White Paper

Project:

Route 2_H SIL Verification for Rosemount Type B Transmitters with Type A Components

Customer:

Rosemount Inc.
(an Emerson Process Management company)
Chanhassen, MN
USA

Contract No.: ROS 12/05-020
Report No.: ROS 12/05-020 R001
Version V1, Revision R5, April 30, 2013
Hal Thomas

The 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.

Management Summary

This report documents SIL Verification when using a sensor sub-system with a combination of a Type B device such as a Rosemount pressure transmitter with a Type A device such as a Rosemount 1199 remote seals.

Three constraints must be checked to fully verify that a design meets a target SIL level. These are:

1. PFH / PFDavg - the probability of dangerous failure must be less than the target number for a set of equipment used in a safety instrumented function. The PFDavg calculation is based on a number of variables but the primary product attribute is the "dangerous undetected" failure rate.

2. Systematic Capability - all products used in a safety instrumented function must meet systematic capability for the target SIL level. This is normally achieved by purchasing a product with IEC 61508 certification for the given SIL level (or better). It may also be done with a prior use justification.

3. Architecture Constraints - For each element in a safety instrumented function, minimum architecture constraints must be met. There are tables in IEC 61511 for this purpose. Alternatively, the more flexible tables in IEC 61508 are commonly used. In IEC 61508:2010, two alternative approaches are permitted. These alternatives are called Route 1_H and Route 2_H.

For example, a sensor sub-system using a Type B Rosemount pressure transmitter and Type A Rosemount 1199 remote seals has a low dangerous undetected failure rate. With this low failure rate, the designs will meet the PFDavg constraint in many low demand applications.

The exida certified Rosemount products have a SIL 3 capability rating and have no problem meeting the Systematic Capability constraint.

Depending on application conditions, the Architecture Constraint may not be met if IEC 61511 tables or IEC 61508 Route 1_H tables are used. However if the Type A and B device can meet IEC 61508 Route 2_H failure data requirements, the IEC 61508 Route 2_H architecture constraint tables can be used. The IEC 61508 Route 2_H architecture constraints are identical to IEC 61511 tables if prior use justification is done.

Several examples demonstrate how a SIL 2 claim limit can be achieved for:

- A 1oo1 (HFT=0) Rosemount 3051 coplanar pressure (1 Remote Seal) transmitter with an 1199 remote seal in high trip service, operating in a severe process severity and low demand application.
- A 1oo1 (HFT=0) Rosemount 3051 Differential Pressure transmitter with two 1199 remote seals in a low level trip service, operating in a severe process severity and low demand application.
- A 1oo1 (HFT=0) Rosemount 3051 Differential Pressure transmitter with two 1199 remote seals in a high level trip service, operating in a severe process severity and low demand application

Table of Contents

1 SIL Verification

1.1 SIL Verification Constraints

Three constraints must be checked to fully verify that a design meets a target SIL level. These are:

1. PFH / PFDavg - the probability of dangerous failure must be less than the target number for a set of equipment used in a safety instrumented function. The PFDavg calculation is based on a number of variables but the primary product attribute is the "dangerous undetected" failure rate.

2. Systematic Capability - all products used in a safety instrumented function must meet systematic capability for the target SIL level. This is normally achieved by purchasing a product with IEC 61508 certification for the given SIL level (or better). It may also be done with a prior use justification.

3. Architecture Constraints - For each element in a safety instrumented function, minimum architecture constraints must be met. There are tables in IEC 61511 for this purpose. Alternatively, the more flexible tables in IEC 61508 are commonly used. In IEC 61508:2010, two alternative approaches are permitted. These alternatives are called Route 1_H and Route 2_H.

1.2 Architecture Constraints

IEC 61511 provides tables showing minimum levels of redundancy depending on SIL target level and a variable called Safe Failure Fraction (SFF).

Table 1: IEC 61511:2003 Architecture Constraint Table - Field Instruments without Prior Use

SIL	Minimum Hardware Fault Tolerance
1	0
2	1
3	2
4	Special requirements apply (see IEC 61508)

With this table, any SIL 2 design would require safety redundant field devices with HFT = 1.

However, IEC 61511 allows for a one SIL level reduction with "prior use" justification. The table would then appear as Table 2.

Table 2: IEC 61511:2003 Architecture Constraints - Field Instruments with Prior Use

SIL	Minimum Hardware Fault Tolerance
1	0
2	0
3	1
4	Special requirements apply (see IEC 61508)

IEC 61511 also allows the more complicated IEC 61508 tables to be used as an alternative. IEC61508:2010 provides two routes to satisfy architecture constraints required to meet a particular SIL (Safety Integrity Level) in a particular safety instrumented function design. They are:

- Route 1_H based on hardware fault tolerance and safe failure fraction concepts for each element; or,
- Route 2_H based on component reliability data from end user feedback, increased confidence levels and hardware fault tolerance for specified safety integrity levels.

The Route 1_H tables are shown in Table 3 and Table 4.

Table 3: IEC 61508:2010 Route 1_H Architecture Constraint Table for Type A elements.

Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % - < 90 %	SIL 2	SIL 3	SIL 4
90 % - < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4
NOTE A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function			

Table 4: IEC 61508:2010 Route 1_H Architecture Constraint Table for Type B elements.

Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
< 60 %	Not allowed	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

This Route 1_H Type B table would allow HFT=0 for SIL 2 if a variable called the safe failure fraction is greater than 90%.

A table can be constructed from the IEC 61508:2010 Route 2_H requirements. This is shown in Table 5.

Table 5: IEC 61508:2010 Route 2_H Architecture Constraints

SIL	Minimum Hardware Fault Tolerance
1	0
2	0
3	1
4	2

Comparing Table 5 with Table 2 shows that the architecture constraint requirements from 61508:2010 Route 2_H are the same as for 61511 field devices with prior use justification.

1.3 Combining Type A and Type B devices in one element

Combining Type A and Type B devices into one element during a SIF (Safety Instrumented Function) verification can sometimes be problematic when using IEC 61508 Route 1_H as there are different requirements for Type A and Type B devices as can be seen comparing Table 3 to Table 4.

Route 1_H is clear. To achieve SIL 2 integrity for HFT=0, an element's SFF must be greater than 60% SFF for a type A device (Table 3) and greater than 90% for a Type B device (Table 4). If one were to combine the hardware in this example into one element, the combined Type B SFF can fall below 90% making it seem like a greater fault tolerance is required, even though it can be shown that the PFD_{avg} is capable of better performance even when using conservative exida FMEDA failure rates.

In all SIF verifications, the end user must include the process to sensor interface. For example, in many applications the interface is an impulse line. Often a manifold valve is also included. The dangerous failures associated with these components are plugging and leaving a valve closed. These failures are a function of the end user's process fluid and management systems, therefore they are site specific and cannot be analyzed during a manufacturer's product certification.

As an example, the use of remote seals actually eliminates or greatly reduces the contribution from these failures, although they introduce the potential for new failure modes the most significant being "fill fluid leakage." Fill fluid leakage is a dangerous failure in some applications, depending upon whether it is for a single Remote Seal or DP service and initiation of function on high or low process measurement. In this example, Route 1_H overly penalizes the overall application, even though the remote seal is a robust type A device, especially relative to plugging service where impulse lines would be much less reliable.

The Architectural Constraints based on HFT and SFF were originally created as an extra design constraint for complex microprocessor based devices where reliable failure rate and failure mode data was questionable primarily because new technology is being introduced faster than reliable failure rate data can be collected. Some consider the Architecture Constraints to be applicable only to complex devices. Considering the above issues, Route 2_H provides a more appropriate means to deal with the confusion created by Route 1_H when using Type A devices that do not achieve the rigid SFF rules imposed by that route.

1.4 Purpose

This white paper provides examples of how to combine a Type B device such as a Rosemount 3051 pressure transmitter with Type A devices such as a Rosemount 1199 remote seals using Route 2_H, demonstrating a SIL 2 claim limit being achieved for:

- A 1oo1 (HFT=0) Rosemount 3051 coplanar pressure (1 Remote Seal) transmitter with an 1199 remote seal in high trip service, operating in a severe process severity and low demand application.
- A 1oo1 (HFT=0) Rosemount 3051 Differential Pressure transmitter with an 1199 remote seal in a low level trip service, operating in a severe process severity and low demand application.
- A 1oo1 (HFT=0) Rosemount 3051 Differential Pressure transmitter with an 1199 remote seal in a high level trip service, operating in a severe process severity and low demand application.

1.5 IEC 61508:2010 Route 2_H Criteria

1.5.1 Reliability Data

One of the primary arguments for creation of the Route 1_H architectural requirement was the recognition that few practitioners have the depth of knowledge and experience required to evaluate failure data and establish failure rates for use in SIF verification calculations. This is especially true for complex Type B devices. Many examples of very optimistic data exist [R3] including of the use "cycle test" results to determine low demand failure rates.

Route 2_H requires the calculation of random hardware failure is based upon:

- Field feedback for devices in use in a similar application and environment, and
- Data collection in accordance with international standards (e.g., IEC 60300-3-2or ISO 14224:), and
- Evaluation with consideration of the quantity of field records
- Expert judgment and where necessary, the undertaking of specific tests

Regression analysis of the data is to utilize a 90% confidence interval to determine the reliability parameters.

1.5.2 Safety Justification

The Route 2_H approach also requires some additional justification.

- For Type A devices, if an HFT greater than 0 would introduce additional failures and perhaps reduce safety then HFT may be reduced to 0 if dangerous failure rates are low compared to the target failure measure.
- Type B elements shall have a diagnostic coverage of greater than or equal to 60 % to meet Route 2_H.

1.6 Application to Rosemount 1199 Remote Seal

The Rosemount 1199 remote seal is a Type A device. Per the Route 2_H rules, no hardware fault tolerance (HFT) is required for SIL 1 or SIL 2 low demand applications. For higher SIL requirements in low demand applications the required HFT can be achieved by the end user with transmitter/seal combination voting architectures (e.g. 1oo2, 2oo3, etc.).

Type A Safety Justification:

- Remote seals are utilized to mitigate potential issues with impulse lines such as plugging. Not using the remote seal would increase the likelihood of failure. In addition, use of the seal(s) decreases the potential for systematic failures by eliminating root valves that have the potential to be left closed by plant personnel.
- The incremental undetected dangerous failure rates due to adding Rosemount 1199 remote seal(s) range from 2e-9 per hour to 8.3e-8 per hour, depending upon whether the application is a low trip, high trip, gauge, differential, normal service or severe service. For a 1 year proof test interval and 95% proof test coverage, the PFD_{avg} ranges from 1.66e-5 to 6.88e-4. This would represent one percent of 1.66e-3 to 6.88e-2.

Failure rate data was determined by *exida* performing a FMEDA. Data used was from the Electrical and Mechanical Component Reliability Handbook [N2] which was derived using field failure data from multiple sources analyzed at a confidence interval of 90% per IEC 61508, Route 2_H. Every component in the remote seal FMEDA had a documented failure data of over ten billion unit operating hours. The rates were chosen to match the *exida* environmental profile for process wetted parts and general field equipment profile for all others. The FMEDA results were further validated for proven in use by analysis of Rosemount field return data, indicating the FMEDA numbers to be conservative. Additional field failure data from end users was collected. The **total unit operating hours of field failure data supporting the component database exceeds sixty billion unit operating hours**.

1.7 Seal Failure Impact on Application

Table 6 shows the failure rates representing the incremental remote seal failure rates when being used with Rosemount transmitters that have been certified by *exida*. These failure rates exclude those mechanical failures that are already included in the transmitter that represent the overlap between the two FMEDA analyses.

It can be seen that the type of process application, i.e. high or low trip, greatly impacts the values for dangerous undetected failures. For DP applications, it is also impacted by whether the high or low side seal that leaks.

When performing a SIL verification that includes Rosemount seal(s) and a transmitter, the dangerous undetected incremental failure rates are to be added to the transmitter dangerous undetected failure rates to obtain the overall dangerous undetected failure rate for the total sensor sub-system.

The user is cautioned while this applies to Rosemount transmitters and seal that have been certified by *exida*, Other FMEDA analyses performed by other companies may treat the analysis boundary differently, not including the components that represent an overlap. This can result in a gap between the seal and transmitter failure rate numbers that is not accounted for. End users should verify the details of any FMEDA boundary interfaces when using equipment that has been analyzed in separate reports.

Table 6: Rosemount 1199 Remote Seal Incremental Failure Rates

Application Description	Failure Description	Effect on Output	Failure Classification	Failure Rate (FIT)	
				Normal	Severe
Trip on High Pressure	Leakage of fill fluid	Fails low	Dangerous Undetected	46	76
			Safe Undetected	0	0
Trip on Low Pressure	Leakage of fill fluid	Fails low	Dangerous Undetected	2	3
			Safe Undetected	44	74
Trip on High DP	Leakage of high side fill fluid	Fails low	Dangerous Undetected	50	83
	Leakage of low side fill fluid	Fails high	Safe Undetected	41	70
Trip on Low DP	Leakage of high side fill fluid	Fails low	Safe Undetected	46	77
	Leakage of low side fill fluid	Fails high	Dangerous Undetected	46	75

1.8 High Pressure Trip in Low Demand Application Example

Configuration: 1oo1 Rosemount 3051C coplanar pressure (1 Remote Sensor) transmitter with an 1199 remote seal in high trip service, operating in a severe process severity application.

Failure rates from the Rosemount 3051C coplanar pressure transmitter were added to the incremental failure rates for a high trip remote seal in severe service (Table 7). These numbers were obtained from the exSILentia SIL verification tool which accurately calculates PFDavg using discrete time Markov models.

exSILentia SILver results

Constraint	**Result**		**SIL 2 Requirement**	**SIL Achieved**
Sensor sub-system PFDavg	3.72E-03		PFDavg max. = 0.01	2
Sensor sub-system SIL Capability	Systematic Capability = SC3	exida IEC 61508 Certified	SC2	3
Sensor sub-system Architecture Constraints	HFT=0	Route 2_H Table	HFT=0	2

Sensor sub-system MTTFS: 1848.1 years

In order to perform the PFDavg calculation part of the Safety Integrity Level verification, the following assumptions have been made.

Mission Time:	10 years
Startup time:	24 hours

The SIF operates in Low demand mode.

Equipment Leg (each):	Rosemount 1199 Remote Seal (Sys. Cap.: 2/3) (My Own)
	Rosemount 3051C SIS Coplanar with SFB, SW Rev 3.0 (SC3)
	High trip
	Alarm Setting: Under Range
	Diagnostic Filtering: On, Alarm Filtering: Off
	Trip On Alarm: Off
β–factor:	- [%]
MTTR:	24 hours
Proof Test Interval:	12 months
Proof Test Coverage:	49 [%]
Maintenance Capability:	MCI 2 (Good – 90%)

Table 7 shows the reliability data used during the SIL verification of sensor group for 1 Remote Seal Transmitter High Trip.

Table 7: Reliability Data Sensor Group for 1 Remote Seal Transmitter High Trip

Component	Failure Rates [1/h]								Arch. Type
	Fail Low	Fail High	Fail Det.	DD	DU	SD	SU	Res.	
Each Leg									
Rosemount 3051C SIS Coplanar with SFB, SW Rev 3.0 [2007.3.06]	2.77E-07	6.20E-08	5.00E-07		7.30E-08			4.09E-07	B
Rosemount 1199 Remote Seal					7.60E-08				A
Total for combination of Rosemount 3051C with Rosemount 1199 Remote Seal	2.77E-07	6.20E-08	5.00E-07		1.49E-07			4.09E-07	B

1.9 Low Level Trip in Low Demand Differential Application Example

Configuration: 1oo1 Rosemount 3051C Differential Pressure transmitter with an 1199 remote seal in a low level trip service, operating in a severe process severity application.

Failure rates from the Rosemount 3051C coplanar pressure transmitter were added to the incremental failure rates for a low trip remote seal in severe service (Table 8). These numbers were obtained from the exSILentia SIL verification tool which accurately calculates PFDavg using discrete time Markov models.

exSILentia SILver results

Constraint	**Result**		**SIL 2 Requirement**	**SIL Achieved**
Sensor sub-system PFDavg	3.35E-03		PFDavg max. = 0.01	2
Sensor sub-system SIL Capability	Systematic Capability = SC3	exida IEC 61508 Certified	SC2	3
Sensor sub-system Architecture Constraints	HFT=0	Route 2_H Table	HFT=0	2

Sensor sub-system MTTFS: 323.6 years

In order to perform the PFDavg calculation part of the Safety Integrity Level verification, the following assumptions have been made.

Mission Time: 10 years
Startup time: 24 hours
The SIF operates in Low demand mode.
Equipment Leg (each): Rosemount 1199 Remote Seals (Sys. Cap.: 2/3) (My Own)
Rosemount 3051C SIS Coplanar with SFB, SW Rev 3.0 (SC3)
Low trip
Alarm Setting: Over Range
Diagnostic Filtering: On, Alarm Filtering: Off
Trip On Alarm: Off
β–factor: - [%]
MTTR: 24 hours
Proof Test Interval: 12 months
Proof Test Coverage: 55 [%]
Maintenance Capability: MCI 2 (Good - 90%)

Table 8 shows the reliability data used during the SIL verification of sensor group Example 2 Low Level Trip.

Table 8: Reliability Data Sensor Group Example 2 Low Level Trip

Component	Failure Rates [1/h]								Arch. Type
	Fail Low	Fail High	Fail Det.	DD	DU	SD	SU	Res.	
Each Leg									
Rosemount 3051C SIS Coplanar with SFB, SW Rev 3.0 [2007.3.06]	2.77E-07	6.20E-08	5.00E-07		7.30E-08			4.09E-07	B
Rosemount 1199 Remote Seal					7.50E-08		7.70E-08		A
Total for combination of Rosemount 3051C with Rosemount 1199 Remote Seal	2.77E-07	6.20E-08	5.00E-07		1.49E-07		7.70E-08	4.09E-07	B

1.10 High Level Trip in Low Demand Differential Application Example

Configuration: 1oo1 Rosemount 3051S Differential Pressure transmitter with an 1199 remote seal in a high level trip service, operating in a severe process severity application.

Failure rates from the Rosemount 3051S coplanar pressure transmitter were added to the incremental failure rates for a high trip remote seal in severe service (Table 9). These numbers were obtained from the exSILentia SIL verification tool which accurately calculates PFDavg using discrete time Markov models.

exSILentia SILver results

Constraint	Result		SIL 2 Requirement	SIL Achieved
Sensor sub-system PFDavg	3.66E-03		PFDavg max. = 0.01	2
Sensor sub-system SIL Capability	SIL 3 Capability	exida IEC 61508 Certified	SIL 2 Capable	3
Sensor sub-system Architecture Constraints	HFT=0	Route 2_H Table	HFT=0	2

Sensor sub-system MTTFS: 868 years

In order to perform the PFDavg calculation part of the Safety Integrity Level verification, the following assumptions have been made.

Mission Time: 10 years

Startup time: 24 hours

The SIF operates in Low demand mode.

Equipment Leg (each): Rosemount 1199 Remote Seals (Sys. Cap.: 2/3) (My Own)
Rosemount 3051C SIS Coplanar with SFB, SW Rev 3.0 (SC3)
High trip
Alarm Setting: Under Range
Diagnostic Filtering: On, Alarm Filtering: Off
Trip On Alarm: Off

β–factor: - [%]

MTTR:	24 hours
Proof Test Interval:	12 months
Proof Test Coverage:	53 [%]

Table 9 shows the reliability data used during the SIL verification of sensor group Example 3 High Level Trip.

Table 9: Reliability Data Sensor Group Example 3 High Level Trip

Component	Failure Rates [1/h]								Arch. Type
	Fail Low	Fail High	Fail Det.	DD	DU	SD	SU	Res.	
Each Leg									
Rosemount 3051C SIS Coplanar with SFB, SW Rev 3.0 [2007.3.06]	2.77E-07	6.20E-08	5.00E-07		7.30E-08			4.09E-07	B
Rosemount 1199 Remote Seal					8.30E-08		7.0E-08		A
Total for combination of Rosemount 3051C with Rosemount 1199 Remote Seal	2.77E-07	6.20E-08	5.00E-07		1.56E-07		7.0E-08	4.09E-07	B

2 Process and Roles

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety and availability with over 400 man-years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations, end-users, and manufacturers, *exida* is a global corporation with offices around the world. *exida* offers training, coaching, project oriented consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, 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

Emerson Rosemount	Original Equipment Manufacturer
exida consulting	Project leader of the technical recommendations developed in this report

2.3 Reference documents

The services delivered by *exida consulting* were performed based on the following standards and industry references in sections 2.3.1 and 2.3.2.

2.3.1 Industry Standards

Item	Identification	Description
N1	IEC 61508-2: ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.3.2 Documentation generated by *exida consulting*

Item	Identification	Description
R1	ROS 11/05-075 R001	Failure Modes, Effects and Diagnostic Analysis Remote Seal 1199
R2	ROS 12/05-020 R001	Combining Rosemount Type B Transmitters with Type A Remote Seals For Use in SIL 2 Applications
R3		White Paper, *Field Failure Data-The Good, Bad and Ugly*, exida, 2012. Available on www.exida.com

2.3.3 Tools

exSILentia Version 3.0.9.785

3 Terms and Definitions

HFT	Hardware Fault Tolerance
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System

4 Status of the document

4.1 Liability

exida consulting provides services and analyses based on methods advocated in international and national standards. *exida consulting* accepts no liability whatsoever for the correct and safe functioning of a plant or installation developed based on this analysis or for the correctness of the standards on which the general methods are based.

4.2 Releases

Version:	V1	
Revision:	R5	
Status:	Released	
Version History:	V0, R0:	First Internal Draft, July 25, 2012
	V0, R1:	Internal Draft Review, August 2, 2012
	V1, R1:	Internal Draft Review, W. Goble, September 20, 2012
	V1, R2:	Incorporate review feedback, W. Goble, December 3, 2012
	V1, R3:	Incorporate review feedback, W. Goble, March 22, 2013
	V1, R4:	Incorporate review feedback, W. Goble, March 25, 2013
	V1, R5:	Incorporate review feedback, T. Stewart, April 24, 2013
Author:	Hal Thomas	
Reviews:	Gregory Sauk, William Goble	

4.3 Future Enhancements

At request of client

4.4 Release Signatures

Harold W Thomas

Harold W Thomas, Partner, CFSE, PE

Gregory Sauk

Gregory Sauk, Senior Safety Engineer CFSE