



Exploration & Production

GENERAL SPECIFICATION

INSTRUMENTATION

GS INS 134

Design and supply of integrated control and safety system

02	10/04	Fully revised
01	10/03	Revised as per marking – Change of Group name and logo
00	02/01	First issue
Rev.	Date	Notes

Contents

1. Scope	4
2. Reference documents.....	4
3. Glossary.....	6
4. Integrated Control & Safety System Functional Description	6
4.1 Subsystem Description	6
4.2 Functional block diagram.....	8
5. Overall Architecture	8
6. ICSS design	9
6.1 General Requirements.....	9
6.2 Hardware	10
6.3 Operating system.....	10
6.4 Interfaces and Industrial Communication Networks	10
6.5 Application software management.....	10
7. Specific Requirements per Subsystem	11
7.1 Safety Shutdown System.....	11
7.2 Ultimate Safety System	12
7.3 Fire and Gas System	12
7.4 Process Safety System.....	13
7.5 Process Control System	14
7.6 Human Machine Interface (HMI).....	15
7.7 Process Data Server (PDS).....	15
8. Specific functional requirements.....	16
8.1 Archiving and historical requirements.....	16
8.2 Sequence of Events.....	16
8.3 Maintenance System	17
9. ICSS Performances	17
10. Packages interface.....	17
11. Cyber Security	18



11.1	Introduction	18
11.2	Architecture.....	18
11.3	Operating System	18
11.4	Industrial Networks and communication	19
11.5	Physical protection.....	19
11.6	SSS and FGS	19
11.7	Human Machine Interface (HMI).....	19
11.8	Process Data Server (PDS).....	20
11.9	Maintenance	21
11.10	FAT	21
11.11	Documentation.....	22
12.	Spareage Requirements	22
13.	Factory Acceptance Test (FAT)	22
14.	Documentation	23
15.	Training courses	23
16.	Specific Cases	23
16.1	PSS combined with SSS	23
16.2	FGS combined with SSS	23
16.3	Requirement for USS.....	23
Appendix 1	Integrated Control & Safety System function descriptions	24
Appendix 2	Hardware design.....	27
Appendix 3	Factory Acceptance Test (FAT)	30
Appendix 4	Documentation.....	31
Appendix 5	Design of the control display system	34
Appendix 6	Glossary	48
Appendix 7	Symbols.....	50

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 fulfil 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 Technical Information System
- Data Communications.

2. Reference documents

The reference documents listed below form an integral part of this General Specification. Unless otherwise stipulated, the applicable version of these documents, including relevant appendices and supplements, is the latest revision published at the EFFECTIVE DATE of the CONTRACT.

Standards

Reference	Title
ISO 9001:2000	Quality management systems - Requirements
IEC 60079	Electrical apparatus for explosive gas atmospheres
IEC 60364	Electrical Installations of Buildings
IEC 61000	Electromagnetic compatibility (EMC)
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC 61511	Functional safety - Safety instrumented systems for the process industry sector
IEC 61131	Programmable controllers - Part 3: Programming languages

Professional Documents

Reference	Title
ISA SP99-dTR99.00.01	ISA SP99: Security Technologies for Manufacturing and Control System
ISA SP99-dTR99.00.0	ISA SP99: Integrating Electronic Security into the Manufacturing and Control System Environnement

Regulations

Reference	Title
Not applicable	

Codes

Reference	Title
Not applicable	

Other documents

Reference	Title
SIREP-WIB-EXERA No. M 2656 X 98 part 2	Ergonomics in process control rooms, Design guidelines

Total General Specifications

Reference	Title
GS ELE 031	Design of earthing and bonding system
GS INS 107	Design and installation of instrumentation links
GS INS 108	Instrumentation for the design of plant rooms and control rooms
GS INS 110	Instrumentation for Package Units
GS INS 150	Design method for System Configuration Standards
GS SAF 261	Pressure protection and relief, emergency shutdown and depressurisation
GS SAF 312	Guidelines for selecting and installing fire and gas detection systems
GS SAF 371	Emergency control facilities
GS TEL 170	Design and installation of Communications Networks

3. Glossary

CPU	Central Processor Unit
CCR	Central Control Room
DCS	Distributed Control System.
ESD	Emergency Shut-Down
EWS	Engineering Work Station
FAT	Factory Acceptance Test
FGS	Fire and Gas System
ICSS	Integrated Control and Safety System
ISS	Internet Safety System
I/O	Inputs/outputs
HMI	Human Machine Interface
MTTR	Mean Time To Repair
MWS	Maintenance Work Station
PCS	Process Control System
PDS	Process Data Server
PLC	Programmable Logic Controller
PSS	Process Safety System
SIL	Safety Integrity Level
SOE	Sequence of Events
SSS	Safety Shutdown System
TIS	Technical Information System
OWS	Operator Work Station
USS	Ultimate Safety System

4. Integrated Control & Safety System Functional Description

The ICSS comprises of the following subsystems:

4.1 Subsystem Description

Safety Shutdown System (SSS)

The SSS 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 depressurisation functions of the facility (e.g. ESD0, ESD1 and ESD2) according to the defined safety philosophies.

**Ultimate Safety System (USS)**

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 SSS but provides a highly reliable back-up to specific ESD actions.

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.

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.

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.

Human Machine Interface (HMI)

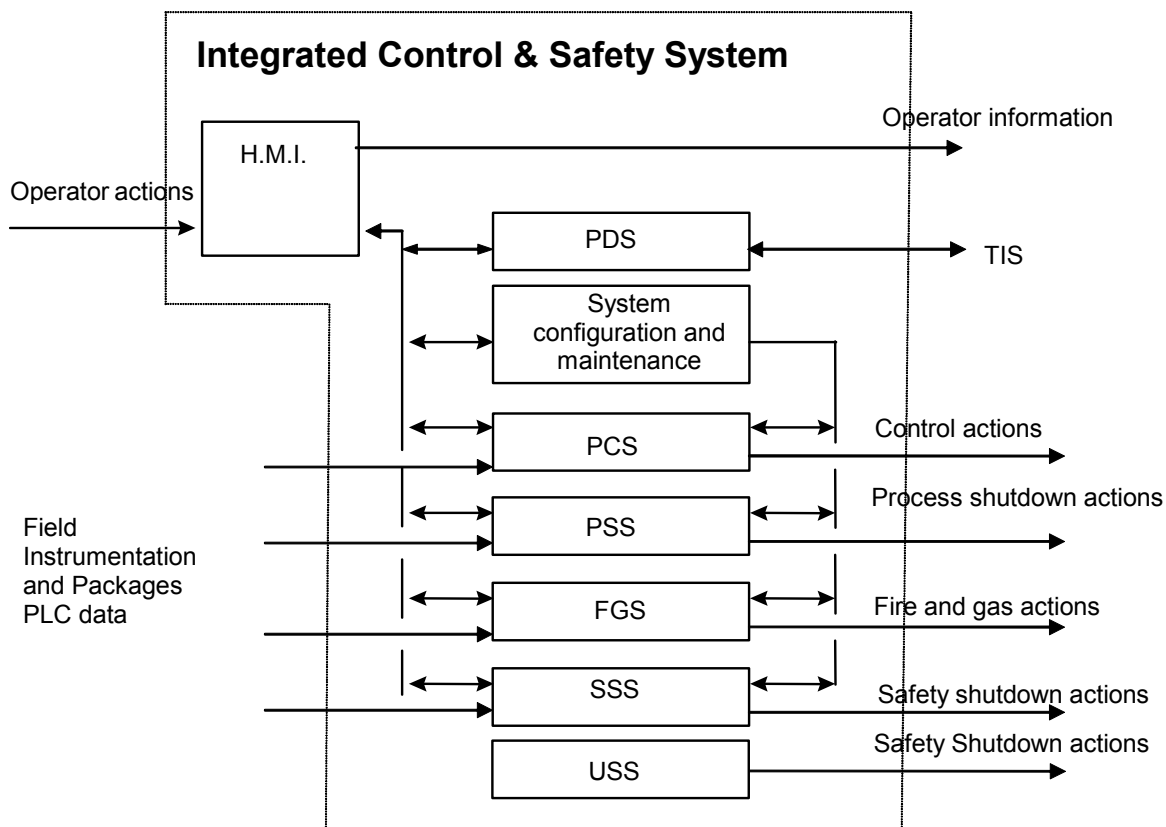
The HMI shall provide the facility for the operator to control and monitor the plant via mimic displays, alarms, trend displays and operator commands. Specific displays can be developed for maintenance purpose.

Process Data Server (PDS)

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

4.2 Functional block diagram

The functional subsystems of the ICSS are highlighted in the following diagram:



5. Overall Architecture

The ICSS shall have a distributed structure with a centralised HMI located in the CCR. The subsystems will remain autonomous and will interface with the HMI via dedicated ICSS network, which will preserve full independence between safety and control functions. The ICSS network shall be physically and functionally independent from the TIS network (Office LAN).

The ICSS shall not be connected to the TIS network unless a specific need has been identified and is required. This connection shall be provided via the PDS.

Typically, nodes from each subsystem shall be distributed in pressurised Instrument Technical Rooms around the facility. Each node will comprise of its system controller, communications cards and I/O interface. The field instruments will be cabled to dedicated marshalling cabinets, segregated per subsystem, for connection to the node. Nodes shall then be interfaced to form a subsystem using the ICSS control or safety network.

Each logic subsystem (SSS, FGS, PSS and PCS) shall be based on dedicated controllers or PLC's and shall be fully independent (hardware and application software).

The architecture shall avoid potential common mode failure points between applications or subsystems. Particular care shall be taken for equipment which drives parallel process lines, or main and backup equipment.

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

Remote Inputs/Outputs architecture may be foreseen with modules mounted inside field junction boxes. In this case the complete assembly shall require being suitable for the relevant hazardous area and meeting the ATEX certification requirements.

6. ICSS design

6.1 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.

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 60511](#). 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.

The ICSS shall be designed to last the lifetime of the installation and shall offer flexibility to allow for future extensions.

Design of the ICSS shall consider the cyber security risks and requirements at the early stage of the project (refer to § 16).

Safety

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

Maintainability

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 replacement of any module with the power supply on shall not affect the working of any other components or cause a system failure.

After any outage, the system shall automatically resume normal operation.

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 modules.

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 networks including security aspect.

Project specification will address hot spare requirement.

Standardisation

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

6.2 Hardware

Hardware design details are given in Appendix 2.

6.3 Operating system

The system shall be supplied with the latest up-to-date software release at the time of FAT. In addition, the ICSS VENDOR 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 synchronised.

All redundant equipment shall be able to change over without disturbing the application.

6.4 Interfaces and Industrial Communication Networks

All communication protocols, installation and cabling rules shall be compliant with the **GS TEL 170** standard. An addressing IP plan shall be prepared and submitted for COMPANY approval. Network management tools (ICSS dedicated) shall be provided by the Supplier and shall comply with the COMPANY standard (**GS TEL 170**).

Communications with packages shall preferably be standardised on a single protocol for the whole project.

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.

6.5 Application software management

The application software 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 modules 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 loosing one controller (or a part of it)
- Too many data exchanges between controllers.

The ICSS shall be configured as per "Function Block Standards" described in **GS INS 150** and the corresponding detailed GS specifications. The displays shall be developed according to **Appendix 5** "Design of the control display system" and the above mentioned standards functions specifications.

However, COMPANY subsidiaries may use their own library of Standards Functions when available.

Instrument engineering database software shall be used as an engineering tool in designing the ICSS system e.g. allocation of Input/Output. The instrument list including all parameters shall be prepared using the same tool.

It is normally expected that the Instrument Engineering CONTRACTOR would compile the instrument list and the ICSS SUPPLIER would update this list with the control and safety systems parameters.

7. Specific Requirements per Subsystem

7.1 Safety Shutdown System

7.1.1 Safety Integrity Level

The SIL requirement, as per IEC 61508/IEC 61511, shall be as defined by GS SAF 261.

7.1.2 Availability

The required availability of the SSS 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 SSS shall be based on a fully redundant programmable system. It shall be based on fail safe design built using high reliability, high availability and fault tolerant equipment.

The system shall include controller nodes with associated I/O cards and communication cards. Depending on the size of the system there may be the requirement of multiple nodes connected together on a dedicated safety network. Executive actions may be transmitted on this network between SSS controllers as long as it has been specifically designed for such a purpose and has the appropriate SIL level approval.

The system shall be fully independent of the control system, although reporting will be via the PCS system network to the ICSS operator work stations located in the control room.

There shall be an SSS shutdown panel located in the control room. This shall be hardwired directly to the SSS system bypassing the ICSS operator stations.

A dedicated engineering work station (EWS) shall be utilised to allow test of configuration modifications prior downloading to the controllers. This EWS shall only be connected to the SSS controllers as necessary. It shall not be a permanent installation.

Diagnostic facilities shall be able to be automatically and manually run. These facilities shall cover the SSS 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 as well as special diagnostic facilities configured into the system e.g. valve partial stroking.

Field devices shall be hardwired to the SSS system. Marshalling cabinets shall be employed to group field cabling and cross-wire for connection to the SSS I/O card.

Interfaces between packages and SSS shall be hardwired.

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

7.2.1 Safety Integrity Level

The SIL requirement, as per the IEC 61508/IEC 61511 shall be as defined by GS SAF 261.

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.

Its inputs will be ESD pushbuttons located in the control room defined by safety philosophies to back-up ESD 1 & 0. These shall be the same buttons that are connected to the SSS 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 SSS system to carry out the ESD function. Upon timeout the USS shall trip its outputs which will generally be connected to power supplies for ESDVs, BDVs 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

The SIL requirement, as per IEC 61508/IEC 61511 shall be as defined by GS SAF 261.

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

The FGS shall be based on a programmable system. It shall generally be of a non-fail safe design utilising 'energise to trip' principles. It shall be built using high reliability, high availability and fault tolerant equipment.

The system shall include controller nodes with associated I/O cards and communication cards. Depending on the size of the system there may be the requirement of multiple nodes connected together on a dedicated safety network. Executive actions may be transmitted on this network.

between FGS controllers as long as it has been specifically designed for such a purpose and has the appropriate SIL level approval.

The system shall be fully independent of the control system, although reporting will be via the PCS system network to the ICSS operator work stations located in the control room.

There shall be an FGS matrix panel located in the control room. This shall be hardwired directly to the FGS system bypassing the ICSS operator stations. This panel will provide an overview status indication for each fire zone. In addition manual pushbuttons to initiate release of extinguishant (CO₂, Deluge, Foam, etc.) shall also be provided. In addition manual start and selection facilities for the fire water pumps will be provided.

A dedicated engineering work station (EWS) shall be utilised to allow test of configuration modifications prior downloading to the controllers. This EWS shall only be connected to the FGS controllers as necessary. It shall not be a permanent installation.

Note: If the same MANUFACTURER and technology are utilised for FGS and SSS, then EWS may be common for both systems.

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

Field devices shall be hardwired to the FGS system. Marshalling cabinets shall be employed to group field cabling and cross-wire for connection to the FGS I/O card.

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

Interfaces between packages and FGS shall be hardwired.

Interfaces between FGS and SSS for executive actions may utilise the safety bus as long as it has been specifically designed for such a purpose and has the appropriate SIL level approval. Alternatively hardwired signals shall be used.

7.4 Process Safety System

7.4.1 Safety Integrity Level

The SIL requirement, as per IEC 61508/IEC 61511 shall be as defined by GS SAF 261.

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.

7.4.3 Specific requirements

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.

The system shall include controller nodes with associated I/O cards and communication cards. Depending on the size of the system there may be the requirement of multiple nodes connected together on a dedicated safety network. Executive actions may be transmitted on this network between PSS controllers as long as it has been specifically designed for such a purpose and has the appropriate SIL level approval.

The system shall be fully independent of the control system, although reporting will be via the PCS system network to the ICSS operator work stations located in the control room.

A dedicated engineering work station (EWS) shall be utilised to allow test of configuration modifications prior downloading to the controllers. This EWS shall only be connected to the PSS controllers as necessary. It shall not be a permanent installation.

Diagnostic facilities shall be able to be automatically and manually run. These facilities shall cover 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 as well as special diagnostic facilities configured into the system e.g. valve partial stroking.

Field devices shall be hardwired to the PSS system. Marshalling cabinets shall be employed to group field cabling and cross-wire for connection to the PSS I/O card.

Interfaces between packages and PSS may be via redundant serial links, designed for this purpose.

Where it is decided that the PSS may use the same type of controllers as the PCS, though the controllers remain separate and dedicated to their function, then the redundant PCS network may be utilised by the PSS, as long as any fault from the PCS system can not interfere with the PSS application.

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 network and thus allow the operator to view and manage the entire facility from the HMI located in the control room. The safety system nodes shall also be connected to this network to allow operator commands and data for reporting to be transmitted. This network shall not be used for executive safety actions.

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

Redundancy will generally be required for critical devices such as controllers, power supplies, main control 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. Depending on the size of the system there may be the requirement of multiple nodes connected together on a control network.

A dedicated engineering work station (EWS) shall be utilised to allow test of configuration modifications prior downloading to the controllers and operator work stations.

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

Field devices shall generally be hardwired to the PCS system. Marshalling cabinets shall be employed to group field cabling and cross-wire for connection to the PCS I/O cards.

Interfaces between packages and PCS may be via serial links or hard wired. The selection will be determined by the quantity of data to be transmitted. Serial link redundancy will be determined by the criticality of the package.

7.6 Human Machine Interface (HMI)

7.6.1 Specific Requirements

All workstations 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 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 can be installed in each instrument technical room for maintenance purpose, 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 Process Data Server (PDS)

7.7.1 Specific requirements

The PDS, based on a server connected to the ICSS network, shall continuously collect and record data from all parts of the ICSS.

It shall also:

- Allow data formatting and calculations (e.g. average, min, max, etc.)
- Provide the interface point to the TIS network to access to any data.

It shall not permit any writing to the ICSS system. The interface shall comply fully with cyber security requirements.

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

7.7.2 Availability

The availability of the PDS shall be as defined by the project specifications. This will in turn determine its redundancy requirements. As the system is not required for the day to day operations but as a reporting and post event analysis tool, then it generally will not require being redundant.

Data storage back-up facilities (hardware and software) will be provided.

8. Specific functional requirements

8.1 Archiving and historical requirements

Archiving and historical functions shall be designed for production and maintenance and to complement normal operating functions. They shall provide a view of the plant and long-term analysis of process changes.

Main functions required are:

- Automatic collection of data (data samples taken at intervals ranging from 5 seconds to 15 minutes, average interval: 1 minute) with pre-processing algorithm (average, min., max.). Data includes (estimated at one third of ICSS and package data): process values, states, events and analysis data, calculated values, maintenance data, manual input, test-run data, test separator data
- Storage of long term historical data (6 months storage)
- Automatic archiving of data on a high-density storage medium (periodic archiving). This archived data shall be available for analysis by the tools used by the supervisory system
- High-level graphic interface dedicated to production and maintenance (management information charts, history curves, event sorting and analysis, correlation, equipment status, availability monitoring, maintenance information charts, etc.)
- Real time study of process and system parameters
- Synchronous graphic representation of multiple data curves mixing analogue values and events for incident analysis
- Retrieval facilities allowing post event analysis (in graphical or tabular format for instance).

Standard and easily configurable supervision tools shall be used.

Dedicated workstations shall be installed in the CCR to access data as per project specification.

8.2 Sequence of Events

The ICSS shall provide a common Sequence of Event (SOE) facility in order to identify and record the time of all events in any part of the system (controllers of all subsystems). Retrieval, selection and printing facilities shall be also supplied.

This will require a clock synchronisation facility throughout the ICSS system. Special attention shall be paid to the quantity of events to handle with the risk of data loss. It shall be safeguarded even in the case of power failure.

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

In case SOE function can not be common for all subsystems, dedicated SOE shall be provided per subsystem. However this alternative is not the preferred solution.

8.3 Maintenance System

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

- HMI diagnostics interface providing detailed displays showing the diagnostic of all subsystems parts, package systems, package digital links, power supplies and networks. When hot spare is provided, it shall be connected to the ICSS and fully monitored
- Facility for configuring and downloading any part of the ICSS application software. 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 release management
- Application software simulation, testing and debugging with user-friendly interfaces
- Software backup management (including configuration, operating system and network)
- Automatic documentation for the whole application.

9. ICSS Performances

The minimum performance requirements shall be under the worst conditions:

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 logic algorithm in the same controller (from sensor input to output to actuator).	1 sec max
Update of data on the active display	1 sec max
Calling up a display	2 sec max
Network load	30%
Additional communication time for data exchanged with external systems	1 sec max

Dependant 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.

10. Packages interface

In general, packages with their own control system shall be supervised and controlled on a higher level from the ICSS.

Communication between these packages and the ICSS shall support commands and information required for control, operator interface, and TIS functions. Communication shall be supported by digital links. However, in the case where only a small amount of data is required to be transferred, then hardwired links shall be preferred.

ICSS shall generally be the master for time synchronisation.

11. Cyber Security

11.1 Introduction

In recent years, Distributed Control System (DCS), Supervisory Controls and Data Acquisition System (SCADA), Process logic Controller (PLC), process control and industrial manufacturing systems referred in this document as Integrated, Control and Safety Systems (ICSS) have increasingly relied on commercial information technologies such as “Ethernet”, “TCP/IP” and “Windows” for both critical and non critical computing and communications.

The use of these commercial protocols and operating systems has made the interfacing of control equipment much easier, but there is now significantly less isolation from the outside world. Network security problems found on the world and enterprise networks can now be passed to ICSS process control networks and operating systems.

This part of the specification gives the requirements to minimise the risks when designing an ICSS.

11.2 Architecture

The ICSS network shall be physically and functionally independent from the TIS network (Office LAN).

The ICSS shall not be connected to the TIS network unless a specific need has been identified and is required. This connection shall be provided via the PDS.

One ICSS shall have at most only one connection point to the TIS network through a dedicated security device (FIREWALL) whose purpose is to filter the traffic between ICSS and TIS network (Ref to [ISA SP99](#)).

Architecture shall be designed in such a way that all functions shall be implemented on the right equipments, in accordance with the reliability/safety and cyber security levels. As an example, operator workstations shall not be used for production management, and control function shall not be implemented on PDS.

11.3 Operating System

Operating system of all equipments within the ICSS shall not be accessible to operator or maintenance team, but only to the assign ICSS administrator (Engineer access: see 7.6.1) with specific access rights and strong authentication. This shall also be the case at power-up.

External mass storage devices (Floppy, CD-ROM, etc.), interfaces ports (serial, USB, etc.) and central processing units, shall not be functionally and/or physically accessible; this can be achieved for example by BIOS configuration or by physical protection (locked enclosure or cabinets).

Configuration of the operating system shall be described in a dedicated document, with restoration procedure after crash.

Antivirus software shall be installed on all ICSS workstations and servers. Configuration of the antivirus software is the responsibility of VENDOR, in order not to impair the behaviour of the device (specifically the operator control workstations). An ICSS server (for example the maintenance/engineering workstation) shall allow for regular updates of all workstations antivirus data base after the manual download of the server.

11.4 Industrial Networks and communication

If any of the ICSS networks uses a share media like public telephone lines or radio links share with other functions (voice/IT data) in order to connect two separate industrial networks, at least a VPN (Virtual private Network) shall be implemented in order to secure the connection.

In case of remote control through radio communication (e.g. satellite platform), a specific study shall be made with Telecom specialists in order to define the need to implement a VPN.

ICSS network configuration shall be described in a dedicated document, with restoration procedure after crash including back-up procedure.

11.5 Physical protection

Care shall be taken in physical location of sensitive devices in Control Room and Technical Rooms. A specific assessment shall be performed.

A computer ICSS specific maintenance (or engineering/computer) room shall be design with restrictive and controlled (code/badge) physical access to all sensitive sub-systems. These subsystems are, but not limited to: configuration workstations, data bases of ICSS configuration, Historical data base, network management tools, network and security devices.

The requirements of § 11.3 (access to mass storage/interface ports, etc.) are not applicable for the sensitive equipments located in the access restricted maintenance room.

Control and technical rooms that do not require a permanent human presence shall be locked and protected by access control systems and shall include tracing/recording mechanisms (i.e. detectors and/or door switches connected on ICSS I/O's with alarm).

11.6 SSS and FGS

All the safety dedicated networks supporting engineering work station or sequence of event recorder or the specific SIL certified safety digital link shall be physically independent and not connected to any other network.

Programming via control (PCS) ICSS network is prohibited and is locked by password/key.

The maintenance/engineering workstation shall be dedicated to SSS & FGS and access restricted (physically and functionally).

11.7 Human Machine Interface (HMI)

A specific access assessment study shall be performed with the HMI design.

Operator workstations should not be used as operator interface for functions not directly related to control. Similarly, control HMI should not be implemented on other functions dedicated equipments (for example PDS consoles).

As per §11.3 all mass storage and interface devices should not be accessible to operator. Physical protection of the central processing units shall be implemented.

At power-up the operator workstation shall be initialized in the “visitor access” mode. For workstation installed in a remote non-permanently manned technical room, after a time out the workstation shall automatically switch back to the “visitor access” mode or power off.

11.8 Process Data Server (PDS)

11.8.1 General requirements

The PDS shall be the dedicated interface between the ICSS and the TIS.

It shall be always possible to disconnect physically the ICSS to TIS (Office LAN) link at any time in case of high cyber risk coming from the office LAN. However the main ICSS functions should not be affected after disconnecting the link.

The outbound traffic from ICSS to the TIS network should be limited to essential communication. In a client – server connection from the ICSS to TIS network, an outbound traffic is when the client is within the ICSS domain and the server outside (see [ISA SP99](#)). Inbound traffics are not permitted without strong authentication and virtual private network (VPN) implementation (see [ISA SP99](#)).

The PDS shall be implemented within a firewall Demilitarised Zone (DMZ: see [ISA SP99](#)) as it communicates with both ICSS network and TIS network (office LAN). ICSS data shall be transferred in the PDS under an outbound traffic from ICSS network.

A specific study shall be performed to describe all the detailed mechanisms for communications through the firewall (source, destination, service or port allowed, purpose) in order to be validated by COMPANY security specialists and to configure the firewall.

Means to back-up historical data and configuration (system/network/software and application) shall be implemented.

11.8.2 Firewall

A firewall (see [ISA SP99](#)) shall be implemented for each ICSS brand, either by field or by platform; this is to avoid the propagation of incident and to avoid uncontrolled traffic between functionally independent systems.

PDS (process data server: PC type machine + software products like IP21 or PI + historical data base) shall be implemented in a DMZ (Demilitarized Zone) of the firewall. The PDS belongs to the control domain.

Additional firewalls may be required in case of centralized affiliate administration of the ICSS.

A specific study shall be performed to define in detail the architecture around the fire wall.

The following rules shall be applied for firewall configuration:

- The base rule set shall be DENY ALL, PERMIT NONE
- Ports and services between the ICSS environment and an external network shall then be enabled and permission granted on a specific case by case basis. The authorised flux will be approved by COMPANY
- All “permit” rules shall be IP address, TCP/UDP, service and port specific
- All rules shall restrict traffic to specific IP addresses
- Any non-IP protocol shall also be filtered

- Traffic should be prevented from transiting directly from the ICSS to the office LAN. All traffic should terminate in the DMZ
- To improve insulation, any protocol/services between the ICSS and DMZ should not be explicitly allowed between DMZ and TIS office LAN (and vice-versa).

All outbound traffic from the ICSS to the TIS network through the DMZ will be source and destination restricted by service and port using static firewall rules.

Firewall brand shall be specified by COMPANY (Netscreen 25), the configuration will be performed by a COMPANY appointed personnel.

Firewall configuration is confidential and shall only be disclosed to an agreed restricted list of persons.

11.9 Maintenance

Direct connections from ICSS (PCS or package) to outside world (internet or other) for maintenance purpose through modems for example are not allowed. A specific study shall be performed for remote access implementation. Remote connection and maintenance shall be allowed after a detailed study between VENDOR and COMPANY.

ICSS Maintenance tools

The ICSS shall be supplied with access management tools allowing for ID/password control and management with logging of access requests.

ICSS internal networks shall be monitored by a dedicated management tools (ICSS dedicated). They shall be provided by VENDOR and shall comply with the COMPANY Standard (GS TEL 170). They shall enable configuration, diagnostic of all networks equipments (Hub/Switches/routers, etc.).

11.10 FAT

Specific tests shall be performed to demonstrate the conformity to specification:

- Testing of ICSS to TIS communication with the configured Firewall
- Testing of antivirus running to verify impact on control and detection capability
- Testing of antivirus update procedure
- Test of network and access administration tools (password/key management, configuration of network equipments, etc.)
- Testing of operating system and network configuration vulnerabilities (using specific tools: i.e. ISS software)
- Testing of all back-up procedures (operating system and network configuration, historical data, specific and application software's)
- Testing of all restoration procedures (operating system and network configuration, historical data, specific and application software's).

11.11 Documentation

A specific document shall contain all related cyber security documents:

- Operating system configuration detailed document (including list of services)
- File system permission description detailed document
- Network configuration detailed document (including list of services)
- ICSS to TIS communication description, this includes the detailed description of the PDS communication mechanisms (list of source/destination/services & ports/function)
- Antivirus configuration detailed document
- Antivirus update and running procedure (system side)
- Back-up and restoration procedure for operating system, network configuration
- Back-up and restoration procedure for Archive and Historical Data
- Back-up and restoration procedure for specific and application software.

12. Spareage Requirements

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

- | | |
|---|-----------------------|
| • Networks and communication capacity | 50% |
| • Installed input/output (per I/O type and per system) - Note 1 | 10% |
| • Spare space for additional slots per subsystem - Note 2 | 10% - minimum 2 slots |
| • 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.

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

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

13. Factory Acceptance Test (FAT)

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

The SUPPLIER shall prepare a full test procedure prior to testing. Specific requirements are described in Appendix 3.

14. Documentation

See Appendix 4.

15. 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).

16. Specific Cases

16.1 PSS combined with SSS

As per **GS 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 SSS. This is typically the case for very simple installations and/or very low complexity packages.

16.2 FGS combined with SSS

As per **GS SAF 261**, it is acceptable that in certain cases the functions pertaining to FGS and SSS 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 modules and associated racks, along with the application software, shall remain segregated and dedicated to their function.

16.3 Requirement for USS

As per **GS SAF 261** an USS system is not compulsory if the design of the SSS is such that the SIL requirement is achieved by the SSS 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 not required.

Appendix 1 Integrated Control & Safety System function descriptions

1. I/O processing

All data shall be suitable for trend historical (short and long-term) display and recording. It shall be possible to select scan rate (time base) per parameter.

1.1 Analogue input

Analogue signal shall be 4/20 mA, 24 VDC.

All analogue inputs shall have:

- Validity checking
- Four alarm thresholds as standard.

1.2 Analogue output

Analogue signal shall be 4/20 mA, 24 VDC.

1.3 Digital input

To avoid spurious states such as switch rebound, the input shall be electronically filtered on the board.

1.4 Digital output

Output shall be either:

- Normally energised (24 VDC)
- Volt free contact.

2. Alarm processing

Alarms record fault conditions and bring plant malfunctions to the operator's attention. They do not initiate safety action.

The major sources of alarm are:

- Input open/short circuit
- System or communication failure
- Violation of an alarm limit or other change of state
- Invalidity
- A discrepancy or abnormal state.

The processing shall allow the latching of selected inputs to record transient alarm inputs.

The ICSS shall be capable of differentiating alarms of four types, categorised according to seriousness (see Appendix 5).

An alarm shall disappear after an operator acknowledgement and after the fault has been cleared. For this purpose, there shall be a button to allow all alarm types to be acknowledged.

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

A "silence button" shall be required for the audible alarm only.

Manual alarm inhibition neutralises the audible alarm and indicator blinking. However indicators continue to change colour. This option is available only at instrument technician level.

3. Inhibitions

Disabled process equipment shall be declared out of service and be functionally disconnected. Consequently a disabled input shall trigger no action on a safety bar.

The two following types of inhibition are envisaged for all inputs.

3.1 Maintenance inhibition

This is protected by a password or key; the inhibition may also be performed through a dedicated interface (Maintenance Inhibit Console with restricted access. Measured values and states shall continue to be displayed but shall not be taken into account for safety actions. Dedicated daily report will be issued, considering also the maintenance inhibitions set from the control panels of the packages.

3.2 start-up inhibition

This is an automatic action. Inhibition start-up neutralises safety actions during transitional phases on controlled equipment. It is activated using the start-up command for the equipment concerned.

It shall be automatically deactivated either by a time-out or after crossing a threshold with a time delay so that transient conditions are disregarded.

3.3 Manual start up inhibition

This is an operator action (clicking a button on screen) available only when the process is stopped. Process inhibition neutralises safety actions for a predefined period.

It shall be automatically deactivated either by a time-out or after crossing a threshold with a transient condition time delay.

The time remaining shall be displayed near the relevant input tag.

4. Time stamping of events

Events, detected errors and malfunctions shall be recorded with a maximum time tagged resolution of 1 s. This requirement is also valid for packages controlled by their own control systems through a periodic time clock synchronisation. For some packages a quick time stamping of 10 ms could be evaluated for some applications; in this case the package controller shall do the time stamping.

5. First-up detection

The first-up alarm is the first of a burst of alarms when an event occurs and shall be recorded and dated.

Thus, each subsystem (SSS, FGS, PSS and package systems) shall have a routine to initiate alarm treatment and logging of first-up faults on each safety bar. In order to discriminate first alarm between different systems a general time synchronisation may be required. For a package, the first detected fault will be transmitted to the ICSS.

6. Invalidity

All analogue inputs shall be processed for invalidity detection (out of 4-20 mA range). The pertinence of a safety action related to an invalid measurement will be highlighted case by case within the functional specifications.

7. Alarm deviation between sensors

When two or more analogue transmitters are used on the same measurement (e.g. one on the PCS the other on the PSS), the inputs shall be continuously compared. A discrepancy alarm shall be generated as soon as the difference between the two indications becomes greater than a predefined limit. This comparison shall be done in the PCS.

8. Timer

All timers shall be configurable and shall be loaded with a default value during controller program initialisation. During transition phases such as process or start-up inhibition, sequence steps, etc.; the countdown shall be displayed for operator information.

Appendix 2 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 ELE 031](#).

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 (SSS, 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 ICSS shall be fed from uninterruptible power supplies, If the power supply is redundant, the ICSS shall support automatic switching between the power supplies for continuous service without risking spurious voltage effects.

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.

3. Cabinets and cabling

Two types of cabinet shall be provided:

- System cabinets (for SSS, PCS, PSS, FGS) including CPU, I/O boards, communication boards, power supplies, etc. These cabinets shall be equipped to receive all signals from and to marshalling cabinets
- 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.

All cabinets supplied shall be fully equipped, wired and ready to be installed on site.

Electronic Equipment for PCS/PSS and SSS and FGS shall be in principle installed in dedicated cubicles.

As far as possible, all components and accessories shall be housed in 19" standard rack-mount cabinets.

These cabinets shall be equipped with lifting rings, lift off doors with internal drawing pockets, removable side panels, internal lighting activated by door limit switch, forced cooling, sub-base and grounding bus bars (IPE, IE, ISE if needed, see **GS ELE 031**).

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

The general arrangement and dimensions of the cabinets shall be submitted for approval before manufacturing.

3.1 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 boards).

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.

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 systems.

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 such as I/O boards and communication boards.

The internal markings (every type of component such as I/O boards, CPU, power supplies, links at each side, termination blocks, etc.) and outside cabinets with "plastic" labels.

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.

4. I/O board specific requirements

4.1 ICSS board protection

Each ICSS board 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 boards 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 fuse protected.

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 boards 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.

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 and SSS outputs these relays must be taken into account in the system reliability and availability calculations.

4.2 I/O board types

All I/O ICSS boards 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).

4.3 I/O assignment

The following basic assignment rules shall be applied:

- Different types of inputs or outputs (digital, analogue) shall be wired on separate I/O boards
- All critical I/O loops normally implemented with a specific redundant configuration shall be hardwired to separate I/O boards installed in different racks
- All I/O loops associated with main/backup equipment control functions shall be hardwired to separate I/O modules and racks
- 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.

5. HMI specific 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). See Security Paragraph: this equipment and the CPU shall not be directly accessible
- 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 colour screen copier(s) (or colour printer) shall be multi-port devices capable of providing a screen copy for a predetermined number of workstations.

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:

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

Appendix 3 Factory Acceptance Test (FAT)

All System Configuration Standards will be tested prior to full system configuration in accordance with the procedure submitted by SUPPLIER and using a real detector of each type.

The SUPPLIER shall prepare a full test procedure prior to testing. For the entire FAT, the SUPPLIER shall make available a team and all necessary measurement, control and simulation apparatus. In addition to means of analysing network flow, ICSS parts and HMI load, response time, etc. the SUPPLIER shall provide physical means of simulating all ICSS inputs and reading all ICSS outputs.

Variable frequency signals shall be configured inside the system to simulate variable information flows. The generation and the analysis of these signals shall be done with the internal facilities of the system. Typically these signals could be triangular signals emitted from several applications. They shall be used to simulate a variable network load.

Special consideration shall be given to the following points:

- The FAT shall cover the complete ICSS. In particular, the interface and network acceptance test shall be run with real interfacing including marshalling cabinets and telecommunication equipment (at least one of each type of interfacing equipment)
- 100% of inputs/outputs and application programs shall be tested
- The “black start” shall be tested
- All communications inside the ICSS shall be tested with a full load simulation. This covers all links between ICSS parts, between ICSS and packages, all telecommunications, etc.
- ICSS functions shall be completely checked out during the FAT (including packages) and including live tests with each type of FGS detector
- Check the behaviour of the system in de-rated situation: redundancy, network alarm management, stop, start and initialisation of sub-system
- Check the system alarm view and the intervention procedures
- Each daily test will be started by a general power cut off during a few minutes. Overall diagnostics shall be performed after this interrupt.

Appendix 4 Documentation

1. Functional Design Specification (FDS)

The FDS shall be considered as a major primary document, which shall be developed in stages as the system design progress. The initial issue of the FDS shall include all hardware aspects as a minimum.

FDS shall be issued at an early stage of the detailed engineering phase of the ICSS project.

When approved, the FDS shall form the base, against which the system production plans, delivery schedule and achieved program will be measured.

The FDS shall describe the hardware and software, in sufficient depth so as to enable COMPANY to verify that the system design meets the requirements of the system specification. In particular, the design of communication interfaces shall be clearly specified.

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 detailed design shall be covered in the FDS; in particular, it shall be defined how standard software modules are grouped in software packages suitable for stand-alone validation and verification tests by means of test programs. The required test programs are considered to be an integral part of each software package, using a programming terminal for manual input and output of test data.

The structure of the FDS shall reflect the mixture of standard and special to project hardware and software required modules.

Standard hardware and software shall be covered by published documents, which will form appendices to the body of the specification. These shall be referenced in the system description, together with any information relevant to the implementation of these items in the particular system configuration.

The appendices shall include all the necessary documentation for preparation of software. Typically this documentation shall include all standard forms and procedures related to specification of the input processing, logging, control, and communication systems.

The FDS shall include a functional description using the Principle for Application Software Design (GS INS 150).

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

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.

A test platform and test procedures shall be set-up to demonstrate the validity of the FDS. Final FDS document shall include the test procedure and results. Tests shall be performed at an early stage of the FDS related study. The test arrangement will be as close as possible as the future site architecture specifically in term of communication network.

The importance of the FDS in the subsequent production and implementation phases cannot be underestimated.



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

2. System documentation

Documentation shall include VENDOR standard documents and project documents.

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

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.

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

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

All hardware, custom software and user manuals, shall be supplied for final agreement.

As a minimum the following system documents shall be included:

- Overall hardware and software descriptions
- Technical description of each hardware item
- Hardware maintenance manual of each component in the system
- Wiring diagrams and cable schedules
- Installation check-out documentation for all the system components
- Certified mechanical drawing of all units (including weights)
- Certified electrical connection diagrams showing all plugs, cable termination blocks and equipment
- System overall earthing arrangement
- Trouble shooting loop diagrams with field data
- File layout and descriptions
- Complete custom programs, listings correlated with unambiguous explanatory comments and headings including detailed control schedule (sequence description). Source programs and associated base program licenses shall be provided
- Software manual with software structure and program description, flow charts, and inter-program interfaces
- Users manuals
- VENDOR general and other specific documentation related to the system (including reliability figures)
- Safety certification dossier, which shall contain copies of all certificates and other documents pertaining to the safety of the system. This dossier shall be prior to the commencement of the installation of the equipment



- System hardware diagnostic programs with user instructions
- System regeneration procedures
- Description and user instructions for the operating system and all other programs and subprograms
- Program flow diagrams and source and object program listings and permanent optical and magnetic storage for all programs and subprograms
- Listings to include all mnemonics and labels and an indication of program size and approximate run time
- A write up covering system reloads, restarts and any other system user function, including procedure to add new features such as new algorithms
- Test procedures
- Certificates and reports
- List of the diskettes/CD for all programs (systems and application). Supplying genuine CD Diskette for system program with original license is mandatory, this applies also to package control PLC
- Purchasing records
- Cross reference index
- Calibration sheets
- VENDOR "Final Test Certificate" to be issued prior to FAT
- Preservation procedure
- Installation procedure
- System black start procedure
- Test reports
- Test logs.

A full description on all items shall be included. Sufficient manuals shall be provided to allow COMPANY to become familiar with all system components. Prior to system delivery, manuals, drawings, flowcharts, application program listing must be supplied to enable COMPANY to maintain both the system hardware and software on a continuing basis.

In the documentation, fault finding, test and maintenance procedures shall be clear and easy to follow; all references to parts and materials shall be clear and consistent to facilitate identification when fault finding and accuracy when re-ordering.

Appendix 5 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 use of the report **SIREP-WIB-EXERA No. M 2656 X 98 part 2**: “Ergonomics in Process Control Rooms” Design guideline could be useful.

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.

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

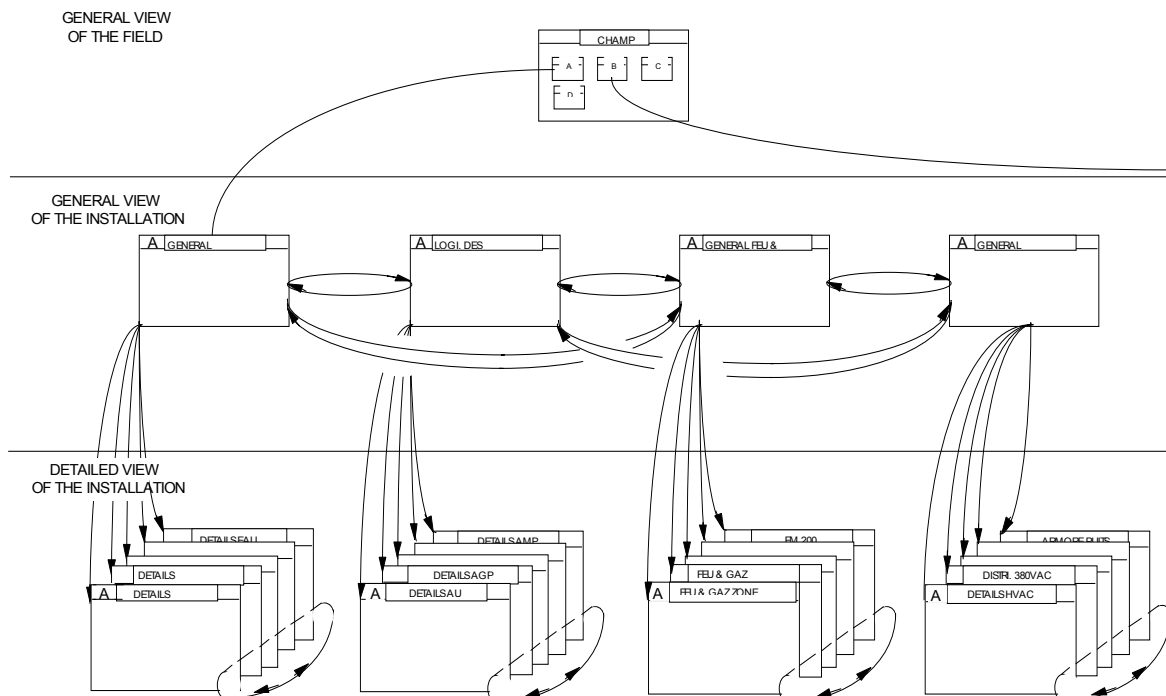
The detailed view is the display in which alarms are recognised and acknowledged.

1.2.1.4 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.

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 or override (forcing) 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.

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

Four levels of access are required:

- Monitoring access: Display of information with no commands
- Operator access: Process control: the access level required for console operators
- Instrument specialist access: Inhibition, forcing, adjusting
- Configuration access: Access to all system functions.

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)

Pointing to an item of dynamic information shall provide access to a detailed display concerning the information.

The dedicated displays associated with this information may be adjustment displays, history displays, metering displays, etc.

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.

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.

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 9.

4. Animation of mimic elements

Important note: In the figures in Appendix 9, 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
- 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**
- 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 7 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 7, 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) 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 7, 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 7, 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 7, 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 7, 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
- The scale is white
- Threshold markers are normally white, red if overshoot.

4.5.3 Animation of trend curves

(See Appendix 7, 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 7, 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 7, 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.

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.

Appendix 6 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.

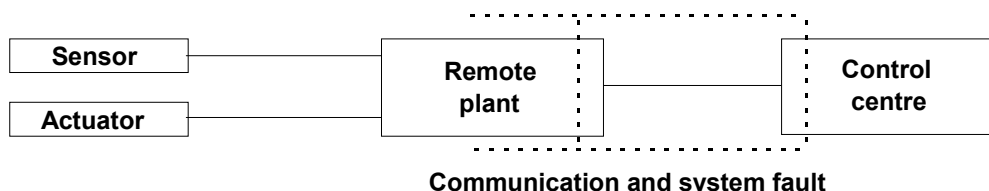
An alarm may be disabled automatically by the system in the following circumstances:

- 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.



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.

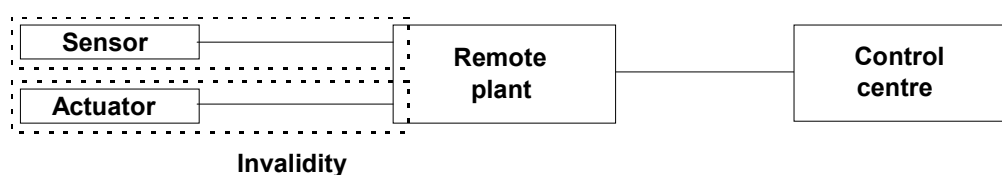
History curve: Computerised display of multi-plot records. This offers additional functionality, including: time stamping, zoom, grouping, etc.

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 importance attached.

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.

Appendix 7 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)



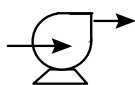
Command part
Controlled part

SDV (Shut Down Valve)



Command part
Controlled part

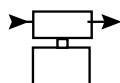
ESDV (Emergency Shut Down Valve)



Controlled part

Command part

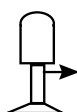
Centrifugal pump



Controlled part

Command part

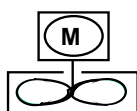
Positive displacement pump



Command part

Controlled part

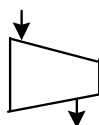
Immersed pump



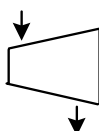
Command part

Controlled part

Air-cooler exchanger or agitator



Compressor



Turbine



Electric motor



Opened

Unstandardized power cut-off device



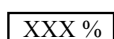
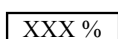
Closed

2. Static symbols

(Non exhaustive Examples)



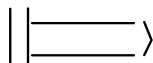
HV (Hand Valve)
Block valve without limit switches



Control valve / choke
HCV (Hand Controlled Valve)



Restriction orifice (fixed pressure drop)



Scraper trap

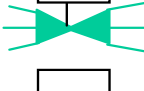
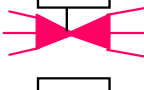
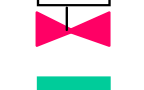


Check valve

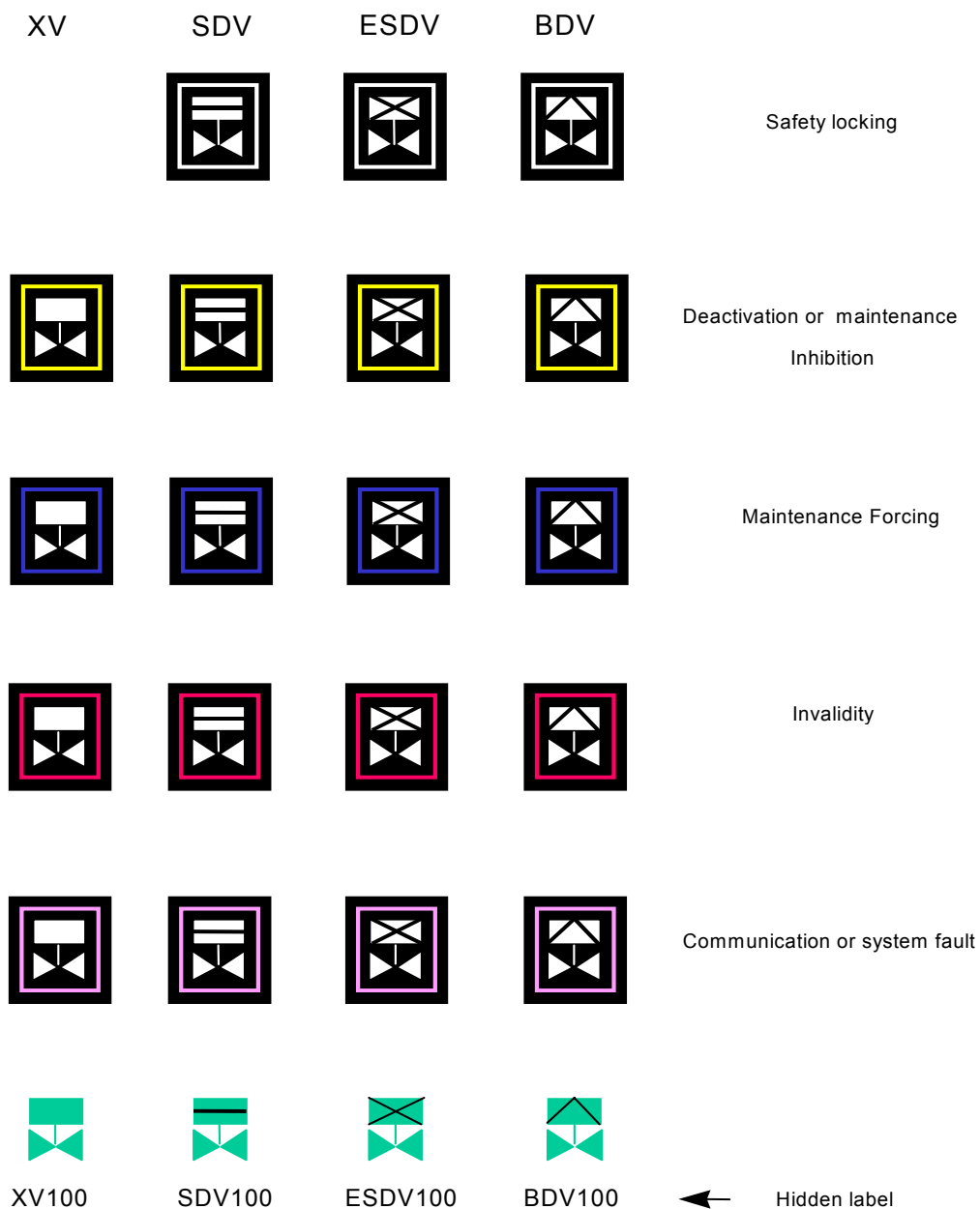
Note: Below colours are indicative and may be changed in project specific specifications.

3. On/off motorised valve

3.1 Animation of the command and controlled parts

Block diagram	Label	
		Safety logic diagram
	White	White
	White	
	Fluid	White
	White	
	Fluid	White
	Fluid blinking	
	Fluid	Blue
	Fluid	
	White	Blue
	Fluid	
	White	Blue
	Fluid blinking	
	White	Red blinking
	Red blinking	
	White	Red
	Red	
	Fluid	Red blinking
	Red blinking	
	Fluid	Red
	Red	
		
ROV100		Hidden label

3.2 Animation of the frames



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

5. HCV, PCV (control valves)



White

Valve closed



Fluid

Valve open

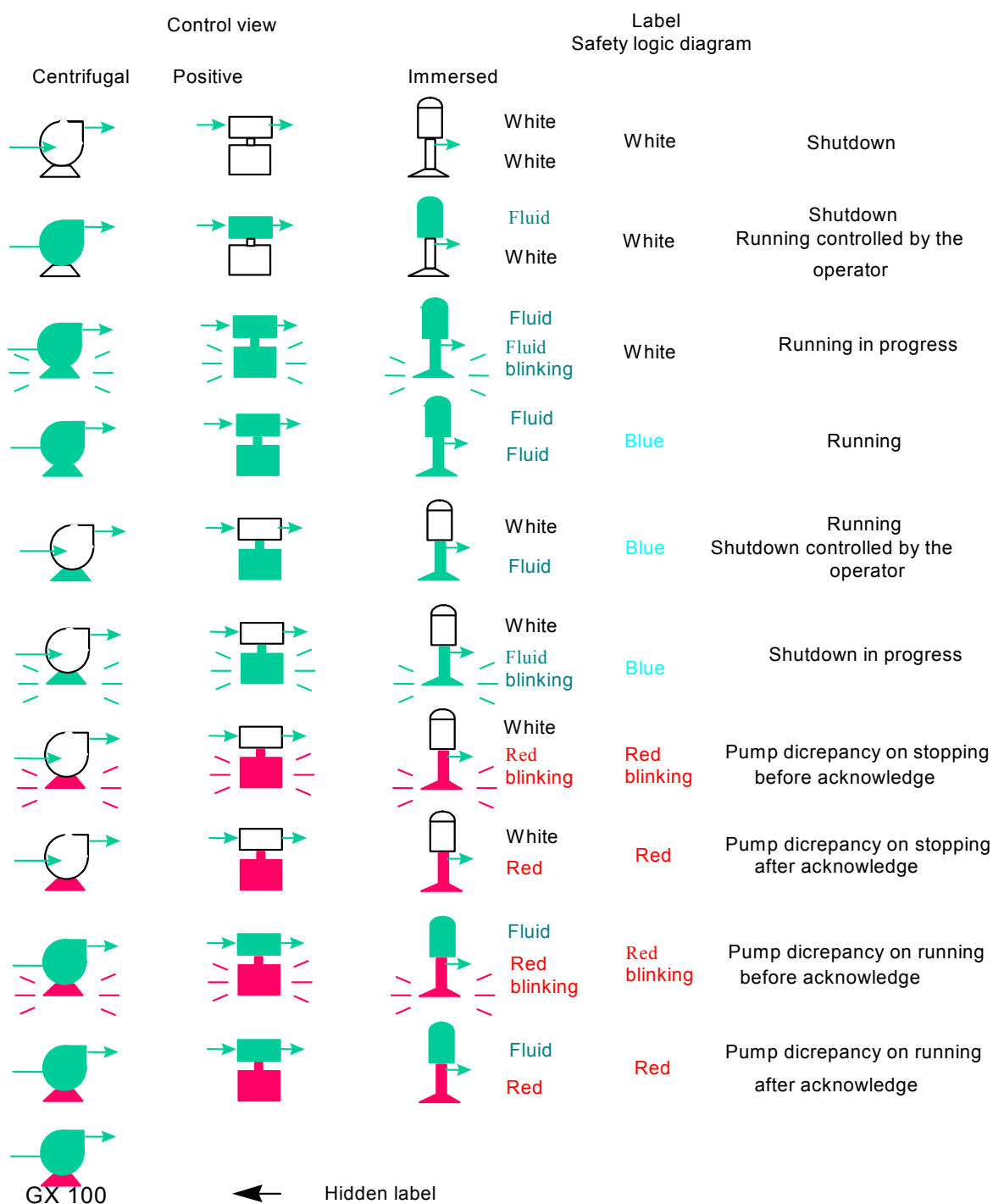


Fluid,
blinking

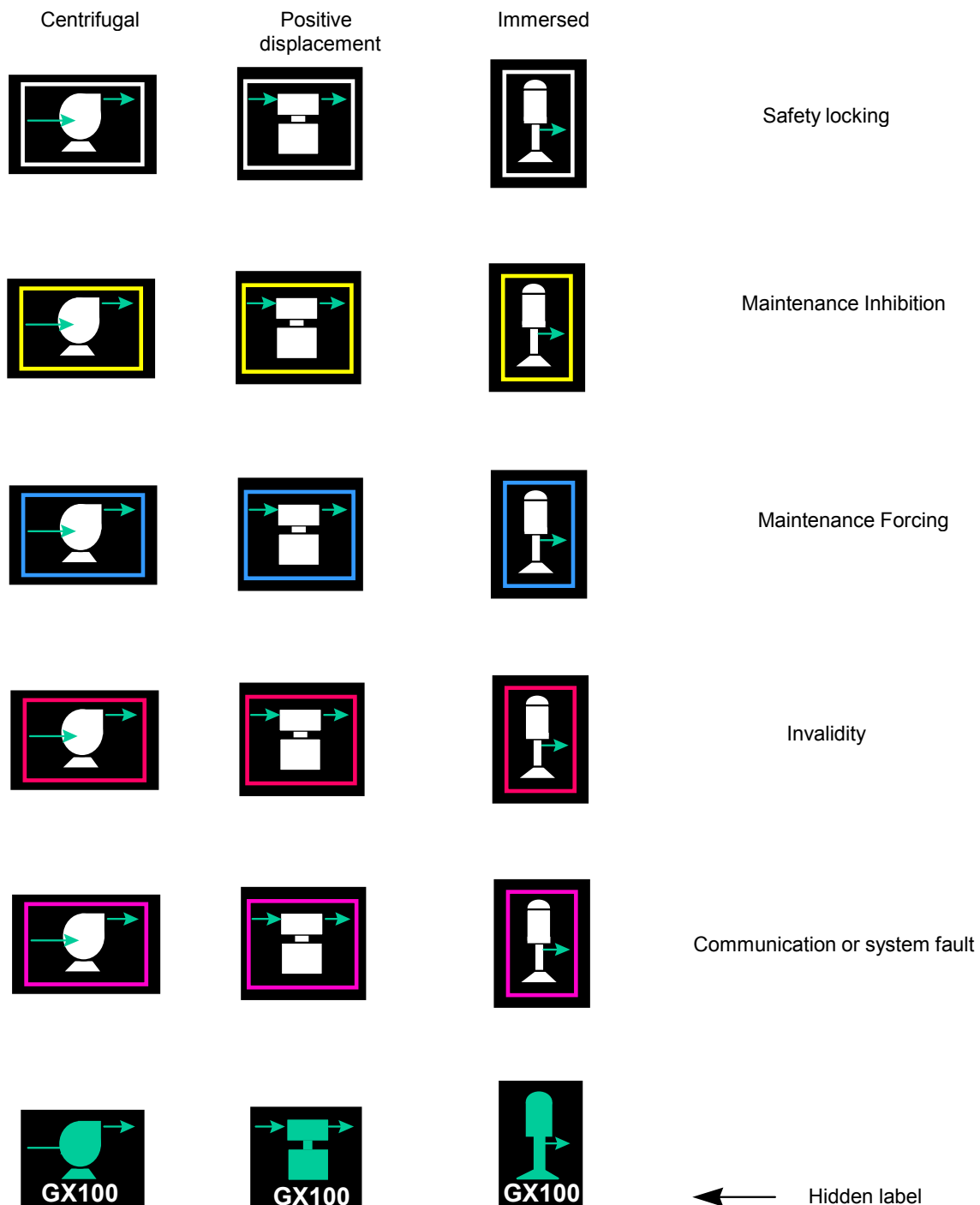
Actuation in progress

6. Pumps

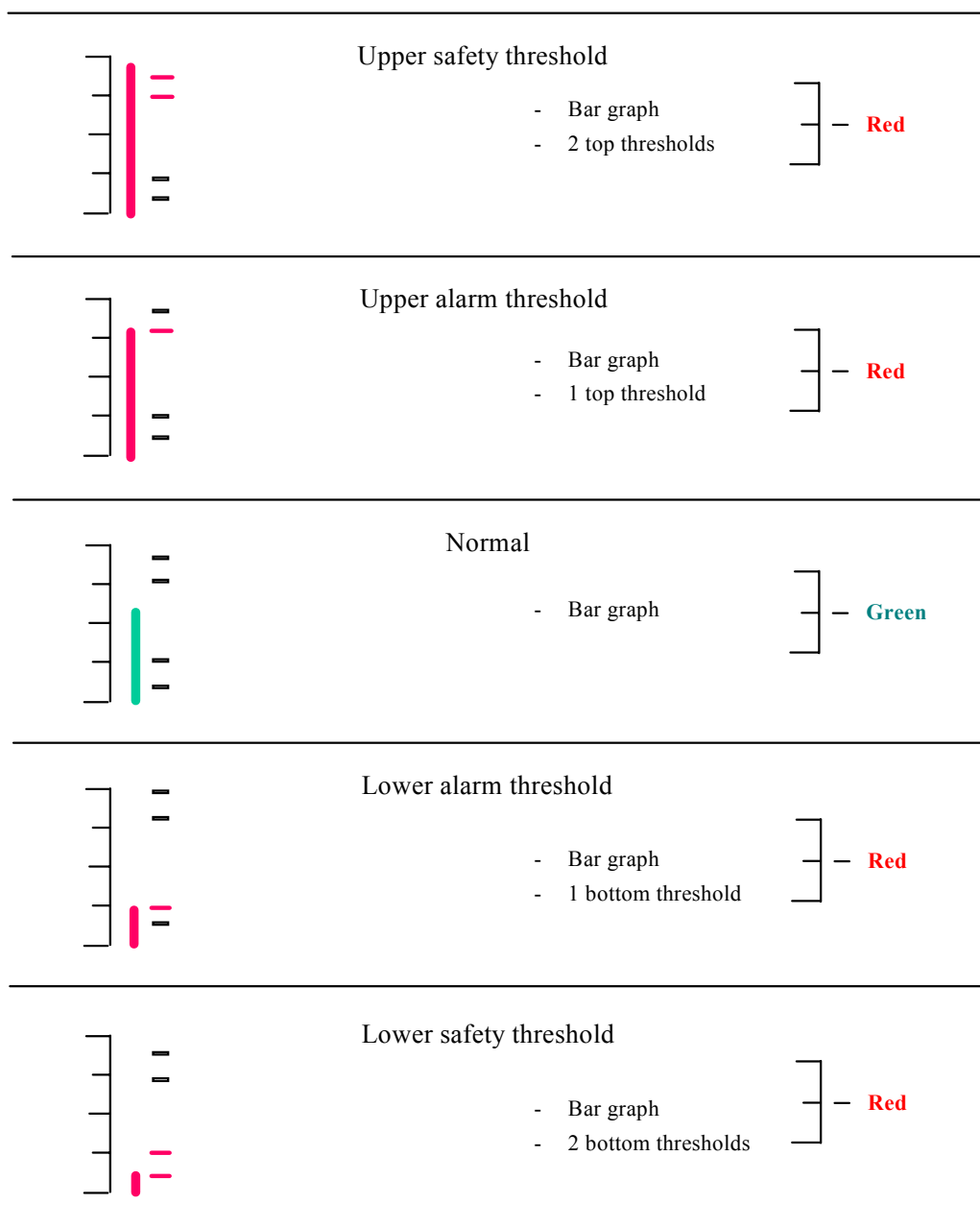
6.1 Animation of simple equipment



6.2 Animation of the frames



7. Bar graph

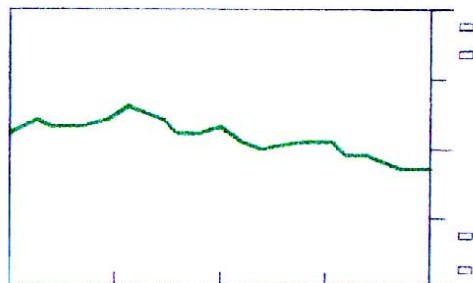


NOTE: Fault detection
after acknowledge

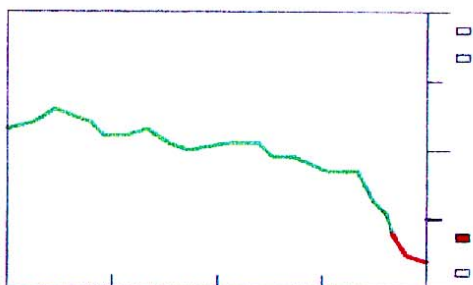
: **Red blinking.**

: **Red.**

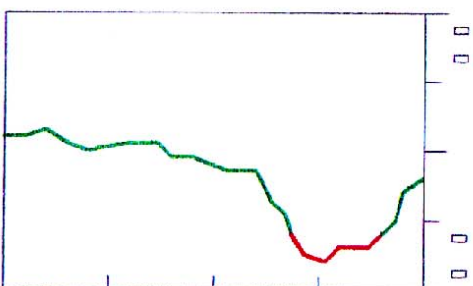
8. Trend curves



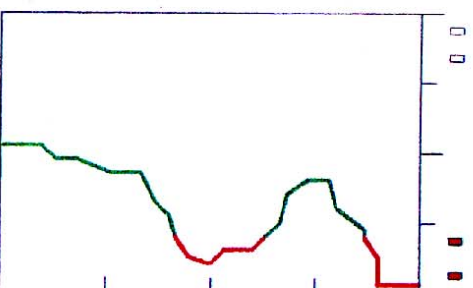
Curve within the thresholds



Lower alarm threshold overshooting



Threshold overshooting storage



Lower safety threshold overshooting

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



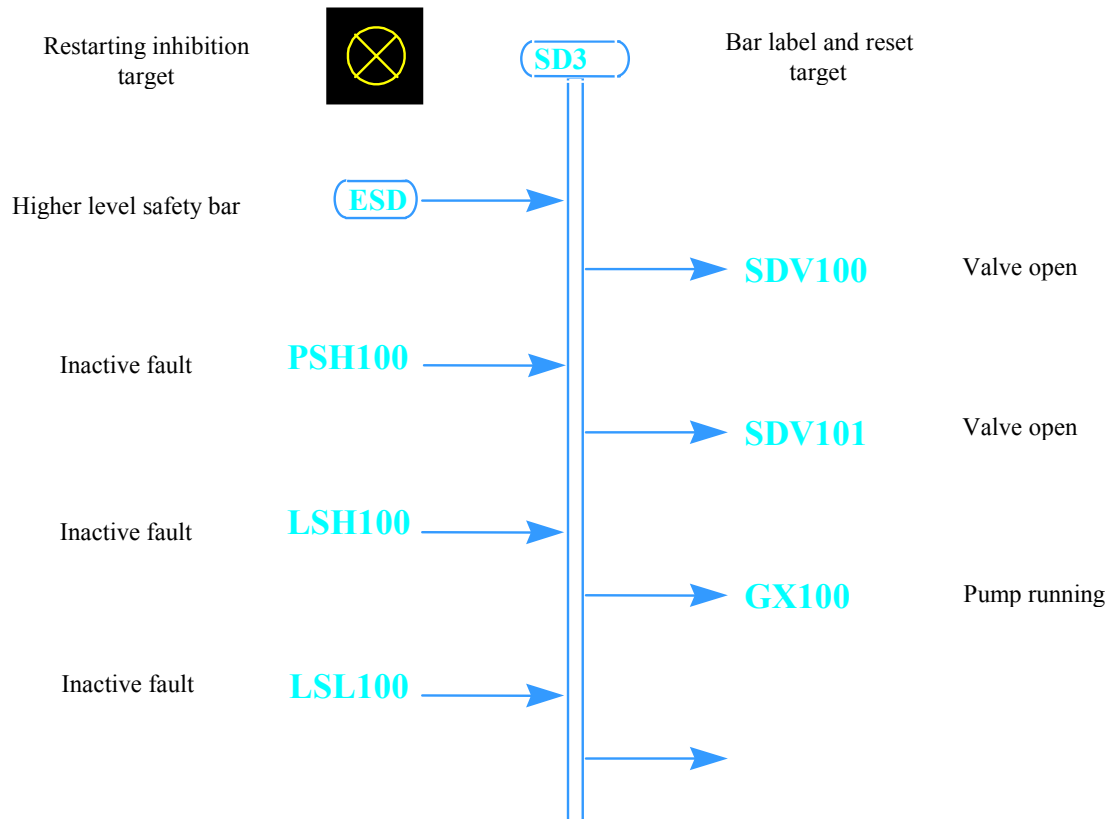
Invalid sensor



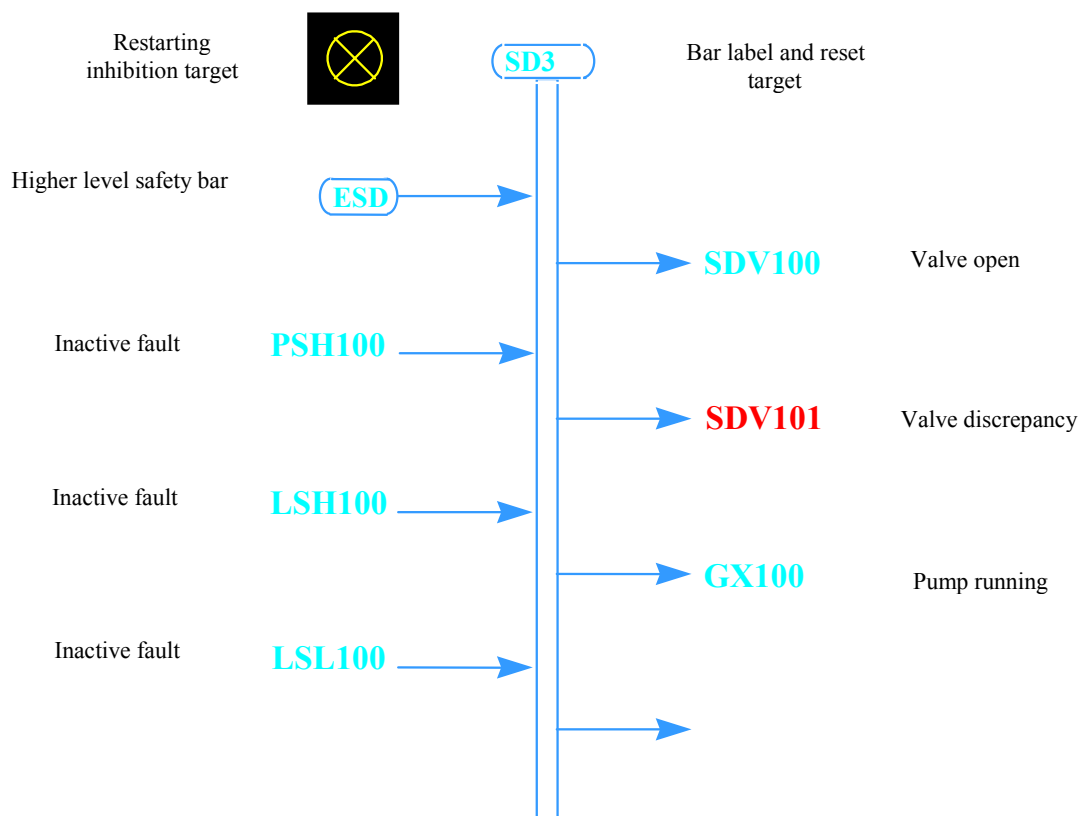
Communication or system fault

10. Safety logic diagram

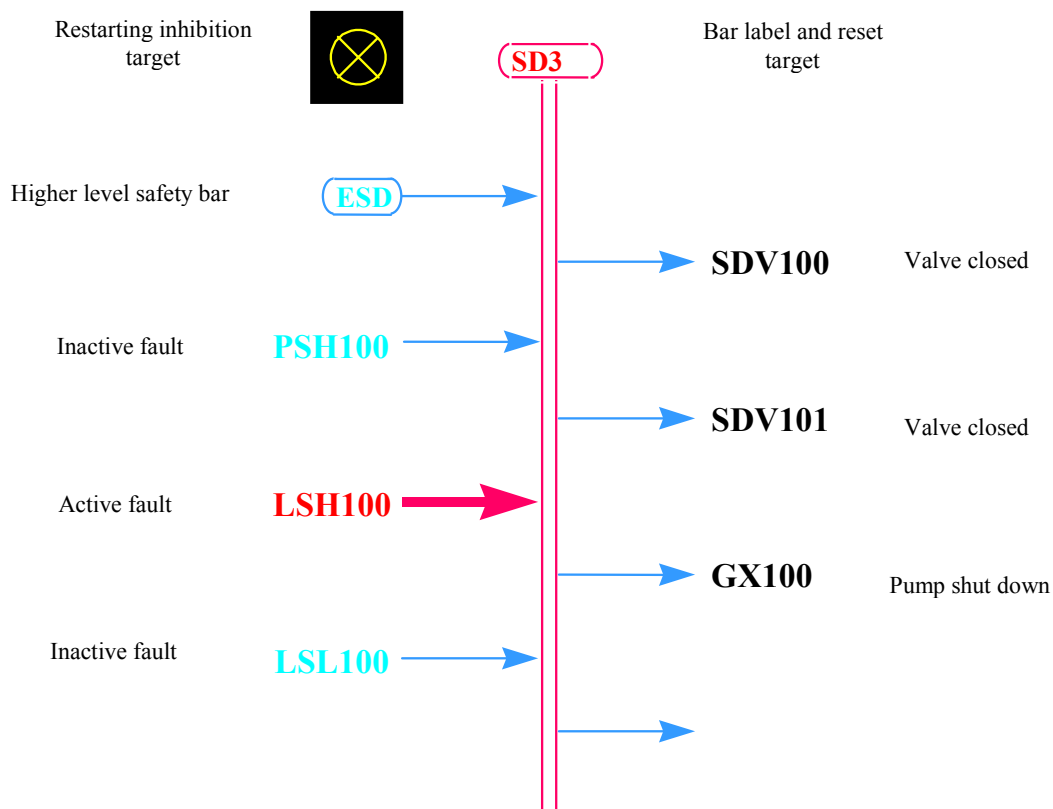
10.1 Armed safety bar



10.2 Armed safety bar - Valve discrepancy



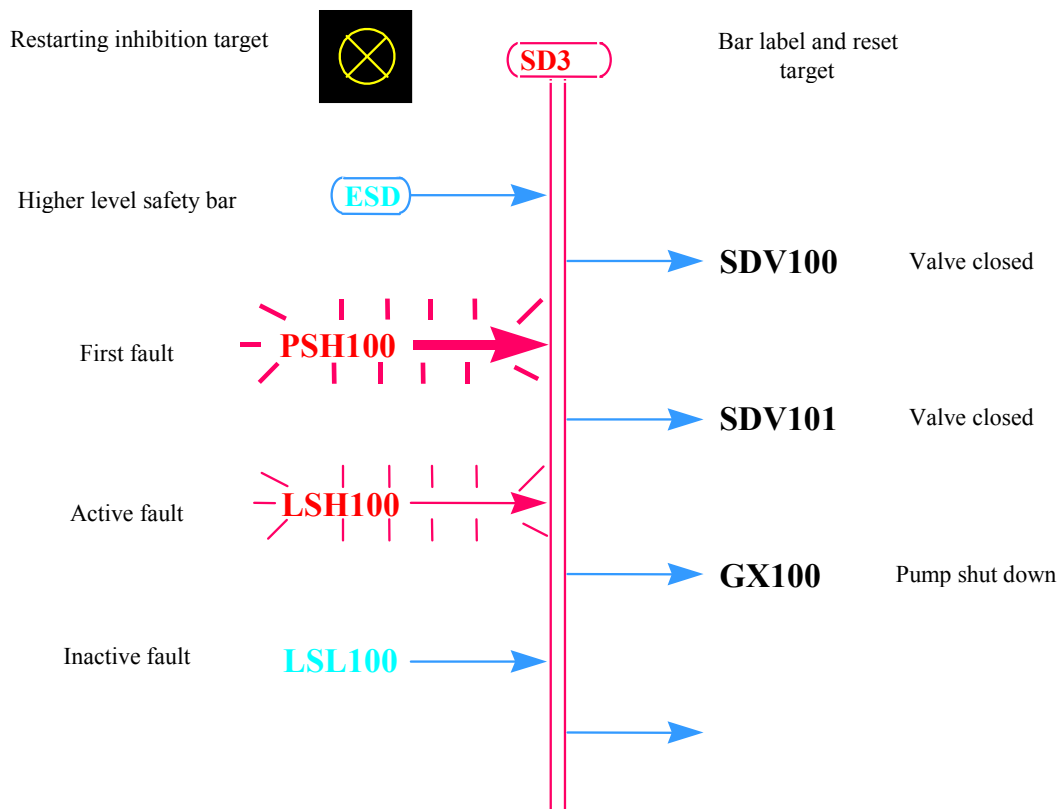
10.3 Safety bar with a fault



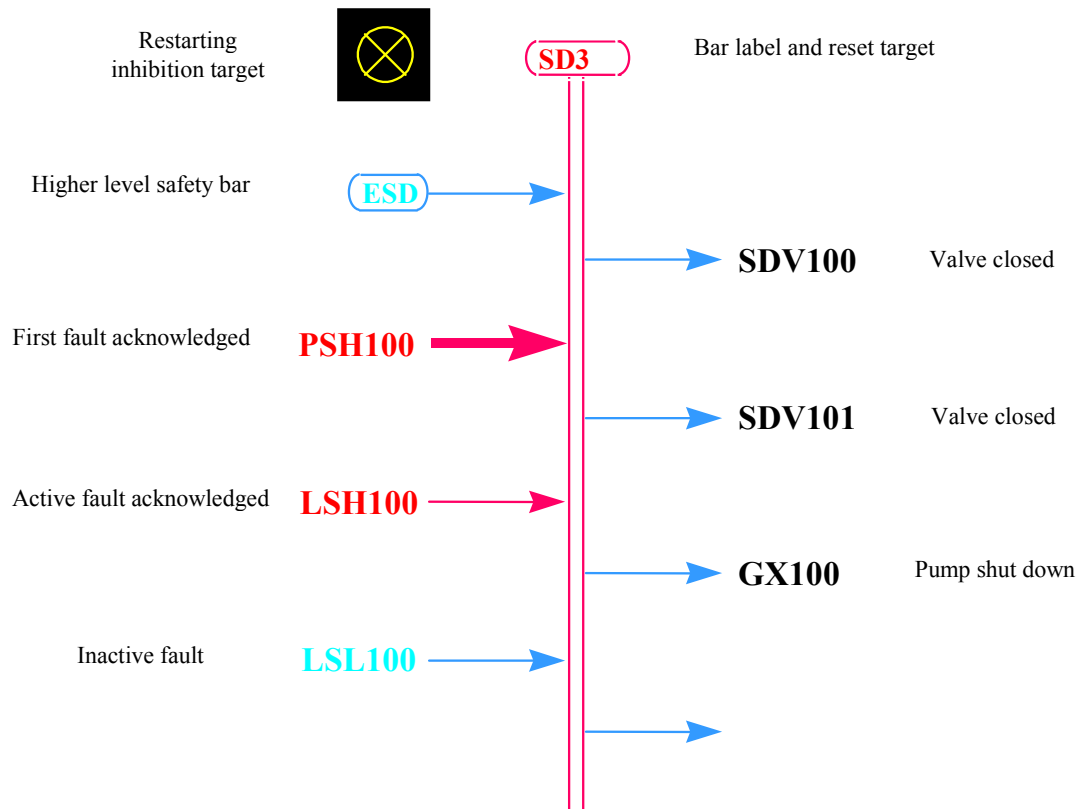
NOTE :

Fault detection	:	Red blinking.
after acknowledge	:	Red.

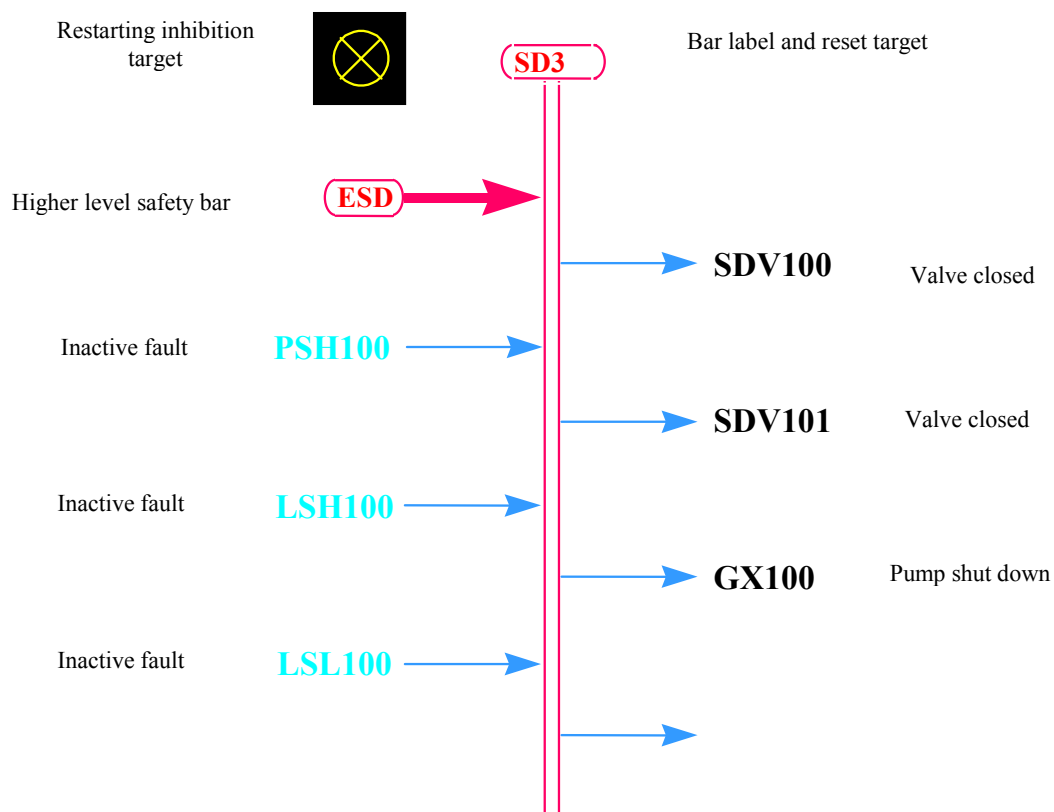
10.4 Safety bar - Fault chain with first fault before acknowledge



10.5 Safety bar - Fault with first fault after acknowledge

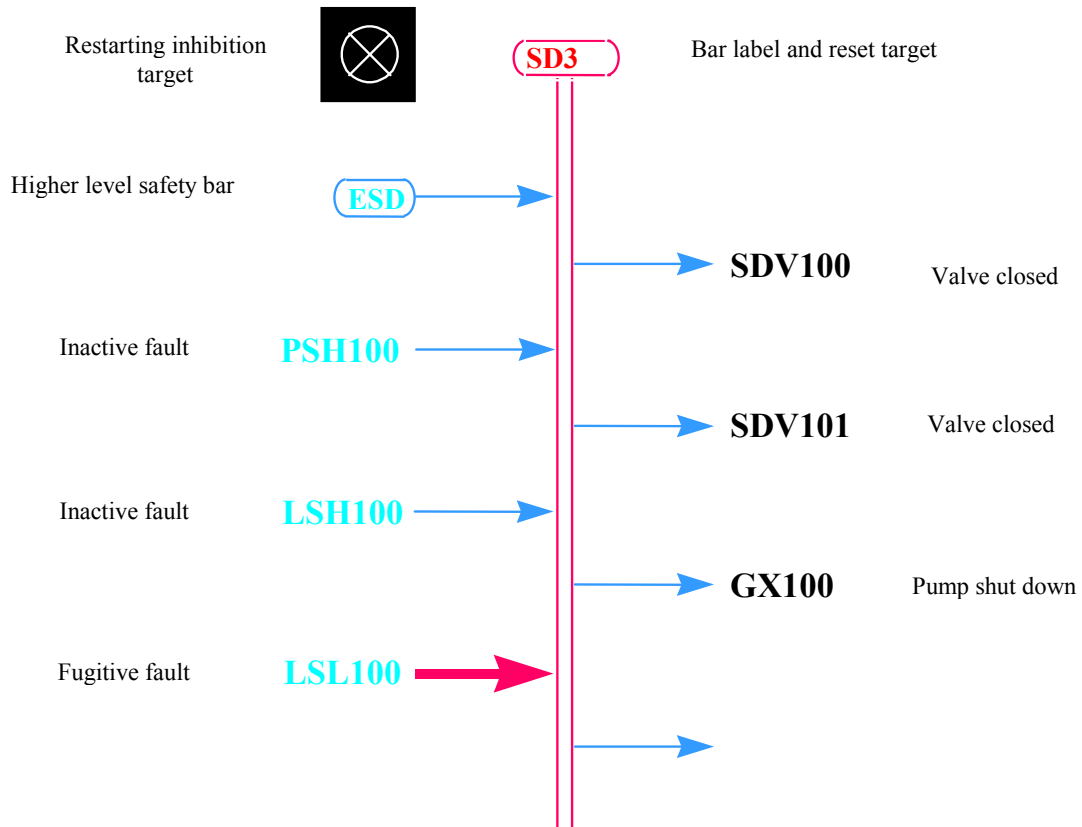


10.6 Safety bar - Higher level fault



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

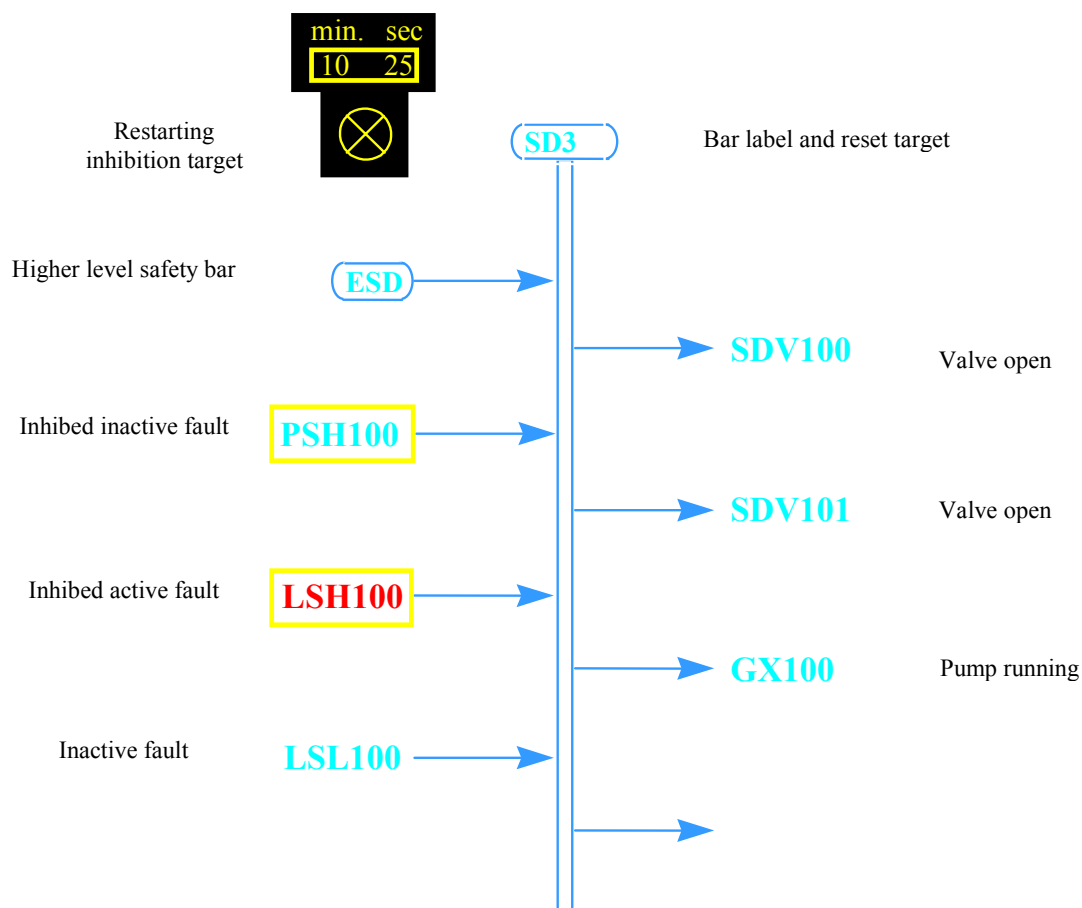
10.7 Safety bar with a fugitive fault



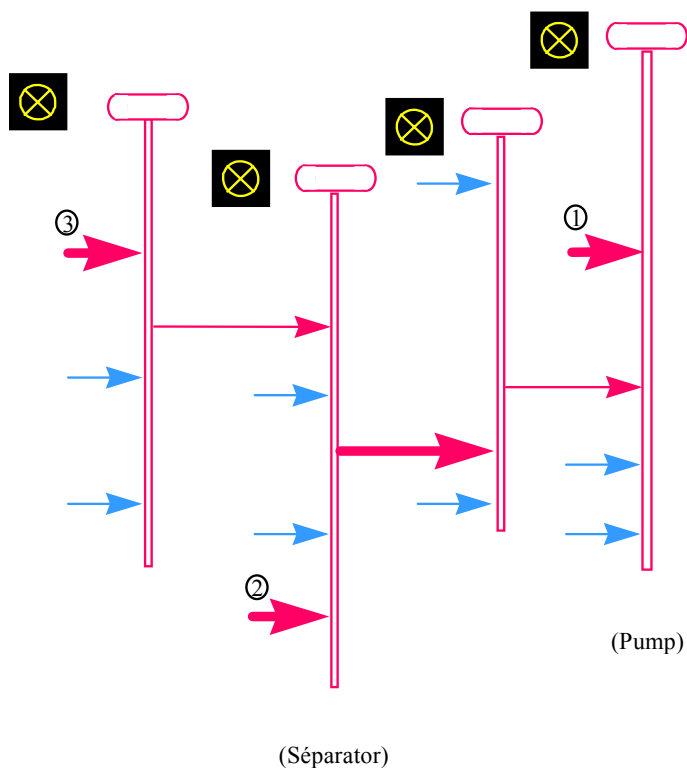
Fault having disappeared before acknowledge : Blue label blinking.
Red arrow blinking.

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.