Instrumented Safety Systems
Engineered Valve Systems for Control and Safety Applications

HIPPS Definition

DINO OLIVIERI
Mokveld Agent
AIS – ISA Giornata di studio HIPPS
Agenda

- Foreword
- Definition
- Safety Requirement Specification
- Reliability Criteria
- Reliability Data
Foreword

High integrity protection systems (HIPS) and especially high integrity pressure protection systems (HIPPS) are an increasingly common feature of oil and gas facilities worldwide. They can provide an alternative to conventional mechanical protective devices (e.g. relief valves) or reduce the load upon them. In some cases, they present the only practical option to facilitate field development and/or expansion. Mokveld has started HIPPS B.U. in 1972.
Within the oil and gas industry, there are various company-specific definitions as to what constitutes a HIPS. According to the ISO/TR 12489 definition, a non-conventional, autonomous, safety instrumented system with sufficiently high safety integrity to protect equipment against exceeding the design parameters is considered a HIPS.
Definition- HIPS High Integrity Protection System

Examples:
- Deviations from industry standards describing mechanical protection systems (e.g. ISO 23251 = API Standard 521, ISO 10418, API RP 14C) are treated as HIPS.
- An ultimate protection relying principally, but not necessary solely, on Safety Instrumented Systems (SIS) is qualified as HIPS, irrespective of its required Safety Integrity Level (SIL).
Definition- HIPS High Integrity Protection System

Examples:
- a final protection layer comprising a combination of partial mechanical and instrumented protective function
- an instrumented protection layer having an integrity requirement of SIL 3 or more
- an instrumented protection layer where the consequence of non-operation is major to catastrophic or disastrous
Definition - HIPPS High Integrity Pressure Protection System

ISO/TR 12489 also defines HIPPS or OPPS as, “a HIPS exclusively devoted to protection against overpressure”.
Definition - HIPPS - summary

Safety Instrumented System (SIS - IEC61508-61511)

Autonomous

Final, instrumented protection layer

Dedicated to protect equipment from overpressure by isolating the pressure source
Instrumented protection systems rely on instruments to provide a safety function for a given process. Such a function is performed by a Safety Loop consisting of one or more initiators (e.g., switches or transmitters), a logic solver (e.g., a Safety Rated PLC) and final elements (e.g., relays or valves).
Definition- HIPPS – INDEPENDENT LAYER

API RP requires 2 independent safety layers

- **First Safety Layer**
- **Second Safety Layer**

- HIPPS
- INSTRUMENTED ESD
- ALARMS
- CONTROL SYSTEM
- PROCESS

Levels of Defense
Definition - HIPPS – RISK PROTECTION

<table>
<thead>
<tr>
<th>ACTUAL REMAINING RISK</th>
<th>TOLERABLE RISK</th>
<th>INTERMEDIATE RISK</th>
<th>INITIAL RISK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk with the addition of other risk reduction facilities and SIS</td>
<td>Risk with the addition of other risk reduction facilities</td>
<td></td>
<td>Risk without the addition of any protective features</td>
</tr>
</tbody>
</table>

**Conceptual Process Design**

Apply Non-SIS Layers

Apply SIS Layers

Determination of Tolerable Risk according IEC 61508

- NECESSARY MINIMUM RISK REDUCTION
- ACTUAL RISK REDUCTION
  - PARTIAL RISK COVERED BY SAFETY INSTRUMENTED SYSTEM
  - PARTIAL RISK COVERED BY:
    - OTHER TECHNOLOGY
    - EXTERNAL RISK REDUCTION FACTORS
  - RISK REDUCTION ACHIEVED BY ALL SAFETY RELATED SYSTEMS AND EXTERNAL RISK REDUCTION FACILITIES
**Definition- HIPPS – PROCESS DESIGN**

- **NO PROTECTION**
  - DESIGN PRESSURE = CLOSED IN TUBING HEAD PRESSURE

- **HYBRID**
  - DESIGN PRESSURE < CLOSED IN TUBING HEAD PRESSURE
  - SRV SIZED FOR ONE WELL CAPACITY

- **“Conventional” API RP14C**
  - DESIGN PRESSURE < CLOSED IN TUBING HEAD PRESSURE
  - SRV SIZED FOR TOTAL WELL CAPACITY

- **Well trip**
  - 1500# 900#

- **ESD**
  - ESD

- **HIPPS**
  - HIPPS

- **SIS**
  - SIS

- **DESIGN PRESSURE = CLOSED IN TUBING HEAD PRESSURE**

- **DESIGN PRESSURE < CLOSED IN TUBING HEAD PRESSURE**

- **SRV SIZED FOR ONE WELL CAPACITY**

- **SRV SIZED FOR TOTAL WELL CAPACITY**
Definition - HIPPS – WHY?

Reduction of the plant risk profile (insurance)
Reduction of Flare System and Piping Size
(or increase process system capacity without modifying flare system)
Regulations issues
Elimination of Separate Platform
Reduction in Weight
Environmental factors for IOCS
- no flaring
- reduced emissions
- perception of public
Production Separator with PSV

API Recommended Practice 14C

- The outlet of the separator blocks,
- The choke does not close,
- The Unit SDV does not close,
- The SRV is sized for full flow of the well
Production Separator with HIPPS

- The outlet of the separator blocks,
- The choke does not close,
- The SRV is sized for thermal relief / leakage only,
- The HIPPS SHALL close is 2 seconds to avoid overpressure in the separator.
Design and Hardware considerations

Shorter stroking times allow tighter design pressures
Dynamic simulation is strongly recommended
System operation (valve closing) may not be fast enough
so the solution may be inadequate (check SRS!)

2 seconds

10 seconds

2.1 barg

11.3 barg
HIPPS - General recommendations

Safety Requirements Specification

HIPPS functions should be defined independently of other safety systems in a specific HIPPS Safety Requirements Specification (SRS), normally produced by the end user. This should consider the complete system comprising sensing element(s), logic solver and final element(s). The HIPPS should be developed and implemented in a similarly complete system manner.
HIPPS - General recommendations

IEC 61511 part 1: performance requirements relating to:
- Functionality
- Availability
- Survivability
- Interdependencies
HIPPS - General recommendations

Additional common requirements:
• HIPPS should execute all safety functions in automatic mode.
• HIPPS should be autonomous, with dedicated sensors, logic and final elements.
• HIPPS should be a physically segregated system, interfaced with the facility automation system for monitoring only. Any communications with HIPPS should not be able to impede or override the safety function(s).
HIPPS - General recommendations

Additional common requirements:

• HIPPS should be designed according to fail-to-safe principles.

• Resetting should not be possible without a clear understanding of the initiating cause and/or fault (eg. Manual reset on SOVs)

• Signals between sensors, logic solver and final elements should be hardwired.
Additional common requirements:

- HIPPS design should define and include allowance for test and maintenance activities. Bypass functions should be avoided. When required, bypass functions should be subject to a thorough assessment of the risk and consequences for system integrity.
- HIPPS packages should be designated as ‘high’ focus with respect to quality management.
HIPPS - General recommendations

Additional common requirements:

- HIPPS design should consider the full safety life cycle.
- As component age the probability of failure increases.
- The component(s) lifetime depends on the test frequency and ability to detect dangerous failure
- Less reliable systems will therefore require higher test frequencies to suit same SIL requirement!
HIPPS - Reliability Criteria

HIPPS components, including sensors, logic solver and final elements should each be designed as fail-safe (i.e. failure of any component/sensor/logic solver/power supply/motive fluids moves final elements to the safe state).
HIPPS components or sub-systems are then selected such that the overall integrity (SIL) target of the HIPPS Safety Instrumented Function (SIF) is achieved.

\[ PFD_{sis} = PFD_I + PFD_{LS} + PFD_{SOV} + PFD_{SDV} \]
Risk graph based on HAZOP defines SIL

C = Consequence parameter
- \(C_A\) = Minor injury
- \(C_B\) = Serious injury to one or more, death to one
- \(C_C\) = Death to several people
- \(C_D\) = Very many people killed

F = Frequency of exposure parameter
- \(F_A\) = Rare to more often exposure
- \(F_B\) = Frequently to continuously

P = Possibility of escape
- \(P_A\) = Possible under certain conditions
- \(P_B\) = Almost impossible

W = Likelihood of event
- \(W_1\) = a relatively slight probability
- \(W_2\) = a relatively medium probability
- \(W_3\) = a relatively high probability
### SIL required defines the design of safety loop

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Probability of Failure on Demand</th>
<th>Risk Reduction Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL</td>
<td>PFD</td>
<td>RRF</td>
</tr>
<tr>
<td>0</td>
<td>No safety requirements (at all)</td>
<td></td>
</tr>
<tr>
<td>a</td>
<td>No special safety requirements (e.g. only a procedure)</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>$\geq 10^{-2}$ to $&lt;10^{-1}$</td>
<td>$&gt; 10$ to $\leq 100$</td>
</tr>
<tr>
<td>2</td>
<td>$\geq 10^{-3}$ to $&lt;10^{-2}$</td>
<td>$&gt; 100$ to $\leq 1.000$</td>
</tr>
<tr>
<td>3</td>
<td>$\geq 10^{-4}$ to $&lt;10^{-3}$</td>
<td>$&gt; 1.000$ to $\leq 10.000$</td>
</tr>
<tr>
<td>4</td>
<td>$\geq 10^{-5}$ to $&lt;10^{-4}$</td>
<td>$&gt; 10.000$ or better</td>
</tr>
<tr>
<td>b</td>
<td>A single safety system is not sufficient (even with redundant components)</td>
<td></td>
</tr>
</tbody>
</table>
HIPPS - Reliability Data

The HIPPS operator should approve the reliability data utilized to demonstrate the integrity achieved by the HIPPS. Reliability data sources include, in order of preference:

1. Field data – but only where the quantity collected is sufficient to be considered statistically significant

See 7.4.10.4: A proven in use safety justification shall be documented that the element supports the required safety function with the required systematic safety integrity. This shall include: the suitability analysis and testing of the element for the intended application and the demonstration of equivalence between the intended operation and the previous operation experience, including the impact analysis on the differences
Database filled since 70’s
Each after-sales related action entered in database

<table>
<thead>
<tr>
<th>Prod. Year</th>
<th>Valve-SN</th>
<th>Location</th>
<th>Country</th>
<th>Product Grp</th>
<th>Description</th>
<th>Spy</th>
<th>Buyer</th>
</tr>
</thead>
</table>
2. **Databases/reference handbooks**— The data selection process should consider similar service and environmental conditions, and maintenance regimes (OREDA3, PDS Data Handbook4, SINTEF5)

3. Failure Mode and Effect Analysis (FMEA) reports

4. Vendor data
PFD / SIL of complete safety loop to be verified

- Architecture to be verified
- Failure rates shall be dependable or “proven in use”:
  - Based on field experience in same application
  - For same stroking time (< 2 sec.)
- Integrated FAT & SAT
Example in Europe

Location: Gasunie Netherlands BBL Balgzand pipeline
Specs: 2 x 1002 Electronic HIPPS protecting ANSI 600 control valves against pressure from ANSI 900 compressor
Example in Europe

Location: NAM Netherlands mobile production unit
Specs: 1002 Mechanical HIPPS protecting ANSI 900 pipeline against pressure from ANSI 2500 wellhead
Example in Europe

Location : Dong Denmark Nybro
Specs : 1oo2 Electronic HIPPS protecting ANSI 600 onshore installation against pressure from ANSI 900 pipeline
Example in Europe

Location: Statoil Germany Zeepipe landfall
Specs: 1oo2 Mechanical HIPPS protecting ANSI 600 onshore installation against pressure from ANSI 900 pipeline
We thank you for your attention