

OWNER

SCADA, Communications and Cybersecurity

Report



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

Rev. A, Issued for Review

Date: September 29, 2026

Project: [REDACTED] [REDACTED]



TORUS

[REDACTED] [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 INS-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	Instrumentation and Controls			

CONTENTS

1.	INTRODUCTION	1
1.1.	PURPOSE	1
1.2.	SCOPE	1
1.3.	EXCLUSIONS	1
2.	BASIS AND REFERENCES	2
3.	SYSTEM ARCHITECTURE	3
3.1.	CONTROL SYSTEM LEVELS	3
3.2.	STATION NETWORK	5
3.3.	INTERNAL LINKS	6
4.	SCADA COMMUNICATION PATHS	7
4.1.	PATHS	7
4.2.	POLLING AND REPORT BY EXCEPTION	7
4.3.	FAILOVER	7
5.	SECONDARY RADIO PATH	9
5.1.	DESIGN INPUTS	9
5.2.	CALCULATION	9
5.3.	SENSITIVITY TO PATH LENGTH	10
5.4.	SURVEY AND MAST	11
6.	CELLULAR AND SATELLITE PATHS	13
6.1.	CELLULAR ACCEPTANCE	13
6.2.	SATELLITE LATENCY	13
7.	SCADA DATA VOLUME	14
8.	INTERFACE TO THE RECEIVING PIPELINE OPERATOR	15
8.1.	DEMARCATON	15
8.2.	HARDWIRED POINTS	15
9.	CYBERSECURITY	16
9.1.	PROGRAM	16
9.2.	ZONES AND CONDUITS	16
9.3.	FIREWALL RULES	16
9.4.	SAFETY SYSTEM SEPARATION	17
9.5.	REMOTE ACCESS	17
9.6.	HARDENING, PATCHING, MALWARE PROTECTION AND BACKUP	18
9.7.	MONITORING, PHYSICAL SECURITY AND TIME	18
9.8.	INCIDENT RESPONSE	18
9.9.	COMPLIANCE WITH API 1164 AND TSA MEASURES	18
10.	CYBER TESTING	20



11. CONCLUSIONS AND NEXT STEPS 21

12. ASSUMPTIONS AND HOLDS..... 22

FIGURES AND TABLES

Figure 3-1. Control System and Network Architecture (INS-DWG-001) 4

Figure 5-1. Fade Margin Against Path Length, 900 MHz Secondary Path 11

Table 3-1: Control System Levels and Nodes.....5

Table 3-2: Internal Communication Links 6

Table 4-1: SCADA Communication Paths.....7

Table 5-1: Radio Path Design Inputs 9

Table 5-2: Radio Path Sensitivity to Path Length 11

Table 6-1: Cellular Acceptance Criteria at the Router Port.....13

Table 7-1: SCADA Data Volume.....14

Table 8-1: Hardwired Points at the Demarcation.....15

Table 9-1: Security Zones and Conduits 16

Table 9-2: Firewall Rule Summary 17

Table 9-3: Cybersecurity Compliance Matrix.....18

Table 10-1: Cyber FAT and SAT 20

Table A-1: Modbus Register Template 24

Table B-1: Telecommunications Equipment 27

APPENDICES

APPENDIX A. MODBUS REGISTER TEMPLATE FOR THE RECEIVING PIPELINE OPERATOR 23

APPENDIX B. TELECOMMUNICATIONS EQUIPMENT.....26

1. INTRODUCTION

1.1. PURPOSE

This report defines how the () will communicate with the Owner's supervisory control and data acquisition (SCADA) host and with the receiving pipeline operator, and how the station control systems will be protected against cyber attack. It sets the network architecture, the protocols, the primary and secondary communication paths, the data interface to the receiving pipeline operator and the cybersecurity measures, so that the systems integrator, the telecommunications contractor and the Owner's cybersecurity function can procure, configure and test the system.

1.2. SCOPE

The scope covers the station control network inside the fence, the wide-area links to the Owner SCADA host, the demarcation to the receiving pipeline operator's remote terminal unit (RTU), the secondary radio path budget, the SCADA data volume, and the cybersecurity program elements that the project delivers: asset inventory, zones and conduits, firewall rules, remote access, hardening, monitoring and cyber testing.

1.3. EXCLUSIONS

The following are outside this report:

- the Owner SCADA host, historian and control center network, which are existing Owner systems;
- the receiving pipeline operator's RTU, its communications and its remote shutoff at the tap, which are that operator's scope (HOLD H-14);
- the control functions carried over these links, which are described in INS-RPT-001, Control Philosophy and Functional Narrative;
- the structural design of the antenna mast and its foundation (Volume 5), and grounding and lightning protection of the mast (Volume 6).

2. BASIS AND REFERENCES

The communications basis is set by GEN-DB-001, Basis of Design, Section 9.9: an Owner RTU in control building B-102, a primary cellular path on a private access point name with a virtual private network (VPN), a secondary licensed 900 MHz radio or satellite path, and a hardwired and Modbus demarcation panel to the receiving pipeline operator. Section 9.8 of the basis requires the RTU, safety programmable logic controller (PLC), flow computer and telecommunications equipment to run for 8 hours on the 24 VDC uninterruptible power supply (UPS). The references used are:

1. API Standard 1164, 3rd Edition (2021), Pipeline Control Systems Cybersecurity (clause numbers to be verified against the edition in force).
2. TSA Pipeline Security Guidelines (March 2018, Change 1 April 2021).
3. TSA Security Directive Pipeline-2021-01 and Pipeline-2021-02 series, current revision; these apply only if the Owner has been notified by TSA as a critical pipeline owner or operator (HOLD, Owner).
4. IEC 62443-3-2, 62443-3-3 and 62443-4-2, Security for industrial automation and control systems.
5. IEEE 1815-2012 (DNP3), including Secure Authentication version 5 (SAv5).
6. API MPMS Chapter 21.1, Electronic Gas Measurement.
7. 47 CFR Part 101 (928 to 960 MHz Multiple Address Systems) and Part 90 (clauses to be verified).
8. IEC 61511-1:2016, Clause 8.2.4, security risk assessment for the safety instrumented system.
9. GEN-DB-001, Basis of Design.
10. INS-RPT-001, Control Philosophy and Functional Narrative.
11. INS-LST-002, I/O List.
12. INS-DWG-001, Control System and Network Architecture.
13. INS-DS-010, BPCS RTU/PLC; INS-DS-011, Safety PLC; INS-DS-014, Control Panels, Junction Boxes and UPS Interface.
14. SAF-SRS-001, Safety Requirements Specification.
15. SAF-RPT-005, Emergency Response Plan.

3. SYSTEM ARCHITECTURE

3.1. CONTROL SYSTEM LEVELS

The station control system is organized in the levels of the Purdue reference model so that each security zone contains equipment of one function and trust level. Figure 3-1 shows the architecture and Table 3-1 lists the nodes at each level.

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

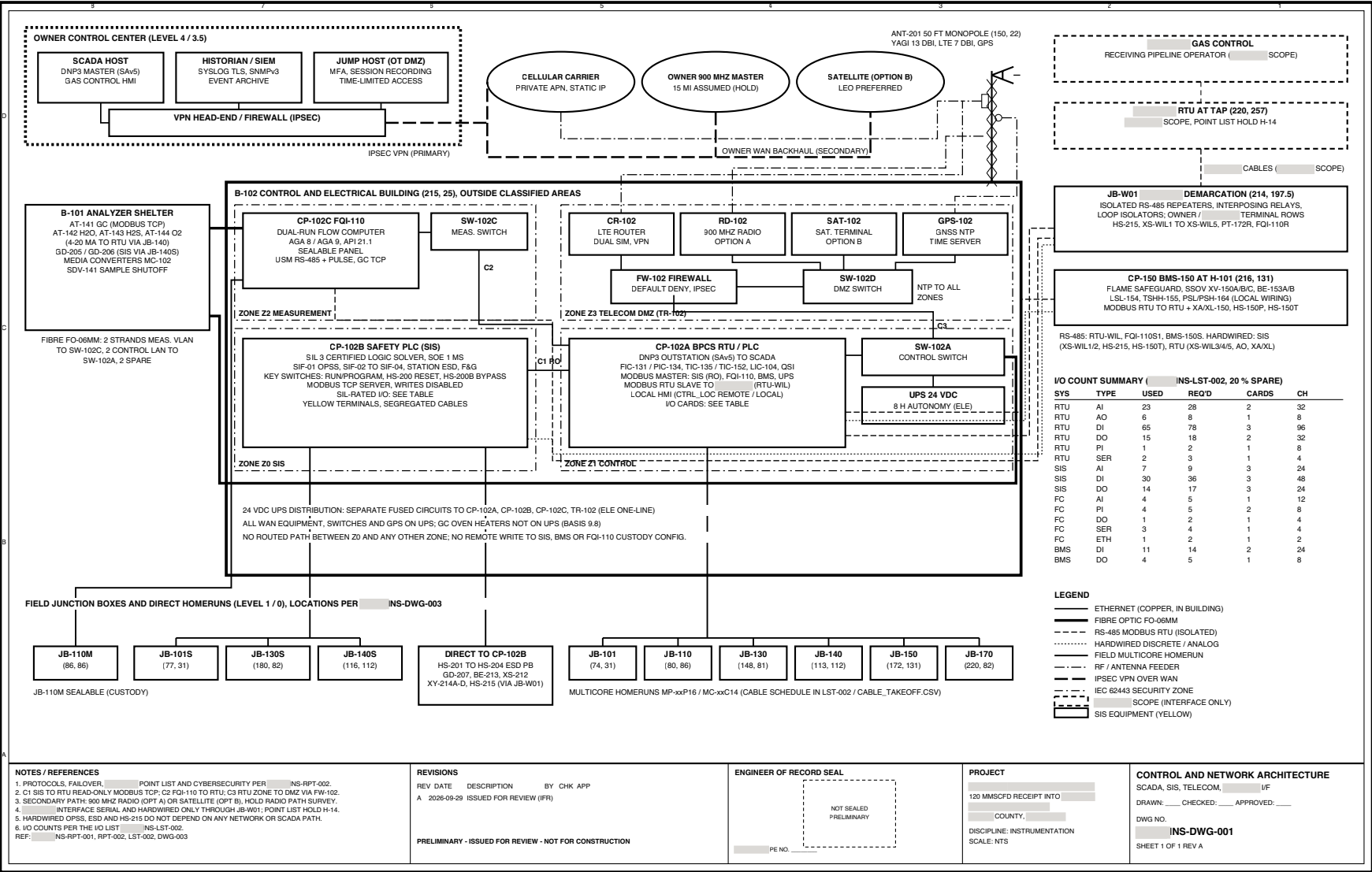


Table 3-1: Control System Levels and Nodes

Level	Node	Location	Function
4	Owner SCADA host, historian and gas control displays	Owner control center	Supervision, nominations, alarm handling, archive
3.5	Owner remote access jump host with multi-factor authentication	Owner control center demilitarized zone (DMZ)	Only path for engineering access
3.5	Station telecom DMZ: firewall FW-102, cellular router CR-102, radio RD-102 or satellite terminal SAT-102, time server GPS-102	Rack TR-102 in B-102	Wide-area termination, VPN, time
3	Basic process control system (BPCS) RTU/PLC with local display	Panel CP-102A in B-102	Control, DNP3 outstation, Modbus server to the receiving pipeline operator
3	Flow computer FQI-110	Panel CP-102C in B-102, sealable	Custody measurement
3	Safety PLC	Panel CP-102B in B-102	Safety instrumented functions (SIFs), emergency shutdown (ESD), fire and gas
2	Gas chromatograph AT-141 and analyzers AT-142 to AT-144	Analyzer shelter B-101	Gas quality
2	Burner management system BMS-150	Panel CP-150 at H-101	Burner management
1 and 0	Field devices through junction boxes	Station	Transmitters, switches, actuators
Interface	Demarcation panel JB-W01	North fence	Hardwired and RS-485 points to the receiving pipeline operator's RTU

3.2. STATION NETWORK

Each zone has its own managed industrial Ethernet switch: SW-102A for the control zone, SW-102C for the measurement zone and SW-102D for the telecom DMZ. The switches are fanless, rated -40 to 75 °C, powered from 24 VDC, and configured with port security, virtual LANs and SNMPv3. The safety PLC shares no switch with any other zone; it connects point to point to a dedicated RTU communication port. This keeps a fault or a flood of traffic in the control network from reaching the safety PLC.

Analyzer shelter B-101 connects to B-102 through one six-strand OM3 armored multimode fiber: two strands carry the measurement network from the gas chromatograph to the flow computer, two carry the analyzer maintenance network in the control zone, and two are spare. Fiber was chosen over copper because the run crosses the classified area between the buildings and fiber carries no lightning or ground-potential difference into either panel.

Addresses are static and recorded in the asset inventory; no dynamic address assignment is used. Serial links are two-wire RS-485, terminated at 120 ohm, with isolated repeaters at every building or panel boundary.

3.3. INTERNAL LINKS

Table 3-2 lists the internal links. Every write from the SCADA host terminates at the RTU; there is no remote write path to the safety PLC, the BMS or the custody configuration of the flow computer.

Table 3-2: Internal Communication Links

Link	Protocol and medium	Data	Direction
Safety PLC to RTU	Modbus TCP; safety PLC as server with write function codes disabled	Status, trips, first-out, OPSS pressures	RTU reads only
Flow computer to RTU	Modbus TCP	Flow, energy, composition, meter diagnostics	RTU reads; writes limited to run status and sampler enable registers
Chromatograph to flow computer	Modbus TCP over fiber	Composition, heating value, relative density	Flow computer reads
Ultrasonic meters to flow computer	Modbus RTU, one RS-485 port per meter, plus dual pulse	Flow and path diagnostics	Flow computer reads
BMS-150 to RTU	Modbus RTU, isolated RS-485	Burner status, first-out, bath temperature	RTU reads; trips are hardwired
UPS to RTU	Modbus TCP (SNMPv3 where offered)	Battery, load, alarms	RTU reads
RTU and flow computer to receiving pipeline operator	Modbus RTU through JB-W01, isolated	Point list template, Appendix A	Operator reads only (HOLD H-14)
RTU to Owner SCADA	DNP3 with SAv5 over IPsec VPN	All SCADA points	Setpoints and commands to the RTU only

4. SCADA COMMUNICATION PATHS

4.1. PATHS

Table 4-1 sets out the three paths. The basis allows the secondary path to be either licensed 900 MHz radio or satellite. This report carries both, because the choice depends on a radio path survey and on the Owner's radio network, neither of which is available yet (HOLD, Owner). The telecom rack and the mast are sized for either option.

Table 4-1: SCADA Communication Paths

Path	Technology	Role
Primary	LTE or 5G router, dual SIM on two carriers where coverage allows, Owner private access point name with static address, IPsec VPN to the Owner head-end	Normal polling and engineering access
Secondary, option A	Licensed 928 to 960 MHz radio, 12.5 kHz channel, 19.2 kbps, to an Owner master site	Automatic failover; preferred if the path survey passes
Secondary, option B	Low earth orbit (LEO) satellite terminal, or L-band geostationary (GEO) where LEO is not available, with IPsec VPN	Automatic failover if no radio path exists

4.2. POLLING AND REPORT BY EXCEPTION

The RTU will act as the DNP3 outstation. Alarms and trips are reported as Class 1 events, status changes as Class 2 and analog changes beyond deadband as Class 3. The SCADA host will poll for events every 60 s and perform a Class 0 integrity poll every 15 minutes, and immediately after a path change or an outstation restart. This gives the controller data no more than 60 s old while using about one quarter of the traffic of a 60 s integrity poll. Analog deadbands are 0.5 % of span for pressure, flow and temperature and 1 % for analyzer values. Custody quantities are read from the flow computer's hourly records, not from live analogs, so that SCADA and the custody record cannot disagree. Setpoint and command writes use DNP3 select-before-operate with SAV5 challenge, and each command is logged with the operator identity from the SCADA host.

4.3. FAILOVER

The router monitors the VPN on the primary path with dead peer detection every 30 s. If the primary path is lost for 90 s (three missed replies) and the secondary path is healthy, the router moves SCADA traffic to the secondary interface and raises a medium-priority alarm. The SCADA host then performs an integrity poll and stretches the integrity interval to 60 minutes, while keeping 60 s event polling, because the radio channel is narrow. Engineering remote access is suspended on the secondary path; only SCADA polling is carried. The router returns to the primary path after it has been healthy for a continuous 10 minutes, which prevents the path from flapping. If both paths are lost for 5 minutes, the RTU sets a communications-lost status, holds the last setpoints, buffers events and archives for at

least 7 days for back-fill, and applies the communications-loss actions of INS-RPT-001 (HOLD H-01). The hardwired safety functions (the overpressure shutdown system (OPSS), the station ESD and the receiving pipeline operator's remote shutdown HS-215) do not depend on any communication path.



5. SECONDARY RADIO PATH

5.1. DESIGN INPUTS

TORUS prepared a link budget for option A so that the mast height and radio equipment could be fixed for the estimate. The master site, the terrain and the clutter are assumed; the budget will be repeated with the surveyed profile (HOLD, site survey). The inputs are listed in Table 5-1.

Table 5-1: Radio Path Design Inputs

Input	Value	Source
Station location and ground elevation	34.95 N, 97.93 W; 1,150 ft MSL	GEN-DB-001 (HOLD H-02)
Master site	15 mi at 045° true; ground 1,250 ft MSL; 200 ft tower	Assumed (HOLD, Owner radio network)
Frequency	952 MHz	Assumed channel in the 928 to 960 MHz band
Highest terrain near midpoint, plus clutter	1,180 ft MSL plus 30 ft	Assumed (HOLD, path survey)
Effective earth radius factor, required clearance	k = 4/3; 0.6 of the first Fresnel zone	Common practice for SCADA paths
Transmitter power, receiver sensitivity	2 W (5 W capable); -104 dBm at 19.2 kbps, bit error rate 10 ⁻⁶	Typical, confirm with vendor data (HOLD H-15)
Antennas	13 dBi Yagi at the station; 9 dBi omnidirectional at the master	Assumed
Station feeder	7/8 in foam-dielectric hardline, 1.2 dB/100 ft, 200 ft (50 ft on the mast plus 150 ft buried to B-102)	Typical (HOLD H-15)
Master feeder	4.4 dB/100 ft, 230 ft	Assumed, conservative (HOLD, Owner)
Connectors and arrestor	0.5 dB and 0.2 dB per end; 2 dB miscellaneous	Allowance
Multipath factors	a = 1 (average terrain), b = 0.25 (average inland climate), mean annual temperature 60 °F	Vigants-Barnett method

5.2. CALCULATION

The free-space path loss, with distance d in statute miles and frequency f in MHz, is:

$$L_{fs} = 36.58 + 20\log_{10} d + 20\log_{10} f = 36.58 + 23.52 + 59.57 = 119.67 \text{ dB}$$

At the path midpoint ($d_1 = d_2 = 7.5$ mi) the first Fresnel zone radius and the earth bulge are:

$$r_1 = 72.1 \sqrt{\frac{d_1 d_2}{f_{\text{GHz}} d}} = 72.1 \sqrt{\frac{7.5 \times 7.5}{0.952 \times 15}} = 143.1 \text{ ft}, \quad h = \frac{d_1 d_2}{1.5 k} = \frac{7.5 \times 7.5}{1.5 \times 1.333} = 28.1 \text{ ft}$$

The ray must pass at or above $1,180 + 30 + 28.1 + 0.6(143.1) = 1,324$ ft MSL at the midpoint. With the master antenna top at 1,450 ft MSL, the station antenna top must be at least 1,198 ft MSL, which is 48 ft above grade. A 50 ft mast was selected; it gives a midpoint clearance of 86.9 ft, or 0.61 of the first Fresnel zone.

The received level at the master, with station feeder loss $L_r = 3.10$ dB and master feeder loss $L_m = 10.82$ dB, is:

$$P_{rx} = P_{tx} - L_r + G_r - L_{fs} + G_m - L_m - L_{misc}$$

$$P_{rx} = 33.01 - 3.10 + 13.0 - 119.67 + 9.0 - 10.82 - 2.0 = -80.6 \text{ dBm}$$

The fade margin is $F = -80.6 - (-104.0) = 23.4$ dB, above the 20 dB minimum that TORUS applies to SCADA paths. The Vigants-Barnett outage probability during the fading season, with D in miles and f in GHz, is:

Vigants-Barnett, non-diversity outage

$$U = a b 2.5 \times 10^{-6} f_{\text{GHz}} D^3 10^{-F/10} = 1.0(0.25)(2.5 \times 10^{-6})(0.952)(15^3)10^{-2.342} = 9.1 \times 10^{-6}$$

The fading season length is $T_0 = (t/50) \times 8.0 \times 10^6$ s, where t is the mean annual temperature in °F. For $t = 60$ °F, $T_0 = 9.6 \times 10^6$ s, and the annual outage is $UT_0 = 88$ s, an availability of 99.9997 %.

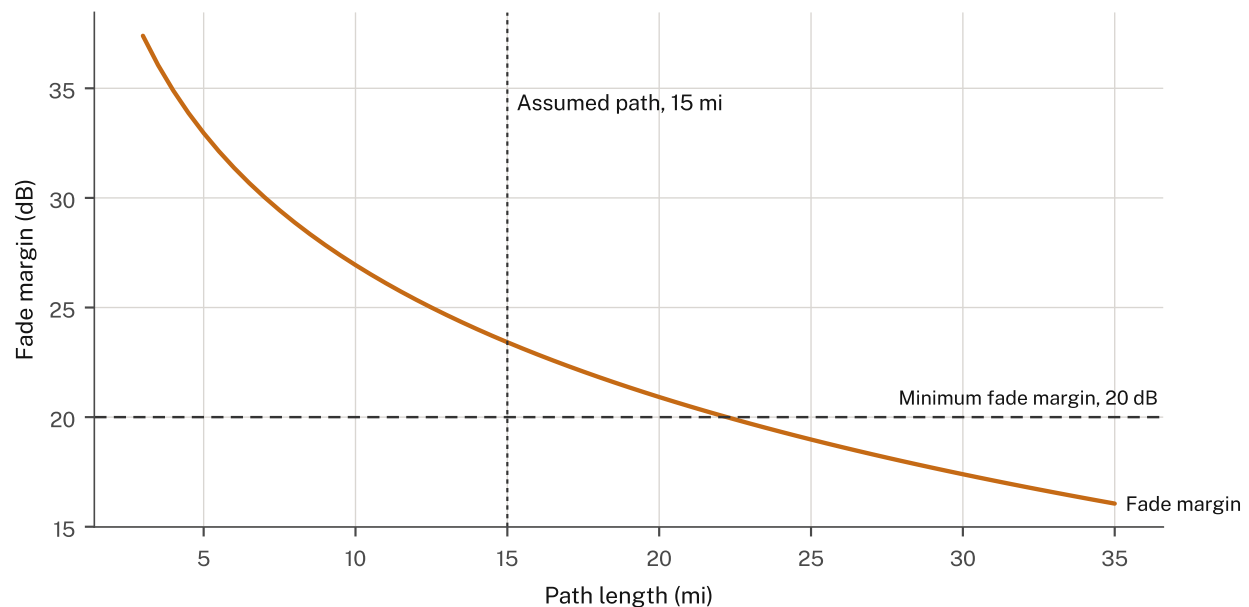
A 50 ft mast gives 0.61 first-Fresnel-zone clearance over the assumed terrain. The fade margin is 23.4 dB and the predicted multipath outage is about 90 s a year.

The effective isotropic radiated power at the station is $33.01 - 3.10 + 13.0 = 42.9$ dBm (19.5 W). It will be checked against the station license and 47 CFR 101.113 once the license is applied for. The radio is set to 2 W for this reason; the full 5 W is held in reserve for a longer path if the license allows.

5.3. SENSITIVITY TO PATH LENGTH

Because the master site is not yet fixed, TORUS evaluated the same equipment over a range of path lengths. Figure 5-1 shows that the fade margin falls to the 20 dB minimum at about 22 mi, and Table 5-2 gives the values.

Figure 5-1. Fade Margin Against Path Length, 900 MHz Secondary Path



Note 1: 2 W radio, 13 dBi Yagi at the station, 9 dBi omnidirectional antenna at the master site, receiver sensitivity -104 dBm at 19.2 kbps. The 50 ft mast is held constant; a longer path also needs a new clearance check.

Table 5-2: Radio Path Sensitivity to Path Length

Path length (mi)	Path loss (dB)	Received level (dBm)	Fade margin (dB)	Annual outage (s)	Meets 20 dB
5	110.1	-71.0	33.0	0.4	Yes
10	116.2	-77.1	26.9	12	Yes
15 (assumed)	119.7	-80.6	23.4	88	Yes
20	122.2	-83.1	20.9	370	Yes
25	124.1	-85.0	19.0	1,130	No; raise power to 5 W
30	125.7	-86.6	17.4	2,810	No; repeater or satellite

5.4. SURVEY AND MAST

Before any radio is purchased, the telecommunications contractor will run a path profile study from 1 arc-second terrain data with land-cover clutter, then confirm it in the field with a test shot at the final coordinates (HOLD H-02). If the terrain is lower than assumed, the mast can drop to 30 ft, which is still needed for the cellular antenna. The mast, ANT-201, is a 50 ft breakpoint monopole located outside all classified areas, with its own ground ring bonded to the station grounding grid and coaxial ground kits

at the top, at the base and at the building entry per NFPA 780 and NFPA 70 Article 810. The feeder runs about 150 ft buried to B-102, which is why 7/8 in hardline was selected over smaller cable. If the path fails, option B satellite becomes the secondary path without any change to the rack.



6. CELLULAR AND SATELLITE PATHS

6.1. CELLULAR ACCEPTANCE

The cellular antenna is a 7 dBi outdoor MIMO antenna on ANT-201, fed by 200 ft of 7/8 in hardline with a loss of 4.7 dB. A signal of -100 dBm at the router port therefore needs about -102 dBm at the antenna. The contractor will survey both candidate carriers for 24 hours at the mast location and height, and the router will be accepted against Table 6-1. If neither carrier meets the minimum, the secondary technology becomes the primary path and the Owner will decide whether a further path is needed (HOLD, Owner).

Table 6-1: Cellular Acceptance Criteria at the Router Port

Metric	Minimum	Target
Reference signal received power (RSRP)	-100 dBm	-90 dBm
Reference signal received quality (RSRQ)	-12 dB	-9 dB
Signal to interference plus noise ratio (SINR)	5 dB	13 dB
VPN round trip to the Owner head-end, 95th percentile	250 ms	100 ms
Tunnel availability over a 7-day soak test	99.5 %	99.9 %

6.2. SATELLITE LATENCY

The one-way propagation delay through a LEO satellite at about 550 km is at least 3.7 ms (round trip typically 25 to 60 ms with processing), and through a GEO satellite at 35,786 km at least 239 ms (round trip typically 600 to 700 ms). DNP3 application timeouts on the satellite path will be set to 5 s for LEO and at least 10 s for GEO. The terminal needs a clear view of the sky, a non-penetrating mount, ice protection for the 0.5 in radial ice of the basis, and UPS power of typically 50 to 100 W (HOLD H-15).

7. SCADA DATA VOLUME

TORUS estimated the SCADA database from the hardwired I/O of INS-LST-002 and an allowance for internal points (flow computer run and station values, controller setpoints and outputs, safety PLC status, BMS, UPS and communications diagnostics, alarm and sequence flags). The result, 151 analogs, 416 binaries and 11 counters, is an estimate for the integrator to finalize. Table 7-1 gives the traffic; the total is about 1.35 MB a day, so a 1 GB a month service plan has ample margin for firmware updates and engineering sessions.

Table 7-1: SCADA Data Volume

Item	Value
Integrity response, including link and IPsec overhead	2,048 bytes every 15 minutes (96 a day)
Event poll, every 60 s	376 bytes response plus 172 bytes request
Daily SCADA traffic	1.00 MB
VPN keep-alive	0.35 MB a day
Total	1.35 MB a day, about 41 MB a month
API 21.1 archive upload	17.5 kB a day
Plan size with a threefold margin	125 MB a month; a 1 GB a month plan is specified
900 MHz channel loading at 19.2 kbps	0.85 s per integrity poll; average 125 bit/s, 0.7 % of the channel

8. INTERFACE TO THE RECEIVING PIPELINE OPERATOR

8.1. DEMARCATION

Panel JB-W01 at the north fence is the physical demarcation between the Owner's systems and the receiving pipeline operator's RTU. Owner cables from B-102 and the operator's cables terminate on separate, labeled terminal rows. Every signal that crosses the demarcation passes through an isolating device: interposing relays for discrete points, galvanic isolators for analog repeats and isolated repeaters for the Modbus links. No Ethernet or routed connection is made between the two networks. This keeps a fault, a surge or a compromise on one side from reaching the other. If the operator later requires Ethernet, it will be added only through a dedicated firewall conduit after a joint risk assessment.

8.2. HARDWIRED POINTS

The hardwired signals in Table 8-1 are a template pending the operator's point list (HOLD H-14). The remote shutdown and the flow permissive are hardwired only, so that neither can be affected by a data link fault. The operator has no Modbus write access; any write function code received on either port is rejected and logged. The Modbus register template is in Appendix A.

Table 8-1: Hardwired Points at the Demarcation

Point	Owner system	Owner I/O	Description	State
RTU port	RTU	Serial	RTU Modbus RTU server port	RS-485
FQI-110 port	Flow computer	Serial	Flow computer Modbus RTU server port	RS-485
XS-WIL1	Safety PLC	DO	Station ESD active	0 = ESD
XS-WIL2	Safety PLC	DO	OPSS trip, SDV-102 closed	0 = trip
XS-WIL3	RTU	DO	SDV-103 closed, station not delivering	1 = closed
XS-WIL4	RTU	DO	Gas quality shut-in in progress	1 = active
XS-WIL5	RTU	DI	Flow permissive from the receiving pipeline operator	1 = permit
HS-215	Safety PLC	DI	Remote shutdown from the receiving pipeline operator	0 = shutdown
PT-172R	RTU	AO	Outlet pressure repeat, 0 to 2,000 psig	4-20 mA, isolated
FQI-110R	RTU	AO	Station flow repeat, 0 to 150 MMSCFD	4-20 mA, isolated

9. CYBERSECURITY

9.1. PROGRAM

The Owner's pipeline cybersecurity program under API 1164 applies to the station. The project will deliver an asset inventory, a zone and conduit model, a cybersecurity risk assessment to IEC 62443-3-2 that includes the security risk assessment of the safety instrumented system required by IEC 61511-1 Clause 8.2.4, hardened configurations, documented firewall rules and cyber test records. The RTU and safety PLC are specified with IEC 62443-4-2 security level 2 capability (INS-DS-010 and DS-011), and the system targets security level 2 under IEC 62443-3-3. Level 2 was chosen because it protects against intentional attack with simple means, which matches the threat to an unmanned rural station, while higher levels would limit the product choice without a corresponding reduction in risk.

9.2. ZONES AND CONDUITS

Table 9-1 defines the zones and conduits. The safety system is placed in its own zone with a single read-only conduit because a compromise of the safety PLC is the only cyber event that could defeat the overpressure protection of the receiving pipeline.

Table 9-1: Security Zones and Conduits

Zone or conduit	Members	Target level	Rules
Z0 Safety	Safety PLC CP-102B and its engineering port	SL 2, SL 3 where the product allows	No routed connection; one conduit (C1, read-only Modbus TCP to the RTU); program changes only locally with the key switch in PROGRAM
Z1 Control	RTU CP-102A, local display, BMS-150 (serial), UPS, B-101 maintenance network	SL 2	Conduits C1, C2 and C3
Z2 Measurement	Flow computer FQI-110, chromatograph AT-141, meter electronics (serial)	SL 2	Conduit C2 to the RTU with an allowed register list; conduit C5 to the receiving pipeline operator (serial only)
Z3 Telecom DMZ	FW-102, CR-102, RD-102 or SAT-102, GPS-102	SL 2	Conduit C3 to Z1 through FW-102; conduit C4 to the Owner wide-area network (IPsec)
C5 Receiving pipeline operator	JB-W01 relays and isolated RS-485	Not applicable	Serial and hardwired only; read-only for the operator
C6 Remote access	Owner jump host to Z1 and Z2 over the VPN	Not applicable	Multi-factor, time-limited, recorded

9.3. FIREWALL RULES

Firewall FW-102 denies all traffic in both directions by default. Table 9-2 lists the only permitted flows.

Table 9-2: Firewall Rule Summary

No.	Source	Destination	Service	Action
1	Owner SCADA front-end (fixed address, via IPsec)	RTU	DNP3 TCP 20000 with SAV5	Allow
2	Owner jump host (via IPsec)	RTU, flow computer, chromatograph engineering ports	Vendor engineering ports, HTTPS	Allow only during an approved session
3	GPS-102	All zones	NTP, UDP 123	Allow
4	RTU, flow computer, switches	Owner log collector	Syslog over TLS 6514, SNMPv3 traps	Allow, outbound only
5	Owner patch repository	Jump host staging share	HTTPS	Allow on schedule
6	Station	Internet	Any	Deny; private access point name, no split tunnel
7	Any	Any	Any	Deny and log

9.4. SAFETY SYSTEM SEPARATION

The safety PLC is on its own segment with a point-to-point link to a dedicated RTU port. It acts as a Modbus TCP server with all write function codes disabled in its configuration, and its address list admits only the RTU. A hardware key switch on CP-102B (RUN and PROGRAM) enables program changes; it is normally locked in RUN, and its position is reported to SCADA as a medium-priority alarm when in PROGRAM. Application changes are made only at CP-102B under management of change, per SAF-SRS-001. The safety system bypass permissive is a local key switch and cannot be set from SCADA.

9.5. REMOTE ACCESS

All remote access passes through the Owner's jump host in the Owner operational technology DMZ, with multi-factor authentication. No vendor will have a direct connection, modem or cloud agent at the station. Each session is requested and approved for a task, enabled for a fixed window (4 hours by default) and recorded on the jump host. Vendor accounts are named, disabled when not in use, and shared accounts are prohibited; default passwords are changed at the factory acceptance test. Remote access is suspended while the station is on its secondary path. Changes to the custody configuration of the flow computer are made only with the receiving pipeline operator's witness and are recorded in the API 21.1 event log (HOLD H-01).

9.6. HARDENING, PATCHING, MALWARE PROTECTION AND BACKUP

At the factory acceptance test the integrator will disable unused services and ports, remove default accounts, set role-based access (viewer, operator, technician, engineer, administrator), apply the Owner's password policy, set a 15 minute session timeout on the local display and block unused USB ports. Only vendor-validated patches will be applied; the Owner reviews security advisories monthly and patches under management of change at the next maintenance window. The local display and any Windows host run application allowlisting, and portable media are scanned before use on site. Configurations of the RTU, safety PLC, flow computer, chromatograph, BMS, switches, firewall and router are backed up after the factory test, after the site test and after every change, stored offline by the Owner with hash values, and restored in a test once a year.

9.7. MONITORING, PHYSICAL SECURITY AND TIME

The firewall, router, switches, RTU and flow computer send syslog and SNMPv3 traps to the Owner's security monitoring, which alerts on failed logins, configuration changes, new devices on a switch port, VPN sessions outside approved windows, the safety PLC key switch in PROGRAM, and a building door opened (ZS-211A or ZS-211B) during an unscheduled session. The fence, locked gates, locked panels and intrusion switches ZS-211A to ZS-211F are reported to SCADA; the flow computer panel is sealable (HOLD H-01). GPS-102 provides stratum 1 time over NTP to all zones, with the SCADA host as a backup source for the RTU only; loss of satellite lock for 24 hours raises an alarm, and time corrections to the flow computer are logged per API 21.1.

9.8. INCIDENT RESPONSE

Cyber incidents are handled under the Owner's cybersecurity incident response plan, which is linked to SAF-RPT-005, Emergency Response Plan, for loss of SCADA, unexplained commands or setpoint changes, and safety PLC key switch alarms. The default response to a suspected compromise is to disconnect the router, place the station in local control with a technician on site, and rely on the hardwired OPSS and ESD, which depend on no network. Reporting to the Cybersecurity and Infrastructure Security Agency applies if the Owner is covered by the TSA directives (HOLD, Owner).

9.9. COMPLIANCE WITH API 1164 AND TSA MEASURES

Table 9-3 maps the principal requirement areas of API 1164 and the TSA measures to the station design. The TSA security directives apply only if the Owner has been notified (HOLD, Owner); the measures are applied in any case as good practice.

Table 9-3: Cybersecurity Compliance Matrix

Requirement area	API 1164 area	TSA measure	Station measure
Asset inventory	Asset management	Baseline measures	Inventory of devices, firmware, addresses and serial numbers at the site test

Requirement area	API 1164 area	TSA measure	Station measure
Risk assessment	Risk assessment	Cybersecurity assessment program	Zone and conduit assessment including the safety system
Segmentation	Network architecture	Segmentation policies and controls	Zones Z0 to Z3; default-deny firewall; no IT connection
Access control	Identity and access management	Access control, multi-factor authentication	Role-based named accounts; multi-factor jump host
Remote access	Remote access	Access control	Time-limited, recorded sessions; no vendor direct access
Monitoring	Monitoring and detection	Continuous monitoring and detection	Syslog and SNMP to Owner monitoring; port security; intrusion switches
Patching and malware	Vulnerability management	Reduce exploitation of unpatched systems	Monthly advisory review; allowlisting; media scanning
Backup and recovery	Recovery	Incident response plan	Offline backups; annual restore test
Incident response	Incident response	Incident response plan and reporting	Owner plan linked to the station Emergency Response Plan
Third-party connection	Third-party connections	Segmentation	Receiving pipeline operator on serial and hardwired links only
Safety system	Safety system considerations	Not specific	Separate zone, read-only conduit, key switch

Note 1: Clause numbers in API 1164 and section numbers in the TSA documents are to be verified against the editions in force at the time of the risk assessment.

10. CYBER TESTING

Each measure will be demonstrated at the factory acceptance test (FAT), the site acceptance test (SAT) or both, as set out in Table 10-1.

Table 10-1: Cyber FAT and SAT

Test	FAT	SAT
Asset inventory and firmware versions match the record	Yes	Yes
Default accounts removed; role access and password policy applied	Yes	Yes
Unused ports and services disabled (port scan of each device from each zone)	Yes	Yes
Each allowed firewall rule works; default deny verified; logs received	Yes	Yes
Modbus writes to the safety PLC rejected and logged	Yes	Yes
Safety PLC key switch position reported	Yes	Yes
DNP3 SAV5: unauthenticated command rejected; key change	Yes	Yes
Write codes on the demarcation ports rejected; isolation verified	Yes	Yes
Failover to the secondary path and back, with timing	No	Yes
Jump host multi-factor login, session expiry and recording	No	Yes
Alerts for failed login, configuration change and new device	Yes	Yes
Backup and restore of each device	Yes	No
All devices within 100 ms of GPS-102	No	Yes
Cellular survey and radio path acceptance	No	Yes

11. CONCLUSIONS AND NEXT STEPS

The station will use a dual-carrier cellular primary path with a licensed 900 MHz radio or a satellite secondary, polled by DNP3 with Secure Authentication, carrying about 1.35 MB a day. Over the assumed 15 mi path a 50 ft mast gives adequate clearance and a 23.4 dB fade margin, with a predicted multipath outage of about 90 s a year; the same equipment remains adequate up to about 22 mi. The safety system sits in its own zone with a single read-only conduit, the receiving pipeline operator is connected only through isolated serial and hardwired signals, and all remote access passes through the Owner's multi-factor jump host.

The next steps are: the Owner fixes the master site and applies for the radio license; the telecommunications contractor runs the path profile and cellular surveys; the receiving pipeline operator issues its point list (HOLD H-14); and the integrator performs the zone and conduit risk assessment before the factory acceptance test.

12. ASSUMPTIONS AND HOLDS

1. The receiving pipeline operator's point list, serial settings, word order and demarcation hardware are to be confirmed (HOLD H-14, receiving pipeline operator).
2. Witness rights, time-correction limits, data retention and communications-loss rules follow the interconnect agreement (HOLD H-01, Owner and receiving pipeline operator).
3. The Owner master site, tower and frequency license are assumed (HOLD, Owner).
4. Terrain profile, clutter and cellular coverage are assumed pending survey (HOLD, telecommunications contractor).
5. Radio, router and terminal performance values are typical and are to be confirmed with vendor data (HOLD H-15).
6. Applicability of the TSA security directives depends on TSA notification of the Owner (HOLD, Owner).
7. Final site coordinates are to be confirmed by survey (HOLD H-02).



APPENDIX A. MODBUS REGISTER TEMPLATE FOR THE RECEIVING PIPELINE OPERATOR



Table A-1 is a template only. Registers, scaling, word order and polling are set by the receiving pipeline operator's point list (HOLD H-14). Floating-point values are IEEE 754 32-bit numbers in two consecutive holding registers, high word first (to be confirmed). Server 1 is the RTU and server 2 is the flow computer. Serial settings are 9,600 or 19,200 baud, 8 data bits, no parity, 1 stop bit, two-wire (to be confirmed).

Table A-1: Modbus Register Template

Register	Server	Point	Description	Units	Type
40001	2	FR_STN	Station flow rate, corrected	Mscf/h	Float
40003	2	ER_STN	Station energy rate	MMBtu/h	Float
40005	2	VOL_TDY	Volume, current contract day	Mscf	Float
40007	2	VOL_YDY	Volume, previous contract day	Mscf	Float
40009	2	NRG_TDY	Energy, current contract day	MMBtu	Float
40011	2	NRG_YDY	Energy, previous contract day	MMBtu	Float
40013	2	P_MTR	Metering pressure, duty run	psia	Float
40015	2	T_MTR	Metering temperature, duty run	°F	Float
40017	2	HHV	Gross heating value, dry	Btu/scf	Float
40019	2	SG	Real relative density	none	Float
40021 to 40043	2	C1 to C6+, N2, CO2	Composition, 12 components	mol %	Float
40045	1	P_OUT	Station outlet pressure	psig	Float
40047	1	T_OUT	Delivery temperature	°F	Float
40049	1	H2O	Water vapor	lb/ MMscf	Float
40051	1	H2S	Hydrogen sulfide	ppmv	Float
40053	1	O2	Oxygen	ppmv	Float
40055	1	CO2	Carbon dioxide, repeat of chromatograph	mol %	Float
40057	1	INERTS	Carbon dioxide plus nitrogen	mol %	Float
40059	1	FIC_SP	Nomination setpoint in force	MMSCFD	Float
40061	1	STS_WORD1	Bit-packed: SDV positions, meter valves, run in service, series test active	none	Unsigned 16
40062	1	STS_WORD2	Bit-packed: ESD active, OPSS trip, quality shut-in, heater mode, communications loss	none	Unsigned 16
40063	1	ALM_WORD1	Bit-packed gas quality alarms	none	Unsigned 16

Register	Server	Point	Description	Units	Type
40064	1	ALM_WORD2	Bit-packed measurement alarms	none	Unsigned 16
40065	2	TS_LAST_HR	Time stamp of the last hourly record	s (UNIX)	Unsigned 32

Note 1: Metering pressure is reported in psia because the custody pressure transmitters PT-111 and PT-121 are absolute-pressure instruments.



APPENDIX B. TELECOMMUNICATIONS EQUIPMENT



Table B-1 lists the telecommunications equipment carried in the instrumentation material take-off.

Table B-1: Telecommunications Equipment

Tag	Quantity	Description
TR-102	1	Telecom rack, 19 in, 42U, lockable front and rear doors, in B-102
FW-102	1	Industrial firewall, four ports minimum, IPsec, 24 VDC, IEC 62443-4-2 SL 2 capable
CR-102	1	Industrial LTE/5G router, dual SIM, 2 x 2 MIMO, IPsec, 24 VDC
RD-102	1	Licensed 928 to 960 MHz data radio, 12.5 kHz, 19.2 kbps, 5 W capable (option A)
SAT-102	1	LEO satellite terminal with pole mount (option B, priced as an alternate)
GPS-102	1	GPS time server with antenna, 24 VDC
SW-102A, C, D	3	Managed industrial Ethernet switches, 8 ports including 2 SFP, 24 VDC
MC-102	4	Fiber media converters, two in B-101 and two in B-102
Radio antenna	1	13 dBi nine-element Yagi, 896 to 960 MHz
LTE antenna	1	7 dBi outdoor MIMO antenna, 698 to 3,800 MHz
ANT-201	1	50 ft breakpoint monopole, galvanized, TIA-222-H, vendor designed
Radio feeder	200 ft	7/8 in foam-dielectric hardline, 50 ft on the mast and 150 ft buried
LTE feeders	2 x 200 ft	7/8 in foam-dielectric hardline
GPS lead	40 ft	GPS antenna coaxial cable
Arrestors	4	Coaxial lightning arrestors (radio 1, LTE 2, GPS 1)
Ground kits	6	Coaxial ground kits
RS-485 repeaters	4	Isolated repeaters (JB-W01 2, CP-150 1, spare 1)
Patch lot	1	Patch cords, fiber jumpers, 24 VDC rack power distribution