SYMBEEO

PUBLIC

DESIGN STUDY

Configuration baselines for a generation fleet under NERC CIP-010: 290 control-network devices, drift reported in 15 minutes

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Automation	Energy	Generator owner and operator
DOCUMENT	**VERSION**	**DATE**
AUT-007	1.0	Oct 22, 2026

WRITTEN BY

Mark Winston, Principal Network Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	AUT-007	Version	1.0
Issued	Oct 22, 2026	Status	Issued by Symbeeo
Classification	Public	Capability	Automation
Industry	Energy	Author	Mark Winston
Role	Principal Network Architect		
Credentials	CCIE, CISSP, CCSP, CCISO, CISM, 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 standards body's, project's or vendor's own current page or document on Oct 22, 2026 · [S*] figure from a page summary 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 at least 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 CIP compliance manager and the OT network lead at a generation operator whose baselines live in spreadsheets, whose monthly configuration export is the only thing standing between an unrecorded change and an audit finding, and who wants every switch, router and firewall inside the electronic security perimeters to have one recorded intent, one recorded change path and a drift alarm that does not wait for the 35th day.

Typical buyer [A]. A US Generator Owner and Generator Operator with six plants — four combined-cycle gas plants and two hydro plants, 5,200 MW in one Interconnection — dispatched from one control center with a backup control center. The operator's CIP-002 assessment places both control centers' BES Cyber Systems at high impact and each plant's at medium impact. Inside the electronic security perimeters (ESPs): 290 network and security devices — 228 switches, 26 routers and 36 firewalls — of which 92 are in the two control centers and 198 in the plants. About 120 configuration changes a month across the fleet.

What is in. The source of truth for every in-scope device; the CIP-010 R1.1 baseline generated from it; the change pipeline with model check, the high-impact test environment and the firmware identity and integrity check; deployment; drift detection; the audit record each change leaves. **What is out.** Servers, HMIs, historians, relays and controllers (their baselines stay in the operator's existing CIP-010 tool); CIP-007 patching and CIP-015 internal network monitoring, which these documents do not address; CIP-005 perimeter design; physical security.

Assumptions. Switches are Cisco Catalyst IE9300 Rugged in the plants and Catalyst 9300 in the control centers, all on one IOS XE release train; routers are Cisco Catalyst 8300; firewalls are FortiGate on FortiOS 7.6 [A]. The operator's Git service and change-ticket system already exist [A]. Firewalls at each ESP boundary are Electronic Access Control or Monitoring Systems (EACMS); switches and routers inside the ESP are BES Cyber Assets or Protected Cyber Assets (PCA), as the operator's CIP-002 record states [A].

Related documents, read Oct 22, 2026.

- SRA-AUT-001, SDD-AUT-001, STP-AUT-001 — this capability's reference architecture, design and test plan (R3, R7, R13 there); SRA-IMP-001 R8, one version-controlled source
- NERC CIP-010-4, Cyber Security — Configuration Change Management and Vulnerability Assessments — `https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-010-4.pdf`
- NetBox releases — `https://github.com/netbox-community/netbox/releases`
- What's new in Red Hat Ansible Automation Platform 2.7 — `https://developers.redhat.com/articles/2026/06/10/whats-new-red-hat-ansible-automation-platform-2-7`

© 2026 Symbeeo. All rights reserved. · Public

- Batfish releases and supported devices — `https://github.com/batfish/batfish/releases` · `https://batfish.readthedocs.io/en/latest/supported_devices.html`
- containerlab, Cisco Catalyst 9000v and Fortinet FortiGate kinds — `https://containerlab.dev/manual/kinds/vr-cat9kv/` · `https://containerlab.dev/manual/kinds/fortinet_fortigate/`

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. CIP-010-4 Table R1 and Table R2: the five baseline items of Part 1.1; authorized changes (1.2); baseline updated within 30 calendar days (1.3); CIP-005 and CIP-007 controls checked before and after (1.4); testing in an environment that models the baseline, high impact only (1.5); software identity and integrity verified (1.6); monitoring at least once every 35 calendar days, high impact, EACMS and PCA (2.1)	NERC · CIP-010-4, enforceable; CIP-010-5 from Jul 1, 2028 per SRA-AUT-001 §9.1	R2–R8: the register quotes the standard's parts, and §4.2 maps each baseline item to where the pipeline reads it	`https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-010-4.pdf`
Our own design, built from published documentation. Cisco Catalyst 9000v kind: a virtual Catalyst 9000 that simulates the UADP or Silicon One Q200 ASIC; 4 vCPU and 18,432 MB RAM per UADP node; NETCONF on port 830	containerlab project · v0.81.1 released Oct 15, 2026	R6 and §4.4: the high-impact test environment of CIP-010 1.5 runs on the same IOS XE train as production, and its differences from the hardware are written down, as 1.5.2 asks	`https://containerlab.dev/manual/kinds/vr-cat9kv/`
Our own design, built from published documentation. Fortinet FortiGate kind: tested with FortiOS 7.0.14; releases from 7.2.0 need a valid license and internet access to activate the VM	containerlab project · page read Oct 22, 2026	§4.4 and §6: the firewall replicas are licensed and activated before the test lab is closed off from any network	`https://containerlab.dev/manual/kinds/fortinet_fortigate/`

No public, dated deployment of a model-checked configuration pipeline at a CIP-registered generation operator was found on Oct 22, 2026; every row is documentation used to build our own design.

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Estate	6 plants · 2 control centers · 290 devices in ESPs (228 switches, 26 routers, 36 firewalls) · ≈ 120 changes a month	[A]

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R2	Baseline items per device	operating system or firmware with version; commercially available or open-source software; custom software; logical network accessible ports; security patches applied	[S] CIP-010-4 1.1
R3	Change authorization	every change that deviates from the baseline authorized and documented [S] CIP-010-4 1.2; in the pipeline, author ≠ reviewer and a change reference on every merge request	[T] SRA-AUT-001 R3
R4	Baseline update after a change	within 30 calendar days [S] CIP-010-4 1.3; here generated at deployment, the same day	[T]
R5	Security controls around a change	CIP-005 and CIP-007 controls that could be affected named before the change and verified after it, results documented	[S] CIP-010-4 1.4
R6	Test before production, high impact	in a test environment that models the baseline; differences from production documented	[S] CIP-010-4 1.5
R7	Software source	identity and integrity of every firmware image verified before a change to baseline items 1.1.1, 1.1.2 or 1.1.5	[S] CIP-010-4 1.6
R8	Monitoring, high impact BES Cyber Systems, EACMS and PCA	at least once every 35 calendar days; detected unauthorized changes documented and investigated	[S] CIP-010-4 2.1
R9	Drift reported	≤ 15 min after it occurs, on all 290 devices, high and medium impact alike	[T] SRA-AUT-001 R7
R10	Configuration source	every device configuration rendered from one version-controlled source	[T] SRA-IMP-001 R8
R11	Audit record	actor, target, time, change, result for every automated action, in a store the actor cannot alter; kept 3 calendar years	[T] SRA-AUT-001 R13; [A] retention
R12	Model check	every change set analyzed against the fleet model before deployment; any unexpected answer blocks it	[T]; [S] Batfish supports IOS-XE and Fortinet
R13	Test environment	12 nodes on 3 hosts: 8 Catalyst 9000v at 4 vCPU and 18,432 MB RAM each, and 4 FortiGate VMs	[S] containerlab; [A] count
R14	Rollback	one site back to its prior configuration ≤ 15 min	[T]
R15	Blast radius	backup control center first, primary 24 h later; one plant per change window	[T]

Fifteen rows; nine carry a standards body's, project's or vendor's figure (four of them beside a design target or assumption), two are design assumptions, four are design targets.

© 2026 Symbeeo. All rights reserved. · Public

3 · Architecture overview

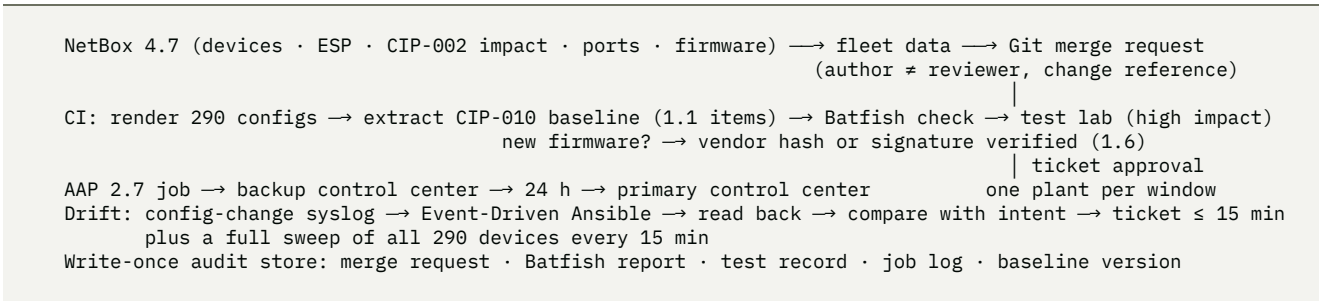


Figure 1. Fleet configuration pipeline and the CIP-010 baseline it keeps

The operator's intent for every device lives in one place; the CIP-010 baseline is not a second record kept by hand but a view generated from that intent on every deployment, and read back from the device every 15 minutes. The 35-day monitoring of Part 2.1 is met many times over, and on the medium-impact plants where the standard does not ask for it.

Table 4. Architecture overview

Role	Product (exact version)	Qty	Capacity used	Why this unit
Source of truth	NetBox 4.7.3 (Oct 13, 2026) [S]	HA pair + DB replica, in the control-center ESP [A]	290 devices, ≈ 9,000 interfaces [A]	holds Cisco and Fortinet devices in one model; custom fields for impact rating and ESP [A]
Executor and events	Red Hat Ansible Automation Platform 2.7 (GA Jun 10, 2026) with Event-Driven Ansible [S]	3 controller nodes; 1 execution node per site, 8 [A]	≈ 120 change jobs a month; ≈ 28,000 device read-backs a day (290 × 96) [A]	job-scoped short-lived tokens; rulebooks start a read-back on a config-change event [S]
Model check	Batfish v2026.08.27 [S]	1 service, in CI	290 configurations per run [A]	IOS-XE and Fortinet on the supported list [S]
Test environment	containerlab v0.81.1 (Oct 15, 2026) with Catalyst 9000v and FortiGate VM [S]	3 hosts [A]	12 nodes: both control-center topologies [A]	NETCONF on 830; UADP simulated [S]

4 · Design by subsystem

4.1 Source of truth.

NetBox holds every in-scope device with its site, ESP, impact rating, role (BES Cyber Asset, PCA or EACMS), firmware and approved services [A]. Nightly, a job lists every device the operator's ESP discovery finds and raises any without a NetBox record [A]. Rejected: one record per site in spreadsheets — it is the current state, and the reason two people's copies disagree.

4.2 Baseline as a generated view.

Each of the five Part 1.1 items is drawn from a named place [A]: 1.1.1 firmware and version from NetBox and the device's own version output; 1.1.2 and 1.1.3 installed packages and scripts from the device's package list (on these platforms, none custom by design); 1.1.4 logical network accessible ports from the rendered configuration's enabled services, checked against the device's own open-port listing; 1.1.5 security patches from the installed maintenance updates [S] items; [A] sources. The baseline is regenerated and versioned on every deployment, so Part 1.3's 30 days becomes the

© 2026 Symbeeo. All rights reserved. · Public

same day (R4) [T]. Rejected: a baseline document separate from the intent — two records of one device drift apart, and the audit then reads the wrong one.

4.3 Change path.

Every change is a merge request with author, independent reviewer and change reference (R3) [T]. The reviewer reads the rendered diff and the baseline diff; a merge request that changes item 1.1.4 lists the CIP-005 and CIP-007 controls it may affect, and the post-deployment job verifies them (R5) [S]. Batfish loads the 290 rendered configurations and answers fixed questions: no new path across an ESP boundary; every firewall rule shadow-free; management access only from the named intermediate systems (R12) [A].

4.4 Test environment for high impact.

Part 1.5 applies to the control centers only [S]. A containerlab topology of 12 nodes — per control center 4 Catalyst 9000v switches and 2 FortiGate VMs — runs on three hosts at 4 vCPU and 18,432 MB RAM per switch node [S] (R13). The record of each test lists the differences from production — simulated ASIC, no Catalyst 8300 replica, virtual firewall — and how each is accounted for, as Part 1.5.2 asks [S]; [A] list. FortiGate VMs are licensed and activated before the lab is closed off from every network [S] containerlab; [A]. Medium-impact plants run the same tested artifact; the standard does not ask them for 1.5 [S].

4.5 Firmware identity and integrity.

No image enters the pipeline until its source is identified and its hash or signature matches the manufacturer's published value (R7) [S]; [A] method. The verification result is attached to the merge request that changes item 1.1.1.

4.6 Deployment and blast radius.

AAP 2.7 deploys through one execution node per site, inside that site's ESP management segment [A]. Backup control center first, primary 24 hours later on the same artifact; one plant per window (R15) [T]. Rollback redeploys the previous signed commit to one site in ≤ 15 minutes (R14) [T]. The automation platform reaches every device in scope, so it is itself categorized and baselined; the design assumes EACMS and applies this document to it [A].

4.7 Drift and evidence.

A configuration-change syslog message starts an Event-Driven Ansible rulebook that reads the device back within a minute; a full sweep reads all 290 devices every 15 minutes regardless (R9) [T]. A difference opens a ticket as a detected unauthorized change, to be documented and investigated (R8) [S]. Each change leaves one record — merge request, Batfish report, test record, firmware check, job log, baseline version — in a write-once store kept three calendar years (R11) [T]; [A].

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
Batfish answer changes without a matching line in the merge request	pipeline stops; nothing reaches a device	[T] R12
Firmware hash or signature does not match	image rejected; merge request blocked; manufacturer's security contact told	[T] R7
Test environment cannot model a change (feature not in Catalyst 9000v)	difference recorded under 1.5.2 with the measure taken; change tested on a spare unit on the bench	[S] CIP-010-4 1.5.2; [A] bench

© 2026 Symbeeo. All rights reserved. · Public

Failure	Behavior	Source
Engineer changes a device by hand	drift ticket ≤ 15 min; change adopted through a merge request or reverted	[T] R9
Execution node at a plant unreachable	changes to that plant queue; read-back sweep for that plant fails and is itself ticketed	[A]
Change degrades a control center after deployment	previous commit redeployed ≤ 15 min; primary untouched for 24 h	[T] R14, R15
Source of truth down	pipeline fails closed; drift compares against the last versioned intent	[A]

6 · Limits

- The baseline covers the 290 network and security devices only; servers, HMIs and controllers keep their own CIP-010 process.
- CIP-007 patching, CIP-015 monitoring and IEC 62443 are not addressed by these documents.
- CIP-010-5 takes effect on Jul 1, 2028 (SRA-AUT-001 §9.1); the pipeline is reviewed against it before that date.
- Catalyst 9000v simulates the ASIC; a forwarding behavior specific to the IE9300 hardware is not proved by the lab.
- Whether the automation platform is an EACMS is the operator's CIP-002 call; this design treats it as one.
- The 120-changes-a-month figure is an assumption; a month of change tickets sets the real load.

7 · Lessons learned

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

8 · The author

WRITTEN BY

Mark Winston

Principal Network Architect

CCIE, CISSP, CCSP, CCISO, CISM, 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.

AUT-007 · Version 1.0 · Oct 22, 2026