SYMBEEO

PUBLIC

DESIGN STUDY

Program governance for a three-supplier OT and IT refresh at a renewables operator

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Consulting & Engineering	Energy	Renewables operator
DOCUMENT	**VERSION**	**DATE**
CON-005	1.2	Nov 6, 2026

WRITTEN BY

David Morgan, Principal Security Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	CON-005	Version	1.2
Issued	Nov 6, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.1, Oct 10, 2026
Capability	Consulting & Engineering	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 10, 2026 (version 1.1). Version 1.2 issued by Symbeeo, Nov 6, 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 the engagement starts."		

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 7
8 · The author 7

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] figure or clause read from the standards body's or publisher's own current page on Sep 24, 2026 · [S*] figure from the page summary where the page itself 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
Sep 27, 2026	1.0	First issue.
Oct 10, 2026	1.1	Approval line now reads: approved by the Founder, issued by Symbeeo. David Morgan remains the author.
Nov 6, 2026	1.2	Independence reworded: vendor commissions, rebates and incentives are declared.

1 · Scope

Who it is for. The program director of a renewable-generation operator who has contracted three suppliers — one for site networks, one for the control-center data center, one for OT security — and who needs one plan, one set of gates and one person with no supplier's interest checking that each supplier's work meets the requirement before the next one builds on it.

Typical buyer [A]. An operator of 38 wind and solar sites and 4 battery-storage sites in two EU member states, dispatched from one control center with a standby. Each site has a SCADA server, 20–120 turbine or inverter controllers, and a WAN link; the program replaces the site networks, rebuilds the control-center data center, and adds OT zone boundaries and monitoring at every site over 24 months.

What is in. Program governance under ISO 21503:2022: design authority, integrated plan, RAID and decision logs, interface agreements between suppliers, stage gates G0–G4 bound to each supplier's signed test record; the requirements register the suppliers were contracted against, kept under change control; regulatory applicability for the electricity network code on cybersecurity; IEC 62443-2-1 security-program maturity measured at the start and at G4. SRA-CON-001 Model B. **What is out.** Any supplier's design or build; commercial management of the supplier contracts; turbine and inverter control systems themselves; site civil works.

Assumptions. The register and baseline (Model A) were issued before this engagement and are taken as G0 [A]. The three suppliers are contracted and each owes an SDD and an STP [A]. The operator's cut-over windows are set by generation forecasts, one site per week at most [A]. The design authority meets every two weeks [A].

Related documents, read Sep 24, 2026. SRA-CON-001, SDD-CON-001, STP-CON-001 (this capability) · ISO 21503:2022, Guidance on program management, https://www.iso.org/standard/82868.html · IEC 62443-2-1:2024, Security program requirements for IACS asset owners, https://webstore.iec.ch/en/publication/62883 · Commission Delegated Regulation (EU) 2024/1366, network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows, https://eur-lex.europa.eu/eli/reg_del/2024/1366/oj/eng · NIS2, Directive (EU) 2022/2555, https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng · PMBOK Guide 8th edition, https://www.pmi.org/standards/pmbok.

© 2026 Symbeeo. All rights reserved. · Public

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 Sep 27, 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. ISO 21503:2022: guidance on program management — terms, roles and practices, including sponsor, program components and stakeholders; revises the 2017 edition	ISO · 2022-02; page could not be opened, summary read Sep 24, 2026	R1 and §4.1: the governance roles and the one-plan, one-log structure are the standard's, applied to three suppliers	https://www.iso.org/standard/82868.html
Our own design, built from published documentation. IEC 62443-2-1:2024, second edition: asset-owner security-program requirements restructured into program elements, with a maturity model for evaluating them; replaces the 2010 edition	IEC · published Aug 7, 2024; webstore page read Sep 27, 2026	R9 and §4.5: the operator's OT security program is measured on the standard's own maturity model at the start and at G4, so the program can show a change in maturity, not only equipment installed	https://webstore.iec.ch/en/publication/62883
Our own design, built from published documentation. Network code on cybersecurity for cross-border electricity flows, in force since June 13, 2024	European Commission · adopted Mar 11, 2024, published May 24, 2024, in force Jun 13, 2024 [S*]; amended since (consolidated text of Sep 14, 2025, not read)	R10 and §4.6: whether the operator is a high-impact or critical-impact entity under the code is a finding for the applicability note	https://eur-lex.europa.eu/eli/reg_del/2024/1366/oj/eng

No public, dated record of program governance for an OT and IT refresh at a renewables operator was found on Sep 27, 2026 (one undated offshore-wind security case was found and left out, having no date); every row is documentation used to build our own design.

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Program control	one integrated plan, one RAID log and one decision log across the three suppliers	[S*] ISO 21503:2022
R2	Program size	42 sites, 1 control center and 1 standby, 3 suppliers, 24 months	[A]
R3	Stage gates	G0–G4; each gate opens only on the signed record SDD-CON-001 §5.2 names for it: register, contracts, SDDs, STPs, horizon-1 closure	[T] from SDD-CON-001 §5.2

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R4	Interface agreements	every supplier-to-supplier boundary numbered, with an owner each side, the protocol, and a test case in an STP	[T]
R5	Interface count	9 agreements expected at G2	[A]
R6	Change control	every change to the contracted register made by a written change order, signed before work starts	[T] from SDD-CON-001 §1.4
R7	Decision record	every design authority decision dated, with options considered and any dissent	[T]
R8	Cut-over rate	≤ 1 site per week, inside the generation-forecast window	[A]
R9	OT program maturity	IEC 62443-2-1:2024 maturity recorded per program element at start and at G4	[S] IEC 62443-2-1:2024
R10	Regulatory applicability	NIS2 and the electricity network code on cybersecurity each marked applicable or not, one sentence of basis each	[S*] EUR-Lex
R11	Independence	assessor declares any commission, rebate or incentive from any of the three suppliers	[A] Symbeeo policy
R12	RAID review	every open item reviewed at every design authority; none older than 2 meetings without an owner's update	[T]
R13	Status report	weekly: % complete per deliverable, slippage against plan	[T] from SDD-CON-001 §1.5
R14	Closing gate	G4 opens when roadmap horizon 1 is closed and lessons are recorded	[T]

Fourteen rows; three carry a published figure, four are design assumptions, seven are design targets.

3 · Architecture overview

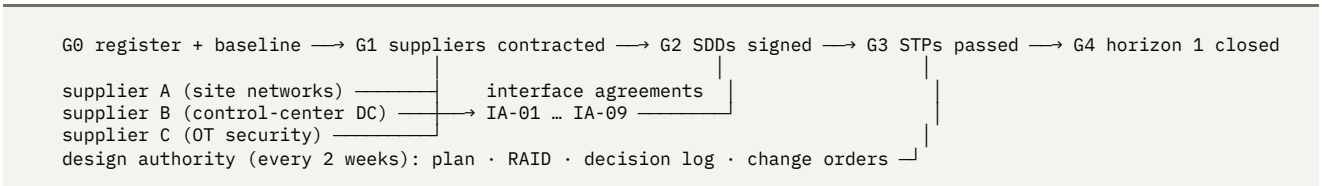


Figure 1. Stage gates and supplier governance

Three suppliers, one plan, and gates that open on signed test records rather than on reported progress.

© 2026 Symbeeo. All rights reserved. · Public

Table 4. Architecture overview

Role	Component (exact name)	Qty	Capacity used	Why this unit
Program standard	ISO 21503:2022	1	3 suppliers, 24 months [A]	Program roles and controls [S*]
Project standard inside each supplier	PMBOK Guide 8th edition	3	one per supplier project	SRA-CON-001 Model B names it for the projects inside the program
OT program measure	IEC 62443-2-1:2024 maturity model	2	start and G4	Maturity per program element [S]
Gate evidence	each supplier's STP acceptance record	3	G3 per supplier	A gate opens on a signed record (R3)
Interface control	numbered interface agreements	9 [A]	every supplier boundary	Owner each side and a test case (R4)

4 · Design by subsystem

4.1 Design authority.

Chair: the program director. Members: the operator's OT, IT and security leads; each supplier's lead architect; the Symbeeo engagement lead as secretary and independent reviewer (SDD-CON-001 §5.1). Decisions go in the decision log with options and dissent (R7). Rejected: one design authority per supplier — it puts the interfaces, where multi-supplier programs fail, in nobody's meeting [A].

4.2 Interfaces.

Nine boundaries expected (R5): for example, site switch to OT zone firewall, zone firewall to control-center fabric, OT monitoring sensor to the security log collector. Each is an interface agreement with an owner each side, the protocol and ports, and a test case in one supplier's STP (R4). An interface without a test case holds G2 closed [A].

4.3 Gates.

G0 is the issued register; G1 is suppliers contracted; G2 is each supplier's SDD signed against the register; G3 is each supplier's STP signed as passed; G4 is horizon 1 closed (R3, R14). A supplier reporting "95 % complete" does not open a gate; a signed record does [A].

4.4 Site cut-overs.

Supplier A's and supplier C's work lands at each site together, one site per week at most (R8), in a window set by the generation forecast. The integrated plan holds the sequence; a site that fails its STP cases rolls back and returns to the queue, and the RAID log records why [A].

4.5 OT program maturity.

At the start, the operator's security program is scored on the IEC 62443-2-1:2024 maturity model per program element (R9); at G4 it is scored again. The difference is reported to the board alongside the equipment installed [A].

4.6 Regulatory applicability.

One sentence each (R10): NIS2, for an electricity producer under national transposition; the network code on cybersecurity, whose obligations depend on whether the operator is identified as a high-impact or critical-impact entity [S*]. A finding, not legal advice.

© 2026 Symbeeo. All rights reserved. · Public

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
Supplier misses a gate	gate stays closed; RAID escalation to the design authority; dependent suppliers re-planned	[T] from SRA-CON-001 F7
Two suppliers disagree on an interface	decision taken at the design authority, dissent recorded; the interface agreement is amended by change order	[T]
Site fails its STP cases at cut-over	rollback in the window; site re-queued; cause in the RAID log	[A]
Generation window lost to weather or grid demand	cut-over moved; plan re-baselined only if the slip exceeds 2 weeks	[A]
Change requested without a change order	work not started; request logged	[T]
Conflict of interest found after start	engagement paused; Founder decision recorded	[T] from SRA-CON-001 F5

6 · Limits

- The design authority governs; it does not manage the supplier contracts or their money.
- A gate proves what the STP tests; a gap in a supplier's STP is a gap in the gate.
- The maturity score is a measure of the security program, not of any single site.
- The applicability note is a finding, not legal advice.
- The cut-over rate depends on the generation forecast, which the program does not control.

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.

CON-005 · Version 1.2 · Nov 6, 2026