Subsea HIPPS Design Methodology

Kevin Mullen
INTEC Engineering Pty. Ltd.

Abstract

This paper brings a formalised approach to the design of a subsea High Integrity Pipeline Protection System (HIPPS) which allows for the down-rating of a subsea flowline below the wellhead shut-in pressure.

The paper draws on the risk-based pipeline design of DNV OS-F101 to determine an acceptable level of integrity for the pipeline. Threats to the integrity of the pipeline, and their frequencies, are assessed. Preventative measures are considered, and any shortfall between the actual level of risk and the acceptable level must be made up by the HIPPS or other means. Using Layers of Protection Analysis (LOPA) allows the HIPPS function to be implemented using tree and manifold valves, procedures, automated shutdowns, as well as a conventional HIPPS module. The risk reduction from each independent layer combines to give the total risk reduction needed.

The LOPA approach is necessary to meet the recently increased requirement for pipeline integrity relating to pressure containment, as "simply" implementing an independent HIPPS may not attain an acceptable level of risk reduction.

The methodology is illustrated with a case study of four high pressure wells tied back through an existing lower rated pipeline.

---

2 Kevin Mullen is an engineer with INTEC Engineering Pty. Ltd. in Perth, Western Australia.
2 INTRODUCTION

A High Integrity Pressure Protection System is an independent safety shutdown system which provides downstream protection against overpressure. It provides this protection via the isolation of flowlines from the pressure source should the pressure from this source rise above a predetermined trip level (independently set within the HIPPS). HIPPS permits a reduction in pipeline wall thickness, improves project economics by reducing pipeline material costs, and allows for the tie-in of green field subsea developments into existing brownfield systems rated to lower working pressures.

A classic subsea HIPPS is shown in Figure 1, where a SIL 3 HIPPS device is used to protect the flowline from high pressure from the wells. This paper asks the questions:

- Why SIL 3?
- Is SIL 3 correct?
- What level of "High Integrity" is actually needed for the Pressure Protection System?

This paper takes account of a new increased safety level introduced by DNV which is applicable to HIPPS.

It provides a rigorous method and formalised approach to the design of subsea HIPPS, and allows cost-effective design which is sufficiently safe.

It does not cover hardware details, or fortified zone design, as these are adequately covered elsewhere.

---

3 "An engineer is someone who can do for ten shillings what any fool can do for a pound"
3 METHODOLOGY

The method that should be used to design a subsea HIPPS is described below:

- Gather information relating to the system, particularly relating to supply pressures and the capability of the low pressure part of the system;
- Determine the acceptable level of risk associated with the operation of the system;
- Determine the nature and the frequency of the hazardous events which may expose the system to overpressure;
- Determine the systems, devices, and procedures which are capable of reducing the level of risk, and evaluate the level of risk reduction for each of them;
- For each of the hazardous events, determine the level of risk reduction required to bring the level of risk down to the acceptable level;
- Decide which of the systems, devices, and procedures investigated in the previous step must be used in order to bring the level of risk down to the acceptable level; and
- Recommend the preferred configuration, and give the list of requirements for design and operation of the HIPPS, including the necessary frequency of testing.

4 HIPPS DESIGN PROCESS

4.1 System Information

Gather information relating to the system in order to evaluate a HIPPS design. This information will include the design premise, the field layout, and details relating to supply pressures and the capability of the low pressure part of the system.

4.1.1 Pressure Regulating System

The Pressure Regulating System (PRS) is implemented with the production chokes on the subsea production trees, in accordance with DNV-OS-F-101.

The production choke may pass excessive pressure from the well into the downstream equipment because of equipment failure or operator error. The probability of failure of the PRS should be assessed by HAZID.

4.2 Acceptable Level of Risk

To establish an acceptable level of risk, it is beneficial to used industry standards rather than company standards. DNV is an independent authority on risk and pipeline systems, so it is natural to use their offshore pipeline code DNV-OS-F101, as it allows both the pipeline system and the HIPPS to be governed by one all-encompassing code. In DNV-OS-F101, overpressurisation of a pipeline due to failure of the HIPPS is defined as an accidental load.
The design format within the DNV-OS-F101 standard is based upon a limit state and partial safety factor methodology, also called Load and Resistance Factor Design format (LRFD). The load and resistance factors depend on the Safety Class, which characterizes the consequences of failure.

Rather than accepting a single fixed level of risk, it is prudent to make the acceptable level of risk lower for operations and systems which are perceived to be more hazardous. This is recognised by DNV-OS-F101, which takes the following parameters into account:

- Pipeline contents;
- Location of the pipeline;
- Risk of human injury or environmental pollution, or economic or political consequences; and
- The frequency of the situation, i.e. temporary for installation or start-up, or long-term for operation.

On the basis of these parameters, DNV-OS-F101 defines a Safety Class, which characterises the consequences of failure. The Safety Classes vary from Low to Very High. The Safety Class may change at various points along the pipeline.

Based upon the Safety Class, DNV-OS-F101 states nominal failure probabilities depending on the applicable limit state. DNV-OS-F101 refers to limit states as "states beyond which the structure no longer satisfies the requirements". The following limit state categories are relevant to pipeline systems:

- Serviceability Limit State (SLS): A condition which, if exceeded, renders the pipeline unsuitable for normal operations. Exceedance of a serviceability limit state category shall be evaluated as an accidental limit state;
- Ultimate Limit State (ULS): A condition which, if exceeded, compromises the integrity of the pipeline;
- Fatigue Limit State (FLS): An ULS condition accounting for accumulated cyclic load effects; and
- Accidental Limit State (ALS): An ULS due to accidental (infrequent) loads.

For SLS, DNV-OS-F101 gives a nominal failure probability of only $10^{-2}$ per annum for the Low Safety Class.

ULS, SLS, and ALS are grouped, with nominal failure probabilities an order of magnitude lower, starting at $10^{-3}$ per annum.
Where the issue is pressure containment, DNV-OS-F101 requires a nominal failure probability between one and two orders of magnitude lower still, i.e. between $10^{-4}$ and $10^{-5}$ per annum.

For the Very High Safety Class where the issue is pressure containment, DNV-OS-F101 requires extremely low nominal failure probability, between $10^{-7}$ and $10^{-8}$ per annum.

It is clear that a HIPPS must be carefully engineered to make sure that it meets the applicable safety requirements. It is unlikely that a "one size fits all" solution can be found.

**4.2.1 HIPPS Classifications**

HIPPS may be classified in three ways:

- Burst critical, where over pressuring the pipeline will cause it to burst;
- Yield critical, where over pressuring the pipeline will not cause it to burst, but will take the pipeline material into the yield condition which precedes failure; and
- No yield, where over pressuring the pipeline exceeds the MAOP but does not take the pipeline into yield.

For burst critical HIPPS designs, pressure containment is critical, and the more stringent nominal failure probability is applicable.

For yield critical and no yield HIPPS designs, pressure containment is not an issue, and the required nominal failure probability is less stringent.

**4.2.2 DNV Nominal Failure Probability**

DNV changed the Nominal Failure Probabilities with the 2007 edition of DNV-OS-F101 to include more stringent requirements for pressure containment [Figure 2].

Before 2007, there was no additional requirement for pressure containment [Figure 3], and acceptable Nominal Failure Probabilities for burst-critical HIPPS systems was one or two magnitudes higher (ten or a hundred times higher).

This means that there is now a significant benefit in designing pipeline systems and HIPPS which are not burst-critical.
4.3 Hazardous Events

It is necessary to determine the nature and the frequency of the hazardous events, and escalation sequences, which may damage the system with overpressure.

A formal method of studying the hazardous events is to carry out a HAZID (Hazard Identification) using a team of experienced subsea engineers. The conceptual design of the system is presented to the team, and they point out potential risks, and estimate the likelihood of those events. Hazards which may be picked up include hydrate formation leading to pipeline blockage, operator error, stuck pigs etc.

The study should be closed out by issuing a HAZID Report.

Table 2-5 Nominal failure probabilities vs. safety classes

<table>
<thead>
<tr>
<th>Limit States</th>
<th>Probability Bases</th>
<th>Safety Classes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>SLS</td>
<td>Annual per Pipeline 1)</td>
<td>$10^{-2}$</td>
</tr>
<tr>
<td>ULS 2)</td>
<td>Annual per Pipeline 1)</td>
<td>$10^{-3}$</td>
</tr>
<tr>
<td>FLS</td>
<td>Annual per Pipeline 3)</td>
<td>$10^{-5}$</td>
</tr>
<tr>
<td>ALS</td>
<td>Annual per Pipeline</td>
<td>$10^{-6}$</td>
</tr>
</tbody>
</table>

1) Or the time period of the temporary phase.
2) The failure probability for the bursting (pressure containment) shall be an order of magnitude lower than the general ULS criterion given in the Table, in accordance with industry practice and reflected by the ISO requirements.
3) The failure probability will effectively be governed by the last year in operation or prior to inspection depending on the adopted inspection philosophy.
4) See Appendix F Table F-2.

Figure 2 Table 2-5 of DNV-OS-F101 (© DNV 2007)

Table 2-5 Acceptable failure probabilities vs. safety classes

<table>
<thead>
<tr>
<th>Limit States</th>
<th>Probability Bases</th>
<th>Safety Classes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>SLS</td>
<td>Annual per Pipeline 1)</td>
<td>$10^{-2}$</td>
</tr>
<tr>
<td>ULS</td>
<td>Annual per Pipeline 1)</td>
<td>$10^{-3}$</td>
</tr>
<tr>
<td>FLS</td>
<td>Annual per Pipeline 2)</td>
<td>$10^{-3}$</td>
</tr>
<tr>
<td>ALS</td>
<td>Annual per Pipeline 3)</td>
<td>$10^{-4}$</td>
</tr>
</tbody>
</table>

1) Or the time period of the temporary phase.
2) The failure probability will effectively be governed by the last year in operation or prior to inspection depending on the adopted inspection philosophy.
3) Refers to the overall allowable probability of severe consequences.

Figure 3 Table 2-5 of DNV-OS-F101 (© DNV 2000, Reprint January 2003)

4.3 Hazardous Events

It is necessary to determine the nature and the frequency of the hazardous events, and escalation sequences, which may damage the system with overpressure.

A formal method of studying the hazardous events is to carry out a HAZID (Hazard Identification) using a team of experienced subsea engineers. The conceptual design of the system is presented to the team, and they point out potential risks, and estimate the likelihood of those events. Hazards which may be picked up include hydrate formation leading to pipeline blockage, operator error, stuck pigs etc.

The study should be closed out by issuing a HAZID Report.
4.4 Systems, Devices, and Procedures for Reduction of Risk

From the previous step, it will be generally apparent that there is a wide discrepancy between the acceptable Nominal Failure Probability and the actual level of risk (potentially as much as 8 magnitudes). It is necessary to determine systems, devices, and procedures which are capable of reducing the level of risk, and evaluate the level of risk reduction for each of them.

A level of risk reduction to encompass 8 magnitudes cannot be realised in a single device. It is clear that a conventional HIPPS (with a SIL rating of typically 3, encompassing 3 magnitudes of risk reduction) will not satisfy the level of risk reduction needed.

Instead, a systems approach is taken. Instead of implementing the HIPPS with a single device, a concept known as Layers of Protection is used [Figure 4].

![Figure 4 Layers of Protection](image)

The Layers of Protection approach uses Independent Safety Layers (ISLs), each designed to prevent or mitigate hazardous events. The ISLs can be instrumented systems (electrical, electronic or programmable electronic) such as HIPPS, systems based on other technology (such as relief valves) or external risk reduction facilities (manual intervention procedures, for example).

Each ISL should be analysed in order to assess Probability of Failure on Demand (PFD), and to assign a Safety Integrity Level (SIL).

Besides a conventional HIPPS module, it is possible to implement safety functions on the subsea Xmas Trees. Independent control loops can be identified, incorporating tree functionality with additional logic solvers to be placed in the Subsea Electronic Module, to ensure no common mode failures. ISLs designed around the production Master Valve (PMV) and the Production Wing Valve (PWV) on the tree can be considered.

Besides the hardware-based safety layers, it can be very cost-effective to implement the risk reduction facilities by using manual intervention procedures, or by automating shutdowns.
into the control system. For example, a hazardous event for a HIPPS-protected pipeline is shutting in at the onshore gas plant. This leaves the subsea wells open, and producing into the pipeline, and they will eventually over-pressurise it. The plant operators should have procedures which instruct them to shut in the subsea wells in this situation, and there should also be an automated shutdown programmed into the control systems to deal with this.

All hazards and means of risk reduction should be documented on Layers of Protection Analysis (LOPA) worksheets.

### 4.5 Ways of Implementing HIPPS

#### 4.5.1 HIPPS Module

Subsea HIPPS is generally implemented as a HIPPS module, which may be built into a manifold. Cameron recently delivered a HIPPS module with a rating of SIL 3 for the Nexus Energy Longtom development.

#### 4.5.2 HIPPS on Tree

A subsea HIPPS function can be designed around the Production Master Valve (PMV) and the Production Wing Valve (PWV) on the tree. By building a HIPPS card into the Subsea Electronic Module on the tree, pressure sensors downstream of the choke can be monitored for over-pressure, and can initiate a shutdown of the PMV and PWV.

#### 4.5.3 HIPPS on Choke

This option follows a similar principle as the control loops discussed above, with the exception of the final element. This is the subsea production choke, which would be automated to step close should a significant rise in pressure be detected downstream of the choke.

Using a choke as the final element is not ideal because:

- Choke response times are slow; and
- Chokes do not typically seal.

Nevertheless, this option may be easy to implement, and may give addition protection to a HIPPS scheme.

#### 4.5.4 Hydraulic HIPPS

The Subsea Hydraulic HIPPS [Ref. 3] introduced by the Energy Equipment Corporation provides an alternative to existing programmable electronic subsea HIPPS controls. The all-hydraulic EEC system uses a dump valve, linked to the HIPPS pipeline valve actuator, to provide an independent means of closing the HIPPS pipeline valve in the event of pipeline over-pressure.
A preliminary analysis of the system, carried out by a third party team of SIL specialists, concluded that the EEC HIPPS is capable of achieving SIL rating 3. The system can be tested and calibrated at surface, and the dual redundant ROV retrievable HIPPS control cell allows intervention and replacement without impacting production. Because the device is completely hydraulic, it provides a strong "contrast" to Electrical/Electronic/Programmable Electronic based systems, with few common modes of failure.

4.6 Risk Reduction

For each of the hazardous events which have been identified by the HAZID, it is necessary to determine the level of risk reduction required to bring the level of risk down to the acceptable level.

Risk reduction can be effected by:

- Manual intervention according to procedures;
- Automatic operation and shutdown via the control systems;
- Conventional HIPPS modules;
- Production Shutdowns on the subsea xmas trees;
- Preventative measures to reduce the likelihood of the hazards identified; and
- Other good practice to mitigate the consequences of the risk.

It is unlikely that a single measure will give the level of risk reduction needed. The designer uses the measures available to provide a robust, layered protection system. Using a diversity of measures reduces the likelihood of any common-mode failure.

The safety layers used should be formalised in Layers of Protection Analysis worksheets. The LOPA summary gives a picture of all initiating causes, the preventative measures used, the effect of any HIPPS modules and safety functions on the Xmas Trees, and gives the Total Residual Risk for the complete system.

4.7 Acceptable Level of Risk

With all possible layers of protection used, the Total Residual Risk will hopefully be reduced below the level of risk required for operation of the system. This means that some layers of protection may be removed to implement a cost-effective yet acceptably safe system.

The measures used should be assessed in a Cost Benefits analysis to get the necessary level of risk reduction at an optimised cost.
4.8 Select Preferred Configuration

On the basis of the LOPA worksheets and the Cost Benefit Analysis, it will be possible to recommend a preferred configuration, and give a list of requirements for design and operation of the HIPPS, including the necessary frequency of testing

4.8.1 Testing Requirements

The PFDs used in the LOPA worksheets are based on annual testing. The safety functions must be tested at this Test Interval as an absolute minimum to maintain the stated level of safety. It is suggested that testing should be carried out more frequently than once per annum, preferably once every 3 months. It can be demonstrated that more frequent testing actually increases the safety of the system, and advantage can be taken of this in the analysis, with the proviso that the testing regime must be implemented by the user.

Partial closure testing may be used at intermediate intervals, to allow testing with no interruption to production.

Testing of each HIPPS function may be done by injecting MEG or methanol at each pressure transmitter in order to temporarily raise the local pressure above the HIPPS trip level [Ref. 2]. This serves another purpose, as it will assist in removing any hydrate which is building up in the pressure tapping or pilot line.

4.8.2 Safety Analysis Report

A Safety Analysis Report should be prepared to document that the required SIL will be achievable for each safety function and preventative measures. This report should be prepared during the design process. It typically addresses:

- System description;
- System general arrangement and block diagram;
- Operation description;
- Failure rates of the components;
- Recommended times between functional testing;
- Test procedures;
- Mean Time To Repair (MTTR);
- System diagnostics;
- Common cause failures; and
- Factory Acceptance Test (FAT) results for safety functions.
5 HIPPS CASE STUDY

5.1 System Information
Consider a new discovery of four high pressure wells which are to be produced through an existing lower pressure rated export pipeline. The Pressure Regulating System (PRS) is implemented with the production chokes on the subsea production trees, which drop the wellhead pressure down to a level which is suitable for the existing pipeline.

Due to the large difference between the wellhead pressures and the pipeline pressure rating, it is assumed that the HIPPS will be burst-critical.

The pipeline code DNV-OS-F101 classifies overpressurisation of the export pipeline due to failure of the HIPPS as an accidental load [Ref. 1].

5.2 Acceptable Level of Risk
DNV-OS-F101 gives differing acceptable levels of risk for different situations, taking into account pipeline contents, the location of the pipeline, and the risk of human injury and environmental pollution, or economic or political consequences. This is summarised in the DNV-OS-F101 definition of Safety Class.

The export pipeline of this case study is classified as:

- Category E (flammable gases such as natural gas);
- Location Class 2 (in areas with frequent human activity); and
- Safety Class High (high risk of human injury, significant environmental pollution or very high economic or political consequences).

In accordance to this classification, DNV states that the Nominal Failure Probability for Pressure Containment must be between $10^{-6}$ and $10^{-7}$. This level of risk (between $10^{-6}$ and $10^{-7}$ per annum) is acceptable to DNV for operation of the system.

5.3 Hazardous Events
It is necessary to determine the nature and the frequency of the hazardous events, and escalation sequences, which may damage the system with overpressure.

This can be established by carrying out a HAZID (Hazard Identification) using a team of experienced subsea engineers.

For this case study, the hazardous events are given in Table 1.
### Table 1: Hazardous Events

<table>
<thead>
<tr>
<th>Type of Failure</th>
<th>Frequency (per annum)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choke failure</td>
<td>$3.1 \times 10^{-2}$</td>
</tr>
<tr>
<td>Hydrate formation and pipeline blockage</td>
<td>$1 \times 10^{-1}$</td>
</tr>
<tr>
<td>Operator error</td>
<td>2</td>
</tr>
<tr>
<td>Leakage through HIPPS valves</td>
<td>$1 \times 10^{-1}$</td>
</tr>
<tr>
<td>Unplanned shut-in at gas plant</td>
<td>5</td>
</tr>
</tbody>
</table>

#### 5.4 Systems, Devices, and Procedures for Reduction of Risk

It is immediately apparent that there is a wide discrepancy between the acceptable level of risk ($10^{-6}$ to $10^{-7}$) and the actual level of risk (as many as 5 occurrences per annum).

A level of risk reduction to encompass 8 magnitudes cannot be realised in a single device. Layers of Protection must be used, with Independent Safety Layers (ISLs) designed to prevent or mitigate hazardous events. The ISLs can be instrumented systems (electrical, electronic or programmable electronic) such as HIPPS, or external risk reduction facilities (such as manual intervention procedures).

Each ISL should be analysed in order to assess Probability of Failure on Demand (PFD) and assign a Safety Integrity Level (SIL).

As a real example, the Statoil Kristin subsea development used a HIPPS system to protect flexible risers. To attain the level of risk reduction needed, they used:

- A subsea HIPPS designed for SIL 3, built into a manifold;
- A subsea Process Shutdown (PSD) designed for SIL 1, built into the subsea Xmas trees; and
- A relief valve (PSV) at the top of the risers on the semi-submersible production vessel.

For this case study, a conventional HIPPS module as well as safety functions on the subsea Xmas Trees are considered. Three independent control loops can be identified, incorporating tree functionality with additional logic solvers to be placed in the Subsea Electronic Module, to ensure no common mode failures. The following ISLs can be considered for this system:

- HIPPS Module;
- Independent Safety Layer 1 – A sensor activating PMV;
- Independent Safety Layer 2 – A sensor activating PWV; and
- Independent Safety Layer 3 – A sensor closing Choke.
5.5 Risk Reduction

For each of the hazardous events which have been identified by the HAZID, it is necessary to determine the level of risk reduction required to bring the level of risk down to the acceptable level. The designer uses the preventative measures available to provide a robust, layered protection system, using a Layers of Protection Analysis.

The LOPA summary sheet is shown in Table 2. This shows how the Total Residual Risk of the HIPPS is determined.

### Table 2 LOPA summary sheet

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Choke Failure</th>
<th>Hydrate Blockage</th>
<th>Operator Error</th>
<th>Leakage through HIPPS valves</th>
<th>Unplanned shut-in at Gas Plant</th>
<th>Frequency</th>
<th>Preventative Measures</th>
<th>Residual Risk (pa)</th>
<th>Total Residual Risk (pa)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>All Hazards</strong></td>
<td>7.2E-02</td>
<td>1.7E-09</td>
<td>1.7E-09</td>
<td>1.7E-09</td>
<td>1.7E-09</td>
<td></td>
<td></td>
<td>8.9E-08</td>
<td></td>
</tr>
<tr>
<td><strong>HIPPS and ISLs</strong></td>
<td>5.6E-07</td>
<td>5.6E-07</td>
<td>5.6E-07</td>
<td>5.6E-07</td>
<td>5.6E-07</td>
<td></td>
<td></td>
<td>5.6E-07</td>
<td></td>
</tr>
<tr>
<td><strong>Residual Risk (pa)</strong></td>
<td>1.7E-09</td>
<td>1.7E-08</td>
<td>1.7E-08</td>
<td>1.7E-08</td>
<td>1.7E-08</td>
<td></td>
<td></td>
<td>8.9E-08</td>
<td></td>
</tr>
</tbody>
</table>

The Total Residual Risk is lower than what is required by DNV (10^-6 to 10^-7). This means that the Mitigating Measures or the number of HIPPS and ISLs can be reduced.

The worksheet for one of the hazards, Hydrate Blockage, is shown in Table 3. This shows how the Initiating Causes are assigned frequencies, How the preventative measures are included, and how the total residual risk from that hazard is determined.

### Table 3 Hydrate Blockage Worksheet in LOPA Workbook

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Hydrate Blockage</th>
<th>Frequency</th>
<th>1.0E-01 (pa)</th>
<th>10%</th>
<th>30%</th>
<th>30%</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initiating Cause</strong></td>
<td>Loss of hydrate inhibitor (low flow, stoppage, low dosage)</td>
<td>3.0E-02</td>
<td></td>
<td>1.0E-02</td>
<td>3.0E-02</td>
<td>3.0E-02</td>
</tr>
<tr>
<td><strong>Preventative Measures</strong></td>
<td>Meter at each injection point to detect restricted flow and/or blockage</td>
<td>1.0E-01</td>
<td></td>
<td>1.0E-01</td>
<td>1.0E-01</td>
<td>1.0E-01</td>
</tr>
<tr>
<td><strong>HIPPS functions</strong></td>
<td>SIL 1</td>
<td>5.5E-02</td>
<td>SIL 1</td>
<td>5.5E-02</td>
<td>SIL 1</td>
<td>5.5E-02</td>
</tr>
<tr>
<td><strong>Residual Risk (pa)</strong></td>
<td>1.7E-09</td>
<td>5.6E-10</td>
<td>1.7E-08</td>
<td>1.7E-10</td>
<td>1.7E-08</td>
<td>1.7E-08</td>
</tr>
<tr>
<td><strong>Total Residual Risk (pa)</strong></td>
<td>1.9E-08</td>
<td>1.9E-08</td>
<td>1.9E-08</td>
<td>1.9E-08</td>
<td>1.9E-08</td>
<td>1.9E-08</td>
</tr>
</tbody>
</table>
It can be seen that with all possible layers of protection used, the Total Residual Risk is reduced to the very low level of 8.9E-08 pa. This is below the level of risk required by DNV for operation of the system (10^{-6} to 10^{-7}), so some layers of protection may be removed to implement a cost-effective yet acceptably safe system.

5.6 Acceptable Level of Risk

With all possible layers of protection used, the Total Residual Risk is below the level of risk required for operation of the system. This means that some layers of protection may be removed to implement a cost-effective yet acceptably safe system. The measures used are assessed in a Cost Benefits analysis to get the necessary level of risk reduction at an optimised cost.

A review of the LOPA worksheets in Table 2 shows that the Independent Safety Layer 3 on the subsea Xmas Tree choke could be removed. This would make the system easier to implement, while still giving an acceptable level of residual risk.

Removing Independent Safety Layer 3 on the subsea Xmas Tree choke gives a Total Residual Risk of 4.8E-07 pa. This is within the range acceptable to DNV for operation of the system (10^{-6} to 10^{-7}).

5.7 Select Preferred Configuration

On the basis of the LOPA worksheets and the Cost Benefit Analysis, it is recommended that this system should include the following ISLs:

- HIPPS Module;
- Independent Safety Layer 1 – A sensor activating PMV; and
- Independent Safety Layer 2 – A sensor activating PWV.

5.7.1 Testing Requirements

The PFDs used in the LOPA worksheets are based on annual testing. However, it is recommended that testing should be carried out more frequently than once per annum, preferably once every 3 months.

Partial closure testing may be used at intermediate intervals, to allow testing with no interruption to production.

5.7.2 Further Recommendations for Case Study

Due to the large difference between the wellhead pressures and the pipeline pressure rating, it has been assumed that the HIPPS is burst-critical. Further work should be carried out to establish if the system is yield-critical rather than burst-critical, as this is less onerous for the design of the HIPPS.
This work would establish the failure probability for the pipeline:

- For a fully rated pipeline the PFD is essentially zero (actually between $10^{-2}$ and $10^{-6}$, depending on Safety Class and Limit State);
- For a burst-critical pipeline the PFD is 1 (i.e. the pipeline will burst if over-pressured); and
- For a yield-critical pipeline the PFD is some intermediate value between zero and 1.
REFERENCES


2 OTC 8180, Subsea High Integrity Pressure Protection Systems for High Pressure Oil and Gas Developments, M.C. Theobald, Kvaerner FSSL Limited, Copyright 1996, Offshore Technology Conference.