

OWNER

Safety Integrity Level Verification

Calculation



Document No.: [REDACTED] SAF-CAL-001

Rev. A, Issued for Review

Date: September 29, 2026

Project: [REDACTED] [REDACTED]



TORUS

[REDACTED], [REDACTED] County, [REDACTED]

ISSUE SUMMARY AND APPROVAL

This page records each issue of SAF-CAL-001. The preparer, reviewer and approver sign for each revision.

Rev.	Date	Issue purpose	Description
A	2026-09-29	Issued for Review	First issue

Contributors

Rev.	Discipline	Prepared by	Reviewed by	Approved by
A	Process Safety			

CONTENTS

1.	OBJECTIVE.....	1
2.	METHODOLOGY	1
3.	DESIGN INPUTS.....	1
4.	ASSUMPTIONS.....	3
5.	REFERENCES	4
6.	CALCULATION.....	4
	6.1. EQUATIONS.....	4
	6.2. SIF-01, OVERPRESSURE SHUTDOWN.....	5
	6.3. OTHER FUNCTIONS	8
	6.4. INDEPENDENT CHECK.....	9
7.	RESULTS AND CONCLUSIONS	9

FIGURES AND TABLES

Figure 6-1. SIF-01 PFDavg Against Full Proof-Test Interval	7
Figure 7-1. Required and Achieved Risk Reduction by SIF.....	10
Table 3-1: Required Risk Reduction	2
Table 3-2: Device Failure Data (typical, HOLD H-15).....	2
Table 3-3: Test, Repair and Common Cause Parameters	3

Table 6-1: SIF-01 Sensitivity 7

Table 6-2: SIF-01 Spurious Trip Rate.....8

Table 6-3: Independent Check of PFDavg 9

Table 7-1: SIL Verification Summary, Selected Designs.....9

1. OBJECTIVE

This calculation verifies that each safety instrumented function (SIF) at the achieves the risk reduction that the layer of protection analysis, SAF-RPT-002, requires of it. For each SIF it determines the average probability of failure on demand (PFD_{avg}), the risk reduction factor (RRF), the hardware fault tolerance against the IEC 61511 minimum, and, for the overpressure shutdown function, the spurious trip rate. It also sets the proof-test and partial-stroke intervals that the Safety Requirements Specification, SAF-SRS-001, carries into operation.

2. METHODOLOGY

TORUS divided each SIF into its sensor, logic solver and final element subsystems and calculated the PFD_{avg} of each with the simplified low-demand equations of IEC 61508-6 Annex B and ISA-TR84.00.02. The SIF PFD_{avg} is the sum of the subsystem values, and the RRF is its reciprocal.

Three refinements were included because each one changes the answer for the governing function. First, proof testing is taken as imperfect: only the fraction PTC of dangerous undetected failures is revealed at the proof test, and the remainder stays hidden until the device is overhauled or replaced at the end of its mission time. Second, common cause failure of redundant devices is represented by the factor β . Third, where the shutdown valve is partial-stroke tested, the fraction of its dangerous undetected failures that the partial stroke reveals is taken as tested at the partial-stroke interval rather than at the full proof test.

Hardware fault tolerance was checked against IEC 61511-1:2016 clause 11.4, Table 6. The spurious trip rate of SIF-01 was calculated from the safe and detected-dangerous failure rates of each subsystem, because a spurious closure of SDV-102 interrupts custody delivery to the receiving pipeline.

All failure rates are generic values typical of the certified product classes and published data. They will be replaced by the selected vendors' certified values when those are received (HOLD H-15), and the calculation reissued.

The governing results were re-derived independently from the IEC 61508-6 Annex B.3.2.2 equations, including the mean restoration time terms that the simplified equations omit. The two methods agree within 3 % for every SIF (Section 6.4).

3. DESIGN INPUTS

The required risk reduction for each function, taken from the LOPA, is listed in Table 3-1.

Table 3-1: Required Risk Reduction

SIF	Function	P&ID interlock	Required	Target PFD_{avg}
SIF-01	PT-133A/B/C 2oo3, safety PLC, SDV-102	I-02	SIL 2, RRF 110	0.0091
SIF-02	LSHH-105, safety PLC, SDV-101	I-03	SIL 1, RRF 55	0.018
SIF-03	LSLL-106, safety PLC, SDV-106	I-04	SIL 1, RRF 60	0.017
SIF-04	LSHH-192, safety PLC, SDV-106	I-05	No SIL	-
SIF-05	BE-153A/B, BMS-150, XV-150A/B	I-06	SIL 2, RRF 850	0.0012
SIF-06	LSL-154, BMS-150, XV-150A/B	I-06	SIL 1, RRF 10	0.10
SIF-07	TSHH-155, BMS-150, XV-150A/B	I-06	No SIL	-

Source: SAF-RPT-002, Layer of Protection Analysis.

The failure data used for each device class are listed in Table 3-2. Rates are per hour. The values are typical of IEC 61508 certified products in each class and of published handbook data; they are not vendor values.

Table 3-2: Device Failure Data (typical, HOLD H-15)

Device class	Used for	λ_{DU}	λ_{DD}	λ_S	PTC
Smart pressure transmitter, SIL 2 capable	PT-133A/B/C	4.0E-08	3.0E-07	1.0E-07	0.95
Vibrating fork level switch	LSHH-105, LSLL-106, LSHH-192	1.5E-07	1.0E-07	2.0E-07	0.90
Bath level switch (heater vendor)	LSL-154	3.0E-07	0	3.0E-07	0.90
Temperature switch, manual reset	TSHH-155	3.0E-07	0	3.0E-07	0.90
Flame rod or self-checking UV scanner	BE-153A, BE-153B	2.0E-07	8.0E-07	5.0E-07	0.95
Safety PLC, SIL 3 certified, one channel path	CP-102B	2.0E-08	5.0E-07	1.0E-06	0.99
BMS logic solver, SIL 2 certified	BMS-150	5.0E-08	5.0E-07	1.5E-06	0.99
24 VDC dump solenoid, de-energize to trip	SY-101, SY-102	2.5E-07	0	4.0E-07	0.95
Electro-hydraulic spring-return actuator	SDV-101, SDV-102	5.0E-07	0	1.0E-06	0.90
NPS 12 full-bore ball valve, tight shutoff	SDV-101, SDV-102	6.0E-07	0	0	0.95
Electric spring-return actuator, fail-safe module	SDV-106	6.0E-07	0	8.0E-07	0.90
NPS 2 ball valve, tight shutoff	SDV-106	4.0E-07	0	0	0.95

Device class	Used for	λ_{DU}	λ_{DD}	λ_S	PTC
Solenoid safety shutoff valve, proof of closure	XV-150A, XV-150B	3.0E-07	0	3.0E-07	0.95

Note 1: The ball valve rates include failure to seal. SDV-102 must hold tight shutoff against up to 1,440 psig, and a valve that closes but passes gas lets the trunk side rise to the upstream pressure. The proof test therefore includes a seat leak test, which is what supports a coverage of 0.95.

The remaining parameters are listed in Table 3-3.

Table 3-3: Test, Repair and Common Cause Parameters

Parameter	Symbol	Value	Source
Full proof-test interval	T_I	1 yr (8,760 h)	SAF-SRS-001
Partial-stroke test interval, SDV-102	T_{PST}	3 months (2,190 h)	SAF-SRS-001
Partial-stroke coverage: solenoid, actuator, valve	C_{PST}	0.95, 0.70, 0.60	Typical, HOLD H-15
Mean time to restoration	$MTTR$	72 h	SAF-SRS-001
Mission time, sensors and logic solvers	T_M	20 yr	Station design life
Mission time, final elements	T_M	10 yr	Valve overhaul interval
Common cause factor, transmitters	β	5 %	IEC 61508-6 Annex D, typical
Common cause factor, diverse flame detectors	β	5 %	IEC 61508-6 Annex D, typical
Common cause factor, redundant valves and switches	β	10 %	IEC 61508-6 Annex D, typical

4. ASSUMPTIONS

1. All failure rates, proof-test coverages and partial-stroke coverages are typical values. *Verification required against the vendors' IEC 61508 certificates and failure modes, effects and diagnostic analysis reports (HOLD H-15).*
2. The required risk reduction rests on the Owner risk criteria assumed in SAF-RPT-002. *Verification required against the Owner's risk matrix.*
3. The partial stroke of SDV-102 is made by de-energizing the trip solenoid SY-102 for a timed interval, so the test exercises the same solenoid that trips the valve. A separate test solenoid is not used.
4. Detected dangerous failures are repaired within 72 h, with spares held on site or at the Owner's district shop and a compensating measure in place during repair.
5. The β factors are typical. *Verification required by Annex D scoring once devices and installation details are fixed.*

6. The SIF-01 trip carries a 0.5 s delay. The 0.5 s delay is kept because 2oo3 voting covers a single faulty transmitter but not a genuine short pressure excursion seen by all three, such as the pulse from control valve or SDV movement; the delay filters those without a spurious trip. Neither the delay nor the stroke time of SDV-102 enters the PFD_{avg} . A full stroke slower than 4 s found at a proof test is treated as a dangerous failure.

5. REFERENCES

1. IEC 61511-1:2016+A1:2017, Functional safety: Safety instrumented systems for the process industry sector, Part 1, clauses 11.4 and 11.9.
2. IEC 61508-6:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 6, Annex B and Annex D.
3. ISA-TR84.00.02-2015, Safety Integrity Level (SIL) Verification of Safety Instrumented Functions.
4. SAF-RPT-002, Layer of Protection Analysis.
5. SAF-SRS-001, Safety Requirements Specification.
6. PRO-CAL-009, Overpressure Protection System Hydraulic Analysis.
7. INS-DS-001, Pressure Transmitters; INS-DS-005, Level, Pressure, Temperature and Flow Switches; INS-DS-006, Electro-Hydraulic SDV Actuators; INS-DS-011, Safety PLC.
8. GEN-DB-001, Basis of Design.

6. CALCULATION

6.1. EQUATIONS

For a single channel (1oo1), the average probability of failure on demand accumulates over the proof-test interval for the tested fraction and over the mission time for the untested fraction, plus the detected failures awaiting repair:

ISA-TR84.00.02, 1oo1 with imperfect proof test

$$PFD_{1oo1} = PTC \frac{\lambda_{DU} T_I}{2} + (1 - PTC) \frac{\lambda_{DU} T_M}{2} + \lambda_{DD} MTTR$$

For voted architectures, the independent term is the probability that enough channels fail together, and the common cause term is the fraction β of a single channel:

ISA-TR84.00.02, 1oo2 and 2oo3

$$PFD_{1oo2} = PTC \frac{[(1 - \beta)\lambda_{DU} T_I]^2}{3} + (1 - PTC) \frac{[(1 - \beta)\lambda_{DU} T_M]^2}{3} + \beta PFD_{1oo1}$$

$$PFD_{2oo3} = PTC[(1 - \beta)\lambda_{DU} T_I]^2 + (1 - PTC)[(1 - \beta)\lambda_{DU} T_M]^2 + \beta PFD_{1oo1}$$

A final element part that is partial-stroke tested has the covered fraction C_{PST} tested at T_{PST} :

ISA-TR84.00.02, partial stroke testing

$$PFD = C_{PST} \frac{\lambda_{DU} T_{PST}}{2} + (1 - C_{PST}) PTC \frac{\lambda_{DU} T_I}{2} + (1 - C_{PST})(1 - PTC) \frac{\lambda_{DU} T_M}{2}$$

The SIF result is the sum over its subsystems:

$$PFD_{SIF} = PFD_{sensors} + PFD_{logic} + \sum PFD_{final}, \quad RRF = \frac{1}{PFD_{SIF}}$$

6.2. SIF-01, OVERPRESSURE SHUTDOWN

SIF-01 closes SDV-102 when two of the three transmitters PT-133A/B/C read 1,225 psig or more. It is the governing function, because it protects the receiving pipeline operator's trunkline and because its final element carries almost all of its PFD_{avg} .

6.2.1. Sensors

The three transmitters have independent taps and sit on separate safety PLC input cards, which is the basis for $\beta = 5\%$. For one transmitter:

$$PFD_{1001} = 0.95 \frac{(4.0 \times 10^{-8})(8760)}{2} + 0.05 \frac{(4.0 \times 10^{-8})(175,200)}{2} + (3.0 \times 10^{-7})(72) = 3.63 \times 10^{-4}$$

The 2oo3 group is then:

$$PFD_{2003} = 1.05 \times 10^{-7} + 2.22 \times 10^{-6} + 0.05(3.63 \times 10^{-4}) = 2.05 \times 10^{-5}$$

Common cause is 89 % of the sensor result. The sensor subsystem is less than 1 % of the SIF total.

6.2.2. Logic Solver

$$PFD_{logic} = 0.99 \frac{(2.0 \times 10^{-8})(8760)}{2} + 0.01 \frac{(2.0 \times 10^{-8})(175,200)}{2} + (5.0 \times 10^{-7})(72) = 1.40 \times 10^{-4}$$

6.2.3. Final Element Without Partial Stroke

SDV-102 is a series assembly of the dump solenoid, the electro-hydraulic spring-return actuator and the NPS 12 ball valve, each with a 10-year mission time:

$$PFD_{SY} = 0.95 \frac{(2.5 \times 10^{-7})(8760)}{2} + 0.05 \frac{(2.5 \times 10^{-7})(87,600)}{2} = 1.59 \times 10^{-3}$$

$$PFD_{act} = 4.16 \times 10^{-3}, \quad PFD_{valve} = 3.81 \times 10^{-3}, \quad PFD_{final} = 9.56 \times 10^{-3}$$

With annual proof testing alone:

$$PFD_{SIF-01} = 2.05 \times 10^{-5} + 1.40 \times 10^{-4} + 9.56 \times 10^{-3} = 9.72 \times 10^{-3}, \quad RRF = 103$$

This is within the SIL 2 band but short of the required RRF of 110. The final element is 98 % of the total, so no change to the sensors or logic solver can close the gap.

6.2.4. Final Element With Quarterly Partial Stroke

With SY-102 pulsed every three months, the covered fraction of each part is tested at 2,190 h:

$$PFD_{SY} = 0.95 \frac{(2.5 \times 10^{-7})(2190)}{2} + 0.0475 \frac{(2.5 \times 10^{-7})(8760)}{2} + 0.0025 \frac{(2.5 \times 10^{-7})(87,600)}{2}$$

$$PFD_{SY} = 2.60 \times 10^{-4} + 5.20 \times 10^{-5} + 2.74 \times 10^{-5} = 3.40 \times 10^{-4}$$

$$PFD_{act} = 1.63 \times 10^{-3}, \quad PFD_{valve} = 1.92 \times 10^{-3}$$

$$PFD_{final} = 3.40 \times 10^{-4} + 1.63 \times 10^{-3} + 1.92 \times 10^{-3} = 3.89 \times 10^{-3}$$

$$PFD_{SIF-01} = 2.05 \times 10^{-5} + 1.40 \times 10^{-4} + 3.89 \times 10^{-3} = 4.05 \times 10^{-3}$$

SIF-01 achieves $PFD_{avg} = 0.0041$ and RRF 247 with annual proof testing and a quarterly partial stroke of SDV-102. It meets SIL 2 and the required RRF of 110 with a margin of 2.2. Without the partial stroke it does not meet the requirement, so the partial stroke test is mandatory.

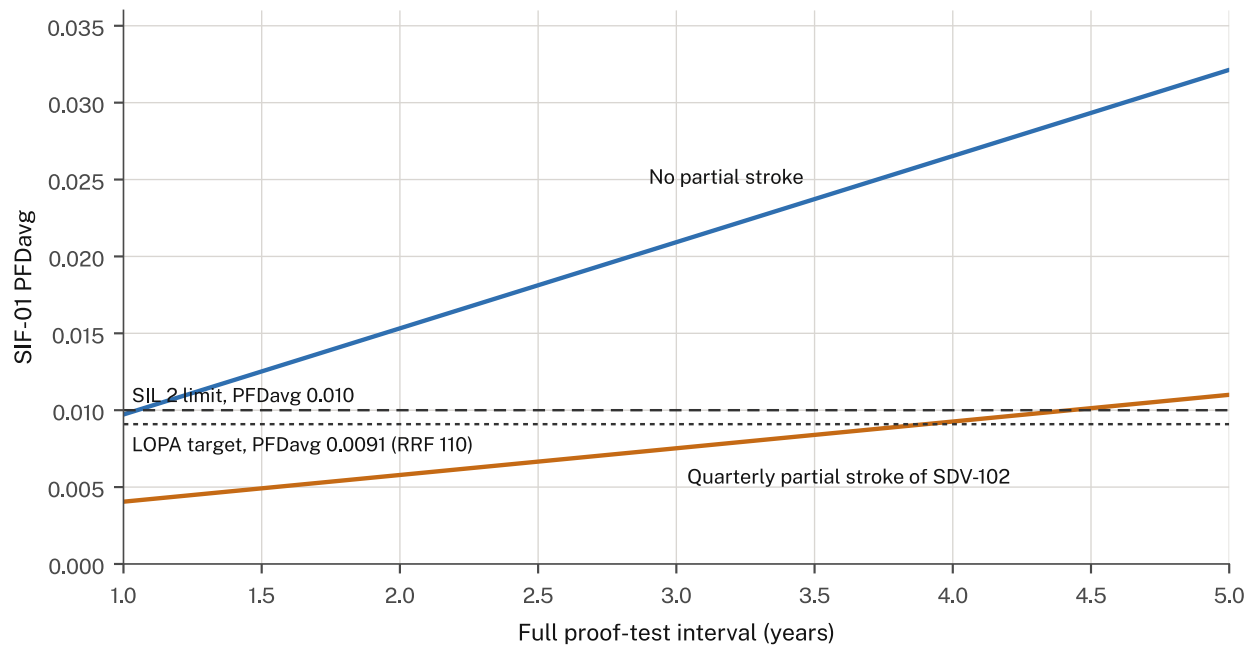
A partial stroke made through a separate test solenoid would leave the trip solenoid untested between proof tests. That arrangement gives RRF 189 and was rejected, because it removes the most frequently demanded component from the quarterly test for no gain.

The OPSS also closes SDV-103. As a second final element in a 1oo2 arrangement it would raise the RRF to 709, but it is not credited: its 20 s stroke is longer than the 7.4 s maximum stroke that the overpressure transient allows with the 1.5 s detection time, including the 0.5 s trip delay (SAF-RPT-002). It backs up the seat tightness of SDV-102 only.

6.2.5. Effect of the Proof-Test Interval

Figure 6-1 shows how the SIF-01 PFD_{avg} grows with the full proof-test interval. Without partial stroking the function falls out of SIL 2 at any interval longer than one year. With the quarterly partial stroke it stays within the LOPA target up to about 3.9 years.

Figure 6-1. SIF-01 PFDavg Against Full Proof-Test Interval



The interval is set at one year for the first period of operation. It may be extended to two years (RRF 173) or three years (RRF 133) once field data from the partial-stroke and proof-test records support the assumed failure rates, as IEC 61511-1 clause 16.3 requires.

6.2.6. Sensitivity

Table 6-1 shows the SIF-01 result for the parameters that matter most. The transmitter β has almost no effect, because the sensors are a small share of the total. The proof-test coverage of the valve assembly has a large effect: at a coverage of 0.90 the design without partial stroking would fail SIL 2 outright. This is why the seat leak test is part of the SDV-102 proof test.

Table 6-1: SIF-01 Sensitivity

Case	PFD_{avg}	RRF	Meets RRF 110
Selected design (T_I 1 yr, quarterly partial stroke)	0.0041	247	Yes
T_I 2 yr, quarterly partial stroke	0.0058	173	Yes
T_I 3 yr, quarterly partial stroke	0.0075	133	Yes
No partial stroke, T_I 1 yr	0.0097	103	No
No partial stroke, valve assembly PTC 0.90	0.0114	88	No
Transmitter β 10 % instead of 5 %	0.0041	246	Yes

6.2.7. Hardware Fault Tolerance and Spurious Trips

IEC 61511-1 Table 6 requires a minimum hardware fault tolerance of zero for SIL 1 and SIL 2 functions in low demand. The 2oo3 sensors have a fault tolerance of one, the certified safety PLC meets its own certificate, and the single SDV-102 has zero, so every subsystem complies. Each device shall carry an IEC 61508 certificate for systematic capability SC 2 or better, or be justified by prior use.

The spurious trip rate of SIF-01 is set out in Table 6-2. The 2oo3 voting makes the transmitters a negligible source of false trips; a single transmitter would contribute a spurious closure about every 285 years instead of every 5,700. The expected spurious trip rate of one every 44 years is well inside the 10-year target of the SRS.

Table 6-2: SIF-01 Spurious Trip Rate

Subsystem	Basis	Rate (per h)	Mean time to spurious trip (yr)
Transmitters, 2oo3	$6(\lambda_S + \lambda_{DD})^2 MTTR + \beta(\lambda_S + \lambda_{DD})$	2.0E-08	5,700
Safety PLC	λ_S	1.0E-06	114
SDV-102 solenoid and actuator	λ_S	1.4E-06	82
SIS 24 VDC distribution, redundant	Typical	2.0E-07	570
Total		2.6E-06	44 (0.023 per yr)

6.3. OTHER FUNCTIONS

The same equations were applied to the remaining functions. The inputs that differ from SIF-01 are the sensor type, the logic solver and the final element.

SIF-02 uses a single vibrating fork and closes SDV-101, whose final element is the same as SDV-102 without partial stroking. It achieves RRF 86 against 55.

SIF-03 uses a single fork and the electric spring-return SDV-106. The requirement is SIL 1 because restriction orifice RO-104 and the 16 in emergency vent EV-193 on T-101 limit the consequence of gas blow-by. The function achieves RRF 104 against 60. Without the orifice and vent it would need SIL 2 (RRF 188). A single fork cannot reach that even at a six-month test interval (RRF 138). Two forks with a quarterly partial stroke of SDV-106 would be needed (RRF 279).

SIF-05, flame failure, needs RRF 850. A single flame detector reaches only 442, because a flame rod that fails to register loss of flame is the dominant failure. Two diverse detectors, a flame rod and a self-checking ultraviolet scanner voted 1oo2 in a SIL 2 certified burner management system, reach 1,651. Shortening the test interval of a single detector to six months was also evaluated and rejected: it reaches only 597.

SIF-06 exceeds its SIL 1 requirement by a wide margin. SIF-04 and SIF-07 have no SIL requirement. They were evaluated for information and are retained as good-practice trips.

6.4. INDEPENDENT CHECK

The PFD_{avg} of every function was recalculated independently from the IEC 61508-6 Annex B.3.2.2 equations. Those equations use the channel-equivalent and group-equivalent mean down times, add the mean restoration time to every term, and carry the untested fraction through an equivalent test interval. The results, in Table 6-3, agree with the calculation within 3 %. The small differences come from the restoration time terms, which the simplified equations omit. No SIF changes its compliance.

Table 6-3: Independent Check of PFD_{avg}

SIF	This calculation	Independent check	Difference
SIF-01, quarterly partial stroke	0.00405	0.00415	+2.4 %
SIF-01, no partial stroke	0.00972	0.00982	+1.0 %
SIF-02	0.0116	0.0117	+1.0 %
SIF-03 and SIF-04	0.00959	0.00967	+0.8 %
SIF-05, two detectors	0.000606	0.000589	-2.9 %
SIF-06 and SIF-07	0.00431	0.00433	+0.4 %

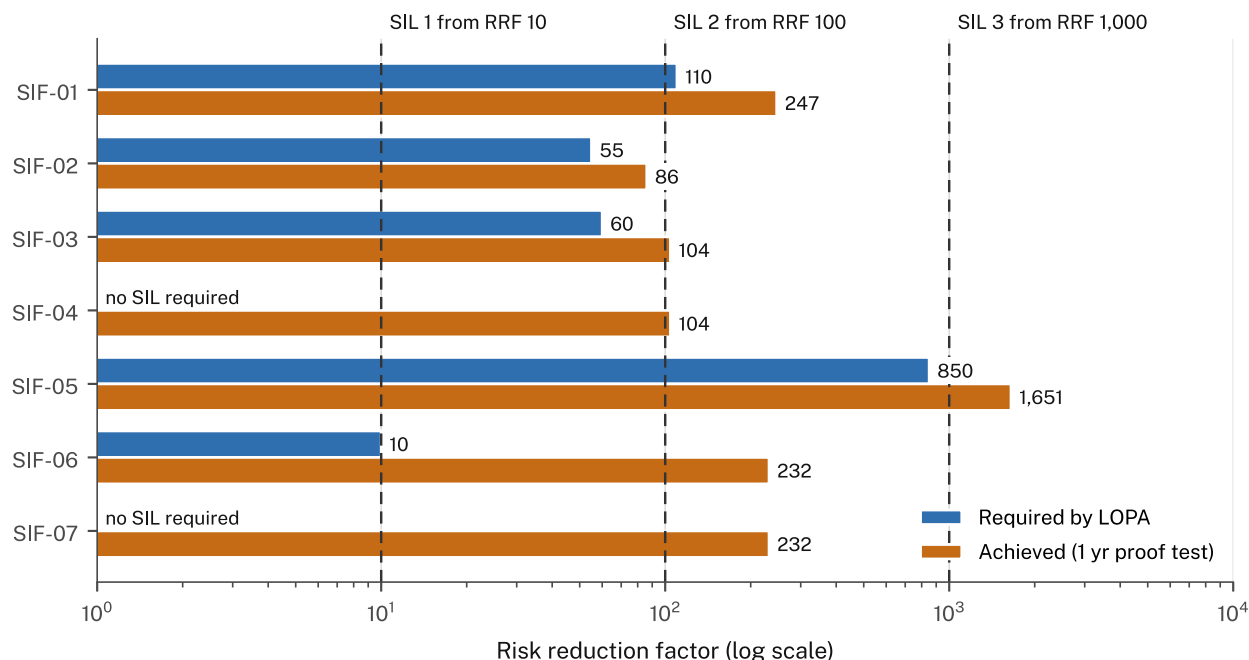
7. RESULTS AND CONCLUSIONS

Table 7-1 and Figure 7-1 summarize the verification. Every function requiring a SIL meets its required risk reduction in the selected design.

Table 7-1: SIL Verification Summary, Selected Designs

SIF	Architecture	Test regime	PFD_{avg}	RRF achieved	RRF required
SIF-01	2oo3 PT, SIL 3 PLC, SDV-102	1 yr, quarterly partial stroke	0.0041	247	110
SIF-02	1oo1 fork, SIL 3 PLC, SDV-101	1 yr	0.0116	86	55
SIF-03	1oo1 fork, SIL 3 PLC, SDV-106	1 yr	0.0096	104	60
SIF-04	1oo1 fork, SIL 3 PLC, SDV-106	1 yr	0.0096	104	No SIL
SIF-05	1oo2 diverse flame detection, SIL 2 BMS, XV-150A/B	1 yr	0.00061	1,651	850
SIF-06	LSL-154, SIL 2 BMS, XV-150A/B	1 yr	0.0043	232	10
SIF-07	TSHH-155, SIL 2 BMS, XV-150A/B	1 yr	0.0043	232	No SIL

Figure 7-1. Required and Achieved Risk Reduction by SIF



Note 1: Achieved values are for the selected designs: SIF-01 with quarterly partial stroke of SDV-102 and SIF-05 with two diverse flame detectors.

The calculation leads to the following requirements, which SAF-SRS-001 carries:

1. SDV-102 shall be partial-stroke tested every three months by pulsing its trip solenoid, and fully proof tested once a year, including a seat leak test and a stroke time measurement of 4.0 s or less.
2. The burner management system for H-101 shall be certified to SIL 2 and shall use two diverse flame detectors voted 1oo2.
3. The SIF-03 requirement of SIL 1 depends on RO-104 and emergency vent EV-193. If either is removed from the design, SIF-03 becomes a SIL 2 function and requires two level switches and partial stroking of SDV-106.
4. The calculation shall be reissued with the vendors' certified failure data (HOLD H-15) before the SIS design is frozen.

The next step is the vendor data review at bid evaluation, when each device's certificate is checked against Table 3-2.