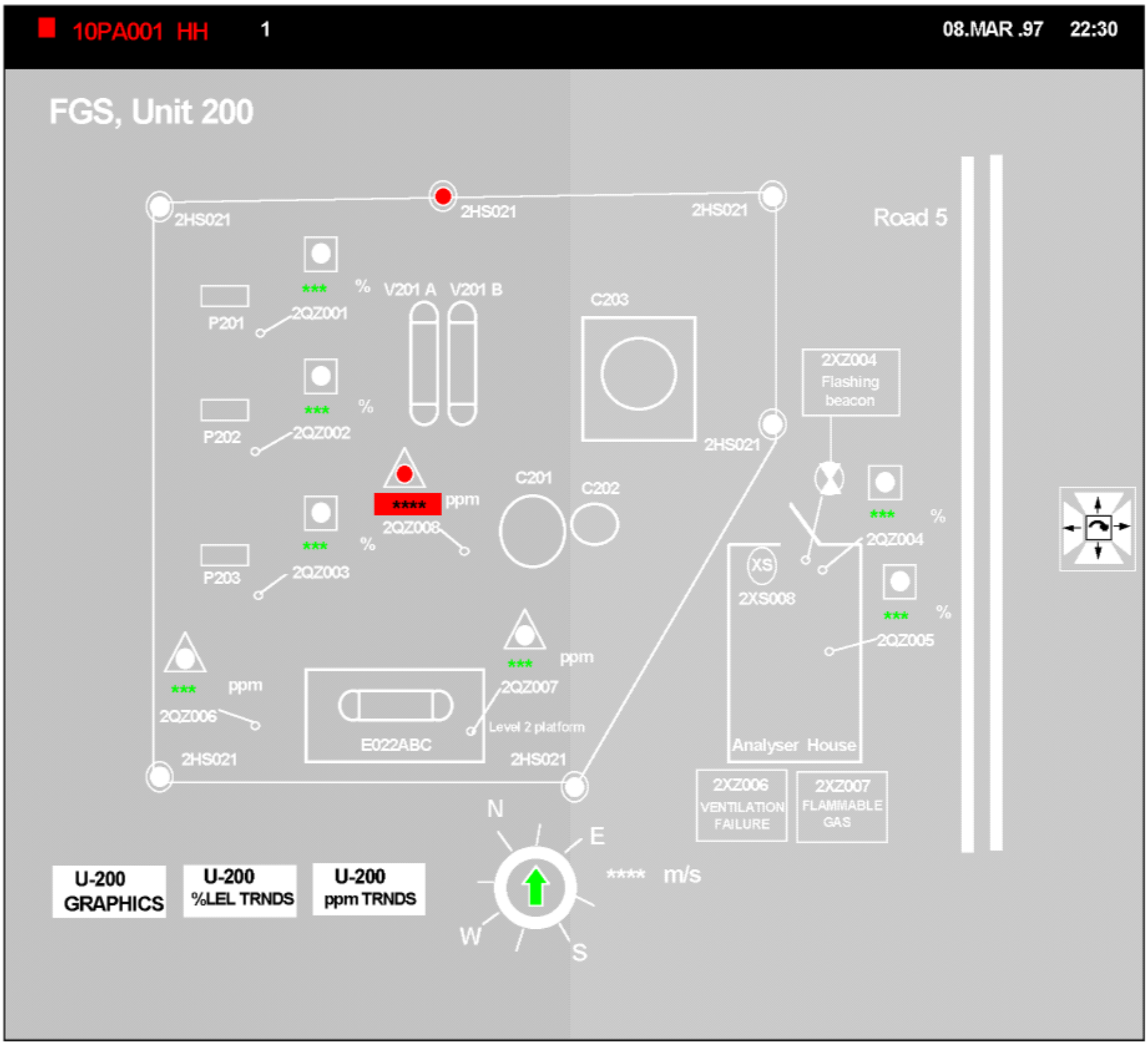
APPENDIX 2 TYPICAL PLANT OVERVIEW DISPLAY (GRAPHS, DIAGRAMS)



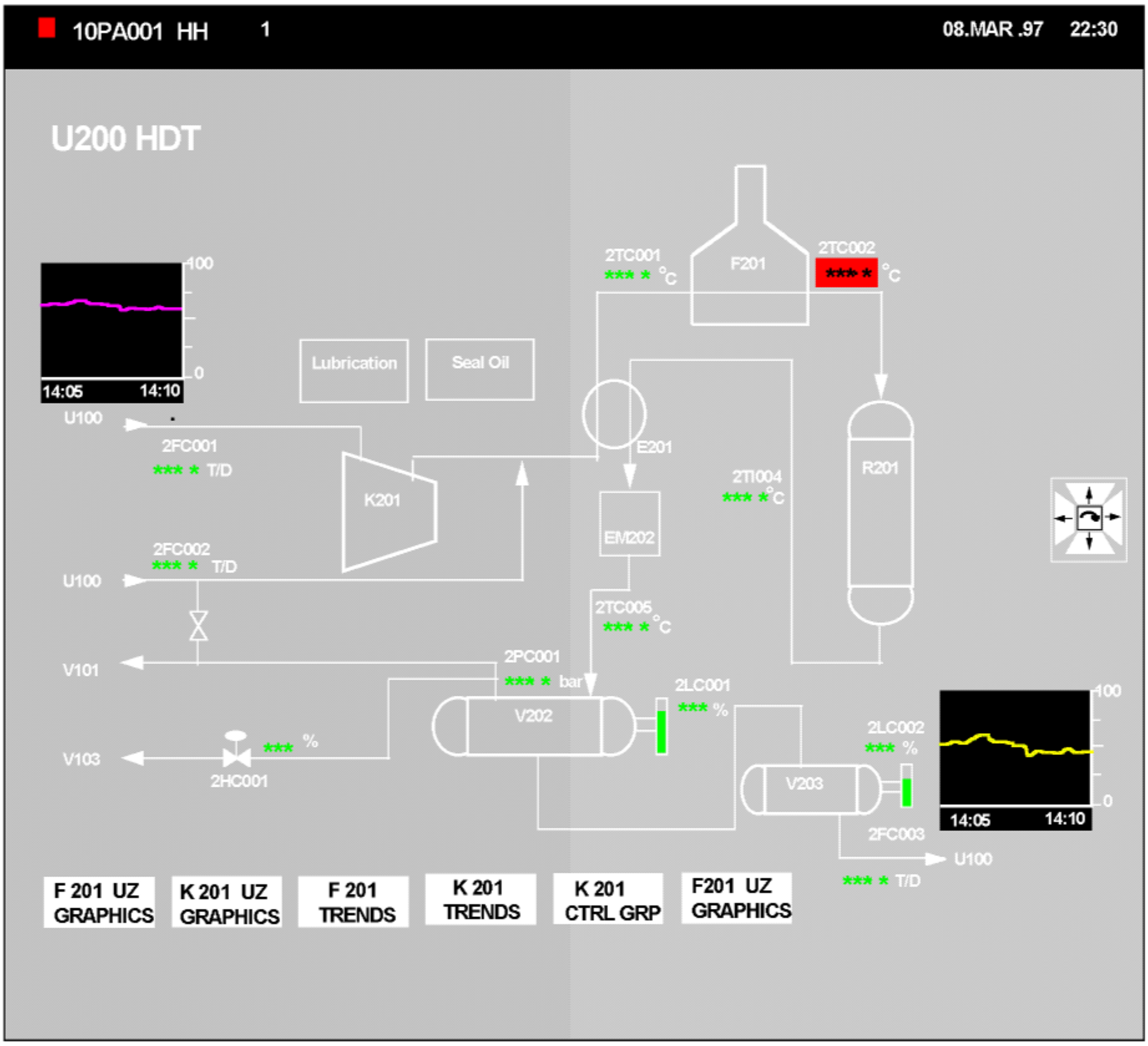
APPENDIX 3 TYPICAL FGS AREA OVERVIEW DISPLAY



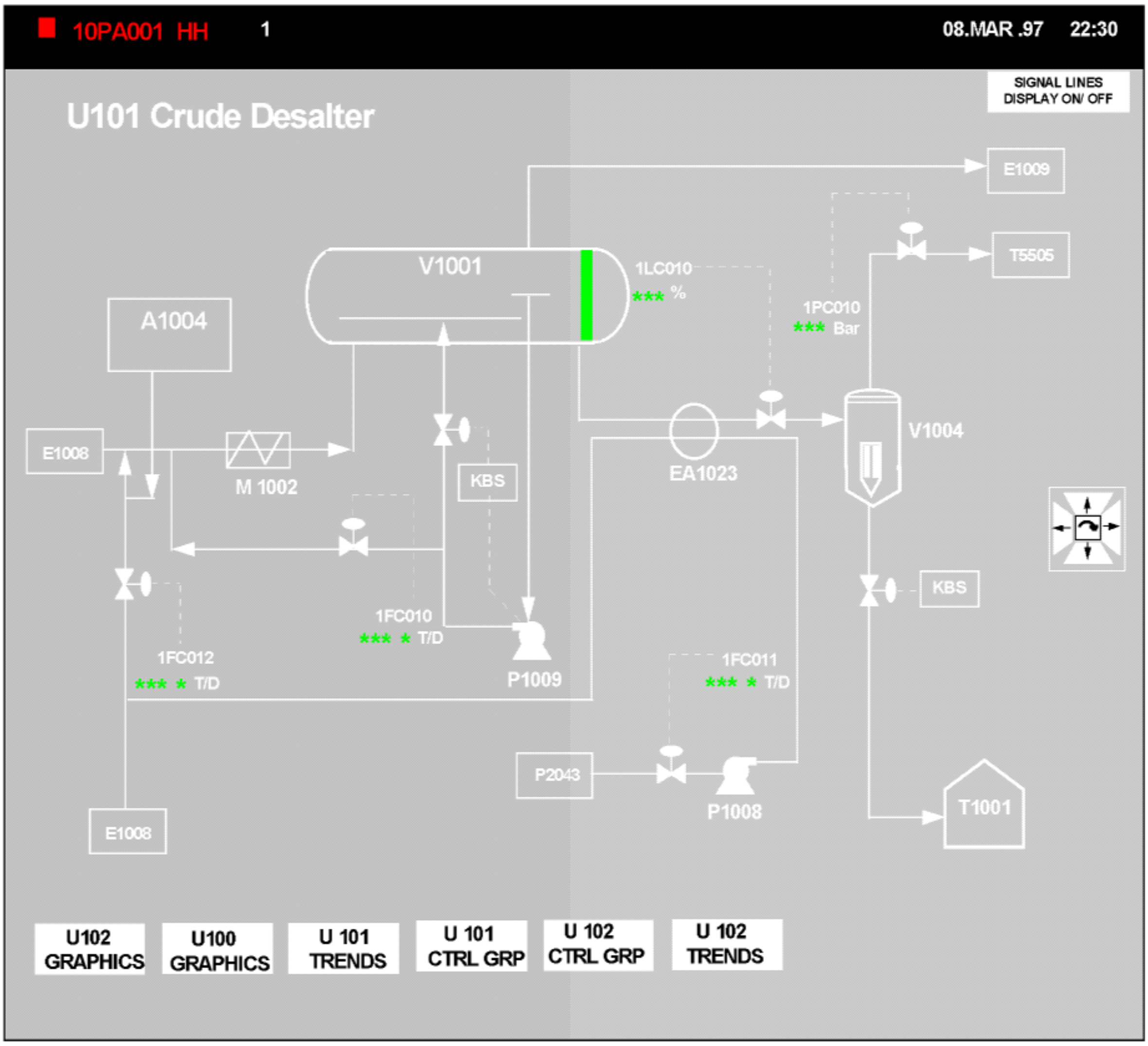
APPENDIX 4 TYPICAL FGS UNIT DETAILED DISPLAY



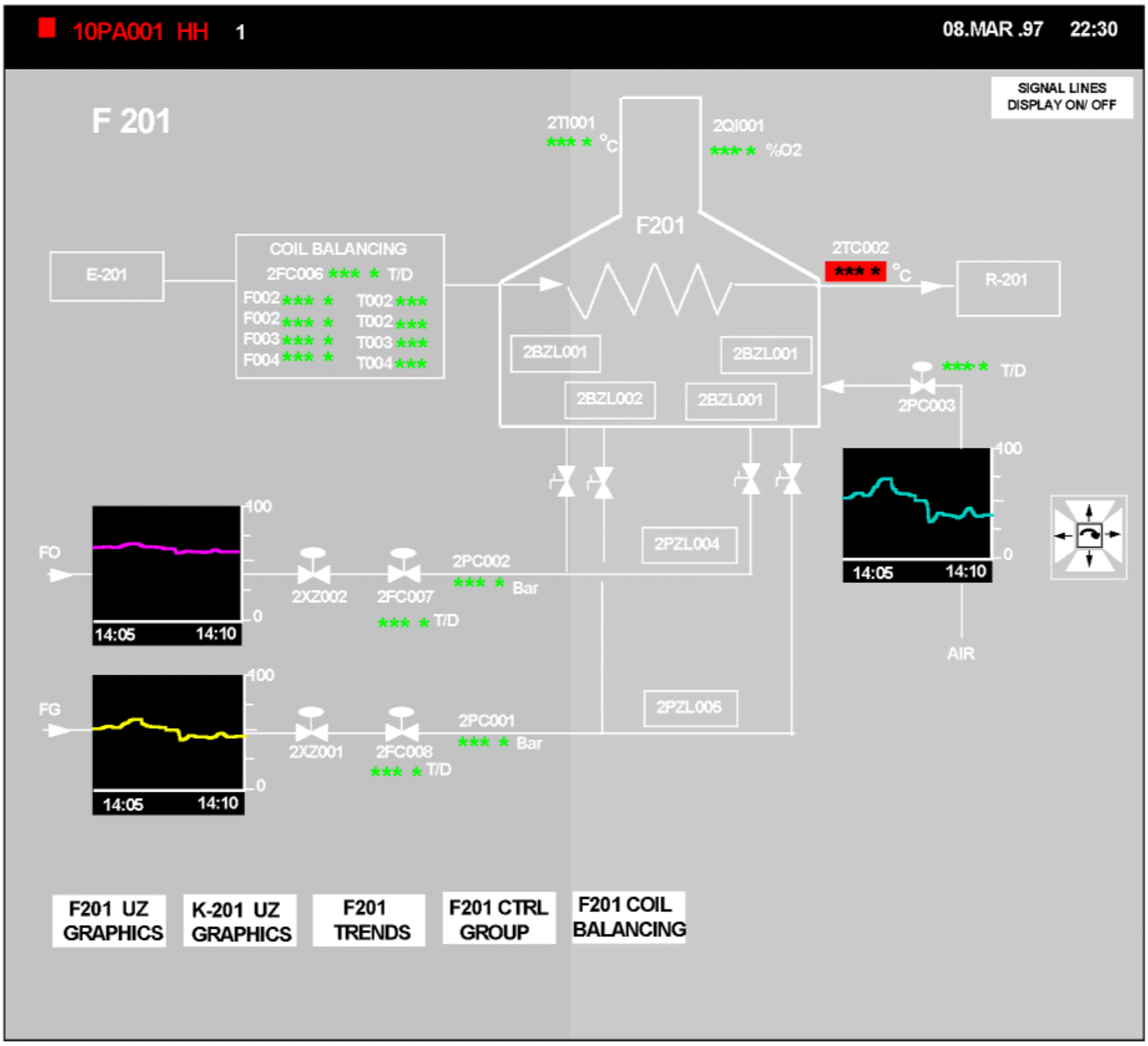
APPENDIX 5 TYPICAL UNIT DISPLAY



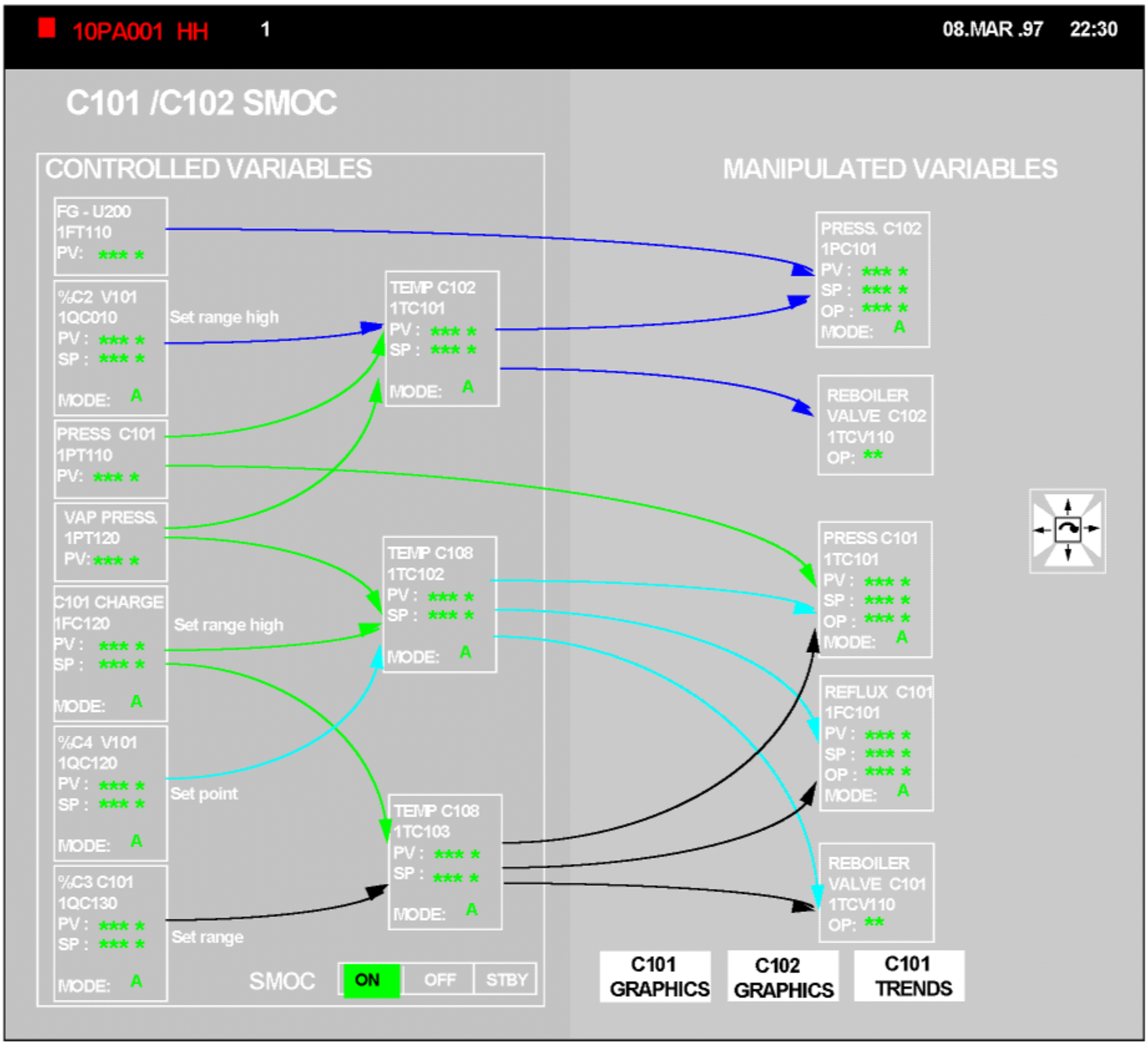
APPENDIX 6 TYPICAL SUB UNIT DISPLAY



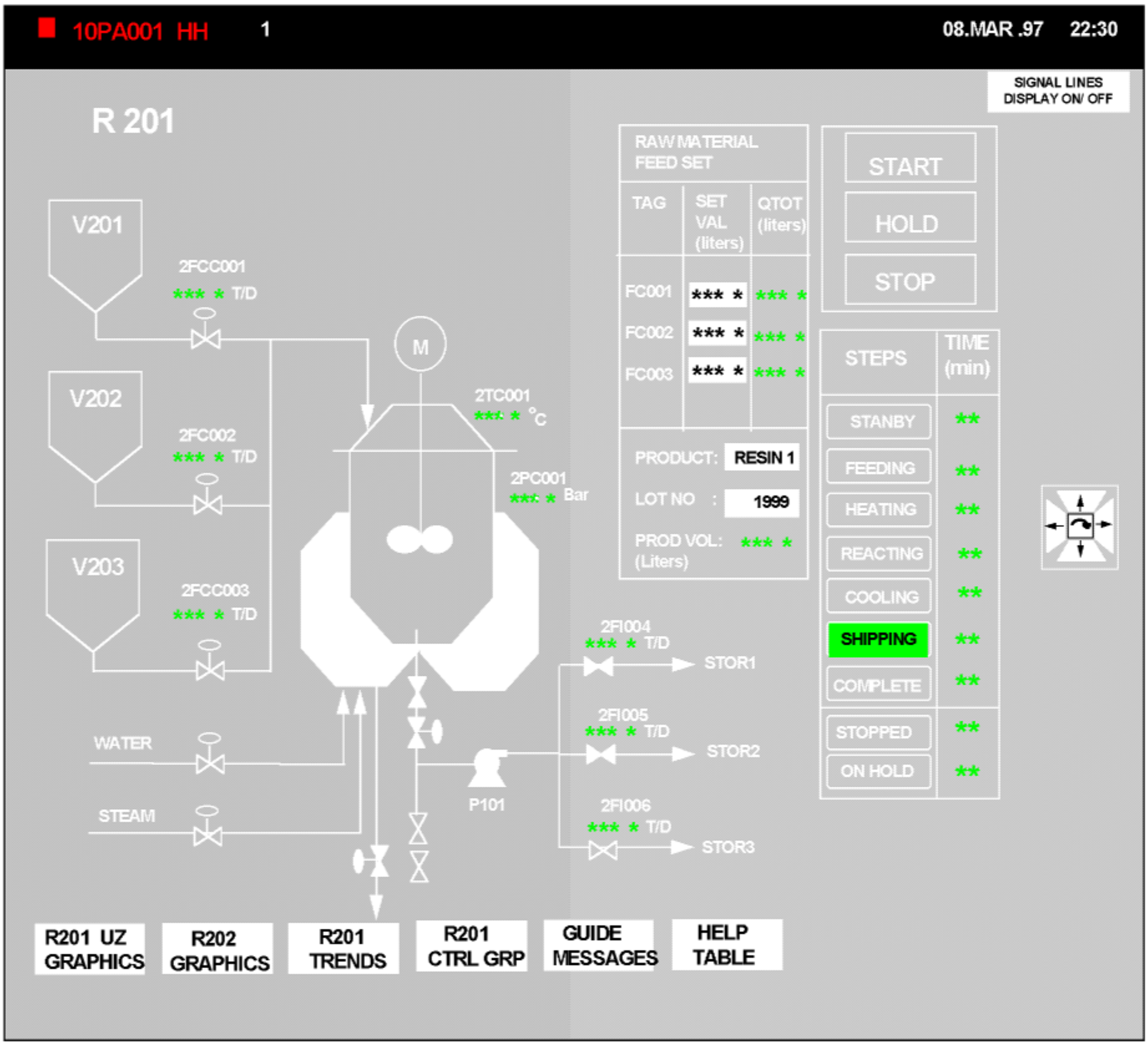
APPENDIX 7 TYPICAL DETAILED PROCESS DISPLAY



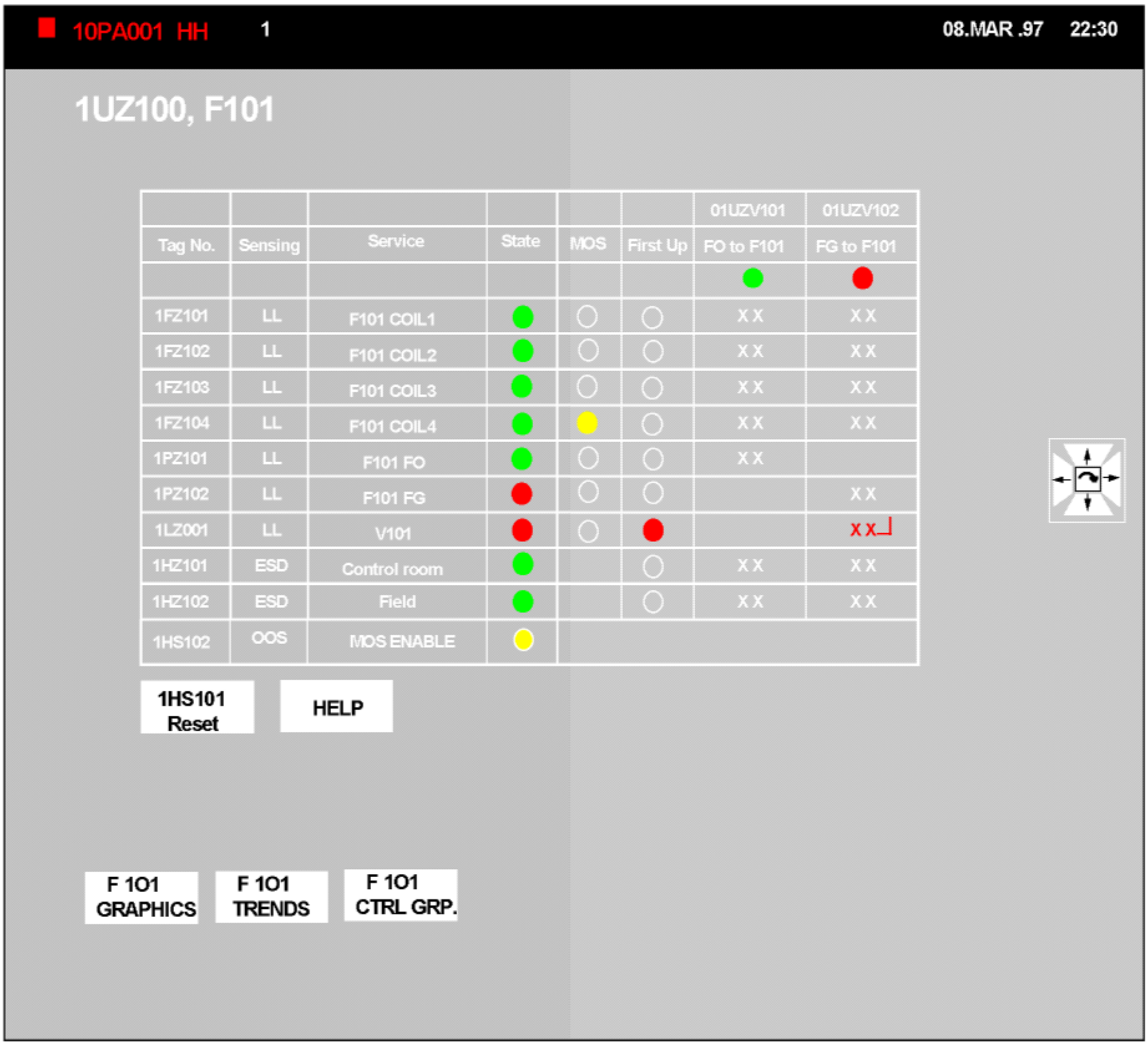
APPENDIX 8 TYPICAL MULTI-VARIABLE CONTROL LOOPS DISPLAY



APPENDIX 9 TYPICAL SEQUENCE DISPLAY



APPENDIX 10 TYPICAL IPF STATUS LOGIC DISPLAY



APPENDIX 11 TYPICAL SYMBOLS GRAPHIC DISPLAY