Safety and Automation System Narrative

CO_2 Capture Facility

Kårstø, Norway

Rev.	Date	Reason for Revision	By	Check	App	App	App
1	12/9/08	REVISED PER COMMENTS I-0162	VC	LBJ	LBJ	BTR	WRE
0	12-NOV-08	ISSUED FOR COMMENT	VC	LBJ	LBJ	BTR	WRE

Bechtel Power Corporation

Job No. 25474

Document No.	Rev.
25474-000-3YD-J01G-00002	1

GASSNOVA

Project No. - Originator - Disc Code - Doc Type - Serial No.

10112936 – PB – I – DRW – 0002

Contents

1.0 SYSTEM OVERVIEW

The purpose of the Safety and Automation System (SAS), a DCS based system, is to control and monitor plant equipment and processes in a safe and efficient manner. The DCS accomplishes these goals by performing the following general functions:

- Enforces protective logic for individual devices, providing safe and orderly shut down of abnormally operating equipment.
- Supervises and controls normal operation of individual devices, freeing the operator to attend to abnormal operating conditions.
- Gathers, organizes, and presents dynamic plant process information to the control room operator, empowering the operator to make informed operating decisions.
- Records data continuously for analysis, troubleshooting, and diagnostics.
- Directs operator commands to the proper individual device, allowing the operator to manipulate the process intuitively.
- Accommodates changes to its architecture and programming, facilitating plant improvements.
- Documents plant operating information, providing data from which plant engineering can make informed improvement decisions.

The DCS provides integrated modulating control, sequential control, and data acquisition for both normal operation and the Process Shutdown System (PSD).

The DCS controls, monitors and records physical and electrical parameters associated with the CCC Plant. The system provides interface with ESD, F&G, CEMS, CCTV, PA and with existing installations. The DCS allows full operation from the new Central Control Room (CCR). This system description describes only the DCS system itself, including those portions of the DCS that are common to all controlled systems, but excludes details about the individual system process controls.

The SAS system described in this document is conceptual and subject to change during detailed design depending on the vendor DCS, ESD and F&G system selected. A detailed conceptual layout of the SAS is provided in the SAS Architecture Drawing [Ref 8.1]. The system is designed to meet the specifications outlined in Exhibit E4.2 – General Technical Specification, Safety and Automation System, and the SAS Design Philosophy [Ref 8.2] and Exhibit E4.4 - General Technical Requirements, Fire and Gas Monitoring and Alarm System [Ref 8.4].

2.0 DEFINITIONS AND ABBREVIATIONS

CCC	CO2 Capture and Compression
CCR	Central Control Room
CPU	Central Processing Unit
CCPP	Combined Cycle Power Plant
CCTV	Closed Circuit Tele Vision
CEMS	Continuous Emissions Monitoring System
DCS	Distributed Control System
DMZ	Demilitarized zone (network)
Ethernet/IP	Ethernet Industrial Protocol
ESD	Emergency Shut Down (System)
FF	Foundation Fieldbus
F&G	Fire and Gas Monitoring and Alarm System
HART	Highway Addressable Remote Transducer
HMI	Human Machine Interface
HSE	Health, Environment and Safety
HVAC	Heating, Ventilation and Air Conditioning
IMS	Information Management System
GPS	Global Positioning System
I/O	Input / Output
IMS	Information Management System
LAN	Local Area Network
LER	Local Equipment Room
LIR	Local Instrument Room
MCC	Motor Control Center
OLE	Object Linking and Embedding
OPC	OLE for Process Control Standard
OS	Operator Station
PA	Public Address
PCS	Process Control System
PLC	Programmable Logic Controller
RIO	Remote Inputs/Outputs
PSD	Process Shut Down (System)
SAS	Safety and Automation System
SCADA	Supervisory Control And Data Acquisition System
SCS	Station Clock System
SIL	Safety Integrity Level
VDU	Visual Display Unit

3.0 COMPONENT DESCRIPTION

The major components of the DCS are as follows:

- Input and Output Cards (I/O)
- Controller Cabinets
- Remote I/Os and Remote I/O Cabinets
- DCS-PLC Interfaces
- Operator Stations (2)
- Auxiliary Trip Panel (for ESD pushbuttons)
- Action Panels for ESD and F&G PLCs
- Large Screen Display (VDU)
- Engineering Workstation (EWS)
- Plant Historian Station
- Data Highway
- IMS Server Station
- Managed Ethernet Switches
- Routers
- DCS Data Highway Switches
- DMZ Network
- Domain Controller and Anti-Virus
- Close Circuit Tele Vision System (CCTV)
- PA System
- Global Positioning System (GPS) Based Clock System
- Color Laser Printer
- CEMS and F&G Laser Printers (B/W)
- ESD/F&G Engineering Laptop

3.1 INPUT AND OUTPUT CARDS (I/O)

The I/O used for the CCC Plant includes a mix of Foundation Fieldbus (FF) digital bus and hardwired I/O. FF is used where practicable for DCS I/O. PSD, ESD and F&G I/O are hardwired.

Foundation Fieldbus segment power supplies and segment power conditioners are dual-redundant, and segment interface cards are non-redundant. Fieldbus Intrinsically Safe Concept (FISCO) is used where required to meet hazardous area requirements. For critical field loops where redundancy is required, I/O will be separated onto different FF segments or hardwired. Multiplexers for digital signals are non-redundant.

The hardwired I/O modules used support all standard industrial signals (analogue/digital inputs/outputs, relay outputs, 4-20 mA, 0-10V, mV, Pt 100 inputs, etc.). All modules are mounted in cabinet racks with prefabricated connections for external wiring. I/O cards are intrinsically safe where required to meet hazardous area requirements. The PSD and ESD I/O cards are SIL-rated as required. Sequence

of Events type digital inputs are used on breaker closed status and relay alarms for electrical equipment 6.6kV and higher. The digital output modules provide both Normally Energized (ESD) and Normally De-energized (F&G) outputs. Analog inputs support HART routing for easy calibration checking and diagnosis with configurable access.

All I/O modules are replaceable under full operating conditions without requiring PCS unit shutdown and without affecting other modules. The system is designed such that a single defect or failure in any module will not affect any other module. A short-circuit in the field will also not lead to a damage of the I/O module.

3.2 CONTROLLER CABINETS

The controller cabinets contain control processors, communication interfaces, terminations, power supplies, and power distribution.

One pair of redundant controllers is designated to each cabinet. During normal operation the primary controller is on-line. The secondary processor will take over control should the primary processor fail its internal diagnostics. The transfer is bumpless; there is no interruption to the I/O card status.

Both the primary and secondary processors of a redundant pair are redundantly connected to the Ethernet Network.

Dual redundant power supplies for these controllers accept dual 230VAC, 50 Hz UPS power feeds.

All controller cabinets are located in the CCR Equipment Room next to the Central Control Room (CCR).

3.3 LOCAL AND REMOTE I/O CABINETS

I/O and FF Gateways are installed locally to the processors in the CCR Equipment Room or installed in remote I/O cabinets mounted in the electrical building or the compressor building in order to minimize the length of the field wiring. For the ESD and F&G systems, all I/O is installed in the CCR Equipment room in order to remove it from the process area as much as possible.

Redundant Fiber Optic cables are used between each remote I/O cabinet and its associated controller cabinet.

Dual redundant power supplies for the remote I/O cabinets accept dual 230VAC, 50 Hz UPS power feeds.

3.4 DCS INTERFACES

The DCS will interface with the PLCs of the ESD, F&G, CEMS systems, and external control systems including Kårstø Gas Plant, Naturkraft CCPP, and the storage system (GASSCO) through managed Ethernet switches and interface servers,

allowing the operator in the control room (CCR) to monitor and/or control these systems.

3.5 INFORMATION MANAGEMENT SYSTEM (IMS)

The IMS server allows users in external networks to view current DCS operating status and retrieve historical data from the plant Historian. The IMS server connects to both the DCS data highway and the DMZ network. The DMZ network provides security between the DCS control network and external general-use networks such as the plant LAN, Gassnova LAN, Bechtel LAN, and any other external networks that may be connected in the future via a router and managed switch. Access to the IMS server configuration is via the engineering station or historian station.

3.6 OPERATOR STATION

The two Operator Stations are located on a console in the CCR.

The Operator Stations present plant information to the operator by displaying dynamic process graphics. Process graphics are pictorial representations of the process. They are designed to collect and efficiently display important information about a particular process. They also allow the operator to select a particular component with the mouse for control. A pop-up graphic window is then displayed from which the operator can select equipment operation states. The process graphic configuration is copied to and resides on the operator station hard disk.

Text occurring on the operators VDUs related to normal operations will be in Norwegian.

An Auxiliary Panel, containing emergency trip pushbuttons for the ESD, is located in the custom console next the operator station.

Two more panels (Action Panels) are provided for status display, manual activation and reset of the ESD and F&G systems. The action panels are mounted in the CCR next to the large screen display.

A Large Screen Display unit is mounted in the CCR for additional supervision and monitoring of the process as a supplement to the operation stations.

3.7 ENGINEERING WORK STATION (EWS)

The EWS performs all of the functions of the operator station. In addition, it allows the engineer to edit the master configuration residing on the engineer station and load it into the controllers. The EWS also can edit the master process graphic configurations, residing on the engineer stations and download it to each operator station. The engineer also accesses the IMS server, domain controller, and interface servers via the EWS.

3.8 PLANT HISTORIAN

The Plant Historian receives and records selected input, output, and calculated values from the data highway. This data can be organized into configurable reports, and dumped to the printers. Data is readily available for trending purposes from any operator station or the EWS, and can be accessed from external networks via the IMS server.

3.9 DOMAIN CONTROLLER AND ANTI-VIRUS SERVER

The Domain Controller is used to set up and administer user accounts on the computers throughout the system. This server also acts as a central point to distribute virus definition file updates to the systems on the network.

3.10 DATA HIGHWAY

The redundant data highway facilitates communication among the Operator Stations, EWS, Plant Historian, OPC Servers, IMS Server, Domain Controller and Anti-Virus Server, controllers, EDS and F&G PLCs, CEMS PLC and with existing installations through various Ethernet switches, routers and interface servers.

(See Ref 8.1, 25474-000-JD-JD-00001 for DCS Network Configuration)

Each of the operator work stations, EWS, IMS Server, EDS and F&G PLCs, and Plant Historian has redundant connections to the data highway through managed Ethernet switches. If one connection is failed, the devices will still be linked to the data highway from the other connection.

Each redundant controller pair also has redundant connection to the data highway through Ethernet switches. This type of design greatly increases the reliability of the whole data highway system.

3.11 VIDEO MONITORING (CCTV)

A video monitoring system (CCTV) is provided for monitoring relevant areas of the CCC Plant. The CCTV is connected to the DCS and its displays are available to the operator as part of the human machine interface and shown as windows within the large display unit or on the operator stations.

4.0 PRINCIPLES OF OPERATION

4.1 STARTUP

The DCS system is intended to operate continuously and accordingly has no standard startup procedure. However, individual components may need to be started or restarted on an as-needed basis, for example if system software is upgraded, new hardware is added to a server, etc. Components do not need to be restarted during normal operation and DCS control program configuration changes. DCS training course material and instruction books, to be provided during detailed design, should be consulted.

4.2 NORMAL OPERATION

During normal operation, the operator is continually seated facing two (2) operator stations. The engineer will use the Engineering Workstation (EWS) as necessary to revise and backup DCS configurations and graphics. DCS operator training course material, plant operating procedures, and DCS instruction books should be consulted for normal operation directions. Normal operation of the DCS includes selecting graphics, selecting equipment states, reacting to alarms, and monitoring key system parameters.

4.3 SHUTDOWN

Since the DCS is intended to be operated continuously, there is no standard shutdown procedure. However, most station operating systems include menu driven shutdown. DCS training course material and instruction books, to be provided during detailed design, should be consulted for detailed shutdown procedures.

4.4 INFREQUENT OPERATIONS

The DCS system is intended to operate continuously and accordingly has no standard infrequent operation procedure. Infrequent software upgrades may require shutdown of some DCS components, and will most likely be performed by vendor specialist. DCS training course material and instruction books, to be provided during detailed design, should be consulted.

4.5 EMERGENCY OPERATIONS

Extensive standard diagnostics are provided with the DCS system. Alarms include, but are not limited to processor mismatch, analog loop out of range, drops off highway, highway health, power supply health, and cabinet temperatures. DCS training course material and instruction books should be consulted for detailed responses and troubleshooting.

5.0 PROCES SHUTDOWN SYSTEM

The CCC Plant is equipped with a Process Shut Down system, defined herein as PSD system.

The PSD system ensures that the process conditions do not exceed specified process safety limits. The Process Shut Down system is functionally independent of the process control function but it is implemented in the same DCS as the SAS with dedicated controllers and I/O cabinets (see above description of the DCS structure and function).

The PSD system automatically shuts down discrete equipment, a system, or the CCC Plant, in a safe and controlled manner, in the event of abnormal operating conditions which could cause permanent damage to the plant, endanger human safety or exceed operating limits to the detriment of plant life.

The inputs and outputs (I/Os) cards of the PSD system are intrinsically safe cards. Each field input is separately protected against possible faults or induced voltage pickup and line break monitoring is provided. All critical inputs which will cause loss of plant performance are triple-redundant with 2 out-of-3 voting for digital inputs and dual redundant with average-select algorithm for analog inputs. Where 2 out-of-3 voting has been incorporated, then 1 out-of-3 discrepancy alarms are generated for the attention of the operator. The average-select algorithms will also provide the operator with alarms in case of discrepancies between the two analog inputs.

I/O for dual or triple redundant loops will be assigned on different cards within the system. Duplicated I/O modules are used where necessary to meet SIL requirements.

The system protects the CCC process against damage without having an effect to the availability and safety of neighboring Naturkraft CCPP and the CO2 Transport and Storage System.

6.0 EMERGENCY SHUTDOWN SYSTEM

The CCC Plant is equipped with an Emergency Shut-down system, defined herein as ESD system.

The ESD system will essentially actuate the appropriate PSD sequence(s) plus de-energize necessary electrical equipment and depressurize the unit (e.g. CO_2 compression system) in a safe manner. The ESD functions are manually initiated by the operator, usually as the result of a fire, major spill, combustible gas detection, etc.

For situations not requiring immediate action an audible and visible alarm will be given in the CCR and also locally. Alarms are sent to, handled and presented in SAS Alarm System.

The ESD system providing alarms and automatic commands is PLC based.

The inputs and outputs (I/Os) cards of the ESD system are intrinsically safe cards. Each field input is separately protected against possible faults or induced voltage pickup and line break monitoring is provided. I/O for dual or triple redundant loops will be assigned on different cards within the system. Duplicated I/O modules are used where necessary to meet SIL requirements.

All trips initiated by the ESD system are alarmed and logged.

The ESD is connected to the DCS Data Highway and all controls status and alarms are accessible by the operator from the operator station in CCR.

Additionally, status, manual activation and reset of the ESD system are available in the CCR also from an "Action Panel" hardwired to the ESD PLC.

For safety reasons all signals to be exchanged with Kårstø Gas Plant, the Naturkraft CCPP and with the Gassnova CO2 Transport and Storage System are hardwired.

7.0 FIRE AND GAS MONITORING AND ALARM SYSTEM

The CCC Plant is equipped with a Fire and Gas Monitoring and Alarm System, defined herein as F&G system. The system will be designed to meet requirements outlined in Exhibit E4.4 - General Technical Requirements, Fire and Gas Monitoring and Alarm System [Ref 8.4].

The F&G is largely an alarm system, but it is also able to take certain actions other than activating remote or local area alarms devices, like shutting off HVAC systems on gas detection, etc. in case of fire or gas and spill detection

The F&G system providing alarms and automatic commands is safety-PLC based. The system will be designed to meet SIL 2 according to IEC 61508 and IEC 61511.

The inputs and outputs (I/Os) cards of the F&G system are intrinsically safe cards. Each field input is separately protected against possible faults or induced voltage pickup and line break monitoring is provided.

Automatic trip signals will be derived from a 2 out of 2 voting logic from 2 detection loops at the same location based on SIL rating for each safety related function. If 2 out of 2 will not meet SIL 2, automatic trip signals will be derived from a 2 out of 3 voting logic from 3 detection loops at the same location.

Where 2 out-of-3 voting has been incorporated, then 1 out-of-3 discrepancy alarms is generated for the attention of the operator. All alarms/trips initiated by the F&G system are alarmed and logged.

The F&G is connected to the DCS Data Highway and all controls status and alarms are accessible by the operator from the operator station in CCR.

Additionally, status, manual activation and reset of the F&G system are available in the CCR also from an "Action Panel" hardwired to the F&G PLC.

For safety reasons all F&G connections to the field and critical connections to other control systems are hardwired.

8.0 REFERENCES

8.1 SAS Architecture Diagram

25474-000-JD-JD-00001 / 10112936-PB-I-DRW-0001, Revision 0

8.2 Exhibit E4.2 - General Technical Specification, Safety and Automation System

10112936-FI-B-CON-0092, Revision 04

8.3 SAS Design Philosophy

25474-000-3YD-JJDG-00001 / 10112936-PB-I-TDO-0001, Revision 0

8.4 Exhibit E4.4 - General Technical Requirements, Fire and Gas Monitoring and Alarm System

10112936-FI-B-CON-0094, Revision 01

8.5 Exhibit E4.3 – General Technical Requirements, Plant Communication

10112936-FI-B-CON-0093-03, Revision 03