



Final Element SIL Verification

Project:

SIL Verification for BM9/BM5/BM5A SSV and GSR Solenoid Assembly

Customer:

Emerson Process Management Regulator Technologies, Inc.
China

Contract Number: Q21/02-090

Report No.: ERD 21/02-090 R001

Version V1, Revision R1, March 22, 2021

Jack Gao



Management Summary

This report documents the results of the Final Element SIL Verification for the SSV Remote Control with Solenoid Valve project. The Final Element SIL Verification was performed by *exida* on behalf of Emerson Process Management Regulator Technologies, Inc.

Industry standards for SIS require that for each Safety Instrumented Function (SIF), a Safety Integrity Level (SIL) target is selected and achievement of that target is confirmed by quantitative analysis. The SIL represents the amount of risk reduction that is required to ensure a tolerable risk is achieved for each specific hazard that is safeguarded by a SIF. For each SIF, this is a function of the risk the process poses without considering the benefit of the SIS. In order to determine the amount of risk reduction that is achieved, the conceptual design of the SIF must be evaluated in a SIL verification. The SIL verification considers probability of failure, minimum redundancy, and SIL capability requirements that result from the target SIL for each SIF.

In some cases suppliers of final elements are asked to provide confirmation that the final element meets specific performance requirements. In these cases verification is performed on just a portion of the equipment in the SIF.

exida supported the Final Element SIL Verification process by performing the following tasks:

- Safety Integrity Level Verification on the final element

This analysis covers only the final element. To determine the performance of the SIF these results must be combined with the results for the sensor and logic elements.

exida in cooperation with Emerson Process Management Regulator Technologies, Inc. performed the SIL Verification to support the SSV Remote Control with Solenoid Valve. The SIL Verification calculation was performed to document the SIL level achieved by the final element(s).



Table 1 shows a summary of the SIL verification results. Details of the SIL verification process are presented in the exSILentia report in Appendix D.



Table 1 Final Element SIL Verification Summary

SIF Tag	SIF Name	Target		Achievable SIL Limits			RRF	Remarks
		SIL	RRF	PFDavg	AC	SC		
SIF-01	BM5/BM5A SSV (contained OS/8*X Series Controller) + GSR Type 75 Series Solenoid Valve	2	100	2	2	2 ¹	131.8	Comply
SIF-02	BM9 SSV (contained OS9/8*X Series Controller) + GSR Type 75 Series Solenoid Valve	2	100	2	2		120.2	Comply

Note: GSR Type 75 Series Solenoid Valve detail model refer to [D4]

¹ Due to the usage of non-certified GSR solenoid, the SIL Capability (SC) requirement in this analysis is only valid based on the assumption that the End User should undertake measures to monitor and gather evidence, or perform a “proven-in-use” assessment, that the probability of dangerous systematic or random faults occurring in the non-certified components is at sufficiently low level compared to the required safety integrity.



Table of Contents

1	Purpose and Scope	7
1.1	Background	7
1.2	Objectives and Scope	7
2	Project Management	8
2.1	<i>exida</i>	8
2.2	Project phases	8
2.3	Roles of the parties involved	8
2.4	Standards and literature used	8
2.5	Reference documents	9
2.5.1	Documentation provided by Emerson Process Management Regulator Technologies, Inc.	9
2.5.2	Documentation generated by <i>exida</i>	9
3	Final Element SIL Verification	10
3.1	Assumptions	10
3.2	Analysis Results	11
3.2.1	Architectural Constraints	11
3.2.2	SIL Capability	12
3.2.3	Probability of Failure on Demand	12
4	Conclusions and Recommendations	14
5	Terms and Definitions	15
6	Status of the Document	17
6.1	Liability	17
6.2	Version History	17
6.3	Future enhancements	17
6.4	Release signatures	17
Appendix A	SIL Verification Methodology	18
A.1	Overview	18
A.2	Modeling Assumptions	19
A.3	Data and Statistics	19
Appendix B	Proof Tests	21
B.1	Base SIF Modeled Proof Test	21
B.2	SIF with PVST Modeled Proof Test	21
B.3	Proof Test Coverage	21
Appendix C	Final Element Schematic	22
Appendix D	Detailed IEC 61511 Compliance Report	23
D.1	SIF-01 BM5/BM5A SSV (contained OS/8*X Series Controller) + GSR Type 75 Series Solenoid Valve	23



D.1.1 General SIF Information	23
D.1.2 Safety Integrity Levels	23
D.1.3 SIL Verification Parameters and Results	23
D.1.4 Final Element Part Configuration.....	24
D.1.4.1 Final Element Group 1: BM5/BM5A SSV (contained OS/8*X Series Controller) + GSR Type 75 Series Solenoid Valve	25
D.1.4.2 Final Element Leg 1-1: Final Element Leg.....	25
D.2 SIF-02 BM9 SSV (contained OS9/8*X Series Controller) + GSR Type 75 Series Solenoid Valve	26
D.2.1 General SIF Information	26
D.2.2 Safety Integrity Levels	26
D.2.3 SIL Verification Parameters and Results	27
D.2.4 Final Element Part Configuration.....	28
D.2.4.1 Final Element Group 1: BM9 SSV (contained OS9/8*X Series Controller) + GSR Type 75 Series Solenoid Valve	28
D.2.4.2 Final Element Leg 1-1: Final Element Leg.....	29



1 Purpose and Scope

This report documents the results of the Final Element SIL Verification for the SSV Remote Control with Solenoid Valve project. The Final Element SIL Verification was performed by exida on behalf of Emerson Process Management Regulator Technologies, Inc.

1.1 Background

The functional safety standards describing the implementation of SIS are based on the safety lifecycle. The safety lifecycle is a management system that will yield a functionally safe system if all steps are implemented properly. The IEC 61511 standard introduces the concept of Safety Integrity Level (SIL). SIL is a measure of the amount of risk reduction that a Safety Instrumented Function (SIF) is capable of providing, as defined by its average Probability of Failure on Demand (PFD_{AVG}) or Probability of Failure per Hour (PFH).

IEC 61511 requires that for each Safety Instrumented Function (SIF), a SIL target is selected and achievement of that target is confirmed by quantitative analysis. The required amount of risk reduction is a function of the unmitigated risk of the process, or the risk the process poses without considering the SIF. In order to determine the amount of risk reduction that is required, the process risk must be compared against guidelines for tolerable risk. The difference between the process risk and the tolerable risk is the required risk reduction capability for the SIF. In order to determine the amount of risk reduction that is achieved, the conceptual design of the SIF is evaluated during SIL verification where probability of failure, minimum redundancy, and SIL capability requirements are analyzed.

In some cases, suppliers of final elements are asked to provide confirmation that the final element meets specific performance requirements. In these cases, verification is performed on just a portion of the equipment in the SIF.

1.2 Objectives and Scope

The objective of this study is to verify, through quantitative analysis, the achieved SIL for the final element(s) identified in the SSV Remote Control with Solenoid Valve project. The SIL verification process yields estimates for average probability of failure on demand (PFD_{AVG}), SIL (with and without architectural constraints), achieved SIL Capability, and mean time to fail spuriously (MTTFS).

This report covers the quantitative aspects of the SIL verification only. Qualitative requirements as for software development are not addressed by the assessment described in this report.



2 Project Management

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 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project-oriented system 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 based on 250 billion hours of field failure data.

2.2 Project phases

This report, the Final Element SIL Verification for the SSV Remote Control with Solenoid Valve project, documents the results of the analysis performed by *exida* on behalf of Emerson Process Management Regulator Technologies, Inc.

exida performed the following tasks as part of this project:

- Safety Integrity Level Verification on the final element

2.3 Roles of the parties involved

Emerson Process Management Regulator Technologies, Inc. - Manufacturer of the BM9/BM5/BM5A SSV and the integrator of the SSV and GSR Solenoid assembly

exida - Project leader for the Final Element SIL Verification

2.4 Standards and literature used

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

[N1]	IEC 61508-2: 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	IEC 61511: 2016	Functional Safety: Safety Instrumented Systems for the Process Industry Sector
[N3]	Safety Equipment Reliability Handbook, 4 th Edition, 2015	<i>exida</i> LLC, Safety Equipment Reliability Handbook, Third Edition, 2015, ISBN-13: 9781-934977-15-6
[N4]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3 rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N5]	O'Brien, C. & Bredemeyer, L., 2009	<i>exida</i> LLC., Final Elements & the IEC 61508 and IEC Functional Safety Standards, 2009, ISBN 978-1-9934977-01-9



2.5 Reference documents

2.5.1 Documentation provided by Emerson Process Management Regulator Technologies, Inc.

[D1]	E-01-PDB-01, Rev 1, 2020.12	Drawing - SSV Remote Control With Solenoid Valve-Rev1
[D2]	808SIL2认证, 12.02.2014	Manufacturer Information
[D3]	44 100 141655, 2020-12-14	ISO 9001 Certificate
[D4]	GSR样本	GSR Type 75 Datasheet
[D5]	Erklärung_075.000423+K	Manufacturer Information
[D6]	Erklärung_075.000733_07 5.000593+K	Manufacturer Information
[D7]	Erklärung_075.000818_07 5.000675+K	Manufacturer Information

2.5.2 Documentation generated by *exida*

[R1]	Q21 02-090 Emerson SIL Verification.exi	exSILentia File
[R2]	ERD 10-12-069 R002 V4R1 BM5 FMEDA report, February 4, 2021	BM5/BM5A FMEDA report
[R3]	ERD 16-08-037 R001 V1R3 BM9 FMEDA report, January 8, 2020	BM9 FMEDA report
[R4]	ERD 21_02-090 R001 V1R1 SIL Verification Report Final Element, March 22, 2021	Final Element SIL Verification report for the Emerson Process Management Regulator Technologies, Inc. SSV Remote Control with Solenoid Valve project.

3 Final Element SIL Verification

Safety Integrity Level (SIL) is an order of magnitude classification of the effectiveness of a Safety Instrumented Function (SIF), as defined by a range of average Probability of Failure on Demand (PFD_{avg}). Table 2 shows the relationship between SIL, PFD_{AVG} , and Risk Reduction Factor (RRF), for the low demand mode of operation.

Table 2 Safety Integrity Levels and Associated Parameters (Low Demand Mode)

Safety Integrity Level	Average Probability of Failure on Demand (PFD_{avg})	Risk Reduction Factor (RRF)
3	10^{-3} to 10^{-4}	1,000 to 10,000
2	10^{-2} to 10^{-2}	100 to 1,000
1	10^{-1} to 10^{-2}	10 to 100

A SIL is assigned to each individual SIF and reflects the amount of risk reduction that is required to move the process risk from its existing level to a level that is considered tolerable. The objective of the SIL verification process is to verify that the equipment that has been selected for the SIF as part of the conceptual design, meets the requirements of the selected SIL, both in terms of PFD_{AVG} and architectural constraints.

3.1 Assumptions

Assumptions can be divided into general modeling assumptions and project specific assumptions. An overview of the general modeling assumptions is provided in Appendix A. Project specific assumptions are listed in this section.

- Based on the SIL selection, it is concluded that each SIFs demand interval is at least twice as long as the longest proof test interval, therefore it is determined that all Safety Instrumented Functions operate in low demand mode.
- The mission time is 10 years; therefore, all equipment will be replaced or refurbished every 10 years.
- The Startup time, the time it will take between a nuisance trip and restart of the unit, is 24 hours
- The Mean Time To Restoration (MTTR) is 24 hours on all equipment.
- The failure rates in [D5], [D6] and [D7] are Dangerous Undetected.
- It is assumed that all devices are implemented in accordance with their safety manuals.
- The proof test coverage (PTC) value is assumed based on standard proof test procedures for GSR solenoid, and its corresponding coverage, when available. Otherwise, generally acceptable values are used. The PTC has a significant impact on the PFD_{avg} calculation. It is recommended that proper proof test procedures be in place to justify the proof test coverage values used in this study, especially for final elements, since their performance most often limits the overall design performance.



- Maintenance will be performed to a good standard (Site Safety Index SSI = 2). During maintenance, 90% of detectable faults will be detected and corrected, and equipment will be reassembled correctly at least 90% of the time (this is a reasonable estimate based on typical industry data). This is indicated as “SSI (Site Safety Index) = 2” in the detailed analysis report.
- Generic SERH equipment data are used in the calculations where specific data is not available. This generic data is normally conservative but should be checked against “actual” equipment data, if and when such data becomes available.
- It is assumed that the only diagnostic capabilities implemented are application level diagnostics.
- The SILver SIL verification software tool used in this work (part of the exSILentia package) 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

3.2 Analysis Results

The results of the Final Element SIL Verification study is shown in Table 3.

Table 3 Final Element SIL Verification Summary

SIF Tag	SIF Name	Target		Achievable SIL Limits			RRF	Remarks
		SIL	RRF	PFDavg	AC	SC		
SIF-01	BM5/BM5A SSV (contained OS/8*X Series Controller) + GSR Type 75 Series Solenoid Valve	2	100	2	2	2 ²	131.8	Comply
SIF-02	BM9 SSV (contained OS9/8*X Series Controller) + GSR Type 75 Series Solenoid Valve	2	100	2	2		120.2	Comply

Note: GSR Type 75 Series Solenoid Valve detail model refer to [D4]

3.2.1 Architectural Constraints

The architecture meets the requirements for SIL 2 based on IEC 61511³.

² Due to the usage of non-certified GSR solenoid, the SIL Capability (SC) in this analysis is only valid based on the assumption that the End User should undertake measures to monitor and gather evidence or perform a “proven-in-use” assessment, that the probability of dangerous systematic or random faults occurring in the non-certified components is at sufficiently low level compared to the required safety integrity.

³ Hardware Fault Tolerance; for details see 11.4.5 of IEC 61511-1.

Table 4 IEC 61511 Architectural Constraints

Safety Integrity Level	Minimum Required Hardware Fault Tolerance
1 (any mode)	0
2 (low demand mode)	0
2 (continuous mode)	1
3 (high demand mode or continuous mode)	1
4 (any mode)	2

3.2.2 SIL Capability

Due to the usage of non-certified GSR solenoid, the SIL Capability (SC) 2 in this analysis is only valid based on the assumption that the End User should undertake measures to monitor and gather evidence or perform a “proven-in-use” assessment, that the probability of dangerous systematic or random faults occurring in the non-certified components is at sufficiently low level compared to the required safety integrity.

3.2.3 Probability of Failure on Demand

The hardware configuration for the SSV Remote Control with Solenoid Valve was listed in Table 5.

Table 5 Hardware Variations

SIF Tag	SIF Name	Diagnostic	Proof Test
SIF-01	BM5/BM5A SSV (contained OS/8*X Series Controller) + GSR Type 75 Series Solenoid Valve	None	Timed full valve stroke test and leak test
SIF-02	BM9 SSV (contained OS9/8*X Series Controller) + GSR Type 75 Series Solenoid Valve	None	Timed full valve stroke test and leak test

Note: GSR Type 75 Series Solenoid Valve detail model refer to [D4]

The PFD_{avg} was calculated for each SIF considering proof test intervals 12 months. The results are show in Figure 1 and Figure 2.

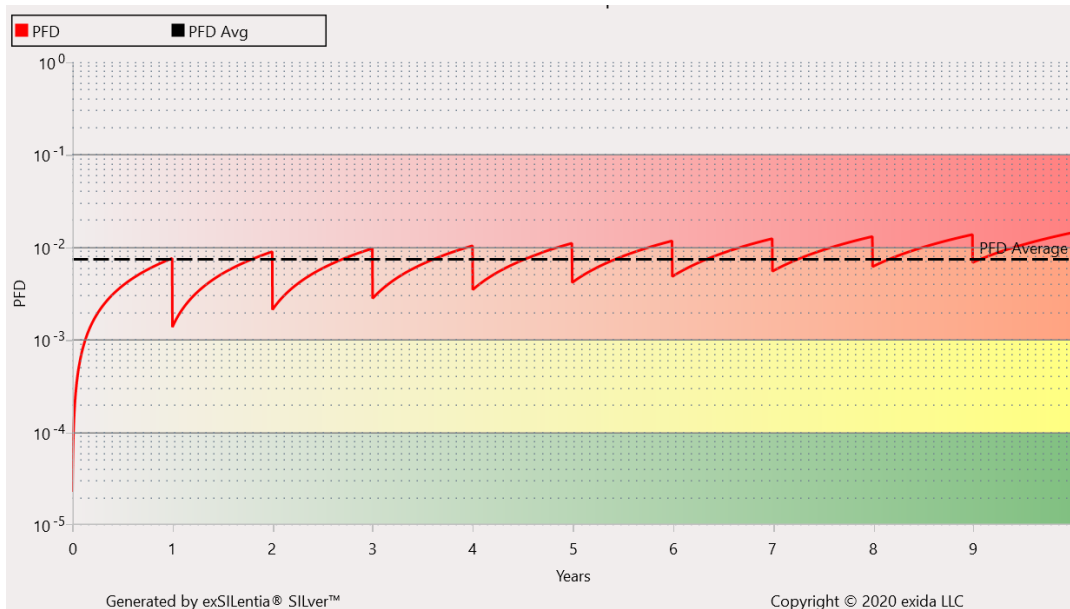


Figure 1 SIF-01 PFD_{avg} Proof Test Intervals 12 months

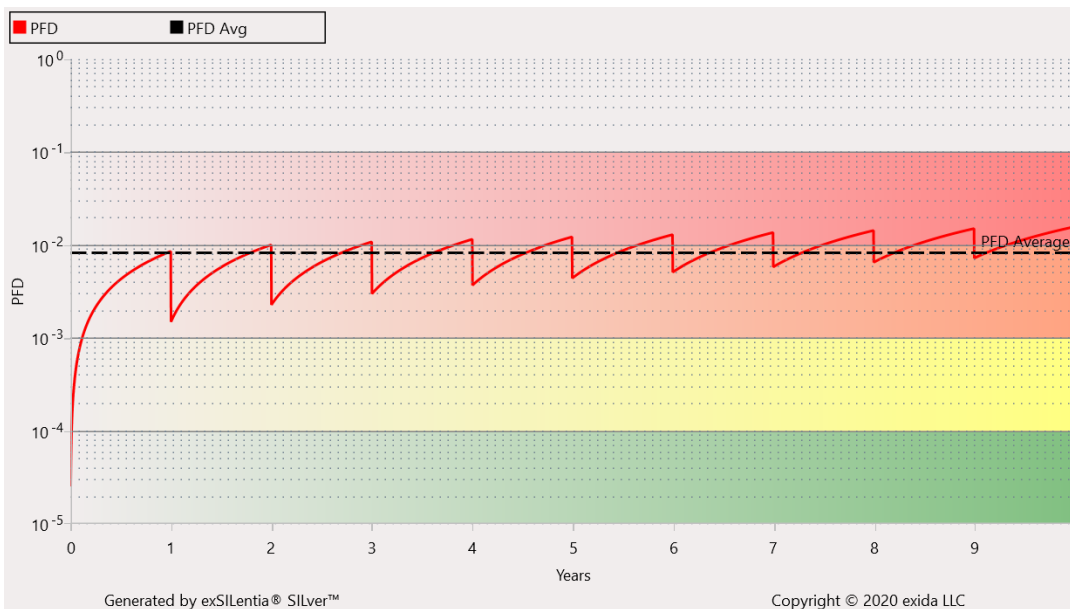


Figure 2 SIF-02 PFD_{avg} Proof Test Intervals 12 months



4 Conclusions and Recommendations

The results of the analysis show that the SSV Remote Control with Solenoid Valve meets the SIL 2. To achieve this proof testing and diagnostic need to be implemented as modeled in the SIL Verification calculations.

This analysis covers only the final element. To determine the performance of the SIF these results must be combined with the results for the sensor and logic elements.



5 Terms and Definitions

ALARP	As Low As Reasonably Practicable
Architectural Constraints	Limitations that are imposed on the hardware selected to implement a safety-instrumented function, regardless of the performance calculated for a subsystem. Architectural constraints are specified (in IEC 61508-2-Tables 2 and 3, and IEC 61511-Tables 5 and 6) according to the required SIL of the subsystem, type of components used, and SFF of the subsystem's components. Type A components are simple devices not incorporating microprocessors, and Type B devices are complex devices such as those incorporating microprocessors.
Availability	The probability that a device is operating successfully at a given moment in time. This is a measure of the "uptime" and is defined in units of percent.
BPCS	Basic Process Control System
Diagnostic Coverage	A measure of a system's ability to detect failures. This is a ratio between the failure rates for detected failures to the failure rate for all failures in the system.
FIT	Failure unit, 1 FIT = 1.00E-9 Failures / Hour
FMEDA	Failure Modes Effects and Diagnostic Analysis <i>A systematic procedure during which each failure mode of each component is examined to determine the effect of that failure on the system and whether that failure is detected by any automatic diagnostic function</i>
HFT	Hardware Fault Tolerance <i>The number of dangerous random failures tolerated by a system while still maintaining the ability to successfully perform the safety function</i>
IEC	International Electrotechnical Commission
MTTFS	Mean Time To Fail Spurious
PFD _{avg}	average Probability of Failure on Demand
PFH	Probability of Dangerous Failure per Hour
PLC	Programmable Logic Controller
PTC	Proof Test Coverage, the percentage failures that are detected during the servicing of equipment.
PTI	Proof Test Interval, the time interval between servicing of the equipment.
RRF	Risk Reduction Factor, the inverse of PFD _{avg}
SERH	Safety Equipment Reliability Handbook

SFF	<p>Safe Failure Fraction</p> <p><i>A measure of safety integrity defined by IEC 61508-2 consisting of the ratio of safe random failures plus dangerous detected random failures divided by all total random failures. It is used to determine minimum levels of hardware fault tolerance (redundancy for safety).</i></p>
SIF	<p>Safety Instrumented Function</p>
SIL	<p>Safety Integrity Level</p> <p><i>Discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the electronic / programmable electronic safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest [IEC 61508-4]</i></p> <p><i>Note – there is an analogy between the SIL of IEC 61508 and the Class / Category of IEC 61513 / IEC 62128 based on a comparison of requirements.</i></p>
SIS	<p>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).</p>
SRS	<p>Safety Requirements Specification</p>
TI	<p>Test Interval, used in risk analysis equations to represent the proof test interval described above</p>



6 Status of the Document

6.1 Liability

exida provides services and analyses based on methods advocated in international and national standards. Input information for the Final Element SIL Verification is obtained from the customer / owner / operator, i.e. Emerson Process Management Regulator Technologies, Inc. *exida* accepts no liability whatsoever for the correct and safe functioning of a plant or installation developed based on this Final Element SIL Verification analysis or for the correctness of the standards on which the general methods are based.

6.2 Version History

Contract Number	Report Number	Revision Notes
Q21/02-090	ERD 21/02-090 R001 V1, R1	Initial

Reviewer: Desmond Lee, *exida*, March 15, 2021

Status: Released, March 22, 2021

6.3 Future enhancements

None are foreseen

6.4 Release signatures

Jack Gao, Senior Safety Engineer

Desmond Lee, CFSE, Senior Safety Engineer



Appendix A SIL Verification Methodology

This appendix will provide an overview of the SIL verification methodology that was applied during the Final Element SIL Verification study.

A.1 Overview

National and International standards that describe the implementation of automated systems for safety related purposes, including IEC 61508, and IEC 61511 present the safety lifecycle model, which is a management system for implementing Safety Instrumented Systems (SIS). These standards define either three or four Safety Integrity Levels (SIL) that represents the effectiveness of each Safety Instrumented Function (SIF). SIL are categories of the average Probability of Failure on Demand (PFD_{AVG}). Table 6 shows categories of SIL and the performance parameters that are related to those categories, including PFD_{AVG} and Risk Reduction Factor (RRF), which is the inverse of PFD_{AVG} , for the low demand mode of operation.

Table 6 Safety Integrity Levels and Associated Parameters (Low Demand Mode)

Safety Integrity Level	Average Probability of Failure on Demand (PFD_{avg})	Risk Reduction Factor (RRF)
3	10^{-3} to 10^{-4}	1,000 to 10,000
2	10^{-2} to 10^{-2}	100 to 1,000
1	10^{-1} to 10^{-2}	10 to 100

The requirements that are defined for a SIS specify both design features (hardware, software, redundancy, etc.) and operational philosophy (inspection maintenance policy, frequency and quality of testing, etc.). These attributes of a SIS, as described above, will determine how that system will function. An important part of the safety lifecycle includes quantitatively describing the effectiveness of each SIF. SIF performance is usually described by the metrics of PFD_{AVG} and Mean Time To Fail Spurious (MTTFS).

SIF performance metrics can be estimated using the historical system performance data of the individual components that comprise a SIF. A number of techniques that estimate the performance metrics based on the performance of the components that comprise a system and a description of how they are logically related have been employed for the task of SIS analysis. Collectively, these techniques are called “fault propagation models”. Some of the most commonly used fault propagation models include fault tree analysis, event tree analysis, reliability block diagrams, and Markov models.

While PFD_{AVG} is the key variable that SIS designers are concerned with, safe failures must also be considered. The safe failures are alternately referred to as nuisance trips, or spurious trips. Safe failures are typically described by the Mean Time To Fail Spurious (MTTFS) metric. Spurious trips can adversely impact the safety of a process in number of ways. Process start-up and shutdown are typically higher risk time periods than normal operation; thus, unnecessarily increasing the number of startups will often have a detrimental effect on safety. In some cases, the nuisance shutdown itself may cause hazards, such as hydraulic hammer of pipe work, that are as great as the hazard that the SIF is protecting against. As a result, reducing the number of spurious trips often increases the safety of the process. Spurious trips may also cause financial losses due to



decreased productivity, lost batches, and decreased product quality. Increasing acceptable MTTFS requirements can often be justified because of the high cost associated with a spurious trip.

A.2 Modeling Assumptions

While performing Final Element SIL Verification study, the following assumptions about the SIS and SIFs under consideration were made when modeling its performance.

- The SIF being evaluated is designed, installed, and maintained in accordance with all applicable national and international standards regarding SIF at a level of Site Safety Index (SSI)=2. Reference: <http://www.exida.com/Resources/Whitepapers/quantifying-the-impacts-of-human-factors-on-functional-safety>
- The failure rate of components is assumed to be constant over the life of the system.
- It is generally assumed that the failure of an individual component is statistically independent of the failure of other components. All failure events are independent events.
- The failed state and the operating state are mutually exclusive; a component must be either completely failed or completely operational at all points in time.
- Once a component has failed, it remains in the failed state until repaired.
- Unless specifically noted otherwise, all repairs will return a component to its original failure-free state.
- Testing frequencies are assumed to be much higher than failure rates.

A.3 Data and Statistics

The analysis presented in this report depends, to a substantial degree, on the reliability and failure data that was used to calculate the various SIF performance parameters. The data needed for a component is usually presented in terms of four variables: failure rate (λ), percentage safe failures, diagnostic coverage of safe failures (Cs), and diagnostic coverage of dangerous failures (Cd), or in terms of failure rates for each mode. Using these component performance parameters and information about system maintenance and testing, the PFD_{AVG} and MTTFS are calculated.

Collection, analysis and presentation of this data are important parts of the analysis process. Quantification of equipment failure rates depends on historical information regarding how events that cause or propagate an accident have occurred in the past. The best source of failure rate data is records of failures and maintenance of equipment that exist in the process plant that is being studied. This information is best because the failure rate describes the actual conditions under which the process equipment is being used. Unfortunately, historical reliability data is often unavailable.

In cases where company specific data is unavailable or incomplete, industry average data has been used. exida has compiled a proprietary equipment failure database. The database is a compilation of failure data collected from a variety of public and confidential sources. exida has selected the most appropriate data from the various sources and combined them on a consistent basis for many types of process equipment and services. Basic event frequencies used in this study are included at the end of the appendices that contain detailed calculation information.



exida recognizes that some data provides a more accurate representation of failure rates than others. The following priority is given to the various data sources that might be available for an equipment item.

1. Results of FMEDA analysis that is integral in the certification report presented by an accredited independent third-party organization when results are within statistical confidence limits of process industry field failure data.
2. Results of FMEDA analysis performed by generally accepted practices, using generally accepted and comparable databases of component reliability. Prior to use of this type of data exida would review and approve of the analysis process and data. NOTE: exida typically does not use MTTF data published by equipment vendors that was determined on the basis of field returns, as that data is often misleading. In the case of this analysis some of the failure rate data was provided by the equipment manufacturer.
3. Compilation of published and proprietary failure rates for instruments used in the process industries.

The exida reliability database is published in the "Safety Equipment Reliability Handbook". 4th Edition (ISBN-13: 9781-934977-15-6).

Appendix B Proof Tests

According to section 7.4.5.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by automatic diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof testing.

B.1 Base SIF Modeled Proof Test

The SIL Verification analysis modeled a timed full valve stroke test and leak test as the proof test. The proof test at the final element level is outlined in Table 7. Refer to the table in B.3 for the Proof Test Coverages.

Table 7 Base SIF Modeled Proof Test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	De-energize the solenoid valve, measure and record the time required for the valve assembly to move to the fully closed position. Confirm that the Safe State was achieved and within the correct time.
3.	Perform a leak test across the valve. Confirm that the leak test was successful.
4.	Re-energize the solenoid. Inspect the valve assembly for any leaks, visible damage or contamination and confirm that the normal operating state was achieved.
5.	Remove the bypass and otherwise restore normal operation.

B.2 SIF with PVST Modeled Proof Test

The SIL Verification analysis modeled a timed full valve stroke test and leak test as the proof test. The proof test at the final element level is outlined in Table 7. In addition to the proof test the SIL Verification modeled a PVST as an application diagnostic. Refer to the table in B.3 for the Proof Test Coverages. The PVST should be implemented in the safety system logic solver and should momentarily de-energize the solenoid and confirm that the valve assembly begins to move and closes the required amount (typically 5% to 10% of travel) within that required time. If the test fails the failure must automatically be annunciated.

B.3 Proof Test Coverage

The Proof Test Coverage for the SIFs is given in Table 8.

Table 8 Proof Test Results – SSV Remote Control with Solenoid Valve

Safety Function	Proof Test Coverage
SIF-01	91%
SIF-02	92%

Appendix C Final Element Schematic

Figure 3 shows the schematic of the SSV Remote Control with Solenoid Valve.

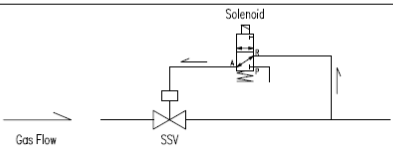
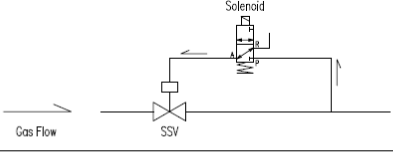
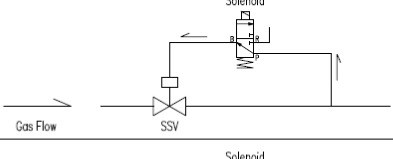
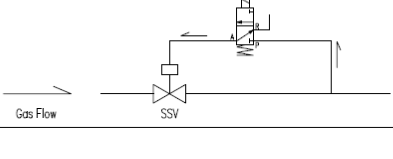
SN	PRESSURE	TYPE	DESCRIPTION	DIAGRAM																				
1	0~2MPa	Universal(UN)	<ul style="list-style-type: none"> • When SSV is open, solenoid valve is de-energized. • When solenoid valve energized, SSV shut off immediately. 																					
2			<ul style="list-style-type: none"> • When SSV is open, solenoid valve is energized. • When solenoid valve de-energized, SSV shut off immediately. 																					
3	0~7.5MPa	Normal Open(NO)	<ul style="list-style-type: none"> • When SSV is open, solenoid valve is de-energized. • When solenoid valve energized, SSV shut off immediately. 																					
4		Normal Close(NC)	<ul style="list-style-type: none"> • When SSV is open, solenoid valve is energized. • When solenoid valve de-energized, SSV shut off immediately. 																					
<p>NOTE : THIS DOCUMENT/DRAWING CONTAINS INFORMATION OF PROPRIETARY NATURE AND IS REPRODUCED OR DISCLOSED OR REPRODUCED IN WHOLE OR IN PART WITHOUT WRITTEN CONSENT FROM FUKUI-JEOM GAS EQUIPMENT (CHINA) CO., LTD.</p>																								
<table border="1"> <tr> <td>EMERSON.</td> <td>CUSTOMER :</td> <td>---</td> <td>MODEL/OPS NO.:</td> <td>---</td> </tr> <tr> <td></td> <td>PROJECT :</td> <td>---</td> <td>DWG. NO.:</td> <td>E-01-PDB-01</td> </tr> <tr> <td></td> <td>DWG. TITLE :</td> <td colspan="2">SSV Remote Control With Solenoid Valve</td> <td>PAGE:</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td>XX of XX</td> </tr> </table>					EMERSON.	CUSTOMER :	---	MODEL/OPS NO.:	---		PROJECT :	---	DWG. NO.:	E-01-PDB-01		DWG. TITLE :	SSV Remote Control With Solenoid Valve		PAGE:					XX of XX
EMERSON.	CUSTOMER :	---	MODEL/OPS NO.:	---																				
	PROJECT :	---	DWG. NO.:	E-01-PDB-01																				
	DWG. TITLE :	SSV Remote Control With Solenoid Valve		PAGE:																				
				XX of XX																				
<table border="1"> <thead> <tr> <th>REV</th> <th>DATE</th> <th>DESCRIPTION</th> <th>PREPARED</th> <th>CHECKED</th> <th>APPROVED</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>2021.12</td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>					REV	DATE	DESCRIPTION	PREPARED	CHECKED	APPROVED	1	2021.12												
REV	DATE	DESCRIPTION	PREPARED	CHECKED	APPROVED																			
1	2021.12																							

Figure 3 SSV Remote Control with Solenoid Valve Schematic



Appendix D Detailed IEC 61511 Compliance Report

The subsequent pages in this appendix provide a detailed overview of the SIL verification results for the SSV Remote Control with Solenoid Valve project. The SIL verification was performed using the exida exSILentia® SILver tool.

D.1 SIF-01 BM5/BM5A SSV (contained OS/8*X Series Controller) + GSR Type 75 Series Solenoid Valve

This chapter details the SIL Verification results, selections, and assumptions for the SIF-01 BM5/BM5A SSV (contained OS/8*X Series Controller) + GSR Type 75 Series Solenoid Valve Safety Instrumented Function.

D.1.1 General SIF Information

The following characterizes the Safety Instrumented Function.

SIF Name: BM5/BM5A SSV (contained OS/8*X Series Controller) + GSR Type 75 Series Solenoid Valve
SIF Tag: SIF-01
SIF Description: When solenoid valve de-energized, SSV shut off immediately

D.1.2 Safety Integrity Levels

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

SIL 2 with RRF ≥ 100

The calculated achieved Safety Integrity Level for this Safety Instrumented Function is:

SIL 2⁴ with RRF = 131.8

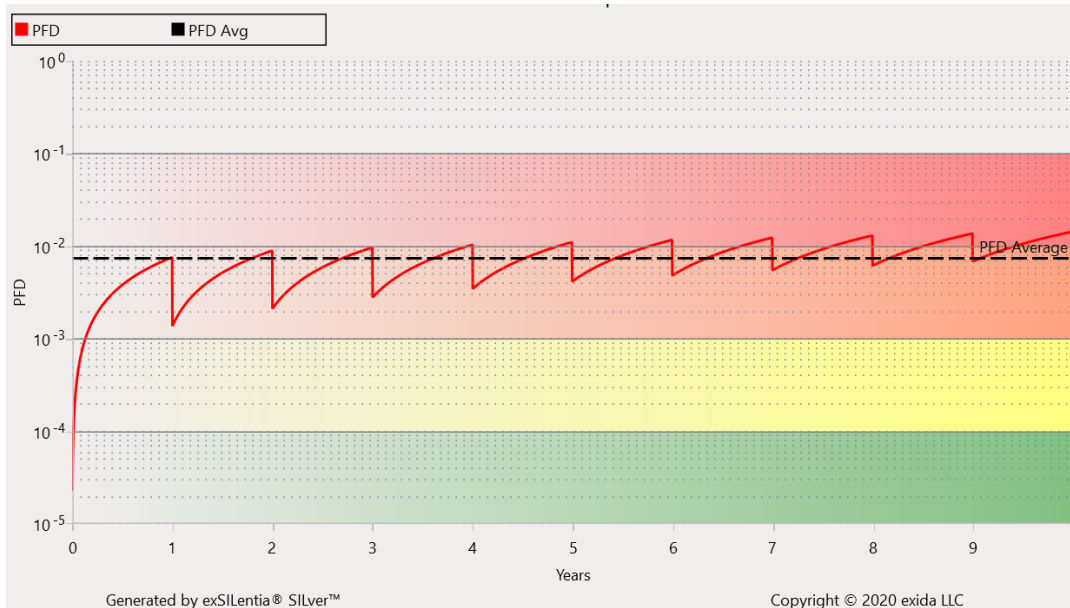
D.1.3 SIL Verification Parameters and Results

This section provides a detailed overview of the Safety Integrity Level verification performed for the SIF-01 BM5/BM5A SSV (contained OS/8*X Series Controller) + GSR Type 75 Series Solenoid Valve Safety Instrumented Function. In order to perform the reliability calculations part of the Safety Integrity Level verification, the following assumptions have been made.

Analysis Date: 12 March 2021
Mission Time: 10 years
Startup Time: 24 hours
Demand Mode: Low
Architectural Constraints: IEC 61511
Consider Systematic: Yes
Capability:
Consider MTTFS: Yes
Site Safety Index: SSI 2

⁴ Due to the usage of non-certified GSR solenoid, the SIL Capability (SC) in this analysis is only valid based on the following assumption that the End User should undertake measures to monitor and gather evidence or perform a “proven-in-use” assessment, that the probability of dangerous systematic or random faults occurring in the non-certified components is at sufficiently low level compared to the required safety integrity.

Include SSI in Failure Rate Yes



Given the reliability data and SIL verification selections and assumptions described in the subsequent subsections in this report the SIF-01 BM5/BM5A SSV (contained OS/8*X Series Controller) + GSR Type 75 Series Solenoid Valve Safety Instrumented Function achieves the functional safety performance as displayed in the following table.

Table 9 SIL Verification Results

PFD _{AVG}	RRF	ACHIEVED SIL			MTTFS (YEARS)
		PFD _{AVG}	ARCH. CONSTRAINTS IEC 61511	SYSTEMATIC CAPABILITY	
7.59E-03	131.8	2	2	2 ⁵	170.72

D.1.4 Final Element Part Configuration

The functional safety and spurious trip behavior of the final element part of the SIF-01 BM5/BM5A SSV (contained OS/8*X Series Controller) + GSR Type 75 Series Solenoid Valve Safety Instrumented Function is quantified as follows.

⁵ Due to the usage of non-certified GSR solenoid, the SIL Capability (SC) in this analysis is only valid based on the following assumption that the End User should undertake measures to monitor and gather evidence, or perform a “proven-in-use” assessment, that the probability of dangerous systematic or random faults occurring in the non-certified components is at sufficiently low level compared to the required safety integrity.

Table 10 Final Element Part SIL Verification Results

PFD _{AVG}	SIL LIMITS		MTTFS (YEARS)	HFT	SSI
	ARCH. CONSTRAINTS IEC 61511	SYSTEMATIC CAPABILITY			
7.59E-03	2	2 ⁶	170.72	0	2

Number of Final Element group(s): 1
 Voting between groups: 1oo1
 β-factor [%]: N/A

D.1.4.1 Final Element Group 1: BM5/BM5A SSV (contained OS/8*X Series Controller) + GSR Type 75 Series Solenoid Valve

The information and reliability data underneath describe the BM5/BM5A SSV (contained OS/8*X Series Controller) + GSR Type 75 Series Solenoid Valve final element group as it has been analyzed in this Safety Integrity Level verification.

Group Name: BM5/BM5A SSV (contained OS/8*X Series Controller) + GSR Type 75 Series Solenoid Valve
 Final Element Legs: Final Element Leg
 Voting within group: 1oo1
 Voting type: Identical
 HFT: 0
 β-factor [%]: N/A
 MRT [Hours]: 24
 Proof Test Interval [Months]: 12
 Proof Test Coverage [%]: 91
 Proof Test Execution: Leak Test; Offline

D.1.4.2 Final Element Leg 1-1: Final Element Leg

The following table shows the equipment that defines final element leg 1-1 Final Element Leg.

Table 11 Final Element Leg 1-1: Final Element Leg Details

FINAL ELEMENT LEG 1-1	SERH VERSION	2 _H	PIU	AC TYPE	SIL CAP
GSR Solenoid		-	-	A	-
Diaphragm Controllers - UPSO		✓	-	A	3
BM5/5A SSV		✓	-	A	3

⁶ Due to the usage of non-certified GSR solenoid, the SIL Capability (SC) in this analysis is only valid based on the following assumption that the End User should undertake measures to monitor and gather evidence, or perform a “proven-in-use” assessment, that the probability of dangerous systematic or random faults occurring in the non-certified components is at sufficiently low level compared to the required safety integrity.



Valve Open On Trip: No
 Tight Shutoff Required: No
 Severe Service: No

The Reliability Data table shows the reliability data used during the SIL verification of final element leg 1-1 Final Element Leg.

Table 12 Reliability Data Final Element Leg 1-1 Final Element Leg

COMPONENT	FAILURE RATES [1/HR]							
	SD	SU	DD	DU	AD	AU	NE	
GSR Solenoid	-	-	-	3.35E-07	-	-	-	
Diaphragm Controllers - UPSO	-	1.56E-07	-	1.15E-07	-	-	-	
BM5/5A SSV	-	2.00E-08	-	4.30E-07	-	-	-	
							SFF [%]	16.7
							ROUTE 2 _H COMPLIANT	-

D.2 SIF-02 BM9 SSV (contained OS9/8*X Series Controller) + GSR Type 75 Series Solenoid Valve

This chapter details the SIL Verification results, selections, and assumptions for the SIF-02 BM9 SSV (contained OS9/8*X Series Controller) + GSR Type 75 Series Solenoid Valve Safety Instrumented Function.

D.2.1 General SIF Information

The following characterizes the Safety Instrumented Function.

SIF Name: BM9 SSV (contained OS9/8*X Series Controller) + GSR Type 75 Series Solenoid Valve
 SIF Tag: SIF-02
 SIF Description: When solenoid valve de-energized, SSV shut off immediately

D.2.2 Safety Integrity Levels

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

SIL 2 with RRF \geq 100

The calculated achieved Safety Integrity Level for this Safety Instrumented Function is:

SIL 2⁷ with RRF = 120.2

⁷ Due to the usage of non-certified GSR solenoid, the SIL Capability (SC) in this analysis is only valid based on the following assumption that the End User should undertake measures to monitor and gather evidence or perform a “proven-in-use” assessment, that the probability of dangerous systematic or random faults occurring in the non-certified components is at sufficiently low level compared to the required safety integrity.

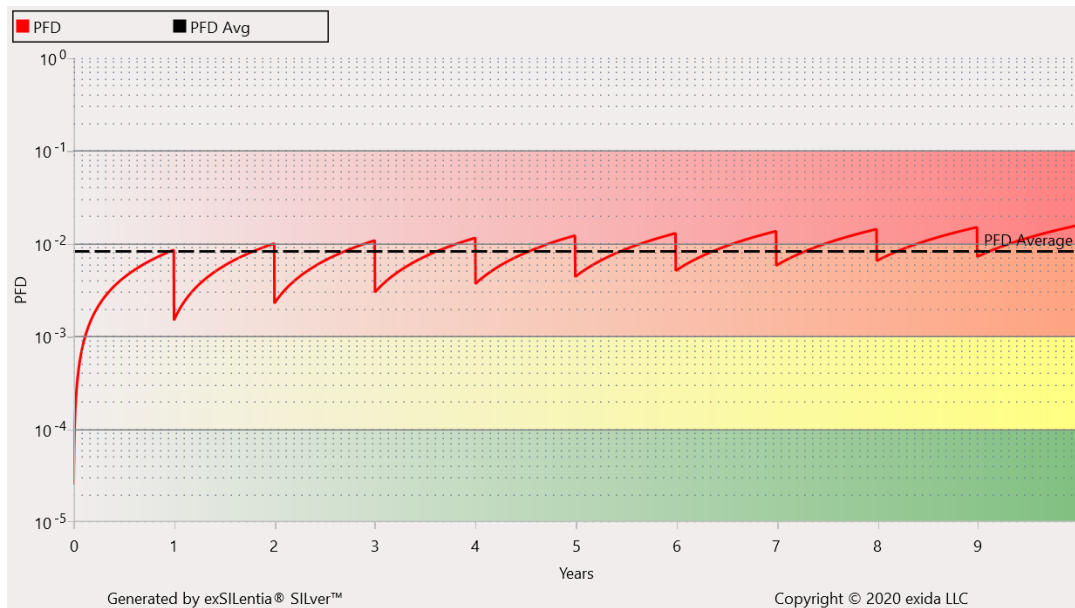


D.2.3 SIL Verification Parameters and Results

This section provides a detailed overview of the Safety Integrity Level verification performed for the SIF-02 BM9 SSV (contained OS9/8*X Series Controller) + GSR Type 75 Series Solenoid Valve Safety Instrumented Function. In order to perform the reliability calculations part of the Safety Integrity Level verification, the following assumptions have been made.

Analyst:

Analysis Date:	12 March 2021
Mission Time:	10 years
Startup Time:	24 hours
Demand Mode:	Low
Architectural Constraints:	IEC 61511
Consider Systematic	Yes
Capability:	
Consider MTTFS:	Yes
Site Safety Index:	Final Elements: SSI 2
Include SSI in Failure Rate	Yes



Given the reliability data and SIL verification selections and assumptions described in the subsequent subsections in this report the SIF-02 BM9 SSV (contained OS9/8*X Series Controller) + GSR Type 75 Series Solenoid Valve Safety Instrumented Function achieves the functional safety performance as displayed in the following table.



Table 13 SIL Verification Results

PFD _{AVG}	RRF	ACHIEVED SIL			MTTFS (YEARS)
		PFD _{AVG}	ARCH. CONSTRAINTS IEC 61511	SYSTEMATIC CAPABILITY	
8.31E-03	120.2	2	2	2 ⁸	159.92

D.2.4 Final Element Part Configuration

The functional safety and spurious trip behavior of the final element part of the SIF-02 BM9 SSV (contained OS9/8*X Series Controller) + GSR Type 75 Series Solenoid Valve Safety Instrumented Function is quantified as follows.

Table 14 Final Element Part SIL Verification Results

PFD _{AVG}	SIL LIMITS		MTTFS (YEARS)	HFT	SSI
	ARCH. CONSTRAINTS IEC 61511	SYSTEMATIC CAPABILITY			
8.31E-03	2	2 ⁹	159.92	0	2

Number of Final Element group(s): 1
 Voting between groups: 1oo1
 β-factor [%]: N/A

D.2.4.1 Final Element Group 1: BM9 SSV (contained OS9/8*X Series Controller) + GSR Type 75 Series Solenoid Valve

The information and reliability data underneath describe the BM9 SSV (contained OS9/8*X Series Controller) + GSR Type 75 Series Solenoid Valve final element group as it has been analyzed in this Safety Integrity Level verification.

Group Name: BM9 SSV (contained OS9/8*X Series Controller) + GSR Type 75 Series Solenoid Valve
 Final Element Legs: Final Element Leg
 Voting within group: 1oo1
 Voting type: Identical
 HFT: 0

⁸ Due to the usage of non-certified GSR solenoid, the SIL Capability (SC) in this analysis is only valid based on the following assumption that the End User should undertake measures to monitor and gather evidence or perform a “proven-in-use” assessment, that the probability of dangerous systematic or random faults occurring in the non-certified components is at sufficiently low level compared to the required safety integrity.

⁹ Due to the usage of non-certified GSR solenoid, the SIL Capability (SC) in this analysis is only valid based on the following assumption that the End User should undertake measures to monitor and gather evidence, or perform a “proven-in-use” assessment, that the probability of dangerous systematic or random faults occurring in the non-certified components is at sufficiently low level compared to the required safety integrity.



β -factor [%]: N/A
 MRT [Hours]: 24
 Proof Test Interval [Months]: 12
 Proof Test Coverage [%]: 92
 Proof Test Execution: Leak Test; Offline

D.2.4.2 Final Element Leg 1-1: Final Element Leg

The following table shows the equipment that defines final element leg 1-1 Final Element Leg.

Table 15 Final Element Leg 1-1: Final Element Leg Details

FINAL ELEMENT LEG 1-1	SERH VERSION	2 _H	PIU	AC TYPE	SIL CAP
GSR Solenoid		-	-	A	-
Diaphragm Controllers - UPSO		✓	-	A	3
BM9 SSV		✓	-	A	3

Valve Open On Trip: No
 Tight Shutoff Required: No
 Severe Service: No

The Reliability Data table shows the reliability data used during the SIL verification of final element leg 1-1 Final Element Leg.

Table 16 Reliability Data Final Element Leg 1-1 Final Element Leg

COMPONENT	FAILURE RATES [1/HR]						
	SD	SU	DD	DU	AD	AU	NE
GSR Solenoid	-	-	-	3.35E-07	-	-	-
Diaphragm Controllers - UPSO	-	1.56E-07	-	1.15E-07	-	-	-
BM9 SSV	-	6.60E-08	-	5.42E-07	-	-	-
						SFF [%]	18.3
						ROUTE 2 _H COMPLIANT	-