

OWNER

Control Philosophy and Functional Narrative

Functional Description for Control System Programming



Document No.: [REDACTED] INS-RPT-001

Rev. A, Issued for Review

Date: September 29, 2026

Project: [REDACTED] [REDACTED]



TORUS

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

N O T I C E

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 INS-RPT-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	Instrumentation and Controls			



CONTENTS

1.	INTRODUCTION	1
1.1.	PURPOSE.....	1
1.2.	SCOPE	1
1.3.	HOW TO USE THIS DOCUMENT	1
2.	REFERENCES	2
3.	CONTROL SYSTEM ARCHITECTURE	3
3.1.	SYSTEMS AND RESPONSIBILITIES.....	3
3.2.	INDEPENDENCE OF THE SAFETY SYSTEM	5
3.3.	SCAN AND RESPONSE TIMES.....	5
3.4.	INTERLOCK REGISTER.....	5
4.	OPERATING MODES AND CONTROL AUTHORITY	7
4.1.	CONTROL LOCATION	7
4.2.	OPERATING STATES	7
5.	FLOW AND PRESSURE CONTROL.....	8
5.1.	FUNCTION.....	8
5.2.	LOW SELECT WITH EXTERNAL RESET FEEDBACK.....	8
5.3.	DUTY AND STANDBY CONTROL VALVES.....	9
5.4.	RESPONSE TO SAFETY TRIPS	10
6.	CUSTODY METER OPERATION.....	11
6.1.	NORMAL OPERATION	11
6.2.	RUN SWITCHING	11
6.3.	SERIES METER VERIFICATION	12
7.	HEATER TEMPERATURE CONTROL	14
7.1.	PURPOSE AND SETPOINT	14
7.2.	HEATER MODE.....	14
7.3.	CASCADE CONTROL	15
7.4.	HEATER OUTLET HIGH-HIGH TRIP.....	16
8.	BURNER MANAGEMENT SYSTEM INTERFACE.....	17
8.1.	HARDWARE REQUIREMENTS	17
8.2.	SEQUENCE	17
8.3.	TRIPS.....	18
9.	LIQUID HANDLING.....	19
9.1.	FILTER SEPARATOR LEVEL CONTROL.....	19
9.2.	SAFETY OVERRIDES	19
10.	FUEL GAS SYSTEM	20
11.	GAS QUALITY SHUT-IN	21



12.	OVERPRESSURE SHUTDOWN SYSTEM	23
12.1.	FUNCTION AND BASIS	23
12.2.	RESET AND REOPENING	24
12.3.	PARTIAL STROKE TEST	24
13.	STATION EMERGENCY SHUTDOWN	26
13.1.	CAUSES AND EFFECTS	26
13.2.	ESD RESET AND RESTART	26
14.	PROCESS TRIPS	28
15.	FIRE AND GAS LOGIC	29
16.	STARTUP, FIRST-OUT AND ALARM MANAGEMENT	30
16.1.	STARTUP PERMISSIVES	30
16.2.	FIRST-OUT	30
16.3.	ALARM MANAGEMENT	30
17.	SAFETY SYSTEM BYPASS MANAGEMENT	32
18.	POWER AND COMMUNICATIONS FAILURE	33
18.1.	POWER FAILURE	33
18.2.	COMMUNICATIONS FAILURE	33
19.	TIME SYNCHRONIZATION AND DATA	35
20.	SUMMARY AND NEXT STEPS	36
21.	ASSUMPTIONS AND OPEN ITEMS	37

FIGURES AND TABLES

Figure 3-1: Control System and Network Architecture (INS-DWG-001)	4
Table 2-1: Reference Documents	2
Table 3-1: Control Systems and Their Functions	3
Table 3-2: Scan and Response Requirements	5
Table 3-3: Interlock Register	6
Table 4-1: Station Operating States	7
Table 5-1: Flow and Pressure Control Loop Data	8
Table 7-1: TIC-135 Setpoint Characterizer	14
Table 8-1: BMS-150 Hardware Requirements	17
Table 8-2: BMS Trip Causes	18
Table 11-1: Gas Quality Shut-In Limits	21
Table 14-1: Process Trips	28
Table 16-1: Station Startup Permissives	30
Table 16-2: Alarm Priorities	31
Table 18-1: Behavior on Power Failure	33



Table 18-2: Behavior on Communications Failure.....33

APPENDICES

APPENDIX A. TYPICAL LOOP DIAGRAMS 38

1. INTRODUCTION

1.1. PURPOSE

This document describes how the

 will be controlled and protected. It sets out every control loop, sequence, interlock, trip and reset in enough detail for the systems integrator to program the station controller (the basic process control system, BPCS), the safety programmable logic controller (safety PLC), the flow computer interfaces and the burner management system (BMS) interface. The Owner will also use it to write the station operating procedures.

1.2. SCOPE

The narrative covers the station between the inlet insulating joint IJ-101 and the outlet insulating joint IJ-102. It includes flow and pressure control, custody meter operation, line heater temperature control and the burner management interface, liquid handling at the filter separator, the fuel gas system, gas quality shut-in, the overpressure shutdown system (OPSS), station emergency shutdown (ESD), process trips, fire and gas logic, alarm handling, bypass management, and behavior on loss of power or communications.

The following are excluded:

- The internal logic of vendor packages (gas chromatograph, analyzers, flow computer custody configuration and burner management sequence timers). This document states only the functions and interfaces they must provide.
- The receiving pipeline operator's remote terminal unit (RTU) and tap valve at the trunkline.
 , as the receiving pipeline operator, designs and operates these; only the interface is described.
- The Owner's supervisory control and data acquisition (SCADA) host configuration, which follows
 INS-RPT-002, SCADA, Communications and Cybersecurity.

1.3. HOW TO USE THIS DOCUMENT

Setpoint values are controlled by
 INS-LST-003, Alarm and Trip Setpoint Schedule. The effects of each cause are tabulated in
 INS-LST-004, Cause and Effect Matrix. Where either of those documents and this narrative disagree, the integrator shall raise the conflict with TORUS before programming.

Logic in this document is written as structured pseudo-code in text blocks. It defines the required behavior, not the integrator's code structure. Values described as adjustable are parameters in the controller with the default value shown, clamped to the stated limits and changed only under the Owner's management of change procedure.

2. REFERENCES

The documents in Table 2-1 are referred to in this narrative.

Table 2-1: Reference Documents

Document	Title
GEN-DB-001	Basis of Design
INS-LST-001	Instrument Index
INS-LST-002	I/O List
INS-LST-003	Alarm and Trip Setpoint Schedule
INS-LST-004	Cause and Effect Matrix
INS-RPT-002	SCADA, Communications and Cybersecurity
INS-DWG-001	Control System and Network Architecture
INS-DWG-002	Typical Loop Diagrams
SAF-RPT-002	Layer of Protection Analysis (LOPA)
SAF-CAL-001	SIL Verification Calculation
SAF-SRS-001	Safety Requirements Specification
SAF-RPT-003	Fire and Gas Detection Philosophy and Layout
SAF-RPT-005	Emergency Response Plan (Site Specific)
PRO-CAL-003	Joule-Thomson, Water Content, Hydrate and Hydrocarbon Dewpoint Calculation
PRO-CAL-009	Overpressure Protection System Hydraulic Analysis
PRO-CAL-010	Fuel Gas System and Utility Consumption Summary
PRO-DWG-101 to 113	Piping and Instrumentation Diagrams

The following codes and standards apply: IEC 61511-1:2016 (safety instrumented systems), ANSI/ISA-18.2 (alarm management), API RP 556 and API 12K (fired heater controls and indirect heaters), API MPMS Chapter 21.1 (electronic gas measurement), AGA Report No. 9 (ultrasonic meters), 49 CFR 192.195, 192.199 and 192.201 (overpressure protection) and API 1164 (pipeline SCADA security).

3. CONTROL SYSTEM ARCHITECTURE

3.1. SYSTEMS AND RESPONSIBILITIES

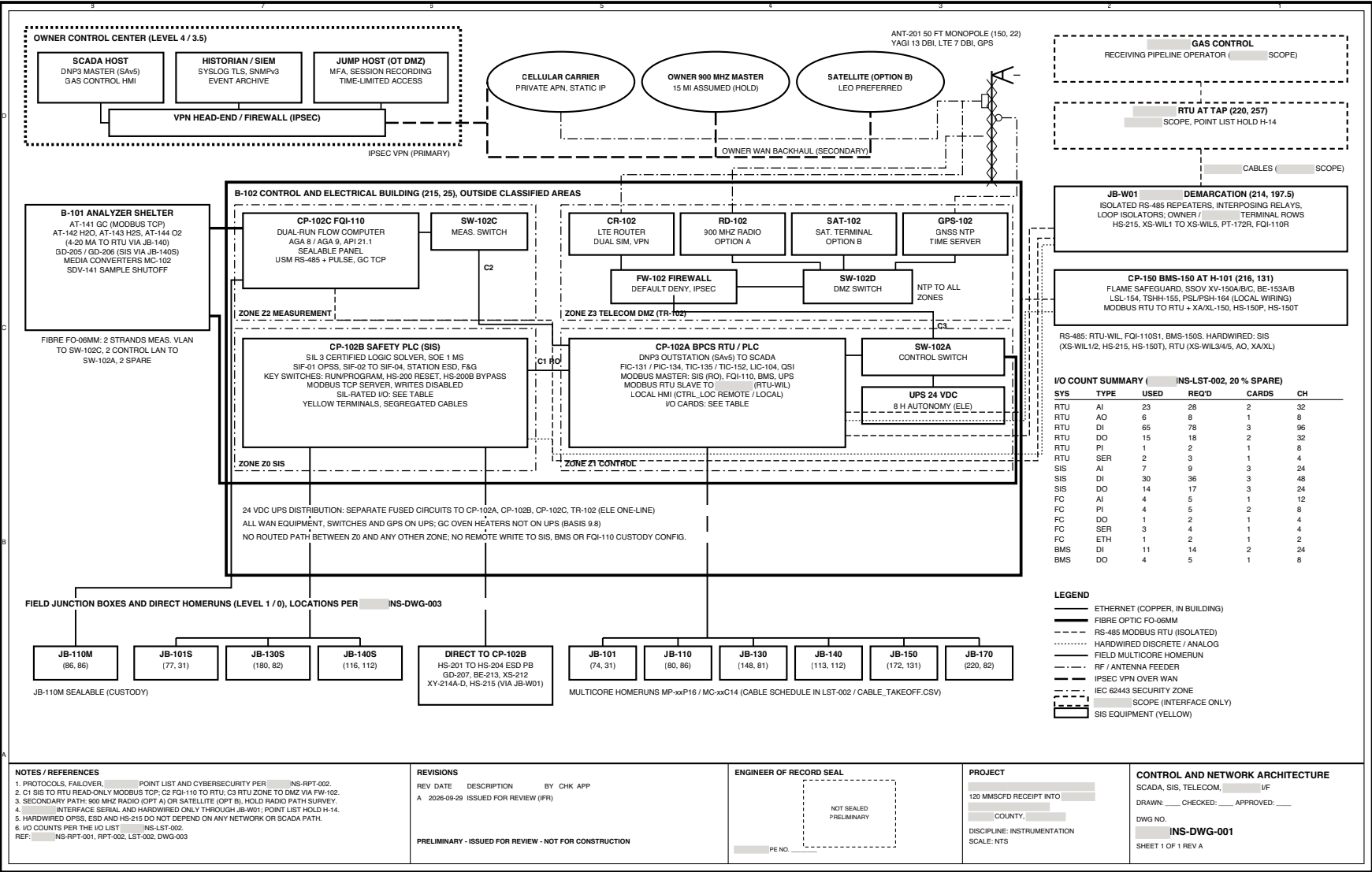
The station is controlled by four independent logic solvers housed in the control building B-102 and at the line heater, supervised remotely from the Owner's gas control center. Table 3-1 states what each system does.

Table 3-1: Control Systems and Their Functions

Level	System	Location	Function
4	Owner SCADA host	Owner gas control center	Remote supervision, nominations, setpoints, alarm response, historian
4	Receiving pipeline operator RTU	tap	Receives station data; issues remote shutdown HS-215 and flow permissive
3	BPCS station controller	Panel CP-102A, B-102	Regulatory control, sequences, gas quality shut-in, BPCS interlocks, data concentration, local operator interface
3	Safety PLC	Panel CP-102B, B-102	OPSS (SIF-01), process trips SIF-02 to SIF-04, station ESD, fire and gas, first-out, bypass management
3	Flow computer FQI-110	Panel CP-102C, B-102 (sealable)	Custody volume and energy, API 21.1 audit trail, sampler pacing, series verification comparison
3	Burner management BMS-150	Panel CP-150 at H-101	Burner sequencing and flame safeguard (SIF-05 to SIF-07)
1, 2	Field devices and local controls	Station	Transmitters, switches, actuators, local stations, self-operated regulators

Figure 3-1 shows the architecture: the panels in B-102, the field junction boxes by system, the security zones and the communication paths to the Owner and to the receiving pipeline operator.

Figure 3-1. Control System and Network Architecture (INS-DWG-001)



3.2. INDEPENDENCE OF THE SAFETY SYSTEM

The safety PLC is independent of the BPCS in every element: controller, input and output cards, field junction boxes (JB-101S, JB-130S and JB-140S), sensors and final elements. Independence is required by IEC 61511-1 so that a single BPCS failure, which is itself the initiating cause in most of the LOPA scenarios, cannot also disable the protection. The two systems are fed from the common uninterruptible power supply (UPS) bus through separately fused circuits.

The BPCS reads safety PLC status over a read-only Modbus TCP link and cannot write to it. The only signal the safety PLC accepts from the BPCS is a hardwired request to close SDV-103 at the end of a gas quality shut-in (Section 11). That signal can only move a valve toward its safe state, so it cannot defeat a safety function. Appendix A reproduces the typical loop diagrams (INS-DWG-002), which show how each class of signal is wired between the field and the panels.

The OPSS transmitters PT-133A, PT-133B and PT-133C are not used for control; PT-134 is the control transmitter. The flow computer is the custody device of record. The BPCS uses flow computer flow as its flow controller input but never writes to the custody configuration.

All shutdown valves (SDVs) are de-energize-to-trip, so a loss of safety PLC power or signal closes them. Motor-operated valves (MOVs), the flow control valves, LCV-104 and TCV-152 fail as-is, because an electric actuator cannot move without power; none of them is credited as a safety final element.

3.3. SCAN AND RESPONSE TIMES

Table 3-2 sets the minimum execution speeds. The safety PLC response is set by the OPSS, whose total response (detection, logic and a 4 s valve stroke) must fit inside the 8.9 s process safety time derived in Section 12.

Table 3-2: Scan and Response Requirements

System	Requirement
Safety PLC	Application scan 100 ms or faster; OPSS input-to-output 500 ms or less, excluding valve stroke; sequence-of-events time stamping at 10 ms resolution
BPCS	Control task 250 ms or faster; sequences 1 s
Flow computer	Flow sampling 1 s or faster, per API 21.1
BPCS to SCADA	DNP3 Secure Authentication: event poll every 60 s, integrity poll every 15 min, unsolicited reporting of emergency and high-priority events

3.4. INTERLOCK REGISTER

The P&IDs number the station interlocks I-01 to I-16. The safety PLC functions are shown on PRO-DWG-111 and the BPCS interlocks on PRO-DWG-113. Table 3-3 lists them with the section of this narrative that defines each.

Table 3-3: Interlock Register

No.	Function	System	Section
I-01	Station ESD	Safety PLC	13
I-02	OPSS, SIF-01 (voting function PY-133)	Safety PLC	12
I-03	V-101 high-high level closes SDV-101, SIF-02	Safety PLC	14
I-04	V-101 low-low level closes SDV-106 and LCV-104, SIF-03	Safety PLC	14
I-05	T-101 high-high level closes SDV-106 and LCV-104, SIF-04	Safety PLC	14
I-06	Burner trip, SIF-05 to SIF-07	BMS and safety PLC	8
I-07	Gas quality shut-in	BPCS	11
I-08	PR-101 closure mechanical interlock	Mechanical	14
I-09	Fire and gas actions	Safety PLC	15
I-10	Flow control low select and control valve switchover	BPCS	5
I-11	PT-134 high-high interlock	BPCS	5
I-12	Level controller overrides	BPCS	9
I-13	Run switching, crossover lock and series verification	BPCS	6
I-14	Heater mode permissives	BPCS	7
I-15	Station startup permissives	BPCS	16
I-16	BPCS actions following safety trips	BPCS	5

4. OPERATING MODES AND CONTROL AUTHORITY

4.1. CONTROL LOCATION

A single software selector in the BPCS sets where operating commands are accepted. In REMOTE, the normal position, the Owner's SCADA host issues setpoints, control valve duty selection, run switching and sequence commands, and the local operator interface in CP-102A only displays. In LOCAL, the local operator interface has command authority and SCADA is read-only. Selecting LOCAL requires a technician log-in at the local interface; returning to REMOTE is initiated locally and acknowledged at SCADA. Every change is recorded in the event log.

Safety resets are never available remotely. ESD, OPSS and trip resets require the key switches and local stations described in Sections 12 to 14, whatever the control location. This is deliberate: the person resetting a shutdown must be at the equipment to confirm that the cause has cleared.

Each actuator's own local/remote selector overrides both control locations. An actuator not in remote cannot be commanded by the BPCS and raises a medium-priority alarm. For a control valve this is also a switchover trigger (Section 5).

4.2. OPERATING STATES

The station will be in one of the states in Table 4-1. The state is displayed at SCADA and determines which alarms are active (Section 16).

Table 4-1: Station Operating States

State	Description
Shut down	ESD latched or station isolated; SDVs closed
Ready	ESD reset, SDVs open, control valves at 0 %, no flow
Delivering	Flow controller in automatic, one meter run in service
Verification	Series meter verification sequence active
Quality shut-in	Gas quality shut-in latched
Maintenance	Local control, technician on site, bypasses as permitted in Section 17

5. FLOW AND PRESSURE CONTROL

5.1. FUNCTION

FIC-131 controls station flow to the rate nominated by the Owner's gas control. PIC-134 limits the pressure downstream of the control valves. The lower of the two controller outputs drives the duty control valve through the low-select function FY-131. A low select was chosen over a cascade because the two objectives never apply together: the station either delivers the nomination or is limited by pressure, and the low select hands over between them without operator action. Table 5-1 gives the loop data.

Table 5-1: Flow and Pressure Control Loop Data

Item	Value
FIC-131 process variable	Station flow, sum of in-service run flows from FQI-110 over Modbus TCP at 1 s, MMSCFD at 14.73 psia and 60 °F
FIC-131 setpoint	Nomination from SCADA, clamped 0 to 120 MMSCFD; ramped at 10 MMSCFD/min (adjustable 1 to 20)
PIC-134 process variable	PT-134, hardwired
PIC-134 setpoint	1,150 psig default; operator range 900 to 1,180 psig; hard clamp 1,180 psig in code; ramp 10 psi/min
Action	Both reverse acting (process variable above setpoint closes the valve)
Initial tuning (field tune)	FIC-131 gain 0.3, integral 20 s; PIC-134 gain 1.0, integral 30 s

The PIC-134 setpoint is clamped at 1,180 psig in code so that no operator entry can bring the control layer within 45 psi of the 1,225 psig OPSS trip. The control valve actuators stroke fully in about 60 s (vendor to confirm, HOLD H-15), which is too slow to hold pressure against a fast transient. PIC-134 is therefore not credited as a protection layer for control valve failure; the OPSS is.

5.2. LOW SELECT WITH EXTERNAL RESET FEEDBACK

Both controllers compute their integral action from the selected output, so the controller that is not in control cannot wind up and the transfer between them is bumpless.

```

OP_FIC := PID(FIC-131, PV = station flow, SP = ramped nomination,
              reset feedback = OP_SEL)
OP_PIC := PID(PIC-134, PV = PT-134, SP = min(PIC_SP, 1,180 psig),
              reset feedback = OP_SEL)
OP_SEL := min(OP_FIC, OP_PIC)                // FY-131 low select
OVERRIDE_ACTIVE := OP_PIC < OP_FIC           // low alarm after 10 min
  
```

IF flow computer link fails OR station flow quality bad THEN

```
FIC-131 to MANUAL, output held at last OP_SEL
PIC-134 stays active through the low select
high alarm "FIC-131 input bad"
IF PT-134 quality bad (below 3.8 mA or above 20.5 mA) THEN
    PIC-134 to MANUAL at 100 % (override removed)
    FIC-131 setpoint frozen (no upward ramp)
    high alarm "PIC-134 input bad, OPSS is the only overpressure protection"
IF PT-134 >= 1,200 psig for 3 s THEN          // I-11
    both control valve demands forced to 0 %; FIC-131 to MANUAL at 0 %
    latch; high alarm
    reset: PT-134 below 1,150 psig AND operator reset
```

The 1,200 psig interlock sits 50 psi above the normal pressure controller setpoint and 25 psi below the OPSS trip, so that the three layers are separated by more than ten times the transmitter reference accuracy of 1.5 psi and cannot overlap on instrument error. Changing FIC-131 from manual to automatic is bumpless because its setpoint tracks the process variable in manual. The PIC-134 setpoint does not track, because a tracking pressure setpoint could follow an abnormal pressure upward. On a cold restart both controllers start in manual with their output initialized to the duty valve position.

5.3. DUTY AND STANDBY CONTROL VALVES

The duty valve is selected from SCADA. The standby valve is held at 0 % demand with its manual isolation valves open, so that it can take over without a site visit. The BPCS monitors the duty valve and transfers control automatically when it fails, as required by the Basis of Design.

```
AVAILABLE(FCV-13x) := ZSO-13xA AND ZSO-13xB      // isolation valves open
                    AND actuator in remote AND no actuator fault
                    AND ZT-13x quality good
                    AND NOT FAILED_LATCH(FCV-13x)
TRIGGER := (|ZT(duty) - DEMAND(duty)| > 5 % for 30 s)
           OR actuator fault OR actuator in local OR ZT(duty) quality bad
           (deviation test inhibited for 60 s after a setpoint step > 10 %)
IF TRIGGER THEN
    FAILED_LATCH(duty) := 1; high alarm "FCV-13x failed, switchover"
    IF AVAILABLE(standby) THEN
        DEMAND(standby) := OP_SEL                // controllers re-initialized, bumpless
        DEMAND(failed)  := 0 %                  // if stuck open, PIC-134 closes standby
        duty := standby
    ELSE
        high alarm "No control valve available"; controllers hold
MANUAL SWITCHOVER (SCADA, both valves available):
    demand ramped from the old to the new valve over 120 s (adjustable),
    controllers in automatic
```

A failed valve latches until an operator clears it after inspection. Automatic switchover only runs from the duty valve to an available standby, never back. This prevents the two valves from alternating if both develop the same fault. The 5 % deviation for 30 s was chosen to be larger than the actuator deadband and travel lag in normal modulation, which the inhibit after setpoint steps also allows for.

5.4. RESPONSE TO SAFETY TRIPS

When the safety PLC reports an OPSS trip, a station ESD, or SDV-101 or SDV-103 not open, the BPCS drives both control valve demands to 0 %, places FIC-131 in manual at 0 % and sets the ramped setpoint to zero (I-16). This prevents the control valves from opening wide against a closed SDV, which would otherwise produce a pressure surge when the SDV reopens. Restart follows Section 16.

6. CUSTODY METER OPERATION

6.1. NORMAL OPERATION

One meter run is in service and one is on standby. The standby run is kept with its inlet MOV closed and its outlet MOV open, so that it stays pressurized from the outlet header. A run is never blocked in at both ends while in service or on standby, because a run isolated in summer sun would reach about 1,570 psig, above the station design pressure. Operating the standby run this way removes the need for thermal relief valves on the meter runs, which would otherwise vent gas to atmosphere.

PT-111 and PT-121 are absolute-pressure transmitters, because the flow computer's equation of state works in absolute pressure and an absolute transmitter removes the error of an assumed atmospheric pressure. Any comparison with the gauge transmitters in the BPCS converts using the 14.10 psia local atmosphere. The crossover MOV-115 is closed and locked in software except during verification. Each run is rated for 100 % of design flow, so there is no automatic two-run operation.

Block-in protection: the BPCS rejects any MOV command that would leave a run with both its inlet and outlet MOVs closed, except in the Maintenance state with the run depressured, when the technician confirms the gauge reading and the open vent at the local interface. A run found with both closed-position switches made raises a high-priority alarm.

The BPCS derives the in-service status of each run from the MOV limit switches and passes it to FQI-110 as run-status flags, so that the flow computer accumulates flow only for runs that are carrying gas.

6.2. RUN SWITCHING

Run switching is initiated by the operator. An automatic switch on a failed meter is available as a configurable option, disabled by default, because a change of custody meter may need the receiving pipeline operator's witness under the interconnect agreement (HOLD H-01). The sequence is make-before-break so that a flow path is always open.

```
PERMISSIVES: MOV-115 closed; all MOVs in remote and healthy;  
              incoming meter healthy (FQI-110); no sequence active;  
              no ESD or OPSS trip  
START STATE: run 1 in service (MOV-111 and MOV-112 open)  
              run 2 on standby (MOV-121 closed, MOV-122 open, pressurized)  
S1  open MOV-121 (incoming run inlet); wait ZSO-121, timeout 90 s  
    // both runs now flowing  
S2  hold 300 s (adjustable); FIC-131 input is the sum of both runs  
S3  close MOV-111 (outgoing run inlet); wait ZSC-111, timeout 90 s  
S4  complete: run 1 on standby with MOV-112 left open;  
    event recorded in the FQI-110 audit log  
ON any MOV timeout or fault: stop, leave valves as they are, medium alarm
```

The outlet MOVs MOV-112 and MOV-122 are closed only during series verification, where the run stays connected through MOV-115, or in the Maintenance state.

6.3. SERIES METER VERIFICATION

The crossover MOV-115 joins the run 1 outlet (downstream of FE-111, upstream of MOV-112) to the run 2 inlet (downstream of MOV-121, upstream of the run 2 flow conditioner). Gas therefore always passes FE-111 first and then FE-121. The test is performed at least quarterly and whenever meter diagnostics drift, with the receiving pipeline operator witnessing (HOLD H-01). It is run at the normal operating rate of 90 MMSCFD or less, because at 120 MMSCFD the series path adds about 3.8 psi of pressure drop and would limit delivery.

MOV-115 is locked in software: the BPCS rejects an open command unless the verification sequence is active, and the sequence requires a supervisor permit and a "witness present" confirmation. Its handwheel is padlocked closed outside tests.

PRECONDITIONS

```
flow stable: |station flow - setpoint| < 5 % for 30 min
30 MMSCFD (adjustable) <= station flow <= 90 MMSCFD
both meters healthy (no path failure, speed-of-sound alarms clear)
gas chromatograph healthy
no ESD, OPSS trip or quality shut-in; all MOVs in remote
witness confirmed
```

```
V1 line up run 1 in service; confirm MOV-122 open
V2 open MOV-115; wait ZSO-115          // run 2 flows in parallel via crossover
V3 close MOV-112; wait ZSC-112        // all flow in series, FE-111 -> FE-121
V4 confirm MOV-121 closed; technician checks the body bleeds of MOV-112
    and MOV-121 and PI-115A, then confirms "seals verified" locally
V5 stabilize 10 min (adjustable 5 to 30)
V6 flow computer compares three consecutive 20 min averages of standard
    volume flow, each meter corrected with its own pressure and temperature:
    
$$DEV = (Q1 - Q2) / ((Q1 + Q2) / 2) \times 100 \%$$

V7 PASS if |DEV| <= 0.3 % for all three averages AND speed-of-sound
    deviation within limit on both meters
    ELSE high alarm "series deviation"; result held; both meters checked
V8 restore: open MOV-112, wait ZSO-112; close MOV-115, wait ZSC-115
    // run 2 back to standby with MOV-122 open
V9 flow computer report (both meters, pressure, temperature,
    composition, diagnostics) logged per API 21.1
ABORT (any step) -> V8:
    flow change > 10 % or flow > 90 MMSCFD; any meter or MOV alarm;
    PT-111 and PT-121 differ by more than 10 psi;
    ESD, OPSS trip or quality shut-in; operator abort
```

The 0.3 % acceptance comes from the Basis of Design. The pressure-difference abort at 10 psi detects a partly closed valve in the series path before it can bias the comparison. If the interconnect agreement requires agreement tests at more than one rate, steps V5 to V7 are repeated at each rate, all at or below 90 MMSCFD.



7. HEATER TEMPERATURE CONTROL

7.1. PURPOSE AND SETPOINT

The line heater keeps the temperature downstream of the control valves (TT-135) above the hydrate and hydrocarbon dewpoint limits. The requirement changes with pressure, so the TIC-135 setpoint is compensated on the control valve outlet pressure PT-134. At each pressure it is the largest of 40 °F, the hydrate temperature plus 10 °F and the hydrocarbon dewpoint plus 10 °F. PRO-CAL-003 calculated these values; Table 7-1 gives the characterizer the BPCS will use, with linear interpolation between points and the end values held outside the table range.

Table 7-1: TIC-135 Setpoint Characterizer

PT-134 (psig)	Setpoint, design gas (°F)	Setpoint, rich gas (°F)
700	42.3	52.2
750	43.5	52.5
800	44.7	52.4
850	45.8	52.1
900	46.8	51.4
950	47.8	50.5
1,000	48.7	49.2
1,050	49.5	49.8
1,100	50.4	50.6
1,150	51.1	51.4
1,180	51.6	51.9

Note 1: Source PRO-CAL-003. The design-gas column applies in normal operation; the rich-gas column applies while the gross heating value alarm from AT-141 is active, because rich gas has a higher hydrocarbon dewpoint.

A straight line between the 750 and 1,150 psig values was considered and rejected. The hydrate curve is concave, and a straight line would set the target up to 0.5 °F too low at 950 psig, which is inside the 10 °F margin the setpoint is meant to guarantee.

With the heater off, gas leaves the control valves at about 19 °F in the winter maximum-pressure-cut case, so the heater is needed in winter. In the normal and minimum-pressure cases the control valve outlet stays above the setpoint without heat, which is why summer bypass is the normal heater mode. To hold 43.5 °F at 750 psig in the winter case, the heater gas outlet must be about 67 °F.

7.2. HEATER MODE

Heater mode ON or OFF is selected from SCADA. The BPCS enables the burner only when the heater bypass is confirmed closed, because firing with the bypass open heats the bath without heating the gas and eventually trips the burner on high bath temperature.

```
HEATER_ON_PERMIT := ZSC-158C (bypass closed) AND NOT ZSO-158C
                    AND no ESD AND safety PLC burner permit
HS-150P (BPCS enable to BMS) := HEATER_MODE_ON AND HEATER_ON_PERMIT
advisory "Heater required":
    HEATER_MODE_OFF AND TT-135 below its setpoint for 5 min
advisory "Bypass open with heater on":
    HEATER_MODE_ON AND ZSO-158C
```

With heater mode OFF, the enable signal is removed, the BMS stops the burner normally, TCV-152 is driven to 0 % and TIC-135 and TIC-152 track in manual. HV-158A and HV-158B carry no position switches; their positions are verified by procedure.

7.3. CASCADE CONTROL

TIC-135 is the master controller and sets the heater gas outlet temperature target for TIC-152, which trims the burner through TCV-152. A cascade was chosen because the water bath responds over tens of minutes, and controlling the heater outlet directly lets TIC-152 correct firing before the slow bath disturbance reaches the control valve outlet. A bath high limit (TIC-151 at 190 °F) is low-selected with TIC-152 so that the burner can never overheat the bath while chasing a gas temperature.

```
IF HEATER_MODE_ON AND XL-150 (BMS release to modulate) THEN
    P_F := 60 s filter(PT-134); IF PT-134 bad THEN P_F := 1,150 psig
    SP_TAB := interpolate(characterizer, P_F) // design or rich column
    TIC-135 SP := max(40 °F, SP_TAB) + operator bias (0 to +10 °F),
                rate limit 1 °F/min
    TIC-135: PV = TT-135; output = TIC-152 SP, clamped 50 to 130 °F
    TIC-152: PV = TT-156; output OP_152
    TIC-151: PV = TT-151; SP 190 °F; output OP_151
    TCV-152 demand := min(OP_152, OP_151) // external reset feedback
ELSE
    TCV-152 demand := low-fire position (vendor, HOLD H-15)
    TIC-135 and TIC-152 track in manual
IF TT-135 bad THEN TIC-152 alone at last good SP (default 70 °F)
IF TT-156 bad THEN TCV-152 holds; high alarm
IF TT-151 bad THEN TCV-152 limited to low fire; high alarm
```

The upper clamp of 130 °F keeps the heater outlet below the 140 °F high-high trip and well below the 120 °F delivery temperature limit once the gas has cooled across the control valves; the lower clamp of 50 °F is below the 67 °F the winter case needs, so it never limits the required duty. Initial tuning, to be refined at commissioning, is TIC-135 gain 1.0 with integral 600 s and TIC-152 gain 2.0 with integral 900 s.

7.4. HEATER OUTLET HIGH-HIGH TRIP

A high-high temperature at the heater gas outlet trips the burner. It protects the coating on downstream piping and the delivery temperature limit if TCV-152 fails open. The trip is detected by the BPCS on TT-156 and passed to the BMS as a hardwired, de-energize-to-trip contact, so that loss of BPCS power also trips the burner.

```
IF heater mode ON AND
  (TT-156 >= 140 °F for 5 s OR TT-156 quality bad for 30 s) THEN
  TY-156 := 0           // BPCS output, normally energized
                        // BMS input TS-156 opens -> burner trip (I-06)
  latch; emergency alarm "TT-156 high-high, burner trip"
RESET: TT-156 below 130 °F AND operator reset -> TY-156 := 1
      BMS restart is local at CP-150
```

This trip is a BPCS function; the SIL assessment in SAF-SRS-001 did not require it to be a safety instrumented function. The high alarm at 130 °F gives the operator time to act before the trip.

8. BURNER MANAGEMENT SYSTEM INTERFACE

8.1. HARDWARE REQUIREMENTS

BMS-150 is supplied with the line heater by the heater vendor. Table 8-1 states the minimum requirements, based on API RP 556 guidance and API 12K practice, which the vendor shall confirm and certify (HOLD H-15). The LOPA set SIF-05 (flame failure) at SIL 2. A single flame detector did not meet that target in the SIL verification, so two diverse detectors voting one-out-of-two are required, and the BMS logic solver shall be certified to IEC 61508 for SIL 2.

Table 8-1: BMS-150 Hardware Requirements

Item	Requirement
Logic solver	Dedicated burner management controller in CP-150, separate from the BPCS, IEC 61508 certified SIL 2 capable
Flame detection	BE-153A (flame rod) and BE-153B (self-checking ultraviolet scanner); loss of flame at either detector trips; both prove pilot and main flame
Fuel isolation	Main safety shutoff valves XV-150A and XV-150B in series with proof-of-closure switches ZSC-150A and ZSC-150B; pilot valve XV-150C downstream of XV-150A
Ignition	Spark igniter BY-153; pilot ignited first, main flame lit from a proven pilot
Trips wired direct to the BMS	TS-156, LSL-154, LSH-154B, TSHH-155, PSL-164A, PSH-164B, safety PLC permit HS-150T, BPCS enable HS-150P
Low-fire start	TCV-152 at low fire before main flame trial, proven by ZSL-152
Outputs	To BPCS: common trip XA-150, release to modulate XL-150, Modbus status and first-out. To safety PLC: trip relay XS-150, which closes SDV-165

No vent valve is fitted between the main block valves. The station is designed for zero routine methane emission, so valve tightness is proven by the proof-of-closure switches and a pre-light valve leak test where the vendor offers one. The pilot is taken downstream of XV-150A so that XV-150A and XV-150C together double-block the pilot supply.

8.2. SEQUENCE

START PERMISSIVES:

HS-150P AND HS-150T AND SDV-165 open
AND LSL-154, LSH-154B, TSHH-155, PSL-164A, PSH-164B healthy
AND ZSC-150A AND ZSC-150B made AND no flame signal
AND low fire proven (ZSL-152) AND no latched trip

PURGE: natural-draft purge, fuel valves closed, 5 min minimum
(vendor to confirm at least four firebox volume changes)

PILOT TRIAL: open XV-150C, energize BY-153; 10 s maximum;
flame proven by BE-153A and BE-153B;
else close XV-150C, lock out, re-purge before any retry

MAIN TRIAL: open XV-150A and XV-150B with TCV-152 at low fire;
 10 s maximum

RUN: after 60 s of stable flame set XL-150 (release to modulate);
 the BPCS cascade takes TCV-152

NORMAL STOP: HS-150P removed -> XL-150 := 0, TCV-152 to low fire,
 close XV-150A, B and C, post-purge by draft

8.3. TRIPS

Every BMS trip closes XV-150A, XV-150B and XV-150C, locks out, and de-energizes the trip relay XS-150. The safety PLC then closes SDV-165, which isolates the heater fuel branch. SDV-165 sits on the heater branch only, so the standby generator's fuel supply stays live and standby power remains available after a burner trip. Table 8-2 lists the trip causes.

Table 8-2: BMS Trip Causes

Cause	Detail	Function
Flame failure	BE-153A or BE-153B; flame failure response time 4 s maximum; detector self-check fault also trips	SIF-05
Low bath level	LSL-154, 5 s delay	SIF-06
High-high bath temperature	TSHH-155 at 200 °F, manual-reset switch	SIF-07
High bath level (coil leak)	LSH-154B, 5 s delay; BPCS also raises an emergency alarm to isolate the coil at HV-158A and HV-158B	HAZOP HZ-05
High-high heater gas outlet temperature	TT-156 at 140 °F through TY-156 and TS-156	BPCS trip
Fuel pressure low or high	PSL-164A at 5 psig, PSH-164B at 20 psig (HOLD H-15), 2 s	Burner protection
Station ESD	HS-150T de-energized	I-01
Proof of closure lost	ZSC-150A or ZSC-150B not made when de-energized	Start inhibit
BMS internal fault or power loss	Watchdog	All outputs de-energize

All BMS trips latch and are reset only at CP-150. The first-out cause is shown locally and sent to the BPCS. SDV-165 is then reopened at its local station HS-165 once the BMS is reset. A normal stop from the BPCS does not open XS-150, so SDV-165 stays open and the burner can relight without a site visit.

9. LIQUID HANDLING

9.1. FILTER SEPARATOR LEVEL CONTROL

LIC-104 holds the V-101 liquid sump level by modulating the dump valve LCV-104 to T-101. The controller and its overrides are set out below.

```
LIC-104: PV = LT-104 (0 to 30 in), SP 12 in, direct acting
          (level up opens LCV-104), gain 2.0, integral 120 s
IF LT-104 <= 6 in THEN                                     // I-12
    LCV-104 := 0 %; hold until LT-104 >= 10 in, then back to automatic
IF LT-191 >= 76.8 in (T-101 at 80 %) THEN                   // I-12
    LCV-104 := 0 %; latch; medium alarm
    reset when LT-191 < 70 in AND operator reset
IF ZT-104 > 50 % for 120 s AND LT-104 fell less than 0.5 in THEN
    medium alarm "possible gas blow-by"
IF SDV-106 not open THEN LIC-104 to manual at 0 %          // no wind-up
IF LT-104 quality bad THEN
    LIC-104 to manual at 0 %; high alarm; safety trips remain active
```

The low-level override at 6 in holds a liquid seal above the dump valve so that gas cannot pass to the atmospheric tank, and it acts well before the 3 in safety trip. The T-101 override at 80 % of the 96 in shell stops liquid transfer 9.6 in before the 90 % safety trip, which gives the operator time to arrange a truck.

9.2. SAFETY OVERRIDES

The low-low level switch LSLL-106 (SIF-03, I-04) and the T-101 high-high switch LSHH-192 (SIF-04, I-05) close SDV-106 and energize the force-close input of LCV-104. SDV-106 was added upstream of LCV-104 because LCV-104 fails as-is and is itself the likely cause of gas blow-by; the LOPA needed a fail-closed final element independent of the control valve. SDV-106 has an electric spring-return actuator. The LCV-104 force-close is an energize-to-close action on a fail-as-is actuator and is not credited. A restriction orifice RO-104 downstream of LCV-104 limits any blow-by to the capacity of the T-101 emergency vent, which together with SDV-106 sets SIF-03 at SIL 1.

If SDV-106 closes while liquid continues to arrive, the V-101 level rises until LSHH-105 closes SDV-101 (SIF-02). T-101 must then be unloaded before restart.

10. FUEL GAS SYSTEM

Fuel is taken downstream of V-101 and upstream of the custody meters, so fuel gas is never measured by FE-111 or FE-121 and is not delivered to the receiving pipeline operator. Two self-operated regulators reduce pressure: PCV-161 to 150 psig and PCV-162 to 25 psig.

Without preheat, the pressure cut across PCV-161 would chill the gas to about -32 °F in the winter case, below the minimum design metal temperature and cold enough to freeze the regulator. The electric preheater E-161 (5 kW rated, explosion-proof, about 4.0 kW duty per PRO-CAL-010) therefore heats the fuel upstream of PCV-161. Its integral controller TIC-161A is set at 105 °F, the outlet temperature needed to keep the PCV-161 outlet at 40 °F or above with the rich gas case (102.7 °F) plus a small margin. E-161 is a self-contained package; the BPCS only monitors it. The high element temperature cutout TSH-161B de-energizes the element and gives a medium-priority alarm with manual reset at E-161, and the common alarm XA-161 covers low outlet temperature, heater fault and loss of power. A frozen PCV-161 shows first as PT-164 low (15 psig) and ends in a burner trip on PSL-164A, so the operator response to XA-161 is to check TI-161C and PT-164 before the burner trips. E-161 is fed from generator-backed power.

PSV-161 protects the section between PCV-161 and PCV-162 and is set at 250 psig, below the 285 psig rating of the Class 150 piping. The BPCS monitors PT-164 downstream of PCV-162 (high alarm 35 psig, low alarm 15 psig) and totalizes FT-163 hourly and daily for the Owner's fuel allocation. The FT-163 high alarm at 6.0 Mscf/h sits just above the calculated maximum demand of 5.6 Mscf/h on lean gas.

SDV-165 closes on station ESD (I-01) and on a burner trip through XS-150 (I-06). Its reset is local at HS-165.

11. GAS QUALITY SHUT-IN

Gas outside the receipt specification is alarmed to the Owner and the receiving pipeline operator. If it stays out of specification for an adjustable delay, 15 min by default, the BPCS starts a controlled shut-in (I-07). The shut-in is a BPCS function, not a safety instrumented function, because off-specification gas is a commercial and integrity concern for the receiving system rather than an immediate hazard at the station. The limits in Table 11-1 are those of the Basis of Design pending the interconnect agreement (HOLD H-13).

Table 11-1: Gas Quality Shut-In Limits

Parameter	Analyzer	Alarm	Shut-in condition
Gross heating value	AT-141	1,140 / 980 Btu/scf	Above 1,150 or below 970 Btu/scf
Carbon dioxide	AT-141	1.8 mol %	Above 2.0 mol %
Total inerts	AT-141	3.6 mol %	Above 4.0 mol %
Water vapor	AT-142	5.0 lb/MMscf	Above 7.0 lb/MMscf
Hydrogen sulfide	AT-143	3.2 ppmv	Above 4.0 ppmv (0.25 gr/100 scf)
Oxygen	AT-144	8 ppmv	Above 10 ppmv
Delivery temperature	TT-173	42 / 118 °F	Below 40 °F or above 120 °F

A faulted analyzer does not start the shut-in timer, because shutting in the station on an instrument fault would interrupt deliveries without a quality problem. Instead the fault raises a high-priority alarm and the Owner takes a spot sample under the agreement.

FOR each parameter:

timer runs while the value is beyond its shut-in limit with good quality; timer resets when the value is back inside by 2 % hysteresis

START := any timer $\geq$ delay (default 900 s, adjustable 0 to 3,600 s)

OR receiving operator permissive lost for 600 s (HOLD H-01, H-14)

ON START:

latch; signal to receiving operator; high alarm

flow setpoint ramps to 0 at 10 MMSCFD/min (adjustable 2 to 20)

WHEN flow < 1.0 MMSCFD AND duty valve < 2 % for 60 s:

both control valves to 0 %

XY-103Q := 1 // hardwired close request to the safety PLC

safety PLC closes SDV-103; confirm ZSC-103

SDV-103 closed signal to receiving operator

RESTART:

all parameters in specification for 30 min

AND receiving operator permissive present

AND supervisor reset at SCADA

-> XY-103Q := 0

-
- > safety PLC reopens SDV-103 only if no ESD is latched
AND $|PT-172 - PT-134| < 50$ psi
 - > FIC-131 to automatic with setpoint ramp from 0

The flow is ramped down before SDV-103 closes so that the station does not slam shut against the receiving system and so that the outlet check valve is not cycled. The 50 psi differential condition prevents SDV-103 from reopening against a large pressure difference.




```
latch OPSS trip
SY-102 := 0 (SDV-102 closes); SY-103 := 0 (SDV-103 closes)
trip signal to receiving operator; first-out; emergency alarm
BPCS (from status): control valves to 0 %, FIC-131 manual at 0 %
PRE-ALARM: median(PT-133A/B/C) >= 1,210 psig -> high alarm
DEVIATION: any channel > 25 psi from the median for 10 s -> high alarm
TRAVEL: ZSC-102 not made within 5 s of the trip -> high alarm
```

A faulted transmitter is voted as tripped so that the function fails toward safety: one faulted channel leaves a one-out-of-two vote on the healthy pair, and two faulted channels trip the station. The 0.5 s delay is kept, and is included in the 1.5 s detection time above. Two-out-of-three voting already covers a single bad transmitter; the delay filters genuine short pressure excursions caused by control valve or SDV movement, which would otherwise trip the station for no reason.

12.2. RESET AND REOPENING

Reset is local only, by key at HS-102 beside SDV-102, after the cause has been identified and recorded.

RESET PERMISSIVES:

```
PT-133A, B and C each below 1,150 psig, healthy, deviation clear
AND no bypass on SDV-102 outputs
AND both control valves at 0 % (ZT-131 and ZT-132 < 2 %)
AND no ESD latched
```

```
ON HS-102R: OPSS trip cleared; SY-102 := 1 (hydraulic pump opens SDV-102)
THEN: SDV-103 reopened locally at HS-103 after equalizing via HV-103H
```

The equalizing bypasses were added so that the SDVs are never reopened against full differential pressure, which damages ball valve seats and would reduce the tightness the OPSS relies on. If the trip was caused by high pressure on the receiving side, PT-133 stays above the reset value and SDV-102 stays closed until the receiving pipeline operator reduces pressure. This is the intended behavior.

12.3. PARTIAL STROKE TEST

A partial stroke test of SDV-102 is mandatory at least every 92 days. The SIL verification showed that without it SIF-01 falls short of its required risk reduction, because the undetected failure rate of the valve and actuator dominates between proof tests. No separate test solenoid is fitted: the safety PLC briefly de-energizes the trip solenoid SY-102 and re-energizes it as soon as the open limit switch clears, limiting travel to about 10 to 15 % (vendor to confirm, HOLD H-15). Using the trip solenoid tests the component that actually closes the valve, which a separate test solenoid would not.

```
PERMISSIVES: technician log-in at the safety PLC interface;
              flow stable; median PT-133 below 1,150 psig;
              no OPSS channel bypassed; no trip latched
```

```
TEST: SY-102 := 0
```

```
IF ZSO-102 opens within 3 s (vendor) THEN SY-102 := 1
ELSE SY-102 := 1; high alarm "SDV-102 partial stroke failed"
IF ZSO-102 not re-made within 30 s THEN
    high alarm "SDV-102 not returned open"
    record date, result and time to leave the open position
OVERDUE: 92 days since the last pass -> medium alarm
```

A genuine OPSS demand during a test is never delayed: the trip logic de-energizes SY-102 and does not re-energize it.

13. STATION EMERGENCY SHUTDOWN

13.1. CAUSES AND EFFECTS

The station ESD (I-01) isolates the station and stops the heater. Its causes are the four ESD pushbuttons HS-201 to HS-204, the receiving pipeline operator's remote shutdown HS-215, confirmed gas in the analyzer shelter B-101, high-high gas at the B-102 air intake, fire at the line heater (BE-213), and loss of 24 VDC power to the safety PLC.

```
ESD := any of HS-201 to HS-204 or HS-215 open
      OR B-101 confirmed gas
      OR GD-207 >= 40 % LEL for 5 s
      OR BE-213 fire for 3 s
ON ESD (latched):
  SY-101, SY-102, SY-103, SY-106, SY-165, SY-141 := 0    // SDVs close
  HS-150T := 0 (burner trip)
  B-102 beacon and horn on; ESD signal to receiving operator
  BPCS (from status): control valves to 0 %; FIC-131 and LIC-104
    manual at 0 %; heater enable removed; sequences aborted;
    MOVs as they are; consequential alarms suppressed
  no automatic blowdown (manual, per SAF-RPT-005)
```

SDV-106 and SDV-141 are included in the ESD effects, beyond the list in the Basis of Design, because an emergency is no time to keep sending liquid to the atmospheric tank or sample gas into the analyzer shelter. SDV-141 works with a restriction orifice so that even before it closes, a tubing failure in B-101 is limited to a release the shelter ventilation can dilute. Automatic blowdown was not provided: the station is small, unmanned and designed for zero routine emissions, and SAF-RPT-005 assigns blowdown to the responding technician, one section at a time.

13.2. ESD RESET AND RESTART

```
STEP 1  all ESD causes clear: pushbuttons pulled out, HS-215 restored,
        gas below 20 % LEL, BE-213 clear
STEP 2  technician turns key HS-200R at CP-102B: ESD latch reset;
        SDVs stay closed
STEP 3  reopen each SDV at its local station after equalization, in order:
        SDV-103 (HS-103R)  outlet; CKV-171 blocks backflow
        SDV-102 (HS-102R)  OPSS reset permissives apply
        SDV-101 (HS-101R)  inlet; control valves at 0 %, so the
                           station fills but does not flow
        SDV-106 (HS-106R)
        SDV-165 (HS-165R)  requires XS-150 made
        SDV-141            on reset when B-101 is clear
```

STEP 4 restart BMS locally at CP-150 if heater mode is ON
STEP 5 startup permissives (Section 16), then FIC-131 to automatic
with setpoint ramp from 0

Reset does not open any valve by itself. The outlet valve is opened first because CKV-171 blocks backflow from the trunkline, so opening it admits no gas. The inlet is opened last so that the station cannot fill and begin to flow before every downstream valve is proven open.



14. PROCESS TRIPS

Table 14-1 summarizes the process trips in the safety PLC. All latch and reset only locally. The required safety integrity level of each is set in SAF-SRS-001.

Table 14-1: Process Trips

Function	Cause	Safety PLC action	BPCS action	Reset
SIF-02 (I-03)	LSHH-105, V-101 level at 26 in, 2 s	Close SDV-101	Control valves to 0 %; LIC-104 stays in automatic to drain V-101	Level normal, HS-101R
SIF-03 (I-04)	LSLL-106, V-101 level at 3 in, 2 s	Close SDV-106; force-close LCV-104	LIC-104 manual at 0 %	Level above 10 in, HS-106R
SIF-04 (I-05)	LSHH-192, T-101 level at 86.4 in (90 %), 2 s	Close SDV-106; force-close LCV-104	LIC-104 manual at 0 %	Level below 76.8 in, HS-106R

LIC-104 stays in automatic after SIF-02 so that the separator drains while the inlet is closed; the fault that raised the level is then investigated before SDV-101 is reset.

The pig receiver closure interlock I-08 is mechanical and has no input or output. The quick-opening closure carries a pressure warning and locking device that prevents it being released while the barrel is pressurized; the locking sequence requires the barrel vent BDV-102 open, and the technician confirms 0 psig on PI-102 before opening. PT-102A gives SCADA an indication of barrel pressure with a 5 psig alarm but is not part of the interlock.

15. FIRE AND GAS LOGIC

The fire and gas philosophy is set out in SAF-RPT-003. The safety PLC implements it as follows (I-09).

B-101 (GD-205, GD-206)

HIGH either $\geq 20\%$ LEL for 5 s -> high alarm, B-101 beacon
HH UNCONF one $\geq 40\%$ LEL for 5 s, the other $< 20\%$ ->
close SDV-141, isolate B-101 non-rated power, high alarm
CONFIRMED one $\geq 40\%$ LEL AND the other $\geq 20\%$ LEL ->
SDV-141, power isolation, station ESD
FAULT below 3.0 mA: not a trip vote; high alarm; with one detector
faulted, the healthy one at 40 % LEL gives the confirmed action
FSL-208 airflow low: high alarm at 30 s;
B-101 non-rated power isolated after 5 min

B-102 (GD-207 at the air intake)

HIGH 20 % LEL, 5 s -> HVAC off, damper closed, beacon and horn
HIGH-HIGH 40 % LEL, 5 s -> station ESD
XS-212 smoke in B-102 -> emergency alarm, HVAC off, beacon; no ESD
BE-213 fire at the heater (20 mA) for 3 s -> station ESD

Confirmation by a second detector was chosen for B-101 so that a single detector fault or a small calibration gas release does not shut in the station, while the unconfirmed high-high still removes the gas source and ignition sources from the shelter. Smoke in B-102 does not cause an ESD because the control building contains no process gas; a fire there is more likely electrical, and shutting in the station would not help. Fire and gas actions latch; beacons clear on acknowledgement once the cause has cleared.

16. STARTUP, FIRST-OUT AND ALARM MANAGEMENT

16.1. STARTUP PERMISSIVES

The BPCS displays the permissives in Table 16-1 as a checklist (I-15). When all are true the operator places FIC-131 in automatic, and the setpoint ramps from zero to the nomination at 10 MMSCFD/min.

Table 16-1: Station Startup Permissives

No.	Permissive	Signal
1	ESD reset, no safety trip latched	Safety PLC status
2	SDV-101, SDV-102 and SDV-103 open	ZSO-101, ZSO-102, ZSO-103
3	SDV-106 open; SDV-165 open if heater mode ON	ZSC-106, ZSC-165 not made
4	V-101 bypass closed	ZSO-103C not made
5	OPSS healthy: three transmitters healthy, no deviation, no bypass	Safety PLC status
6	One meter run lined up, standby run outlet MOV open, MOV-115 closed	MOV limit switches
7	Flow computer healthy	XA-110
8	Duty control valve available	Section 5 logic
9	Receiving pipeline operator flow permissive	Permissive input
10	No quality shut-in; gas chromatograph healthy or agreed fallback	Shut-in latch, XA-141, PSL-141L
11	V-101 level normal, LIC-104 in automatic	LT-104 between 6 and 20 in
12	24 VDC bus healthy	EI-210A above 22.8 VDC
13	Heater mode correct (advisory; an override is logged)	TT-101, PT-101, PT-134

The V-101 bypass is a permissive because unfiltered gas at the meters degrades custody accuracy, and the Basis of Design allows bypass operation only with the receiving pipeline operator's approval.

16.2. FIRST-OUT

The safety PLC captures the first cause in each group (ESD, OPSS, SIF-02, SIF-03 and SIF-04, fire and gas) within one scan, holds it until reset, and time-stamps all later causes to 10 ms. The BMS keeps its own first-out. The BPCS displays both and forwards them to SCADA and the Owner's historian.

16.3. ALARM MANAGEMENT

Alarms follow ANSI/ISA-18.2 with the four priorities in Table 16-2. Every alarm has a rationalized setpoint, priority and response in INS-LST-003. Response times assume a remote operator at the Owner's gas control center and a field technician on call.

Table 16-2: Alarm Priorities

Priority	Meaning	Target response
Emergency	Safety trip, ESD, fire or confirmed gas	Immediate; call-out and emergency response plan
High	Imminent loss of protection, custody or delivery	15 min
Medium	Equipment problem, degraded operation	1 h
Low	Maintenance and advisory	Next site visit

Analog alarms carry a deadband of 1 % of span. Shelving is done at SCADA with supervisor authorization for at most 24 h. After an ESD or OPSS trip, consequential alarms (low flow, valve position, low downstream pressure) are suppressed for 10 min by state-based suppression, so that the operator sees the cause rather than a flood of effects. Alarms that chatter more than three times in 60 s are reported for rationalization.

17. SAFETY SYSTEM BYPASS MANAGEMENT

Bypasses of safety inputs are needed for testing and repair, but each one reduces protection. The safety PLC therefore enforces the following rules.

- The bypass permit requires the maintenance key HS-200B at CP-102B and a technician log-in at the safety PLC interface. Removing the key removes all bypasses.
- Bypasses are per input channel. SDV solenoid outputs cannot be bypassed while the station is in service; SDVs are tested with their section isolated.
- Only one bypass at a time is allowed per safety function. An OPSS channel bypass degrades the vote to one-out-of-two.
- A bypass lasts at most 8 h (adjustable to 12 h) and is removed automatically at expiry.
- ESD pushbuttons, HS-215 and BE-213 cannot be bypassed. A gas detector may be bypassed only with a portable monitor in place.
- Each bypass raises a medium-priority alarm while active, is logged with user and time, and is reported to the receiving pipeline operator when it affects SIF-01.

18. POWER AND COMMUNICATIONS FAILURE

18.1. POWER FAILURE

The response to each power failure is set out in Table 18-1. The UPS carries the control systems and SDV solenoids for at least 8 h without the generator, as the Basis of Design requires.

Table 18-1: Behavior on Power Failure

Event	Behavior
Utility loss	Automatic transfer to G-101 in about 10 s. 480 V actuators stop and hold position; SDV solenoids, controllers and telecom stay on the 24 VDC UPS. Control resumes on power return. Medium-priority alarm
Generator fails to start	UPS carries control; high-priority alarm. SDVs stay open but cannot be reopened after a trip until 480 V returns, because the hydraulic pumps need it
24 VDC bus low	Alarms at 22.8 VDC (medium) and 21.6 VDC (high). On loss of 24 VDC the safety PLC outputs de-energize and all SDVs close
BPCS restart	Controllers start in manual with outputs initialized to valve position; setpoints restored from retentive memory; no automatic valve moves
Safety PLC restart	All functions come up tripped and require local reset
Flow computer restart	Custody archives retained; power-fail event logged per API 21.1

18.2. COMMUNICATIONS FAILURE

Path supervision, failover timing and polling are defined in INS-RPT-002. The station continues to run safely on loss of any communication path, because every protective function is local. Table 18-2 gives the station response.

Table 18-2: Behavior on Communications Failure

Failure	Behavior
Primary SCADA path lost	Automatic failover to the secondary path (licensed radio or satellite); medium-priority alarm
Both SCADA paths lost for 5 min	Station continues with last setpoints; PIC-134, OPSS and ESD remain active; gas control calls the technician and informs the receiving pipeline operator by phone. An optional communication-loss shut-in timer, disabled by default, can start the quality shut-in ramp (HOLD H-01)
Receiving operator serial link lost	Medium-priority alarm; delivery continues; data back-filled from flow computer archives
Remote shutdown HS-215 circuit open	Station ESD. The loop is normally closed, so a damaged cable fails safe; this was accepted because a false shutdown is preferable to a lost shutdown path

Failure	Behavior
Receiving operator permissive lost	High-priority alarm; quality shut-in ramp after 600 s (HOLD H-14)
Flow computer to BPCS lost	FIC-131 to manual hold; high-priority alarm; custody measurement continues
Chromatograph to flow computer lost	Flow computer uses last good or fixed composition per the agreement; high-priority alarm
BMS serial link lost	Medium-priority alarm; hardwired XA-150 and XL-150 keep control functions
Safety PLC status link lost	High-priority alarm; BPCS holds control valves and inhibits upward ramping; protection unaffected



19. TIME SYNCHRONIZATION AND DATA

A GPS time server in the telecom rack provides network time to the BPCS, safety PLC, flow computer, chromatograph and operator interfaces. The safety PLC takes time only from this local source over its read-only network segment, so that no external connection can reach it. Flow computer clock changes are logged in the API 21.1 event log, and daily correction is kept within the limit set by the interconnect agreement (HOLD H-01).

The flow computer keeps hourly and daily quantity transaction records, the audit trail and the alarm and event logs per API 21.1, with at least 35 days of hourly records held locally. The BPCS buffers SCADA data for at least 7 days during a communication loss and back-fills. Safety PLC sequence-of-events records and the BMS first-out are forwarded to the Owner's historian.



20. SUMMARY AND NEXT STEPS

The station will run unattended under the Owner's remote supervision. The BPCS controls flow to the nomination with a pressure override, switches control valves automatically on failure, runs meter changes and verification as make-before-break sequences, and holds the control valve outlet above the hydrate and dewpoint limits with a pressure-compensated heater cascade. An independent safety PLC provides the OPSS, the process trips, the station ESD and fire and gas logic, all de-energize-to-trip and reset only at the equipment. The burner management system is a SIL 2 package with two diverse flame detectors.

The tightest design margin is the OPSS: with the trip at 1,225 psig and a 4 s stroke, its 5.5 s response fits an 8.9 s process safety time, and that result depends on the extent of the blocked-in trunkline. The next steps are:

1. Confirm the trunkline segment length and valve spacing with the receiving pipeline operator, which sets the OPSS process safety time (HOLD H-04).
2. Obtain vendor data for the actuators, BMS timings and switch settings, and update this narrative and INS-LST-003 (HOLD H-15).
3. Agree the witness, verification, data and point-list requirements with the receiving pipeline operator (HOLD H-01, H-13, H-14).
4. The integrator will prepare the functional design specification and test procedures from this narrative and INS-LST-004 for Owner review before factory acceptance testing.

21. ASSUMPTIONS AND OPEN ITEMS

The assumptions below apply. Items marked for verification must be confirmed before the next issue.

1. Actuator stroke times, BMS timings, the low-fire position and the fuel pressure switch settings are typical values. *Verification required (HOLD H-15).*
2. The receiving trunkline is NPS 24 x 0.344 in X60 with a maximum allowable operating pressure of 1,200 psig, and 1 mile of it can be blocked in downstream of the tap. *Verification required (HOLD H-04).*
3. Meter verification frequency, witness requirements, communication-loss rules and data retention follow the Basis of Design. *Verification required (HOLD H-01).*
4. Gas quality limits are those of the Basis of Design. *Verification required (HOLD H-13).*
5. The receiving pipeline operator's permissive and point list are as assumed in INS-RPT-002. *Verification required (HOLD H-14).*
6. The 30 MMSCFD minimum rate for series verification is to be confirmed by the measurement design (MEA-CAL-002, Measurement Uncertainty Analysis).
7. Initial controller tuning values are starting points to be refined at commissioning.

APPENDIX A. TYPICAL LOOP DIAGRAMS



