

SHELL INTERNATIONAL CHEMICALS B.V.
AMSTERDAM - THE NETHERLANDS

SHELL EO/EG PROCESS MEMORANDUM 115

SUBJECT : PROCESS CONTROL AND SAFEGUARDING SYSTEMS

DATE OF ISSUE : APRIL 2005

This document provides requirements for preparation of specifications for the distributed control system and the safeguarding system. It is assumed that the user is familiar with the present state of the art of process automation and safeguarding equipment. Normal operational requirements and technical details are therefore not included in this memorandum.



TABLE OF CONTENTS

1.	GENERAL REQUIREMENTS	3
2.	MONITORING AND CONTROL SYSTEM	4
2.1	Digital control system (DCS).....	4
2.1.1	Alarm handling	7
2.2	Specific EO/EG plant functionality	7
2.2.1	Temperature profile guidance in the EO reactor.....	7
2.2.2	Flammable limit guidance.....	8
2.2.3	Guidance and check of pre-start-up sequence procedures.....	8
2.3	Instrumented protective systems	8
2.3.1	Maintenance override switches	9
2.3.2	Operational override switches.....	10
2.4	Field instrumentation	10
2.4.1	Local panels	10
2.4.2	Transmitters and valves	10
2.4.3	Fire & gas detection.....	11
2.5	Ergonomic requirements.....	11
3.	POWERSUPPLY	13
3.1	DCS.....	13
3.2	Instrumented Protective Systems.....	14
4.	EARTHING	15



1. GENERAL REQUIREMENTS

The panel operators in the control room shall have access to all relevant process variables via a Distributed Control System (DCS). The operator interface should be fully integrated. The plant operators should be able to carry out all actions via the DCS workstations.

The monitoring and control system shall provide for operation of the plant in a stable, efficient and reliable manner with minimum off-spec product. The DCS should contain all control and computing functions needed to perform these tasks.

It must be designed for steady state plant control with sufficient flexibility to operate at conditions away from design. The control systems shall be designed in such a way that the effect of operational variations and disturbances in one section of the plant will have a minimised effect on other sections.

The degree of automation/control should be selected in a cost-effective manner in line with licensee's wishes/philosophy.

A separate (separate from the DCS) instrument protective system shall be installed.

It is recommended that the control building is equipped with a blast proof air-conditioned auxiliary room. The auxiliary room is intended to house all instrument and supporting electrical systems for process for control, data collection, safeguarding, telecommunication, etcetera.



2. MONITORING AND CONTROL SYSTEM

The design of the entire automation system, control room, console, etcetera shall be done in accordance with DEP 32.00.00.11. - Human-machine interface in a control Room. The design shall cover aspects such as:

- Plant conditions and operator task analysis
- Control room design, ergonomic aspects, lighting etc.
- DCS console design
- Graphic design, hierarchy, navigation etc.
- Alarm management, prioritising, masking techniques etc.
- System management and security

If control requirements for certain parts of the plant go beyond the capabilities of the DCS, or if use of other control equipment (process computer) is more economical, this may be considered alternatively. However, the concept of full integration of information/operation should as far as practicable be adhered to.

2.1 Digital control system (DCS)

The DCS is a microprocessor-based system. It should be built up in a modular structure, both functionally and physically. The modules should be independent with respect to failure. The DCS will contain, at minimum, modules of the following type:

- Field Stations (Process data acquisition, PID control and computing functions) located in the auxiliary room.
- Operator Interface Modules (with VDU's, keyboards, printers for alarm/event recording, printers for report generation and a video copier) located in the control room. In an adjacent room a separate Operator Interface Module with read-only functions may be installed for supervisory staff.
- Engineering work station.

In addition, the DCS may contain Gateway Modules for communication with other equipment, such as process computer, IPS, F&G system.

In order to provide the operator with the tools necessary for reliable and proper



control, the DCS should contain at least the following functionality:

- Steady state and dynamic control
- Process data collection
- On/Off switching
- Alarm generation
- Graphic displays
- Group displays
- Loop displays
- Alarm summary displays
- Sequence logic
- Trending (real time and historical)
- Reporting
- System Diagnostics with adequate system alarm presentation

Under all plant conditions (steady state, upset etc.) the invocation time for a display to appear on the VDU shall be as follows (the invocation time is duration from the pressing of the last key until the appearance of the last information on the screen):

<u>Display Type</u>	<u>Invocation Time</u>
alarm displays	max. 2 seconds
group information	max. 2 seconds
overview real time trend	max. 5 seconds
historical trend	max. 7 seconds
graphic displays (incl. live updates)	max. 2 seconds
all other displays	max. 7 seconds

The monitoring and control system shall be reliable and robust. Provisions shall be made to prevent loss of control functionalities that might lead to plant upset, off-spec product, damaged equipment or shutdown. To fulfil these requirements, the system redundancy shall be as specified below:



<u>Item</u>	<u>Redundancy</u>
Control Network	Dual
Controller	At least 1 to 'n' ($n \leq 8$)
Analog input signal	None
Analog input card	None
Analog input (controlled) card	Redundant
Analog output signal	None
Analog output card	None
Analog output (controlled) card	Redundant
Digital output card	None
Video electronics	Backed up on multi-unit basis
VDU keyboard	Backed up on multi-unit basis
Power supply (Controllers)	Redundant
Multiplexer	None
Gateways (general)	None
PLC Gateways (IPS, F&G)	Redundant
MOV system Gateways	Redundant
Alarm Printers	Dual manually switchable, shared with report printers
Report Printers	Dual manually switchable, shared with alarm printers
Floppy /cartridge disk drivers.	Dual
Hard disks for mass storage	Redundant

Bear in mind that the total configuration is stored on the disk in the Engineering Work Station. This disk should be mirrored, i.e. storage on one disk should be automatically copied to the mirror disk.

The DCS shall include facilities for trending and deviation indications, in order to keep the operator aware of non-steady process conditions and to allow him to observe the development of imminent disturbances. The operator control actions during normal operational conditions should be restricted to adjustments of a minimum number of setpoints.



The DCS should provide the panel operator with the possibility to define deviation limits for the process variables and range limits for the control valve signals. An operator should be alerted when a process condition is not at its target value or a valve position has reached its limit. Deviation indications are only used for operator guidance and should not belong to the alarm categories.

Adequate disc capacity shall be available and allocated for storage of historical data for 10 seconds (all controlled variables and points indicated on the PFD's as having recording function) or 1 minute snapshots (all other variables), hourly averages, shift averages and daily averages, as well as for 10000 alarms and events.

Archiving facilities including playback shall be available for post-mortem analysis or as a reference on catalyst performance, without interrupting system operation. The recommended storage period should be sufficient to comprise at least one catalyst cycle (SOC - EOC).

It is advised to design the DCS with at least 30% spare capacity for hardware, network capacity, gateways and interface modules and software.

2.1.1 Alarm handling

See with DEP 32.00.00.11 - Human-machine interface in a control room.

2.2 Specific EO/EG plant functionality

Following functions are required for the EO/EG plant to improve operations/start-up:

- Temperature profile guidance in the EO Reactor.
- Flammable limit guidance.
- Guidance and check of pre-start-up sequence procedures.

2.2.1 Temperature profile guidance in the EO reactor

It is very effective for optimum operation to observe the temperature profile in the EO reactor catalyst bed/coolant continuously.

All temperature process values shall be calculated into level averages, which can



be displayed as an axial temperature profile and into radial temperature profiles at various levels of the reactor. This feature provides fast visual information and assists the operator to take corrective action.

Process related parameters like Peak Temperature Difference (PTD) shall also be shown by the DCS.

2.2.2 Flammable limit guidance

It is profitable to operate the plant as close as possible to the flammable limit because of increased selectivity. However, too small a margin between the actual oxygen concentration and the flammable limit shall be avoided in order to avoid the risk of a runaway.

Data from online analysers are used for the calculation of the flammable limit. Calculation results are continuously presented to the operator interface.

2.2.3 Guidance and check of pre-start-up sequence procedures

The operator is automatically guided through the pre start-up sequence and checks are done whether the correct pre-start-up sequence of actions is undertaken by gathering necessary signals, already present in the DCS, such as valve position signals, control signals, interlock conditions etc.

2.3 Instrumented protective systems

The EO/EG process consists of three major safeguarding systems:

- O₂ feed flow control and shut-down system
- CO₂ removal unit shut-down system
- Glycol reactor shut-down system

These shutdown systems are described in detail in process memoranda 111, 112 and 113.

Other types of trip actions, which are part of the safeguarding, are:

- back flow protection



- temperature trip on pump handling EO concentrations > 10% weight
- trip of residual gas compressor
- gas breakthrough protection
- protection of various columns
- others

Safeguarding systems should be designed in accordance with:

- DEP 32.80.10.30 - Instrumented protective systems
- DEP 32.80.10.10 - Classification and implementation of instrumented protective functions

In general, all components used in SIL 1, 2 and 3 functions shall be independent of components used for monitoring and control functions. Pre-alarms shall be regarded as one of the monitoring and control functions.

The systems (PLC or solid state) shall be German TÜV certified for IPF class V or SIL class 3. Certified systems are:

- PLC types:
 - Honeywell SMS
 - Hima
 - Triconex
 - Yokogawa (Prosave)
- Solid state types:
 - Yokogawa (type: Maglog 24)
 - Hima (type: Planar F)

2.3.1 Maintenance override switches

Testing of sensors and actuating elements of safeguarding systems is required to maintain the integrity of a system (ensure maximum acceptable probability of failure on demand, see DEP 32.80.10.10) and for complying with local requirements.

Therefore to enable testing of sensors maintenance override switches (MOS) shall be provided in accordance with DEP 32.80.10.10.



2.3.2 Operational override switches

Operational override switches (OOS) shall be implemented in accordance with DEP 32.80.10.10. However, where possible, operational override switches should be avoided by using automatic timer functions in the IPS.

2.4 Field instrumentation

2.4.1 Local panels

The use of local panels depends on the Licensee's operational philosophy with regards to start-up, operation, and shutdown of large pieces of equipment such as compressors. All logic and control hardware for local panels however shall be installed in the auxiliary room.

2.4.2 Transmitters and valves

In general all field instrumentation shall be 'smart' with 2 wire 4-20mA or digital signal transmission.

The term 'smart' in this context denotes the following features to be incorporated in the transmitter:

- The transmitter's output is selectable between a floating 4-20 mA signal and a digital signal being vendor's proprietary protocol.
- The transmitter's parameters, such as zero, span, engineering units, sensor type, etc. is remotely adjustable via the Engineering Work Station in order to store the data per instrument. For field maintenance checks use of a hand-held 'communicator' is envisaged.
- The transmitter offers a very high rangeability in order to maximise the advantages of remote adjustments without the need for changing the sensor/measuring cell. The rangeability shall typically be better than 1:100.
- The transmitter offers internal signal linearization features such as square rooting (for flow by means of orifices), thermocouple curves etc.
- The transmitter is equipped with sensors measuring secondary parameters having a systematic effect on the primary measurement (e.g. coldjunction,



static pressure. etc.). The transmitter compensates for these systematic effects and thus increasing the accuracy.

- The transmitters are equipped with self-diagnostic features to ensure proper functioning of the device. In case an error is detected the output is directed to a pre-set state (upscale, downscale, best guess).

Process connected switches such as pressure switches, temperature switches, flow switches (other than for lube oil, utility instrument air and utility nitrogen services), are not allowed.

As a rule all transmitters may be blind. Local and local panel indicators shall be applied where specifically required as indicated on the PFD.

Accuracy of Instruments shall be 0.2% of span, sensitivity 0,05% and repeatability +/- 0.1% of span as a maximum.

Control valves are to be pneumatically operated, and equipped with pneumatic, electro-pneumatic or 'smart'-pneumatic positioners. Where pneumatic positioners are used, local P/I converters shall be used to optimise control loop performance.

Attention should be given to the opening/closing times (normally less than 3 seconds, unless mentioned otherwise) of valves in on/off service connected to the safeguarding systems.

2.4.3 Fire & gas detection

All pumps in EO service (> 10 wt % EO) are to be equipped with gas detectors (preferably EO type).

Fire & Gas detection and alarm systems shall be in accordance with DEP 32.30.20.11 "Fire, Gas and Smoke Detection Systems".

2.5 Ergonomic requirements

The number of panel operators required to control the plant from the console and hence the number of VDU's and keyboards on a console should be such that an acceptable workload for the operators is expected. A typical figure of 200 to 250 control loops per panel operator is realistic for a process plant under steady state



conditions (one control loop is one modulated final control element). The number of VDU's should be such that additional operators can assist during a plant upset.

For the EO/EG process (inside battery limit facilities only), it is possible to efficiently start up and shutdown a plant (having only one EO Reactor) with 6 VDU's. During steady state operation 4 VDU's should be adequate to operate the plant. The remaining 2 VDU's could be used for general displays during steady state operation; during start-up/shutdown or plant upsets, requiring increased attention, they provide additional workspace for a second operator.

The actual number of VDU's to be installed is left to the Licensee's operating philosophy.

As part of all the graphics to be configured in accordance with DEP 32.00.00.11 and as per licensee's wishes, the following process graphics are recommended:

- IPF status logic display.
- Oxygen shutdown system including oxygen mixing nozzle and nitrogen vessels.
- Graphic presentation of the temperature distribution for the reactor shell/tube side.
- Oxygen mixing nozzle, feed/product exchanger, EO reactor.
- Primary product cooler and associated steam drums.
- Glycol reactor section with feed pumps and water surge drum.
- Recycle gas loop.
- Lean absorbent loop.
- Carbonate loop.
- Around water surge drum in glycol unit.
- Around LE column and EO purification column and feed to glycol reactor
- Every column with temperature/pressure profiles.
- Plant overview.
- Steam balance.



3. POWERSUPPLY

3.1 DCS

The DCS shall as a minimum be powered from UPS typically in accordance with Figure 1.

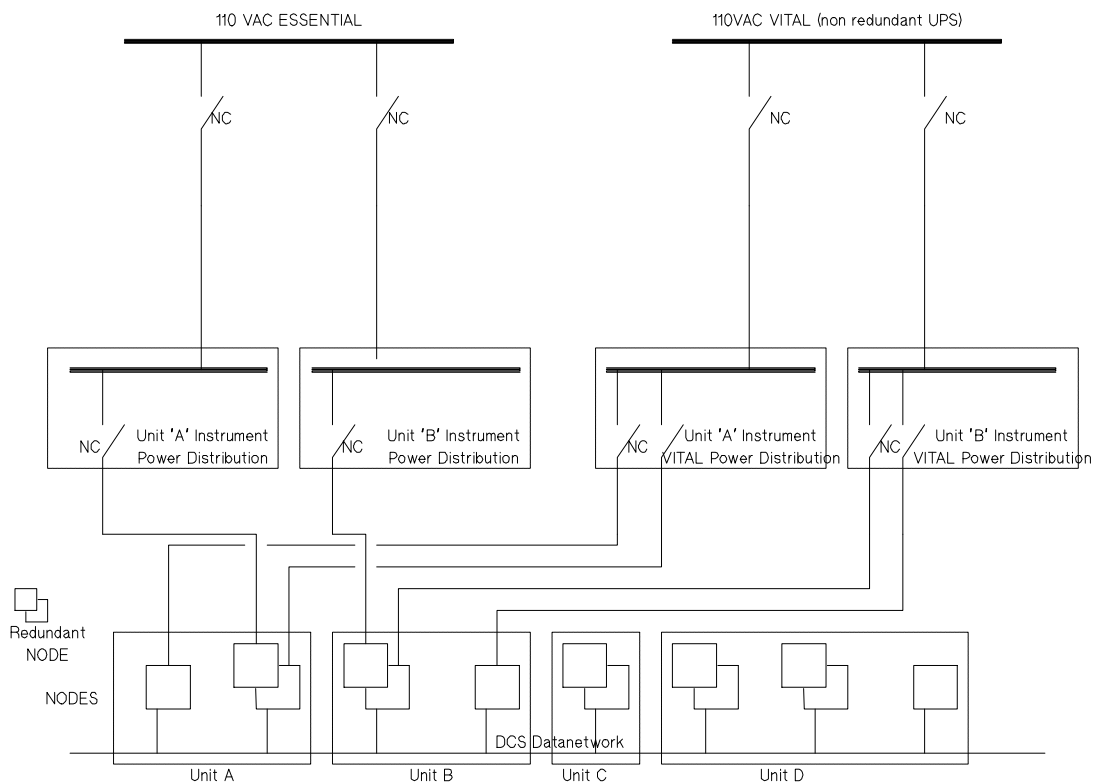


Figure 1: Typical redundant power distribution for 110VAC consumers in the DCS.

Power supply distribution shall be segregated in process units to allow unit wise maintenance and shutdown. Power supply to DCS shall be from two different sources, Vital A (UPS) and one essential (backed up by diesel generator) or Vital B (UPS). Each power supply (single failure) is allowed to fail without giving rise to loss of control, I/O monitoring, alarming, and the ability for the operator to view and manipulate the process.

- Power packs shall be included for powering system components and process transmitter and converters at 24 volt DC.
- Dual standard power packs shall be used for the powering of data acquisition and controller sub-system equipment.



- Individual loop fusing shall be provided.
- The system shall include for double pole isolators and overcurrent protection for all incoming supplies. Sufficient isolation facilities on the DC subsystems shall be provided to enable maintenance and replacement of components with minimum disturbance.
- Workstations and peripherals shall have internal overcurrent and isolation facilities.
- Field instruments for control and monitoring are best powered from the DCS.

3.2 Instrumented Protective Systems

IPS shall be powered from two different sources, Vital A (UPS) and one essential (backed up by diesel generator) or Vital B (UPS). Each power supply (single failure) is allowed to fail without causing a plant trip. Each power source shall be capable of supplying all the power required. Otherwise power supply shall be in accordance with DEP 32.80.10.30.



4. EARTHING

Instrument Systems, power supply, signal cabling etc. shall be earthed for personnel safety and to achieve electro magnetic immunity. Measures to achieve EMC are best chosen in accordance with IEC 1000-5-2 and BS6651:1992 Appendix C (lightning). Lightning shall be included as a possible "disturbance source."

DCS and IPS vendor earthing requirements shall be strictly adhered to.

