SYMBEEO

PUBLIC

DESIGN STUDY

OT segmentation for a utility's substations under IEC 62443

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Security	Utilities	Electricity distributor
DOCUMENT	**VERSION**	**DATE**
SEC-002	1.3	Oct 10, 2026

WRITTEN BY

David Morgan, Principal Security Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	SEC-002	Version	1.3
Issued	Oct 10, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.2, Sep 27, 2026
Capability	Security	Industry	Utilities
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 10, 2026. Issued by Symbeeo, Oct 10, 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 5
4 · Design by subsystem 6
5 · Failure behavior 7
6 · Limits 7
7 · Lessons learned 8
8 · The author 8

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] figure read from the vendor's own current page on Sep 18, 2026 · [S*] figure from the vendor's page summary where the page itself could not be opened · [A] design assumption for 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
Sep 18, 2026	1.0	First issue.
Sep 20, 2026	1.1	Public implementations added; figures reconciled with published sources.
Sep 27, 2026	1.2	Figures and platform details rechecked against published sources.
Oct 10, 2026	1.3	Approval line now reads: approved by the Founder, issued by Symbeeo. David Morgan remains the author.

1 · Scope

Who it is for. The head of OT security of an electricity distributor whose substation networks were built flat, one broadcast domain per substation and often one across several, and who must show an auditor zones and conduits under IEC 62443-3-2 before the next regulatory cycle.

Typical buyer [A]. An electricity distributor with 120 substations. Each substation has 8–40 IEDs and RTUs, one or two engineering workstations, and a WAN link to a control center; two control centers, active and standby. Protection traffic is IEC 61850 GOOSE and Sampled Values inside the substation; SCADA to the control center is IEC 60870-5-104 or DNP3.

What is in. Zone and conduit model per substation; a ruggedized firewall at each substation as the zone boundary; ruggedized access and aggregation switching inside the substation; passive OT asset discovery feeding the firewall policy; central policy management; the change method that keeps each substation's cut-over inside its window. **What is out.** Control-center IT/OT DMZ design; SCADA application changes; the WAN transport itself; physical security.

Assumptions. Fortinet is the substation firewall vendor [A]; Cisco is the substation switching and OT visibility vendor [A]. Substation cabinets have DIN rail, -40 °C to +70 °C ambient, no forced air [A]. Each substation has one maintenance window of two hours or less, arranged with the protection engineers [A]. No protection-relay traffic crosses the firewall: GOOSE and SV stay in the substation LAN [A].

Related documents, read Sep 18, 2026. Fortinet rugged product matrix (FGR-70G / FGR-60G / FGR-60F), https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinet-rugged-product-matrix.pdf · Fortinet rugged products page, https://www.fortinet.com/products/rugged · Cisco Catalyst IE3400 Rugged Series datasheet, https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-ie3400-rugged-series/cat-ie3400-rugged-series-ds.html · Cisco Catalyst IE9300 Rugged Series datasheet, https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-ie9300-rugged-series/catalyst-ie9300-rugged-series-ds.html · Cisco Cyber Vision datasheet, https://www.cisco.com/c/en/us/products/collateral/security/cyber-vision/cyber-vision-ds.html · Cisco Substation Automation — The New Digital Substation, Version 3.3 Design Guide (September 2025), read Sep 20, 2026, https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Utilities/SA/3-3/SA-3-3-DG.pdf · Cisco blog, Brazilian power utility secures grid network with IE3400 and Cyber Vision (Dec 20, 2023), read Sep 20, 2026, https://blogs.cisco.com/industrial-iot/keeping-the-lights-on-brazilian-power-utility-wins-cybersecurity-award-for-securing-grid-network-with-cisco ·

© 2026 Symbeeo. All rights reserved. · Public

Fortinet case study, energy provider segments its OT network with FortiGate Rugged and FortiManager (page undated; its case-study PDF dated Aug 23, 2023), read Sep 20, 2026 and Sep 27, 2026, https://www.fortinet.com/customers/alperia and https://www.fortinet.com/content/dam/fortinet/assets/case-studies/cs-alperia.pdf.

1c · Public implementations this design follows

Deployment rows are real public deployments, each dated. Where no public deployment matches, the row is Vendor documentation: the vendor's document that this design, Symbeeo's own, is built on.

Table 2. Public implementations this design follows

Implementation	Who published it · date	What it settles for this design	URL
Vendor documentation. Substation Automation Design Guide 3.3: IEC 62443 zones and conduits, Cyber Vision inline sensors on IE3400 / IE9300 / IE3500 / IR8340, GOOSE and SV as Layer 2 multicast inside the substation	Cisco · 2025-09	R11, R12, §4.1 and §4.4: the sensor-on-switch model and the rule that protection traffic never leaves the substation LAN are the vendor's validated design, not this document's invention	https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/Utilities/SA/3-3/SA-3-3-DG.pdf
Deployment. A Brazilian distribution utility deployed IE3400 switches and Cyber Vision across 600+ distribution substations, feeding an OT SOC	Cisco · Dec 20, 2023	R1 and §3: 120 substations on IE3400 plus Cyber Vision is one-fifth of a published deployment on the same platform; discovery before enforcement (§4.4) is how that deployment found unneeded protocols to shut down	https://blogs.cisco.com/industrial-iot/keeping-the-lights-on-brazilian-power-utility-wins-cybersecurity-award-for-securing-grid-network-with-cisco
Deployment. An energy provider segmented its OT network with FortiGate Rugged firewalls under FortiManager and FortiAnalyzer	Fortinet · Aug 23, 2023 (case-study PDF)	R15 and §4.6: rugged FortiGate as the OT zone boundary with one central management plane, deployed to remote sites from FortiManager templates, is a published Fortinet customer deployment; the case study places the OT devices at 200 sites but gives no firewall count, so it settles the pattern, not the sizing	https://www.fortinet.com/customers/alperia

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Substations in scope	120	[T]
R2	Flat OT networks remaining after the program	0	[T]
R3	Change window per substation	under 2 hours, one visit	[T]

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R4	Substation firewall environmental rating	IEC 61850-3 and IEEE 1613 certified; -40 °C to +75 °C; DIN rail	[S] FGR-70G, FGR-60G
R5	Substation firewall throughput	8 Gbps firewall, 2.5 Gbps IPS, 1.3 Gbps threat protection, 7.1 Gbps IPsec	[S] FGR-70G
R6	Substation firewall interfaces	6 × GE RJ45, 2 × SFP	[S] FGR-70G
R7	OT protocol inspection	IPS signatures for common ICS/OT/SCADA protocols	[S] Fortinet rugged page
R8	Substation access switch	8 × GE copper + 2 × SFP, -40 °C to +75 °C, IEC 61850-3 / IEEE 1613	[S] IE-3400-8T2S
R9	Substation aggregation switch (larger sites)	24 × GE SFP + 4 × 1/10G uplinks, StackWise, IEC 61850-3 / IEEE 1613	[S] IE-9320-22S2C4X
R10	Port security inside the zone	802.1X with multidomain authentication; MACsec-256 on the Advantage license	[S] IE3400
R11	Asset discovery	passive DPI of ICS protocols on a switch-hosted sensor; Center capacity 50,000 components, 300 sensors per hardware appliance	[S] Cyber Vision
R12	Zone model	one Level 2 substation zone per site, one Level 3 control zone per control center, conduits only across the firewall	[A]
R13	Conduit rule count per substation	20 or fewer explicit allow rules; implicit deny	[A]
R14	SCADA continuity during cut-over	no loss of SCADA polling longer than 60 s	[A]
R15	Central management	one policy plane for 120 firewalls; per-substation policy derived from a template	[A]

Fifteen rows; eight carry a vendor figure, four are design assumptions, three are design targets.

3 · Architecture overview

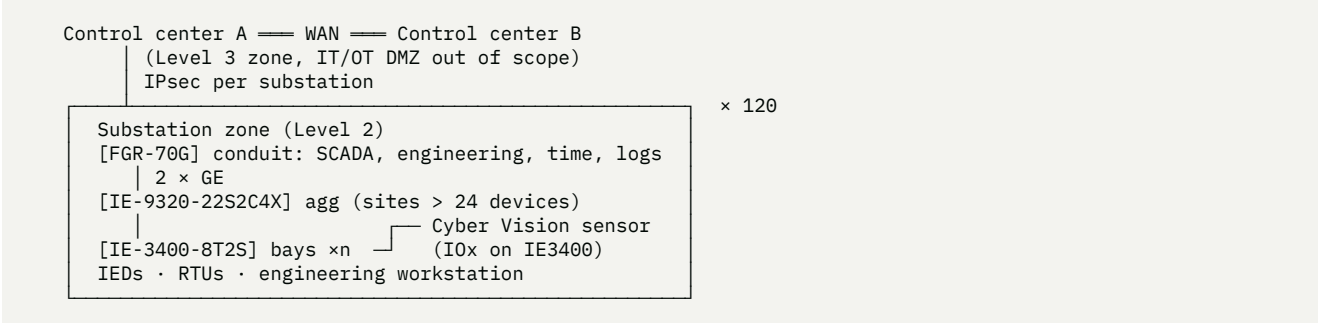


Figure 1. Substation zone and conduit

© 2026 Symbeeo. All rights reserved. · Public

One firewall per substation as the sole conduit to the control zone; ruggedized Cisco switching inside the zone with the OT sensor on the switch; passive discovery builds the allow list before the firewall is turned to enforce.

Table 4. Architecture overview

Role	Product (exact model)	Qty	Capacity used	Why this unit
Substation zone boundary	Fortinet FortiGate Rugged 70G (FGR-70G)	120	under 100 Mbps of 1.3 Gbps threat protection [S]/[A]	IEC 61850-3 / IEEE 1613, DIN rail, 8 × ports, 5G option exists for out-of-band [S]
Small-substation alternative	Fortinet FortiGate Rugged 60G (FGR-60G)	0 day one	—	Same rating, 1.1 Gbps threat protection [S]; kept as the option for sites at the low end of the 8–40 device range [A]
Bay access switch	Cisco Catalyst IE-3400-8T2S	360 (3 per site average) [A]	8 copper ports per bay group [A]	IEC 61850-3 / IEEE 1613, 802.1X, MACsec-256, hosts the Cyber Vision sensor [S]
Substation aggregation	Cisco Catalyst IE-9320-22S2C4X	40 (sites with more than 24 devices) [A]	24 SFP downlinks, 4 × 1/10G uplinks [S]	IEC 61850-3 / IEEE 1613, stacking [S]
OT asset discovery	Cisco Cyber Vision Center, CV-CNTR-M8N hardware appliance	2 (one per control center)	120 sites of 8–40 devices, well under 50,000 components / 300 sensors [S]	One inventory, pushed to policy [S]
Firewall management	Fortinet central management (FortiManager family)	2 (HA pair)	120 devices [A]	One policy plane, template per substation [A]

4 · Design by subsystem

4.1 Zone and conduit model.

Each substation is one IEC 62443 zone at Purdue Level 2; each control center is a Level 3 zone. The only conduit between them is the substation firewall. Inside the substation, protection traffic (GOOSE, SV) stays on the substation LAN and is never routed [A]. Rejected: sub-zones per bay on day one — the switch policy (802.1X, MACsec) covers intra-zone control without adding 120 more firewall policies; sub-zones are a Phase 2 option [A].

4.2 Substation firewall.

FGR-70G on DIN rail, two GE ports toward the WAN router (or the built-in 5G option on the FGR-70G-5G-DUAL where the WAN is cellular [S] model exists, [A] use), two ports to the aggregation or bay switch. Policy: IEC 60870-5-104 or DNP3 to the SCADA front-end processors, engineering protocols to the engineering VLAN only, NTP, syslog, and management; implicit deny both ways. IPS OT signatures in monitor mode for 30 days, then block [A]. Rejected: FGR-60F — 500 Mbps threat protection [S], under half the FGR-70G's 1.3 Gbps; it carries the same IEC 61850-3 / IEEE 1613 listing on the matrix [S], so throughput decides.

4.3 Switching.

IE-3400-8T2S per bay group; IE-9320-22S2C4X as the aggregation switch where a site exceeds 24 devices. 802.1X with multidomain authentication on every IED-facing port; MAC authentication bypass for IEDs that cannot do 802.1X

© 2026 Symbeeo. All rights reserved. · Public

[A]; MACsec-256 on links between switches [S]. Operating range -40 °C to +75 °C at 200 LFM, -40 °C to +70 °C in a vented enclosure without a fan [S], so the cabinet airflow is a survey item per site.

4.4 Asset discovery and policy build.

Cyber Vision sensor runs on the IE3400 (IOx) [S]; the Center at each control center groups assets into substation zones and produces the communication map [S]. The firewall allow list for each substation is written from that map, not from interviews, so the rule count (R13) is what the traffic shows.

4.5 Change method per substation.

Pre-staged FGR-70G with the site's policy loaded from the template; switch configs pre-staged. On site: install firewall in-line in transparent mode with all-allow logging (30 min), confirm SCADA polling unbroken (15 min), switch to the enforced policy (15 min), observe (30 min), hand back. Total inside 2 hours (R3) [A]; rollback is the transparent all-allow policy, one command.

4.6 Central management and logging.

One management pair; firewall logs to the client's SIEM (out of scope here). Per-substation policy is a template with site variables; no hand-edited policy on any firewall [A].

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
Substation firewall fails closed	Substation loses SCADA to the control center; local protection unaffected because GOOSE/SV never cross the firewall; field visit to swap the pre-staged spare	[A]
WAN link to a substation down	SCADA loss for that site until the link returns; the FGR-70G-5G-DUAL variant provides a second transport where fitted	[S] model, [A] use
One bay switch down	IEDs on that switch lose the station bus; other bays unaffected; spare on the truck	[A]
Cyber Vision Center down	Discovery pauses; firewall policy unchanged; no traffic impact	[A]
Management pair down	Firewalls keep enforcing the last policy; no policy changes until restored	[A]
Policy error at cut-over	Rollback to the transparent all-allow policy inside the window	[A]

6 · Limits

- The FGR-70G carries 1.3 Gbps of threat protection [S]; a substation with a high-rate engineering or video feed needs a separate check before the model is fixed.
- The two-hour window depends on the pre-staged policy being right; a site with undiscovered traffic will need a second visit.
- 802.1X on IEDs is limited to what the IED firmware supports; MAB is the fallback and is weaker.
- Sub-zoning inside a substation is not in this design.

© 2026 Symbeeo. All rights reserved. · Public

- The 40 aggregation and 360 bay switches in §3 are planning assumptions [A]; the count per substation is a survey output.

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-002 · Version 1.3 · Oct 10, 2026