Final Element Architecture Comparison

2oo2 with diagnostics: Lower False Trip Rate and High Safety

Project:
Safety Cycling Systems Architecture Review

Customer:

Safety Cycling Systems, L.L.C.
1018 Laurel Ave.
Denham Springs, LA.
USA

Contract No.: SCS 06/12-24
Report No.: SCS 06/12-24 R001
Version V1, Revision R1, April 2, 2007
William M. Goble

Management summary

The purpose of this report is to summarize a quantitative analysis of three final element configurations for the purpose of comparing the conventional 1oo1 architecture and the 1oo2 architecture with a 2oo2 architecture made with the Safety Cycling Systems diagnostic apparatus.

The 1oo1 architecture was done to provide baseline results for comparison purposes. The 1oo2 architecture shows the expected safety improvement achieved by this conventional approach including the expected higher false trip rate. The 2oo2 architecture shows substantial **improvement in safety** over the 1oo1 but with an even greater improvement in false trip rate assuming that on-line repair can be made.

Overall this means that plant operations can be made sufficiently safe in many applications without any negative impact on production. When this is compared with conventional approaches on an economic basis, the return could be great given the typical high cost of lost production due to a false trip. The overall results are presented in Table 1.

Table 1: Overall results.

	CD	SIF PFDsvg	SIL	RRF	SIF MTTFS	FE PFDavg	FE MTTFS
1oo1		2.01E-02	1	50	162	1.98E-02	199
1oo2		2.78E-03	2	359	93	2.50E-03	105
2oo2 SCS Diag.	90%	4.16E-03	2	240	595	3.87E-03	1958
2oo2 SCS Diag.	95%	2.26E-03	2	442	595	1.98E-03	1955

The 2oo2 architecture using the Safety Cycling Systems approach provides improved safety and significantly improved MTTFS (low false trip rate). If the diagnostic coverage factor could reach 95%, superior safety and a significantly improved MTTFS would both be achieved.

Table of Contents

1 Purpose and Scope

The purpose of this report is to summarize the findings of a quantitative comparison of three final element architectures within the context of a safety instrumented function (SIF). A SIF with a 1oo1 final element (FE) architecture was done to provide a baseline comparison number. A second SIF with a 1oo2 FE architecture was done to show the results of the conventional approach to achieving higher safety. A SIF with a 2oo2 architecture was analyzed to show the impact of the Safety Cycling Systems diagnostic apparatus in a safety instrumented function application.

2 Process and Roles

2.1 exida

exida is one of the world's leading knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TÜV and manufacturers, *exida* is a partnership with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

SCS	Inventor of the 2oo2 diagnostic apparatus
exida	Project leader and assessor for the Final Element Comparison

2.3 Standards used

The services delivered by *exida* were performed based on the following standards.

N1	IEC 61508: 2000 Parts 1 to 7	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

2.4.1 Documentation provided by the customer

D1	101906	SafetySIL Controller, Theory of Operation
D2	ContinuousAnimation22.gif, 3/7/2007	Animated drawing of operation

2.4.2 Documentation generated by *exida*

R1	exSILentia Project Files, April 2, 2007	Results from exSILentia SILver analysis, appended to this report.

3 Findings of the Analysis

3.1 The SCS Apparatus

SCS has described and prototyped an apparatus that measures valve seat leakage when one valve is closed in a 2oo2 parallel piped configuration with a special mechanical adaptor. This device can be used to detect potentially dangerous failures in safety instrumented function final element. When the two parallel piped valves are given alternative full stroke commands from a logic solver (or other control device), the SCS apparatus will measure differential pressure changes. Via these measurements, the diagnostic apparatus can detect valve leakage greater than a tolerable amount.

3.2 The SIF Equipment

For comparison purposes the SIF was chosen with equipment to minimize the impact of sensors and logic solver on the results. This approach will show the maximum impact of the final element. Three safety rated sensors are used in a 2oo3 voting arrangement. This set of equipment was chosen to provide very high safety and availability. A high availability redundant SIL 3 logic solver was chosen to also provide high safety and availability. This same set of equipment is used in all three SIF configurations. Details are presented in the appendix.

3.3 1oo1 Architecture

The final element in the 1oo1 architecture is a remote actuated valve. A solenoid valve is used as the final element interface device. A generic air operated hard seat ball valve is interfaced to the solenoid. The trip mode is close to trip. Clean service and no partial valve stroke testing are assumed. The results of the analysis are shown in Figure 1.

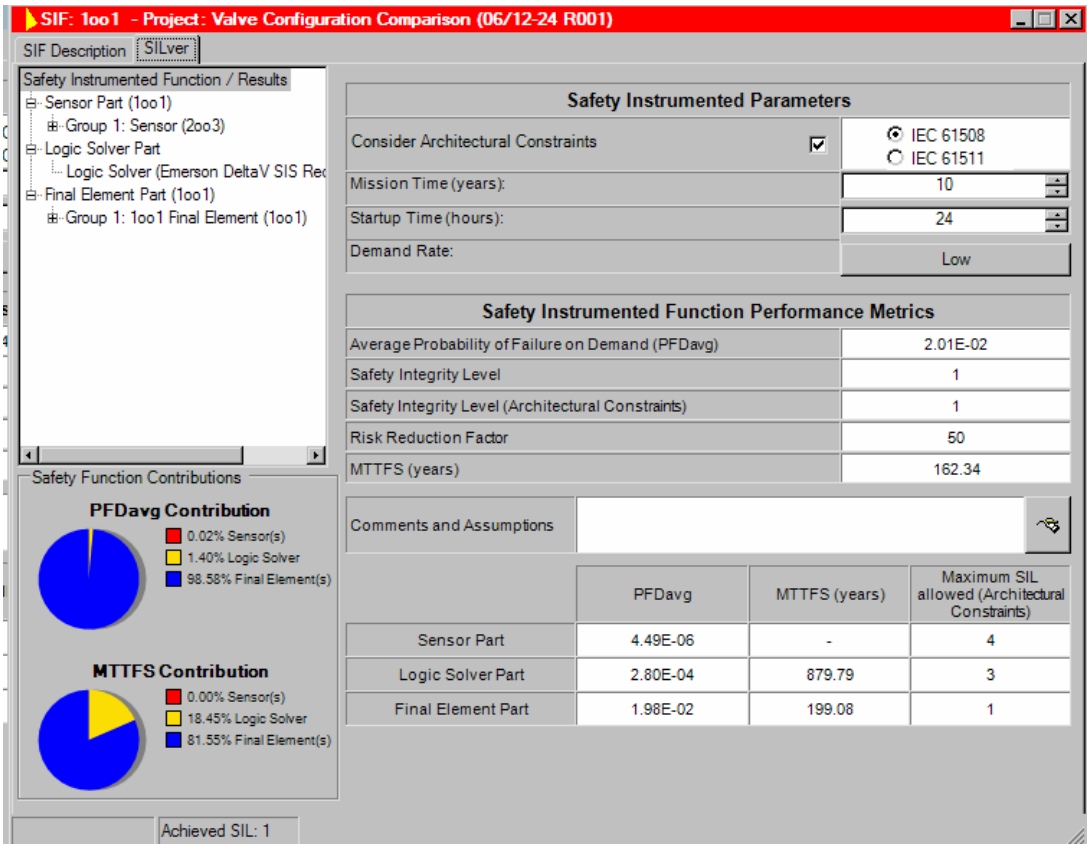


Figure 1: exSILentia results for 1oo1 architecture.

The 1oo1 architecture provides a baseline for comparison. The SIF reached a SIL 1 level with a risk reduction factor of 50. The PFDavg results were dominated by the final element as shown in the PFDavg pie chart. The MTTFS (a measure of false trip rate) was 162 years and was again limited by the final element as shown in the MTTFS contribution pie chart.

3.4 1oo2 Architecture

The 1oo2 architecture uses two sets of equipment defined for the 1oo1 architecture that are piped in series such that either valve will provide the trip protection function. The results of the exSILentia analysis are shown in Figure 2.

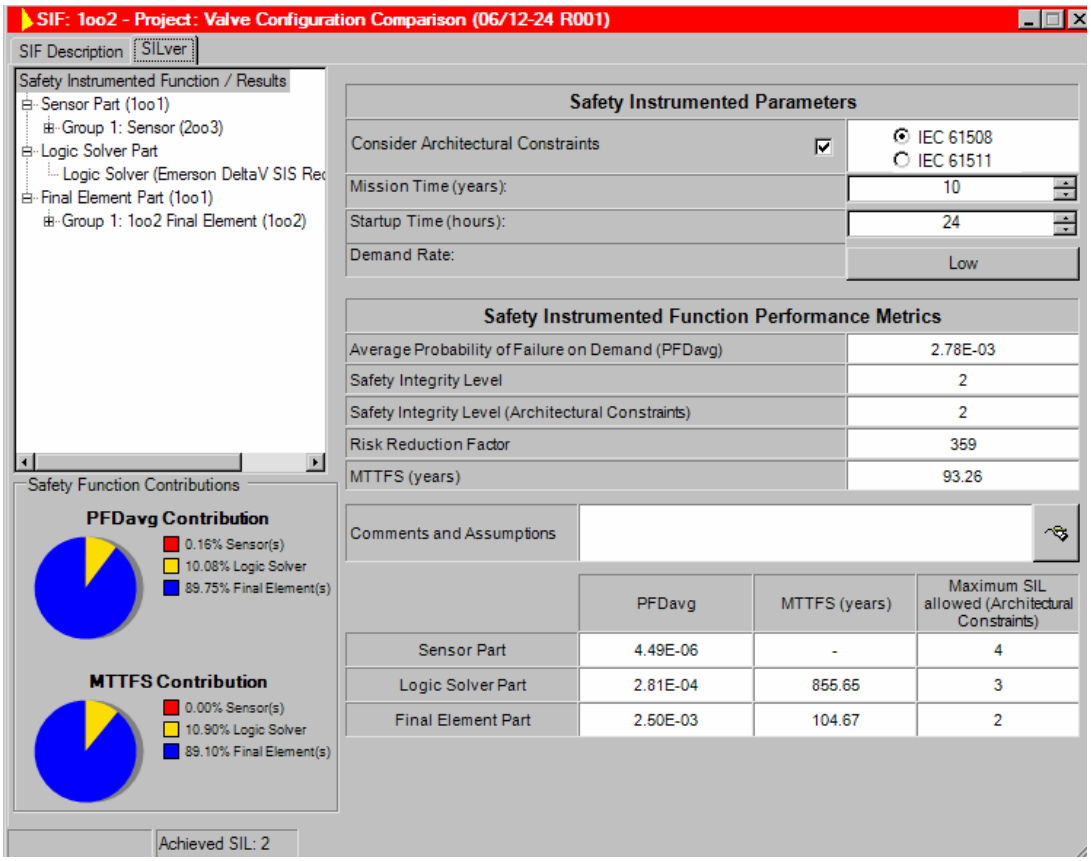


Figure 2: exSILentia results for 1oo2 architecture.

As expected, the 1oo2 architecture achieved a much higher safety rating that reached SIL 2 with a risk reduction factor of 359. Again the PFDavg was dominated by the final element as shown in PFDavg contribution pie chart. The MTTFS of the SIF dropped considerably to 93 years and this was caused primarily by the final element as shown in the MTTFS contribution pie chart.

3.5 2oo2 Architecture – Diagnostic Coverage = 90%

The 2oo2 architecture consists of two valves piped in parallel. This arrangement is counter-intuitive for safety because both valves must close to provide the safety function. This arrangement provides maximum protection against a false trip caused by a safe valve failure. The results for this architecture assuming a diagnostic coverage factor of 90% for the final element are shown in Figure 3.

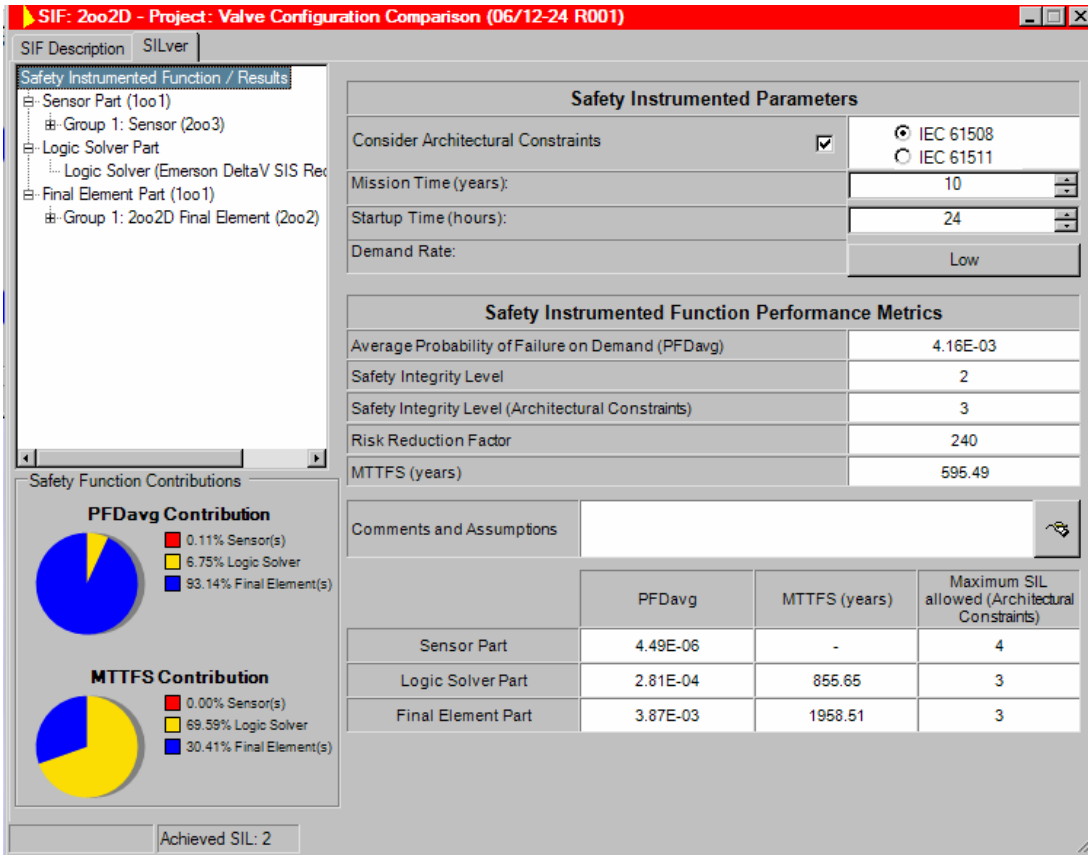


Figure 3: exSILentia results for 2oo2 architecture @ CD=90%.

3.6 2oo2 Architecture – Diagnostic Coverage = 95%

In the 2oo2 architecture protection against a false trip is inherently provided by the architecture. Safety integrity is provided by the diagnostics. When the diagnostic coverage factor increases from 90% to 95% the safety integrity is substantially improved. The results for a 2oo2 architecture assuming a diagnostic coverage factor of 95% for the final element are shown in Figure 4.

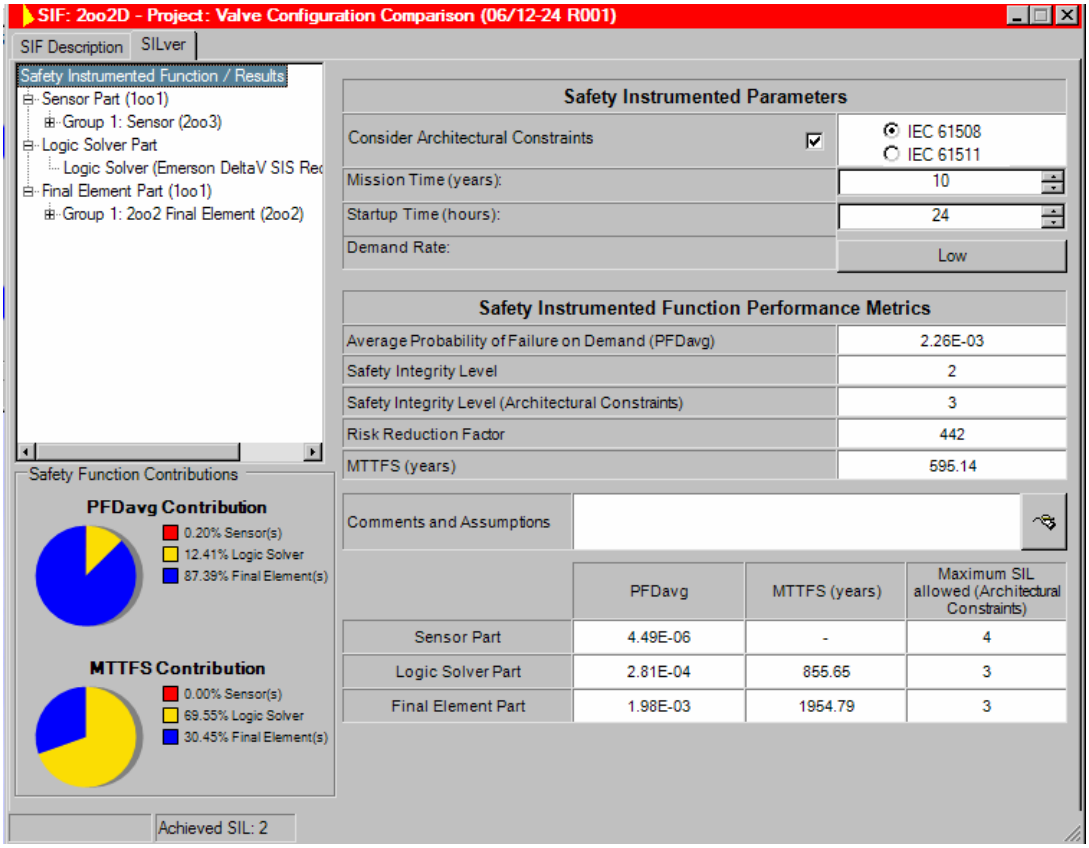


Figure 4: exSILentia results for 2oo2 architecture @ CD=95%.

4 Comparison of Results

Table 2 shows a summary of the results. Each architecture is shown on a separate line.

Table 2: Overall results

	CD	SIF PFDsvg	SIL	RRF	SIF MTTFS	FE PFDavg	FE MTTFS
1oo1		2.01E-02	1	50	162	1.98E-02	199
1oo2		2.78E-03	2	359	93	2.50E-03	105
2oo2D SCS Diag.	90%	4.16E-03	2	240	595	3.87E-03	1958
2oo2D SCS Diag.	95%	2.26E-03	2	442	595	1.98E-03	1955

5 Potential of 2oo2 Final Element Architecture using the SCS Apparatus

The comparison of these architectures shows the potential of the 2oo2 architecture when high diagnostic coverage is combined with *on-line repair*. No analysis has been done of the actual diagnostic coverage capability of the SCS device as this will change with valve type and tight shutoff characteristics. However in general, the ability to reach a value of 90% or higher seems reasonable based on many existing solenoid, actuator and valve FMEDA results.

It should be noted that the results assumed average restoration time of 24 hours for valves with detected dangerous failures.

6 Terms and Definitions

CD	Coverage Dangerous
FE	Final Element
FIT	Failure In Time (1x10-9 failures per hour)
FMEA	Failure Modes Effects Analysis
FMEDA	Failure Modes, Effects and Diagnostic Analysis
FSM	Functional Safety Management
HFT	Hardware Fault Tolerance
IEC	International Electrotechnical Commission
MTTFS	Mean Time To Fail Spuriously
O/S	Operating System
PFD	Probability of Failure on Demand
RRF	Risk Reduction Factor
SCS	Safety Cycling Systems, L.L.C.
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIR	Safety Integrity Requirement
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
SRS	Safety Requirements Specification

7 Status of the document

7.1 Releases

Version:	V1	
Revision:	R1	
Version History:	V1, R1:	Released Version, April 2, 2007
	V0, R1:	Internal Draft; March 6, 2007
Authors:	William M. Goble	
Review:	V0, R1:	client

7.2 Future Enhancements

None anticipated.

7.3 Release Signatures

Dr. William M. Goble, Principal Partner

APPENDIX A exSILentia Report Results

1 Project Valve Configuration Comparison

This exSILentia detailed report is automatically generated by the exida exSILentia tool for the Project:

Valve Configuration Comparison

Unique Project scenario identifier: 15

1.1 General Information

Project Identification:	06/12-24 R001
Project Name:	Valve Configuration Comparison
Company:	System Cycling
Project Leader:	Bill Goble
Project Initiated On:	06 Mar 2007
Project Description:	-

2 1oo1, Base Case - 1oo1

This chapter displays the analysis results for Safety Instrumented Function Base Case - 1oo1.

2.1 General Information

The following characterizes the Safety Instrumented Function.

SIF Name Base Case - 1oo1
SIF Tag 1oo1
SIF Description
SIF Reference
Unit Name Comparison
Hazard
Consequence

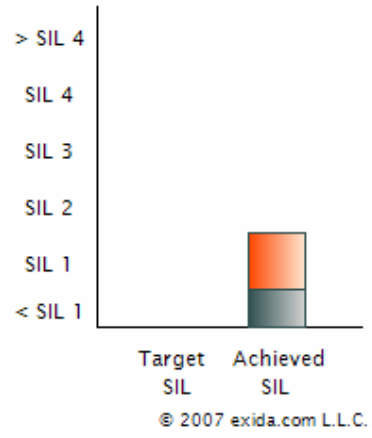
2.2 Safety Integrity Levels

The target Safety Integrity Level determined for this Safety Instrumented Function is:

To Be Determined

SIL verification determined that the Safety Integrity Level achieved by the Safety Instrumented Function is:

SIL 1



2.3 SILver

This section provides a detailed overview of the Safety Integrity Level verification performed for Safety Instrumented Function 1oo1 Base Case - 1oo1. In order to perform the reliability calculations part of the Safety Integrity Level verification, the following assumptions have been made.

Mission Time: 10 years

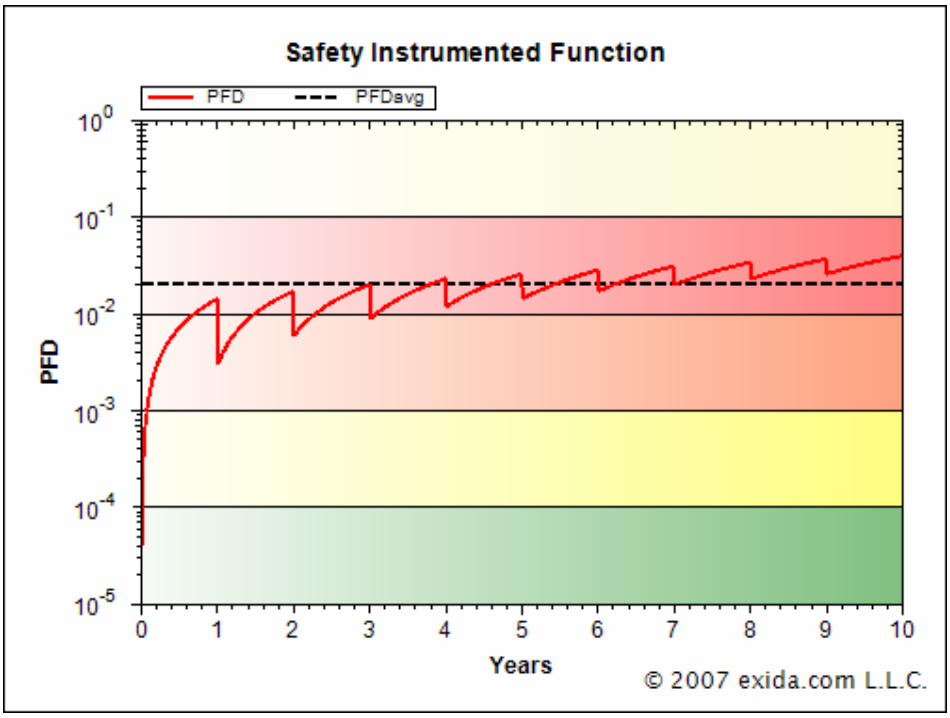
Startup time: 24 hours

Demand Rate: low

The SIF operates in Low demand mode.

The SIL verification has been performed by Bill Goble, on 06 Mar 2007.

Comments:



Given the reliability data and calculation details described in the subsequent subsections in this report the 1oo1 Base Case - 1oo1 Safety Instrumented Function achieves the functional safety performance as displayed in Table 1.

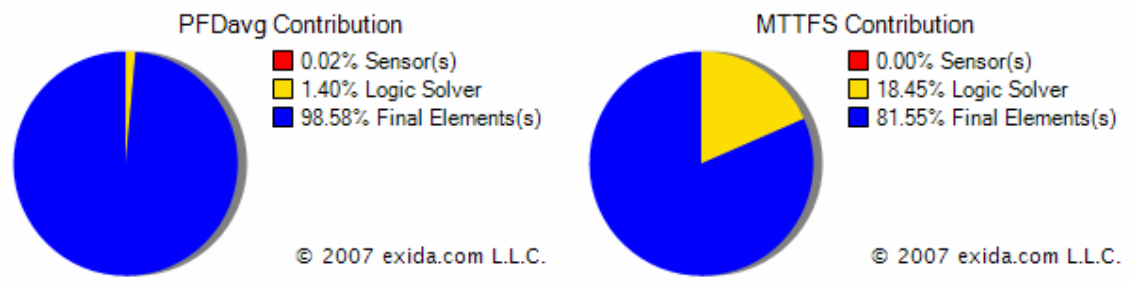
Table 1 Functional Safety Performance

PFDavg	RRF	SIL (PFDavg)	SIL (Architectural Constraints IEC 61508)
2.01E-02	**50**	**1**	**1**

The 1oo1 Base Case - 1oo1 Safety Instrumented Function was also evaluated on spurious trip behavior. The results expressed in the MTTFS are displayed in Table 2.

Table 2 Spurious Trips

MTTFS (years)
162.34



2.3.1 Sensor Part Configuration

The functional safety and spurious trip behavior of the sensor part of the 1oo1 Base Case - 1oo1 Safety Instrumented Function is quantified as follows.

Sensor part PFDavg: 4.49E-06

Sensor part HFT: 1

Sensor part MTTFS: - years

Sensor part Architectural Constraints (IEC 61508) allow use up to SIL 4.

The Sensor part of the 1oo1 Base Case - 1oo1 Safety Instrumented Function consists of 1 Sensor Group(s). The voting between these Sensor Groups is 1oo1.

2.3.1.1 Sensor Group 1: Sensor

The information and reliability data underneath describe the Sensor sensor group as it has been analyzed in this Safety Integrity Level verification.

Voting within group:	2oo3
HFT:	1
Voting type:	Identical
Equipment Leg (each):	Clean Service
	Rosemount 3051S SIS Coplanar, High trip
	Alarm Setting: Under Range
	Diagnostic Filtering: On
	External Comparison, with 95% effectiveness
β-factor:	5 [%]
MTTR:	8 hours
Proof Test Interval:	60 months
Proof Test Coverage:	98 [%]

Table 3 shows the reliability data used during the SIL verification of sensor group Sensor.

Table 3 Reliability Data Sensor Group Sensor

Component	Failure Rates [1/h]								Arch. Type	SFF [%]
	Fail Low	Fail High	Fail Det.	DD	DU	SD	SU	No Effect		
Each Leg										99.7
Clean Service									A	-
Rosemount 3051S SIS Coplanar	2.77E-07	6.20E-08	5.00E-07	*8.39E-07* *9.08E-07*	7.30E-08 *7.30E-08* *3.65E-09*			4.09E-07 *4.09E-07* *4.09E-07*	B	-

The data shown in blue and italic indicates the effect of the diagnostic filtering performed by the logic solver on the sensor group data.

The failure rates displayed in red & italic font show the adjusted failure rates due to the External Comparison. An External Comparison diagnostic coverage factor of 95% is assumed. This is more conservative than the 99% that could be claimed based on IEC 61508.

Note: External Comparison is not effective to detect failures in Digital (Static) signals.

2.3.2 Logic Solver Part Configuration

The functional safety and spurious trip behavior of the logic solver part of the 1oo1 Base Case - 1oo1 Safety Instrumented Function is quantified as follows.

Logic Solver part PFDavg: 2.80E-04

Logic Solver part HFT: 0

Logic Solver part MTTFS: 879.79 years

Logic Solver part Architectural Constraints (IEC 61508) allow use up to SIL 3.

The information and reliability data underneath describe the Logic Solver logic solver group as it has been analyzed in this Safety Integrity Level verification.

Logic Solver Name: Logic Solver

Equipment: Emerson DeltaV SIS Redundant SLS

MTTR: 8 hours

Proof Test Interval: 60 months

Proof Test Coverage: 98 [%]

β-factor: 2 [%]

Architectural Constraint Type: B

Table 4 shows the reliability data used during the SIL verification of logic solver group Logic Solver.

Table 4 Reliability Data Logic Solver Logic Solver

Component	Number used in analysis per leg	Failure Rates [1/h]				SFF [%]
		Safe Detected	Safe Undetected	Dangerous Detected	Dangerous Undetected	
Main Processor	1	1.10E-06	1.50E-08	1.30E-06	6.00E-09	99.8
Power Supply	1	2.25E-06	-	2.50E-07	-	100.0
Analog In Module	1	-	-	-	-	100.0
Analog In Channel	3	2.90E-08	-	2.30E-08	8.00E-12	-
Digital Out Low Module	1	-	-	-	-	100.0
Digital Out Low Channel	2	2.00E-08	-	1.20E-08	-	-

2.3.3 Final Element Part Configuration

The functional safety and spurious trip behavior of the final element part of the 1oo1 Base Case - 1oo1 Safety Instrumented Function is quantified as follows.

Final Element part PFDavg: 1.98E-02

Final Element part HFT: 0

Final Element part MTTFS: 199.08 years

Final Element part Architectural Constraints (IEC 61508) allow use up to SIL 1.

The Final Element part of the 1oo1 Base Case - 1oo1 Safety Instrumented Function consists of 1 Final Element Group(s). The voting between these Final Element Groups is 1oo1.

2.3.3.1 Final Element Group 1: 1oo1 Final Element

The information and reliability data underneath describe the 1oo1 Final Element final element group as it has been analyzed in this Safety Integrity Level verification.

Voting within group: 1oo1
HFT: 0
Voting type: -
Equipment Leg (each): ASCO 8316 NC, low power & zero minimum
Generic Air Operated Ball Valve, Hard Seat - Clean service, Full Stroke, Close on Trip
β-factor: -
MTTR: 24 hours
Proof Test Interval: 12 months
Proof Test Coverage: 80 [%]

Table 5 shows the reliability data used during the SIL verification of final element group 1oo1 Final Element.

Table 5 Reliability Data Final Element Group 1oo1 Final Element

Component	Failure Rates [1/h]					Arch. Type	SFF [%]
	DD	DU	SD	SU	No Effect		
Each Leg							38.6
ASCO 8316 NC, low power & zero minimum		1.59E-07		8.50E-08	4.43E-07	A	-
Generic Air Operated Ball Valve, Hard Seat - Clean service, Full Stroke, Close To Trip		1.48E-06		5.00E-07		A	-

3 1oo2, 1oo2 Comparison on Final Element

This chapter displays the analysis results for Safety Instrumented Function 1oo2 Comparison on Final Element.

3.1 General Information

The following characterizes the Safety Instrumented Function.

SIF Name 1oo2 Comparison on Final Element
SIF Tag 1oo2
SIF Description
SIF Reference
Unit Name Comparison
Hazard
Consequence

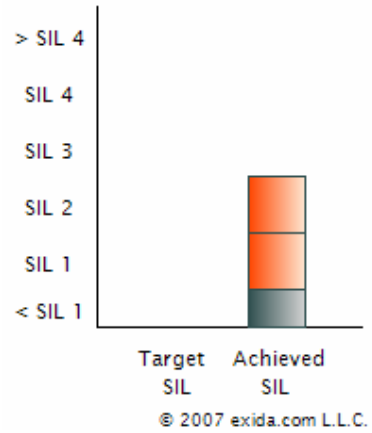
3.2 Safety Integrity Levels

The target Safety Integrity Level determined for this Safety Instrumented Function is:

To Be Determined

SIL verification determined that the Safety Integrity Level achieved by the Safety Instrumented Function is:

SIL 2



3.3 SILver

This section provides a detailed overview of the Safety Integrity Level verification performed for Safety Instrumented Function 1oo2 Comparison on Final Element. In order to perform the reliability calculations part of the Safety Integrity Level verification, the following assumptions have been made.

Mission Time: 10 years

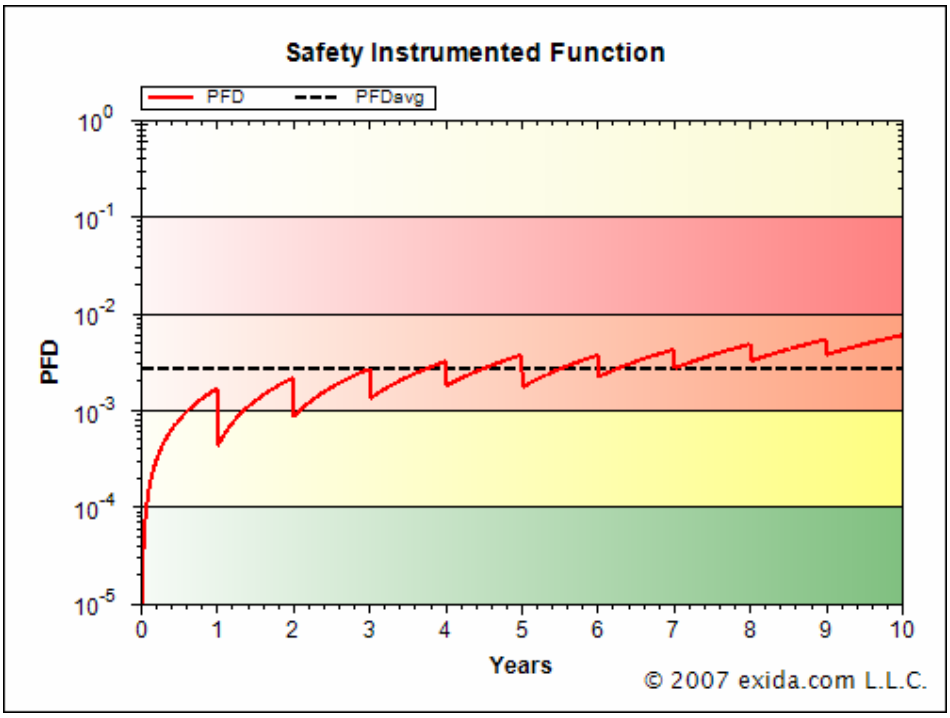
Startup time: 24 hours

Demand Rate: low

The SIF operates in Low demand mode.

The SIL verification has been performed by Bill Goble, on 06 Mar 2007.

Comments:



Given the reliability data and calculation details described in the subsequent subsections in this report the 1oo2 Comparison on Final Element Safety Instrumented Function achieves the functional safety performance as displayed in Table 6.

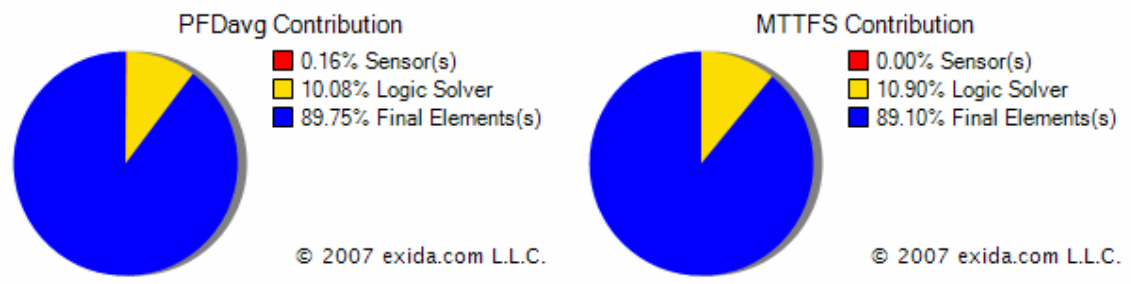
Table 6 Functional Safety Performance

PFDavg	RRF	SIL (PFDavg)	SIL (Architectural Constraints IEC 61508)
2.78E-03	**359**	**2**	**2**

The 1oo2 Comparison on Final Element Safety Instrumented Function was also evaluated on spurious trip behavior. The results expressed in the MTTFS are displayed in Table 7.

Table 7 Spurious Trips

MTTFS (years)
93.26



3.3.1 Sensor Part Configuration

The functional safety and spurious trip behavior of the sensor part of the 1oo2 1oo2 Comparison on Final Element Safety Instrumented Function is quantified as follows.

Sensor part PFDavg: 4.49E-06

Sensor part HFT: 1

Sensor part MTTFS: - years

Sensor part Architectural Constraints (IEC 61508) allow use up to SIL 4.

The Sensor part of the 1oo2 Comparison on Final Element Safety Instrumented Function consists of 1 Sensor Group(s). The voting between these Sensor Groups is 1oo1.

3.3.1.1 Sensor Group 1: Sensor

The information and reliability data underneath describe the Sensor group as it has been analyzed in this Safety Integrity Level verification.

Voting within group:	2oo3
HFT:	1
Voting type:	Identical
Equipment Leg (each):	Clean Service
	Rosemount 3051S SIS Coplanar, High trip
	Alarm Setting: Under Range
	Diagnostic Filtering: On
	External Comparison, with 95% effectiveness
β-factor:	5 [%]
MTTR:	8 hours
Proof Test Interval:	60 months
Proof Test Coverage:	98 [%]

Table 8 shows the reliability data used during the SIL verification of sensor group Sensor.

Table 8 Reliability Data Sensor Group Sensor

Component	Failure Rates [1/h]								Arch. Type	SFF [%]
	Fail Low	Fail High	Fail Det.	DD	DU	SD	SU	No Effect		
Each Leg										99.7
Clean Service									A	-
Rosemount 3051S SIS Coplanar	2.77E-07	6.20E-08	5.00E-07	*8.39E-07* *9.08E-07*	7.30E-08 *7.30E-08* *3.65E-09*			4.09E-07 *4.09E-07* *4.09E-07*	B	-

The data shown in blue and italic indicates the effect of the diagnostic filtering performed by the logic solver on the sensor group data.

The failure rates displayed in red & italic font show the adjusted failure rates due to the External Comparison. An External Comparison diagnostic coverage factor of 95% is assumed. This is more conservative than the 99% that could be claimed based on IEC 61508.

Note: External Comparison is not effective to detect failures in Digital (Static) signals.

3.3.2 Logic Solver Part Configuration

The functional safety and spurious trip behavior of the logic solver part of the 1oo2 Comparison on Final Element Safety Instrumented Function is quantified as follows.

Logic Solver part PFDavg: 2.81E-04

Logic Solver part HFT: 0

Logic Solver part MTTFS: 855.65 years

Logic Solver part Architectural Constraints (IEC 61508) allow use up to SIL 3.

The information and reliability data underneath describe the Logic Solver logic solver group as it has been analyzed in this Safety Integrity Level verification.

Logic Solver Name: Logic Solver

Equipment: Emerson DeltaV SIS Redundant SLS

MTTR: 8 hours

Proof Test Interval: 60 months

Proof Test Coverage: 98 [%]

β-factor: 2 [%]

Architectural Constraint Type: B

Table 9 shows the reliability data used during the SIL verification of logic solver group Logic Solver.

Table 9 Reliability Data Logic Solver Logic Solver

Component	Number used in analysis per leg	Failure Rates [1/h]				SFF [%]
		Safe Detected	Safe Undetected	Dangerous Detected	Dangerous Undetected	
Main Processor	1	1.10E-06	1.50E-08	1.30E-06	6.00E-09	99.8
Power Supply	1	2.25E-06	-	2.50E-07	-	100.0
Analog In Module	1	-	-	-	-	100.0
Analog In Channel	3	2.90E-08	-	2.30E-08	8.00E-12	-
Digital Out Low Module	1	-	-	-	-	100.0
Digital Out Low Channel	2	2.00E-08	-	1.20E-08	-	-

3.3.3 Final Element Part Configuration

The functional safety and spurious trip behavior of the final element part of the 1oo2 1oo2 Comparison on Final Element Safety Instrumented Function is quantified as follows.

Final Element part PFDavg: 2.50E-03

Final Element part HFT: 1

Final Element part MTTFS: 104.67 years

Final Element part Architectural Constraints (IEC 61508) allow use up to SIL 2.

The Final Element part of the 1oo2 Comparison on Final Element Safety Instrumented Function consists of 1 Final Element Group(s). The voting between these Final Element Groups is 1oo1.

3.3.3.1 Final Element Group 1: 1oo2 Final Element

The information and reliability data underneath describe the 1oo2 Final Element final element group as it has been analyzed in this Safety Integrity Level verification.

Voting within group: 1oo2
HFT: 1
Voting type: Identical
Equipment Leg (each): ASCO 8316 NC, low power & zero minimum
Generic Air Operated Ball Valve, Hard Seat - Clean service, Full Stroke, Close on Trip
β-factor: 10 [%]
MTTR: 24 hours
Proof Test Interval: 12 months
Proof Test Coverage: 80 [%]

Table 10 shows the reliability data used during the SIL verification of final element group 1oo2 Final Element.

Table 10 Reliability Data Final Element Group 1oo2 Final Element

Component	Failure Rates [1/h]					Arch. Type	SFF [%]
	DD	DU	SD	SU	No Effect		
Each Leg							38.6
ASCO 8316 NC, low power & zero minimum		1.59E-07		8.50E-08	4.43E-07	A	-
Generic Air Operated Ball Valve, Hard Seat - Clean service, Full Stroke, Close To Trip		1.48E-06		5.00E-07		A	-

4 2oo2D, 2oo2 Comparison on Final Element

This chapter displays the analysis results for Safety Instrumented Function 2oo2 Comparison on Final Element.

4.1 General Information

The following characterizes the Safety Instrumented Function.

SIF Name 2oo2 Comparison on Final Element
SIF Tag 2oo2D
SIF Description
SIF Reference
Unit Name Comparison
Hazard
Consequence

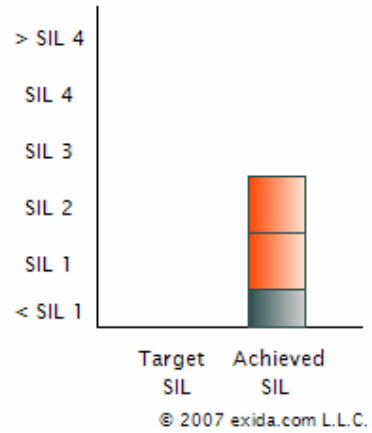
4.2 Safety Integrity Levels

The target Safety Integrity Level determined for this Safety Instrumented Function is:

To Be Determined

SIL verification determined that the Safety Integrity Level achieved by the Safety Instrumented Function is:

SIL 2



4.3 SILver

This section provides a detailed overview of the Safety Integrity Level verification performed for Safety Instrumented Function 2oo2D 2oo2 Comparison on Final Element. In order to perform the reliability calculations part of the Safety Integrity Level verification, the following assumptions have been made.

Mission Time: 10 years

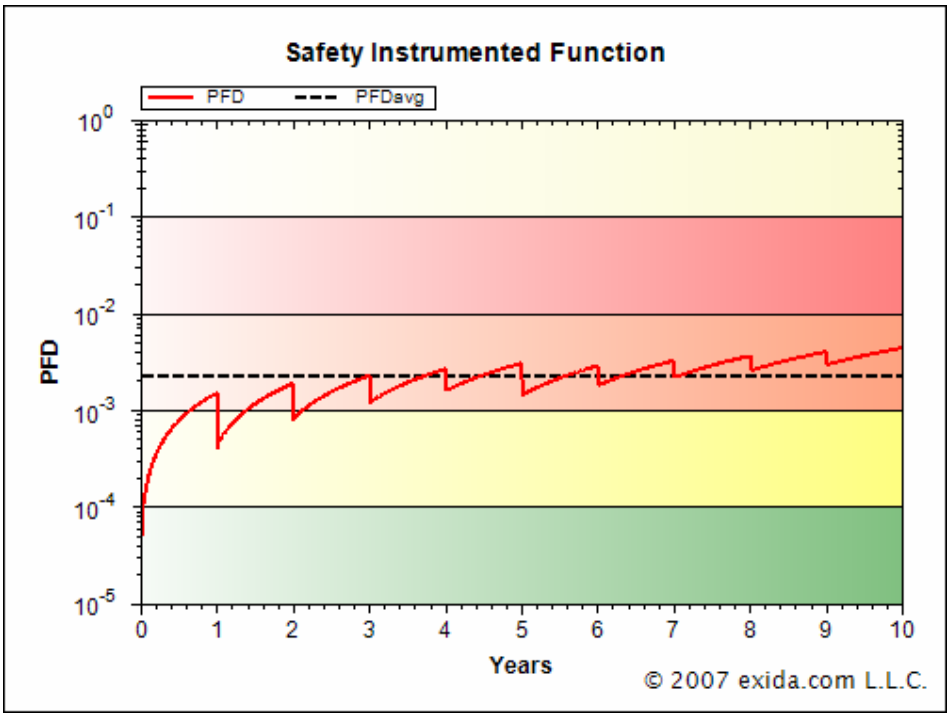
Startup time: 24 hours

Demand Rate: low

The SIF operates in Low demand mode.

The SIL verification has been performed by Bill Goble, on 06 Mar 2007.

Comments:



Given the reliability data and calculation details described in the subsequent subsections in this report the 2oo2D 2oo2 Comparison on Final Element Safety Instrumented Function achieves the functional safety performance as displayed in Table 11.

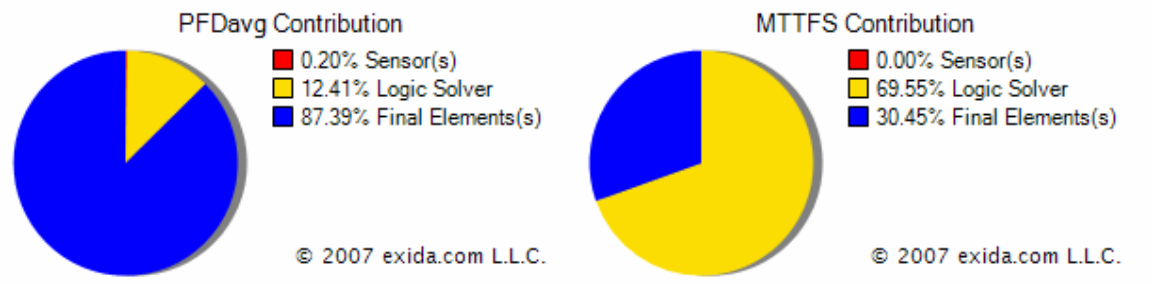
Table 11 Functional Safety Performance

PFDavg	RRF	SIL (PFDavg)	SIL (Architectural Constraints IEC 61508)
2.26E-03	**442**	**2**	**3**

The 2oo2D 2oo2 Comparison on Final Element Safety Instrumented Function was also evaluated on spurious trip behavior. The results expressed in the MTTFS are displayed in Table 12.

Table 12 Spurious Trips

MTTFS (years)
595.14



4.3.1 Sensor Part Configuration

The functional safety and spurious trip behavior of the sensor part of the 2oo2D 2oo2 Comparison on Final Element Safety Instrumented Function is quantified as follows.

Sensor part PFDavg: 4.49E-06

Sensor part HFT: 1

Sensor part MTTFS: - years

Sensor part Architectural Constraints (IEC 61508) allow use up to SIL 4.

The Sensor part of the 2oo2D 2oo2 Comparison on Final Element Safety Instrumented Function consists of 1 Sensor Group(s). The voting between these Sensor Groups is 1oo1.

4.3.1.1 Sensor Group 1: Sensor

The information and reliability data underneath describe the Sensor sensor group as it has been analyzed in this Safety Integrity Level verification.

Voting within group:	2oo3
HFT:	1
Voting type:	Identical
Equipment Leg (each):	Clean Service
	Rosemount 3051S SIS Coplanar, High trip
	Alarm Setting: Under Range
	Diagnostic Filtering: On
	External Comparison, with 95% effectiveness
β-factor:	5 [%]
MTTR:	8 hours
Proof Test Interval:	60 months
Proof Test Coverage:	98 [%]

Table 13 shows the reliability data used during the SIL verification of sensor group Sensor.

Table 13 Reliability Data Sensor Group Sensor

Component	Failure Rates [1/h]								Arch. Type	SFF [%]
	Fail Low	Fail High	Fail Det.	DD	DU	SD	SU	No Effect		
Each Leg										99.7
Clean Service									A	-
Rosemount 3051S SIS Coplanar	2.77E-07	6.20E-08	5.00E-07	*8.39E-07* *9.08E-07*	7.30E-08 *7.30E-08* *3.65E-09*			4.09E-07 *4.09E-07* *4.09E-07*	B	-

The data shown in blue and italic indicates the effect of the diagnostic filtering performed by the logic solver on the sensor group data.

The failure rates displayed in red & italic font show the adjusted failure rates due to the External Comparison. An External Comparison diagnostic coverage factor of 95% is assumed. This is more conservative than the 99% that could be claimed based on IEC 61508.

Note: External Comparison is not effective to detect failures in Digital (Static) signals.

4.3.2 Logic Solver Part Configuration

The functional safety and spurious trip behavior of the logic solver part of the 2oo2D 2oo2 Comparison on Final Element Safety Instrumented Function is quantified as follows.

Logic Solver part PFDavg: 2.81E-04

Logic Solver part HFT: 0

Logic Solver part MTTFS: 855.65 years

Logic Solver part Architectural Constraints (IEC 61508) allow use up to SIL 3.

The information and reliability data underneath describe the Logic Solver logic solver group as it has been analyzed in this Safety Integrity Level verification.

Logic Solver Name: Logic Solver

Equipment: Emerson DeltaV SIS Redundant SLS

MTTR: 8 hours

Proof Test Interval: 60 months

Proof Test Coverage: 98 [%]

β-factor: 2 [%]

Architectural Constraint Type: B

Table 14 shows the reliability data used during the SIL verification of logic solver group Logic Solver.

Table 14 Reliability Data Logic Solver Logic Solver

Component	Number used in analysis per leg	Failure Rates [1/h]				SFF [%]
		Safe Detected	Safe Undetected	Dangerous Detected	Dangerous Undetected	
Main Processor	1	1.10E-06	1.50E-08	1.30E-06	6.00E-09	99.8
Power Supply	1	2.25E-06	-	2.50E-07	-	100.0
Analog In Module	1	-	-	-	-	100.0
Analog In Channel	3	2.90E-08	-	2.30E-08	8.00E-12	-
Digital Out Low Module	1	-	-	-	-	100.0
Digital Out Low Channel	2	2.00E-08	-	1.20E-08	-	-

4.3.3 Final Element Part Configuration

The functional safety and spurious trip behavior of the final element part of the 2oo2D 2oo2 Comparison on Final Element Safety Instrumented Function is quantified as follows.

Final Element part PFDavg: 1.98E-03

Final Element part HFT: 0

Final Element part MTTFS: 1954.79 years

Final Element part Architectural Constraints (IEC 61508) allow use up to SIL 3.

The Final Element part of the 2oo2D 2oo2 Comparison on Final Element Safety Instrumented Function consists of 1 Final Element Group(s). The voting between these Final Element Groups is 1oo1.

4.3.3.1 Final Element Group 1: 2oo2 Final Element

The information and reliability data underneath describe the 2oo2 Final Element final element group as it has been analyzed in this Safety Integrity Level verification.

Voting within group: 2oo2
HFT: 0
Voting type: Identical
Equipment Leg (each): ASCO 8316 NC, low power & zero minimum
Generic Air Operated Ball Valve, Hard Seat - Clean service, Full Stroke, Close on Trip
Full Valve Stroke Testing is performed; 95% coverage.
β-factor: 10 [%]
MTTR: 24 hours
Proof Test Interval: 12 months
Proof Test Coverage: 95 [%]

Table 15 shows the reliability data used during the SIL verification of final element group 2oo2 Final Element.

Table 15 Reliability Data Final Element Group 2oo2 Final Element

Component	Failure Rates [1/h]					Arch. Type	SFF [%]
	DD	DU	SD	SU	No Effect		
Each Leg							96.9
ASCO 8316 NC, low power & zero minimum	*1.51E-07*	1.59E-07 *7.95E-09*	*8.50E-08*	8.50E-08 *0.00E+00*	4.43E-07 *4.43E-07*	A	-
Generic Air Operated Ball Valve, Hard Seat - Clean service, Full Stroke, Close To Trip	*1.41E-06*	1.48E-06 *7.40E-08*	*5.00E-07*	5.00E-07 *0.00E+00*		A	-

The failure rates displayed in red & italic font show the adjusted failure rates due to the Full Stroke Test performed (if any). Diagnostic coverage factor(s) for the Full Stroke Test is (are) provided on a per leg basis.

5 SILver Group Reuse Overview

This chapter provides an overview of the various groups that were defined during the SIL verification analyses of the Valve Configuration Comparison project. The reuse of groups is available between Safety Instrumented Functions to account for identical hardware used in those different Safety Instrumented Functions. The group reuse allows users to specify a specific group once, reuse it, and with all future changes made to a single group cascading to all Safety Instrumented Functions it is used in.

This overview indicates the groups that were reused, the number of times they were reused, and the Safety Instrumented Functions that they were used in.

5.1 Sensor Groups Reused

No Groups Reused

5.2 Logic Solver Groups Reused

No Groups Reused

5.3 Final Element Groups Reused

No Groups Reused

6 Abbreviations

IPL	Independent Protection Layers
HFT	Hardware Fault Tolerance
MTTFS	Mean Time To Fail Spurious
MTTR	Mean Time To Restore
PFDavg	Average Probability of Failure on Demand
PFH	Probability of a Dangerous Failure per Hour
PIU	Proven In Use
RRF	Risk Reduction Factor
SERH	Safety Equipment Reliability Handbook
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SRS	Safety Requirements Specification
β-factor	Beta factor, indicating common cause susceptibility

DD	Dangerous Detected
DU	Dangerous Undetected
SD	Safe Detected
SU	Safe Undetected
AD	Annunciation Detected
AU	Annunciation Undetected

7 Disclaimer, Assumptions, Equipment Data

7.1 Disclaimer

The user of the exSILentia software is responsible for verification of all results obtained and their applicability to any particular situation. Calculations are performed per guidelines in applicable international standards. *exida.com L.L.C.* accepts no responsibility for the correctness of the regulations or standards on which the tool is based. In particular, *exida.com L.L.C.* accepts no liability for decisions based on the results of this software. The *exida.com L.L.C.* guarantee is restricted to the correction of errors or deficiencies within a reasonable period when such errors or deficiencies are brought to our attention in writing. *exida.com L.L.C.* accepts no responsibility for adjustments made to this automatically generated report made by the user.

7.2 Assumptions SILect

The severity level translation into tolerable frequencies is based on the risk calibration selected by the user.

Unmitigated frequencies are directly calculated from initiating event frequencies and probabilities for enabling conditions and Independent Protection Layers using algebraic formulas.

The required Risk Reduction Factor, and therefore Target SIL, is obtained directly from the relation between tolerable frequency and unmitigated frequency.

The tolerable fatality frequency used in the **Health and Safety Executive - HSE UK** tolerable risk calibration is based on *The Setting of Safety Standards: A Report by an Interdepartmental Group of External Advisors*, London, HM Stationery Office, 1996.

The tolerable fatality frequency used in the **IEC 61511 part 3, Annex C** tolerable risk calibration is based on IEC 61511 part 3, Functional Safety: Safety Instrumented Systems for the process industry sector - Part 3: Guidance for the determination of Safety Integrity Levels, Geneva Switzerland, IEC, 2003.

exida.com L.L.C. holds no responsibility for the above mentioned tolerable fatality frequencies nor any other tolerable fatality frequencies used in the SILect tool.

SIL Threshold example

Assume a calculated Required Risk Reduction Factor of 29, which would fall in the 10 - 100 Risk Reduction range. With a SIL Threshold Ratio of 1, a calculated Risk Reduction Factor of 29 would result in a Target SIL of SIL 2. The calculated Risk Reduction Factor is in this case greater than the SIL determination threshold which lies at 10 (10 * 1). With a SIL Threshold Ratio of 3, a calculated Risk Reduction Factor of 29 would result in a Target SIL of SIL 1. The calculated Risk Reduction Factor is in this case less than the SIL determination threshold which lies at 30 (10 * 3). The SIL determination threshold (the boundary between one SIL level and the next one up) is calculated by multiplying the relevant lower limit of the Risk Reduction range times the SIL Threshold Ratio.

7.3 Assumptions SIF SRS

All information that is output of the SIF SRS tool is directly linked to user input. No calculations are performed, nor is the information provided by the user changed in any way. The Target Safety Integrity Level listed in the SIF SRS (if any) is derived from user input into the SILect tool.

7.4 Assumptions SILver

De-energize-to-trip

SILver is designed to verify Safety Instrumented Systems (SIS) that are based on the de-energize-to-trip principle. De-energize-to-trip implies that on loss of power the SIS will go to a safe state.

A list of all other assumptions on which SILver is based can be found in the online SILver Help.

7.5 Equipment data

exida has compiled a proprietary equipment failure database. This database is a compilation of failure data collected from a variety of public and confidential sources and presents an industry average. The database is published as the “Safety Equipment Reliability Handbook” ISBN-13: 978-0-9727234-1-1. The reliability data collection process as described in this book applies to the SILver equipment data collection process.

The user is responsible for determining the applicability of the failure data to any particular environment. The stress levels assumed to determine the equipment failure rate are average for an industrial environment and can be compared to the RAC Ground Benign classification. Accurate plant specific data is preferable to general industry average data. Industrial plant sites with high levels of stress must use failure rate data that is adjusted to a higher value to account for the specific conditions of the plant.