

E I G E N I A B . V .

Cyber Digital Twin · Fail Fast, Fail Safe

CASE STUDY · BATTERY ENERGY STORAGE · REPRESENTATIONAL REFERENCE SITE

A Battery Storage site, built as a Cyber Digital Twin to assist with the Cyber Resilience Act

BESS-REF-001 is a representational utility BESS built from a client-supplied engineering reference package and cited public sources. It shows how EIGENIA turns a register into a model, a model into evidence, and evidence into a go or no-go for the test bench. It is not a model of any real facility or vendor product.

Example

BESS-REF-001: 4 × 1,075 kW / 4,300 kWh units, MV collection, POI, controls, OT network, physical security

Built from

Client reference package (138 assets, 422 interfaces) + 24 public sources

Regimes

CRA, NIS2, RED DA, Battery Regulation, NCCS, NERC CIP, UL 9540 / NFPA 855

Summary

At 03:00 a vendor account logs in over a cellular router nobody on site has looked at in months. By 03:07 it is on the engineering workstation, and by 03:09 it is trying to raise the charge limit on a battery controller that sits a metre from 24 modules of lithium iron phosphate. Whether that ends as a log entry or a fire depends on decisions made years earlier: which conduits exist, which functions trust the network, and who was responsible for each box.

A grid battery is a product, a power plant and a networked control system at the same time, and each face sits under a different regime. The Cyber Resilience Act governs the products inside the fence; NIS2 governs the company that operates them; RED, the Battery Regulation, UL 9540 and NFPA 855 each claim a slice. This case study shows how EIGENIA builds the whole site as a Cyber Digital Twin first, so that scoping, threat modelling and test planning are answered from one model rather than from a stack of drawings.

BESS-REF-001 follows the client's uploaded engineering reference package: four integrated MP2XL-class units, with the Tesla Megapack 2 XL used only as a public comparable for envelope and ratings [8]. EIGENIA added the parts a reference architecture needs and the package did not hold: two MV skids, a control house, engineering workstation, OT network with an IP plan, DMZ, physical security, an O&M building, earthing, lightning protection, standby power, teleprotection and external links to the TSO, an aggregator and neighbouring DER. Geometry is procedural, behaviour is simulated, and every record carries an evidence tag.

REPRESENTATIONAL ONLY

This is a reference example built to demonstrate the EIGENIA Cyber Digital Twin. It is not Tesla's design or any operator's site. Client engagements are built from the client's own controlled drawings, registers, protocol maps, firmware inventories and test data.

195 register records: 138 from the client package, 57 added and flagged	2,565 named meshes in the 3D model, every one keyed to a twin ID	458 typed interfaces: AC, DC, data, safety and coolant
72 IP nodes on 15 VLANs, from unit LANs to the DMZ	10 simulated sequence steps, from cold start to LOTO	15 listed deviations from the uploaded register

WHERE THE CRA MAY NOT APPLY

The CRA governs products with digital elements made available on the EU market. The BMS, PCS, site controller, RTU, switches, firewalls and routers are in scope for their manufacturers. The installed site is not a product, and EMS code developed by the owner for its own use and never made available is arguably outside it. The operator falls under NIS2 instead. Section 03 sets out each regime.

APPROACH: CLIENT PACKAGE PLUS PUBLIC SOURCES

The client package fixed the asset list, interfaces, telemetry schema and pad layout. Public sources [1]–[24] filled the reference-architecture gaps. Where both ran out, engineering judgement filled the gap and the value is tagged ASSUMED. Every record is tagged DOCUMENTED, DERIVED, ASSUMED or SIMULATED.

02

The product

BESS-REF-001 is a fenced 78 × 34 m yard. Four integrated units of 8.8 × 1.65 × 2.785 m sit in two rows on the package's pad centres [8]. Each holds 24 battery modules [9], power conversion, a BMS, a thermal system, a customer interface bay and fire and off-gas safety. Units 1 and 2 are liquid-cooled; units 3 and 4 are modelled forced-air so the two designs can be compared side by side (DEV-02). Two MV skids step 480 V-class output up to the collection voltage, a kiosk houses the MV switchgear, and a main transformer feeds the point of common coupling and the TSO line.

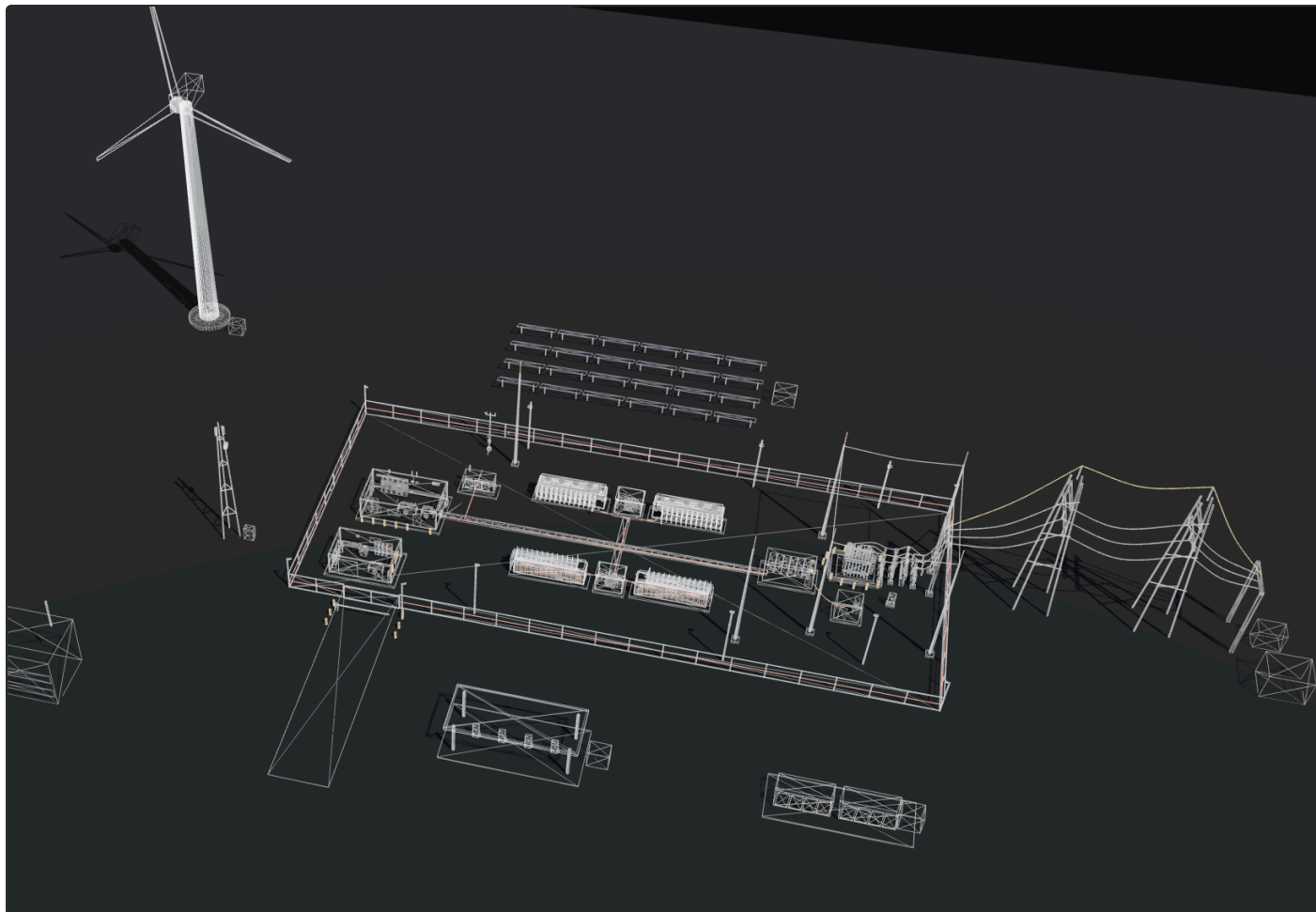


Figure 1. The reference site in wire render. Battery yard, MV skids and fibre trench in the centre, substation, POI and TSO line to the right, control house and O&M building at the gate, and schematic links to PV, wind, EV hub, VPP mast and neighbouring BESS outside the fence. Clicking any part in the viewer opens its register record.

DOCUMENTED [8] 1,075 kW / 4,300 kWh 4-hour C012 rating of the public comparable.	DOCUMENTED [8] 8.8 × 1.65 × 2.785 m Enclosure envelope, 38,100 kg max.	DOCUMENTED [9] 24 modules per unit From a public regulatory filing.	DOCUMENTED [8] −30 to 50 °C Ambient operating range.	DOCUMENTED [4][10] Cyber-physical system BMS, site controller, HVAC, fire, HMI over industrial protocols.
--	--	---	--	---

TAG	MEANING IN THIS TWIN	RECORDS
DOCUMENTED	Existence stated in a cited source or published register class. Geometry is still assumed.	98
DERIVED	Computed or inferred from documented values or the client register by a stated method.	39
ASSUMED	Register class "assumed", every added record, all procedural geometry, the IP plan.	58
SIMULATED	Every dynamic state, telemetry value and event from the SIM-1 simulator.	all runtime data

What is inside the fence

A 4.3 MW battery sounds like four boxes on a pad. Modelled part by part, it is closer to a small substation, a data room and a fire-protected industrial plant sharing one fence line. Every row below is a group of named parts in the 3D model, each with its own register record, interfaces and evidence tag.

ZONE	EQUIPMENT IN THE TWIN	TWIN IDS
Battery yard	4 integrated units holding 96 battery modules, 48 power stages, 4 BMS controllers, 4 customer interface bays with main breakers and CTs, 4 thermal systems (2 liquid, 2 air), 4 gas and smoke detection panels, 4 explosion-control exhaust fans, 12 deflagration vents, 4 strobes and E-stops, 4 unit edge switches	AST-BESS-01 to -04 and children
MV collection	2 MV skids, each with an LV incomer panel, a ~2.5 MVA oil-immersed step-up transformer and a ring main unit; MV switchgear kiosk with 6 cubicles and bay controllers	AST-MVSKID-01/02, AST-SWG-001
Substation and POI	Main step-up transformer with radiators, 4 ONAF fans, conservator, Buchholz relay and tap changer; surge arresters, current transformers, circuit breaker and disconnecter per phase; line gantry; revenue meter; protection relay; teleprotection terminal; RTU kiosk	AST-XFMR-001, AST-PCC-001, AST-METER-001, AST-RELAY-001, AST-TP-001, AST-RTU-001
Control house	Five racks: site controller, OT core switch, OT and DMZ firewalls, GNSS clock, historian, IDS sensor, jump host, DMZ historian replica, log collector, optional data diode; out-of-band and vendor LTE routers; three-screen HMI desk; engineering workstation; fire alarm panel with ESD station; station service panel; UPS; transfer switch	AST-CTRLHOUSE-001 and 20 child records
Standby power	~150 kVA enclosed diesel genset with belly tank, radiator fan and controller	AST-GEN-001, AST-ATS-001
Physical security	78 × 34 m fence with sliding gate and barrier arm, 6-zone fence vibration sensor, card-and-PIN readers at the gate and four doors, 5 pole cameras with a video server, 6 lighting masts, crash-rated bollards	AST-FENCE-001, AST-PIDS-001, AST-ACS-001, AST-CCTV-001, AST-NVR-001, AST-LIGHT-001, AST-BOLL-001
O&M building	Workbench and battery-module service cart, tool crib, PPE and arc-flash lockers, eyewash, lockout/tagout board with group lock box, earthing sets and hot sticks, two maintenance workstations, Wi-Fi, a maintenance laptop	AST-OMB-001, AST-OMWS-001, AST-LOTO-001, AST-MLT-001
Earth, lightning, environment	Buried copper mesh at ~5 m with earth rods and bonds to every pad; 6 lightning masts with shield wires over the substation; weather mast with anemometer, vane and pyranometer	AST-EARTH-001, AST-LPS-001, AST-WX-001
Outside the fence (schematic)	TSO substation over two line towers with OPGW fibre; 24-table PV plant with inverter station; wind turbine; 4-charger EV hub; neighbouring BESS; aggregator telecom mast; owner operations centre; OEM cloud	AST-GRID-001, AST-DER-*, AST-ROC-001, AST-VENDOR-CLOUD-001

Why this matters now

RED cybersecurity requirements became mandatory for internet-connected radio equipment on 1 August 2025, which catches the routers, Wi-Fi access points and modems inside a BESS. CRA reporting obligations started on 11 September 2026, ahead of full application on 11 December 2027. NIS2 now reaches market participants providing storage and aggregation services. At the same time, public research describes BESS as distributed computers with batteries attached, managed through vendor clouds [20], and vendors routinely ask for remote access for warranty analytics [18].

REGIME	WHAT IT COVERS HERE	APPLIES TO BESS-REF-001?
CRA [R1]	Products with digital elements made available on the EU market	Products yes, site no. BMS, PCS, EMS software, RTU, switches, firewalls and routers for their manufacturers. Owner-built EMS code not made available is arguably out of scope.
NIS2 [R2]	Energy-sector entities, including storage and aggregation service providers	Yes, for the operator , as an entity. Size and national transposition decide essential or important.
RED DA 2022/30 [R3]	Internet-connected radio equipment	Yes for LTE routers, Wi-Fi APs and embedded modems, until the CRA takes over.
Battery Regulation 2023/1542 [R4]	Industrial batteries above 2 kWh	Yes. Due diligence, carbon footprint, battery passport from February 2027.
Network Code on Cybersecurity [R5]	Electricity entities with cross-border impact	Unlikely for 4.3 MW alone; aggregation by a VPP may change the classification.
NERC CIP, UL 9540, NFPA 855, IEEE 1547 [2][3][5]	US grid reliability, product safety, installation, interconnection	NERC CIP likely not at this size; UL 9540/9540A, NFPA 855 and IEEE 1547 yes in US deployments. None of the safety standards carries cyber requirements.
IEC 62443, IEC 62351, NIST SP 800-82 [6][24]	Zones and conduits, protocol security, OT controls	Voluntary. The engineering basis for evidence in every regime above.

The squeeze on a storage operator

The operator buys CRA-marked products, runs them under NIS2, connects them to a TSO under an interconnection agreement and dispatches them through an aggregator. Four parties ask for the same facts: what is inside, how it connects, how a vulnerability is found and fixed, and who is told. Holding those facts once, in one model keyed to the client's own asset IDs, is cheaper than answering four times.

EIGENIA POSITION

We do not assume the CRA applies. Phase 1 records the scoping decision per twin ID, with the reasoning, and the twin carries that decision so it can be revisited when delegated acts and guidance settle.

The same six-phase method

PHASE	FOR BESS-REF-001	TWIN OUTPUT
1 Scope and classify	Decide regime per item: unit, PCS, BMS, EMS, RTU, network, physical security, site. Classify CRA items against Annex III and IV.	Scope record per twin ID
2 Risk assessment	Threats per zone and conduit: vendor LTE pivot, VPP setpoint abuse, BMS firmware tampering, transient laptops, fence-to-cabinet access.	Threat trees keyed to IF- and AST- IDs
3 Requirements and design	Annex I Part I mapped to controls: zones, plausibility checks, independent safety layer, data diode option.	Requirements traceability
4 Secure development and vulnerability handling	Annex I Part II for in-scope products: SBOM, coordinated disclosure, signed firmware, patch windows that respect dispatch contracts.	xBOMs, VEX, patch procedure
5 ALARP review	Residual risk argued as low as reasonably practicable, with safety functions that never depend on the network.	Residual risk register
6 Handover to the test bench	Package, viewer, simulator and evidence delivered; go or no-go with listed gaps.	This package

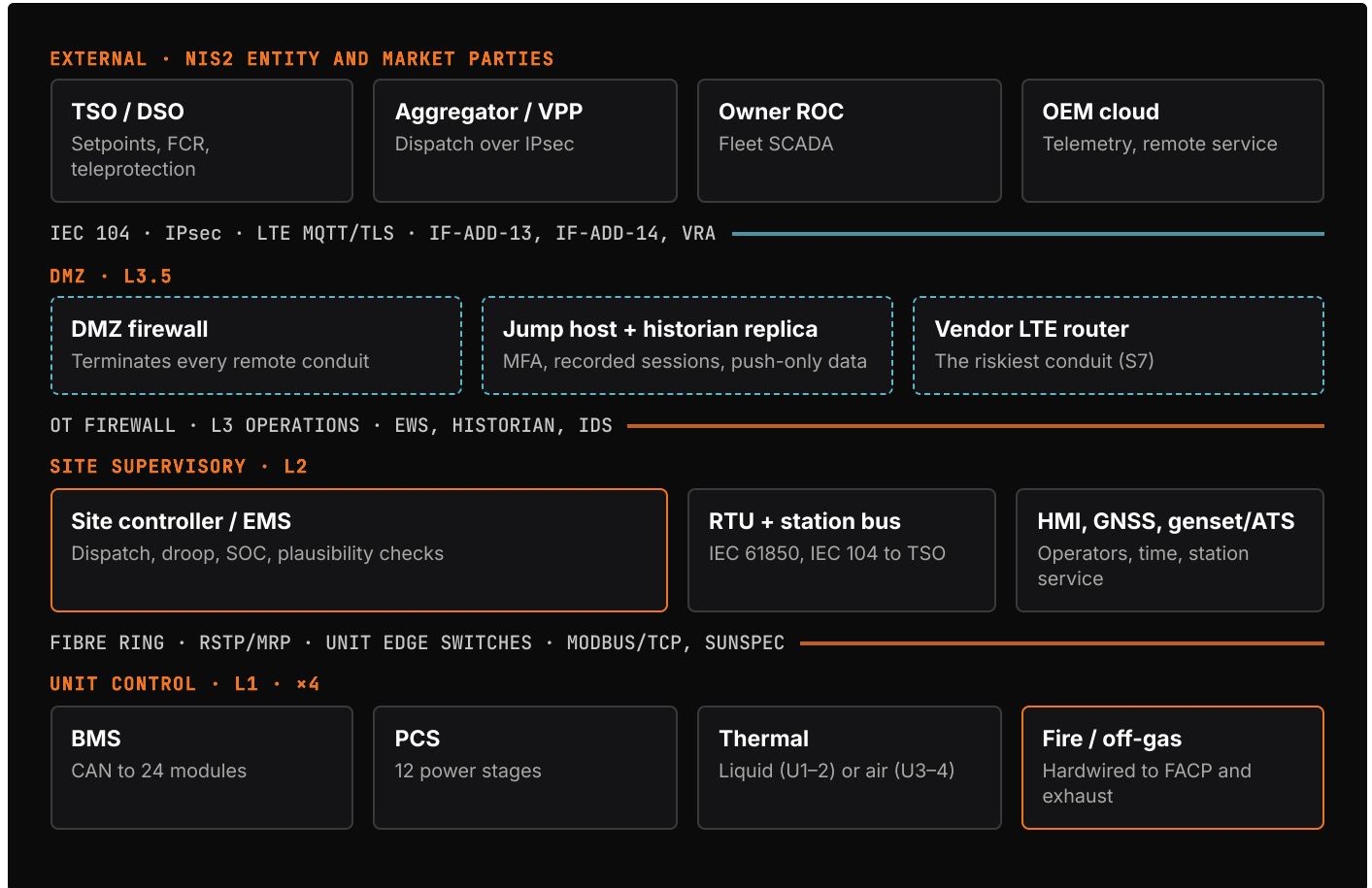
Zones inside the site

ZONE (VLAN)	CONTAINS	CONDUIT TO
Unit control, L1 (11–14)	BMS, PCS, thermal, gas panel, CIF meter per unit	Unit edge switch on the fibre ring
Site supervisory, L2 (20)	Site controller, HMI, GNSS clock, MV skid IEDs, genset, ATS	Core switch, OT firewall
Station bus (30)	Relay, bay controllers, POI meter, transformer monitor, RTU	Core switch; TSO over IEC 104
Safety monitor (40)	FACP status (trips stay hardwired)	Read-only to HMI
Operations, L3 (50)	EWS, historian, IDS, log collector	OT firewall
DMZ, L3.5 (60, 61)	Jump host, historian replica, vendor LTE router, optional data diode	VPP, owner ROC, OEM cloud
Physical security (70), IT (80, 90), OOB (95)	CCTV, ACS, PIDS, VMS; O&M PCs and Wi-Fi; break-glass console	Separate switches; no route to L1

DESIGN RULE

The twin is never a command path. Safety functions (BMS protection, gas-triggered exhaust, deflagration vents, FACP and ESD loop, protection relay, teleprotection) do not depend on any IP network, and the simulator shows them acting with the network compromised.

Inside the machine



Following a kilowatt-hour out of the fence

Energy leaves a module as DC, rises through copper risers to a power stage above the bay, and joins a 480 V-class AC bus along the back wall. It passes the unit's main breaker and current transformers in the customer interface bay, crosses to the MV skid's LV panel, is stepped up, switched by the ring main unit, and carried in the trench to the MV switchgear. From there it goes through the main transformer, surge arresters, current transformers, the POI breaker and disconnecter, and up the gantry onto the TSO line. Each hop is a typed interface in the register, and each switching device is a mechanism the simulator opens and closes.

Control takes a different road. The BMS talks CAN to its 24 modules, Modbus/TCP to the unit edge switch, and the edge switch joins a fibre ring back to the control house. Safety takes a third road that never touches IP: gas detectors start the exhaust fan over a relay, the fire alarm panel drops the ESD loop, and the protection relay trips the POI breaker over GOOSE backed by copper.

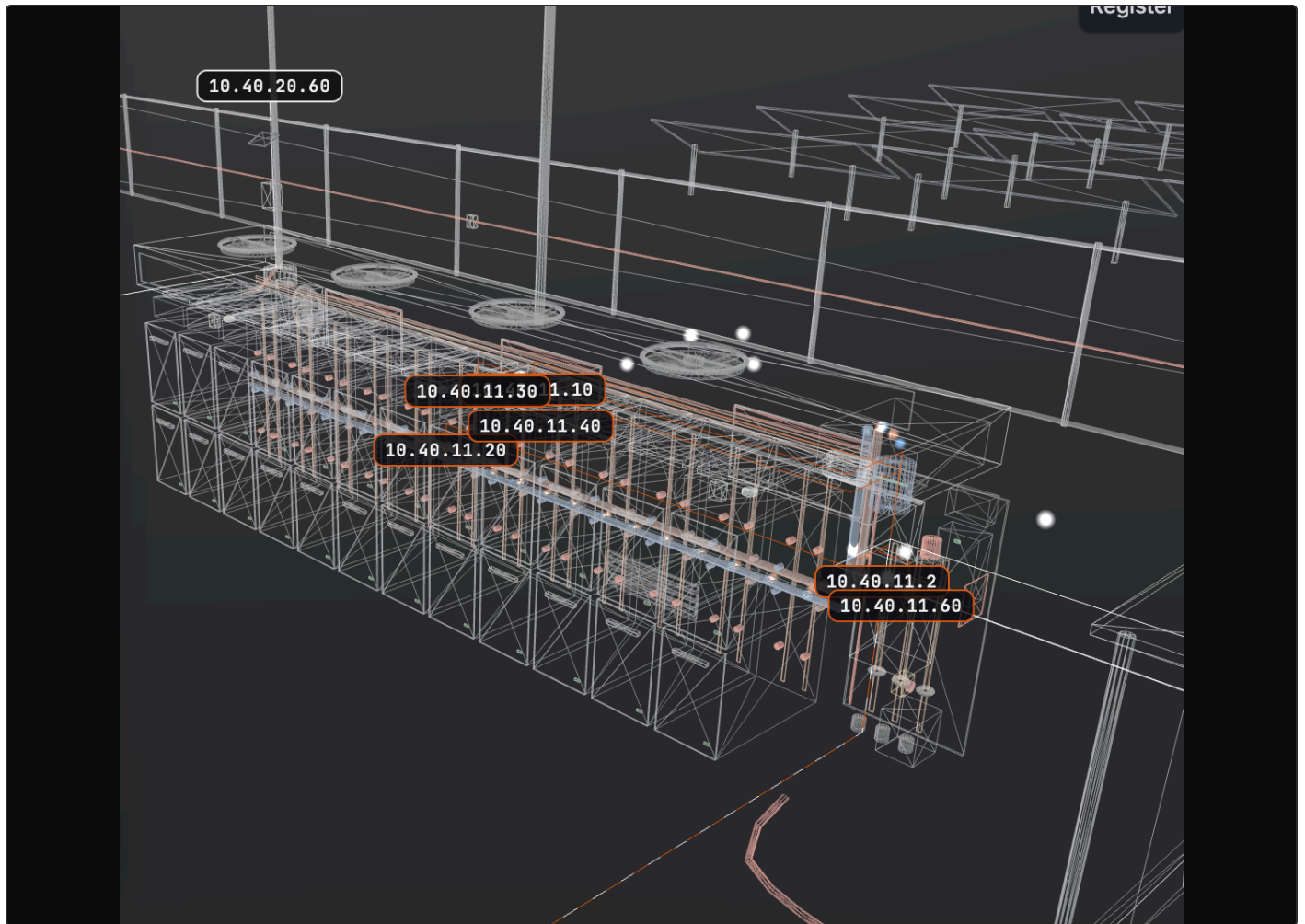


Figure 2. Unit 1 in wire render with the network overlay on: 24 modules, DC risers, coolant manifolds, the liquid-cooled thermal roof and the customer interface bay. Tags show the unit LAN (VLAN 11): edge switch .2, BMS .10, PCS .20, thermal .30, gas panel .40, CIF meter .60. The 12-bay layout is ASSUMED (DEV-03); the module count is documented [9].

Liquid versus air, side by side

The client register describes every unit as liquid-cooled. Units 3 and 4 were deliberately modelled with packaged air conditioning (DEV-02) so the two designs can be compared on the same site, under the same dispatch.

	UNITS 1–2 · LIQUID GLYCOL	UNITS 3–4 · FORCED AIR
Heat path	Coolant manifolds behind every module, pump and chiller module, roof heat exchanger with 4 fans	End-wall packaged HVAC with 2 condenser fans, roof supply duct, 12 ceiling diffusers, louvred doors
Simulated cell temperature at full discharge	~29.5 °C	~32.5 °C
Dominant failure	Pump trip: flow stops, cells rise ~20 °C, derate at 42 °C (step S6)	Compressor or refrigerant loss: slower rise, larger air volume
Controller and network surface	Chiller/pump controller on the unit LAN (10.40.1n.30)	HVAC controller on the unit LAN, often with its own vendor web UI
Explosion control interaction	Sealed enclosure; exhaust fan and vents carry the full load	Air path must close on gas detection or it feeds the exhaust problem

Every link, typed

192 Coolant	136 Data	96 DC	26 AC	9 Safety
-----------------------	--------------------	-----------------	-----------------	--------------------

THE CONDUITS THAT DECIDE THE THREAT MODEL

Five paths carry anything from outside to the control plane: the vendor LTE router, the VPP and ROC tunnels through the DMZ firewall, the RTU's IEC 104 link to the TSO, and the maintenance laptop patched into a unit switch. The last one bypasses every firewall.

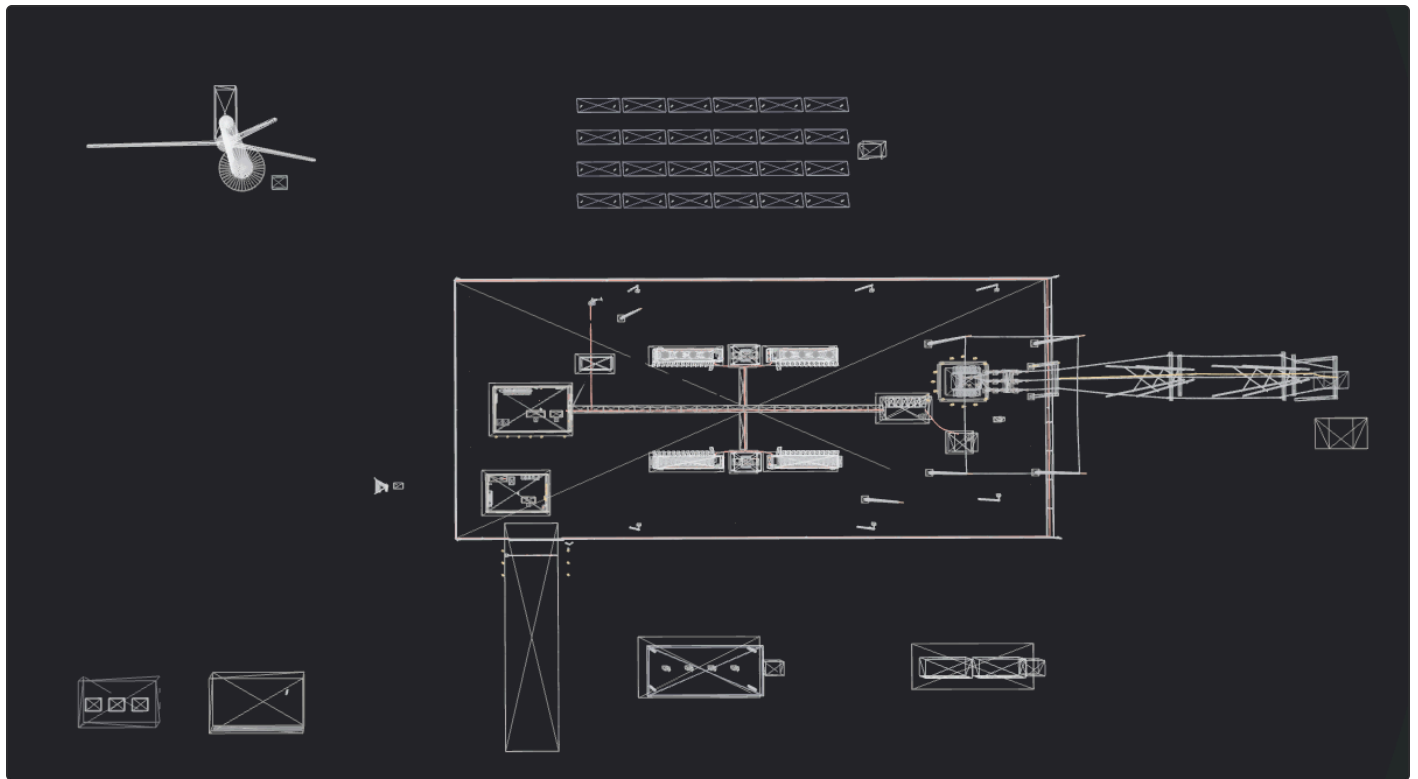


Figure 3. Plan view. The fibre trench runs from the control house past both unit rows and MV skids to the switchgear, with the transformer, POI gantry and line towers to the right. The IP plan (10.40.0.0/16) is ASSUMED (DEV-08); external endpoints use documentation-only ranges.

06

Eight bills of materials, one record

Every entry resolves to the same AST- twin IDs as the 3D model and the client register.

BOM	HOLDS	STATUS IN THIS PACKAGE
HBOM	Units, modules, PCS, BMS, transformers, RMUs, relays, switches, firewalls	104-line bill of materials; manufacturers unknown except the comparable
SBOM	EMS, HMI, historian, firewall OS, jump host, IDS	Skeleton; client package CycloneDX files carried in baseline
FBOM	BMS, PCS, IED, switch and router firmware	Skeleton; signing chain unknown
CBOM	IPsec, TLS, MQTT certificates, OSDP keys, firmware signing keys	Not started
MBOM	Assemblies, skids, factory tests	Assembly tree exported
DBOM	Telemetry in the client schema, commands, retention	I/O map (63 tags) and 5,292 telemetry records
NBOM	Nodes, VLANs, links, firewall conduits	IP plan, 15 VLANs, 92 links
Model BOM	Simulator, equations, parameters, V&V	sim.js, controller logic, validation report

07

Supply chain, tier by tier

The client package names one manufacturer, the comparable, as reference-only. Public sources document that Megapack is built at the Lathrop Megafactory in California and at Megafactory Shanghai for non-US markets, with LFP cells from CATL and LG Energy Solution and, since 2026, from Tesla's own plant in Sparks, Nevada [S1][S2][S3]. Every other supplier below is a candidate to investigate, tagged ASSUMED.

TIER	ITEMS · CANDIDATE SUPPLIERS (HQ)	CYBER QUESTION
0 Integrator and operator	Integrated units, EMS, cloud: Tesla (US), Fluence (US/DE), Wärtsilä (FI), Sungrow, BYD, CATL (CN)	Who holds remote access, and can it write to the BMS?
1 Power and protection	PCS: SMA (DE), Power Electronics, Ingeteam (ES), EPC Power (US). Transformers and RMUs: Hitachi Energy, Siemens, Schneider, SGB-SMIT. Relays: SEL (US), SIPROTEC (DE)	Which carry firmware, who signs it, and do any contain undocumented radios?
1 OT network and security	Switches: Hirschmann, SCALANCE (DE), Moxa (TW). Firewalls: Fortinet, Palo Alto. Diode: Fox-IT (NL), Waterfall (IL). IDS: Nozomi, Claroty, Dragos	Patch cadence on edge VPNs; EU-sovereign options
2 Components	LFP cells (CN, KR, US), chillers and HVAC (Envicool, Pfannenberg), gas detection (Honeywell, Dräger), gensets (Caterpillar, Cummins)	Single-source items, country of origin, tariff and FEOC exposure
3 Services and physical security	CCTV (Axis, Bosch, Hanwha), PIDS (Senstar, RBtec), ACS (Nedap, Genetec), telecom	Avoid FCC Covered List vendors for critical-infrastructure surveillance [S4][S5]

08

From vulnerability to report

For a CRA product inside the fence, an actively exploited vulnerability starts the manufacturer's Article 14 clock. For the operator under NIS2, a significant incident starts the Article 23 clock. The twin holds both paths and maps each product to its manufacturer contact.

The 24-hour clock

EARLY WARNING 24 h 	NOTIFICATION 72 h 	CRA FINAL REPORT 14 days 	NIS2 FINAL REPORT 1 month 
---	--	--	--

The BESS-specific constraint is the patch window. A unit offline for a firmware update is capacity not delivered under an FCR or VPP contract. The procedure takes one unit out at a time, keeps three on dispatch, and verifies BMS limits against the signed baseline before reclosing contactors.

09

How an adversary would attack it

Vendor remote access pivot

VRA → DMZ jump host → EWS → U2 BMS • simulated in S7

1. Abuse the OEM LTE router or a stolen vendor account
2. Reach the jump host, then RDP to the EWS
3. Write BMS limits and an out-of-range site setpoint over Modbus

CONTROLS

- Vendor router lands in a DMZ, never the OT LAN
- EMS plausibility check and function-code allow-list
- BMS hardware limits independent of the network; IDS alert; WAN block

Fleet dispatch abuse through the aggregator

VPP cloud → DMZ firewall → site controller • chain C7

1. Compromise the VPP platform
2. Send synchronised setpoints to this site, the neighbouring BESS and the EV hub
3. Push system frequency outside limits

CONTROLS

- Rate and range limits in the EMS
- TSO override through the RTU
- Data diode option: outbound telemetry only (DEV-15)

A third path, a maintenance laptop on a unit maintenance port (S10, chain C8), bypasses every firewall and is countered by transient-asset policy, port locks and IDS. The cascading-failure register in the package traces eight chains from initiator to the barrier that stops them.

The failure modes that matter most

The client package held ten FMEA lines with severities only. EIGENIA extended it to sixteen and scored each one; the full list is in 09-safety. The six below carry the highest risk priority, and three of them start in the network.

FAILURE MODE	CONSEQUENCE	BARRIER	RPN
BMS firmware tampering	Protection limits altered; runaway becomes possible	Signed firmware, independent hardware limits (to confirm with vendor)	140
Cell or module overtemperature	Off-gas, deflagration risk, unit loss, 4.3 MW offline	BMS limits, gas detection, exhaust, vents, ESD	108
Remote setpoint manipulation	Overload, SOC abuse, frequency disturbance across a fleet	Plausibility checks, allow-lists, TSO override	96
Transient laptop malware	Malware on a unit LAN behind every firewall	Transient-asset policy, port locks, IDS	96
Gas detector failed low	No exhaust start; gas accumulates to LFL	2-out-of-3 voting, bump tests, passive vents	90
Contactors welded closed	Unit cannot be isolated by ESD	Upstream breaker and RMU, verified LOTO	64

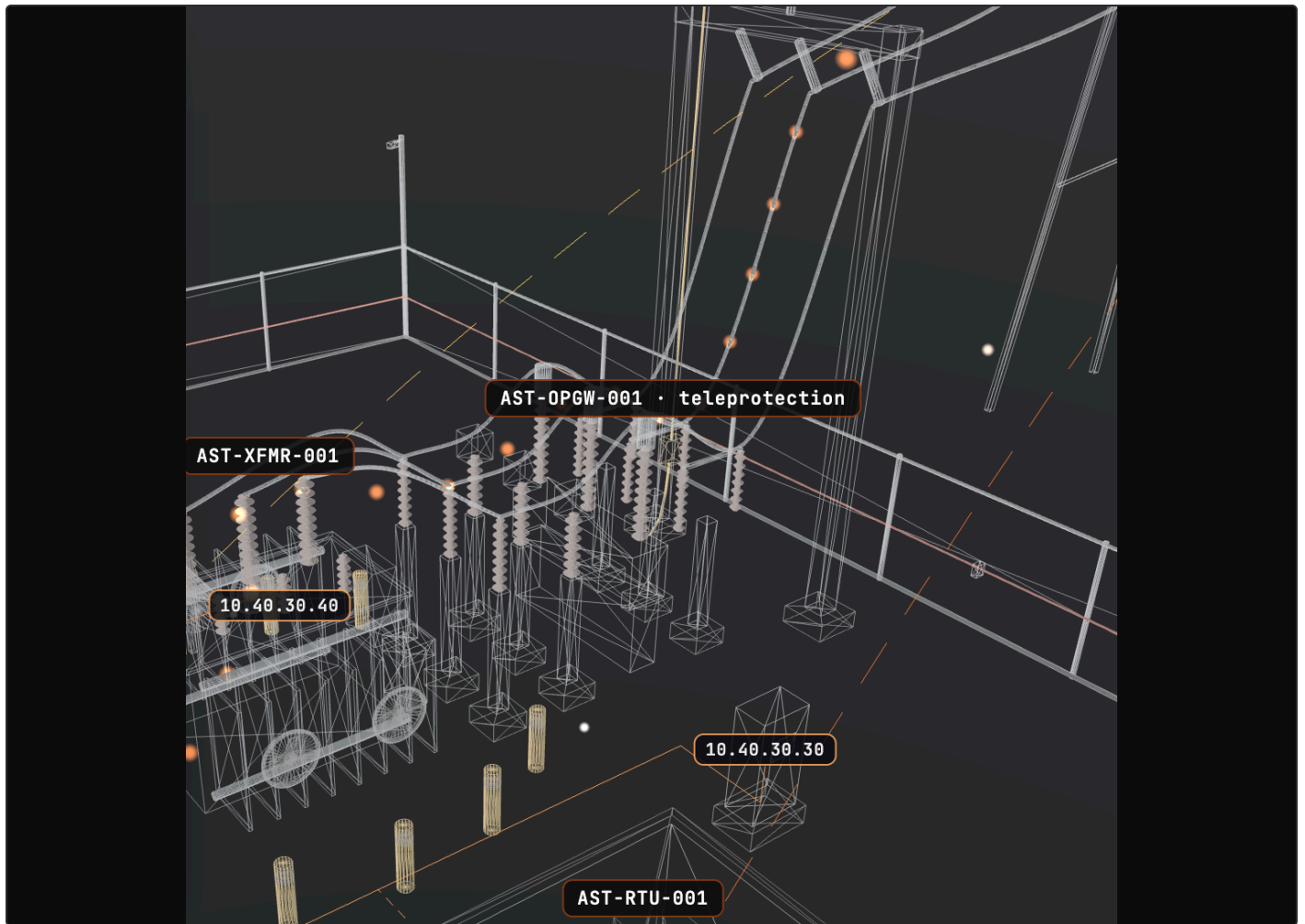


Figure 4. Substation and POI in wire render: main transformer AST-XFMR-001 (monitor 10.40.30.40), surge arresters, CTs, breaker and disconnector, the POI meter (10.40.30.30), RTU kiosk AST-RTU-001 and the teleprotection fibre AST-OPGW-001 running up the gantry to the TSO line. Vehicle barriers ring the transformer. Particles show simulated power flow.

10

Annex I requirements, mapped to evidence

Applies to the products in CRA scope. For the operator the same mapping serves as NIS2 Article 21 evidence.

ANNEX I	REQUIREMENT	TWIN EVIDENCE
Part I (2)(b)	Secure by default configuration	Contactors open until permissives pass (S1); OOB router disabled by default
Part I (2)(d)	Protection from unauthorised access	DMZ, MFA jump host, function-code allow-list; intrusion rejected (S7)
Part I (2)(f)	Integrity of data and commands	Plausibility check rejects SOC 1.05 and +6.5 MW (S7)
Part I (2)(h)	Availability of essential functions	Derate and redistribution on pump trip (S6); genset on loss of grid (S9)
Part I (2)(j)	Limit attack surface	Five external conduits enumerated; diode option removes two
Part I (2)(l)	Record and monitor activity	IDS on SPAN ports, log forwarder, event log in the package
Part II (1)	Identify components, SBOM	Eight-BOM structure keyed to twin IDs
Part II (2), (8)	Remediate without delay, secure updates	One-unit-at-a-time patch procedure with signed baseline check

11

The CRA evidence pack

Digital files

FOLDER	CONTENTS
01-model	Full GLB and glTF, OBJ + MTL, 12 subsystem GLBs
02-structure	Part register, catalogue, bill of materials, assembly tree, materials, system map
03-kinematics	94 mechanisms: bay doors, deflagration vents, fans, disconnectors, gate, barrier
04-controller	Controller logic, 10-step sequence, I/O map, event log, telemetry in the client schema
05, 11	Interface register, connections, anchors; VLAN and IP plan
09, 10, 12	FMEA, safety-critical systems, cascading failures; supplier register; regulatory applicability
06-08, 13	Sources, viewers, validation report, SHA-256 manifest, client baseline copies

Test bench readiness

Twenty automated checks pass: every mesh named, every register record has geometry, all 458 interface endpoints resolve, 72 unique site IP addresses, deterministic replay, ESD opens every contactor, no propagation to adjacent units, and the cyber write is rejected.

Requirements Traceability Matrix

SCENARIO	STEP	RESULT
Startup permissives	S1, S2	ESD, FACP, BMS, thermal, comms and grid permissive before closing
Under-frequency response	S5	Full output in under 1 s at 49.55 Hz
Cooling failure	S6	Derate at 42 °C, recovered on standby pump
Cyber-physical unsafe command (HAZ-003)	S7	Rejected; WAN blocked; control LOCAL + TSO
Thermal runaway (HAZ-001)	S8	Isolation, exhaust, vents, site ESD; no propagation
Loss of primary power (FLT-001)	S9	UPS, genset, ATS transfer and return

NOT YET COVERED

Protection coordination, arc-flash and earthing studies; vendor register maps; UL 9540A data; GNSS spoofing and core-switch loss are listed but not simulated.

Ready for the test bench

One unified data model

Geometry, interfaces, network, controller sequence and telemetry share the client's AST- IDs. A bench engineer who clicks unit 2's BMS sees its register record, IP 10.40.12.10 on VLAN 12, its CAN links to 24 modules, its live simulated state of charge and the event that isolated it.

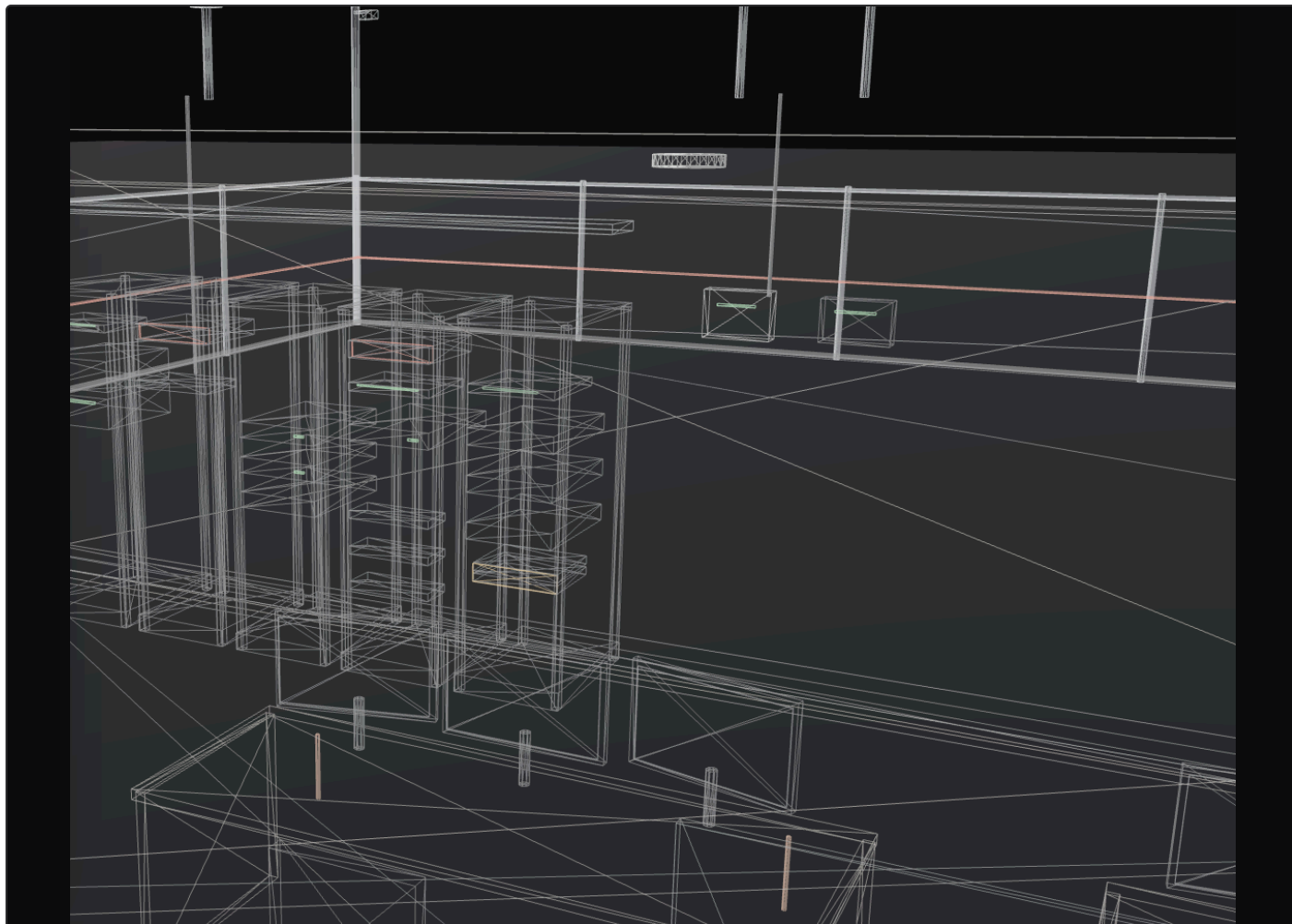


Figure 5. Inside the control house: racks holding the site controller, OT core switch, OT and DMZ firewalls, GNSS clock, historian, IDS, jump host and DMZ replica, with the out-of-band and vendor LTE routers on the back wall. One unified set of IDs links each box to its register record, IP and conduits.

Ten steps through the simulator

The animated twin plays one deterministic loop of about two and a half minutes. Each step changes what moves in the scene and what the controller panel shows, and each can be replayed with its fault switched off.

STEP	WHAT HAPPENS	WHAT TO WATCH
S1 Cold start	ESD loop, FACP, BMS, thermal, comms and grid permissive checked	Contactors stay open until every permissive passes
S2 Synchronise	Disconnecter, POI breaker, RMUs, then unit contactors close	Switching order in the event log
S3 Charge from PV	2.8 MW of PV into the switchgear, 3.4 MW into the units	Yellow PV flow, fans tracking cell temperature
S4 Evening peak	VPP dispatch to 4.0 MW export over IEC 104	Air units running warmer than liquid units
S5 Under-frequency	Grid drops to 49.55 Hz; droop drives full output in under a second	Frequency trace on the EWS trend
S6 Pump trip	Unit 1 loses coolant flow, derates to 50 %, recovers on standby pump	Load moving to units 2–4
S7 Cyber intrusion	Vendor LTE → jump host → EWS → Modbus writes to unit 2 BMS	Red attack packets, IDS alert, write rejected, WAN blocked
S8 Thermal runaway	Unit 2 module 14 vents; exhaust, isolation, vents, site ESD	Smoke, strobes, barrier raised for the fire service
S9 Loss of grid	TSO line trips; UPS, genset start, transfer and return	Genset fan and exhaust, ATS source
S10 Shutdown and LOTO	Breakers open, earths applied, maintenance laptop connects	Transient asset flagged by the IDS

Q1 What is in scope? Scope per twin ID: product, operator or site.	Q2 How does it connect? 458 interfaces, 15 VLANs, five external conduits.	Q3 How does it behave? Deterministic 10-step run with five fault switches.	Q4 What is missing? Studies, register maps, firmware inventory, real IP plan.
--	---	--	---

Vulnerabilities, prioritised the way a bench needs them

Reachability first: a flaw on a device reachable from the vendor LTE path or the VPP tunnel ranks above one on an isolated unit LAN, and anything that can alter BMS limits ranks above anything that can only disturb dispatch.

A checklist for both assessment routes

For CRA products, Module A self-assessment or Modules B + C for important classes. For the operator, the same evidence feeds NIS2 risk management and the interconnection agreement.

Pull, not push: 5S for the test bench

The bench pulls what it needs from the package by ID; the manifest proves which version was tested.

The preparedness service and the go / no-go decision

ILLUSTRATIVE DECISION FOR THE EXAMPLE

Go for a software-in-the-loop bench on the simulator, viewer and network model. No-go for a hardware bench until vendor register maps, the firmware signing chain and protection settings are supplied.

13

For bench testers: a guide

What you can expect

A site you can open in a browser, a simulator that gives the same answer every time, a network you can click through, and records that say what is known and what is guessed.

How to use it

- **Open**
Serve 07-viewer and open the animated twin. Verify SHA256SUMS first.
- **Navigate**
Pick a part; read its twin ID, IP, VLAN, evidence tag and interfaces.
- **Exercise**
Toggle the five faults and the data diode option; compare the event log to sequence.json.
- **Report**
Raise findings against AST- and IF- IDs.

What you will not have to do

Reverse-engineer an architecture from single-line diagrams, guess which items are in CRA scope, or reconcile asset names across documents.

Why use EIGENIA

The same six-phase method and the same package format for every product, from a satellite to a battery site.

BENCH SAFETY

No command from the twin reaches equipment. Safety-function tests run on hardware only behind a physical interlock with a written safety case.

HONEST LIMITS

Geometry is procedural, the IP plan and controller laws are assumed, and no figure is vendor or operator production data.

The technical file, compiled

ANNEX VII ITEM	WHERE IT LIVES
General description and intended purpose	README, part register, bill of materials
Design, development and production	Assembly tree, kinematics, controller logic, I/O map
Cybersecurity risk assessment	Zones, IP plan, interface register, threat trees, cascading failures
Vulnerability handling, SBOM	xBOM skeletons, reporting and patch procedure
Test reports	Validation report, checks.json, event log
EU declaration of conformity	Per product, by its manufacturer; not for the site

FOR THE OPERATOR

The same file is reissued as NIS2 risk-management evidence, with the supplier register supporting Article 21(2)(d) supply-chain security.

What this gives the manufacturer

For a manufacturer, the twin turns "is my product in scope?" into a record per item, with the reasoning attached. For an integrator, it shows which of its boxes sit on a conduit an attacker can reach, and which safety functions must keep working when the network does not. For an operator, it is NIS2 risk-management evidence that already uses its own asset IDs. All three get the same package: a model, a simulator that exercises the controls regulators ask about, an investigative supplier list, and an explicit list of what is still unknown.

BESS-REF-001 holds 195 records, 458 interfaces and 72 network nodes. A real site will hold more. The method does not change with size; the configuration does.

Beyond this reference site

The next step is a client twin: the same package built from as-built drawings, vendor register maps and firmware inventories, connected to a hardware-in-the-loop bench.

FROM REFERENCE TO CLIENT TWIN

A reference package and public sources were enough to build this example; they are not enough to assess a real site. In a client engagement EIGENIA works from controlled registers, drawings, protocol maps, firmware and test data, and the twin that results is a very high-fidelity model of the actual installation.

Sources

REF	SOURCE
[2]	US DOE, Energy Storage Safety Strategic Plan, 2024
[3]	UL Solutions, UL 9540A test method
[4]	Sandia, Physical security and cybersecurity of ESS, 2020
[5]	IEEE 1547-2018
[6]	NIST SP 800-82
[8]	Tesla, Megapack 2 XL datasheet Rev 2.0, 2025
[9]	Town of Pembroke, MP2XL applicant filing, 2025
[10]	Sandia, Cybersecurity considerations for BESS, 2026
[13]	INL, BESS Cyber-Informed Engineering white paper, 2024
[18]	Utility Dive, Cybersecurity concerns for energy storage
[20]	Insane Cyber, BESS cybersecurity, 2026
[22]	NFPA 855
[S1]	Tesla Megapack: Megafactories and LFP cell suppliers
[S2]	Tesla North, Megapacks with US-made LFP cells, 2026
[S3]	Tesla, Form 10-Q, June 2025
[S4]	FCC Covered List
[S5]	ICTally, FCC camera ban 2026
[R1]	Regulation (EU) 2024/2847, Cyber Resilience Act
[R2]	Directive (EU) 2022/2555, NIS2
[R3]	Delegated Regulation (EU) 2022/30 under RED
[R4]	Regulation (EU) 2023/1542, Batteries
[R5]	Delegated Regulation (EU) 2024/1366, Network Code on Cybersecurity

The full list of 24 sources with locators is in 06-sources/SOURCES.md of the twin package.

NO WARRANTY

This case study and the model it describes are a representational example for illustration and education only, without warranty. They make no declaration that any figure, component, configuration or finding is correct for any real product or site. Tesla and Megapack are trademarks of Tesla, Inc.; this work was produced independently from public information and a client-supplied reference package and implies no endorsement or assessment by Tesla or any supplier named. Supplier entries are investigative candidates, not findings. Regulatory summaries are not legal advice.