

OWNER

Safety Requirements Specification

Safety Instrumented Functions per IEC 61511-1



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

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-SRS-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. INTRODUCTION.....1

1.1. PURPOSE.....1

1.2. SCOPE 1

1.3. EXCLUSIONS.....1

1.4. REFERENCES.....1

2. SAFETY INSTRUMENTED FUNCTIONS.....3

3. GENERAL REQUIREMENTS.....4

3.1. TERMS.....4

3.2. REQUIREMENTS COMMON TO ALL FUNCTIONS.....4

4. SIF-01 OVERPRESSURE SHUTDOWN SYSTEM 5

4.1. DESCRIPTION.....5

4.2. PROCESS SAFETY TIME.....5

4.3. REQUIREMENTS 5

4.4. PROOF AND PARTIAL STROKE TESTING.....7

4.5. BYPASS 7

5. SIF-02 SEPARATOR HIGH-HIGH LEVEL.....8

6. SIF-03 AND SIF-04 SEPARATOR LOW-LOW LEVEL AND TANK OVERFILL.....9

6.1. SIF-03 SEPARATOR LOW-LOW LEVEL.....9

6.2. SIF-04 TANK HIGH-HIGH LEVEL 9

7. SIF-05 HEATER FLAME FAILURE 10

7.1. DESCRIPTION.....10

7.2. REQUIREMENTS 10

8. SIF-06 AND SIF-07 HEATER BATH PROTECTION 11

9. PROOF TEST SUMMARY 12

10. HARDWARE.....13

11. APPLICATION PROGRAM 14

12. BYPASS AND OVERRIDE 15

13. SECURITY 16

14. VERIFICATION, VALIDATION AND ASSESSMENT 17

15. CONCLUSIONS AND OPEN ITEMS 18

FIGURES AND TABLES

Table 2-1: Safety Instrumented Functions 3

Table 4-1: SIF-01 Requirements.....6

Table 5-1: SIF-02 Requirements 8

Table 6-1: SIF-03 Requirements 9

Table 7-1: SIF-05 Requirements 10

Table 8-1: SIF-06 and SIF-07 Requirements 11

Table 9-1: Proof Test Intervals..... 12

Table 14-1: Verification, Validation and Functional Safety Assessment 17

1. INTRODUCTION

1.1. PURPOSE

This Safety Requirements Specification (SRS) states what each safety instrumented function (SIF) at the must do and how reliably it must do it. It meets the content requirements of IEC 61511-1:2016 Clause 10.3. It is the document against which the safety programmable logic controller (safety PLC) in panel CP-102B and the burner management system BMS-150 will be designed, programmed, factory tested, validated at site and maintained through the life of the station.

The functions and their integrity targets come from the layer of protection analysis in SAF-RPT-002, Layer of Protection Analysis. The reliability each function achieves is shown in SAF-CAL-001, SIL Verification. Where this document states a requirement, the design shall meet it; where it states a verified value, the value is carried from SAF-CAL-001.

1.2. SCOPE

The SRS covers seven SIFs: the overpressure shutdown system (OPSS) that protects the receiving pipeline operator's trunkline, two separator level trips, the tank overfill trip, and three burner management functions on line heater H-101. It also sets the general hardware, software, testing, bypass and security rules for the safety instrumented system (SIS) as a whole.

1.3. EXCLUSIONS

The following functions are implemented in the safety PLC or the BMS but carry no safety integrity level (SIL) claim. They follow the hardware, software and change management rules of Sections 9 to 13, but not the per-function integrity requirements:

- Station emergency shutdown, P&ID interlock I-01, and the fire and gas actions in SAF-RPT-003, Fire and Gas Detection Philosophy and Layout.
- Closure of the heater fuel valve SDV-165 on a burner trip, through safety PLC input XS-150.
- The heater gas outlet high-high temperature burner trip at 140 °F on TT-156, which protects equipment and delivery temperature. No LOPA scenario requires it.

The gas quality shut-in, interlock I-07, is a basic process control system (BPCS) function in the station remote terminal unit (RTU) and is outside this SRS. The pig receiver closure interlock, I-08, is mechanical and has no instrumented logic.

1.4. REFERENCES

1. IEC 61511-1:2016, Functional safety: Safety instrumented systems for the process industry sector, Part 1.
2. ISA-TR84.00.02-2015, Safety Integrity Level (SIL) Verification of Safety Instrumented Functions.

3. ISA-TR84.00.03-2019, Automation Asset Integrity of Safety Instrumented Systems.
4. ISA-TR84.00.09-2023, Cybersecurity Related to the Functional Safety Lifecycle.
5. API RP 556, 2nd Edition (2011), Instrumentation, Control, and Protective Systems for Gas Fired Heaters.
6. 49 CFR 192.195, 192.199, 192.201 and 192.739, overpressure protection and inspection of pressure limiting stations.
7. SAF-RPT-001, Preliminary HAZOP; SAF-RPT-002, Layer of Protection Analysis; SAF-CAL-001, SIL Verification.
8. PRO-CAL-009, OPSS Overpressure Analysis.
9. INS-RPT-001, Control Philosophy and Functional Narrative; INS-LST-003, Alarm and Trip Setpoint Schedule; INS-LST-004, Cause and Effect Matrix.
10. INS-DS-001, DS-005, DS-006, DS-011 and DS-014, instrument and SIS hardware datasheets.
11. INS-RPT-002, SCADA, Communications and Cybersecurity.

2. SAFETY INSTRUMENTED FUNCTIONS

Table 2-1 lists the SIFs, the hazard each prevents and the integrity each requires. The required SIL follows from the LOPA scenario named in the table and from the Owner risk criteria, which are provisional (see Section 15).

Table 2-1: Safety Instrumented Functions

SIF	P&ID interlock	Function	Logic solver	LOPA scenario	Required SIL
SIF-01	I-02	OPSS: two of three outlet pressure transmitters at 1,225 psig close SDV-102	Safety PLC	L-01	SIL 2
SIF-02	I-03	V-101 high-high level closes SDV-101	Safety PLC	L-02	SIL 1
SIF-03	I-04	V-101 low-low level closes SDV-106	Safety PLC	L-03	SIL 1
SIF-04	I-05	T-101 high-high level closes SDV-106	Safety PLC	L-04	None
SIF-05	I-06	H-101 flame failure closes the burner shutoff valves	BMS-150	L-05	SIL 2
SIF-06	I-06	H-101 low bath level closes the burner shutoff valves	BMS-150	L-07	SIL 1
SIF-07	I-06	H-101 high-high bath temperature closes the burner shutoff valves	BMS-150	L-07	None

Note 1: SIF-04 and SIF-07 have no SIL requirement because the LOPA found the other protection layers sufficient. They are kept as good-practice trips, built and tested to the same rules as the SIL-rated functions.

3. GENERAL REQUIREMENTS

3.1. TERMS

The requirement tables in Sections 4 to 8 use four terms in the sense of IEC 61511-1. The safe state is the condition the process must reach and hold to prevent the hazardous event. The process safety time is the time from the process reaching the trip point to the hazardous event if the SIF does not act. The SIF response time is the time from the process variable crossing the setpoint to the final element reaching the safe state; it shall be less than the process safety time with margin. De-energize to trip means that a loss of signal, a loss of power or a broken wire drives the function to its safe state.

3.2. REQUIREMENTS COMMON TO ALL FUNCTIONS

Every SIF shall be de-energize to trip at its inputs and its outputs. Every trip shall latch and shall be reset only manually, locally at the equipment, after the process has returned to normal and the cause has been recorded. No SIF shall be reset remotely from the SCADA host. This rule was chosen over remote reset because the station is unmanned: a local reset puts a qualified person at the equipment before it restarts.

Every SIF shall operate over the site ambient range of -5 to 110 °F, with field devices rated to -40 °F, and every field device shall be suitable for the area classification at its location, which is at least Class I, Division 2, Group D, T3. Field circuits shall carry lightning surge protection.

A detected dangerous fault in a SIF sensor or output circuit shall raise a priority 2 alarm at SCADA. The mean time to restoration (MTTR) assumed in SAF-CAL-001 is 72 h, which requires the Owner to keep a spare transmitter, a spare solenoid valve and a spare SIL-rated I/O card of each type at its area shop. If a fault in a single-channel function is not repaired within 72 h, the function shall trip unless compensating measures are documented in a risk assessment approved by the Owner.

The SIS shall not depend on the BPCS. The RTU reads SIS status through a read-only link and cannot write to the safety PLC. Where the RTU also acts on a trip, for example by driving the control valves closed, that action is not credited in any SIF.

4. SIF-01 OVERPRESSURE SHUTDOWN SYSTEM

4.1. DESCRIPTION

The OPSS protects the receiving pipeline operator's 24 in trunkline, whose maximum allowable operating pressure is 1,200 psig (HOLD H-04). The station piping is rated 1,440 psig and the Owner's upstream compression can, on a control failure, deliver more than the trunkline can accept. If the control valves were then open, or the outlet pressure override failed, trunkline pressure would rise. Under 49 CFR 192.201 the pressure-limiting protection must keep the trunkline below the lower of its maximum allowable operating pressure plus 10 % and the pressure producing a hoop stress of 75 % of specified minimum yield strength. For the assumed NPS 24 by 0.344 in X60 trunkline the stress limit governs, at 1,290 psig.

Three pressure transmitters downstream of the control valves vote two out of three (2oo3) in the safety PLC and close SDV-102 at 1,225 psig. The trip point leaves 65 psi to the limit for detection and valve stroke, and sits 45 psi above the 1,180 psig maximum setting of the PIC-134 outlet pressure override, so that transmitter error and control overshoot do not cause spurious trips. The original basis setting of 1,250 psig left too little time for the valve to close. The OPSS also closes SDV-103. That closure adds a second barrier against leakage past SDV-102, but it is not credited because SDV-103 takes up to 20 s to close.

4.2. PROCESS SAFETY TIME

PRO-CAL-009, Overpressure Protection System Hydraulic Analysis, took the worst credible case: a 1,440 psig source, both control valves wide open and 1 mile of blocked-in trunkline. Pressure at the trip point rises at 7.30 psi/s, so the process safety time from 1,225 psig to 1,290 psig is 8.9 s. With a 1.5 s detection and logic allowance, which includes the 0.5 s trip delay, and a 4 s SDV-102 stroke, the response time is 5.5 s and the peak pressure is about 1,264 psig, 26 psi below the limit; the longest stroke that still holds the limit is $8.9 - 1.5 = 7.4$ s. PRO-CAL-009 gives 1,260 psig and 7.9 s on a 1.0 s detection time; this specification uses the 1.5 s values. At the original 1,250 psig trip the process safety time would be only 5.8 s, and a 10 s stroke would let the pressure reach 1,319 psig.

The process safety time is 1.62 times the response time. An independent check in SAF-RPT-002 agrees with PRO-CAL-009 within 0.3 %. The result still depends on the blocked trunkline length, which the receiving pipeline operator has not yet confirmed (HOLD H-04), and the response time requirement shall be reconfirmed when those data are received.

4.3. REQUIREMENTS

Table 4-1 sets the requirements for SIF-01.

Table 4-1: SIF-01 Requirements

Item	Requirement
Hazard	Trunkline pressure above 1,290 psig from upstream overpressure with the control valves open (LOPA L-01)
Sensors	PT-133A, PT-133B and PT-133C, 0 to 2,000 psig, SIL 2 capable, each on its own tap and root valve on 12"-G-1033-A6, sharing no tap or impulse line with PT-134, each wired to a separate safety PLC input card
Voting	2oo3. A channel outside 3.6 to 21.0 mA, or deviating more than 25 psi from the median for 10 s, alarms and is voted as tripped; two faulted channels trip the function
Setpoint and delay	PAHH-133 at 1,225 psig with a 0.5 s trip delay. The delay is required 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. SIS pre-alarm PAH-133 at 1,210 psig, above the 1,200 psig BPCS high-high alarm
Logic solver	Safety PLC CP-102B, certified to IEC 61508 SIL 3
Final element	SDV-102, NPS 12 Class 600 full-bore ball valve with a self-contained electro-hydraulic spring-return actuator and 24 V dump solenoid SY-102 on the uninterruptible power supply; full closing stroke 4.0 s or less; travel alarm if the valve is not closed 5 s after the trip command
Safe state	SDV-102 closed with seat leakage not above API 598 rate A (valve vendor to confirm); SDV-103 closed
Demand mode and rate	Low demand; about 0.011 demands per year (SAF-RPT-002)
Integrity required	SIL 2; risk reduction factor (RRF) at least 110; average probability of failure on demand (PFDavg) at most 9.1×10^{-3}
Integrity verified	PFDavg 4.05×10^{-3} , RRF 247, with a quarterly partial stroke and an annual proof test (SAF-CAL-001)
Process safety time	8.9 s, 1,225 to 1,290 psig at 7.30 psi/s (PRO-CAL-009)
Response time	5.5 s maximum: 0.5 s transmitter, 0.5 s trip delay, 0.5 s logic and output, 4.0 s stroke
Spurious trip rate	Mean time to spurious trip at least 10 years; verified 43.6 years (0.023 per year)
Manual shutdown	Local close pushbutton HS-102C at SDV-102; station ESD also closes SDV-102
Reset	Local key switch HS-102R only, permitted when all three transmitters read below 1,150 psig and the cause has been recorded

Note 1: Without the partial stroke test the function reaches only RRF 103 and fails its target. The quarterly partial stroke is therefore a requirement, not an option.

4.4. PROOF AND PARTIAL STROKE TESTING

The function shall be proof tested every 12 months. The annual test also meets the 49 CFR 192.739 annual inspection of pressure limiting devices. The proof test shall reach the coverages assumed in SAF-CAL-001, 0.95 for the transmitters, the solenoid and the valve and 0.90 for the actuator, and shall include, in order:

1. Apply a calibrated pressure to each transmitter through its test tee with the root valve closed, and confirm each channel trips at 1,225 psig within ± 5 psi, that the SIS pre-alarm operates at 1,210 psig, and that each pair votes correctly.
2. Confirm the SIS de-energizes SY-102 and that SDV-102 closes fully within 4.0 s, timed from the sequence of events record, and that the travel alarm is set at 5 s. A stroke longer than 4.0 s is a failed test.
3. Leak test the SDV-102 seat with differential pressure applied, bleeding the section between SDV-102 and SDV-103 through BDV-183. The seat leak test is what holds the valve coverage at 0.95; without it the function fails its target.
4. Confirm SDV-103 closure, the control valve close command, first-out capture and the alarms to SCADA and to the receiving pipeline operator.

The partial stroke test shall be made every three months from the SIS operator interface by de-energizing SY-102 for a timed interval set by the actuator vendor, so that the valve moves 15 to 20 % toward closed and returns. Testing through the trip solenoid, rather than through a separate test solenoid, was chosen because it also tests the solenoid, which raises the solenoid coverage from zero to 0.95 and the RRF from 189 to 247. The open limit switch ZSO-102 shall change state and return; if the valve does not return in the set time, the test shall trip the valve fully closed. A partial stroke shall not be started while the median transmitter reading is above 1,200 psig. A genuine demand during a test shall always trip.

4.5. BYPASS

One transmitter channel at a time may be bypassed for maintenance, using the maintenance override key HS-200B together with a selection at the SIS operator interface. The bypass shall expire automatically after 8 h, raise a priority 3 alarm at SCADA and be recorded. With one channel bypassed the remaining two vote 1oo2. The function as a whole, or SDV-102, shall not be bypassed while the station is delivering gas; SDV-102 may be bypassed for maintenance only with SDV-103 closed and under a work permit.

5. SIF-02 SEPARATOR HIGH-HIGH LEVEL

A liquid slug that overfills the filter separator V-101 would carry liquid into the custody meters, the heater coil, the control valves and the trunkline. SIF-02 closes the station inlet valve SDV-101 on a high-high level. Table 5-1 sets its requirements.

Table 5-1: SIF-02 Requirements

Item	Requirement
Hazard	Liquid carryover from V-101 (LOPA L-02)
Sensor and setpoint	LSHH-105 vibrating fork on its own nozzle, independent of LT-104, set 26 in above the sump bottom
Voting and delay	1oo1; 2 s
Final element and safe state	SDV-101, NPS 12 electro-hydraulic spring-return, closed; station inflow stopped
Integrity	SIL 1, RRF at least 55; verified RRF 86 ($PFD_{avg} 1.16 \times 10^{-2}$), annual proof test
Process safety time	Time for the sump to fill from 26 in to the vane pack at the largest slug rate; at least 60 s assumed, pending V-101 vendor data (HOLD H-15)
Response time	25 s maximum, set by the 20 s SDV-101 stroke
Proof test	Annual wet test of the fork (by raising sump level, or by removal and immersion), with coverage at least 0.90; SDV-101 full stroke and stroke time
Bypass	By maintenance override for up to 8 h, alarmed; LT-104 high alarm and the level controller shall be in service during the bypass
Reset	Local at HS-101R with the level below the 20 in high alarm

6. SIF-03 AND SIF-04 SEPARATOR LOW-LOW LEVEL AND TANK OVERFILL

6.1. SIF-03 SEPARATOR LOW-LOW LEVEL

If the separator liquid dump valve LCV-104 fails open, gas at up to 1,150 psig blows through the drain line into the atmospheric liquids tank T-101, which could rupture. The first protection is passive: restriction orifice RO-104 limits the blow-by rate to what the 16 in emergency vent EV-193 on T-101 can relieve. With that orifice and vent in place the LOPA requires SIL 1; without them it would require SIL 2 and a redundant sensor. The passive design was chosen because it removes the dependence on a fast-acting trip for a hazard whose process safety time is short.

SIF-03 closes SDV-106, a fail-closed valve upstream of LCV-104, on low-low level. It also commands LCV-104 closed, but because LCV-104 has an electric actuator that needs power to move, that command is not credited. Table 6-1 sets the requirements.

Table 6-1: SIF-03 Requirements

Item	Requirement
Hazard	Gas blow-by from V-101 to T-101 (LOPA L-03)
Sensor and setpoint	LSLL-106 vibrating fork, set 3 in above the sump bottom; 1001
Delay	2 s
Final element and safe state	SDV-106, NPS 2 ball valve with an electric spring-return fail-closed actuator, closed; stroke 5 s maximum
Integrity	SIL 1, RRF at least 60; verified RRF 104 ($PFD_{avg} 9.59 \times 10^{-3}$), annual proof test
Process safety time	Seconds to tens of seconds from 3 in to gas breakthrough at the maximum dump rate (process to confirm); hence the low setpoint and short delay
Response time	8 s maximum
Proof test	Annual: drain the sump below 3 in with LCV-104 in manual under a permit to confirm the trip; SDV-106 full stroke with a seat leak check
Startup	No startup bypass: at startup SDV-106 is closed and opens only after reset with the level above the 6 in low alarm
Reset	Local at HS-106R with the level above 6 in

6.2. SIF-04 TANK HIGH-HIGH LEVEL

SIF-04 closes SDV-106 and commands LCV-104 closed when the level in T-101 reaches 86.4 in, 90 % of the 96 in shell, as sensed by the top-mounted fork LSHH-192. The LOPA found that an overfill is contained in the tank's secondary containment and that the operator response to the level transmitter alarms is sufficient, so no SIL is required. The function is kept because it costs one switch and uses the same final element as SIF-03. It shall be tested annually with SIF-03 and reset locally at HS-106R once the level is below 76.8 in.

7. SIF-05 HEATER FLAME FAILURE

7.1. DESCRIPTION

If the burner flame on H-101 goes out while fuel is flowing, or fails to light, unburned gas accumulates in the firebox and can explode when it finds an ignition source. SIF-05 detects loss of flame and closes the burner fuel valves.

A single flame detector reached RRF 442 against the required 850. Two diverse detectors were therefore specified: a flame rod BE-153A and a self-checking ultraviolet scanner BE-153B, voting so that either detector losing flame trips (1oo2). Diverse detection principles were chosen over two identical detectors so that one common cause, such as fouling of a sight path or a rod insulator, cannot blind both. With the SIL 2 certified BMS the function reaches RRF 1,651.

7.2. REQUIREMENTS

Table 7-1 sets the requirements for SIF-05.

Table 7-1: SIF-05 Requirements

Item	Requirement
Hazard	Firebox explosion on flame failure or failed light-off (LOPA L-05)
Sensors	BE-153A flame rod and BE-153B self-checking UV scanner, 1oo2
Logic solver	BMS-150, certified to IEC 61508 SIL 2, performing purge timing, trial for ignition, proof of closure and flame supervision following API RP 556
Final elements and safe state	Main burner shutoff valves XV-150A and XV-150B in series, closed; pilot valve XV-150C closed. The pilot branch shall be taken downstream of XV-150A so the pilot is also double-blocked. SDV-165 also closes through XS-150 (not credited)
Integrity	SIL 2, RRF at least 850; verified RRF 1,651 (PFDavg 6.06×10^{-4}), annual proof test
Flame failure response time	4 s maximum from loss of flame to the shutoff valves de-energized; valve closing time 1 s maximum
Trial for ignition	Pilot 10 s maximum, main flame 10 s maximum, heater vendor to confirm (HOLD H-15); a failed trial locks out
Light-off permissives	Natural-draft purge of 5 min with XV-150A and XV-150B proven closed; low bath level, high bath temperature and fuel pressure switches healthy; SIS permissive HS-150T energized
Spurious trip rate	Mean time to spurious trip at least 5 years
Proof test	Annual: flame removal test of each detector, shutoff valve closure and proof-of-closure test, valve leak proving, and timing of the flame failure response and trials for ignition
Bypass	Not permitted in any mode
Reset	Manual at the BMS panel CP-150 after lockout; no remote reset

8. SIF-06 AND SIF-07 HEATER BATH PROTECTION

Low bath level exposes the heater firetube, which then overheats and can fail. High bath temperature boils off the bath and can release hot fluid. Both are detected by switches wired to BMS-150, which closes the burner shutoff valves. Table 8-1 sets the requirements for both functions.

Table 8-1: SIF-06 and SIF-07 Requirements

Item	SIF-06 low bath level	SIF-07 high-high bath temperature
Hazard	Firetube overheating and failure (LOPA L-07)	Bath boil-off and hot fluid release (LOPA L-07)
Sensor and setpoint	LSL-154, at least 2 in above the firetube top (heater vendor)	TSHH-155, 205 °F, manual reset
Delay	5 s	None
Final elements	XV-150A, XV-150B, XV-150C closed; SDV-165 through XS-150, not credited	Same as SIF-06
Integrity	SIL 1, RRF at least 10; verified RRF 232	No SIL; verified RRF 232 for information
Response time	7 s maximum	5 s maximum
Proof test	Annual: lower the bath level or use the vendor's test float	Annual: heated-bath test of the switch
Bypass and reset	Not permitted; manual reset at CP-150	Not permitted; manual reset at the switch and at CP-150

9. PROOF TEST SUMMARY

Table 9-1 brings the testing requirements together so the Owner can schedule them. Intervals are those used in SAF-CAL-001. An interval may be extended only when field failure data support it; SAF-CAL-001 shows that SIF-01 with quarterly partial stroking would still meet its target at a 2 year interval (RRF 173) or a 3 year interval (RRF 133).

Table 9-1: Proof Test Intervals

SIF	Proof test interval	Partial stroke	Sensor coverage	Final element coverage	Verified RRF
SIF-01	12 months	Every 3 months	0.95	0.90 to 0.95	247
SIF-02	12 months	None	0.90	0.90 to 0.95	86
SIF-03	12 months	None	0.90	0.90 to 0.95	104
SIF-04	12 months	None	0.90	0.90 to 0.95	104
SIF-05	12 months	None	0.95	0.95	1,651
SIF-06	12 months	None	0.90	0.95	232
SIF-07	12 months	None	0.90	0.95	232

Note 1: SIF-04 and SIF-07 carry no SIL requirement; their verified RRF is shown for information.

Note 2: Coverage is the fraction of dangerous undetected failures the proof test reveals. Final element ranges cover the actuator (0.90) and the solenoid and valve (0.95); the valve value depends on the seat leak test.

10. HARDWARE

The safety PLC in CP-102B shall be physically and functionally separate from the RTU in CP-102A, with its own cabinet, processor, I/O, power supplies and application program, as IEC 61511-1 Clause 11.2 requires for independence. BMS-150 shall be separate from both.

SIS field wiring shall pass only through the SIS junction boxes JB-101S, JB-130S and JB-140S and through dedicated multicore cables. SIS and BPCS signals shall never share a junction box, a multicore cable or a terminal strip. The ESD pushbuttons, the heater area flame detector BE-213, the B-102 gas detector GD-207 and the remote shutdown input from the receiving pipeline operator shall be wired directly to CP-102B. SIS cables shall carry yellow sleeves at each end and at every junction box, SIS field devices shall carry yellow stainless steel tags, and SIS terminals shall be yellow.

SIS sensors shall not share process taps, impulse lines or root valves with BPCS sensors. Final element solenoids shall be driven directly from SIL-rated output channels. Where an interposing relay cannot be avoided it shall be SIL-rated and included in the SIL verification.

The safety PLC shall be fed from redundant 24 V power supplies on the station uninterruptible power supply, which carries the SIS for at least 8 h. Loss of SIS power trips every function to its safe state. The safety PLC shall record a sequence of events at 1 ms resolution for every SIS input and output, time-synchronized to the station GPS clock.

Every SIS device shall be certified to IEC 61508 with a systematic capability at least equal to the SIL of the function it serves, or shall be justified by prior use under IEC 61511-1 Clause 11.5.3. Vendor certificates and failure data are open (HOLD H-15). The minimum hardware fault tolerance of IEC 61511-1:2016 Clause 11.4 is zero for SIL 1 and SIL 2, and every function meets it.

11. APPLICATION PROGRAM

The safety PLC program shall be written in the limited-variability language of the certified controller, using function blocks from its certified library, with one program module for each SIF. The cause and effect matrix in **INS-LST-004** is the functional specification for the program.

Trips shall latch. The program shall capture the first trip in each group, record the sequence of events and map alarm and status points to a read-only Modbus TCP table for the RTU. Voting, fault handling, bypass timers and reset permissives shall be exactly as Sections 4 to 8 state. Bypass and partial stroke functions shall be coded so that a genuine demand during a bypass of another channel, or during a partial stroke, always trips.

Program changes shall be made only under management of change as IEC 61511-1 Clause 17 requires, with version control, a change log and validation of the changed program offline before it is loaded.

12. BYPASS AND OVERRIDE

Every bypass shall require the maintenance override key HS-200B and a selection at the SIS operator interface, shall be limited to one channel of one function at a time, shall expire after 8 h, and shall raise a priority 3 alarm at SCADA. Each bypass shall be recorded with the person who authorized it, the start time, the expiry and the compensating measures in place. No bypass is permitted on the flame supervision of SIF-05 or on the bath protections of SIF-06 and SIF-07, because the heater cannot be safely run without them.

13. SECURITY

A security risk assessment of the SIS is required by IEC 61511-1 Clause 8.2.4. It is part of the station cybersecurity assessment in
INS-RPT-002, which places the SIS in its own network zone behind a read-only gateway. The following requirements apply:

1. The safety PLC shall have a hardware key switch for program and run modes, kept locked in run. A program download shall be possible only locally with the key.
2. No write access to the SIS shall exist from the SCADA host, the RTU, the internet or the receiving pipeline operator. Remote diagnostic access shall be read-only, through the Owner's jump host with multi-factor authentication and session recording.
3. The SIS engineering workstation shall be a dedicated, hardened laptop kept disconnected and under Owner control.
4. The remote shutdown from the receiving pipeline operator shall be a hardwired contact, not a network command.

14. VERIFICATION, VALIDATION AND ASSESSMENT

The SIS will be verified, validated and assessed through the stages in Table 14-1. Functional safety assessment (FSA) stage 3 is the gate before gas is introduced to the station and is an input to the pre-startup safety review in SAF-LST-001.

Table 14-1: Verification, Validation and Functional Safety Assessment

Stage	Activity	Output	Responsible
FSA 1	Assessment after HAZOP, LOPA and this SRS, before detailed design	FSA 1 report; LOPA and HAZOP actions closed	Independent assessor appointed by the Owner
Design verification	SIL verification with vendor failure data; review of SIS design, loop diagrams and cause and effect	SAF-CAL-001 at Revision 0	TORUS, checked independently
FSA 2	Assessment after SIS design, before factory testing (optional)	FSA 2 report	Independent assessor
Factory acceptance test	CP-102B and BMS-150 programs tested against this SRS and the cause and effect matrix, including bypass and reset rules	Signed test record	Integrator, witnessed by the Owner
Site acceptance and validation	Loop checks; end-to-end trip test of each SIF; response times measured from the sequence of events; setpoints and partial stroke function confirmed; OPSS setpoint and SDV-102 closure witnessed by the receiving pipeline operator	SIS validation report	Commissioning team, Owner, receiving pipeline operator
FSA 3	Assessment before gas is introduced	FSA 3 report	Independent assessor
FSA 4	Periodic assessment in operation, first at one year and then with each LOPA revalidation	FSA 4 report	Owner
FSA 5	After any modification or at decommissioning	Management of change record	Owner

In operation, the Owner will record every demand and every spurious trip and review them each year against the rates assumed in SAF-CAL-001, including the SIF-01 demand rate of about 0.011 per year. Personnel who work on the SIS shall be qualified for the covered task under 49 CFR 192 Subpart N and competent in the sense of IEC 61511-1 Clause 5.2.2.

15. CONCLUSIONS AND OPEN ITEMS

Each of the seven functions meets its integrity requirement with the architecture and test intervals set out above. Three design choices are necessary for that result and are now requirements of this SRS: the quarterly partial stroke of SDV-102 through its trip solenoid, which lifts SIF-01 from RRF 103 to 247; the diverse two-detector flame supervision in a SIL 2 certified BMS, which lifts SIF-05 from RRF 442 to 1,651; and the restriction orifice RO-104 with the T-101 emergency vent, which holds SIF-03 at SIL 1.

The SRS will be revised to Revision 0 after FSA 1, once the following open items are closed:

1. Owner risk criteria, on which every required SIL depends (Owner; SAF-RPT-002).
2. Upstream lateral maximum allowable operating pressure, which sets the OPSS demand (Owner, HOLD H-16).
3. Trunkline data and blocked segment length, which set the SIF-01 process safety time and may tighten the 5.5 s response time (receiving pipeline operator, HOLD H-04).
4. Vendor failure data, proof test coverage and certificates for every SIS device, and the heater BMS timings (vendors, HOLD H-15).
5. Process safety times for SIF-02 and SIF-03, which need V-101 sump data (TORUS process, with the V-101 vendor).
6. SDV-102 seat leakage class (TORUS process, with the valve vendor).