

## Considerations in designing HIPPS

Willem-Jan Nuis, Mr.  
Rens Wolters, Mr.

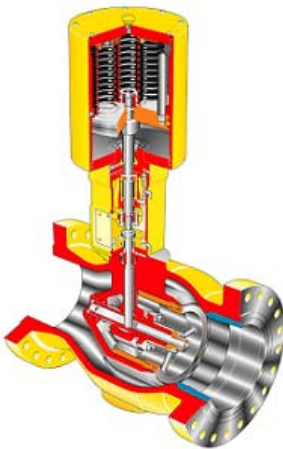
Mokveld Valves bv, Gouda, The Netherlands

01 July, 2004

**HIPPS** is an abbreviation for **H**igh **I**ntegrity (**P**ressure) **P**rotection **S**ystem, which is a specific application of a Safety Instrumented System (SIS) designed in accordance with IEC 61508. The function of a HIPPS is to protect the downstream equipment against over-pressure by closing the source. Usually this is done by timely closing one or more dedicated safety shut-off valves to prevent further pressurisation of the piping downstream of those valves.



Due to environmental constraints and cost saving, HIPPS has gained popularity over the last years as the last line of defence, replacing pressure safety valves (PSV), blow down and flare systems. Although HIPPS is applied for more than a quarter of a century, design and implementation of HIPPS is still not as obvious as one might expect. The main reason for this is the way the IEC 61508 and the more recently introduced IEC 61511 standards are written. The oil and gas industry for years has been accustomed to work with prescriptive standards.



Valve S99 RZDX  
Actuator S94M

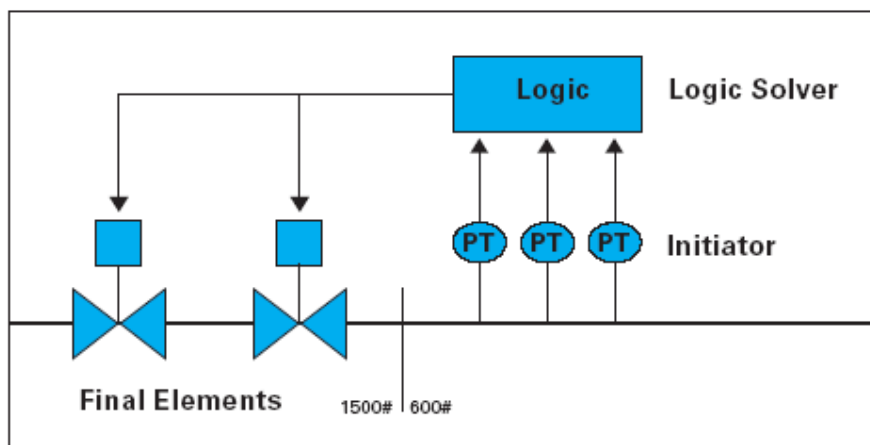
Standards like API 6A and API RP series, ASTM, ASME all precisely prescribe how to design and manufacture equipment, an installation, or material. The IEC 61508 and IEC 61511 however are performance based standards. They describe the process how to reach a solution rather than prescribing the solution itself. The IEC therefore leaves room for interpretation, which in some cases causes confusion or leads to over- or under-engineered solutions, thus requiring end-users to watch over their contractors and contractors to verify suppliers to assure that a safe system is installed.

Apart from the fact that the IEC 61508 leaves room for interpretation, it handles the final elements only superficially and focuses on the logic solver. This leads to the common misunderstanding that the word 'system' is to be understood as a synonym for controller or logic solver. The IEC however defines a 'system' as the complete loop, being the logic solver, initiators and final elements.

HIPPS and other SIS therefore have to be primarily treated as a complete loop and should not be designed on separate component level. The gap left by the IEC 61508 regarding the mechanical components (valves, solenoids), has been patched by the introduction of the IEC 61511. The latter standard specifically refers to final elements and initiators and provides some practical examples on how to interpret the IEC 61508.

## Risk of under-specifying

The misunderstanding that 'system' stands for controller and that a SIS can be designed on component level, is the cause for the biggest problem in the implementation of HIPPS. Namely the under-specification of mechanical components and the acceptance of component Safety Integrity Level (SIL) certification, instead of verification of the complete loop SIL.



*Typical safety Loop.*

This starts with the engineering specifications used to define and purchase a HIPPS. Sometimes the specification is over-emphasising on the controller while the other components in the loop get at best a single paragraph in the thumb thick material requisition. This is surprising, considering that valves, transmitters and solenoids often are more critical from a safety perspective than the controller. For the final elements sometimes a simple reference to an Emergency Shut Down (ESD) specification is made instead of well defined requirements for such critical safety equipment.

A proper requisition for HIPPS should therefore include as a minimum:

- General description of the process to be protected.
- General description of how HIPPS is integrated into the process and other safety systems, including the objectives of what the HIPPS shall protect, and how and when it is activated.
- Attention should be given to the number of the safety levels, the layering and sectionalisation
- The required SIL level of the loop and the minimum acceptable initial loop average Probability of Failure on Demand ( $PFD_{average}$ ).
- The required minimum proof test interval, and a description on how the operator proposes to proof test the HIPPS. This is directly related to the production availability and therefore an important issue in the specifications.
- Specification of the system response time and the criticality thereof in relation to the time before over-pressure occurs.

- Specifications how the HIPPS supplier shall proof that the supplied system  $PFD_{average}$  meets the specified SIL level. Attention shall be given to the Safe Failure Fraction (SFF), architectural constraints, and justification of the common cause failure factor (Beta).
- Specification that the HIPPS supplier shows (during the bid-phase) that the failure data of the components are valid for this application (e.g. failure rate for final element applicable for stroking time?)
- Detailed specification of the final element (shut-off valve) describing materials, design standards, actuator sizing / integration, details of the instrumentation such as solenoids and actuator. Specific safety aspects shall be addressed. Reference to a design standard like DIN 3381 can be considered.
- Detailed specification of the pressure transmitters and their safety aspects.
- Detailed specification of the controller including the required logging, local read out, test buttons, and communication to other controllers like the DCS. Event recorders shall be considered, also to record proof-tests.
- Components tests and integrated Factory Acceptance Test (FAT) requirements for the complete system.
- Documentation requirements which may include procedures and checklists for the Site Acceptance Test (SAT) and proof testing of the system.

A proper requisition determines the reliability as well as the availability of the safety system.

### **Certification doesn't prove system is safe**

Another consequence of the Oil and Gas industry's history of descriptive standards, is the love for certificates. Certificates suggest to relieve the engineer from the responsibility to verify the 'difficult to check' performance of a component. A good example of this is the hazardous area classification and the related Ex certification. When the hazardous area is correctly classified any component with the right Ex certificate can be used in that area without further checking.

Since PFD calculations, dependability of failure rates and the check if a component is fit for a certain SIL level is very complicated, the question for SIL certificates came very quickly from the industry. The issuance of 'SIL certificates' for components however has started the dangerous perception that buying certified equipment assures plant safety without further verification. However for the same reason that an Ex i component does not protect against explosions when used in circuits without Ex i barriers, component SIL certificates do not assure the plant safety, nor that the SIL level for the 'system' is met.

First we have to go back to the IEC. The IEC defines a SIL level, with its PFD and architecture, for a complete safety loop only and not for the subsystems. The IEC has no rules or specifications how to qualify a component for a certain SIL level, while the term SIL only applies to the complete system. Therefore one should ask how to obtain a SIL certificate if no rules to certify components exist? Or actually, why obtain a component certificate within the frame of a performance-based standard, where the words verification and validation of the 'system' are part of the foundation.

Component manufacturers adapt to the questions from the market by assuming a certain architecture for the complete system of which the certifiable component is a part. Assumptions are made for common cause, proof test interval, typical process duty, and response times for which their failure rates are applicable. Based on assumptions a component is then certified, which naturally limits the applicability of the certificate. Dependability of failure rates is already a difficult concept, dependability of a certificate takes the word difficult to a completely different level.

Failure rates obtained from operating experience in the nuclear industry does not mean that those failure rates are dependable and applicable in the Oil and Gas industry. Or closer to home, failure rates obtained

from operating experience such as an isolation valve in an oil application does not qualify that valve for a fast stroking duty in a HIPPS in upstream gas service.

To assess the applicability of a SIL certificate, the report should be closely studied. In most cases the certificate's only purpose is to serve as a justification for the failure rates provided by the manufacturer. In all cases the verification of the system's overall PFD and the system's architecture should fit the required SIL level of the system. Simply piling up certificates of components might result in a system which no longer fulfils the correct SIL level.

There are probably a dozen other topics that can be addressed when discussing common mistakes in designing and implementing HIPPS. With this article we try to reach awareness that responsible engineering is important, especially when it is considered that lives are at stake when a high SIL level HIPPS fails.