Safety Requirements Specification

Sub-sea High Integrity Pressure Protection System

Genesis has extensive experience in the design of high integrity pressure protection systems (HIPPS) for both surface and sub-surface offshore installations.

HIPPS are frequently used in oil & gas sub-sea completions, when the pressure rating of the sub-sea production pipeline is less than the closed in tubing head pressure of the sub-sea wells. For these applications, the installation of a fully rated production pipeline would be prohibitively expensive and so a HIPPS is used to provide the necessary protection. Safety instrumented systems (SIS) of this nature are normally designed to IEC 61508 and IEC 61511 to mitigate the potential commercial risk arising from loss of integrity of the production pipeline. This safety requirements specification (SRS) highlights the important features of a typical sub-sea production pipeline HIPPS.

Key Features

- High integrity pressure protection (HIPPS) up to SIL 3 in demand mode
- Designed for a sub-sea environment
- IEC 61508 / IEC 61511 compliant
- Configurable solid state logic solver
- Simplex input / output structure
- Dual sensor pressure transmitters
- 6 dedicated analogue inputs
- 2 dedicated digital outputs
- Hard wired configuration of set points
- Dual redundant control and power systems
- High level of security to prevent unauthorised changes
- Designed to facilitate functional testing
- Human machine interface
- Remote trip reset facility
- Remote closure of valves facility

Applications

- Sub-sea wellhead completions
- Sub-sea production pipeline protection
- Sub-sea installation with supervisory control via topside master control station (MCS)

Description

HIPPS designed to protect sub-sea production pipelines demand a high level of design integrity because of the frequently hostile environments they operate in.

Following installation of a sub-sea HIPPS, access for modification or maintenance is very difficult, if not impossible. It is therefore essential that the design process is robust to ensure loss of function in service is minimised.

IEC 61508 and IEC 61511 both provide a comprehensive and robust structure to the design process through a lifecycle approach. The lifecycle process covers the complete life of the safety instrumented system from initial hazard and risk assessment to final decommissioning. Its purpose is to minimise systematic error in the design process.

The safety requirements specification is particularly important because independent research conducted by the UK Health and Safety Executive reveals the main source of failure in the design process to be in the specification of systems and equipment.

WRITE PROJECTS

1 SAFETY REQUIREMENTS SPECIFICATION

A safety requirements specification is a key document in the safety lifecycle design of any safety instrumented system. Its purpose is to describe the safety function to be performed and the required safety integrity level to be achieved. The specification then goes on to describe the hardware and software (if applicable) features together with other necessary functions. The following are the key parts of a sub-sea HIPPS safety requirements specification.

1.1 System Component Configuration

In safety instrumented systems with a target integrity level of ≥SIL 2, architecture plays an important role. For this reason, the following sub-system configuration is typical for a sub-sea HIPPS package.

- dual two out of three (2oo3) voted pressure sensors
- dual redundant 2oo3 voted solid state logic solver
- simplex 1oo2 voted barrier valves

Sub-sea HIPPS packages are normally located on the sub-sea manifold where additional non-safety related systems are installed to provide supervisory control and status monitoring to a topside MCS, situated on the receiving platform.

1.1.1 Mode of Operation

HIPPS typically operate in 'Demand Mode', defined by IEC61511 as:-

'Demand mode is where a specified action (for example, closing a valve) is taken in response to process conditions or other demands. In the event of a dangerous failure of the safety instrumented system, a potential hazard only occurs in the event of a failure in the process or the basic process control system.'

1.1.2 Process Operating Modes

The actual process can be in one of several operating modes so it is important that the design of the HIPPS can accommodate all of the anticipated states. The normal operating mode is defined as routine steady-state operations. Abnormal operating modes may be any or all of the following.

- Process start-up
- Individual well / manifold start-up
- HIPPS safety instrumented system (SIS) test
- Sub-system maintenance
- Process shutdown

The HIPPS function design should include for all of the above operating modes (normal and abnormal), with the exception of HIPPS SIS test and sub-system maintenance.

1.2 HIPPS Functionality and Integrity

1.2.1 Equipment Selection

Equipment items selected for use as safety critical components in the HIPPS should be either certified compliant with IEC 61508 or have a valid 'Proven in Use' Case to support their selection (reference Routes 1_H and 2_H in IEC 61508).

1.2.2 Pressure Isolation

Two barrier valves, installed in series within the manifold pipework, provide pressure isolation. The barrier valves are connected to the logic solver via interface electrical/hydraulic directional control valves. As noted above, the barrier valves are configured as a 1oo2 voted system and each valve must be capable of complete pressure isolation acting individually.

1.2.3 Pressure Detection

Three pressure transmitters are located between the barrier valves in the manifold pipework. Each pressure transmitter contains dual pressure sensors providing dual redundant signals to the solid state logic solver. Pressure transmitters are 'close coupled' without isolation valves to prevent clogging of impulse lines and to reduce the effects of production pipeline vibration. An installed fourth pressure transmitter is advisable as a maintenance spare for connection by a seabed remote operated vehicle (ROV).

1.2.4 Logic Solver

The normal choice of logic solver for this type of application is an IEC 61508 certified SIL 3 hardwired configurable device. It only contains input and output connections for six pressure sensors and two barrier valves. The architecture functions as a dual redundant 2oo3 voted device containing dual redundant safety critical control boards (SCCBs).

1.2.5 System Integrity

The HIPPS has limited functionality in that its primary purpose is to detect pressure and close isolation valves in the event of the measured pressure being in excess of the set trip value. This is a necessary feature of the HIPPS to ensure it retains its design intent of being a high integrity system, i.e. the system is dedicated and has no other functionality.

1.2.6 Surface to Sub-surface Connections

Electrical power, hydraulic power, communications signals and utilities (such as Methanol to prevent hydrate formation during start-up) are contained in an umbilical bundle connecting surface to sub-surface systems.

1.2.7 Action on Loss of Power

In dormant protection systems typical of HIPPS installations, the preferred action on loss of electrical or hydraulic motive power is to de-energise to trip to achieve a failsafe design intent. In this case, the barrier valves move to their safe state, i.e. the closed position.

1.2.8 Redundancy

Redundancy is a function of the architectural constraints of the sensor, logic solver and final element sub-systems. Complying with architectural constraints requirements is an integral part of completing the SIL verification of the HIPPS safety instrumented system. For high SIL systems, it may be necessary to consider both redundancy and diversity in the choice of component parts.

1.2.9 Diagnostics

The logic solver should be equipped with diagnostics so that in the event of a failure in one of the dual redundant SCCBs, the remaining board assumes control. Should the second board fail then the output channels should trip, bringing the HIPPS barrier valves to the safe state.

A similar set of diagnostics should monitor the input and output sub-systems so that detection of a fault in either sub-system, should cause the logic solver to trip the HIPPS barrier valves to the safe state.

1.2.10 Overt Faults

If an overt fault occurs during normal operation, then this should result in a vote to trip. If repair of the system is not possible within the mean time to repair (MTTR) assumed in the SIL verification calculations then the HIPPS should be manually shutdown from the MCS until the fault can be repaired.

1.2.11 HIPPS Reset

Following a trip condition, when the HIPPS barrier valves have closed, the system should remain in this state until the pressure in the production flowline returns to a value below the trip setting. At this point, a reset signal from the remote topside MCS can be applied to return the HIPPS to the normal operable state.

1.2.12 System Response Time

The response time of the HIPPS, from detecting high pressure in the production pipeline to closing the barrier valves is a function of the process safety time (PST).

Process safety time is defined by IEC61511 as:-

'The time period between a failure occurring in the process or the basic process control system (with potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety instrumented function is not performed.'

The response time of the HIPPS should be designed to operate and achieve pressure isolation in 50% of the process safety time.

1.2.13 Power System

Dual redundant high voltage AC power supplies feed the HIPPS sub-sea electronics module via the umbilical bundle. The supplies are conditioned into a single DC regulated supply, which is then converted via DC/DC converters to provide separate supplies for the logic solver dual redundant SCCBs.

1.2.14 Operator Interface

A human machine interface (HMI) is required in the topside MCS to give the operator full view of the HIPPS:-

- Input values and status
- Output states
- SIS shutdown 'First-out' status
- Permissive screens for start-up
- Operator interface – SIS logic solver communications status
- SIS logic solver hardware diagnostics screens

The HIPPS logic solver can exchange supervisory information with the MCS, but the safety critical components must remain totally independent of the MCS.

1.2.15 Security

The HIPPS should be designed to prevent unauthorised changes to the safety critical settings in the solid state logic solver. The settings should be made by changes to resistor configuration on the SCCBs and should only be made by authorised personnel under a management of change (MOC) procedure. It should not be possible to alter trip settings via the topside MCS or the operator HMI.

1.2.16 Functional Testing

The HIPPS should be designed for periodic testing to ensure its reliability, with minimal impact on normal operations.

A system of bypass valves might be considered to perform testing, but where the controls for this reside depends on the consequences of failure of the bypass system.

If a failure of the bypass system could result in overpressure of the production pipeline, then the bypass controls should be designed as a safety instrumented system. If failure of the bypass system does not lead to the overpressure consequences, then the normal non-safety related control system may be used.

1.2.17 Environmental Conditions

Environmental conditions are of critical importance for the integrity of a sub-sea HIPPS. The following are important environmental conditions that should be included in a HIPPS safety requirements specification.

- Process temperature range
- Process flow temperature
- Operating Depth
- Sea water temperature range
- Sea bed temperature
- Equipment design temperature range (electronics)
- Equipment design temperature range (sub-systems)
- Storage air temperature
- Exposure to the elements
- Vibration

Published by Write Projects Limited