

OWNER

Layer of Protection Analysis

Safety Integrity Level Assignment



Document No.: [REDACTED] SAF-RPT-002

Rev. A, Issued for Review

Date: September 29, 2026

Project: [REDACTED] [REDACTED]



TORUS

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

NOTICE

This document was prepared by TORUS for the use of the client named on the cover, under the terms of the agreement between TORUS and the client. It reflects the information available and the scope agreed at the date of issue. Information supplied by the client or by vendors has been used as received unless this document states that it was checked. Codes, site data and vendor information change over time, and conclusions may need to be revisited when they do. A document that is not issued for construction, or that is not sealed where a seal is required, shall not be used for construction. Use of this document by anyone other than the client is at that party's own risk.



ISSUE SUMMARY AND APPROVAL

This page records each issue of SAF-RPT-002. 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.	INTRODUCTION	1
1.1.	PURPOSE	1
1.2.	SCOPE AND EXCLUSIONS	1
2.	METHOD	2
2.1.	LOPA APPROACH	2
2.2.	RULES FOR CREDITING PROTECTION LAYERS	2
3.	RISK CRITERIA AND DATA	4
3.1.	TOLERABLE FREQUENCIES	4
3.2.	INITIATING EVENTS AND PROTECTION LAYERS	4
4.	SCENARIO ANALYSIS	6
4.1.	L-01, TRUNKLINE OVERPRESSURE (SIF-01)	6
4.2.	L-02, LIQUID CARRYOVER FROM V-101 (SIF-02)	6
4.3.	L-03, GAS BLOW-BY TO T-101 (SIF-03)	7
4.4.	L-04, T-101 OVERFILL (SIF-04)	7
4.5.	L-05, HEATER FIREBOX EXPLOSION (SIF-05)	8
4.6.	L-06 TO L-09, HEATER AND FUEL GAS SCENARIOS	8
4.7.	L-10 TO L-12, SCREENED SCENARIOS	9
5.	OPSS PROCESS SAFETY TIME	10
5.1.	GOVERNING CASE	10
5.2.	INDEPENDENT CHECK	10
5.3.	FINDINGS	11
6.	SIL ASSIGNMENT	12
7.	RECOMMENDATIONS	14
8.	CONCLUSIONS	15
9.	ASSUMPTIONS AND OPEN ITEMS	16

FIGURES AND TABLES

Figure 5-1. Trunk Pressure After an OPSS Trip, 1 Mile Blocked Trunk	11
Figure 6-1. Required and Achieved Risk Reduction	12
Table 3-1: Tolerable Mitigated Event Frequencies (HOLD, Owner Criteria)	4
Table 3-2: Initiating Event Frequencies	4
Table 3-3: Independent Protection Layers Credited	5
Table 4-1: L-01 Demand on the OPSS	6
Table 4-2: L-06 to L-09 Results	8
Table 6-1: Required SIL by Function	12

Table 7-1: LOPA Recommendations 14

1. INTRODUCTION

1.1. PURPOSE

This report assigns the required risk reduction, and so the required Safety Integrity Level (SIL), to each safety instrumented function (SIF) at the . It is the SIL assignment step of the IEC 61511 safety lifecycle. The scenarios analyzed are those that the Preliminary HAZOP, SAF-RPT-001, carried forward for layer of protection analysis (LOPA).

The report also establishes the process safety time of the overpressure shutdown system (OPSS), which protects the receiving pipeline operator's trunkline. That time sets the response the OPSS must achieve, and it governs the stroke time of the shutdown valve SDV-102.

1.2. SCOPE AND EXCLUSIONS

Twelve scenarios, L-01 to L-12, are analyzed. Seven SIFs result, SIF-01 to SIF-07. The analysis covers the station from insulating joint IJ-101 to IJ-102, including the heater H-101, the fuel gas system and the liquids tank T-101.

The following are excluded:

- The receiving pipeline operator's hot tap, tap valve and remote shutoff, which are designed by that operator.
- The Owner's upstream compression and lateral, except as the source of the overpressure demand in L-01.
- Verification that each SIF achieves its required SIL. That is done in SAF-CAL-001, SIL Verification.
- Fire and gas detection, which follows the performance-based approach of SAF-RPT-003, Fire and Gas Detection Philosophy and Layout.

2. METHOD

2.1. LOPA APPROACH

TORUS followed the method of the Center for Chemical Process Safety (CCPS) LOPA guideline. For each scenario, the frequency of the initiating event is multiplied by any enabling condition, by the conditional modifiers that apply to the consequence (ignition, presence of people, probability of harm) and by the probability of failure on demand (PFD) of each independent protection layer (IPL). The result is the mitigated event frequency. Dividing it by the tolerable frequency for the consequence gives the risk reduction factor (RRF) the SIF must supply:

CCPS LOPA, mitigated event frequency

$$f_{mit} = \sum_i f_{IE,i} P_{en,i} \times \prod_j P_{cm,j} \times \prod_k PFD_{IPL,k}, \quad RRF_{req} = \frac{f_{mit}}{f_{tol}}$$

The required SIL follows from the RRF bands of IEC 61511-1 for low-demand mode:

- An RRF of 10 or less needs no SIL. A basic process control system (BPCS) function or good practice is enough.
- An RRF above 10 and up to 100 needs SIL 1.
- An RRF above 100 and up to 1,000 needs SIL 2.
- An RRF above 1,000 and up to 10,000 needs SIL 3.

Each scenario was evaluated for every consequence category that applies to it: safety, environment and commercial or regulatory. The category needing the highest risk reduction governs. This matters here because the station is unmanned: in several scenarios the chance of harming a person is low, and the environmental or regulatory consequence sets the requirement.

2.2. RULES FOR CREDITING PROTECTION LAYERS

A layer was credited as an IPL only if it is independent of the initiating event and of the other layers credited, specific to the scenario, auditable, and able to act within the time available. Four rules follow from the station being unmanned and remotely operated:

1. A BPCS function is credited at a PFD of 0.1, at most once per scenario. It is never credited where the initiating event is itself a BPCS failure.
2. An alarm with remote operator response is credited at 0.1 only in three conditions. The alarm must be independent of the initiating event. At least about 30 minutes must separate the alarm from the consequence. The response must be written in INS-LST-003, Alarm and Trip Setpoint Schedule. The Owner's gas control is staffed around the clock, and a field call-out takes about 60 minutes (to be confirmed by the Owner).
3. A relief valve or containment dike sized for the scenario is credited at 0.01. A check valve is credited at 0.1, and only where it is inspected under a maintenance program.

-
4. A technician is in a process area for about 1.2 hours a day. The occupancy modifier is therefore $1.2 / 24 = 0.05$ (to be confirmed by the Owner).



3. RISK CRITERIA AND DATA

3.1. TOLERABLE FREQUENCIES

The Owner has not yet issued its corporate risk matrix. Until it does, the tolerable frequencies in Table 3-1 are used. They are typical of those applied by US midstream operators. The regulatory category treats a breach of the 49 CFR 192.201 pressure limit on the receiving trunkline as a major regulatory consequence in its own right, whether or not the pipe fails.

Table 3-1: Tolerable Mitigated Event Frequencies (HOLD, Owner Criteria)

Category	Consequence	Tolerable frequency (per yr)
S5	Multiple fatalities, on or off site	1E-06
S4	Single fatality	1E-05
S3	Lost-time or major injury	1E-04
E3	Reportable release on site	1E-04
E2	Contained spill or minor release	1E-03
C3	Loss of \$1 M to \$10 M, or breach of the 192.201 pressure limit	1E-04
C2	Loss of \$100,000 to \$1 M	1E-03

3.2. INITIATING EVENTS AND PROTECTION LAYERS

The initiating event frequencies in Table 3-2 are typical CCPS values. The table references in the CCPS guidelines will be confirmed when the LOPA is revalidated on the construction P&IDs.

Table 3-2: Initiating Event Frequencies

Initiating event	Frequency (per yr)	Scenarios
Control loop failure, including the Owner's upstream compressor pressure control	0.1	L-01, L-02, L-03, L-07b
Valve left in the wrong position after maintenance	0.1	L-03
Self-operated regulator failure	0.1	L-09
Flameout on a fired heater	1	L-05
Water-bath heater coil tube rupture	0.001	L-06
Loss of heater bath fluid	0.1	L-07
Heater trip or failure to fire in winter	1	L-08
Tubing or fitting leak inside an analyzer shelter	0.1	L-11
Rupture of NPS 12 station and outlet piping, about 700 ft	0.0001	L-12

The protection layers credited and the conditions attached to each are listed in Table 3-3.

Table 3-3: Independent Protection Layers Credited

Protection layer	PFD	Condition for credit
PIC-134 pressure override in the BPCS	0.1	Only where the initiating event is outside the station BPCS
Alarm and remote operator action	0.1	Rule 2 of Section 2.2
PSV-161, fuel gas relief	0.01	Sized for PCV-161 wide open
RO-104 with T-101 emergency vent EV-193	0.01	Vent sized for the orifice-limited blow-by
T-101 containment dike	0.01	110 % of tank volume
PR-101 closure pressure-warning device	0.1	Quick-opening closure device
PR-101 closure interlock I-08	0.01	Mechanical interlock with BDV-102
B-101 ventilation, monitored by FSL-208	0.1	
B-101 gas detection closing SDV-141	0.1	Fire and gas function
CKV-171 check valve	0.1	With an internal inspection program

4. SCENARIO ANALYSIS

4.1. L-01, TRUNKLINE OVERPRESSURE (SIF-01)

The Owner's lateral normally supplies 900 to 1,150 psig, below the 1,200 psig MAOP of the trunkline. The station can therefore overpressure the trunkline only if the Owner's upstream compression raises the lateral above the trunkline limit. For the assumed trunk, NPS 24 x 0.344 in API 5L X60 (HOLD H-04), that limit is 1,290 psig. Under 49 CFR 192.201(a)(2)(i), the pressure at 75 % of specified minimum yield strength governs over MAOP plus 10 % (1,320 psig).

The upstream MAOP and the setting of the Owner's compressor discharge relief are not yet known (HOLD H-16). The analysis assumes the relief is set above 1,290 psig, so that an upstream control failure can reach the station. If the Owner confirms that the lateral cannot exceed the 1,225 psig trip, the demand on the OPSS disappears.

Two initiating events were combined, as shown in Table 4-1. PIC-134 is credited against the upstream failure, because it is independent of the Owner's compressor controls. It is not credited against a failure of the station's own control system. Operator response was not credited, because the pressure passes from the trip setpoint to the limit in seconds (Section 5).

Table 4-1: L-01 Demand on the OPSS

Initiating event	Frequency (per yr)	Enabling condition	IPL	Demand (per yr)
Upstream compressor pressure control failure	0.1	Relief above 1,290 psig, 1.0	PIC-134, 0.1	0.010
Station control failure, FCV-131 open	0.1	Upstream above 1,290 psig, 0.01	None	0.001
Total				0.011

The regulatory consequence governs. A breach of the 192.201 limit is itself a C3 event, so the mitigated frequency is 0.011 per year against a tolerable 0.0001, an RRF of 110. The safety case gives an RRF of 16.5. That case assumes a 1 % chance of trunkline rupture at up to 120 % of MAOP, a 30 % chance of ignition and a 50 % chance of people in the hazard zone. It governs only if the trunk's class location, which the receiving pipeline operator has not yet provided, puts many more people near the line.

SIF-01 requires SIL 2, RRF 110 (PFD_{avg} 0.0091 or lower).

4.2. L-02, LIQUID CARRYOVER FROM V-101 (SIF-02)

If the level controller LIC-104 fails, or a liquid slug arrives ahead of a pig, liquid can rise past the filter separator's vane pack. It is then carried to the ultrasonic meters, the heater coil and the trunkline. The two initiating events total 0.2 per year. About half of such events would carry damaging quantities of

liquid. The high level alarm on LT-104 is credited only for the half of events caused by the dump valve, because a failed LT-104 cannot alarm on itself. The combined factor is 0.55, giving a mitigated frequency of 0.055 per year for a commercial loss of \$100,000 to \$1 M.

SIF-02 requires SIL 1, RRF 55.

4.3. L-03, GAS BLOW-BY TO T-101 (SIF-03)

If dump valve LCV-104 opens with the sump empty, gas at up to 1,150 psig passes into the atmospheric 100 bbl tank T-101 through line 2"-L-1060. The tank's pressure-vacuum relief valve is sized for breathing and flash gas, not for blow-by, and is not credited. The initiating events are a control failure (0.1 per year) and the valve being left open after maintenance (0.1 per year, half the time with an empty sump), a total of 0.15 per year.

Without further protection, tank rupture with a person present would require an RRF of 188, a SIL 2 function. TORUS recommended instead that the blow-by be limited at its source. Restriction orifice RO-104 caps the gas flow at a rate that the 16 in emergency vent EV-193 on T-101 can relieve. This mechanical layer (PFD 0.01) reduces the safety case to an RRF of 1.9, which needs no SIL.

The environmental case then governs. Gas still vents to atmosphere until the level trip closes SDV-106. The low level alarm and remote shutdown are credited only on the share of events caused by the controller, a combined factor of 0.4. The result is 0.060 per year against a tolerable 0.001.

The orifice and vent were preferred to a SIL 2 instrumented function for three reasons. They are passive. They remove the rupture hazard entirely rather than reducing its frequency. And a SIL 2 function would need two level switches and quarterly partial-stroke testing of SDV-106 (SAF-CAL-001).

SIF-03 requires SIL 1, RRF 60, on condition that RO-104 and EV-193 are installed as designed.

4.4. L-04, T-101 OVERFILL (SIF-04)

If a truck is not dispatched when LT-191 alarms, liquid continues to arrive until the tank overfills. At the design upset rate of 60 bbl per day, the tank takes 4.8 hours to fill from the high-high switch to overflow. That leaves time for the independent high-high alarm on LT-191 and a remote response (PFD 0.1). The 110 % containment dike (0.01) holds any overflow. The mitigated frequency of a reportable release, 0.0001 per year, equals the tolerable frequency.

SIF-04 requires no SIL. It is retained in the safety PLC as a good-practice trip.

4.5. L-05, HEATER FIREBOX EXPLOSION (SIF-05)

H-101 is a natural-draft heater with no purge fan, so no protection layer is independent of the burner management system. Two cases were combined. Flame failure while firing occurs about once a year; with a 10 % chance of delayed ignition, 5 % occupancy and a 50 % chance of fatality it gives 0.0025 per year. Failed light-off gives 0.0060 per year. That case assumes 12 light-offs a year, a 10 % chance that the pilot fails to light, a 10 % chance of explosion, the operator always present and a 5 % chance of fatality in the small firebox. The total, 0.0085 per year, is set against a tolerable frequency of 0.00001 for a single fatality.

SIF-05 requires SIL 2, RRF 850.

4.6. L-06 TO L-09, HEATER AND FUEL GAS SCENARIOS

The remaining heater and fuel gas scenarios are summarized in Table 4-2. None needs a SIL-rated function, for the reasons given in the table and below.

Table 4-2: L-06 to L-09 Results

Scenario	Governing category	Mitigated frequency (per yr)	RRF	Result
L-06 Coil tube rupture into the bath	C3	0.0010	10	No SIF; relief by bath vent
L-07 Low bath level, firetube exposed	C2	0.010	10	SIF-06 specified at SIL 1
L-07b Bath over-temperature	C2	0.0010	1.0	SIF-07, no SIL
L-08 Hydrate downstream of the control valves	C2	0.0030	3.0	No SIF; alarms adequate
L-09 Fuel gas overpressure downstream of PCV-161	S4	0.0000038	0.4	No SIF; PSV-161

For L-06, the protection is mechanical: the heater vendor will size the bath and expansion-tank vent for a full-bore coil rupture at 1,440 psig, following the API 521 tube-rupture approach. The bath high level switch LSH-154B trips the burner on the swell from a coil leak. It is supported as an early warning but not credited.

For L-07, the RRF falls exactly on the boundary between no SIL and SIL 1. SIF-06 is specified at SIL 1. API 12K practice treats low bath level as a primary heater trip, and the verified design exceeds SIL 1 by a wide margin at no extra cost.

For L-07b, the bath heats over hours, and the bath temperature alarm on TT-151 is independent of a failed fuel valve TCV-152. The alarm is therefore credited.

For L-08, the heater-outlet temperature in winter is about 19 °F, which is above the -20 °F minimum design metal temperature. There is no brittle fracture case.

4.7. L-10 TO L-12, SCREENED SCENARIOS

Three scenarios were screened and need no SIF.

L-10, pig receiver closure opened under pressure, gives an RRF of 1.2. The closure has a pressure-warning device and the mechanical interlock I-08 with the barrel vent BDV-102. Both are credited.

L-11, gas release in analyzer shelter B-101, gives an RRF of 0.1. Ventilation and the fire and gas function are credited.

L-12, reverse flow from the trunkline into a station rupture, gives an RRF of 0.1. It relies on the check valve CKV-171 and on the receiving pipeline operator's remote shutoff at the tap.

5. OPSS PROCESS SAFETY TIME

5.1. GOVERNING CASE

PRO-CAL-009, Overpressure Protection System Hydraulic Analysis, models the worst credible overpressure transient. It assumes a 1,440 psig source at IJ-101, both control valves failed wide open and 1 mile of trunkline blocked in at both ends, so that the excess flow packs a fixed volume.

The original basis tripped the OPSS at 1,250 psig with a 10 s stroke of SDV-102. At that setting the process safety time is only 5.8 s, and even a 5 s stroke brings the peak to the 1,290 psig limit. The trip has therefore been lowered to 1,225 psig and the SDV-102 full stroke set at 4 s or less, per PRO-CAL-009. A lower trip of 1,210 psig was rejected: it would sit only 30 psi above the 1,180 psig maximum setting of the PIC-134 outlet pressure override, leaving too little room for transmitter error and control overshoot. At 1,225 psig the trip is 45 psi above that setting. A faster stroke than 4 s was not pursued, because it raises surge in the station piping for little gain.

The values used in this report are those of PRO-CAL-009:

- At the 1,225 psig trip the station passes about 1,210,000 lb/h and the trunk pressure rises at 7.30 psi/s.
- The time from the trip to the 1,290 psig limit is $65 / 7.30 = 8.9$ s. This is the process safety time.
- Detection, a 0.5 s trip delay and logic take 1.5 s and SDV-102 closes in 4 s, so the SIF-01 response time is 5.5 s. The process safety time is 1.62 times the response.
- With the flow held at its full value until the valve is closed, the peak is about 1,264 psig, 26 psi below the limit. PRO-CAL-009 reports 1,260 psig on a 1.0 s detection time; the extra 0.5 s at 7.30 psi/s adds about 4 psi.
- The maximum allowable stroke is the process safety time less the 1.5 s detection time, $8.9 - 1.5 = 7.4$ s. This report uses 7.4 s rather than the 7.9 s of PRO-CAL-009, which assumed 1.0 s detection.

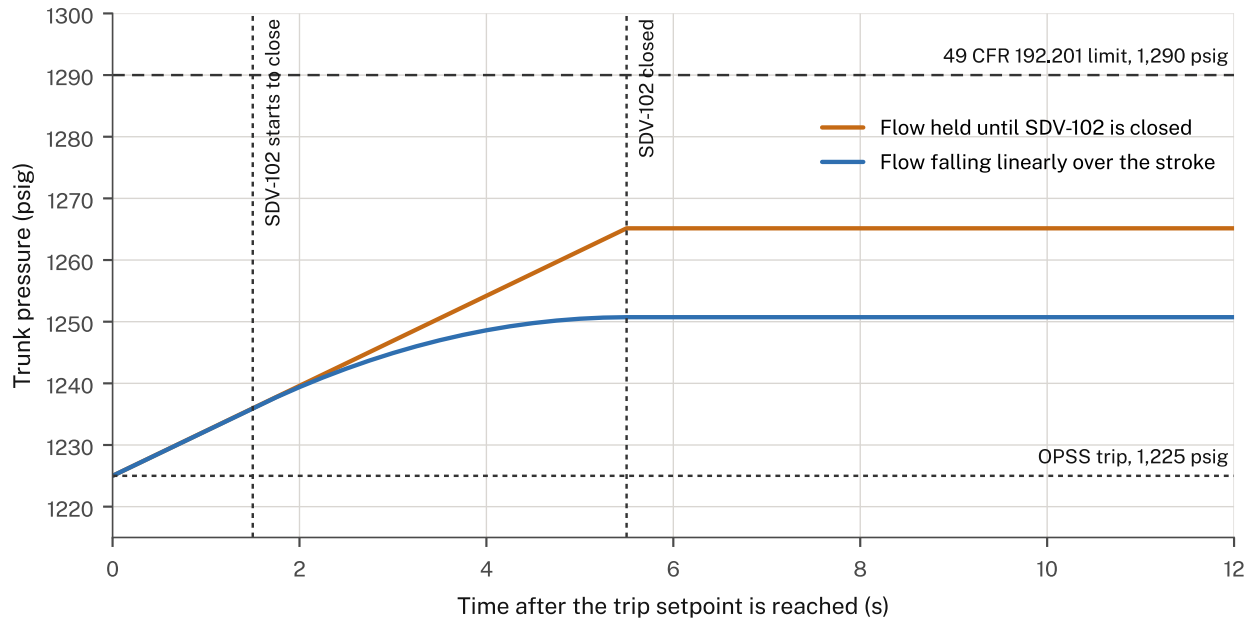
The 0.5 s delay is kept because 2oo3 voting covers a single faulty transmitter but not a genuine short pressure excursion seen by all three, such as the pulse from control valve or SDV movement; the delay filters those without a spurious trip.

5.2. INDEPENDENT CHECK

TORUS re-derived the transient independently. The packed volume is 15,840 ft³ and the speed of sound at 1,225 psig and 60 °F is 1,261 ft/s, giving a capacitance of 46.1 lb/psi. The flow through the wide-open valves was solved from the ISA-75.01 gas equation, using the station resistances of PRO-CAL-009 with the gas density in each loss term taken at the actual pressure. The check gives 1,209,000 lb/h and 7.28 psi/s, within 0.3 % of PRO-CAL-009, and the same process safety time of 8.9 s.

Figure 5-1 shows the pressure after the trip for two closure assumptions. With the flow held until SDV-102 is closed, which bounds the result, the peak is about 1,265 psig. With the flow falling linearly over the stroke, which is closer to how a ball valve behaves, the peak is about 1,250 psig.

Figure 5-1. Trunk Pressure After an OPSS Trip, 1 Mile Blocked Trunk



Note 1: 1 mile of blocked trunk, both control valves wide open, 1,440 psig source, trip 1,225 psig, 1.5 s detection including the 0.5 s trip delay, and a 4 s stroke of SDV-102.

5.3. FINDINGS

With the 1,225 psig trip, the 0.5 s delay and a 4 s stroke the trunk stays at least 26 psi below the 1,290 psig limit in the credible transient. The margin still rests on the 1 mile blocked-segment assumption and the conservative 1,440 psig source (HOLD H-04, HOLD H-16). The Safety Requirements Specification carries the following requirements:

- The OPSS trip, PAHH-133, shall be set at 1,225 psig, with the SIS pre-alarm at 1,210 psig.
- The detection and logic time of SIF-01, including the 0.5 s trip delay, shall not exceed 1.5 s.
- The full stroke of SDV-102 shall not exceed 4.0 s, verified at every proof test.
- An SDV-102 travel alarm shall be set at 5 s.

SDV-103 also closes on an OPSS trip. Its 20 s stroke is longer than the 7.4 s allowable, so it is not credited; it backs up the seat tightness of SDV-102. When the receiving pipeline operator's tap valve is closed, the station outlet piping alone is exposed. That piping is rated for 1,440 psig, and this case is not a trunkline overpressure.

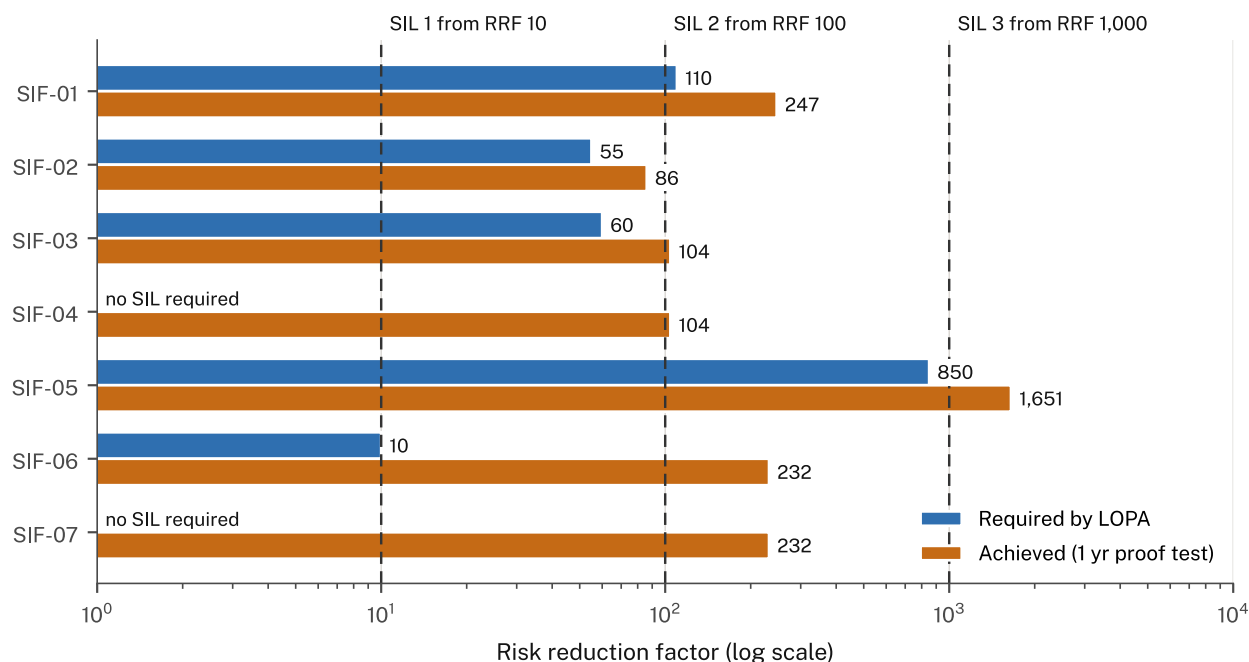
6. SIL ASSIGNMENT

The required SIL of each function is summarized in Table 6-1. Figure 6-1 compares the required risk reduction with that achieved by the verified designs in SAF-CAL-001. The two SIL 2 functions, SIF-01 and SIF-05, meet their targets only with the design features adopted from the verification. Those features are the quarterly partial stroke of SDV-102 and the second, diverse flame detector on H-101.

Table 6-1: Required SIL by Function

SIF	Function	Scenario	Governing category	Required RRF	Required SIL
SIF-01	PT-133A/B/C 2oo3 at 1,225 psig closes SDV-102 and SDV-103	L-01	C3 regulatory	110	SIL 2
SIF-02	LSHH-105 closes SDV-101	L-02	C2	55	SIL 1
SIF-03	LSSL-106 closes SDV-106	L-03	E2	60	SIL 1
SIF-04	LSHH-192 closes SDV-106	L-04	E3	1.0	None
SIF-05	BE-153A/B flame failure closes XV-150A/B/C	L-05	S4	850	SIL 2
SIF-06	LSL-154 closes XV-150A/B	L-07	C2	10	SIL 1
SIF-07	TSHH-155 closes XV-150A/B	L-07b	C2	1.0	None

Figure 6-1. Required and Achieved Risk Reduction



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.



7. RECOMMENDATIONS

The recommendations in Table 7-1 arise from this analysis. LP-03, LP-04, LP-05 and LP-07 have been adopted in the current design. LP-02 is resolved by the change of OPSS trip and stroke, and LP-06 is closed because LP-03 was adopted.

Table 7-1: LOPA Recommendations

No.	Recommendation	Responsible	Scenario
LP-01	Confirm the upstream lateral MAOP and the compressor discharge relief setting (HOLD H-16). If the upstream can exceed 1,440 psig, the station piping itself needs overpressure protection beyond the fire-case PSV-101	Owner, Process	L-01
LP-02	Resolved: the OPSS trip was lowered from 1,250 psig to 1,225 psig and the SDV-102 stroke set at 4 s or less, per PRO-CAL-009. The shortest blocked trunk segment remains to be confirmed by the receiving pipeline operator under HOLD H-04	Process, receiving operator	L-01
LP-03	Install RO-104 and T-101 emergency vent EV-193, with the vent vendor confirming capacity at the final orifice bore (adopted)	Process, Mechanical	L-03
LP-04	Partial-stroke SDV-102 quarterly by pulsing its trip solenoid (adopted)	Instrumentation	L-01
LP-05	Close SDV-103 on an OPSS trip. Specify SDV-102 to seat leakage rate A and include a seat leak test in the proof test (adopted)	Instrumentation, Process	L-01
LP-06	Closed: a second level switch and partial stroking of SDV-106 are needed only if LP-03 is withdrawn	Instrumentation	L-03
LP-07	Specify a SIL 2 certified burner management system with two diverse flame detectors. Take the pilot gas downstream of XV-150A so that XV-150A and XV-150C double-block the pilot (adopted)	Instrumentation, heater vendor	L-05
LP-08	Heater vendor to size the bath and expansion-tank vent for a full-bore coil rupture at 1,440 psig	Heater vendor, Process	L-06
LP-09	Confirm that closure interlock I-08 is a trapped-key interlock with BDV-102	Mechanical	L-10
LP-10	Confirm that every component downstream of PCV-162 is rated for the PSV-161 relieving pressure	Process	L-09
LP-11	Owner to issue its risk matrix; revalidate this LOPA against it	Owner	All
LP-12	Owner to confirm technician visit frequency. Revisit L-03 and L-05 if visits exceed about 2.4 hours a day	Owner	L-03, L-05
LP-13	Confirm the receiving pipeline operator's remote shutoff at the tap and maintain a CKV-171 inspection program	Receiving operator, Owner	L-12
LP-14	Include the alarms credited in L-02, L-04, L-07b and L-08 in the alarm management audit	Owner, Instrumentation	Several

8. CONCLUSIONS

Two functions require SIL 2. The overpressure shutdown system, SIF-01, needs SIL 2 because breaching the 1,290 psig limit on the receiving trunkline is a regulatory consequence in its own right. The heater flame failure function, SIF-05, needs SIL 2 because no other layer protects the firebox. SIF-02, SIF-03 and SIF-06 require SIL 1. SIF-04 and SIF-07 require no SIL and are retained as good-practice trips.

The SIF-03 requirement of SIL 1 depends on the restriction orifice RO-104 and the emergency vent EV-193. Without them the blow-by scenario would need a SIL 2 function.

With the trip lowered to 1,225 psig, the OPSS has a process safety time of 8.9 s in the governing transient, against a response of 5.5 s with the 0.5 s trip delay and the 4 s stroke of SDV-102. The peak is about 1,264 psig, 26 psi below the limit, and an independent check agrees within 0.3 %. The margin still depends on the trunk data to come from the receiving pipeline operator.

The next step is to revalidate this analysis at the HAZOP of the construction P&IDs. By then the Owner's risk criteria (LP-11), the upstream MAOP (HOLD H-16) and the trunk data (HOLD H-04) should be in hand.

9. ASSUMPTIONS AND OPEN ITEMS

1. Tolerable frequencies are typical values pending the Owner's risk matrix. *HOLD, Owner.*
2. The upstream relief is set above 1,290 psig. *HOLD H-16, Owner.*
3. Trunkline size, grade, MAOP and block valve spacing are as assumed. *HOLD H-04, receiving pipeline operator.*
4. Initiating event frequencies and IPL values are typical CCPS values. *TBV, table references to be confirmed at revalidation.*
5. Occupancy is 0.05 and field call-out is 60 minutes. *TBV, Owner.*
6. Emergency vent EV-193 capacity is sufficient for the flow through RO-104. *TBV, tank and vent vendors (HOLD H-15).*

