

GENERAL SPECIFICATION

INSTRUMENTATION

GS EP INS 134

Design and supply of integrated control and safety system

10	11/2012	Revised as per marking
09	01/2012	Revised as per marking
08	01/2011	Revised as per marking
07	10/2009	Revised as per marking
00	02/2001	First issue
Rev.	Date	Purpose of the revision

Owning entity: DEV/TEC

Managing entity: DEV/TEC/INS

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 2 of 99

Contents

1. Scope	4
2. Reference documents.....	4
3. Glossary.....	6
4. Integrated Control & Safety System Functional Description	7
4.1 Subsystem Description	7
5. Overall Architecture	8
5.1 General Design	8
5.2 Field Instrument Connections.....	9
5.3 Communication Networks	9
6. ICSS design	10
6.1 Life Cycle and Obsolescence Management	10
6.2 General Requirements.....	11
6.3 Hardware	13
6.4 Operating system.....	13
6.5 Interfaces and Industrial Communication Networks.....	13
6.6 Interfaces with 3 rd Party Systems	14
6.7 Remote Maintenance and Diagnostic (RMD)	14
6.8 Application software(s) development.....	15
6.9 ICSS database.....	16
7. Specific Requirements per Subsystem	16
7.1 Emergency Shut-Down System	16
7.2 Ultimate Safety System (optional)	17
7.3 Fire and Gas System	18
7.4 Process Safety System.....	19
7.5 Process Control System.....	20
7.6 Human Machine Interface (HMI)	21
7.7 Historian server.....	21
7.8 Process Data Server (PDS)	22

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 3 of 99

8. Specific functional requirements.....	22
8.1 Safety-Related Sequence of Events.....	22
8.2 Maintenance tools requirements	23
8.3 Instrument Management System	24
8.4 Alarm Management Function	24
9. ICSS System Performance	25
10. Packages interface.....	26
11. Spareage Requirements	27
12. Factory Acceptance Test (FAT)	27
13. Documentation	27
14. Training courses	27
15. Specific Cases.....	28
15.1 PSS combined with ESD system	28
15.2 FGS combined with ESD system	28
15.3 Requirement for USS.....	28
16. Reference System	28
Bibliography.....	29
Appendix 1 ICSS General Architecture	30
Appendix 2 HVAC / ICSS / addressable fire detection system	31
Appendix 3 Function descriptions	32
Appendix 4 Hardware design	36
Appendix 5 Tests Requirements	41
Appendix 6 Functional Design Specification (FDS)	52
Appendix 7 Documentation	54
Appendix 8 Design of the control display system	61
Appendix 9 Glossary.....	76
Appendix 10 Symbols	79

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 4 of 99

1. Scope

This specification defines the minimum requirements for the design, fabrication, configuration, testing, installation and operation of an Integrated Control & Safety System for a petroleum installation.

The Integrated Control & Safety System shall ensure the safe operations of the facilities and fulfill the requirements of the operating and safety philosophies.

The ICSS shall perform the following main functions:

- Emergency Shutdown
- Fire and Gas Detection and Protection
- Process Shutdown
- Control and automation of process and utility equipment
- Human Machine Interface
- Alarm processing and management
- Interfaces with packages (main machines, electrical network system, HVAC, etc.)
- Events and historical data management including Sequence of Events
- Interface with Company enterprise network (SIE)
- Data Communications.

It shall be noted that the design, fabrication, configuration, testing and installation of ICSS shall also be compliant with cyber-security requirements, specified in **GS EP INS 135**.

2. Reference documents

The reference documents listed below form an integral part of this General Specification.

External Documents

Unless otherwise stipulated, the applicable version of these documents, including relevant appendices and supplements, is the latest revision published at the effective date of this document.

Reference	Title
ATEX European Directive 94/9/EC	European Directive on the approximation of the laws of the Member States concerning equipment and protective systems intended for use in potentially explosive atmospheres
EEMUA 191	Engineering Equipment and Material User's Association Alarm Systems - A Guide to Design, Management and Procurement
IEC 61000	Electromagnetic compatibility (EMC) - Part 5: Installation and mitigation guidelines

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 5 of 99

Reference	Title
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC 61511	Functional safety - Safety instrumented systems for the process industry sector
IECEX	IEC System for Certification to Standards relating to Equipment for use in Explosive Atmospheres (IECEX System)
ISA 18.2	Management of Alarms Systems for the Process Industries
SIREP-WIB-EXERA No. M 2656 X 98 part 2	Ergonomics in process control rooms, Design guidelines

Total General Specifications

Unless otherwise stipulated, the applicable version of these documents, including relevant appendices and supplements, is the latest revision published in the applicable yearly collection.

Reference	Title
GS EP EXP 131	Design and installation of Process Data Server
GS EP INS 101	Instrumentation engineering, supply and construction general requirements
GS EP INS 103	Instrumentation Database Management
GS EP INS 107	Design and installation of instrumentation links
GS EP INS 108	Instrumentation for the design of plant rooms and control rooms
GS EP INS 110	Instrumentation for package units
GS EP INS 131	Standard Functions and Functional Analysis Development Requirements
GS EP INS 135	Cyber Security requirements for design and supply of ICSS and Package Systems
GS EP INS 150	Design method for system configuration - Standard functions
GS EP INS 196	Input and Output Standard Functions
GS EP INS 197	Process Standard Functions
GS EP INS 198	Safety and Fire & Gas Standard Functions
GS EP SAF 261	Emergency Shutdown and Emergency De-Pressurisation (ESD & EDP)
GS EP SAF 312	Fire and Gas detection systems

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 6 of 99

Reference	Title
GS EP TEC 007	Obsolescence and Lifetime Cycle Management
GS EP TEL 170	Design and installation of Communications Network

3. Glossary

CPU	Central Processor Unit
CCR	Central Control Room
DCS	Distributed Control System
DMZ	Demilitarized zone
DVT	Design Validation Test
ESD	Emergency Shut-Down (SIS)
EWS	Engineering Work Station
FAT	Factory Acceptance Test
FDS	Functional Design Specification
FGS	Fire and Gas System (SIS)
ICSS	Integrated Control and Safety System
IMS	Instrument Management System
ISS	Internet Safety System
I/O	Inputs/Outputs
HMI	Human Machine Interface
MTTR	Mean Time to Repair
MWS	Maintenance Work Station
OS	Operating System
OTS	Operator Training Simulator
PCS	Process Control System
PDS	Process Data Server
PLC	Programmable Logic Controller
PSS	Process Safety System (SIS)
SIE	Enterprise Information System
SII	Industrial Information System
SIL	Safety Integrity Level
SIS	Safety Instrumented System

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 7 of 99

SOE	Sequence of Events
SVTS	Smart Valve Test System
OWS	Operator Work Station
UCP	Unit Control Panel
USS	Ultimate Safety System (SIS)

4. Integrated Control & Safety System Functional Description

The ICSS comprises of the following main subsystems:

4.1 Subsystem Description

4.1.1 Safety Instrumented Systems (SIS)

4.1.1.1 Emergency Shut-Down System

The ESD system forms part of the facility's safety systems. Its prime function is to shutdown the facilities to a safe state in case of an emergency situation, thus protecting personnel, the environment and the asset. It shall carry out the emergency shutdown and depressurization functions of the facility (e.g. ESD0, ESD1 and SD2) according to the defined safety philosophies.

4.1.1.2 Ultimate Safety System (USS) - optional

The USS forms part of the facility's safety systems. It is an autonomous system which is designed to act in parallel with the ESD system to carry out specific emergency shutdowns upon manual initiation. It does not duplicate the ESD system but provides a highly reliable back-up to specific ESD actions.

4.1.1.3 Fire and Gas System (FGS)

The F&G detection and protection system forms part of the facility's safety systems. Its function is to mitigate against the effects of any fire and/or gas releases in order to protect personnel, the environment and the asset. The F&G system will continuously monitor the facilities and initiate the protective actions as defined in the safety philosophies.

4.1.1.4 Process Safety System (PSS)

This PSS forms part of the facility's safety systems. Upon command, it shall automatically carry out the safe shutdown of particular units or equipment (e.g. SD3) as defined by the safety philosophies.

4.1.2 Process Control System (PCS)

The PCS system forms part of the facility's control systems. It shall ensure a safe, reliable and efficient control and monitoring of the process plant and utilities.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 8 of 99

4.1.3 Human Machine Interface (HMI)

The HMI shall provide the facility for the Operator to control and monitor the plant via mimic displays, alarms, trend displays and Operator commands. Specific displays can be developed for maintenance purpose.

4.1.4 Process Data Server (PDS)

The Process Data Server shall provide central data acquisition, archiving in order to provide trends and reports for information management.

4.1.5 Maintenance Stations (MWS)

Maintenance work Stations shall provide functions to carry out normal instrument maintenance activities such as loop verifications, inhibits (if required by project specifications), system diagnostic status.

4.1.6 Engineering Stations (EWS)

Engineering Working Stations shall allow access to configuration and detailed diagnostics of the system.

4.1.7 Sequence of Events Stations (SWS)

The Sequence of Events (SOE) station shall provide the SOE recorder function. It shall provide access to the SOE files and allow files from multiple nodes to be merged to give an overall coherent sequence of events of the plant.

4.1.8 Instrument Management System (IMS)

The IMS shall provide secured access to “smart” devices (instruments and valves) and present on-line information to assist maintenance personnel.

5. Overall Architecture

5.1 General Design

The ICSS shall have a distributed structure with a centralised HMI located in the CCR.

Refer to [GS EP INS 108](#) for CCR detailed requirements.

The ICSS Operator Work Stations (OWS) will provide a common HMI to ensure that the operator is able to monitor and control the whole plant. This shall include the main process and utilities as well as subsea equipment (where applicable) and process & utility packages.

Reporting of safety-related data will be via the PCS to the OWS located in the control room.

Each subsystem (ESD system, FGS, PSS and PCS) shall be based on dedicated controllers or PLC's and shall be fully independent of other subsystems (hardware and application software(s)), except in specific cases as described in § 15.

The safety systems (ESD, FGS, PSS) shall be based on diverse hardware and software from those used for PCS. The architecture shall avoid potential common mode, common cause and dependant failures between subsystems hardware or application software(s).

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 9 of 99

Depending on the application size, multiple nodes may be required per subsystem.

Typically, nodes from each subsystem shall be distributed in pressurized Instrument Technical Rooms located around the facility.

Each node will comprise of its controller, communications cards and I/O interface.

5.2 Field Instrument Connections

The field instruments shall be hardwired to marshalling cabinets, segregated per subsystem.

Marshalling cabinets shall be used to group field cabling and cross-wiring to the subsystems I/O cards.

Any safety-related I/O which is non fail safe shall be fully line monitored.

Remote Input/Output architecture may be foreseen with cards mounted inside field junction boxes or with cabinets located in Instrument Technical rooms.

In all cases where remote I/O is used, care shall be taken to ensure that impact to operations, including black start, maintenance, availability through segregation are all fully addressed.

When remote I/Os racks are used, the I/O bus design shall be such as a loss of one remote I/O rack will not impact the other remote I/Os racks: for instance the de-energization of one remote I/O rack shall not impede the control and monitoring of the other remote I/O racks.

Use of remote I/O architecture shall be subject to Company approval.

In the case of remote I/O mounted inside field junction boxes, then the complete assembly shall require to be suitable for the prevailing environmental conditions, zone 1 hazardous area, and complying with [ATEX European Directive 94/9/EC / IECEx](#) standards and SIL requirements.

5.3 Communication Networks

The system architecture shall be based on Appendix 1, ICSS General Architecture, and the following networks provided:

- **PCS Network**

This network shall interconnect the various nodes of the PCS system including controllers, workstations and servers. The network shall be fully redundant including communication cards.

- **PCS Services Network**

This network shall allow for OWS and historian equalisation, anti-virus dispatching, printers and other service functions for the ICSS. In addition it shall provide the connection from the PDS node to the firewall for interfacing to the SIE. The network should not need to be redundant.

- **SIS Safety Networks**

This network shall provide connections between all safety nodes belonging to the safety systems for information exchange, and if necessary executive actions.

Depending on project requirements, individual safety network may be assigned to each safety system (ESD system, PSS or FGS).

This network shall be physically independent and not directly connected to any other network. It shall be fully redundant.

Communication cards assigned to this safety network shall be fully segregated from other communication cards.

Executive actions may be transmitted by this safety network between safety controllers belonging to the same safety subsystem as long as it has been specifically designed for such purpose and has the appropriate SIL rating approval.

- **SIS-PCS Data Exchange Network**

This network provides the interface between safety systems and PCS in order to allow safety system data to be displayed to the operator on the OWS.

The network shall be fully redundant, including communication cards.

This communication shall not be based on IT equipment (i.e. servers). The use of open protocols, such as OPC, for interfacing with the PCS is not permitted for reasons of high obsolescence, cyber security and additional hardware & software.

- **SIS Maintenance Network**

This safety-related maintenance network shall connect nodes of the safety system to the SOE work station (SWS), Maintenance Work Station(s) (MWS) and Engineering Work Station(s) (EWS).

This network does not require to be redundant.

- **Remote I/O Network**

When remote I/O racks are required by project ICSS architecture then dedicated networks shall be provided with a redundant configuration. Each subsystem with remote I/O shall have its own dedicated network.

Intra-site communications (e.g. Wellhead platform and Central complex, remote CCR...) shall be subject to a specific study to address which networks require to be extended between sites and whether the networks remain fully within SII or whether they connect to other sites via SIE.

Main and back-up telecommunication means shall be addressed.

6. ICSS design

6.1 Life Cycle and Obsolescence Management

Facilities are typically designed with an expected design life in the order of 25 years. It is not practical to achieve such a design life for electronic based equipment without the requirement for upgrading.

The ICSS design shall therefore take into account the requirement that the system will require to be upgraded during the design life of the facilities. These requirements shall be incorporated from Basic Engineering.

Hardware and Software included in the ICSS Supplier bid shall be standard products actively being enhanced, produced and sold with a minimum field proven duration of one year.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 11 of 99

The ICSS scope shall be given specific attention to ensure all systems, components, software and individual elements and the respective running tools, test equipment, software and human skills can be maintained or replaced such that the original function and integrity of the whole ICSS can continue in an uninterrupted manner for the field life.

Strategy for managing obsolescence needs to be regularly updated as an integral part of the core functions:

- Design and development
- Sourcing and production
- In-service sustainability
- ICSS Supplier support.

As early as the bid stage, an obsolescence dossier shall be established and continuously updated during the lifetime cycle (refer to Appendix 7 - Documentation - for detailed requirements).

ICSS Supplier shall detail his lifecycle management strategy focusing on product obsolescence, support options and further migration alternatives.

ICSS Supplier shall guarantee that:

- ICSS components (including software and hardware) shall be fully supported and available over a period of at least 15 years after the SAT
- Maintenance services including availability of engineering services shall be available to support the ICSS during the plant life time.

A dedicated obsolescence and lifetime cycle management plan shall be established during the FEED/Basic Engineering in accordance with **GS EP TEC 007** to define which design provisions of the initial equipment are required to facilitate future revamps with minimal disturbance to the process, utilities, fixed cabling infrastructure, such as:

- Tie-in points for the future equipment, while the original equipment is still functioning
- Avoidance of common components for redundant safety, process and utilities related equipment
- Modularized design (i.e. strict segregation of equipment and functions) to allow a phased revamping without a complete plant shutdown
- Standard interface connectors allowing new cables to be plugged in between cabinets
- Allocation of sufficient revamping footprint space for the hook up of future equipment
- Definition of required size of access doors, outdoor access platforms, maneuvering space inside technical rooms, equipment handling facilities.

6.2 General Requirements

The ICSS shall be based on “off the shelf” standard products of a field proven design. It shall have a high degree of availability, reliability and tolerance to faults and fulfil the projects requirements.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 12 of 99

The system shall be engineered and designed to take into account the full life cycle from design, installation, commissioning, start-up, operations and maintenance through to decommissioning, as per [IEC 61511](#). The design shall particularly take into account any requirement of the facilities to undergo a phased commissioning and start-up where certain parts of the system may be operational whilst other parts are being constructed or commissioned.

ICSS Supplier shall demonstrate the ICSS capacity and flexibility to cope with the project requirements (I/O, interfaces to other control systems and packages, data processing including control algorithms, etc.) and the future extensions.

This demonstration shall also address the full integration of other control systems (e.g. subsea control unit), whose controllers shall be ICSS nodes, such control systems being provided by packages Vendors.

In such case, ICSS Supplier keeps the technical responsibility of the package control system and of its interface integration and definition in the ICSS communication network. Special attention shall be paid to the firmware release for all cards.

Equipment not used for the control and safety of the plant (e.g. Operator training simulator) shall not be connected to the ICSS communication network.

6.2.1 Safety

All control methods, circuitry and operating/maintenance procedures shall be designed to provide maximum safety for operating and maintenance personnel.

6.2.2 Maintainability/Availability

The system shall be designed to allow for easy maintenance.

Access to all equipment for maintenance shall be designed into the system from the start.

Failure and subsequent on line replacement of any module shall not affect the working of any other components or cause a system failure.

On line replacement of any faulty redundant module shall be performed without affecting the relevant application.

Changeover of any redundant faulty equipment (from duty to back-up and back-up to normal configuration) shall be performed without affecting the relevant application.

After any outage, the system shall automatically resume normal operation, including redundant configurations restart (e.g. logic solvers, communication interfaces/gateways), without any manual action.

The system shall incorporate a comprehensive set of diagnostic facilities to enable efficient fault detection. These diagnostics shall allow for the identification of faults down to individual module level. System fault repair will consist of the replacement of faulty cards.

The ICSS shall be equipped with all necessary software/hardware tools allowing accurate system trouble shooting, with clear displays showing the faulty elements, and management of the system communication networks including security aspect.

Project specification will address hot spare requirement.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 13 of 99

6.2.3 Standardisation

The system shall be designed in a modular fashion. The number of parts in each subsystem shall be minimised and standardised in order to reduce spare parts holding. Standardisation will also minimise the maintenance and Operator training requirements.

Standardisation shall apply to all software and hardware components (e.g. operating system, communication network equipment, etc.) of the subsystem.

6.2.4 Certification/Classification requirements of ICSS used on floaters

For floaters (FSO, FPSO, FPU) used for the production of oil and gas offshore, Classification Society requires that the control and safety systems are suitable to work with an ambient temperature of 45°C for equipment not located in air conditioned room, and 35-40°C for equipment installed in air conditioned room.

The control and safety systems equipment and any associated components (e.g. including switches, routers...) shall have to be designed for an ambient relative humidity of 95% at 55°C.

They shall be type approved by the project selected Classification Society.

Factory Acceptance Test of the control and safety systems shall be witnessed by the project selected Classification Society.

6.3 Hardware

Hardware design details are given in Appendix 4.

6.4 Operating system

The system shall be supplied with the latest up-to-date software release at the time of FAT. In addition, ICSS Supplier shall be required to make available all the updates during the guarantee period. A specific update procedure will be issued focusing on requirements and consequences during software upgrading installation.

All ICSS elements shall be time synchronized.

6.5 Interfaces and Industrial Communication Networks

All communication protocols, installation and cabling rules shall be compliant with the **GS EP TEL 170** standard. An addressing IP plan shall be prepared and submitted for Company approval.

Dedicated communication network management tools shall be provided by the ICSS Supplier and shall comply with the Company standard (**GS EP TEL 170**).

Time synchronization between all ICSS equipment shall be configured to allow events and incidents analysis.

ICSS shall be the clock master for time synchronization of all packaged units.

It shall be possible for any subscriber device to be added to, or removed from, the ICSS communication networks without having to shutdown the network and without impairing the safety and security of the system.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 14 of 99

Fibre optic cables shall be used to interconnect parts of ICSS when located in different buildings.

As a general rule, such links shall be redundant and run on different cable routings.

6.6 Interfaces with 3rd Party Systems

3rd party systems include any system residing within the SII domain.

6.6.1 Interfaces with P3 type packages

All data required for the safe operation of the package shall be transmitted between the ICSS and the package UCP by hardwired signals or using a serial link.

However, data only required for remote monitoring or historical analysis shall be transmitted to the PDS node, except when the quantity of data is so small that a dedicated connection to the PDS node cannot be justified. Company shall approve any such justification.

For further details refer to [GS EP INS 110](#).

6.6.2 Interfaces with P4 type packages

By their nature, P4 packages are not critical for the safe control and operations of the facilities.

P4 packages shall transmit their data to the PDS node to allow for the data to be analysed and trended by functions within the SIE domain.

The PDS node for P4 packages will generally be dedicated to this function and independent from other PDS nodes.

Refer to [GS EP INS 110](#) for further information.

6.7 Remote Maintenance and Diagnostic (RMD)

According to project specific requirements, vendors may require to have access to the ICSS systems remotely, from outside the Company SIE network for maintenance or diagnostic purposes. All remote access requirements shall require a specific study which shall be subject to approval by Company RSSC.

There are 2 types of Remote Maintenance and Diagnostic:

- **Type 1**

Remote Maintenance by monitoring of specific plant data for supervision and analysis purposes (permanent connection and read only).

- **Type 2**

Remote Diagnostic for troubleshooting, diagnostic or administrative purpose (Antivirus Patch, COTS update...). This access shall be limited in time (non permanent connection read/write function).

The general principle is that direct connections between the systems within the SII domain and the outside world via Internet for any purpose through the use of modems etc are forbidden.

The remote vendor shall gain access to Company SIE network via Company DMZ (i.e. Total Connect).

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 15 of 99

The remote vendor shall not have direct access to SII but access via intermediary servers.

Any form of remote maintenance or diagnostics on Safety Instrumented Systems (PSS, ESD, FGS, HIPS) is forbidden.

For ICSS, type 1 is not applicable. Relevant plant data is made available via PDS system to functions within the SIE domain.

Type 2 may be required for PCS, depending upon project specific requirements.

Type 2 access shall only be given to vendor with specific means and procedures. These means and procedures shall allow the site personnel a permanent and full control of the remote access operation, initiation and stop. Logging of all operations shall be performed.

A specific remote access server shall be installed in SII/SIE DMZ. This RMD server will receive/transmit data from/to system within SII domain. Remote access vendor will then be able to communicate with the RMD server through an SSL connection via Company DMZ (Total Connect).

Refer to [GS EP INS 135](#) for additional information and requirements.

6.8 Application software(s) development

Standard Functions are developed to define the Hardware interface and Software requirements for individual instrument and equipment.

They shall be based on requirements of the [GS EP INS 150](#), [GS EP INS 196](#), [GS EP INS 197](#) and [GS EP INS 198](#).

However, Company subsidiaries may use their own library of Standards Functions if already developed.

These Standard Functions are key requirements for the development of the Functional Analysis which would then define how these functions are applied to specific process/utility and safety sub systems.

The Functional Analysis shall be the basis of the development of the application software(s) and shall be established in accordance with the [GS EP INS 131](#).

Applications software(s) shall be designed, programmed and documented to facilitate maintenance, modification and future expansion. For this reason it shall be of a modular structure. However, simply breaking a large program down into arbitrary cards will not satisfy this requirement.

Special attention shall be paid to the functions split within the different controllers belonging to the same subsystem to avoid:

- Any process shut-down when losing one controller (or a part of it)
- Too many data exchanges between controllers.

Particular care shall be taken for equipment which control parallel process lines, or main and backup equipment.

Controllers shall handle applications and data flow during normal and upset conditions while continuing to meet the specified performance, safety and availability criteria.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 16 of 99

The displays shall be developed according to Appendix 8 “Design of the control display system” and the above mentioned standards functions specifications.

Standard Functions, graphic displays, application software(s), shall be consistent whatever the concerned equipment throughout the plant.

6.9 ICSS database

Instrument database software shall be used as an engineering tool in designing the ICSS system e.g. allocation of Input/output.

The ICSS Supplier is responsible for all ICSS fields, part of this database. This shall include not only the “system” database but also include the wiring from the marshalling termination strips up to FTA associated to I/O cards.

ICSS data shall be incorporated into the project instrumentation database as per requirements of **GS EP INS 103**.

ICSS database shall also include Subsea Equipment data (where applicable) and packages data, exchanged with the ICSS.

7. Specific Requirements per Subsystem

7.1 Emergency Shut-Down System

7.1.1 Safety Integrity Level

All loop components (logic solver, I/O cards, FTA's, relays, etc.) shall be SIL certified as defined in **GS EP SAF 261** alternative 1 (§ 6.3.2 Logic solvers).

7.1.2 Availability

The required availability of the ESD system shall be as specified in the project Instrument and Control Philosophy It shall be at least 99.99% based on an MTTR of 4 hours, unless otherwise specified in the project specifications.

7.1.3 Specific Requirements

The ESD system shall be based, as a minimum, on a fully dual fault tolerant programmable system (e.g. tolerance to simultaneous faults of one I/O module and one CPU). It shall be based on fail safe design built using high reliability and high availability equipment.

The system shall include controller nodes with associated I/O cards and communication cards.

Depending on the size of the system, multiple nodes connected to the dedicated SIS safety networks may be required.

Interfaces between packages and ESD system shall be hardwired.

Field I/O shall be monitored by I/O loop monitoring.

The ESD system shall be fully independent of the PCS. ESD controllers shall interface to the PCS controller via the SIS-PCS data exchange network in order to allow data to be displayed on the ICSS OWS. This interface shall also provide reset facilities from the OWS to ESD.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 17 of 99

An Engineering Work Station (EWS) shall be provided to allow access to configuration. Note all modifications to configuration shall be fully verified offline and be in compliance with the change control procedures prior to downloading to the controllers. This EWS shall only be connected to the ESD system controllers as necessary. It shall not be a permanent installation.

A Maintenance Work Station (MWS) shall be provided, based on project requirements, to provide instrument maintenance functions. Inhibit maintenance functions shall be provided on MWS or OWS depending upon project specifications.

A Sequence of Events Station (SWS) shall be provided in order to collate and analyse the SOE files from the controller nodes.

Diagnostic facilities shall be able to run automatically and manually. These facilities shall include the ESD system including controllers, I/O cards, communication cards, networks, as well as field input/outputs.

Matrix panel

An ESD panel shall be incorporated in the control room Operator Control Desk. This panel shall be hardwired directly to the ESD system bypassing the ICSS Operator stations.

This panel will include main ESD levels (e.g. ESD0, ESD1 and ESD2) and EDP (emergency depressurisation) status for each fire zone and push-buttons to initiate main ESD trips and EDP per fire zone.

In addition it will include maintenance inhibit key-switch, if applicable depending on the project specific control philosophy.

A "Black Start Key" shall allow utilities to be restarted after a total black out. This key shall allow restoration of the DC power, when set to "ON", and must be switched back to normal before production can resume. Its status shall be monitored.

7.2 Ultimate Safety System (optional)

7.2.1 Safety Integrity Level

The SIL requirement, as per [IEC 61508/IEC 61511](#), shall be as defined by [GS EP SAF 261](#) (§ 6.5.4 USS) or the Project SIL study.

All loop components (logic solver, FTA's, I/O cards, relays, etc.) shall meet the safety function SIL requirement.

7.2.2 Availability

The required availability of the USS shall be as specified in the project Instrument and Control Philosophy It shall be at least 99.99% based on an MTTR of 4 hours, unless otherwise specified in the project specifications.

7.2.3 Specific Requirements

The principle of the USS is that it is a simple stand alone system with a minimum number of I/O which will provide a back-up to a small number of manual ESD actions.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 18 of 99

Its inputs will be ESD pushbuttons located in the control room defined by safety philosophies to back-up ESD1 & 0. These shall be the same buttons that are connected to the ESD system. The USS functionality will be transparent to the Operator.

Upon reception of a trip command the USS will initiate a timer to allow time for the ESD system to carry out the ESD function. Upon timeout the USS shall trip its outputs which will generally be connected to power supplies for safety valves (ESDV's, BDV's) and main process equipment, thus initiating the fail safe shutdown of the facilities.

The USS system shall be based on a non-programmable system. It shall be of a fail safe design built using high reliability, high availability and fault tolerant equipment. It may interface with the PCS via serial links in order to report status and diagnostic information to the ICSS HMI.

A minimum number of I/O shall be utilised and the logic treatment kept to a minimum.

The USS will provide individual maintenance inhibit and isolate functions for each of its loops and shall be fully self-testing; all status and faults concerning these facilities will be reported to ICSS.

7.3 Fire and Gas System

7.3.1 Safety Integrity Level

All loop components (logic solver, I/O cards, FTA's, relays, etc.) shall be SIL certified as defined in the **GS EP SAF 261** alternative 1 (§ 6.3.2 Logic solvers).

7.3.2 Availability

The required availability of the FGS shall be as specified in the project Instrument and Control Philosophy. It shall be at least 99.99% based on an MTTR of 4 hours, except if otherwise specified in the project specifications.

7.3.3 Specific Requirements

FGS Design

The FGS shall be based, as a minimum, on a fully dual fault tolerant programmable system (e.g. tolerance to simultaneous faults of one I/O module and one CPU). It shall be of a non-fail safe design utilising "energise to trip" principles using high reliability and high availability equipment.

The System shall include Controller nodes with associated I/O cards and communication cards.

Depending on the size of the system, multiple nodes connected to the dedicated SIS safety network may be required.

Interfaces between packages and FGS shall be hardwired.

Any I/O which is non failsafe shall be line monitored.

The FGS system shall be fully independent of the PCS system. The FGS controller shall interface to the PCS controller via the SIS-PCS data exchange network in order to allow data to be displayed on the ICSS OWS. This interface shall also provide reset facilities from the OWS to FGS.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 19 of 99

Interfaces between FGS and ESD system for executive actions may utilise the SIS safety network as long as it has been specifically designed for such a purpose and has the appropriate SIL rating approval. Alternatively hardwired signals shall be used.

If the same Manufacturer and technology are elected for ESD and FGS system then EWS, MWS and SWS may be common for both safety systems and connected via the SIS maintenance network. Alternatively a dedicated SIS maintenance network shall be provided for FGS with its own dedicated EWS, MWS and SWS.

Diagnostic facilities shall be able to run automatically and manually. These facilities shall include the FGS system including controllers, I/O cards, communication cards, networks, as well as field input/outputs.

Matrix panel

An FGS matrix panel shall be incorporated in the control room Operator Control Desk. This shall be hardwired directly to the FGS system bypassing the ICSS Operator stations. This panel will include one common status indication for each fire zone. In addition pushbuttons to initiate release of extinguishing agent (CO₂, Foam, etc.), manual start and selection facilities of the fire water pumps shall be provided.

Pushbuttons may have double contacts when initiation required direct to the equipment (ie one contact to FGS, 2nd contact direct to equipment).

7.3.4 Offices Buildings/Living Quarter

Addressable fire detection system may be provided for Offices Building or Living Quarter.

This addressable fire detection system shall be SIL 2 certified and shall comply with IMO SOLAS requirements for FPU/FPSO.

This system will comprise of a network of addressable smoke, heat and MAC loops reporting back to a central control unit.

In case of activation of any detector, the system shall identify the exact location of the detector and report it via the ICSS Operator workstations.

The system will not perform executive actions. The addressable fire detection system shall interface the PCS by serial link and the plant FGS by hardwired links for executive actions.

The gas tight & fire dampers shall be controlled by the FGS. Limit switches shall be hardwired to FGS.

7.4 Process Safety System

7.4.1 Safety Integrity Level

All loop components (logic solver, I/O cards, FTA's, relays, etc.) shall be SIL certified as defined in the **GS EP SAF 261** alternative 1 (§ 6.3.2 Logic solvers).

7.4.2 Availability

The required availability of the PSS shall be as specified in the project Instrument and Control Philosophy. It shall be at least 99.97% based on an MTTR of 4 hours, unless otherwise specified in the project specifications.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 20 of 99

7.4.3 Specific requirements

PSS design

The PSS shall be based on a programmable system. It shall be based on fail safe design built using high reliability, high availability and fault tolerant equipment.

I/Os module redundancy will be required for critical I/O as per Project specifications.

Interfaces between packages and PSS shall be hardwired.

The system shall include controller nodes with associated I/O cards and communication cards.

Depending on the size of the system, multiple nodes connected to the dedicated SIS safety network may be required.

The PSS system shall be fully independent of the PCS system. The PSS controller shall interface to the PCS controller via the SIS-PCS data exchange network in order to allow data to be displayed on the ICSS OWS. This interface shall also provide reset facilities from the OWS to PSS.

Interfaces between PSS and ESD system for executive actions may utilise the SIS safety network as long as it has been specifically designed for such a purpose and has the appropriate SIL rating approval. Alternatively hardwired signals shall be used.

If the same Manufacturer and technology are elected for ESD and PSS system then EWS, MWS and SWS may be common for both safety systems and connected via the SIS maintenance network. Alternatively a dedicated SIS maintenance network shall be provided for PSS with its own dedicated EWS, MWS and SWS.

Diagnostic facilities shall be able to run automatically and manually. These facilities shall include the PSS system including controllers, I/O cards, Communication cards, networks, as well as field input/outputs. Field I/O shall be monitored by I/O loop monitoring.

7.5 Process Control System

7.5.1 Availability

The required availability of the PCS shall be as specified in the project Instrument and Control Philosophy. It shall be at least 99.95% based on an MTTR of 4 hours, unless otherwise specified in the project specifications.

7.5.2 Specific Requirements

The PCS shall ensure a safe, reliable and efficient control and monitoring function for the facility.

It shall also provide the “backbone” of the ICSS communication network and thus allow the Operator to view and manage the entire facility from the HMI located in the control room.

Redundancy shall be required for critical equipment such as controllers, power supplies, main PCS network and associated communications cards. I/O cards do not require being redundant as long as the overall availability of the system is met.

The system shall include controller nodes with associated I/O cards and communication cards.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 21 of 99

Depending on the size of the system, multiple nodes connected to the PCS network may be required.

A dedicated EWS shall be provided. This shall be fully independent of any safety system EWS. It shall connect to the PCS using the PCS Network. A single EWS shall generally be unique on the PCS network.

MWS functionality shall be provided within specific defined OWS, normally located in Central ITR.

7.6 Human Machine Interface (HMI)

7.6.1 General arrangement

All Operator Work Stations shall offer the same control and command capabilities, and access the entire plant, whatever the concerned subsystem (fire and gas, emergency shutdown, process safety or process control).

Multiple levels of security access shall be provided as per **GS EP INS 150** (typically engineer, method, maintenance, Operator and visitor) protected by hardware or software key:

In addition to the workstations used by Operators in the CCR, a workstation may be installed in each instrument technical room for plant maintenance and operation activities, as per project requirements.

The HMI functional description shall be split into two main parts:

- Operator interface
- System maintenance functions (e.g. system diagnostic mimics including packages communication links status).

7.6.2 Operator interface requirements

The Operator interface shall require the following main functions:

- Process and unit overviews
- Dynamic graphic displays for the entire ICSS and packages
- Trend/historical displays for all analogue values of the ICSS, including packages
- Alarm management displays (priorities, acknowledgement by operating area, alarm annunciator with direct access to process displays, first-up alarm, alarm masking)
- Events displays (Operator actions, status, inhibition and forcing status, diagnostics and abnormal states)
- Reporting (logs, material/energy reports, event lists, etc.)
- Printing facilities (event, display, etc.)
- Retrieval facilities for events and data historical.

7.7 Historian server

Redundant servers shall provide trends/historical for display on the Operator Work Stations.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 22 of 99

Main functions required are:

- Automatic collection of data (data samples taken at intervals ranging from 1 second to 15 minutes, average interval: 1 minute) with pre-processing algorithm (average, min., max.). It includes all ICSS and package data: process values, states, events and analysis data, calculated values, maintenance data, manual input, test-run data, test separator data
- 6 months duration storage (note 1)
- Automatic archiving of data on a high-density storage medium (periodic archiving) (note 1)
- Synchronous graphic representation of multiple data curves mixing analogue values and events for incident analysis
- Data storage back-up facilities.

Note 1: When PDS is requested (refer to the next paragraph), storage duration of the historian server may be reduced (typically 4 weeks) and automatic archiving of data will not be requested.

7.8 Process Data Server (PDS)

PDS will be implemented when required by Project specifications.

PDS and its interfaces (i.e. data acquisition nodes) shall be designed and developed in accordance with **GS EP EXP 131** requirements.

Any writing or inbound traffic to the ICSS system shall be forbidden. The interface shall fully comply with cyber security requirements as per **GS EP INS 135**.

Refer to Appendix 1 - ICSS General Architecture.

PDS shall allow communication between the Industrial Information Systems (SII) domain and the Company office network (SIE) through firewall.

It shall continuously collect and record data from ICSS, 3rd Party Systems and packages as per Project requirements.

Refer to **GS EP INS 110** for detail requirements for package communication links with the PDS.

Failure of the PDS shall have no impact on the overall functioning of the ICSS.

Number of concurrent users and license size including spare for future modifications/extensions shall be defined in project specifications.

8. Specific functional requirements

8.1 Safety-Related Sequence of Events

Safety-related SOE Work Station (SWS) shall be provided to automatically collect time-stamped events from SIS controllers.

The different SOE files from all SIS controllers shall be brought together by the SWS to ensure an overall Sequence of Event function for the plant.

Special attention shall be paid to the quantity of events to handle with the risk of events loss s further to an avalanche of events due to high level shut-down, leading potentially to de-energization of SWS (for instance in case of gas detection in ITR).

Upon resumption of power the original events leading up to the shutdown shall remain available to ensure post-event analysis is possible.

Retrieval, selection and printing facilities shall also be supplied.

The resolution of SOE recording is generally 100 ms, unless otherwise specified in the project specifications.

Safety-related SOE will remain independent of PCS Operator Work Stations.

As per project specifications, some time - stamped event data may be required by the PDS. This would typically be for calculations & monitoring of critical equipment, such as ESDVs where closing time logging will be required. This logging function shall not be done by the safety system but be a function within the PDS.

Communication between PDS and SWS shall be part of the cyber security risks assessment, as per **GS EP INS 135**.

In case some particular alarms and events from specific packages are deemed critical for adequate plant operation, then a dedicated Basic Engineering study shall identify a suitable solution which shall be subject to Company approval. In that case, the above shall be limited to a few essential (grouped) events.

Refer to **GS EP INS 110** for detailed requirements.

8.2 Maintenance tools requirements

The ICSS shall have the following functionality as a minimum in order to allow for an efficient maintenance of the system:

- OWS shall provide:
 - Maintenance displays providing detailed displays showing the diagnostic of all subsystems parts, package systems, package digital links, power supplies and communication networks.
- EWS shall provide:
 - Facility for configuring and downloading any part of the ICSS application software(s) On-line downloading of software applications shall be easy and unrestricted under password protection, without impact to the plant facility
 - Hardware management database
 - Application software(s) release management
 - Application software(s) simulation, testing and debugging with user-friendly interfaces
 - Software backup management (including configuration, operating system and communication network)
 - Automatic documentation for the whole application.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 24 of 99

- MWS shall provide:
 - Safety system diagnostic displays. It shall monitor the whole safety system: controllers, I/O and communication cards, networks components as well as field input/outputs loops. Those diagnostics shall be able to run automatically and manually
 - Maintenance status of field loops
 - Maintenance inhibit commands management as alternative; refer to Appendix 2 of this Specification.

8.3 Instrument Management System

When required by Project specifications, the Instrument Management System will provide secured access to “smart” devices (instruments and valves) and present on-line information (diagnostic, performance, parameters) to maintenance personnel.

The full Hart functionalities, described hereafter, shall be provided only for non-safety related devices connected to “pass through” I/O cards.

Access to configuration & calibration of safety related devices from the IMS, and in addition from the Safety System itself shall be forbidden and locked. Hart data shall be available for trouble shooting and diagnostic only.

Data collection from P3 type packages is optional feature, and as defined in the project specifications.

Facility will be provided to include conventional devices through manual registration.

IMS shall also support Third Party software for partial stroking test of safety related ON/OFF valves when SVTS facilities are used.

Refer to **GS EP INS 110** for detail requirements on package communication links with the IMS.

Available functionalities will include, but not limited to:

- Device database
- Browser function
- Device configuration & calibration
- Loop check
- Export facility
- Audit trail management
- Self-documentation
- Troubleshooting
- Alarm report.

8.4 Alarm Management Function

Alarm management shall be provided within the OWS.

Such functions will comply with the [EEMUA publication no. 191](#) and the [ISA 18.2](#) requirements.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 25 of 99

It will provide as a minimum:

- Facilities for categorisation, filtering, suppression and prevention of avalanche during upset while still providing adequate indication
- Help system with alarm-related texts or hyperlinks
- Alarm report / lists (active, suppressed alarms...)
- Alarm analysis (e.g. "top 10").

9. ICSS System Performance

The minimum performance requirements shall be under the worst conditions (note 1):

Operator command from HMI interface to ICSS output	1 sec max
Display of an alarm on the HMI	1 sec max
Execution of any control loop algorithm	1 sec max
Execution of any complete process logic algorithm in the same controller (from reading the input values from the input modules to changing states of the outputs)	1 sec max (note 3)
Execution of any complete logic algorithm in the same safety or F&G controller (from reading the input values from the input modules to changing states of the outputs)	250 ms max (note 2 & note 3)
Time to exchange data between PCS controllers	1 sec max
Time to exchange data between safety or F&G controllers	500 ms max
Update of data on the active display	1 sec max
Calling up of any active element on a display	1 sec max
Calling up of any display	2 sec max
Additional communication time for data exchanged with P3 type packages	1 sec max
Time synchronization between ICSS elements	± 25 ms

Depending on project requirements, for specific high speed functions (such as electrical control functions when optionally performed by the PCS), faster response times (down to 10 ms) may be required from some ICSS components.

Note 1: The worst conditions shall include:

- 50% of I/O reported with a changed value at each scan
- 100 alarms generated every second.

The project ICSS specification shall define the number of simultaneous users (i.e. OWS).

Note 2: A maximum cycle time (or "throughput" time) of 500 ms may be accepted when the input change occurs just after the inputs reading.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 26 of 99

Note 3: cycle time values shall take into account the final configuration (i.e. with project installed spares I/Os/ modules).

10. Packages interface

In general, packages which have their dedicated control system shall be supervised and controlled at a higher level from the ICSS.

Serial links shall be used for communication between UCP and PCS, although hardwired links shall be used for small amounts of data points (less than 25).

In addition, critical data between UCP and PCS (e.g. speed control, feedback for rotating machinery) shall be hardwired.

The communication protocol of the serial link will be standardized on a single protocol for the whole project/facility.

Unless the project specification(s) state differently, the default design rules for serial interface with the PCS are:

- Using an industrial communication protocol with the lowest possible inherent obsolescence: not using protocols requiring an intermediate server(s) with operating system: instead communication cards with embedded operating system using a standard and field proven protocol such as ModBus shall be used
- The use of custom-built protocols, software and hardware is not permitted
- By default a TCP/IP link over Ethernet; serial RTU type links are only permitted when TCP/IP communication ports/cards are technically not possible / available on the market
- As an alternative, Profibus DP may be considered
- A direct connection to the ICSS communication network is permitted only if identical controllers are used within the package UCP and for the PCS
- In case of redundant links: each link shall have completely segregated components (incl. communication cards or controllers) to avoid common-mode failures.

The use of open protocols, such as OPC, for interfacing with the PCS is not permitted for reasons of high obsolescence, cyber security and additional hardware & software.

Concerning the availability of the serial link, the default rules are:

- Single (simplex) serial link: by default
- Redundant serial link: when the loss of HMI in the CCR is considered not acceptable
- Dual-redundant serial link: shall only be used for links in case the loss of communication induces a package shutdown.

Whether the loss of HMI in the CCR is considered not acceptable (therefore requiring a redundant link) shall be defined during Basic Engineering phase by a multi-disciplinary team (typically Operations, Process, Safety and ICSS engineers), and can be re-assessed during Detail Engineering as deemed necessary.

The input & output links between UCP and Safety systems (i.e. the PSS, ESD and F&G systems) shall always be hardwired.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 27 of 99

11. Spareage Requirements

The ICSS shall be designed to facilitate possible extensions. It shall be sized to include all components (hardware and software) needed for future extensions (over and above spare parts):

- Networks and communication capacity Note 3
- Installed input/output (per I/O type and per subsystem) 10%
Note 1
- Spare space for additional slots per subsystem cabinet 10% - minimum 2 slots
Note 2
- Processing capability (per processor or controller) for each part of the system 30%
- Operator interface capacity for each part of the system 30%
- Available space inside cabinets per subsystem - Note 2 1 rack
- Power supply capacity 40%

Note 1: Marshalling cabinets shall be provided with terminals to accommodate spare installed I/Os.

Those 10% spare will be distributed all over the subsystems cabinets.

Minimum 2 slots apply to each subsystem cabinet.

Note 2: Marshalling cabinets shall be provided with spare space to accommodate such extensions.

Note 3: The communication network architecture shall be designed to allow for the above required spareage.

The ICSS shall be sized in accordance with these values at installation start-up, unless otherwise specified by project requirements.

12. Factory Acceptance Test (FAT)

This section covers the requirements for inspection and testing after completion of fabrication and prior to shipment.

Testing requirements are described in Appendix 5.

13. Documentation

Refer to Appendix 7.

14. Training courses

A complete set of training courses shall be included in the scope of the project, covering all different aspects (operation, maintenance and configuration).

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 28 of 99

15. Specific Cases

15.1 PSS combined with ESD system

As per **GS EP SAF 261**, the presence of a PSS is not a compulsory requirement and it is acceptable that in certain cases the functions normally achieved by the PSS are carried out by the ESD system. This is typically the case for very simple installations and/or very low complexity packages.

15.2 FGS combined with ESD system

As per **GS EP SAF 261**, it is acceptable that in certain cases the functions pertaining to FGS and ESD system are performed by common equipment. This is typically the case where low numbers of I/O are being handled. However, in these cases it shall be ensured that there is no impact to the reliability nor availability of the F&G and ESD functions. Even if common equipment is used, I/O cards and associated racks, along with the application software(s), shall remain segregated and dedicated to their function.

15.3 Requirement for USS

As per **GS EP SAF 261** an USS system is not compulsory if the design of the ESD system is such that the SIL requirement is achieved by the ESD system and FGS alone (for instance simple wellhead platforms).

A specific study shall be carried out to fully justify and demonstrate that an USS system is required.

16. Reference System

A reference system might be considered to allow modifications testing and de-bugging.

Project specification will define the boundaries and minimum equipment to be provided.

Such system shall be standalone and consequently not connected to any ICSS communication network (control, safety and engineering).

This system shall be engineered and designed in the same way than the ICSS, including same hardware and software release.

All ICSS requirements shall apply (e.g. testing, cyber security related constraints, documentation).

Design and supply of integrated control and safety system

Rev.: 10

Effective date: 11/2012

Page: 29 of 99

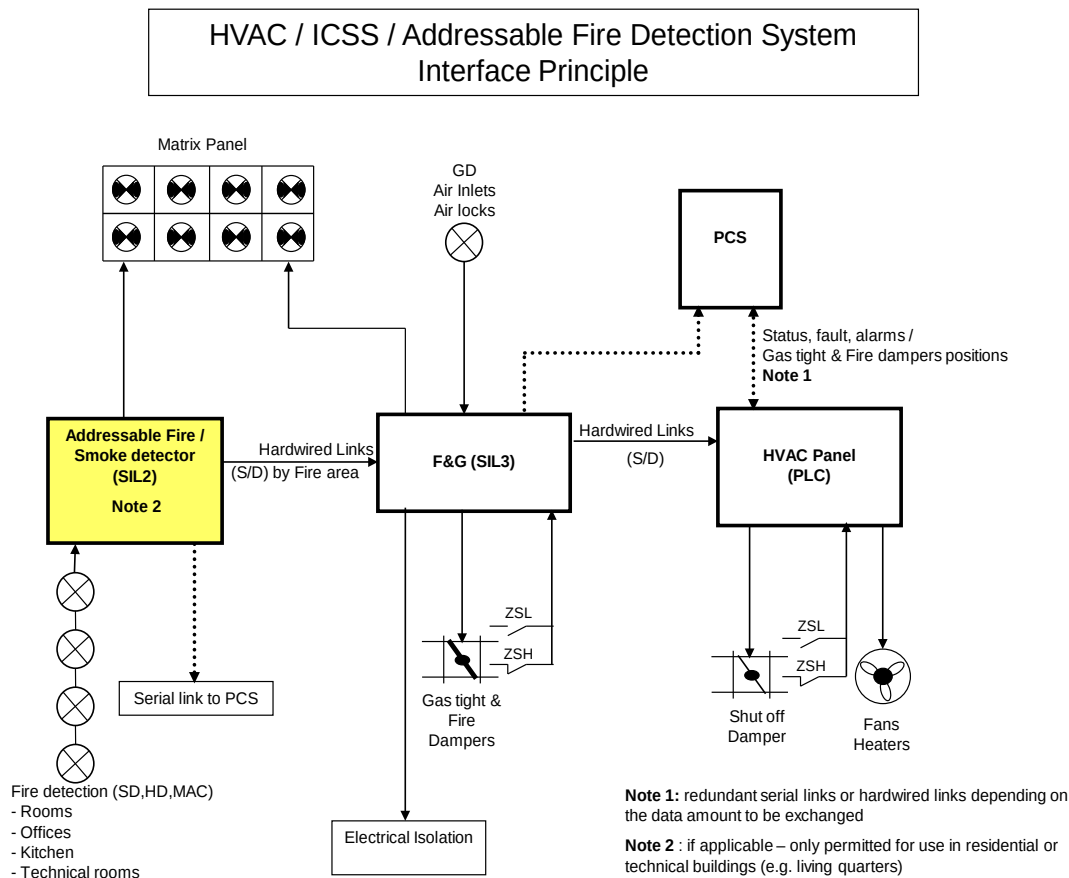
Bibliography

IEC 60079	Parts related to the Electrical apparatus for explosive gas atmospheres
IEC 60364	Parts related to the Low-voltage electrical installations and Electrical installations of buildings
IEC 61131-3	Programmable controllers - Part 3: Programming languages
GS EP SAF 371	Emergency control facilities

This document is the property of TOTAL S.A., it contains confidential information which may not be disclosed to any third party, reproduced, stored or transmitted without the prior written consent of TOTAL S.A.
The information contained in this document does not substitute to the applicable laws and regulations.

Appendix 2 HVAC / ICSS / addressable fire detection system

INTERFACE PRINCIPLE



General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 32 of 99

Appendix 3 Function descriptions

1. Alarm processing

The main alarm sources include:

- Measurement exceeding threshold
- Status change
- Valve / motor discrepancy
- Input / Output out of range
- Deviation between process and safety transmitters measuring the same process parameter (e.g. pressure, temperature and level)
- System or communication failure
- Abnormal state (as per Project functional Analysis).

Alarms do not initiate safety action.

Alarms shall be classified over 4 different levels depending on their criticality.

The alarm shall be acknowledged from only one Operator station, the acknowledgement shall be broadcasted to all other stations.

A "silence button" shall be required.

Alarm masking disables the audible alarm and indicator blinking. However colour change on the mimics will be maintained.

Refer to **GS EP INS 150** for detailed alarm management description and to **GS EP INS 196** - Chapter 5 - RAI for deviation alarm requirements.

2. Maintenance Functions

This section defines maintenance inhibit and input enable/disable principles, this last command being used only when transmitters/detectors are processed by voting logics.

In case of brown field development and potentially new development within the same asset, the existing maintenance inhibit procedure will be maintained, unless otherwise specified in the project documents (e.g. operating philosophy, instrumentation and control philosophy).

3. Definitions

3.1 Maintenance inhibit

Process-related instrument

Maintenance inhibit command of the transmitters assigned to the PCS will be applied to all associated thresholds. Therefore, a single inhibit command will be available.

The consequent actions are specified individually in each Standard Function.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 33 of 99

Safety-related instrument

When several thresholds are used in the Safety Logic Diagrams, each threshold will be inhibited individually.

Activation of maintenance inhibit command will prevent the input signal to be processed by the Safety Bar logic.

3.2 Input enable/disable

When included in voting logic, the enable/disable command will prevent the input signal to be processed by the voting logic (necessary for calibration purpose for instance).

The primary voting logic arrangement shall automatically be reconfigured in accordance with the downgraded voting logic arrangement defined in the Voting Logic Standard Function, as per **GS EP SAF 312**. This is applicable to all fire and gas detectors and to some specific safety-related transmitters.

When the input enable/disable is active, the fault status will be forced.

This allows simultaneous calibration of input signals related to the same voting logic without initiation of the voting logic output signal (refer to the Voting Logic Standard Function).

3.3 Maintenance inhibit facilities

3.3.1 ESD / PSS maintenance inhibit

A first maintenance inhibit MASTER hard wired key-switch shall enable the maintenance inhibit function and provide security control against accidental inhibit operation. No maintenance inhibit can be initiated until this MASTER key-switch is set in the ENABLE position.

All active maintenance inhibits will be reset when this key-switch is switched to the DISABLE position.

Adequate authority level shall operate this MASTER key switch.

A second maintenance inhibit hard wired key-switch shall allow the transfer of the individual maintenance inhibit command to the ESD system and PSS during a limited time interval (by default 30 minutes). This inhibit key switch will be set in the maintenance inhibit while the above MASTER key-switch is in the ENABLE position. Generally, this inhibit key switch is operated by the control room Operator in line with the relevant work permit requirements.

All individual maintenance inhibit commands will be set /reset using the Operator Work Station (OWS).

Use of Maintenance Work Station (MWS) may also be considered as an alternative, as per Project Instrumentation and control philosophy.

In this case, redundant stations maybe provided and installed in the same physical location to ensure inhibit function continuous availability.

Access to maintenance inhibit commands shall be access restricted (e.g. maintenance mode).

The individual maintenance inhibit command will be latched in the safety system logic.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 34 of 99

It will stay set until one of the following conditions is met:

- The maintenance inhibit is reset from either OWS, or MWS
- The maintenance inhibit MASTER key-switch is switched to the DISABLE position.

3.3.2 FGS maintenance inhibit

The above principles will equally apply to FGS maintenance inhibits.

3.4 Input enable/disable facilities

The above principles will apply.

3.5 Hardware Implementation

The inhibit MASTER key-switch and the second maintenance key-switch shall be common to maintenance inhibit and input enable/disable functions.

Those key-switches will be hardwired to one ESD controller and then dispatched to all over safety controllers (ESD, PSS and FGS) through the SIS safety network. Hardwired links between safety systems may be considered as an alternative where the SIS safety network is not available.

Both key-switches shall be mounted on the ESD/FGS matrix panel in the CCR and line monitored.

The inhibit MASTER key-switch will be of “stay put” type with key reset and protected by lift flap, unlike the inhibit key-switch of a spring return type.

3.6 Maintenance inhibit & input enable/disable logging

The status of the above key-switches (i.e. MASTER key-switch and maintenance key-switch) shall be logged by the FGS / PSS / ESD system as event.

Maintenance inhibit and input enable/disable status shall be classified as events, as well.

Their number and their duration shall be available through the Operator Working Station and recorded.

Report and dedicated display shall be generated periodically and upon Operator request showing all current inhibitions.

It shall include also maintenance inhibit related to all packaged units, even if they are not set from the ICSS.

4. Start-up inhibit function

This command shall be designed to allow temporary inhibition of some inputs in ALARM, in order to defeat the associated safety logic and reset the concerned safety bar (e.g. low pressure safety threshold at pump outlet when the pump is stopped).

It will be initiated by the Operator or automatically, depending on the Project Functional Analysis.

It will be logged whatever the mode of initiation.

Refer to [GS EP INS 198](#) - Chapter 4 - Safety Bar Standard Function - for detailed description.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 35 of 99

5. First-up fault

The first-up fault is the first of a burst of alarms initiating trip or safety action.

It shall be recorded and time stamped.

Refer to **GS EP INS 198** - Chapter 4 - Safety Bar Standard Function - for detailed description.

6. Invalidity measurement detection

Invalidity detection shall be performed on all analogue I/Os.

Associated safety-related actions shall be as per Project Safety concept and Analysis Functional: e.g. trip initiator of the concerned Safety Bar or/and alarming.

7. Timer

All timers shall be configurable and shall have a default value.

Their values might be displayed as per the Project Functional Analysis and Standard Functions.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 36 of 99

Appendix 4 Hardware design

1. Generalities

The hardware of all parts of the ICSS shall be designed and configured to carry out the functions described in this specification. Moreover special consideration shall be given to:

- Environmental (temperature, humidity, vibration, etc.) and transport conditions
- Design of the cooling requirements for equipment mounted in enclosures
- Protection of the electronic components from static electricity and electromagnetic radiation; all hardware components of the ICSS shall allow use of High Frequency Communication tools such as walkie-talkies, and shall comply with [IEC 61000](#)
- Earthing and powering of all parts and components, in compliance with Company reference document [GS EP INS 101](#) and [GS EP INS 107](#).

Each ICSS input/output shall be individually protected against electrical failure.

All digital outputs shall have a configurable failure position (hold, close or open).

Dedicated marshalling cabinets shall be used per system (ESD system, PCS, PSS, FGS, etc.). The grouping of terminal blocks and termination panels shall be done in a way to follow process unit arrangement.

2. Power supply

The Project Basic Engineering shall define the voltage source type(s) distributed to the ICSS and associated earthing regime (i.e. IT, TT or TN-S, of which IT is the default regime offshore).

Unless specified differently by the project specifications, the ICSS shall be designed to be fed by:

- 2 off independent AC UPS power supplies (designated UPS-A and UPS-B)
- 1 off normal AC power supply.

The UPS power supplies shall be used in a 2 x 100% configuration serving all control, safety related equipment, while the normal power supply shall be used for non-critical equipment such as lighting, power sockets, ventilation and heating (unless considered critical).

The incoming UPS power feeders shall not be bonded together: a strict galvanic separation must be ensured.

Generally, each work stations shall be fed by one UPS feeder (alternate sources for alternate work stations).

Each power input to the ICSS shall be powered via dedicated breakers and protections circuits such that no single system component failure causes loss of power supply to other components. The design of the electrical distribution shall include the short circuit and selectivity calculations. Power supply failure shall be alarmed and logged.

I/O and system components power distribution shall be designed to avoid common mode failure, especially for field devices processed by voting logics or associated to main and back-up process & utilities equipment.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 37 of 99

Appendix 4

I/O cards power supplies shall be individually protected.

When not powered by the I/O cards, field devices shall be fed by two redundant dc power supplies either through FTA (Field Termination Assemblies), or through field terminal blocks.

Single rectifier bridge diode blocks joining 24Vdc supplies are forbidden; separate 24Vdc diodes and heat sinks shall be used.

Gas and Fire detectors power supplies shall be redundant and designed for 100% of the load in nominal mode with 40% spare capacity as per section 11 of this specification; inrush-current may not be considered.

Isolation transformer/converter should be provided in the cabinets on the incomers since the provided UPS AC voltage source is of a floating type.

The instruments shall be powered with 24V DC referenced to earth from the ICSS.

All power supplies/converters and miscellaneous associated components shall be of the industrial type and DIN rail mounted.

3. Communication network components

All network components (hubs, switches, routers, etc.) shall be of industrial type: either rack or DIN mounted with redundant power supplies.

They shall not downgrade the whole reliability.

They shall be validated and fully supported by ICSS Supplier.

4. Field Remote I/O Requirements

When specified, remote I/O's shall comply with the requirements included in the § 5.2 of this document.

Remote I/O's are considered as "smart junction boxes". They consist of I/O cards, power supplies, communication bus interface and field terminals enclosed in boxes or cubicles according to the number of sensors or actuators they have to cope with.

Maintenance facilities shall include:

- Replacement of I/O or power supply modules under power
- Diagnostic data available at the ICSS maintenance/Operator stations in the same way as for standard I/O's
- Parameters of smart transmitters available in technical rooms for commissioning purpose.

5. Cabinets and cabling

Two types of cabinet shall be provided:

- System cabinets including CPUs, I/O cards, communication cards, power supplies, etc.
Each Subsystem (ESD, PCS, PSS and FGS) shall have dedicated cabinets, except for specific cases described in the § 15 of that specification.
- Marshalling cabinets equipped to receive all process and safety signals from and to the field, the electrical room, or other technical rooms or to receive signals from other systems such as package control systems, etc.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 38 of 99

Appendix 4

Subsystems shall have dedicated marshalling cabinets.

When available space inside the technical room is limited, combined marshalling/system cabinets might be studied. However, physical segregation between marshalling and systems sections and easy access to any equipment/device/terminal requirements shall be fulfilled.

Such arrangement shall be submitted to Company for approval.

Special consideration shall be given to:

- The accessibility of all parts and components, in particular the design and layout for easy removal and replacement of components
- The internal markings (every type of component such as I/O cards, CPU, power supplies, links at each side, termination blocks, etc.) and outside cabinets with Traffolyte labels.

These cabinets shall be equipped with lifting rings, lift off doors with internal drawing pockets, removable side panels, key lockable, internal lighting activated by door limit switch, forced cooling, sub-base and grounding bus bars (IPE, IE, ISE if needed, see [GS EP INS 101](#) and [GS EP INS 107](#)).

FGS and Safety system cabinets will be fitted with doors including safety-glass windows, with a non-glazed part on the door bottom to allow for the installation of an air inlet filter.

All communication cables shall be screened.

Cable trays shall be sized to keep at least 30% spare space after use of spare I/O's.

Refer to [GS EP INS 108](#) for technical / plant rooms detailed requirements.

5.1 Marshalling cabinets

Marshalling cabinets shall be equipped with Field Terminal Blocks (FTB, mirroring the field junction box) and Field Termination Assemblies (FTA, mirroring the I/O cards).

Marshalling cabinets shall be used to cross-wire signals between FTB and FTA.

Inter-connection between ICSS and marshalling cabinets shall be via pre-wired and pre-tested system cables with multi-way connectors.

The marshalling cabinet shall be provided with equipment necessary to supply the field instruments, when not supplied directly from the ICSS I/O cards.

Where necessary as per project requirements, intrinsic safety barriers, galvanic isolation devices, surge protection devices, interposing relays (plug-in type with sockets and sealed) shall be mounted on vertical rails. When used for safety functions, they shall meet the SIL requirements.

Field terminal blocks in marshalling cabinets shall be of cage clamp interruptible or equivalent terminals, with the necessary polarity distribution, switching and protection, test points, and earthing terminations.

Facilities to connect smart handheld configurator devices or instrumentation management system shall be provided.

Signals segregation (cables, routings) shall be compliant with [GS EP INS 107](#) requirements.

Routing for all IS circuits shall be segregated from all other circuits and separately identified.

Routing of all signal circuits shall be segregated from all power circuits.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 39 of 99

6. I/O board specific requirements

6.1 ICSS Card Protection

Each ICSS card power supply shall be overload protected.

When instruments (such as flowmeters, analysers and gas detectors) have their own power supply or use an external power supply, analogue I/O cards shall be protected by fuse on the input signal.

When an analogue input board powers the instrument on a separate (3rd) wire that wire shall be protected by means of fast acting fuse.

Otherwise each input and/or output shall be individually short circuit protected and shall have electrical insulation between the ICSS and the facility.

I/O cards shall be designed so that a short circuit or high voltage on one input (or output) shall not induce a fault on any other input (or output) on the same module.

Individual fast acting fuses will be rated appropriately (e.g. 63 mA for 4/20 mA input loop).

Galvanic isolation shall be provided as a minimum for:

- Analogue inputs from analyzers or AC powered sources devices
- All signals exchanged between different systems (for instance between PSS and PCS, between UCP(s) and ICSS)
- Instruments supplied by different power supplies and hardwired to the same FTA.

6.2 I/O Card types

All I/O ICSS cards shall be provided with dedicated connectors for connections with their Field Termination Assemblies (FTA) in the marshalling cabinets.

The analogue input and output signal range shall be 4-20 mA (except for specific cases such as flowmeters and specific sensors using 0/4 mA or 20/22 mA for dedicated purposes).

The Digital output shall be able to switch a minimum of 24 V dc with 1 A. If not possible the necessary relays will be installed in the FTA. For PSS, FGS and ESD system, these relays must be taken into account in the system reliability and availability calculations.

6.3 I/O assignment

The following basic assignment rules shall be applied:

- Spare for the different types of inputs or outputs (digital, analogue) shall be considered on separate I/O cards
- One output shall be provided per device (e.g. valve, motor, breaker, fire damper, etc.)
- All I/O loops which control either parallel process lines or equipment, or main & back-up equipment shall be hardwired to separate I/O cards
- Detectors / transmitters configured in 2°°N voting logic shall be assigned to a minimum number of cards (Y) to avoid voting logic activation in case of a single faulty acquisition card including the associated FTA.

Y = minimum cards quantity	1°2	2°2	2°3	2°N with N> 3
ESD application	Not applicable	Not applicable	3	N/2 rounded up
FGS application	2 For H2 detection only	2 For smoke detection only	2	N/2 rounded up

- All I/O loops associated with main/backup equipment shall be hardwired to separate I/O cards
- An allocation diagram shall be issued to show the assignment of all I/O with tag number on each system, rack, and I/O board.

7. Work Station Hardware requirements

The Operator and maintenance workstations shall include at least:

- A display unit with a high resolution colour graphic screen of at least 21", capable of displaying mixed alphanumeric and graphic data
- A sealed membrane keyboard with alarm annunciator LEDs
- A track-ball or mouse equipped with push buttons
- Input/output mass storage units (floppy disk, DVD, CD-ROM drive), this equipment and the CPU shall not be directly accessible as required by the **GS EP INS 135**
- All Operator workstations hardware shall be identical
- The printer(s) shall be of the monochrome laser type. They shall have a storage buffer of not less than 1 Mbyte
- The color screen copier(s) (or color printer) shall be multi-port devices capable of providing a screen copy for a predetermined number of workstations.

The Engineering work Station for PCS shall be as the above requirements except for QWERTY type keyboard in place of membrane. Whereas, EWS for safety systems shall be a laptop, not normally connected to the system with its own dedicated printer.

All ICSS components including the control system, safety systems and packages shall be controlled from a single Operator interface in the control room. This interface shall include:

- Operator Workstations on a dedicated control desk built following good ergonomic practices
- An ESD matrix panel
- A fire and gas matrix panel
- A communication panel
- A large video display connected on a workstation as per project specification
- Specific operator interfaces for dedicated equipment if necessary.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 41 of 99

Appendix 5 Tests Requirements

1. Testing Methodology

The testing activity shall include the following phases:

- Standard Functions Tests
- Design Validation Tests (DVT)
- Factory Acceptance Tests (FAT)
- Integrated Factory Acceptance Tests (IFAT)
- Yard /On site Acceptance Tests (SAT)
- Sustained Performance Tests.

ICSS Supplier shall demonstrate that ICSS hardware supply and configuration meets the project requirements at each of the above testing stages.

The ICSS arrangement during IFAT will reflect the final ICSS site configuration/architecture, including all ICSS communication networks and interfaces with SIE or other networks. Different IFAT configurations will be implemented, as per project architecture:

- For each single facility
- Interconnection of different offshore facilities
- Interconnection of different offshore and onshore facilities (onshore plant or CCR).

This means that a full IFAT shall be performed for each facility and then additional IFATs as necessary. The IFATs shall focus principally on communication network extensions, data transmission, remote monitoring/control /diagnostic/troubleshooting and general ICSS performance, in normal mode as well as in downgraded situation.

In case of extensions or brown field developments, the actual load shall be simulated to ensure actual performances will not be impacted by the extension.

The tests will include equipment not part of the ICSS project scope of supply (e.g. Package Vendor UCPs, Servers, Routers, Firewall, Telecommunication equipment...) which will be provided by other Vendors, as per Project specifications.

2. Testing Preparation

ICSS Supplier shall give Company notification of the readiness for any tests one calendar month prior to the beginning of the tests, unless specified differently by the Project.

Before commencement of tests witnessed by Company, ICSS Supplier shall produce evidence that the internal tests based on the approved Test plan have been carried out successfully by submitting the results of his own testing.

ICSS Supplier shall prepare a Test Plan including:

- Full set of test procedures for approval by Company
- Test organization and reporting

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 42 of 99

Appendix 5

- Software modification control procedure
- Testing Schedule including Internal tests
- Resources and Equipment list
- Test log book
- List of all documentation required for the tests.

The FAT and IFAT programs shall be organized as per Project specifications in order to allow for gradual commissioning/start-up activities of the facilities.

ICSS Supplier shall provide all necessary tools and consumables required for the proper performance of the tests. This includes all necessary measurement, control and simulation equipment, such as but not limited to:

- Hardwired Inputs / Outputs Simulation: ON/OFF switches simulate DI (Digital Input), potentiometers to simulate AI (Analog Input), Lights or LEDs to simulate DO (Digital Output), Amperemeter to simulate AO (Analog Output)
- Communication network load and serial link analyzers
- Dummy equipment
- Fibre optic patch panel, patch cords...).

The capacity of such tools shall be as per project requirement (e.g. sufficient for a whole process sub-system, complete fire zone).

ICSS Supplier may be required to conduct several tests, which may be considered as non-standard by the ICSS Supplier.

ICSS Supplier shall arrange to have his Vendors present during the tests and guarantee that the team present during the tests is competent for the scope of the testing.

In addition to Company and Contractors, Certification / Classification Authority may also be required to witness ICSS FAT/IFAT.

Testing shall be performed using project documents in latest AFC status (Approved for Construction) approved by the Company. They shall include, but not be limited to:

- FDS
- Standard functions specifications
- Package standard functions specifications
- Data communication exchange tables
- Functional analysis / Control narrative / sequence for process functions including utilities and interfaces with P3 type packages
- Cause & Effect matrixes and Shut-down Logic Diagrams for Safety functions including Fire and Gas
- I/O database
- PID (Piping and Instruments Diagrams).

3. Recordings and corrections follow-up

All tests shall be recorded in the Test log book, including test number record, test name, duration, test results, events, punch list including failure details, and comments added manually to supplement test documentation.

All errors / discrepancies detected during the tests shall be corrected during the concerned test.

In case of major finding, the testing may be stopped until the correction has been implemented.

ICSS Supplier shall repeat the concerned sequence testing and/or perform any re-testing to verify the correct operation of the system. Furthermore, ICSS Supplier shall demonstrate that no other section of the application has been impacted by the modification; else this re-testing shall be extended to those sections.

After all tests the ICSS Supplier shall issue complete test reports with completed test sheets, copies of displays, printouts etc as necessary. All test sheets will be scanned and available on an electronic PC format.

Impacted documentation shall be updated to reflect the system configuration at the end of the IFAT.

ICSS Supplier shall ensure that a strict software control procedure is applied so that once one test is completed and accepted the configuration software is frozen.

4. Documentation compliance

At each phase of testing, the full compliance of the ICSS shall be checked according to the project documentation and purchase order.

All the documentation produced by the ICSS Supplier will be checked and must be as per the supplied equipment and software configured.

It is the responsibility of the ICSS Supplier to update as necessary all the documentation to reflect the "as built" hardware and software.

5. "Standard Functions" Tests

All project "Standard Functions" shall be tested prior to any application configuration.

These tests shall demonstrate the full functionality of Project Standard Functions in normal and abnormal conditions (loss of power supply, communication network failure, default value, cold start...).

They shall include the verification of:

- Internal logic and interfaces with other Standard Functions
- HMI (mimics, face plates/detailed mimics, alarms and events list, trends...).

The actual equipment/devices selected for the project shall be assembled, with no simulated equipment, to ensure full compatibility. It shall include, but not be limited to:

- I/Os cards
- Field Termination Assemblies
- Interfaces devices (e.g. IS barriers, Surge Protection Device, Hart multiplexer, relays, ON/OFF valves Partial Stroke Testing interfaces modules...) as per project requirements.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 44 of 99

Transmitter/F&G detector/ Control valve positioner/detector of each type.

6. Design Validation Test (DVT)

At an early stage of the ICSS engineering, ICSS Supplier shall demonstrate that the proposed design meets project requirements.

If firmware or software versions differ between DVT and FAT, the DVT shall be performed again during the FAT.

ICSS Supplier shall propose to Company a list of critical subjects to be tested as per project specifications.

This test shall include the following, but not be limited to:

6.1 ICSS functionalities

- Redundancy of any equipment including power supplies
- Change-over and hot swap
- System reaction in downgraded situations:
 - Loss of power on the different ICSS components such as, but not limited to: controllers & logic solvers, main racks, I/O racks, remote I/Os racks, communication cards (PCS communication network, safety networks, I/O bus, safety / process communication), switches, routers, optical converters...
 - The system behavior shall be monitored when resumed to normal situation/configuration.
 - This analysis will encompass the following, but not limited to: bumpless take-over where redundant or TMR configuration applies, response time, alarming, automatic restart...

The system diagnostic facilities and alarm view shall be checked for each test.

- Power supply grounding, earth fault monitoring system and localization.

6.2 ICSS subsystems interfaces

- Alarm and Events server interfaces with ICSS subsystems and packages P3 (where applicable)
- IMS interfaces with ICSS subsystems (i.e. PCS, PSS, ESD and FGS)
- PDS interfaces with the ICSS communication network focusing on redundancy, capacity/limitation and interfaces with historian server if applicable).

6.3 Capacity and performance tests

These tests shall address HMI, servers, communication network and interface equipment, process and safety controllers with simulation of the calculated estimated data transfer load.

Minimum “freetime” of control and safety controllers shall be determined.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 45 of 99

6.4 Packages systems Interface tests

ICSS Supplier shall demonstrate that all interface links with 3rd Party systems (e.g. P3 type packages UCPs, Subsea Control Unit (SCU)...) are working satisfactorily. It shall be the Supplier responsibility to plan and manage all aspects of these tests.

Those tests will include as per project specification, but not be limited to:

- PCS interfaces with P3 type packages
- PDS interfaces with ICSS communication network
- ICSS /SCU interface
- IMS interface with P3 type packages
- IMS interface with Partial Stroke Test devices of ON/OFF safety valves (where applicable).

If several packages have interface links with the same characteristics, the DVT will only be performed once.

These tests shall encompass:

- Communication test itself
- Response time
- Redundancy and changeover with recovery to normal situation
- Black start with a specific focus on redundant equipment (e.g. data synchronization between master and slave...).

Different categories shall be defined with its own interface characteristics:

- Type and firmware version
- Programming tools version
- Protocol
- Cable type and wiring
- Data organization: structure, naming rules...

6.5 Cyber-security tests

As per requirements of the **GS EP INS 135**, the DVT shall demonstrate how cyber security requirements will be implemented on ICSS equipment and communication networks. A simplified configuration is accepted: one workstation of each type, one control network and one safety network with all specific network devices and one controller of each type. However when redundancy is specified for the project, the tests shall be performed in a redundant configuration.

ICSS Supplier shall define a "hardware standard configuration" to be tested, and once validated, to be propagated to all corresponding equipment.

This hardware standard configuration shall be validated for each type of equipment (switch, OWS, EWS, controller...) and for all communication networks.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 46 of 99

These tests shall include the following parts, but not be limited to:

- Remote access where applicable
- Audit of operating system configuration
- Audit of communication network configurations
- Audit of configuration settings (access control list, permissions, passwords...)
- Identification of each type of controller
- Possible vulnerabilities (list of UDP & TCP ports open, active services on each controller, robustness to Layer 2-7 attacks).

7. Factory Acceptance Test (FAT)

The Factory Acceptance Test shall be a series of tests to demonstrate that all Subsystems (e.g. PCS, ESD, FGS, PSS, HMI, IMS, PDS...) meet the project design and functional requirements.

FAT shall be carried out for each subsystem.

Project HMI shall be used for the FAT of the safety systems (i.e. F&G, ESD and PSS).

Prior to the start of the FAT, ICSS Supplier shall install the latest version available on the market of the firmware, software and operating systems.

7.1 Mechanical Inspection

The Mechanical Inspection of all cabinets and equipment (e.g. ESD/F&G matrix panel) shall include the following minimum requirements.

- Visual inspection of quality, layout, labels, paint finish, lighting, sizing, wiring, cabling, routing, spares, accessibility, etc.
- Quantity of equipment in accordance with the Purchase Order (including consumables and spare parts)
- Spareage capacity
- Conformity to the documents and project requirements.

7.2 Hardware Tests

The Hardware Panel Typical Test shall include the following minimum requirements.

- Insulation tests
- Heat dissipation tests,
- Continuity tests
- Earthing tests.

The following tests shall also be carried out during the Hardware Tests to confirm the Radio frequency Interference performance:

- Test 1 with 5W hand held radio transmitter operated at 1 meter from each side panel/door with all doors and covers in place. = No effect.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 47 of 99

Appendix 5

- Test 2 as above with doors open but covers, if any, in place. = No damage to the equipment and no effect on operation. Continuous values shall not change by more than 1% full-scale deflection.
- Test 3 result as above with a randomly selected input or output module per cabinet on an extended card, if appropriate, and with all CPU and memory cards and theirs covers in place = same effects as Test 2.

7.3 I/O Test

This test shall apply to 100% of hardwired inputs/outputs using simulator panel hardwired to marshalling cabinets or Field Termination Assemblies.

The demonstration of the correct configuration of the loop shall be made in checking all relevant parameters (e.g. scale, engineering units, control & alarm & trip thresholds, alarm & events list, historical...) by means of the project HMI (i.e. displays and associated face plates configured for the project).

7.4 Logic/Control Tests

The Logic/Control Tests shall include:

- 100% functional test of all control logic and sequences
- 100% functional test of all safety system logic including Fire and Gas functions as per Shut-down logic diagrams and C&E matrices
- Full testing of interlocks and realignments where data is exchanged between different subsystems (e.g. PCS and PSS) or between ICSS and packages UCPs (measurements, interlocks, permissive status, safety trip status, clock synchronization...)
- Verification of all mimics and displays including mimics' structure, call up and chaining.

7.5 System Tests

System tests shall include all tests which have not been fully tested during the tests described above.

In addition, tests described in the above paragraphs shall be repeated in case of any change of firmware or software release since DVT or Standard Functions test.

These tests shall include but not be limited to:

- Electrical power tests
 - Voltage variation tests
 - Each daily test will start with an overall power switch-off during a few minutes. Overall diagnostics shall be performed after this interrupt.
- "Black start" procedure test: after any outage, the system shall automatically resume normal operation without any manual action
- Subsystem configuration and download
- Subsystem on line re-configuration
- Redundancy, "hot swap" and recovery functionalities to be completed as necessary

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 48 of 99

- System reactions in downgraded situation to be completed as necessary
- Full testing of all interfaces to be completed as necessary.

8. Packages P3 systems interface tests

Interface tests with P3 type packages shall be fully tested.

This test is not only a communication test, but a complete test for all required interfaces.

It can be performed, depending on project requirements and schedule:

- Either at ICSS Supplier premises with the assistance of the Package Vendor, or
- At package Vendor premises with the ICSS Supplier assistance.

In this last case, the ICSS Supplier shall supply the equipment necessary for the package control and monitoring from the ICSS HMI (through project mimics) using project equipment and not simulators. In addition, others functions shall also be tested, such as acquisition of data by IMS, Alarm & Events server and PDS respectively, as per projects requirements.

This ICSS Roll-around Test Unit (RATU) will include, for instance, controller(s), communication module(s), Operator Work Station & Engineering Work Station, and all equipment and servers necessary as per project requirements (e.g. IMS, PDS, Alarm & Events server), all packaged in cabinet(s) or enclosure for easy transportation to the Package Vendor premises.

The interface test will include:

- Data communication test
- Exchanged data verification (e.g. signal type, tags, addresses, engineering units), flow charts or logics tests including interlocks
- All ICSS HMI aspects through ICSS Standard Functions implementation: monitoring, alarms list, first fault, maintenance inhibit...
- The different operating modes (e.g. local and remote, automatic and manual)
- Clock synchronization
- Communication failure management:
 - Bumpless change-over in case of faulty communication channel when redundant communication applies and communication recovery
 - Black start.
- Communication response time and data flow load
- Hardwired signals between ICSS and UCP
- All exchanged data with the different servers and routers (IMS, PDS, Alarm & Events server) as per project requirements.

This test shall be based on the package interface specification.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 49 of 99

9. Integrated Factory Acceptance Test (IFAT)

The IFAT shall be performed after the completion of the subsystems FAT in the following sequence depending on the project requirements:

- For each individual offshore and onshore facility of the project, all ICSS subsystems shall be interconnected together including interfaces P3 type package UCPs. In case some UCPs will not be made available due to schedule constraints, the corresponding load and interfaces will be simulated.

If different ICSS sections or domains have been defined (e.g. Topsides, Utilities, Hull and LQ, Subsea Control Unit, LNG train), all of them shall be interconnected together.

- For the whole field when the project includes different locations/facilities (e.g. wellhead platform, process facility, storage facility, remote onshore central control room), all ICSS shall be interconnected together through telecommunications means.

The IFAT shall include as a minimum:

- All integration aspects (e.g. communication networks, nodes hook-ups, database...)
- All communication interfaces testing (redundancy, configuration, software and hardware)
- All common/shared subsystems, including as a minimum:
 - HMI including reports and print-out
 - IMS
 - PDS
 - Alarm Management system
 - Safety-related SOE and merged Alarms and Events
 - Historians
 - Clock synchronization.
- Performance tests and response time with all subsystems/equipment interconnected with the full load
- Spareage requirements checking
- Verification and test of all Cyber Security requirements as described in the [GS EP INS 135](#) not performed previously
- Test of all back-up /restoration procedures (e.g. operating system and communication network configuration, application software, historian database...).

At the end of the IFAT, Company shall conduct a number of days of operation tests. For this purpose, the Supplier shall make free to Company all interconnected systems and provide necessary assistance.

During the IFAT, all documentation and licenses shall be reviewed. The documentation shall be based on the project requirements.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 50 of 99

10. OTS / ICSS interactions

For medium/large size projects, an OTS (not part of this General Specification) is very likely to be required, based on:

- Dynamic process models
- ICSS simulation software and application
- Operators and instructor interfaces.

The OTS will be used to help validation of the control and safety system configuration such as:

- ICSS database (e.g. alarms, set points)
- Process control strategies and ICSS configuration & application, especially for complex algorithms such as OCWR (Overall Control Wells and Risers) and offloading system.

As the functionality and accuracy of the OTS increase during the project execution, intermediate and successive validation phases will be performed if required by the project specification.

11. Additional equipment testing

When a Reference system is required, it shall be tested as well to demonstrate it meets the project requirements. The above tests related to FAT shall be performed.

Operating system, software release, hardware and firmware versions, software application shall be the same as for the ICSS.

Spare parts shall be fully checked and functionally tested.

Consumables delivered with the ICSS shall also be visually checked (quality, quantity, conformity, etc.).

12. Yard Acceptance Test and On site Acceptance Test

ICSS Supplier will be expected to assist with unpacking, installing and hook up the system ready for commissioning.

Yard / On site acceptance test will therefore demonstrate that all equipment are correctly powered up, fully operational to allow loop commissioning tests to start and that no alteration has occurred due to transportation, installation and assemblies activities.

The Site Acceptance test (SAT) will consist of a series of tests to demonstrate that:

- All equipment have not been affected during transport and handling
- Equipment has not been affected during transport and handling
- Equipment has been correctly installed and assembled
- All equipment/software has been delivered including consumables and spare parts
- All documentation relevant to the ICSS has been delivered
- Powering and earthing are fully operational
- All software is correctly installed and revision noted
- System integrity has not been affected in transport

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 51 of 99

Appendix 5

- Systems are fully functional
- All devices, cards, cables and connectors are well fastened and running properly
- Redundancy functionality is fully operational
- All systems and faulty alarms are cleared
- Field interfaces are fully functional,
- Communication interfaces and networks are fully functional,
- Back-up systems are fully operational.

13. Sustained Performance Test

This test shall be performed after the completion of the Onsite test and commissioning. Its goal is to verify that ICSS reliability & availability meet contractual requirements. Test duration will be as per project contractual requirements.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 52 of 99

Appendix 6 Functional Design Specification (FDS)

1. Definition

The ICSS FDS shall describe all hardware and software, in sufficient depth so as to enable Company to verify that the system design meets the requirements of the system specification.

The FDS shall be considered as a major primary document, which shall be developed continuously during the ICSS engineering with the initial revision issued at the start of the detailed engineering.

No equipment procurement or software work shall commence before the relevant section of the FDS has been approved.

2. Content

FDS shall be issued for each ICSS subsystems.

2.1 ICSS Design

The document shall provide an overview of the specific project ICSS architecture and description of all hardware and software components.

FDS shall include as a minimum, but not limited to the functional description of the following aspects:

- ICSS overall overview
- ICSS architecture
- ICSS communication network architecture with all components
- Cyber security requirement
- Sub System overview
- Sub System architecture with all components
- Sub System functionalities
- Sub System hardware specifications
- Sub system software specifications
- P3 type packages interfaces description
- Sub Systems integration requirements
- Electrical power supply design and distribution
- Swap-over strategy (for system upgrade only)
- Spares philosophy.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 53 of 99

2.2 ICSS / Subsystem performances and limitations

The FDS shall clearly specify the limitations of the system design, not only at the overall system level, but also at the level of hardware and software modules, so that the system constraints are clearly identified.

The FDS shall include a detailed description of response times, load factors and the overall system availability on the same basis as in the proposal.

The document shall clarify the behavior of each sub system under defined fault conditions, so that the effects to subsystem or total failures are clearly understood.

Fault conditions shall encompass the loss of electrical power on any component, the fault of any communication network and any communication with the P3 type packages.

2.3 Validation

The validity of the FDS shall be demonstrated through the different tests described in the Appendix 5 - Tests Requirements.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 54 of 99

Appendix 7 Documentation

1. Preamble

For the purposes of this Appendix the term “document” shall be deemed to include all documents and drawings.

The below list of minimum document requirements is intended to define the minimum requirements related to documents to be provided by the ICSS Supplier and issued for Company review or approval.

The Vendor standard documentation table of contents shall be marked with applicable or not applicable status, as to reflect the delivered system.

The list is not exhaustive and any document necessary for the execution of the work shall be prepared by Supplier and shall be made available for Company review if requested.

The required final documentation shall be included in one of the three dossiers listed below, in accordance with the attached list:

- Design Data Dossier
- Certification Data Dossier
- Operating & Maintenance Manual.

Supplier shall prepare and submit for approval a specific detailed Supplier Document Register and Schedule (SDRS) on which he shall have marked, based on the classification guidelines herein and the attached lists, the classification of the documents (for approval or review) and the associated planned issue dates of these documents.

Supplier is required to mark each document issued, with a stamp for “Documentation Class” and to enter the appropriate class number. Where the assignment of a particular class is in doubt Supplier shall refer to Company for agreement.

The following legends apply to the minimum document requirement lists:

- Class 1 - for approval: Supplier may not proceed until Company has given written approval.
- Class 2 - for review: Supplier may proceed if Company has made no comment after fifteen (15) working days from receipt by Company, except if specified otherwise in Project requirements.
- Class 3 - for reference only: Company reserves the right to comment but Supplier may continue with his work.

2. Generalities

Documentation shall include Supplier standard documents and project documents.

The supplied documentation shall be of a coherent structure, consistent from one document to the next. Documents shall be fully indexed and cross-referenced.

Use of conventions in engineering drawings, software flow sheets, and descriptive text, shall be stated explicitly or reference made to the relevant standards.



General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 55 of 99

Appendix 7

The issue number and date of issue of all system documentation shall be stated on each document. Changes from previous issue shall be identified.

The final revision will be “as commissioned” status.

Engineering tools shall provide on line documentation of the system configuration and maintenance and operation user's guide based on electronic files on a CD-ROM.

All documents and drawings issued by the Supplier shall be produced in an electronic format compatible with recent and standard office computer software.

Final documentation shall be supplied to the Company on a CD-ROM in the quantity defined by the project.

Additionally, a paper copy may be required as defined by the project.

Unless mentioned by the project, all documentation shall be in English language.

3. Document list

Item	Description	Class
	Engineering Dossier	
	General	
EG1	ICSS Overall architecture (FDS)	1
EG2	ICSS architecture (FDS)	1
EG3	ICSS communication network architecture with all components (FDS)	1
EG4	Sub system overview (FDS)	1
EG5	Sub system detailed architecture (FDS)	1
EG6	Obsolescence Dossier	1
EG7	Cyber Security Specification (as per GS EP INS 135) (FDS)	1
EG8	Functional Design Specification structure	1
EG9	Functional Design Specifications per subsystem (e.g. PCS, HMI, IMS, PDS...)	1
EG10	Alarm & Event Specification (FDS)	1
EG11	Historian Server Specification (FDS)	1
EG12	Alarm Management Specification (FDS)	1
EG13	Clock Synchronization Design (FDS)	1
EG14	Communication network Management Specification (FDS)	1
EG15	Package Interface Specifications (FDS)	1
EG16	Operator Interface Design including Graphic Display Specification (FDS)	1
EG17	Reports Specification	1
EG18	System load and Performance calculations with spare capacity	2
EG19	System Earthing Design and Arrangement (FDS)	1
EG20	System electrical power supply design and arrangement	1
EG21	ICSS component numbering Specification	2
EG22	Black Start Procedure	2
EG23	Reliability/Availability Data	1
EG24	Typical Standards per loop diagram per subsystem	1
EG25	Back-up procedures	

	Hardware Engineering	
EH1	Hardwired I/O schedule & Assignment (subsystem, cabinet, rack, card, channel)	2
EH2	Rack Loading Schedules	2
EH3	Console Arrangement & Lay out & Nameplates	1
EH4	ESD / F&G Matrix Panel Arrangement & Lay out	1
EH5	Control Desk Arrangement & Lay out & Nameplates	1
EH6	Cabinet / Panel / Enclosure Arrangement & Layout & Nameplates	1
EH7	Earthing System Drawings	2
EH8	Electrical Power Requirements (start-up, average, rating)	2
EH9	Heat Emission Data Sheet	2
EH10	Weight Data Sheets	2
EH11	Noise Level Data Sheets	2
EH12	Equipment Data Sheets (e.g. FTAs, IS barriers, relays, power supplies, patch panels, routers...)	2
EH13	Instrument Datasheet	2
EH14	Bill of Materials/ Material Take Offs	2
EH15	Cables schedule	2
EH16	Cables Specification / Data sheet including fibre optic cables and connectors	2
EH17	Cable Block Diagrams	2
EH18	Field Termination Assemblies Details	3
EH19	Marshalling Cross-Wiring Diagrams	2
EH20	Interconnection Diagrams including connectors and cable terminations	2
	Software Engineering	
ES1	PCS Standard Functions Specification	1
ES2	PSS Standard Functions Specification	1
ES3	ESD Standard Functions Specification	1
ES4	F&G Standard Functions Specification	1
ES5	Package Interface Standard Function Specification	1
ES6	Serial link Map Definition/Data communication exchange tables	1
ES7	Completion of Instrumentation Database including ICSS database	2
ES8	Alarm and Trips list	2
ES9	I/O list per subsystem	3

ES10	Graphic Display Sketches	3
ES11	Organic Analysis	3
	Testing (refer to § 2 of the Appendix 5)	
T1	Test Plan	1
T2	Test Procedure	2
T3	Test Reports	2
T4	Calibration Sheet	3
	Packing and Shipment Preparation	
P1	Packing, Marking And Shipping Procedures	2
P2	Preservation and Site Storage Procedures	2
P3	Handling Procedures	3
P4	Delivery Notes / Bills of Lading	3
P5	Packing Lists	3
	Site assistance	
S1	Installation and Assembly/Hook-up drawings	1
S2	Spare parts for Start-up and Commissioning	2
S3	Yard / Site Acceptance Test procedure	1
S4	Yard / Site Acceptance Test reports	3
	Certification Dossier	
C1	SIL Certificates	3
C2	SIL Loop Calculations where applicable	2
C3	Hazardous Area certificates	3
C4	Third Party Hazardous area Certification	3
C5	Marine Type Classification Certificates	3
C6	Intrinsically Safety Loop Calculations where applicable	3
C7	RFI/EMI certificates	3
	Maintenance & Operating Dossier	
M1	Maintenance & Operating Dossier Structure & Index (Note 2)	1
M2	Obsolescence Dossier (to be completed at the field start-up phase)	2
M3	System Software & Application Software User Manual	3
M4	Hardware User Manual	3
M5	Maintenance Software Manual	3
M6	Maintenance Hardware Manual	3

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 59 of 99

Appendix 7

M7	SIL dossier	2
M8	Spare parts list (for 2 years)	2
M9	Close Out Report	2
M10	List of all Software including release number and version	3
M11	List of all Licenses with products references and Owner's name	3
M12	Source Programs and Application Software on external storage	3

Note 1: Functional Design Specification (FDS) will be formed by multiple documents as per the requirements of Appendix 6. Some of them have been identified as such in the above list.

Note 2: Maintenance & Operating Dossier Structure & Index shall be completed as per project maintenance engineering requirements. It shall include documents already included in other Dossiers, such as but not be limited to: Black Start procedure, Back-up procedures, FDS, Marshalling cross-wiring diagrams...

All references to parts and materials shall be clear and accurate to facilitate identification and purchase orders.

4. Obsolescence Dossier Content

The Obsolescence Dossier shall be established as per requirements of the **GS EP TEC 007** considering the complete life cycle including:

- Bid stage
- Design phase
- Project delivery phase
- Operation & maintenance phase.

Based on the project lifetime, the ICSS Supplier will evaluate:

- Cost of obsolescence
- Resolution costs for obsolete system or main sub system.

The contents of the dossier shall include as a minimum:

- Equipment Inventory
 - Bill Of Material (BOM)
 - . Comprehensive list with identification of all components up to the card level including Third Party equipment (e.g. routers, switches, servers)
 - . Software releases.
 - Obsolescence status of all main equipment, components and software:
 - . End of spare parts availability
 - . End of support (i.e. design engineering support, technical after sale support)
 - . Product Change Notice (PCN)

Design and supply of integrated control and safety system

Rev.: 10

Effective date: 11/2012

Page: 60 of 99

Appendix 7

. Product Discontinuance Notice (PDN)

. End of Life (EOL).

- Supplier support
 - Availability
 - Location.
- Replacement strategy of all components and associated software
- Replacement schedule.

All above data shall be tabled in a database or spreadsheet application.

The obsolescence dossier shall be further complemented during the detailed engineering stage and shall detail all aspects of equipment life cycle.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 61 of 99

Appendix 8 Design of the control display system

1. Scope

This appendix sets out the basic principles involved in defining the content and organising the displays in the control screens.

Note: Below some parameters (mostly colours) are on a **grey background**. This indicates that they are indicative and may be changed in project specific specifications.

The display system associated with the supply of a package must, as far as possible, follow the concepts set out below or the specific project specification if this exists.

The report [SIREP-WIB-EXERA No. M 2656 X 98 part 2](#): "Ergonomics in Process Control Rooms" Design guideline could be used.

1.1 Classification of displays

The displays available to the Operator are classified according to their functions:

- Mimic displays
- Sequence displays
- Group displays
- Adjustment displays
- Alarm displays
- Inhibition or forcing displays
- Graphic history displays
- System maintenance displays.

The group, adjustment, alarm and history displays are mainly preformatted views.

However, the mimic, sequence and inhibited or forced device displays must be fully defined to provide a representation specific to requirements.

1.2 Display content

1.2.1 Mimic displays

These displays are created with all the information needed to control a process; they are the Operator's main working displays.

It is felt that the maximum number of variables supplied by mimic should not exceed 30.

The content of the displays is based on a three-level hierarchical organisation of the control display system:

- General view of the field
- General view of the installation
- Detailed view of the installation.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 62 of 99

To this general hierarchy is added a system of differentiation by function:

- Process control
- Safety logic diagram
- Management of fire and gas detection systems (fire extinguishing included)
- Management of utilities.

All these displays could have direct inter-link, for example from a process view it is possible to jump to the associated safety or utility view.

1.2.1.1 General view of the field

1.2.1.1.1 Description

There is only one general view for each field, pooling all process information.

The display comprises blocks, each representing an installation in the field. Each block contains the main parameters of the installation.

1.2.1.1.2 Control

No control or control pre-selection is shown.

1.2.1.1.3 Alarm

No alarm or alarm acknowledgement needs to be shown.

1.2.1.2 General view of the installation

1.2.1.2.1 Description

A number of general views are associated with the installation, in particular:

- General view of the process
- General view of safety shutdown levels
- General view of fire and gas detection systems
- General view of the utility.

The general view contains information crucial to the installation within each domain.

1.2.1.2.2 Alarm

Alarm groups are shown.

1.2.1.3 Detailed view of the installation

1.2.1.3.1 Description

The detailed views are associated with the functional systems or sections of the installation, and provide the Operator with all the information and actions needed to control the systems.

The lines at the limits of the screen are intersected by the shutdown valves.

1.2.1.3.2 Control

The detailed view contains all the controls needed to control the installation.

1.2.1.3.3 Alarm

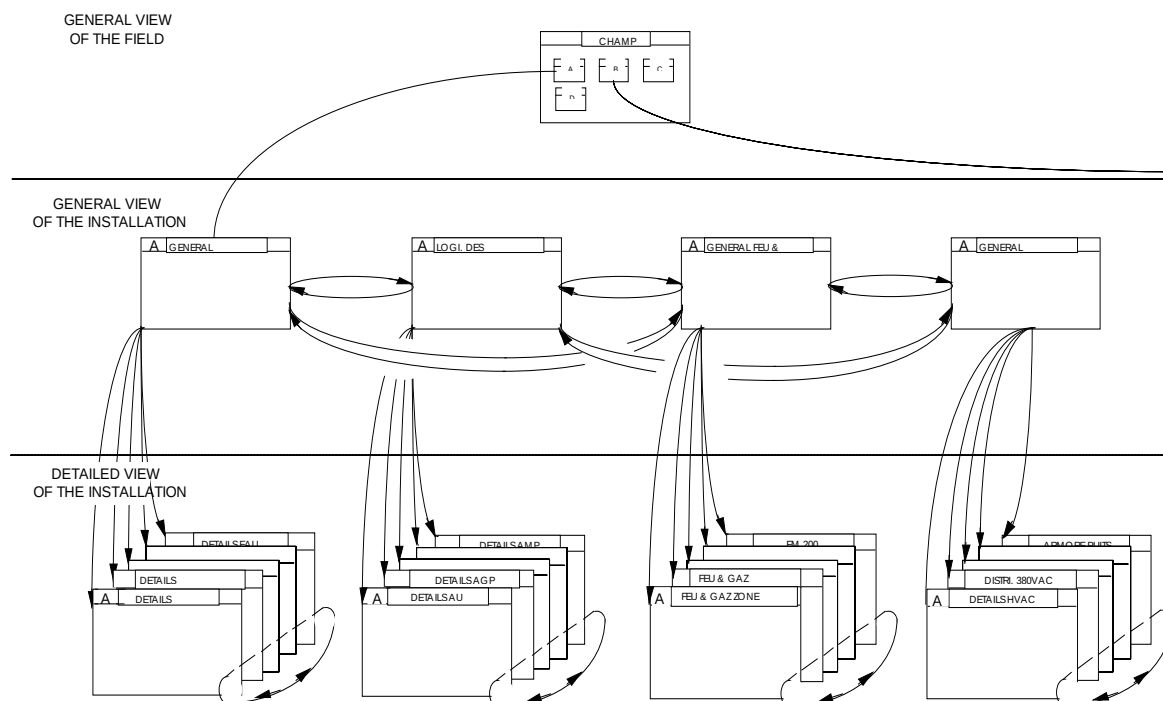
The detailed view is the display in which alarms are recognised and acknowledged.

1.2.1.3.4 Display system tree structure

Whatever display is currently shown on screen, the general view of the field must always be accessible.

From the general view of the field, connections to the general views of the installation shall be set up via the general view of the process.

The Operator shall be able to browse around within the detailed views using the next/previous keys or dynamic display zone, shown on the displays by a **cyan** arrow labelled with the name of the target.



1.2.2 Sequence displays

These provide Grafcet or List representations of the progress of sequential actions performed automatically or by the Operator.

The sequence displays show plant start-up and shutdown sequences.

Animation may be based on the use of reverse video, highlighting, etc., used to highlight the stages and transitions.

In some cases, details of these displays may be incorporated in the control displays.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 64 of 99

1.2.3 Group displays

These shall provide an analogue representation of the controllers, grouped according to operational or functional control logic.

These shall be designed to assist the Operator in changing set points, entering MANU/AUTO commands, aligning measurements with set points, performing cascaded switchovers, indicating alarm thresholds, and so on.

1.2.4 Adjustment displays

These displays can be accessed only by the Instrument specialists. They show all the adjustable information associated with a process variable: control loop setting parameters, alarm and protection thresholds, etc.

These displays can be accessed by the Operator for information.

1.2.5 Alarm displays

These contain all active alarms. They are organised hierarchically and by system or functional subsystem.

Two types of display are required:

- Chronological record of alarms grouped by installation
- Active alarms: functions for sorting by degree of urgency, installation, identification shall be defined.

Four levels of colour-coded alarms are normally required:

- No alarm indication (White)
- Low priority alarm (Yellow)
- High priority alarm (Orange)
- Very high priority alarm (Red).

The control system may dynamically establish the degree of urgency according to the state of the process or the level of control. At its limit, it shall impose a zero level, indicating total absence of any alarm (if a machine is shutdown, for example). The degrees of urgency must be defined during the project.

Alarms may be acknowledged and disabled from all types of display in which they appear. These actions shall automatically be reflected in the other displays.

For the mimic displays, all alarms, whatever their priority, shall appear red.

1.2.6 Inhibition displays

These displays contain a list of all signals likely to be inhibited, or all units likely to be forced on or off.

When a measurement signal is inhibited, its label shall appear framed in yellow.

1.2.7 Graphic history displays

All the trend records needed to control and monitor installations shall be contained in these displays.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 65 of 99

The Operator can obtain additional information through the following functions:

- Change of scale and origin of the time axis and/or the Y axis
- Zoom effect
- Analyses such as average, rate of change, etc.

1.3 Access to the displays

1.3.1 Access levels

Five levels of access are required:

- Visitor No accessible command
- Operator Normal process control and safety reset
- Maintenance First level of intervention
- Method Process parameters modifications
- Engineer All system modifications including system configuration modifications.

1.3.2 Calling up displays

Displays can be called up as follows:

- From a menu
- Direct from the keyboard using special keys
- Via a label typed in
- Direct from alarm-related displays.

It is important to have at least two ways of calling up displays available at the same time, and that they should always be the same.

1.3.3 Display linkages

For mimic displays, the linkages should be functional:

- Display linkages may be created by:
 - Pointing to a sensitive area, around the edges of the mimic, delimited by a cyan blue line. These areas are the fluid inlet and outlet points
 - Use of keys for browsing through the mimics: **Next/Previous**.
- Linkages from one level of the tree structure to another shall be based on:
 - The use of special keys.

1.3.4 Windowing (face plate, pop-up display)

All dynamic elements/objects shall be linked to dedicated face plates showing detailed information.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 66 of 99

1.4 Reserved screen area

One or more preformatted screen areas shall be reserved to display alarms, titles and commands for calling up other displays.

1.4.1 Alarm panel

An alarm window shall be included to provide a real time display of the most important alarm based on the alarm's chronology and priority.

This alarm shall be displayed permanently whatever the display currently shown on screen.

The Operator may, at any time, and by pressing the key providing direct access to alarms, call up the display containing the alarm.

1.4.2 Title and display call-up window

This window provides the Operator with information and key functions for linking to the following displays (non-exhaustive list):

- Name of installation (in uppercase)
- Status of installation (Inhabited or Uninhabited)
- Title of the display
- Link to process display
- Link to safety shutdown display
- Link to fire and gas display
- Link to utility display
- Direct alarm access link
- Indication of number of functions inhibited and/or forced
- Date
- Time.

2. Use of colour coding for fixed patterns

2.1 General

Background: All colours, provided that the colour is soft (pastel) and contrast is acceptable.

Equipment outlines shall provide effective contrast in hard copy.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 67 of 99

2.2 Colour conventions

2.2.1 Piping

Piping shall be coloured according to the main fluid carried. Colour coding shall be as follows:

Product	Colour
Gas	Yellow
Oil	Green
Water	Blue
Steam	Blue
Air	Marine
Water drains	Blue
Oil drains	Green
Gas oil	Magenta
Glycol	Magenta
Amine	Magenta
Chemical products	Magenta

If necessary, the conventions may be complemented by adjusting the thickness of the fluid lines.

Instrumentation lines between measurements and associated valves, when shown, shall appear as dotted lines, with the same colour for all mimics (white, for example, thin line).

2.2.2 Single wire electrical lines

Single wire electrical lines shall be colour coded as follows (up to a maximum of four).

Voltage	Colour
> 5.5 kV	Cyan
5.5 kV	Yellow
380 V	Green
220 V and below	Magenta

If additional distinguishing features are required, line thickness and brightness may be used, etc.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 68 of 99

2.3 Written information

2.3.1 Units

Measurements shall be identified according to their type and by their normal units:

- "barG" Bar relative
- "barA" Bar Absolute
- "Nm³/d" Normal m³/d (0°C, 1013 millibars)
- "Sm³/d" Standard m³/d (15.6°C, 1013 millibars)
- "m³/d" At service T and P
- Etc.

Wherever possible, the requirements of the ISO standard shall be observed; however, local or trade practices may be retained (m³/d or m³/h instead of m³/s for example).

2.3.2 Identification

To keep the user interface as uncluttered as possible, labels (or identification details) on instruments shall not always appear on the mimics.

The console Operator shall be provided with a key for toggling these items on or off.

3. Representation of elements

The representation of the animated and non-animated symbols is available in Appendix 10.

4. Animation of mimic elements

Important note: In the figures in Appendix 10, the background is white so those lines specified as white in the text are shown black in the figures.

4.1 Types of elements (non-exhaustive list)

- On/off valves
- Hand Valves (HV)
- Control valves (may be animated according to percentage opening)
- Simple Equipment such as pumps, air coolers, etc.
- Bar graphs
- Trend curves
- History curves
- Numeric values
- Status indications: Information on states or alarms
- Faults

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 69 of 99

- Safety logic bars
- Commands.

4.2 Basic principles

4.2.1 General

4.2.1.1 Flow - No flow principle

- Flow → Colour of the fluid
- No flow → White

The colour of an element must comply with this animation principle depending on whether it presents an obstacle to the flow of the fluid.

4.2.1.2 Blinking principle

- Appearance of fault → Blinking red (becomes fixed when acknowledged)
- Transient state → Colour of fluid blinking

The blinking principle shall be applied to all of the elements concerned (outline and internal fill pattern). Unless otherwise indicated.

4.2.1.3 Frame colour principle

- Communication or system fault → Magenta frame
- Inhibition → Yellow frame
- Maintenance override (forcing) → Blue frame
- Invalidity → Red frame
- Safety locking → White frame

Even if several states are present simultaneously, only one frame shall appear based on order of importance. From most to least important: magenta, yellow, blue, red, white.

4.2.1.4 Timer principle

Delay countdown associated with transient phases (inhibition, sequence, etc.):

- Count started: current time in yellow normal video.

When the timer is displayed digitally, the time unit shall be shown.

4.2.2 Symbol animation

4.2.2.1 Two-part symbols (control and controlled)

- The **control** part can be one of two colours: white or the colour of the fluid
 - Closed, shutdown → White
 - Opening, running → Colour of the fluid

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 70 of 99

- The **controlled** part shall be colour coded as follows:
 - Closed, shutdown → White
 - Open, running → Colour of the fluid
 - Actuation in progress → Colour of the fluid blinking
- Discrepancy: only the **controlled** part is affected
 - Discrepancy → Red blinking
 - Discrepancy acknowledged → Red fixed

4.2.2.2 Single-part symbols

Just one part is animated:

- Closed, shutdown → White
- Open, running → Colour of the fluid
- Fault → Red blinking
- Fault acknowledged → Red fixed

4.2.3 Non-permanent information

This is used to avoid overloading the mimics.

There are:

- Non-active information
This information (valve name, pump name, etc.) appears if requested by the Operator.
- Active information
This information (sequence graphs, Operator help, etc.) appear:
either:
 - At the request of the Operator
 or:
 - At the initiative of the system in response to control events (security fault, alarm, inhibition, invalid sequence, etc.).

System permitting, the concept of depth may be used.

4.2.4 Recognition of active areas

The active screen areas shall be marked by the appearance of a hand or arrow when selected by the Operator.

The active screen areas shall be bounded by a light blue line for linkage areas.

For higher-level systems, the control mode shall be stated explicitly as follows: single-well/multi-well, hand/auto, on/off, normal/standby, etc.

4.3 Animation of valves

4.3.1 Motorised on/off valves

Note: The valves are differentiated by the graphic symbol representing the control part.

The table below summarises the animations of the control and controlled parts of all motorised on/off valves.

- 1 = Open or normal
- 0 = Closed or fault.

Timer	Valve status	Indicator states		Animation		
		Control indicator	Fault indicator	Control part	Controlled part	Identification in safety logic diagram
Finished	Open	1	1	Fluid	Fluid	Blue
	Closed	0	1	White	White	White
Not finished	Opening	1	1	Fluid	Fluid blinking	Blue
	Closing	0	1	White	Fluid blinking	White
Finished	Discrepancy on opening	1	0	Fluid	Red	Red
	Discrepancy on closing	0	0	White	Red	Red

The table above gives the standard animation for a motorised valve. Reading from top to bottom, the table shows all standard stable or transient states in normal operation and all cases of discrepancy.

4.3.1.1 XV/SDV/ESDV/BDV

Animation of the frames shall be applied to all motorised on/off valves, apart from the white frame (locked by safety system), which shall not apply to the XV valve (see Appendix 10 paragraph 3.2).

For well valves, the SSV (Surface Safety Valves) shall normally rank equal to the SDV's, while the SCSSV (Surface Controlled Subsurface Safety Valves) shall rank equal to the ESDV's.

4.3.2 Other valves

4.3.2.1 HV (Hand Valve)

(See Appendix 10, paragraph 4)

When represented and not animated, they shall be the colour of the fluid.

- When there is only one limit switch, the operating and discrepancy state animation shall not be provided. Depending on the position of the limit switch (open end or closed end), the respective states shall be "open/not open, closed/not closed".
- Where there are two limit switches, the discrepancy for this type of valve shall not be a true discrepancy between the control (strictly hand local therefore not known to the PCS)

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 72 of 99

and the information returned from the equipment, but rather an indeterminate or impossible position.

4.3.2.2 HCV, FCV, PCV, etc. (Hand Control Valve, Flow Control Valve, Pressure Control Valve)

(See Appendix 10, paragraph 5)

Depending on the situation, the state of closure may be animated, bearing in mind that the state of opening is equivalent to a state of non-closure. This animation may be a function of the analogue valve control signal.

Blinking may be used to indicate a change in progress.

4.4 Animation of simple Equipment (pumps, etc.)

(See Appendix 10, paragraph 6.1)

Animation shall be based on the state of the Equipment, mostly ascertained from information taken from the electrical control module.

The frame principle shall also be applied to pumps (see Appendix 10, paragraph 6.2).

4.5 Animation of analogue values

The frame principle shall apply.

In the event of communication invalidity or fault, it would be best to have the analogue value inside the frame disappear.

4.5.1 Animation of numeric values

Numeric values are characterised by their physical units; they are assigned a configurable display format. The name of the corresponding sensor is disabled, and appears on request.

Animation of the numeric value shall be as follows:

- Normal → Just one colour contrasted with the background for all mimics
- Threshold overshoot → Red blinking
- Acknowledged overshoot threshold → Red fixed

4.5.2 Animation of bar graphs

(See Appendix 10, paragraph 7)

The bar graphs shall be represented by a coloured bar, a graduated scale showing 0, 25, 50, 75 and 100%, alarm threshold markers and safety threshold markers.

The animation shall work as follows:

- Bar graph:
 - Green when the analogue quantity is between the high and low thresholds
 - Red blinking when a threshold has been overshoot but not acknowledged
 - Red fixed when acknowledged

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 73 of 99

- The scale is white
- Threshold markers are normally white, red if overshoot.

4.5.3 Animation of trend curves

(See Appendix 10, paragraph 8)

The trend curves shall be represented within a frame, with the Y axes showing percentage values (0, 25, 50, 75 and 100) and the X axes showing time values.

As with bar graphs, alarm and safety threshold markers may be attached.

The curve shall change colour when a threshold is overshoot, but only in the part affected by the violation.

The inhibition frame shall be positioned around the numeric value displayed corresponding to the current time.

4.5.4 Animation of history curves

The Y axes shall be marked with physical units and not percentage values.

The colours of the curves shall be independent of the types of fluids.

Absence of a line shall indicate a communication fault.

4.6 Animation of status indications

The appearance/disappearance of a status indication shall be dictated by the state of a control function, according to the control systems:

- Appearance/disappearance of text in a window
- Text highlighted in a list.

4.7 Animation of faults

(See Appendix 10, paragraph 9)

Fault messages shall appear only when active. All fault messages (whether active or not) concerning a display shall appear when requested by the Operator.

4.8 Animation of safety logic diagrams

(See Appendix 10, paragraphs 10)

The representation of the safety logic diagrams shall comprise three components:

- On the left, causes
- In the middle, the safety bar
- On the right, actions.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 74 of 99

4.8.1 Animation of causes

- Normal:
 - Fault description → Blue
 - Arrow → Blue
- Permanent fault not acknowledged:
 - Fault description → Red blinking
 - Arrow → Red blinking
- Permanent fault acknowledged:
 - Fault description → Red fixed
 - Arrow → Red fixed
- First fault on safety bar:
 - Arrow → Red thicker
- Fugitive fault not acknowledged:
 - Fault description → Blue blinking
 - Arrow → Red blinking

When the safety bar is reset, the fault arrows return to their normal blue colour.

4.8.2 Animation of the safety bar

The safety bar and its description shall appear as follows:

- Bar tripped → Red
- Bar set → Blue

This bar has two controls: inhibition restart and reset.

Wherever possible, the description of the bar shall be in the reset control area.

For a bar that has been tripped, there must be just one thick first fault arrow and only one.

4.8.3 Animation of actions

Labels attached to controlled devices shall be colour coded according to their true states:

- Started, running → Blue
- Tripped, off → White
- Discrepancy, fault → Red (blinking before acknowledgement, fixed after)

4.8.4 Animation of restart inhibition functions

When a timer is associated with a restart inhibition function, the Operator must be kept informed of the progress of the inhibition timer with a bar graph, a numeric down counter, etc. depending on the capabilities of the system.

4.9 Animation of controls

Wherever possible, only those controls allowed according to the state of the process shall appear.

All controls must be enabled.

For any control command, there must be a visible indication that it has been recognised by the system. For slowly changing processes, an appropriate means shall be provided to indicate the current trend (bar graph, counter, hourglass, etc.). For high-level control functions, the control shall be indicated by a change of status indication.

All keyboard input must be echoed by a beep.

4.10 Animation of linkage areas

The linkage area shall be bounded by a **cyan blue** line. Animation of the text inside that area shall depend on the presence of a fault associated with the mimic to which it provides a link.

4.11 Animation of logical Operators & selectors

All logical Operators (e.g. "OR", "AND", etc.) shown on mimics (PID's, safety logic charts, C&E matrix) shall be animated.

Where safety related, the logical Operators animation (status and I/O's) shall be defined as per the safety bar I/O animation.

Safety related logical Operators shall not be provided with reset facility.

Depending on the project specification, inhibition facility can be implemented; in that case the representation shall be the same (e.g. yellow frame).

In addition any selector (e.g. low, high, automatic, manual, etc.) shall also be animated (see § 6.3.4 of the **GS EP INS 197** for example).

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 76 of 99

Appendix 9 Glossary

Alarm: Visual manifestation (change of colour and blinking of a marker, a numeric value, etc.), audible manifestation (warning), message indication, fault indication (discrepancy in a valve, etc.).

Alarm disabling (masking): Alarm disabling is an Operator action designed to prevent sounding of the audible alarm and temporary blinking when a threshold is overshoot. However, the colour change functionality remains enabled.

Alarm disabling from a console is automatically extended to all of the installation's consoles. However, alarm disabling from the consoles of one installation is not extended to the consoles of another installation, even if the other installation controls the first at a higher or lower level.

This action is permanent and must be deliberately deactivated.

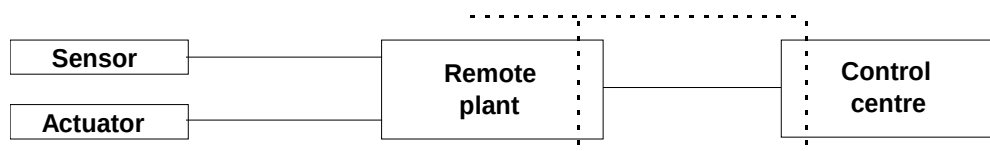
An alarm may be disabled automatically by the system in the following circumstances:

- Appearance of a first fault (to eliminate the alarm cascade)
- When an automatic control function adjusts the urgency of the alarm (for example, a lube oil PAL is assigned zero urgency if the compressor is shutdown).

In this case, the automatic disabling is temporary and deactivated automatically by the control system.

Background: Non-animated part of a display.

Communication and/or system fault: Abnormal situation in the link between a remotely connected processing plant and the control centre.



Communication and system fault

Control level: Profile characterising the various options available to the Operator to control an installation. The following example is given by way of indication:

- Level 1: control of an on/off valve on the discharge side of a pump
- Level 2: control, via a simple automatic control function, of a pump + valve subsystem at the discharge side
- Level 3: control, via a higher level automatic control system, of a set of three pumps with two running and one on standby.

Depth: Possibility of superimposing several images.

Maintenance inhibition: (See Taking out of service).

Display system tree structure: Hierarchical organisation of the display system.

Driven mode: Control mode in which Equipment is controlled by an automatic control function.

Fault: Abnormal situation in a part of an installation or a part of the control system requiring the particular attention of the Operator, notified by an alarm (for example: separator low level, valve discrepancy).

Free-mode: Control mode in which Equipment is controlled directly by the Operator.

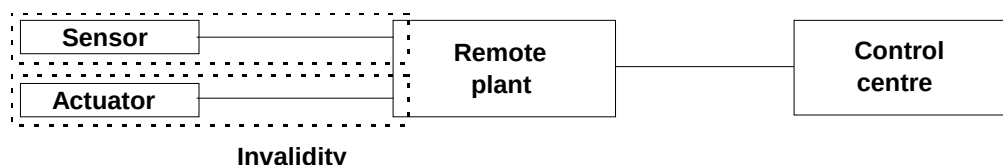
History curve: Computerised display of multi-plot records. This offers additional functionality, including: time stamping, zoom, grouping, etc.

Horizontal linkage: Method of accessing a display on the same level in the tree structure.

Invalidity: situation affecting a sensor or an actuator, the state of which cannot be relayed by the remote processing unit to which it is connected.

- Sensor, actuator fault
- Board or sensor/remote unit link fault.

This situation is known to the remote unit and the control centre.



Operation: Movement of a device resulting from a control function.

Pointing: Action on the part of the Operator based on the use of a tracker ball or mouse to point to an area of the screen.

Reset: Control initiated by the Operator on a safety function, which, provided the conditions are correct, will enable restart operations.

Status indication: Status name, associated with operation, informing the Operator as to the state of a sequence (for example: "Ready", "Discharging", "Imposed operation", etc.), or the control level of an automatic control function (for example: "Free", "Driven", "Single well", "Multi-well").

Symbol: Graphic representation of a component or Equipment.

Symbol frame: Display of a symbol status indication in the form of an animated frame (communication fault, inhibited, forced, invalid, locked, etc.).

Taking out of service: Inhibition for maintenance, initiated by the Instrument specialist.

The item taken out of service is also returned to service by the Instrument specialist. These two actions can be carried out both remotely and locally.

Temporary restart inhibition: Automatic temporary inhibited state imposed to neutralise the cause of a fault and therefore enable a safety bar to be reset.

Other names include: start-up override, process inhibition.

Transient state: A short-lived state.

Trend curve: Representation over a short period of one or more parameters. This shall preferably be included in a control display. For a particular mimic, even a particular control station, the time shown shall be the same for all simultaneous curves.

Urgency: Classification of alarms according to the degree of important attached.



General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 78 of 99

Appendix 9

Vertical linkage: Method of accessing a display on a different level in the tree structure.

Workstation: Hardware used for supervision and/or control. A workstation may comprise one or more monitors, printers, etc.

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 79 of 99

Appendix 10

Appendix 10 Symbols

1. Animated symbols



HV (Hand Valve) With limit switches



Command part

Controlled part

ROV (Remote Operated Valve)



Command part

Controlled part

BDV (Blow Down Valve)



Command part

Controlled part

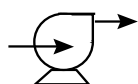
SDV (Shut Down Valve)



Command part

Controlled part

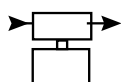
ESDV (Emergency Shut Down Valve)



Controlled part

Command part

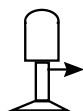
Centrifugal pump



Controlled part

Command part

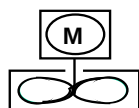
Positive displacement pump



Command part

Controlled part

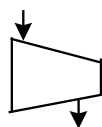
Immersed pump



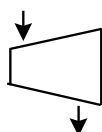
Command part

Controlled part

Air-cooler exchanger or agitator



Compressor



Turbine



Electric motor



Opened

Unstandardized power cut-off device



Closed

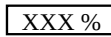
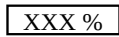
General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 81 of 99

2. Static symbols

(Non exhaustive Examples)



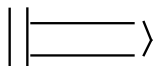
HV (Hand Valve)
Block valve without limit switches



Control valve / choke
HCV (Hand Controlled Valve)



Restriction orifice (fixed pressure drop)



Scraper trap



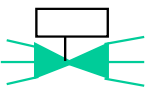
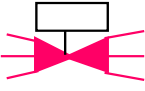
Check valve

Note: Below colours are indicative and may be changed in project specific specifications.

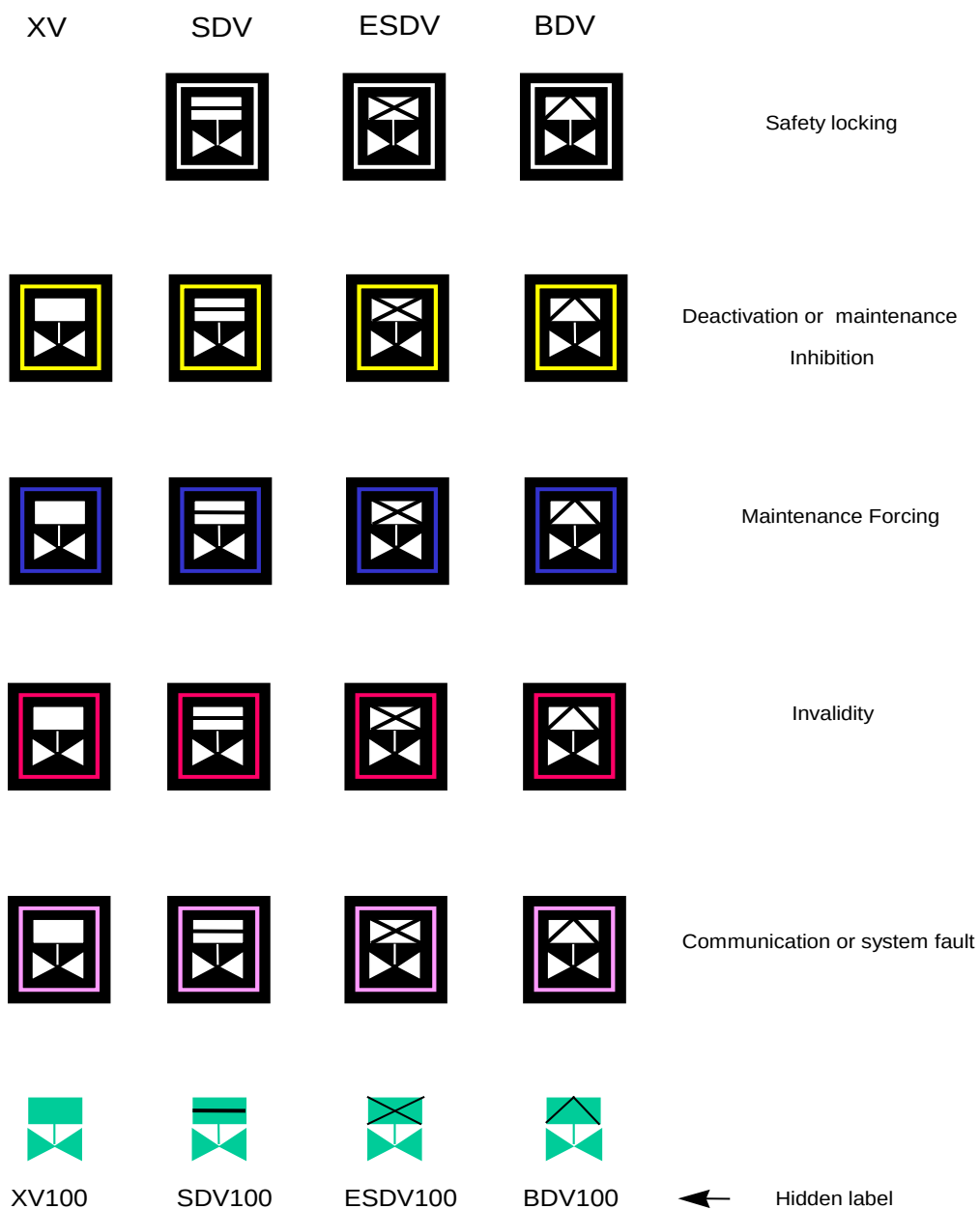
3. On/off motorised valve

3.1 Animation of the command and controlled parts

Block diagram Label
Safety logic diagram

	White White	White	Valve closed
	Fluid White	White	Valve closed Opening controlled by the operator
	Fluid Fluid blinking	White	Valve opening in progress
	Fluid Fluid	Blue	Valve open
	White Fluid	Blue	Valve open Closing controlled by the operator
	White Fluid blinking	Blue	Valve closing in progress
	White Red blinking	Red blinking	Valve discrepancy on closing before acknowledge
	White Red	Red	Valve discrepancy on closing after acknowledge
	Fluid Red blinking	Red blinking	Valve discrepancy on opening before acknowledge
	Fluid Red	Red	Valve discrepancy on opening after acknowledge
			
ROV100		Hidden label	

3.2 Animation of the frames



General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 84 of 99

4. HV (Hand Valve)

4.1 Valve equipped with two switches



White

Valve closed



Fluid blinking

Valve actuation in progress



Fluid

Valve open



Red blinking

Valve fault before acknowledge



Red

Valve fault after acknowledge



Hidden label



Valve in an undertermined position after a time delay

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 85 of 99

Appendix 10

5. HCV, PCV (control valves)



White

Valve closed



Fluid

Valve open

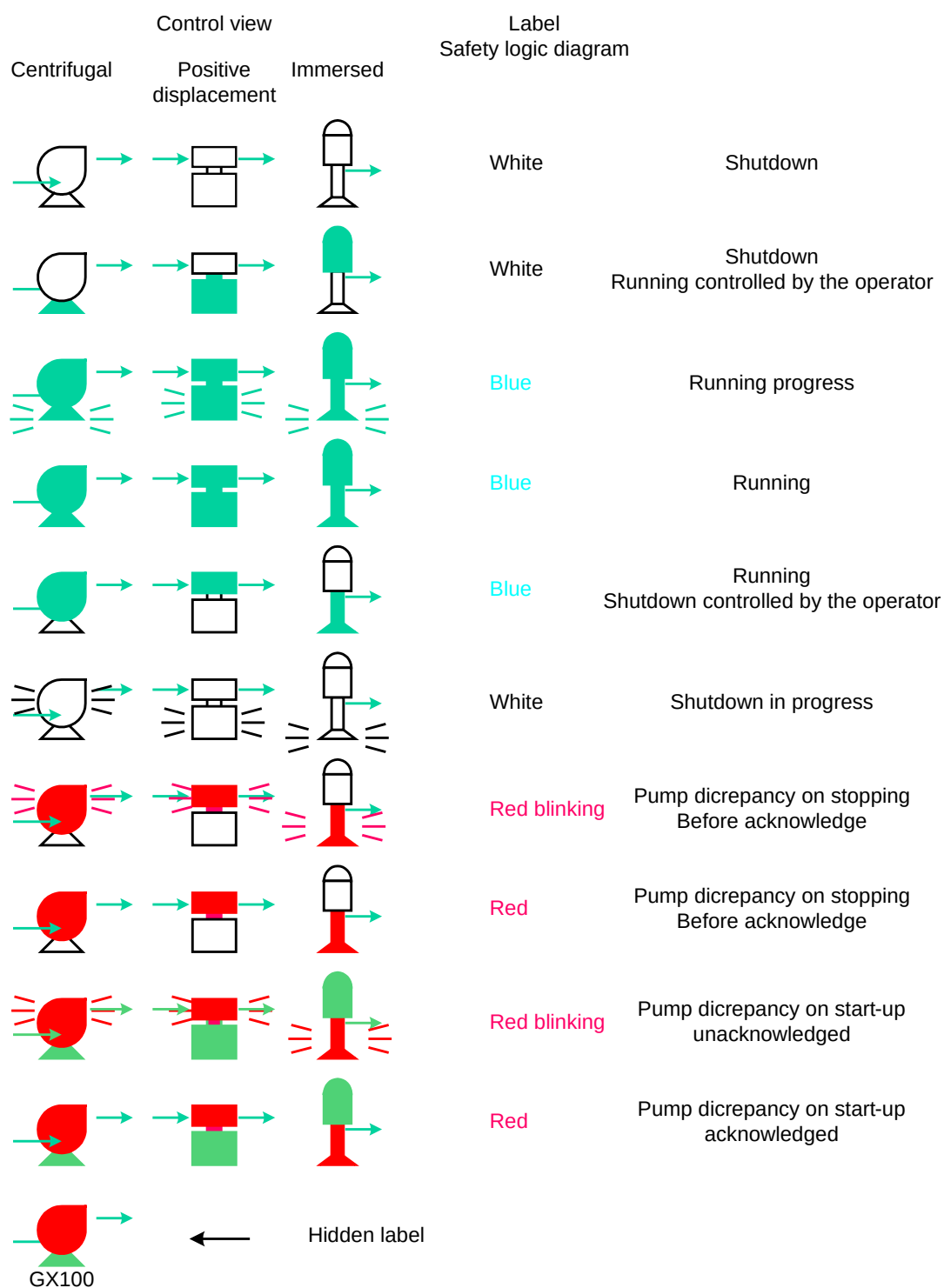


Fluid,
blinking

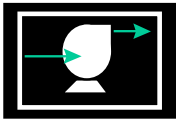
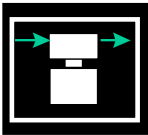
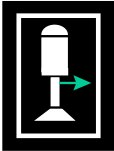
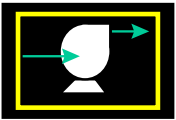
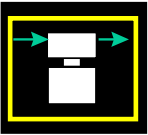
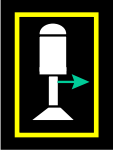
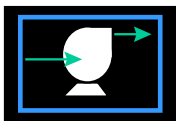
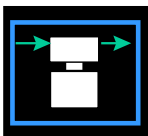
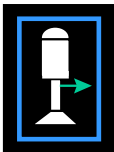
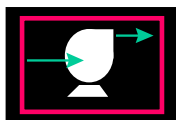
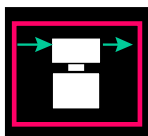
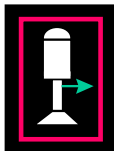
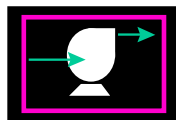
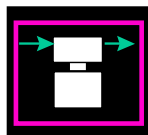
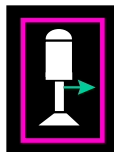
Actuation in progress

6. Pumps

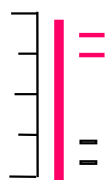
6.1 Animation of simple equipment



6.2 Animation of the frames

Centrifugal	Positive displacement	Immersed	
			Safety locking
			Maintenance Inhibition
			Maintenance Forcing
			Invalidity
			Communication or system fault
			← Hidden label

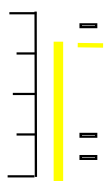
7. Bar graph



Upper safety threshold

- Bar graph
- 2 top thresholds

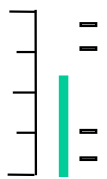
— **Red**



Upper alarm threshold

- Bar graph
- 1 top threshold

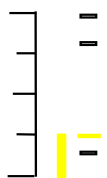
— **Yellow**



Normal

- Bar graph

— **Green**



Lower alarm threshold

- Bar graph
- 1 bottom threshold

— **Yellow**



Lower safety threshold

- Bar graph
- 2 bottom thresholds

— **Red**

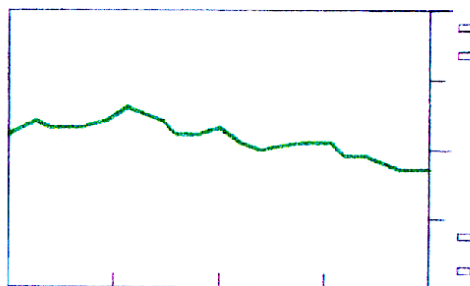
NOTE:

When not acknowledged

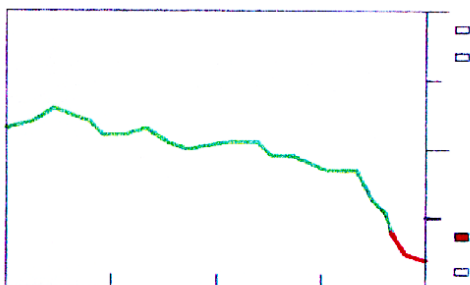
Yellow or Red

Blinking of the bar and corresponding threshold

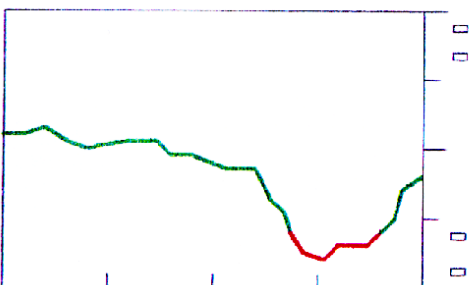
8. Trend curves



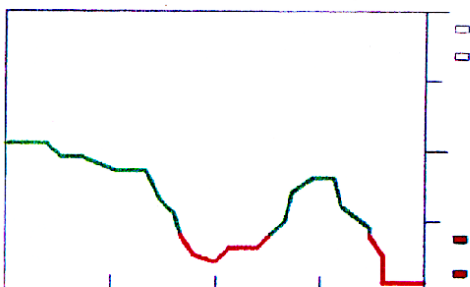
Curve within the thresholds



Lower alarm threshold overshooting



Threshold overshooting storage



Lower safety threshold overshooting

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 90 of 99

Appendix 10

9. Fault

9.1 Threshold overshooting schema

Safety logic diagram	Control view	
		Inactive fault (Callable hidden label)
		Unacknowledge active fault
		Acknowledge active fault
		Inhibited sensor
		Invalid sensor
		Communication or system fault

General Specification		GS EP INS 134
Design and supply of integrated control and safety system		
Rev.: 10	Effective date: 11/2012	Page: 91 of 99

10. Safety logic diagram

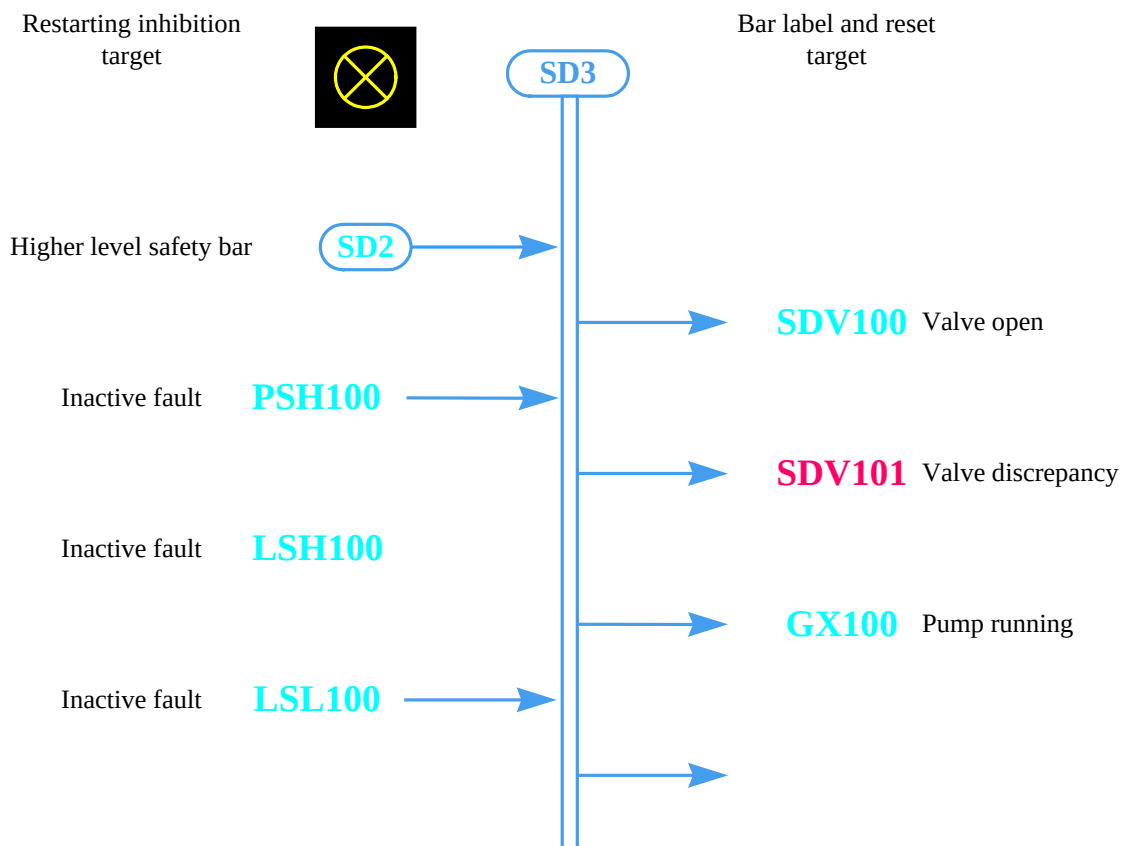
The safety logic diagrams shown in the next sections are based on a vertical representation, but horizontal representation can also be used to be in line with the Affiliate current practice.

Safety bar representation shall be selected at the Basic Engineering stage.

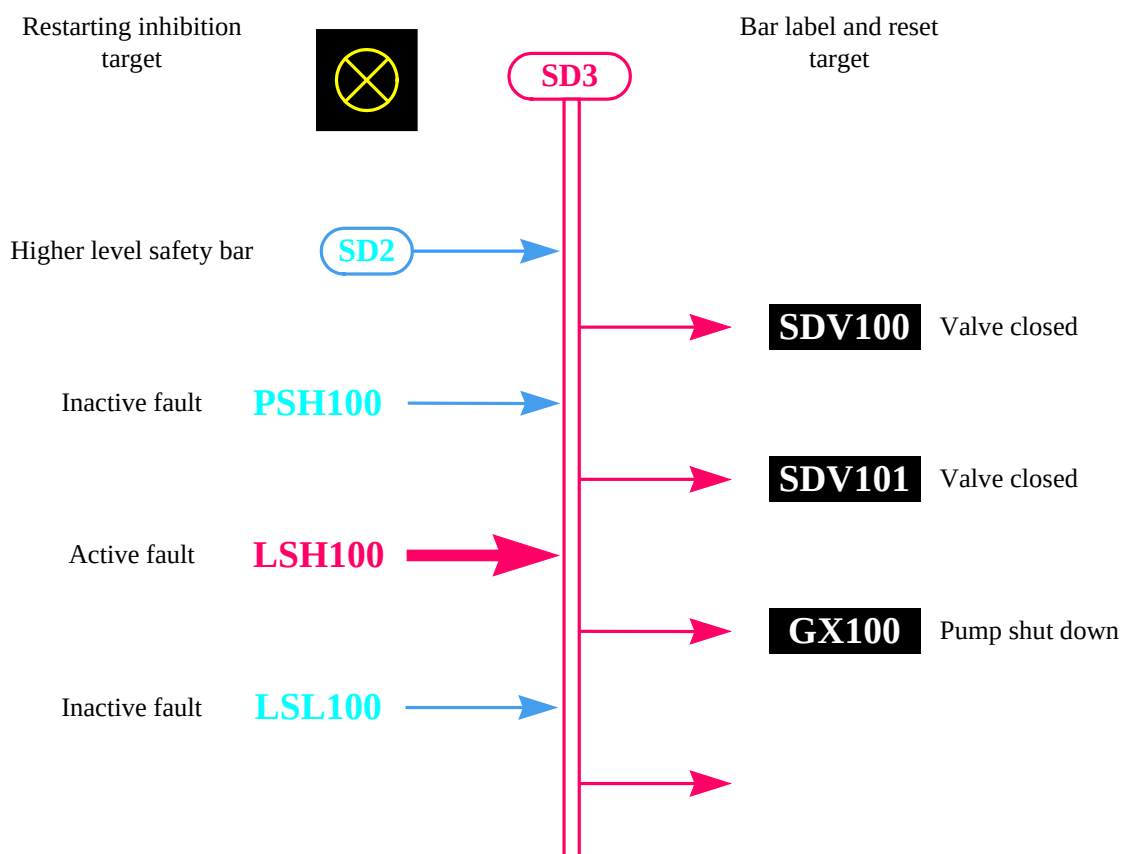
10.1 Armed safety bar



10.2 Armed safety bar - Valve discrepancy

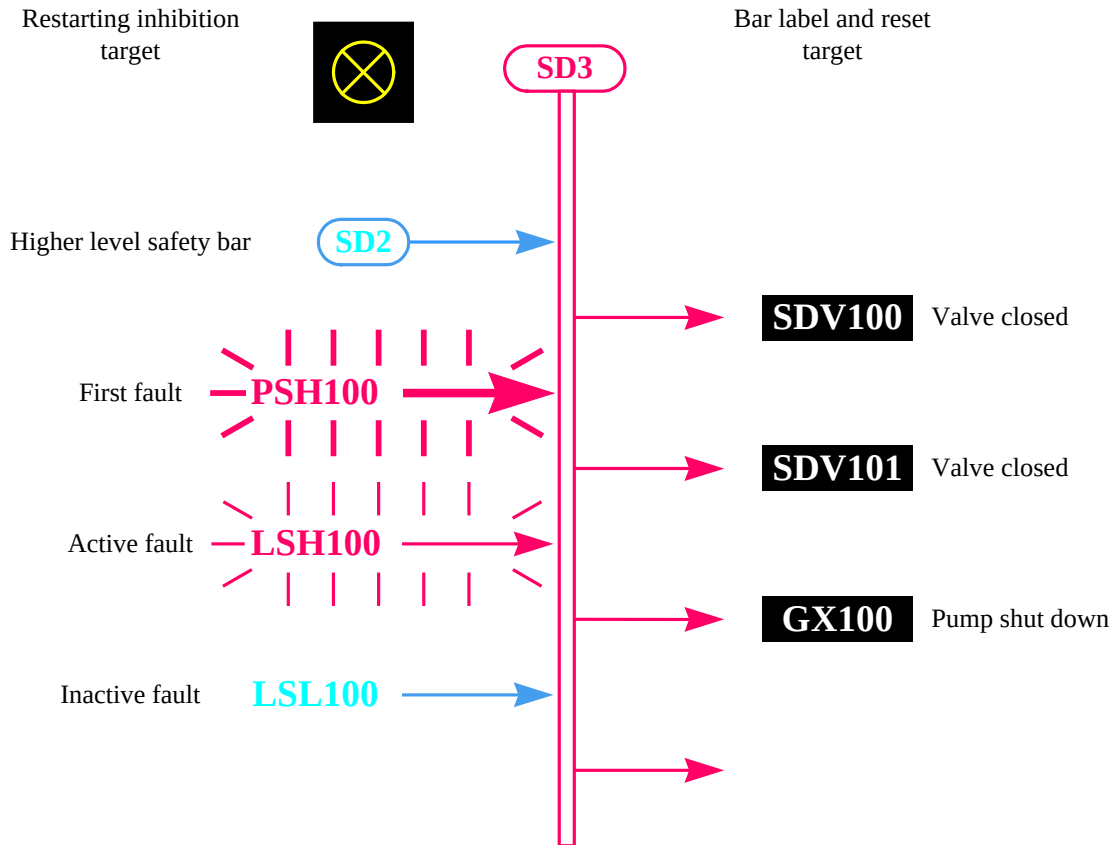


10.3 Safety bar with a fault

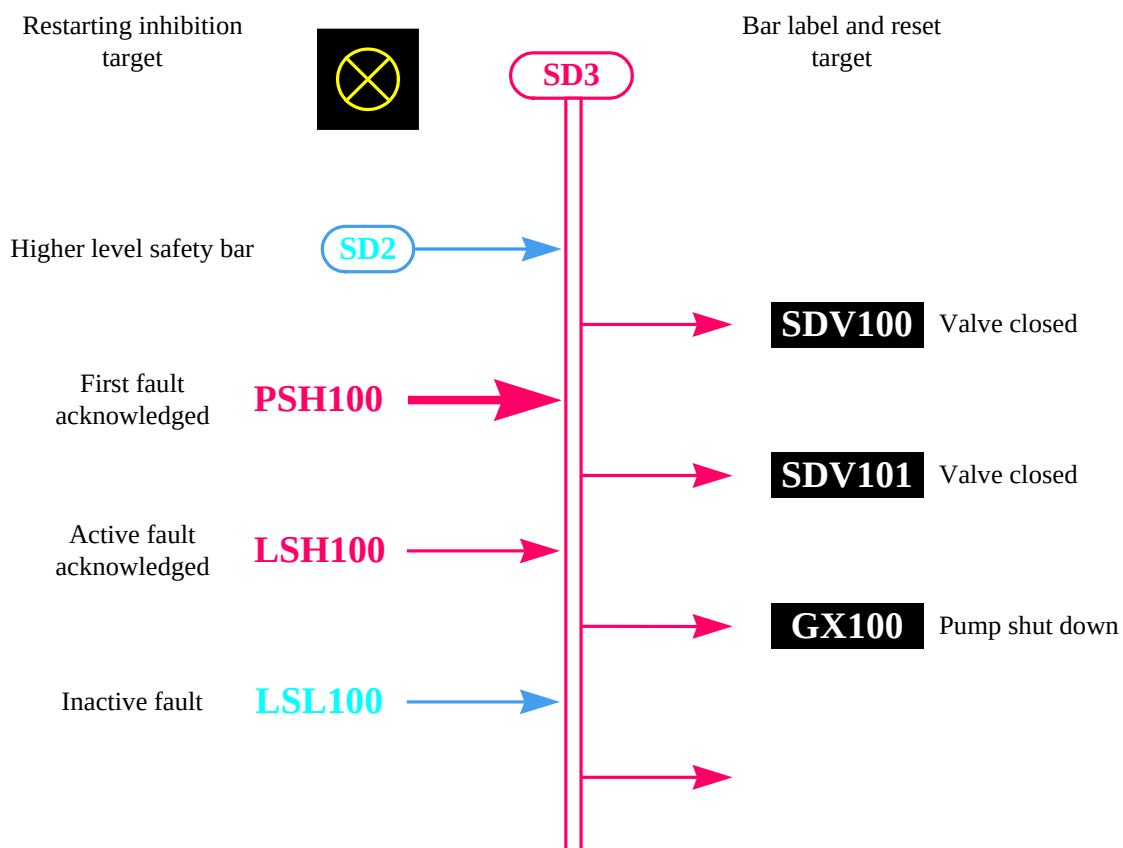


NOTE : Fault detection : Red blinking
 after acknowledge : Red

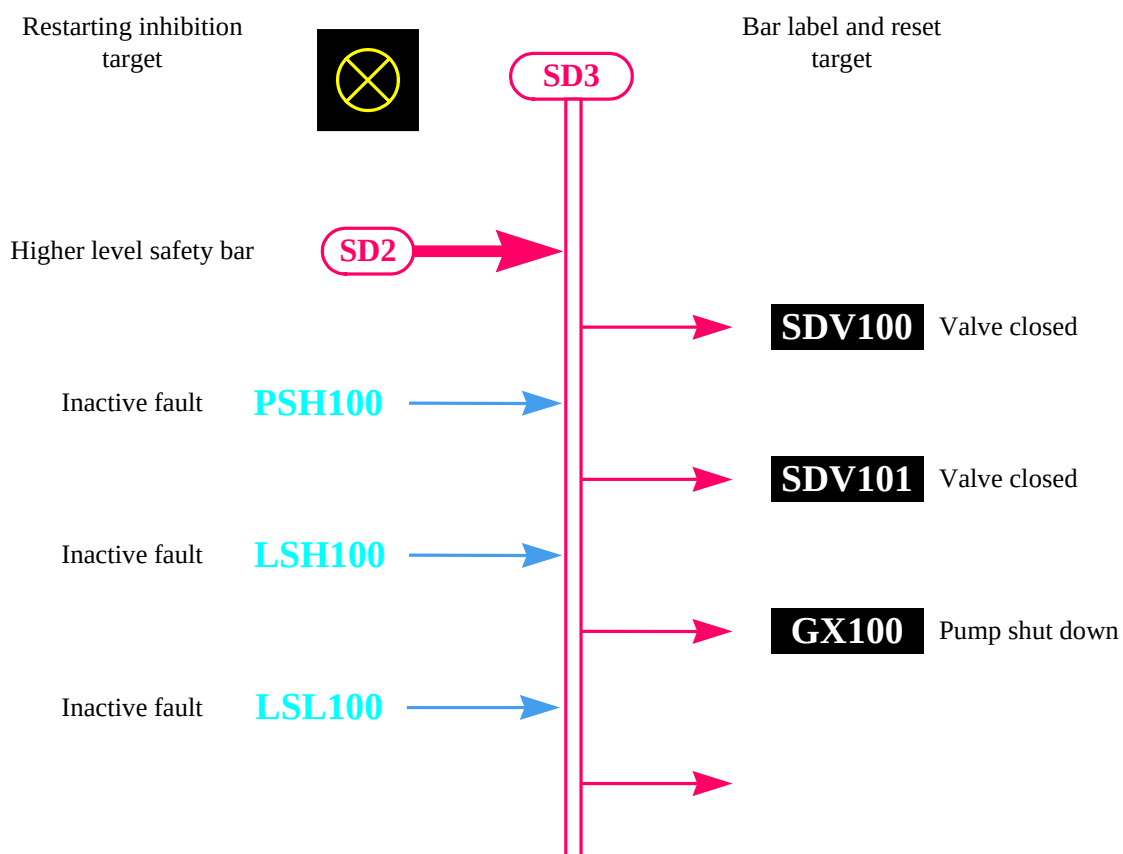
10.4 Safety bar - Fault chain with first fault before acknowledge



10.5 Safety bar - Fault with first fault after acknowledge

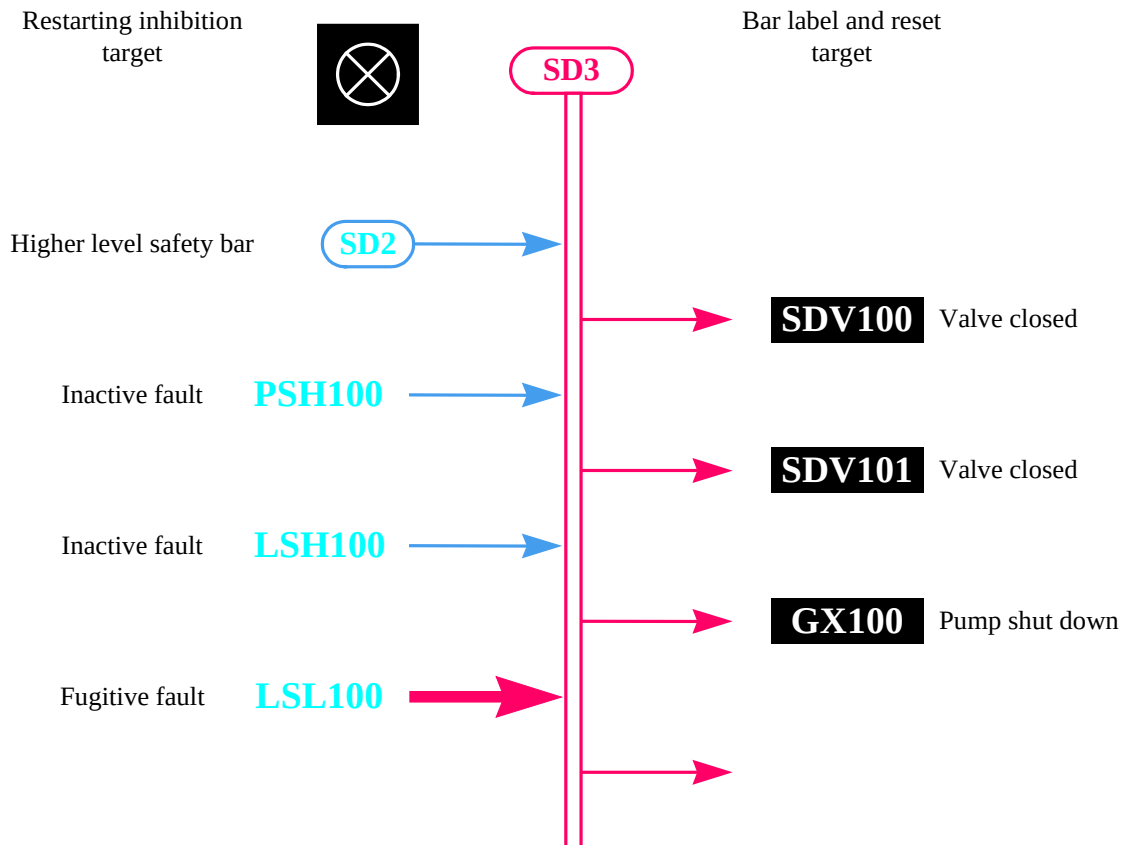


10.6 Safety bar - Higher level fault



NOTE : The arrow is blinking before acknowledge.
Automatic reset by the higher level if no other fault is detected

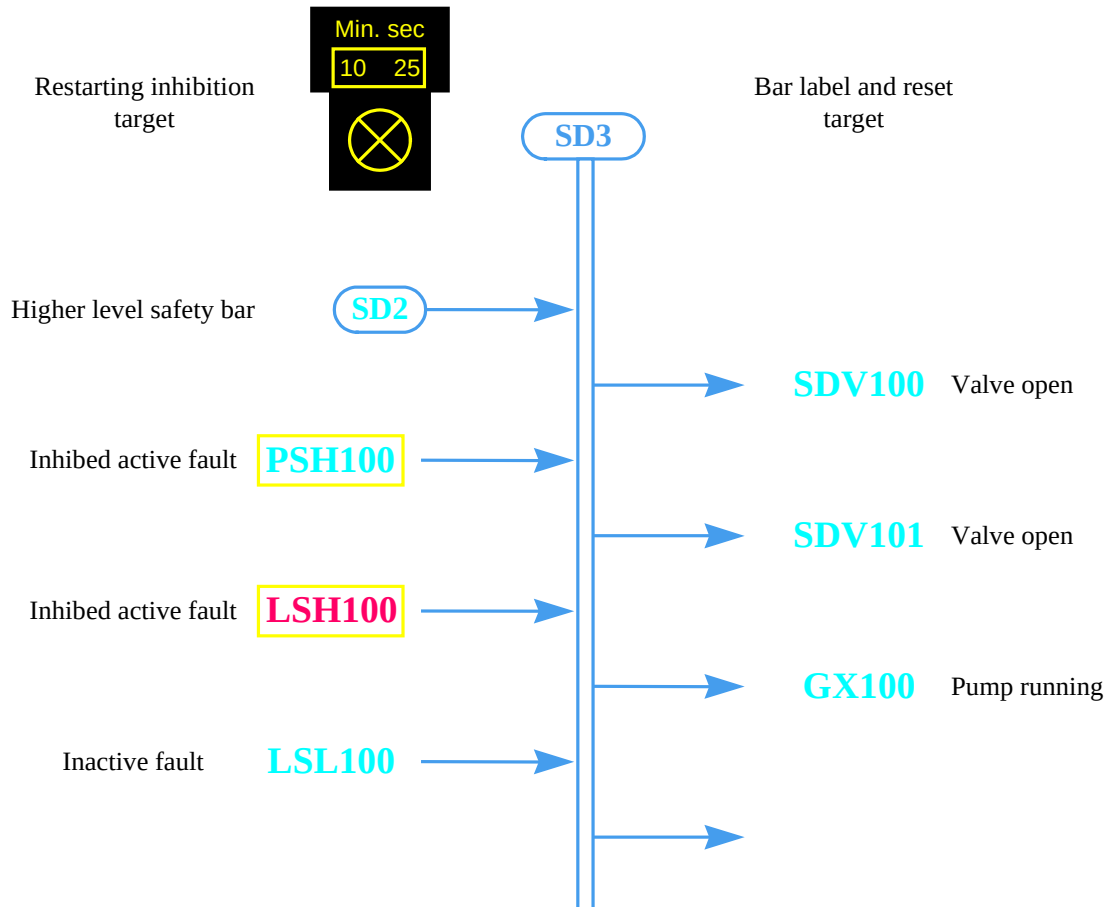
10.7 Safety bar with a fugitive fault



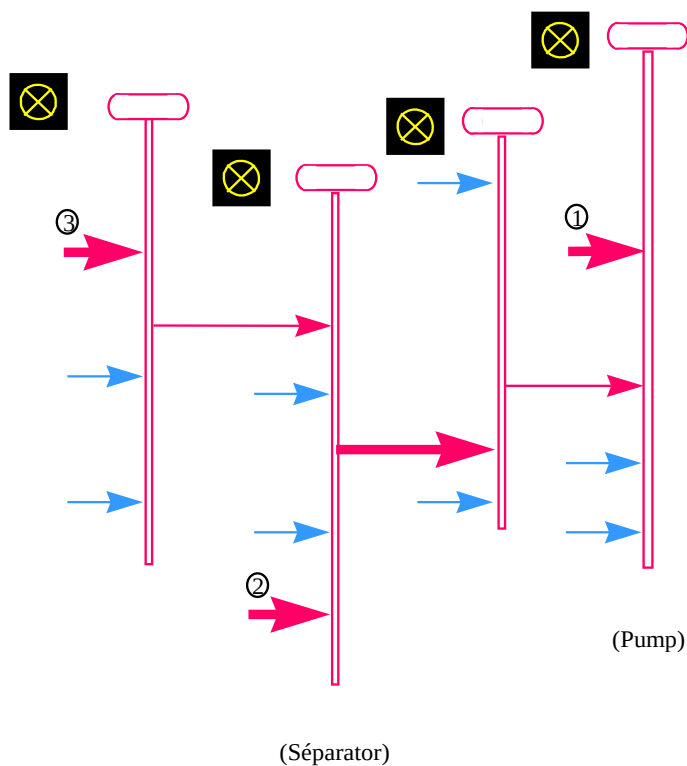
Fault having disappeared before acknowledge : Blue label blinking.
Red arrow blinking.

after acknowledge : Blue label.
Red arrow.

10.8 Safety bar - Inhibited faults



10.9 Example of a fault chain



The faults have appeared in the indicated order.