



# Tri-Sen TetraSentry™ Hydraulic Trip System SIL Verification Report

Harry L. Cheddie P. Eng

Cteris Consulting Inc. - Director  
ASQ Certified Reliability Engineer (CRE)  
ASQ Certified Quality Engineer (CQE)  
Certified Functional Safety Expert (CFSE)

Document ID	Revision	Status	Date
C10-12-18 R1	1	Final	4 January 2011

## CONFIDENTIAL INFORMATION

This document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

## Abbreviations

CCPS	Center for Chemical Process Safety
LOPA	Layer of Protection Analysis
MTTFS	Mean Time to Fail Spurious
MTTR	Mean Time to Repair
$PFD_{avg}$	Average Probability of Failure on Demand
PTI	Proof Test Interval
RRF	Risk Reduction Factor
SIF	Safety Instrumented Function
SIL	Safety Integrity Level

## Table of Contents

Abbreviations.....	2
1 Introduction .....	4
2 Summary of results .....	4
3 System description.....	5
3.1 Component details .....	6
4 Analysis of Failure Modes for TetraSentry .....	7
5 Fault tree illustrating the basis of the PFD <sub>avg</sub> calculations.....	12
6 Results.....	13
6.1 Calculation assumptions and basis.....	13
6.2 Component failure rates.....	13
6.3 Calculation Results .....	15
7 Status of the Document .....	16
8 Conclusions .....	16
Appendix A - Reference Documents.....	17
Appendix B - Symbols .....	18

## 1 Introduction

This report provides the design details and the basis/results of a Safety Integrity Level (SIL) evaluation for Tri-Sen's TetraSentry hydraulic trip system.

The TetraSentry is a fault tolerant trip system used to dump the oil supply to turbine trip valves allowing a safe shutdown of the associated turbine.

The Safety Integrity Level (SIL) achieved for the trip system is an indication of its ability to function correctly when required. Four possible discreet integrity levels (SIL-1, SIL-2, SIL-3, & SIL-4) have been defined in the standard ANSI/ISA-84.00.01-2004 (IEC 61511 Mod). Each level relates to the average probability of failure when a demand is placed on the system ( $PFD_{avg}$ ). This relates to the risk reduction as per the table below:

SIL	Risk Reduction Factor (RRF)
1	10 - 100
2	100 - 1000
3	1000 - 10,000
4	10,000 - 100,000

One of the primary factors in determining the SIL achieved is the frequency of proof testing. As such, this report documents the Risk Reduction Factor (RRF) achieved for various test intervals.

This report provides the following performance parameters as related to the system:

- Average Probability of Failure on Demand ( $PFD_{avg}$ )
- Achieved SIL based on  $PFD_{avg}$
- Achieved SIL based on architectural constraints
- The spurious trip rate for the system/Mean Time To Fail Spuriously (MTTFS).

The parameters listed above are provided for the following test intervals.

- 3 months
- 6 months
- 1 year
- 2 years
- 5 years

## 2 Summary of results

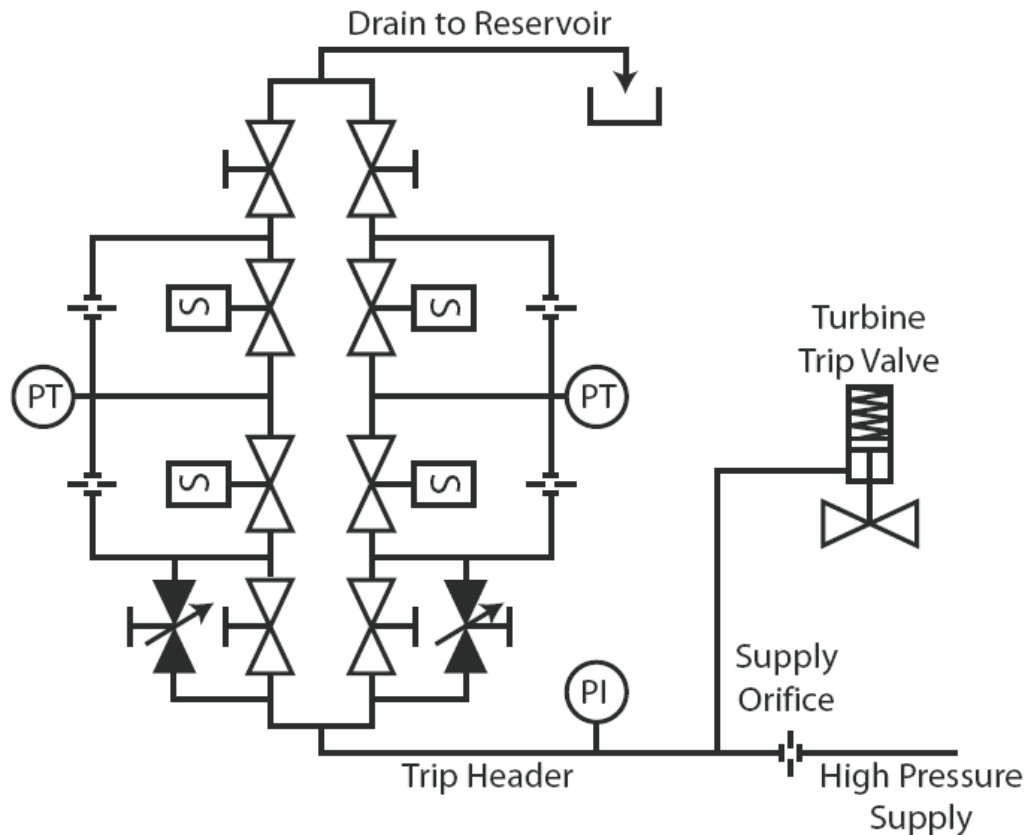
The TetraSentry hydraulic trip system is fit for use in applications up to SIL-3, with very low spurious trip rates. This assessment is based upon the fault tolerance, extensive diagnostics, ease of on line testing, and on line repair capabilities of the system.

A summary of the results of the evaluation is located in § 6.3 of this report.

### 3 System description

A simplified schematic of the trip system is as per Figure 1 below:

Figure 1 - TetraSentry™ simplified schematic



The trip system consists of two parallel sets of solenoid valves. Each set consists of two valves, which are connected in series. During normal operation, all four solenoid valves are closed, causing the full supply pressure of the control oil to be applied to the turbine trip valve actuator.

A trip will occur when both valves in at least one parallel set opens, causing the trip header to drain faster than the control oil supply can refill the header, via the supply orifice.

The two pressure transmitters provide the status of the Pilot/Trip valves, the upstream block valves, and the downstream block valves, if mal-operation of the valves occurs.

Supply and vent orifices are provided to enable the system to be tested on-line. During testing the Pilot/Trip valves are opened and the correct operation of each valve can be determined by observing PT01 and PT02 readings. The upstream and downstream block valves allow the system to be repaired online.

### 3.1 Component details

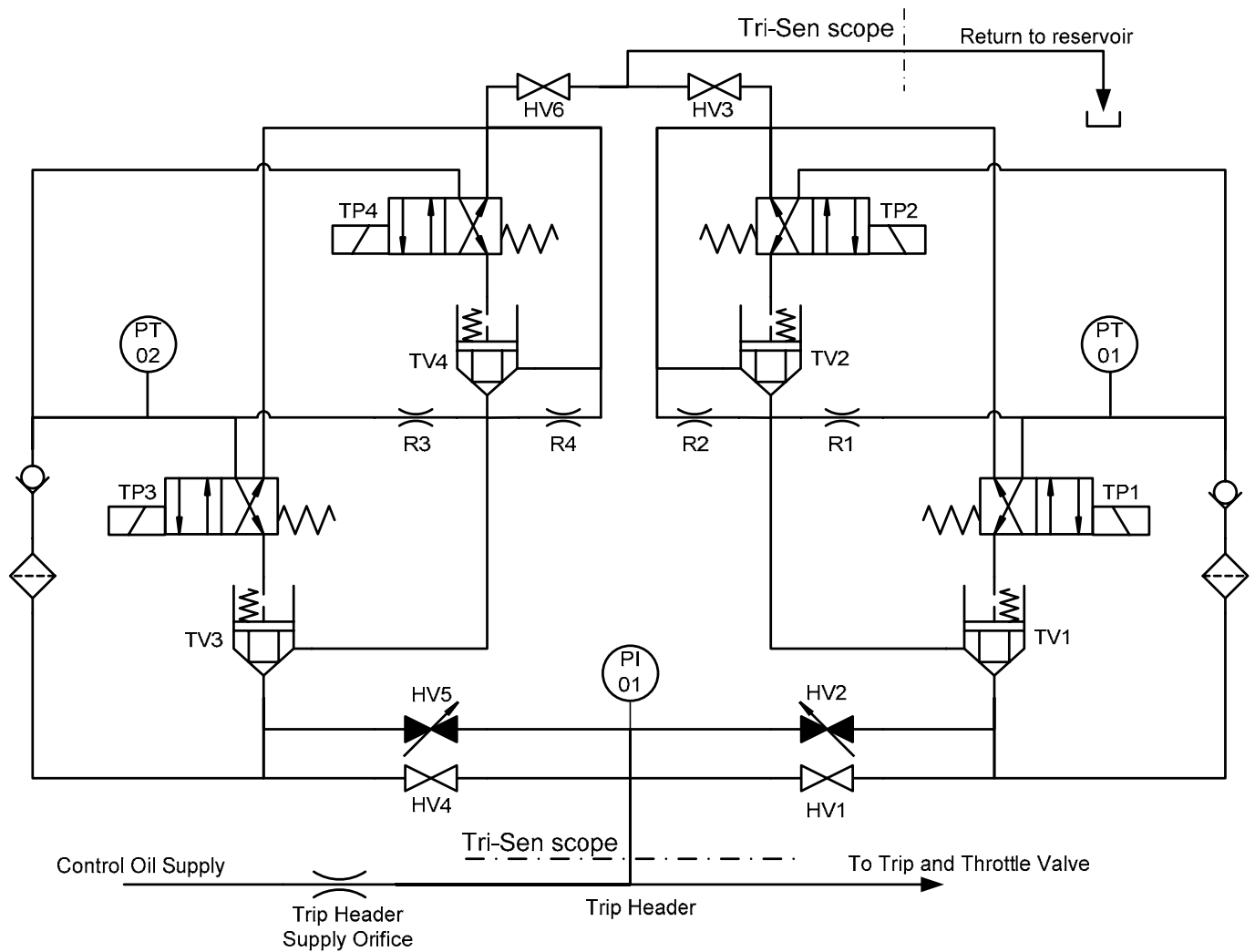
The model numbers for the trip valves in the TetraSentry are:

- Solenoid-operated directional control valves - Parker model D1VW020HNJET with model BK209M bolt kit
- Cartridge valves - Parker model CE032C01N00N

## 4 Analysis of Failure Modes for TetraSentry

The TetraSentry system with all the major components identified is illustrated in Fig 2 below. The scope of this review is within the “Tri-Sen scope” boundaries.

Figure 2- TetraSentry™ hydraulic schematic.



Note: Refer to appendix C for symbol legend.

The failure modes and effects for the system components are outlined below in Table 1.

Table 1 - Failure modes and effects for system components

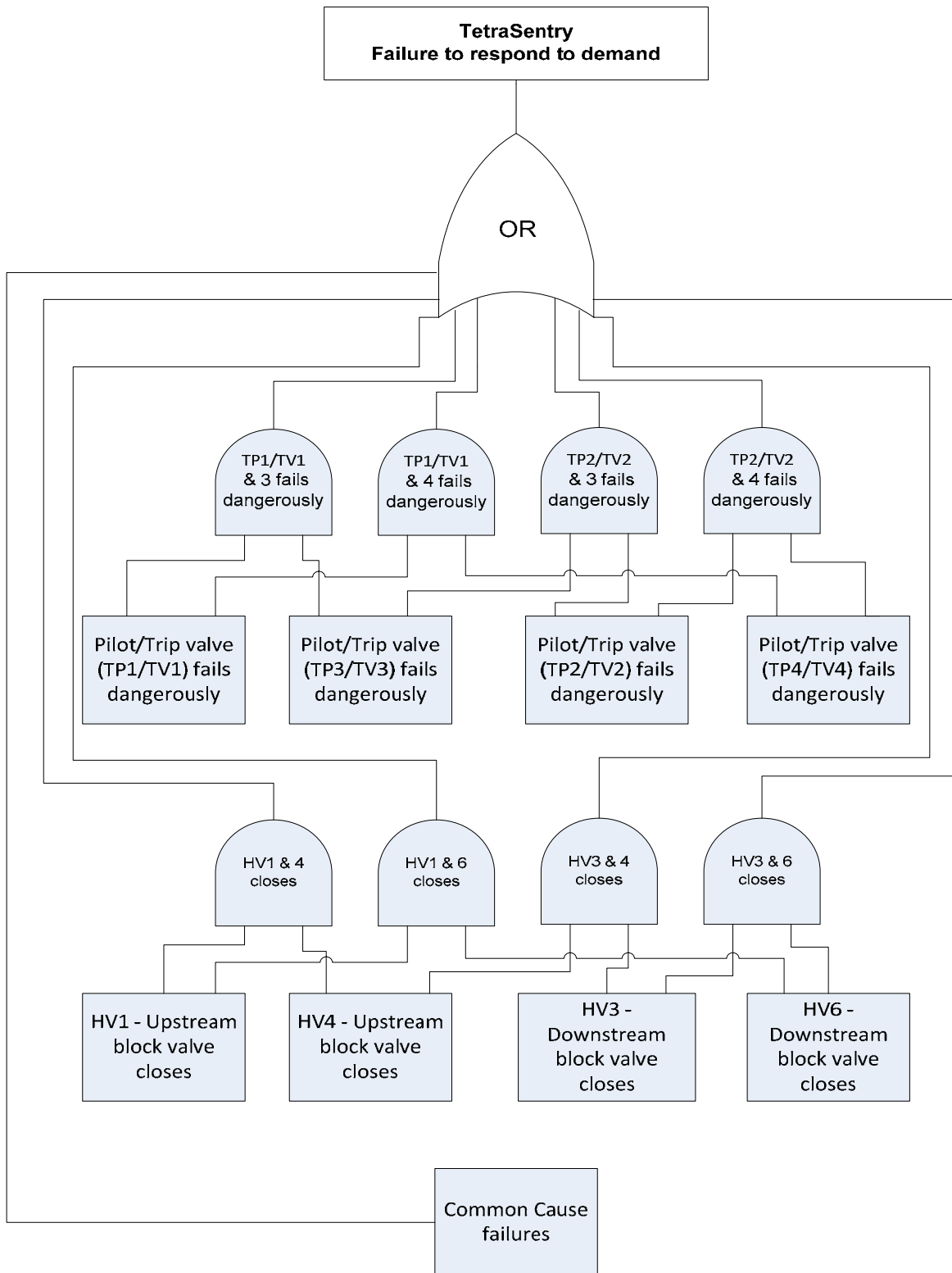
Component	Normal operation mode	Failure Modes/Cause	Failure Effect	Failure Type	Diagnostics
Pilot/Trip valve (TP1/TV1)	Solenoid Energized - Valve closed	Valve opens due to valve failure or coil burnout	No immediate effect on system operation. Potential for spurious trip of turbine if Pilot/Trip valve (TP2/TV2) also fails in same mode.	Safe failure	PT01 shows HIGH pressure - No change to PT02
		Valve leaking			
		Valve fails to open on demand	No immediate effect on demand operation. Potential for trip system demand failure if Pilot/Trip valve (TP3/TV3) or (TP4/TV4) also fails in same mode and failures are not detected.	Dangerous failure	None. Failures can only be detected during proof testing
Pilot/Trip valve (TP2/TV2)	Solenoid Energized - Valve closed	Valve opens due to valve failure or coil burnout	No immediate effect on system operation. Potential for spurious trip of turbine if Pilot/Trip valve (TP1/TV1) also fails in same mode.	Safe failure	PT01 shows LOW pressure (2 psig) No change to PT02
		Valve leaking			
		Valve fails to open on demand	No immediate effect on system operation. Potential for trip system demand failure if Pilot/Trip valve (TP3/TV3) or (TP4/TV4) also fails in same mode and failures are not detected.	Dangerous failure	None. Failures can only be detected during proof testing
Pilot/Trip valve (TP3/TV3)	Solenoid Energized - Valve closed	Valve opens due to valve failure or coil burnout	No immediate effect on system operation. Potential for spurious trip of turbine if Pilot/Trip valve (TP4/TV4) also fails in same mode.	Safe failure	PT02 shows HIGH pressure - No change to PT01
		Valve leaking			

Component	Normal operation mode	Failure Modes/Cause	Failure Effect	Failure Type	Diagnostics
		Valve fails to open on demand	No immediate effect on system operation. Potential for trip system failure if Pilot/Trip valve (TP1/TV1) or (TP2/TV2) also fails in same mode and failures are not detected.	Dangerous failure	None. Failures can only be detected during proof testing
Pilot/Trip valve (TP4/TV4)	Solenoid Energized - Valve closed	Valve opens due to valve failure or coil burnout	No immediate effect on system operation. Potential for safe failure if Pilot/Trip valve (TP3/TV3) also fails in same mode.	Safe failure	PT02 shows LOW pressure. No change to PT01
		Valve leaking			
		Valve fails to open on demand	No immediate effect on system operation. Potential for trip system failure if Pilot/Trip valve (TP1/TV1) or (TP2/TV2) also fails in same mode and failures are not detected.	Dangerous failure	None. Failures can only be detected during proof testing
HV1 - Upstream block valve	Valve open	Valve closed	No immediate effect on system operation. Potential for system failure if block valve HV4 or HV6 also fails in same mode and failures are not detected.	Dangerous failure	PT01 shows LOW pressure. No change to PT02
HV2	Valve closed	None of concern			
HV3 - Downstream block valve	Valve open	Valve closed	No immediate effect on system operation. Potential for system failure if block valve HV4 or HV6 also fails in same mode and failures are not detected.	Dangerous failure	PT01 shows HIGH pressure - No change to PT02
HV4 - Upstream block valve	Valve open	Valve closed	No immediate effect on system operation. Potential for system failure if block valve HV1 or HV3 also fails in same mode and failures are not detected.	Dangerous failure	PT02 shows LOW pressure. No change to PT01
HV5	Valve closed	None of concern			

Component	Normal operation mode	Failure Modes/Cause	Failure Effect	Failure Type	Diagnostics
HV6 - Downstream block valve	Valve open	Valve closed	No immediate effect on system operation. Potential for system failure if block valve HV1 or HV3 also fails in same mode and failures are not detected.	<b>Dangerous failure</b>	PT02 shows HIGH pressure - No change to PT01
R1 - Supply Orifice	Passing flow	Cavity supply orifice plugged	Loss of diagnostics and inability to carry out proof testing	Diagnostics Failure	PT01 shows LOW pressure. No change to PT02
R2 - Vent Orifice	Passing flow	Cavity vent orifice plugged	Loss of diagnostics and inability to carry out proof testing	Diagnostics Failure	PT01 shows HIGH pressure - No change to PT02
R3 - Supply Orifice	Passing flow	Cavity supply orifice plugged	Loss of diagnostics and inability to carry out proof testing	Diagnostics Failure	PT02 shows LOW pressure. No change to PT01
R4 - Vent Orifice	Passing flow	Cavity vent orifice plugged	Loss of diagnostics and inability to carry out proof testing	Diagnostics Failure	PT02 shows HIGH pressure - No change to PT01
FL1	Passing flow	Control filter DP high	Loss of diagnostics and inability to carry out proof testing	Diagnostics Failure	PT01 shows LOW pressure. No change to PT02
FL2	Passing flow	Control filter DP high	Loss of diagnostics and inability to carry out proof testing	Diagnostics Failure	PT02 shows LOW pressure. No change to PT01
CK VLV1	Passing flow	Fail close	Loss of diagnostics and inability to carry out proof testing	Diagnostics Failure	PT01 shows LOW pressure. No change to PT02
CK VLV2	Passing flow	Fail close	Loss of diagnostics and inability to carry out proof testing	Diagnostics Failure	PT02 shows LOW pressure. No change to PT01
PT1	Active	Output signal high, low, or frozen	Loss of diagnostics and inability to carry out proof testing	Diagnostics Failure	Not applicable

Component	Normal operation mode	Failure Modes/Cause	Failure Effect	Failure Type	Diagnostics
PT2	Active	Output signal high, low, or frozen	Loss of diagnostics and inability to carry out proof testing	Diagnostics Failure	Not applicable

## 5 Fault tree illustrating the basis of the PFD<sub>avg</sub> calculations



## 6 Results

### 6.1 Calculation assumptions and basis

**Mission Time:** Is the time between full testing (100% test efficiency), or replacement of the components. A period of 10 years has been used in this evaluation.

**Start-up Time:** A conservative value of 24-hours has been utilized in starting up the facility.

**Proof Test Intervals:** Various testing intervals are used in the calculations.

**Beta ( $\beta$ ) Factor:** A value of 5% has been used to address potential common cause failures for multiple components.

**MTTR (Mean Time to Repair):** 24 hours.

The calculations are based on IEC61508 requirements. Components are considered to be “Proven in use”

### 6.2 Component failure rates

The failure rates used in the calculation for the key components are as per table 2 below.

The components associated with dangerous failures are:

- The solenoid operated valves, and cartridge valves<sup>1</sup> labeled TPx and TVx as per Fig 2
- Hand valves labeled HVx as per Fig 2

For dangerous failure a diagnostic coverage factor of 0 is used. For safe failures a coverage factor of 0.7 has been used, i.e. based on the diagnostics, it is assumed that none of the dangerous failures will be detected, and as a result of the high and low pressure alarms and operator intervention, 70% of the safe failures will be detected and corrected.

For operator action, a coverage factor of 0.9 is the normally acceptable value. However, in this analysis, a more conservative value of 0.7 has been used.

Inadvertent closing of hand valves can be considered as a human error

For a single hand valve failure, with well trained personnel and with no stress, a failure rate of  $1.0 \times 10^{-3}$ / opportunity is used.<sup>2</sup> This is a widely accepted and used value in the process industry.

---

<sup>1</sup> Failure rate data for the solenoid operated valves and associated cartridge valve was obtained from Pilot valve component statistics in *Reliability Data for Control and Safety Systems*. Trondheim, Norway: SINTEF. 1998.

<sup>2</sup> Equivalent to the value used for failure of a “Lock-out and Tag-out” procedure as found in *Layer of Protection Analysis, Simplified Process Risk Assessment*. New York, NY: Center for Chemical Process Safety. 2001.

Assuming two opportunities/ year, the dangerous failure rate assumed for each hand valve is then  $2.0 \times 10^{-3}$ / year. The analysis makes the assumption that 70% of these failures will be detected by the system's diagnostics.

Table 2 - Failure rates for key components

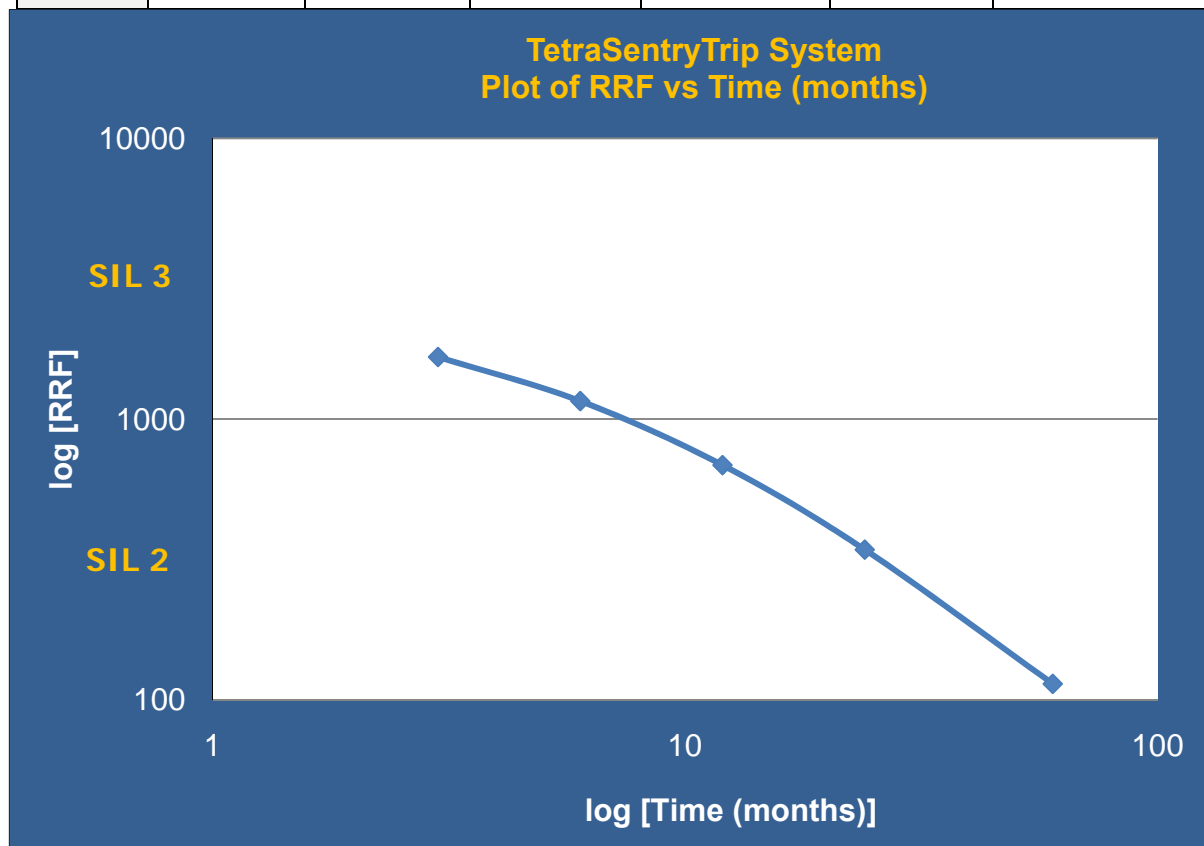
Component	$\lambda$ (Dangerous undetected)	$\lambda$ (Safe undetected)	$\lambda$ (Safe detected)
Solenoid operated valves and associated cartridge valve	$1.14 \times 10^{-6}/\text{hr}$	$7.5 \times 10^{-7}/\text{hr}$	$1.75 \times 10^{-6}/\text{hr}$
Hand valves	$6.85 \times 10^{-8}/\text{hr}$	-	-

### 6.3 Calculation Results

#### Summary of SIL Verification Calculations for Testing Intervals

Description of the System: The TetraSentry is a fault tolerant trip system that is used to dump the oil supply to the turbine trip valves.

Test Interval (Months)	RRF Achieved (Risk Reduction Factor)	PFDavg	SIL Achieved based on PFDavg	SIL (Architectural constraints)	Final SIL	Mean time to fail spurious (MTFS) (Yrs)
3	1664	6.01E-04	3	3	3	1568
6	1159	8.63E-04	3	3	3	1409
12	685	1.46E-03	2	3	2	1176
24	342	2.92E-03	2	3	2	901
60	114	8.78E-03	2	3	2	569



## 7 Status of the Document

Revision	Date	Description
Draft	24 December 2010	Draft report submitted for review and comments
Final	4 January 2011	Final report

## 8 Conclusions

1. The TetraSentry hydraulic trip system is fit for use in applications up to SIL-3, provided that the proof test interval (PTI) is suitable for the SIL requirement.
2. Due to the fault tolerance, on line testing, and repair capabilities, the spurious trip rates for proof test intervals (PTI) varying from 3 months to 5 years is very low. For a PTI of 3 months the MTTFS is 1568 years, and for 5 years the MTTFS is 569 years.
3. The signals from PT01 and PT02 should be connected to the SIS logic solver that operates the TetraSentry solenoid valves. The logic associated with the alarming also needs to be part of the same SIS logic solver
4. Although the proof test procedure can be carried out manually, it is recommended that the testing be automatically scheduled and automated as much as possible. The logic associated with the automatic proof testing needs to be in the SIS logic solver that operates the TetraSentry solenoid valves.
5. Although the pressure indicator PI01 shown in Fig. 2 is not part of the scope of this review, it is recommended that a pressure transmitter with high and low pressure alarms be provided.
6. Final verification calculations of the complete SIF, including sensors, logic solver, and all final elements has to be completed by the end user to determine the SIL achieved for the complete function, to ensure that the function satisfies that SIL requirement.

## Appendix A - Reference Documents

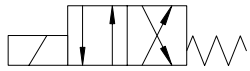
\_\_\_\_\_. *ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) Functional Safety- Safety Instrumented Systems for the Process Industry Sector*. Edition 1. Research Triangle Park, North Carolina, USA: ISA. 2004.

\_\_\_\_\_. *IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems*. Edition 1. Geneva, Switzerland: IEC. 2003.

\_\_\_\_\_. *Layer of Protection Analysis, Simplified Process Risk Assessment*. New York, NY: Center for Chemical Process Safety. 2001.

\_\_\_\_\_. *Reliability Data for Control and Safety Systems*. Trondheim, Norway: SINTEF. 1998.

## Appendix B - Symbols



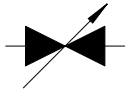
Directional Control Valve –  
solenoid operated



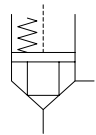
Block valve – normally open



Block valve – normally closed



Bleed valve – normally closed



Cartridge valve – 2 way



Filter



Check valve



Restriction orifice



Pressure Transmitter



Pressure Gage