SYMBEEO

PUBLIC

DESIGN STUDY

Pipeline OT that keeps running with IT cut off: TSA Security Directive Pipeline-2021-02G segmentation for 55 stations and terminals

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Security	Energy	Liquids pipeline operator
DOCUMENT	**VERSION**	**DATE**
SEC-008	1.0	Oct 22, 2026

WRITTEN BY

David Morgan, Principal Security Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	SEC-008	Version	1.0
Issued	Oct 22, 2026	Status	Issued by Symbeeo
Classification	Public	Capability	Security
Industry	Energy	Author	David Morgan
Role	Principal Security Architect		
Credentials	CCISO, CISSP, CISSP-ISSEP, CISM, CISA, CRISC, PMP, CCSP, Adopting Zero Trust (Forrester)		
Approval	Approved by Edwin Ozer, Founder, Oct 22, 2026. Issued by Symbeeo, Oct 22, 2026. Design study: every figure is vendor-published, a design target or a marked assumption.		
Sign-off	"An engagement under this design is signed by the practice lead before any build proceeds."		

Contents

1 · Scope 3
1c · Public implementations this design follows 4
2 · Requirements register 4
3 · Architecture overview 6
4 · Design by subsystem 6
5 · Failure behavior 7
6 · Limits 8
7 · Lessons learned 8
8 · The author 8

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] figure or clause read from the regulator's, standards body's or vendor's own current page or document on Oct 22, 2026, or carried from a Symbeeo document that read it, where the text names that document · [S*] figure from a page summary or a reseller's copy where the owner's own page could not be opened · [A] assumption about the typical buyer, to be confirmed by the signing engineer · [T] design target taken from the design's stated outcome or derived from it. Every figure carries one tag. No figure comes from any prior engagement, file or asset. A row with more than one tag is counted once: as a published figure if any tag is [S] or [S*], otherwise as an assumption if any tag is [A], otherwise as a design target.

Table 1. Revision history

Date	Version	Change
Oct 22, 2026	1.0	First issue.

1 · Scope

Who it is for. The CISO and the head of pipeline control at an operator TSA has designated as critical, who must show the agency that the pipeline keeps moving product if the corporate network is lost to ransomware, and who knows the hard part is not the firewall but the billing, scheduling and measurement links nobody has written down.

Typical buyer [A]. A US liquids pipeline operator: 2,100 km of crude and refined-products lines, 46 unmanned pump stations, 9 terminals and tank farms, one control center and one backup control center 480 km apart. SCADA at the control centers polls every station over a private OT WAN from two carriers. Corporate IT — ERP, batch scheduling and shipper nominations, custody-transfer accounting, email and the security operations center — runs from headquarters, which shares a building with the primary control center. Today station OT and corporate IT meet at 14 places, five of them undocumented.

What is in. The IT–OT interdependency list and the external-connection list the directive asks for; the zone model; one OT DMZ per control center as the only IT–OT path; the station and terminal firewalls; remote access and its revocation; continuous monitoring inside OT; the islanding test that proves OT runs with IT cut off. **What is out.** Safety instrumented systems, which stay without a routable connection; the SCADA application itself; the TSA-approved Cybersecurity Implementation Plan, incident response plan and assessment program as documents (this design supplies their network evidence); CIP-007-style patching; physical security.

Assumptions. Fortinet is the security vendor at stations and in the OT DMZ, FortiOS 7.6 the baseline, as in SRA-SEC-001 [A]. The operator's TSA-approved implementation plan already names segmentation as the measure this design delivers [A]. The OT WAN carries no IT traffic today and none after [A]. Station power and the OT WAN are outside this document and assumed available during the islanding test [A].

Related documents, read Oct 22, 2026.

- SRA-SEC-001, SDD-SEC-001, STP-SEC-001 — this capability's reference architecture, design and test plan (R4, R11, R12 there; FortiGate 200G figures in R7)
- SEC-007 — FortiAnalyzer 1000G figures, read Sep 25, 2026 from the data sheet FAZ-DAT-R88-20260715
- TSA, Security Directives and Emergency Amendments — `https://www.tsa.gov/sd-and-ea`
- Industrial Cyber, summary of the Pipeline-2021-02 revision (interdependencies, external connections, zones) — `https://industrialcyber.co/transport/network-segmentation-mfa-among-cybersecurity-measures-laid-down-in-tsa-security-directive-for-pipeline-operators/`

© 2026 Symbeeo. All rights reserved. · Public

- Dragos, Pipeline-2021-02F summary (effective May 3, 2025, superseding 02E) — https://dragos.brightspotcdn.com/50/f3/be642e4149b087e54182ef6cf7ad/tsa-security-directive-pipeline-2021-02f-infographic-09-25.pdf
- Fortinet FortiGate Rugged 70G, reseller listing (the Fortinet data sheet could not be opened) — https://www.shi.com/product/50297439/Fortinet-FortiGate-Rugged-70G

1c · Public implementations this design follows

Each row is labeled. **Public deployment**: a named operator's real deployment, published and dated by the operator, its vendor or a partner, used where one exists. **Our own design**: the dated vendor or standards documentation this design was built from, where no public deployment of the design exists. Labels and dates checked Oct 22, 2026.

Table 2. Public implementations this design follows

Implementation	Who published it · date	What it settles for this design	URL
Our own design, built from published documentation. Security Directive Pipeline-2021-02G, in force May 3, 2026 to May 2, 2027: IT/OT segmentation so OT keeps running if IT is compromised; access control; continuous monitoring	TSA · security directive list, accessed Oct 22, 2026; term and summary as in SRA-SEC-001 §9.1	R2 and R15: the directive is performance-based and reissued yearly; this design meets its segmentation outcome and is reviewed at each reissue	https://www.tsa.gov/sd-and-ea
Our own design, built from published documentation. The segmentation policies must list and describe IT and OT interdependencies, list all external connections to OT, and set zone boundaries by criticality, consequence and operational necessity [S*]	Industrial Cyber · summary of the revised directive; the directive text is issued to designated operators, not published	R3 and §4.1: the interdependency list is a deliverable in its own right, built before any rule is written	https://industrialcyber.co/transport/network-segmentation-mfa-among-cybersecurity-measures-laid-down-in-tsa-security-directive-for-pipeline-operators/
Our own design, built from published documentation. Pipeline-2021-02F effective May 3, 2025, superseding 02E; applies to owners and operators of TSA-designated critical pipeline systems or facilities [S*]	Dragos · infographic, September 2025	R15: the yearly reissue pattern that puts 02G in force on May 3, 2026	https://dragos.brightspotcdn.com/50/f3/be642e4149b087e54182ef6cf7ad/tsa-security-directive-pipeline-2021-02f-infographic-09-25.pdf

No public, dated deployment by a named pipeline operator that shows its segmentation design was found on Oct 22, 2026; operators do not publish it. Every row is documentation used to build our own design.

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Estate	46 pump stations · 9 terminals · 2 control centers · 2,100 km · 14 IT–OT touch points today	[A]

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R2	Segmentation outcome	OT can keep operating if IT is compromised, and the reverse	[S*] TSA Pipeline-2021-02 series, summaries
R3	Segmentation record	IT–OT interdependencies listed and described; every external connection to OT listed; zone boundaries by criticality, consequence and operational necessity	[S*] Industrial Cyber summary
R4	Islanded operation	OT runs ≥ 72 h at nominated throughput with every IT–OT path cut; tested twice a year	[T]
R5	IT–OT paths	only through the OT DMZ at the two control centers; zero direct IT-to-station paths	[T]
R6	Device classes	managed · contractor laptop · OT, each with a posture rule	[S] SRA-SEC-001 R4, NIST SP 1800-35
R7	Remote access revocation	identity disabled → OT remote access lost ≤ 5 min	[T] SRA-SEC-001 R11
R8	Vendor remote access	approved per session, recorded, ≤ 4 h per session, no standing accounts	[A]
R9	Use cases shown at acceptance	policy enforcement · least privilege · lateral movement blocked, station to station and IT to OT	[S] SRA-SEC-001 R12, NIST SP 1800-35 §6
R10	Continuous monitoring	every station's and terminal's OT traffic inspected; alert on the control-center OT console ≤ 5 min	[T]
R11	Station firewall	FortiGate Rugged 70G: 1.3 Gbps threat protection, 1.5 Gbps NGFW, 2.5 Gbps IPS, 8 Gbps firewall (64-byte UDP), 1.4 million sessions; fanless, DIN rail, –40 to 75 °C; IEC 61850-3, IEEE 1613	[S*] reseller listing
R12	OT DMZ firewall	FortiGate 200G: 6 Gbps threat protection, 7 Gbps NGFW, 9 Gbps IPS, 8 × 10GE SFP+, 8 × 5GE RJ45	[S] via SRA-SEC-001 R7
R13	Load ceiling	peak design load at or below 50 % of the published figure for the features turned on	[A] design rule
R14	Log retention	12 months online, 24 months archive, held inside OT	[T] SRA-SEC-001 R10
R15	Directive term	Pipeline-2021-02G in force May 3, 2026 to May 2, 2027; design reviewed at each reissue	[S] via SRA-SEC-001 §9.1

Fifteen rows; seven carry a regulator's, standards body's or vendor's figure (three of them [S*] only), three are design assumptions, five are design targets.

© 2026 Symbeeo. All rights reserved. · Public

3 · Architecture overview

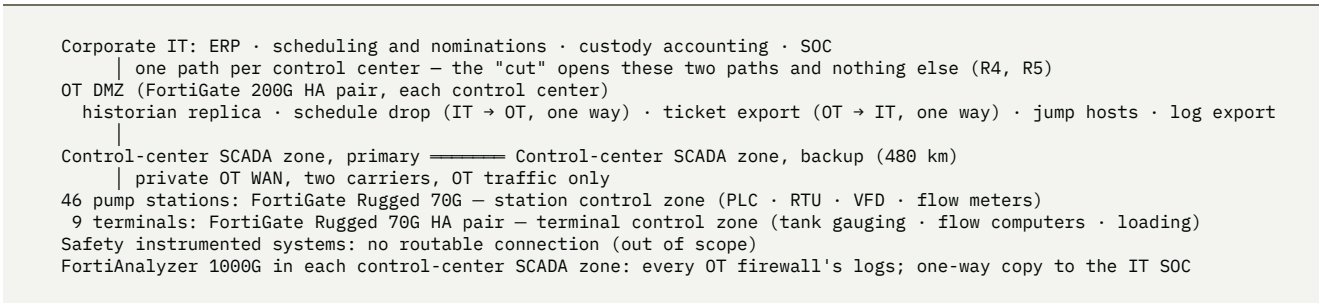


Figure 1. Zones, the two IT–OT paths and the cut

Every dependency OT has on IT is turned into a one-way data drop that OT can run without for 72 hours. Cutting IT off is then two links at two DMZs, not a hunt across 14 touch points, and it is tested, not assumed.

Table 4. Architecture overview

Role	Product (exact model)	Qty	Capacity used	Why this unit
Station and terminal firewall	Fortinet FortiGate Rugged 70G	64: one per pump station, a pair per terminal	≈ 20 Mbps peak of 1.3 Gbps threat protection, under 2 % [A]/[S*]	Fanless, DIN rail, –40 to 75 °C, IEC 61850-3 [S*]; sized for the cabinet, not throughput
OT DMZ firewall	Fortinet FortiGate 200G	4 (HA pair per control center)	≈ 300 Mbps of 6 Gbps threat protection, 5 % [A]/[S]	Inside the 50 % ceiling (R13); 10GE to the SCADA core [S]
OT logging	Fortinet FortiAnalyzer 1000G	2 (one per control center)	≈ 1,500 logs/s peak of 20,000 sustained, under 8 % [A]/[S]	660 GB/day, 32 TB [S] via SEC-007 R17; logs stay in OT (R14)

4 · Design by subsystem

4.1 The interdependency list first.

Before any rule is written, each of the 14 touch points is traced to the business function behind it [A]: batch schedules pushed from the scheduling system; custody-transfer tickets pulled by accounting; historian data read by engineering; vendor support; time; antivirus updates. Each one is either removed, or turned into a one-way drop through the OT DMZ with a stated fallback for 72 hours without it (R3, R4) [T]. Two examples: the control center holds the next 7 days of batch schedule on the OT side, so scheduling can be cut; flow computers keep custody tickets locally and the OT DMZ buffers 30 days of them, so accounting resynchronizes after the cut rather than stopping the line [A]. Rejected: segmenting first and finding dependencies when something breaks — the dependency that stops a pipeline is usually commercial, not technical.

4.2 Zones.

Five zones by consequence [A]: corporate IT; OT DMZ; control-center SCADA; station and terminal control; and vendor access, which exists only inside the DMZ. Safety instrumented systems have no routable connection and stay that way. Every external connection to OT — carriers, the two control centers' DMZs, the vendor access zone — is listed with an owner (R3) [S*]; [A].

© 2026 Symbeeo. All rights reserved. · Public

4.3 OT DMZ.

One FortiGate 200G pair per control center, active-passive [S] SRA-SEC-001 R7; [A] mode. Nothing passes from IT to the SCADA zone directly; IT and OT each talk to a server in the DMZ (R5) [T]. Sizing: ≈ 300 Mbps of historian replication, schedule drops and log export [A] against 6 Gbps threat protection [S] is 5 %, under the 50 % ceiling (R13). The cut is an administrative shutdown of the two IT-facing DMZ interfaces, scripted and logged, that any control-room supervisor can run [A].

4.4 Stations and terminals.

A FortiGate Rugged 70G at every pump station, a pair at every terminal where loading runs continuously [A]. Station rules allow only SCADA polling from the two control centers and engineering access from the jump hosts; station to station is denied, so a compromised station cannot reach its neighbor (R9) [S] use case; [A] rules. Load is ≈ 20 Mbps at peak against 1.3 Gbps threat protection [S*]; the unit is chosen for the cabinet — fanless, DIN rail, −40 to 75 °C — not for throughput.

4.5 Remote access.

Engineers and vendors reach OT only through jump hosts in the OT DMZ, with multi-factor sign-in [A]. Employees' access follows their identity: disabled in the directory, OT remote access gone within 5 minutes (R7) [T]. Vendors get a session, approved for one task, recorded and closed at 4 hours (R8) [A]. Contractor laptops are their own device class with a posture rule (R6) [S] and never join a station network directly [A].

4.6 Continuous monitoring.

Each station firewall inspects OT traffic with industrial protocol signatures and sends logs to the FortiAnalyzer in its control center, inside OT; an alert reaches the OT console in ≤ 5 minutes (R10) [T]. A one-way copy goes to the IT SOC through the DMZ, so the SOC sees OT without being able to reach it [A]. Logs are held 12 months online and 24 months in archive (R14) [T]; at ≈ 1,500 logs/s against 20,000 sustained [S], online retention is expected to fit and is measured at first build [A].

4.7 The islanding test.

Twice a year, with the shippers told in advance, the control-room supervisor runs the cut at both DMZs and the pipeline runs on OT alone for 72 hours at nominated throughput (R4) [T]. Pass: no station loses SCADA; no batch misses its schedule; custody tickets reconcile after reconnection with zero gaps [T]. The first test runs at 24 hours, the second at 72 [A]. The result is the evidence the operator gives TSA for R2.

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
Corporate IT compromised	the cut is run at both DMZs; OT runs on its 7-day schedule and local tickets	[T] R4
Station firewall fails	station control runs locally; SCADA loses that station; technician dispatched with a spare unit	[A]
Primary OT DMZ pair fails	backup control center's DMZ carries the one-way drops; OT unaffected	[A]
Both control centers lose the OT WAN to a station	station runs on its local control logic and shuts down safely on its own limits	[A]

© 2026 Symbeeo. All rights reserved. · Public

Failure	Behavior	Source
Vendor session exceeds 4 h	session closed by the jump host; a new approval needed	[A] R8
Islanding test finds a hidden IT dependency	test stopped, link restored, dependency added to the list with a fallback before the next test	[T] R3

6 · Limits

- The directive's text is issued to designated operators and was not read; R2 and R3 rest on the summaries named in §1c and on SRA-SEC-001 §9.1.
- The FortiGate Rugged 70G figures come from a reseller listing, not Fortinet's own data sheet; they are read again from the data sheet at design freeze.
- The 72-hour figure is a target set with the typical buyer's operations; the true limit is commercial and is found by the first test.
- The safety instrumented systems, the SCADA application and the station control logic are not assessed here.
- Patch management under the directive is not addressed by this document.

7 · Lessons learned

None yet — this is a design study; populated after the first build against it.

8 · The author

WRITTEN BY

David Morgan

Principal Security Architect

CCISO, CISSP, CISSP-ISSEP, CISM, CISA, CRISC, PMP, CCSP, Adopting Zero Trust (Forrester)

Signed off by Edwin Ozer, Founder.

© 2026 Symbeeo. All rights reserved. · Public

SYMBEEO

Each vendor's tool shows you their option. We show you all of them against one requirement.

Compared. Then Delivered.

hello@symbeeo.com · symbeeo.com

© 2026 Symbeeo. All rights reserved.

Product and company names and logos are their owners' trademarks, shown only to identify the lines Symbeeo sources. Naming a vendor or showing its logo does not mean the vendor sponsors or approves Symbeeo's comparisons or any recommendation Symbeeo makes.

Figures are as published by their sources on the dates given in this document; figures marked [A] are assumptions.

SEC-008 · Version 1.0 · Oct 22, 2026