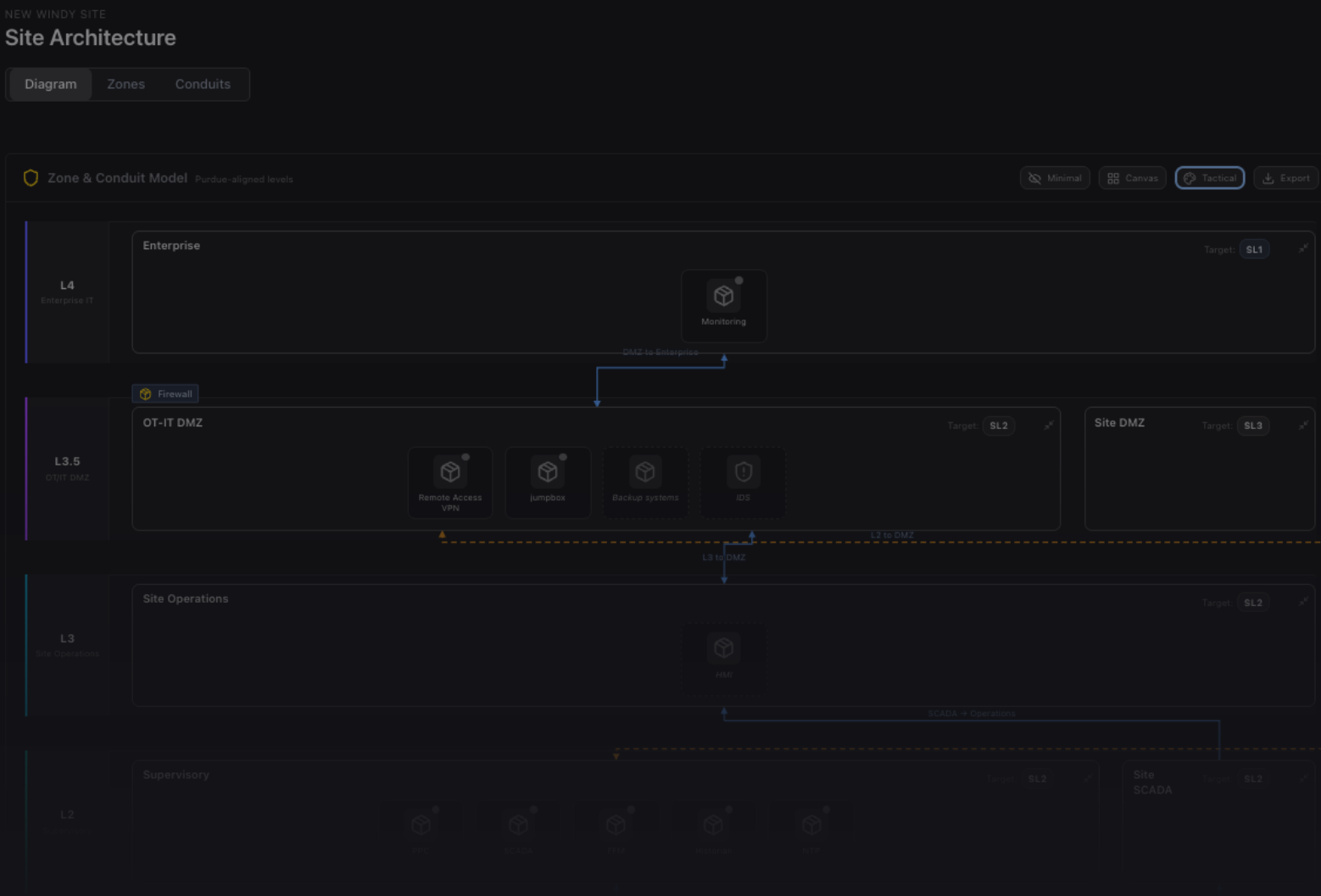


THE CAPA SUITE · SECURE BY DESIGN

Secure by Design

Security built into the design — the architecture, the asset register and the living record of every digital system on the site.

A renewable site is not one system. It is an assembly of generation assets, balance of plant, a substation, site control, and a set of corporate and vendor systems that reach into all of them. Secure by Design captures that assembly before the plant is built — how it is zoned, what is deployed where, and what changes over its life.

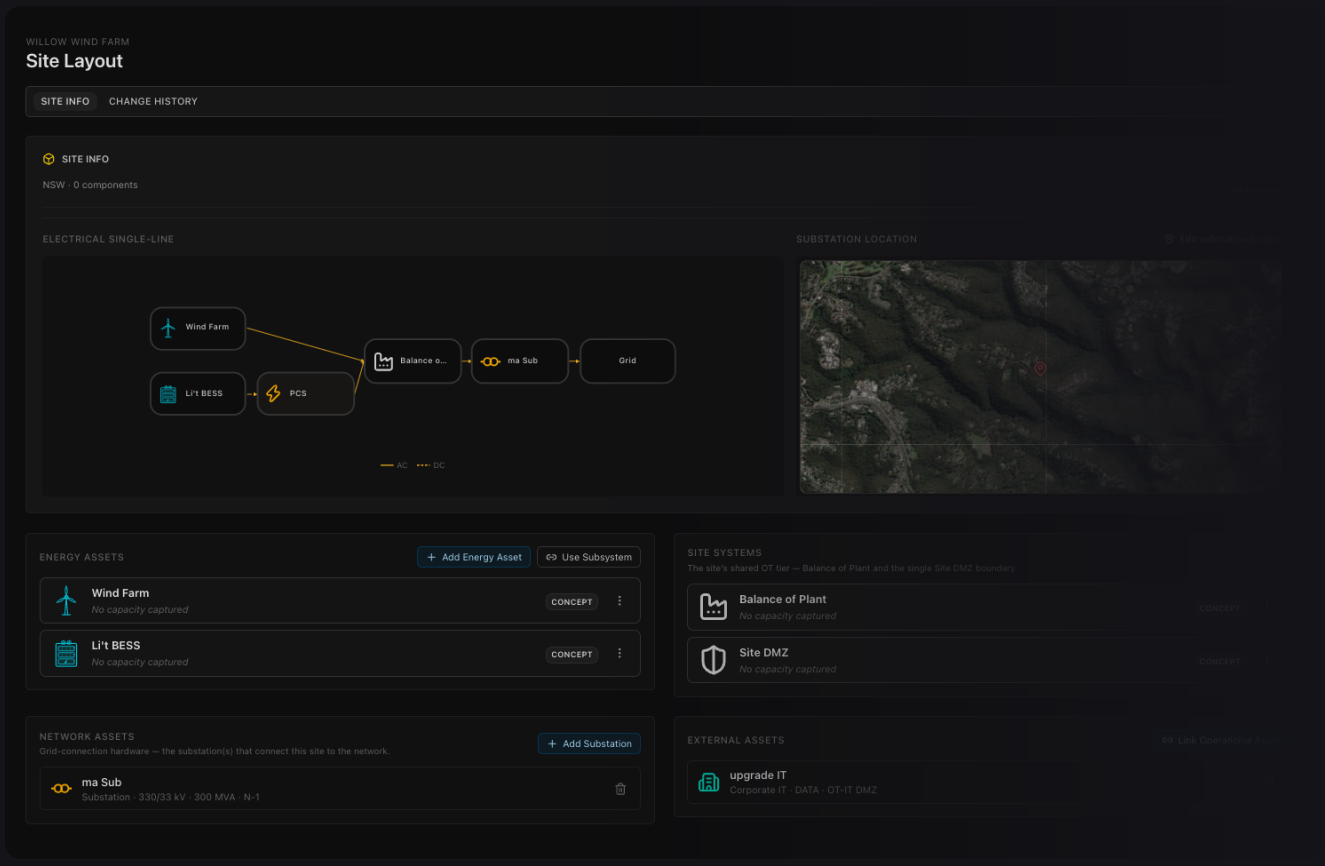
Secure by Design is delivered through three modules — **Site Designer** to model the zone-and-conduit architecture from the drawings, the **Asset Register** to inventory every system and version, and the **Site Journal** to hold the change-controlled record for the life of the asset. Every other CAPA stream — Risk & Compliance and Secure in Operation — builds on this foundation.

CAPA\

THE MODEL

Site as an Assembly

Generation, balance of plant, substations, corporate and vendor systems; many parts, many responsibilities — one secure design.

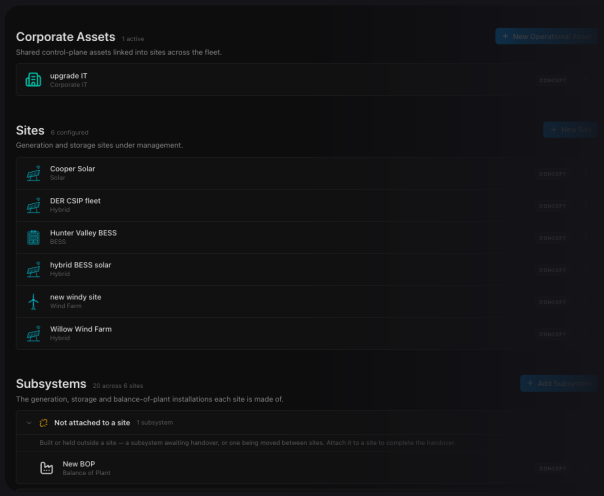


Site design as a composition

Sites are often rolled out in stages, sometimes with different technology stacks and operating arrangements, offering flexibility to expand.

One organisation, many sites

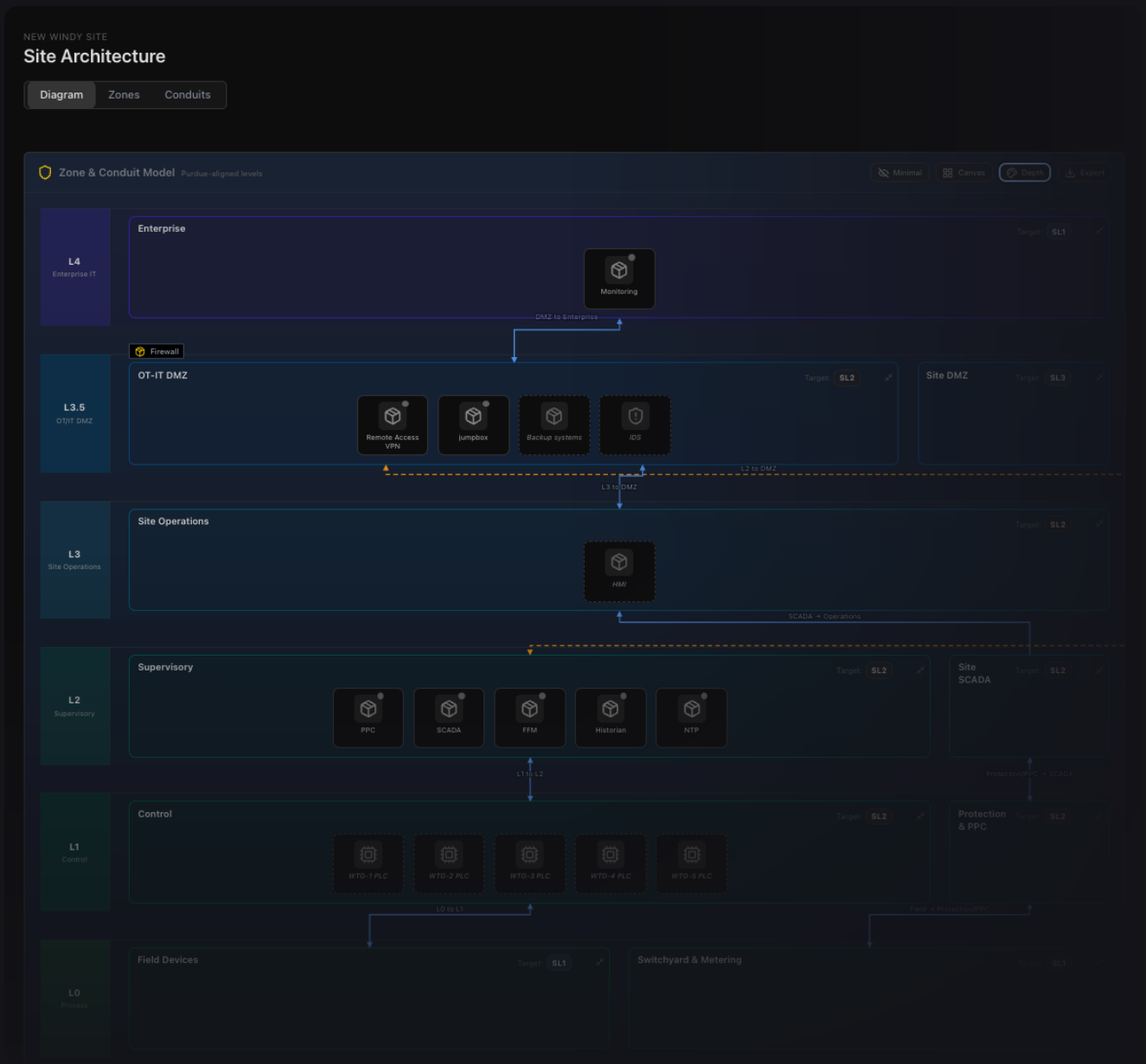
Operators run portfolios of sites and asset types. Corporate assets are shared across the fleet, each site carries its own subsystems, and operational responsibilities can be clearly delegated.



DESIGN VIEW

Site Architecture

Security design tools at concept and design using the IEC 62443 zone and conduit patterns with Purdue reference levels.



DESIGN STAGE

Establish the point of truth

- Zones and conduits defined against the Purdue levels
- Boundary devices, protocols and direction of flow recorded per conduit
- Typically built with the EPC and OEMs at concept or detail design stage

OPERATING LIFE

Keep it truthful

- The as-designed model becomes the as-built, then the as-operated
- Changes to zones, conduits or boundary rules are recorded as part of change control processes
- Cornerstone of the risk plan and effectiveness of cyber related mitigations.

INVENTORY VIEW

Asset Register

Every system deployed at each site, each version installed and running, the zone it sits in, and who is responsible for it.

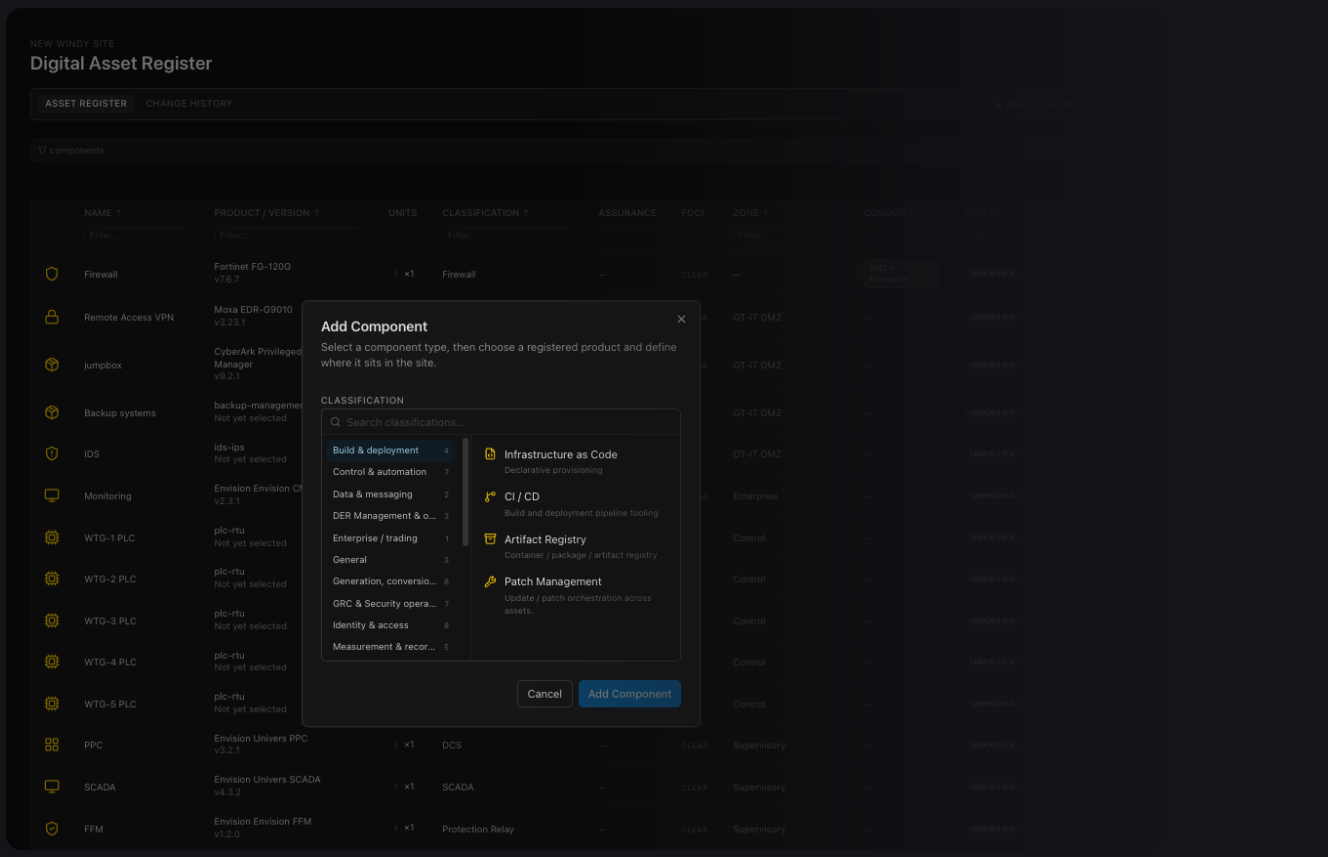
The architecture says how the site is meant to be secured. The register reveals the vendor and version. This supports every vulnerability report for a match on a CVE or advisory.

What is recorded

- Product, vendor, model and deployed version
- The zone it sits in and the conduits it uses
- Sub-components and embedded software within each product
- Owner, maintainer and the contract it sits under

What it answers

- Does this advisory affect us, and at which sites?
- What is the oldest firmware still running in the protection zone?
- Which systems does this vendor touch, across the portfolio?
- What changed between the last audit and this one?



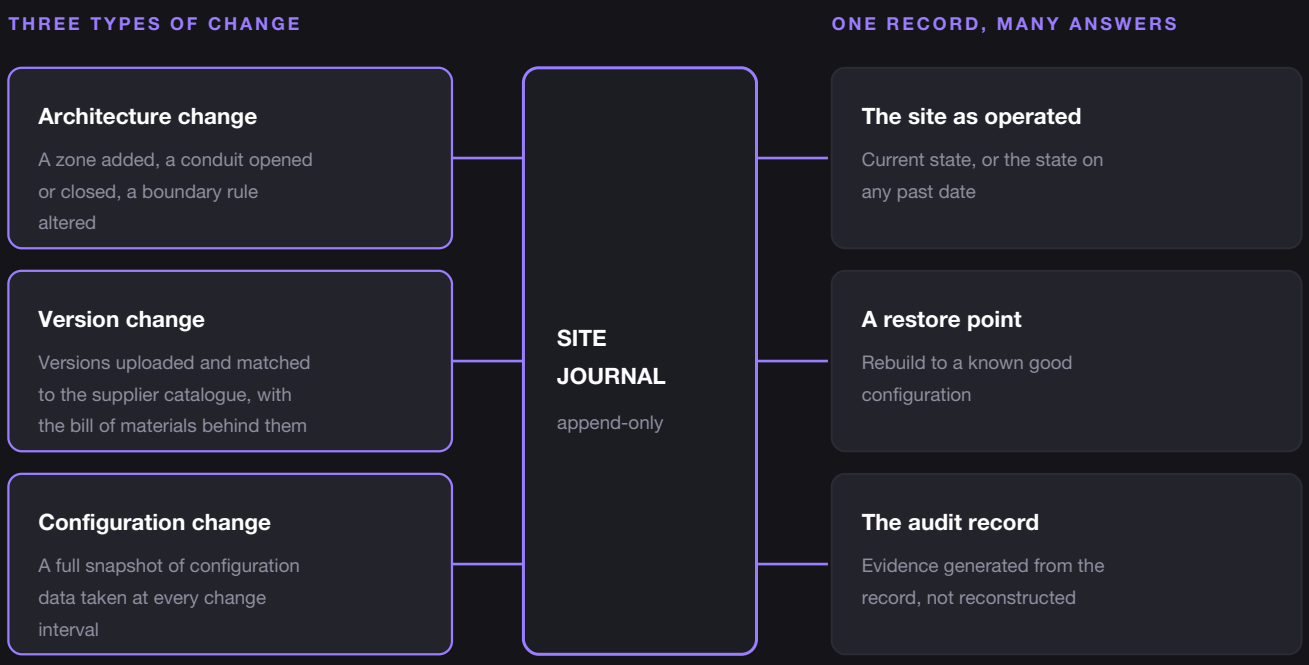
One register, many functions

The register is not merely a compliance artefact or guesswork at the production system inventory. It is the reference model used in every audit, compliance and risk management exercise and as a result is kept up to date at all times.

JOURNAL AS CHANGE CONTROL

Digital Change Management

Three types of change — architecture, version and configuration — each captured as it happens, accumulating into the site's historical blueprint.



Architecture change

- Changes made against the zone and conduit model, not redrawn from scratch
- New zones, conduits opened or closed, boundary rules altered
- The as-designed model becomes the as-built, then the as-operated

Version change

- Software and firmware versions uploaded as they are deployed
- Matched to the supplier catalogue, with the bill of materials behind each product
- The estate's true version position, per site and across the portfolio

Configuration change

- A full snapshot of configuration data at every change interval
- The exact settings in force on any given date can be recovered
- Drift between the documented and the deployed becomes visible

---

The historical blueprint

Taken together, these three change types are not a change log sitting beside the design. They *are* the design — the site as it was drawn, as it was built, and as it stands today, with every step in between still readable. That is the Site Journal.

THE FOUNDATION

Central to risk and cybersecurity

Secure by Design is the foundation — the architecture, asset register and site record that every other stream reads from.

Compliance needs to know what is in scope. Risk needs to know which systems make a High Consequence Event possible. Vulnerability management needs to know what version is deployed where. Detection needs to know what normal looks like. All of them are the same question asked from different angles, and all are answered from one place.

S1 · SECURE BY DESIGN

Site Designer

Zone-and-conduit design and target SLs, from the drawings.

Asset Register

A live inventory of every system, mapped to its zone.

Site Journal

The change-controlled record, inherited by everything.

S2 · RISK & COMPLIANCE

Risk Management

High Consequence Events and kill-chain mitigations.

Compliance

Controls mapped to evidence, overlaps resolved once.

Supply Chain

Vendor assurance, including foreign-interference risk.

S3 · SECURE IN OPERATION

Vulnerability Management

Advisories triaged against the versions deployed.

Personnel & Access

Access against named systems and conduits.

Threat Detection & Response

Detection and recovery for the site as modelled.

ABOUT CAPA

CAPA Intelligence is an Australian based cybersecurity company servicing the global electricity / renewables sector, and global supply chains involved in supporting critical infrastructure. Our clients sit across the supply chain – governments, networks, retailers, system operators, IPPs, integrators and OEMs with operations in Australia and abroad.

Contact info@capaintelligence.com to arrange a demo

capaintelligence.com