



THE OPERATIONAL INTELLIGENCE PLATFORM FOR INDUSTRIAL CYBERSECURITY

From Visibility to Understanding.

Industrial environments generate enormous volumes of data. Very little of it becomes understanding. ASTRICS turns industrial telemetry into one shared operational understanding — read by every capability in the platform.

ONE PLATFORM • ONE LANGUAGE • ONE SOURCE OF TRUTH

THE PROBLEM

You can see every asset. You still can't answer the question.

When a critical decision has to be made, teams still reach for spreadsheets, manual processes and institutional knowledge to work out what the data actually means.

Visibility answers *what*.
It rarely explains *why*.

Industrial operations are more than connected devices. Every asset supports a process. Every process supports a business outcome. Every decision carries operational, financial and regulatory consequences. Without context, even the most advanced telemetry is just data.

UNDERSTANDING MEANS KNOWING

- Why an asset exists
- Who owns it
- What depends on it
- What business impact it carries
- What process it supports
- How critical it is
- How it communicates
- Which regulatory obligations apply

Alerts ranked by severity, not consequence

Severity says how bad the bug is. It says nothing about what fails when the asset does.

Compliance rebuilt before every audit

Evidence assembled by hand from registers nobody trusts — then set aside until next year.

Every team keeps its own spreadsheet

Security, engineering, operations and compliance each hold a different version of the same estate. None of them agree.

The challenge isn't seeing more. It's understanding more.

Traditional platforms were built to answer one question — and they answer it well:

“What happened on the network?”

Industrial organisations have always spoken different languages.

Security teams discuss vulnerabilities.

Engineers discuss assets.

Operations discuss uptime.

Executives discuss business risk.

Compliance teams discuss regulations.

ASTRICS brings them together through one operational model — and answers the questions that follow.

- 01 What happened?
- 02 Why did it happen?
- 03 What operations are affected?
- 04 What business processes are impacted?
- 05 Who owns the affected assets?
- 06 What risks should be prioritised?
- 07 Which compliance obligations are involved?
- 08 What should happen next?

That shift turns cybersecurity from an isolated technical function into an operational capability the whole organisation can use.

Not another OT security platform.

Most OT platforms discover assets, decode protocols and generate alerts — then stop. ASTRICS starts where they stop.

TRADITIONAL OT SECURITY PLATFORMS		ASTRICS
Discover assets	→	Understand operations
Decode protocols	→	Create operational context
Generate alerts	→	Deliver actionable intelligence
Technical dashboards	→	Business, operational and compliance intelligence
Multiple disconnected tools	→	One integrated operational platform
Manual asset enrichment	→	Continuous active enrichment
Interaction visualisation	→	Complete architecture and network diagrams
Separate Syslog platform	→	Native event log collection and analysis
Compliance reporting	→	Continuous compliance assurance
Technical data	→	Shared operational understanding

Powered by the ASTRICS Intelligence Core.

Every capability in ASTRICS is built on a single intelligence foundation that continuously understands industrial assets, communications, operational processes, business dependencies and governance requirements. Rather than keeping separate datasets for security, operations, compliance and reporting, ASTRICS enriches one shared operational model — and every decision across the platform is made from it.

Operational	The role every asset plays within industrial processes.
Business	Ownership, criticality, business services and operational priorities.
Architecture	Where assets belong and how they communicate across zones and conduits.
Governance	Lifecycle status, accountability and organisational responsibility.
Compliance	Alignment with IEC 62443 and organisational requirements, through active enrichment.
Threat	Threats prioritised by operational impact — not technical severity alone.

One Intelligence Core.
One Operational Model.
One Trusted Source of Truth.



One understanding. Layered, not stitched.

ASTRICS layers intelligence progressively. Each layer reads the one beneath it and enriches it for the one above — raw industrial data in, operational decisions out.

RAW DATA → DECISIONS

Business Intelligence

Executive Dashboards · Operational KPIs · Business Impact · Compliance Reporting · Decision Support

Operational Intelligence

Operational Workflows · Risk Assessment · AI Assistant · Dependencies · Impact Analysis · Lifecycle Management

Context Intelligence — the ASTRICS Intelligence Core

Operational Context · Business Context · Asset Metadata · Active Enrichment · Criticality · Ownership · Relationships

Industrial Intelligence

Protocols · Communications · Threat Intelligence · Behaviour Analytics · Syslog · Event Analytics · Vulnerability Intelligence

Industrial Environment

Assets · Controllers · Networks · Endpoints · PLCs · HMIs · Servers · IIoT

Every dashboard, alert, workflow, compliance report and AI answer references exactly the same operational understanding.

Four disciplines. One operational model.

ASTRICS is organised the way industrial teams already work — and every discipline reads the same Intelligence Core.

1

Understand

Every asset is continuously enriched with operational, business, architecture, governance and compliance context — so ASTRICS knows what each device does for the plant, not just that it exists.

BUSINESS OUTCOME

One Operational Understanding

ASSET INVENTORY · ASSET PASSPORT ·
SINGLE LINE DIAGRAMS

2

Protect

Communications, protocol behaviour, events, threat and vulnerability intelligence are read inside the operational context they occur in — so every detection is ranked by consequence, not severity alone.

BUSINESS OUTCOME

One Security Posture

RISK QUEUE · EVENTS & SYSLOG

3

Orchestrate

An alert can become an investigation, a maintenance job, a risk assessment, a compliance review, a change request or an executive decision — all from the same understanding. Built-in AI answers in plain language.

BUSINESS OUTCOME

One Coordinated Response

OPERATIONAL ASSISTANT · WORKFLOWS

4

Govern & Assure

Architecture, asset lifecycle, operational risk, IEC 62443 alignment and compliance posture are validated continuously — governance embedded in everyday operations, not an annual reporting exercise.

BUSINESS OUTCOME

One Trusted Operational Record

COMPLIANCE · ZONES & CONDUITS ·
INCIDENTS

Everything becomes part of one continuous operational discipline.

One understanding. Every screen reads it.

The asset register, the architecture diagrams, the risk ranking, the compliance verdicts and the AI answers are all views of one dataset — not separate products stitched together. The pages that follow are concept views of the platform.

Fleet Command

One posture number per obligation, across every site — built to answer “are we defensible today, and where are we not” in seconds, not in a reporting cycle.

- 1

Readiness by chapter

Each control area scored and weighted by the assets actually in scope, so the weakest obligation is obvious.
- 2

Impact-ranked attention list

What needs a decision today, with the plant consequence and the statutory clock beside it.
- 3

Evidence age as a first-class metric

If evidence is stale, the posture is a guess — so freshness is measured and shown.



Asset Passport

One asset's complete operational record — and every value on it carries its source, so an auditor can follow any figure back to where it came from.

- 1

Provenance on every attribute

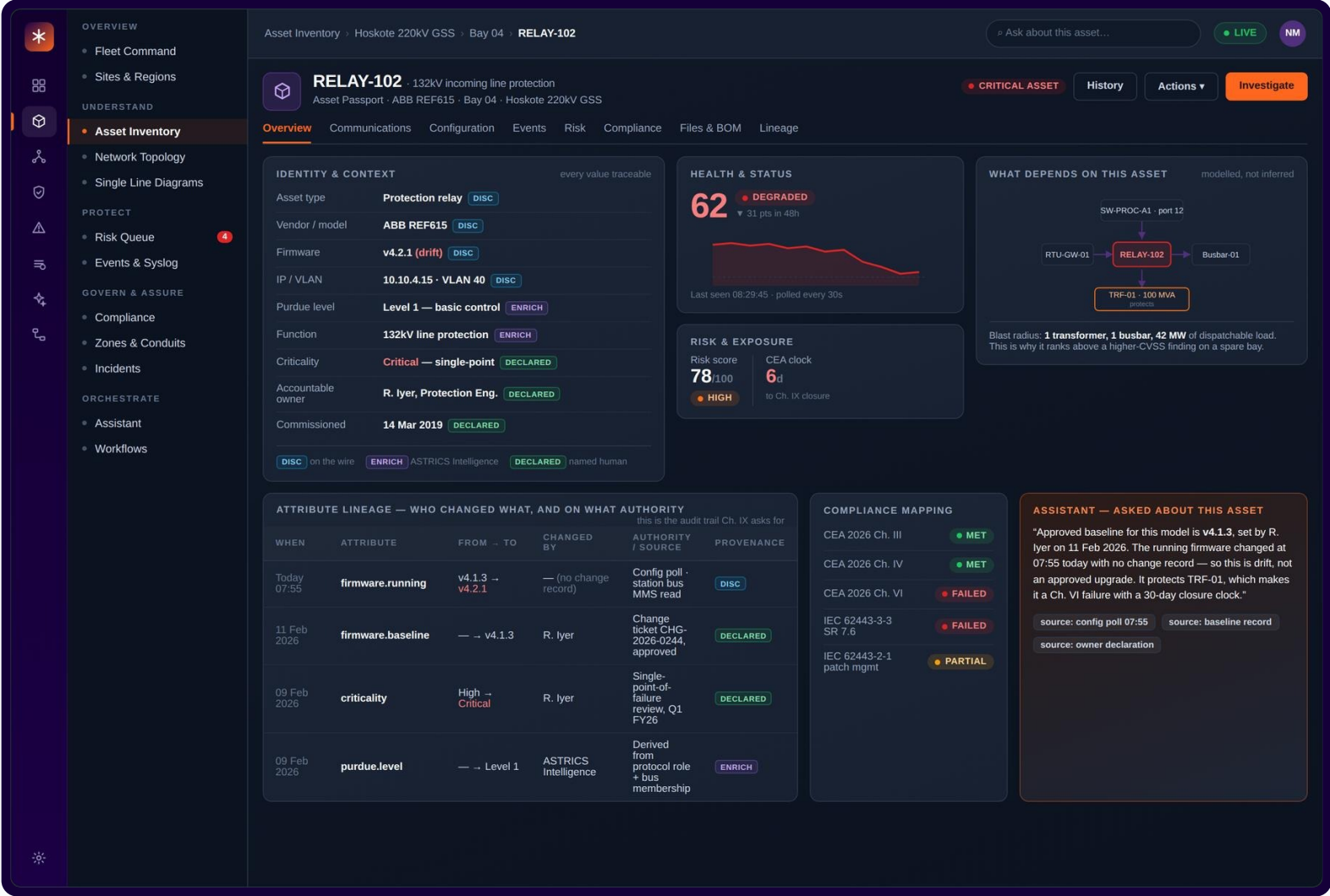
Discovered on the wire, enriched by ASTRICS Intelligence, or declared by a named human owner.
- 2

Blast radius, not just severity

What this asset protects and what fails with it — modelled from declared relationships.
- 3

Attribute lineage

Who changed what, when, and on whose authority: the audit trail Chapter IX actually asks for.



Single Line Diagram with Asset Context Overlay

The engineer's own drawing, alive. Cyber context is painted onto the layer operators already think in, so a finding reads as a bay, a transformer and a load.

- 1

Generated from the live register

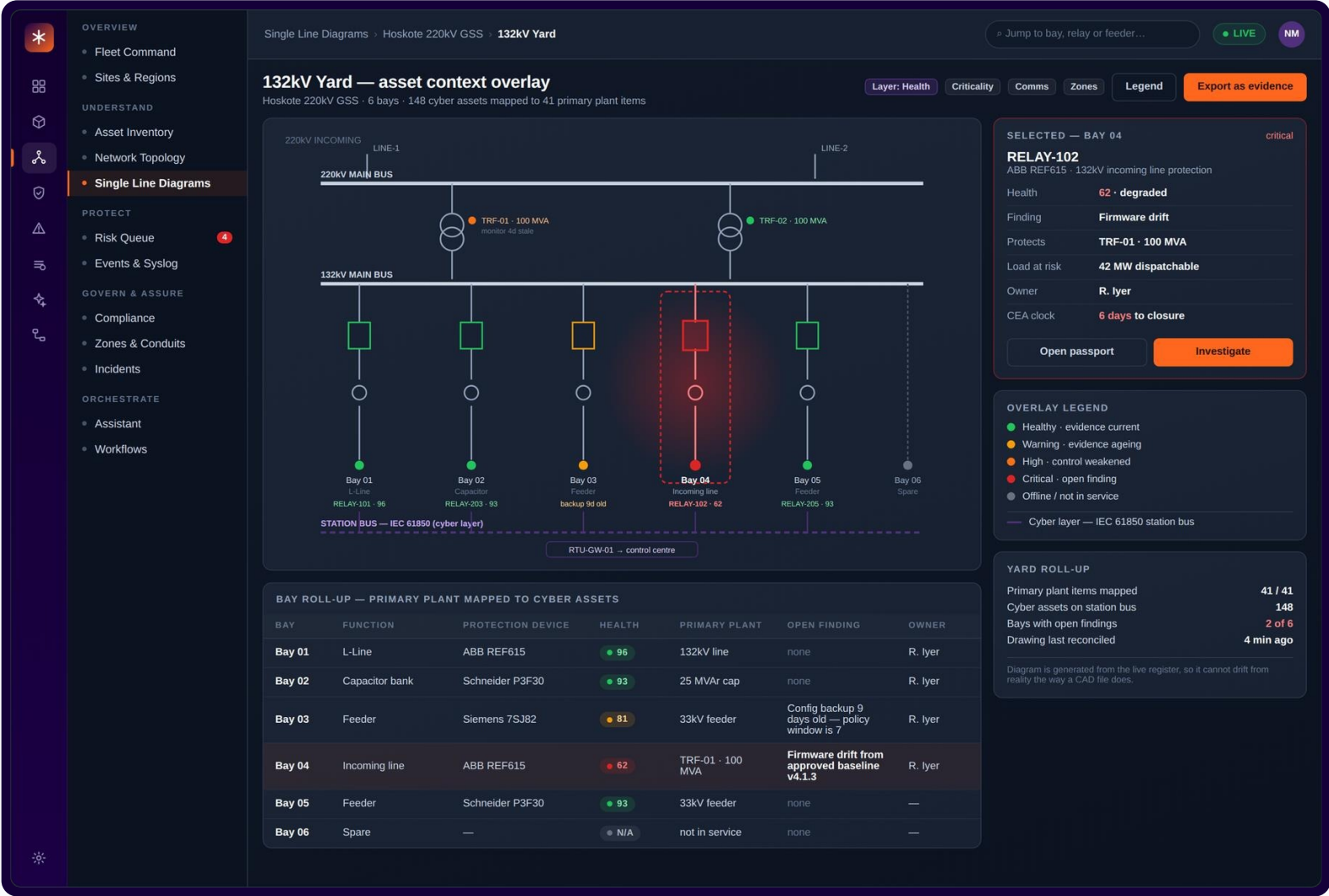
The diagram cannot drift from reality the way a CAD file left in a drawer does.
- 2

Plant mapped to cyber assets

148 cyber assets tied to 41 primary plant items — the mapping is the deliverable.
- 3

Exportable as evidence

The same view an engineer reads is the artefact an auditor accepts.



Compliance Console — CEA 2026 & IEC 62443

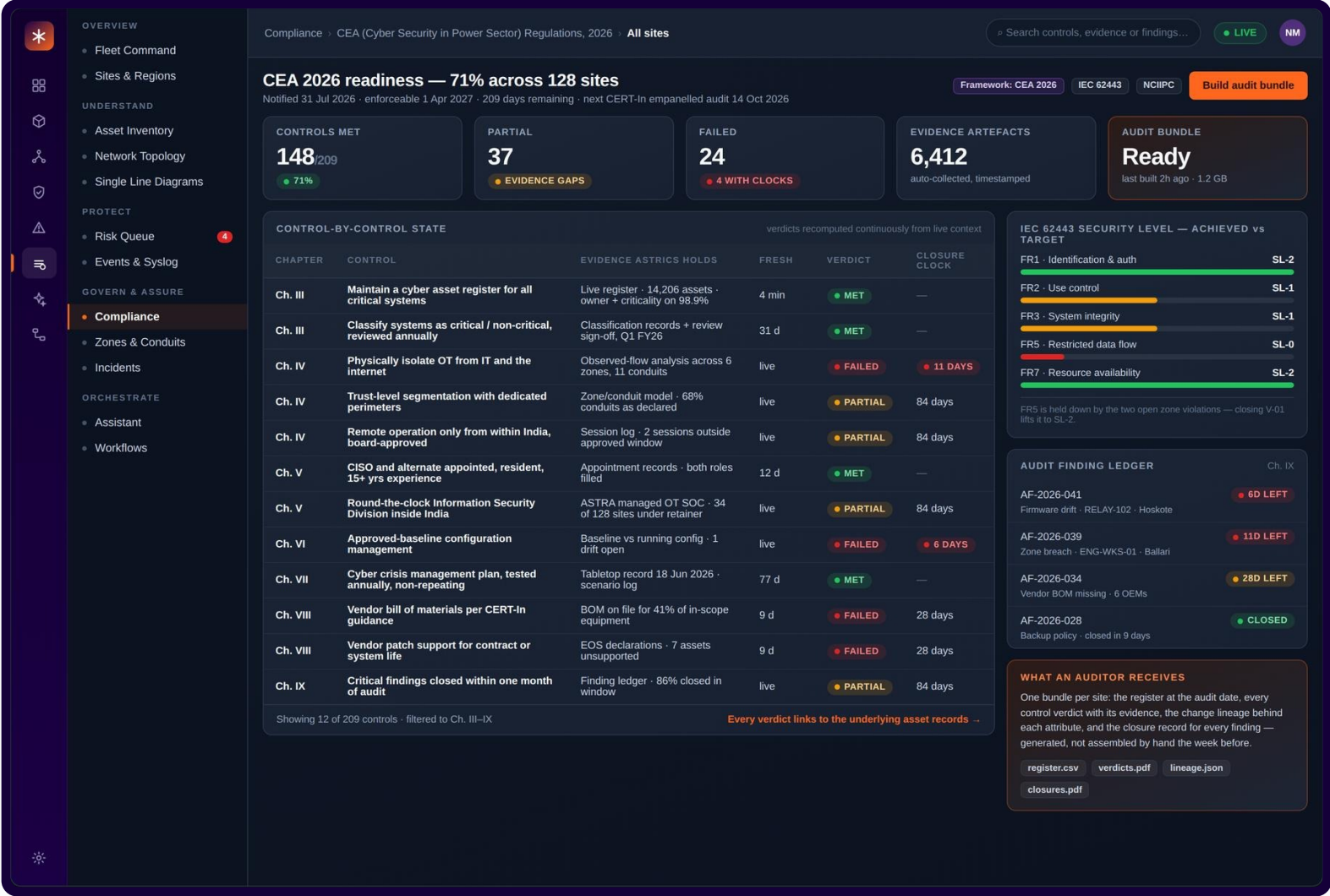
Compliance as a live state rather than an annual project: every control carries its current verdict, the evidence behind it, and the clock attached to any failure.

- 1

Control-by-control verdicts
Recomputed continuously from live context, not reconstructed the week before an audit.
- 2

Findings with statutory clocks
Chapter IX gives 30 days on critical findings — the ledger counts them down.
- 3

The bundle an auditor receives
Register, verdicts, lineage and closures, generated rather than assembled by hand.



The register, and the architecture it has to prove

Asset Inventory — Karnataka — Hoskote 220kV GSS

Asset register — 1,284 assets in scope
Hoskote 220kV GSS · recorded 4 min ago · 12 changes since last audit snapshot

Site: Hoskote 220kV x · Purdue: L1-L2 x · Criticality: Critical x · Add filter

1,284 total · 61 critical · 14 no owner · 1,223 classified

ASSET	TYPE	VENDOR / MODEL	LOCATION	PROTOCOL	PURDUE	CRITICALITY	OWNER	HEALTH	EVIDENCE
RELAY-102	Protection relay	ABB REF615	Bay 04	IEC 61850	L1	CRITICAL	R. Iyer	62	2d
RELAY-101	Protection relay	ABB REF615	Bay 01	IEC 61850	L1	CRITICAL	R. Iyer	96	1d
BCU-04	Bay control unit	Siemens 6MD5	Bay 04	IEC 61850	L1	CRITICAL	R. Iyer	94	1d
TRF-01-MON	Transformer monitor	Qualtron 509	TRF Yard	Modbus TCP	L1	CRITICAL	A. Deshpande	81	4d
RTU-GW-01	Gateway / RTU	SEL-3530 RTAC	Control room	DNP3 - 61850	L2	CRITICAL	S. Nair	92	1d
HMI-SCADA-01	HMI / operator station	Wonderware 2023	Control room	OPC UA	L2	HIGH	S. Nair	90	2d
SW-PROC-A1	Managed switch	Hirschmann RSP20	Bay 01-03	IEC 61850	L1	HIGH	R. Iyer	98	1d
SW-STN-CORE	Station-bus switch	Moxa EDS-4014	Control room	IEC 61850	L2	HIGH	R. Iyer	95	1d
RELAY-205	Protection relay	Schneider P3F30	Bay 05	Modbus TCP	L1	MEDIUM	—	93	9d
MFH-BUS-A	Multifunction meter	Eltrease EM5436	Bus A	Modbus RTU	L1	MEDIUM	—	99	6d
ENG-WKS-02	Engineering station	Del / Win10 LTSC	Control room	MMS - ROP	L2	HIGH	S. Nair	74	3d
GPS-CLK-01	Time source	Meinberg M300	Control room	PTP / NTP	L2	HIGH	R. Iyer	97	1d
CCTV-NVR-01	Physical security	Hikvision DS-96	Perimeter	RTSP	L2	LOW	Facilities	—	21d
UNK-10.20.4.87	Unidentified	—	Bus A VLAN	ARP only	?	UNKNOWN	—	—	0d

Showing 14 of 1,284 · 1 selected

REGISTER COMPLETENESS — ACCOUNTABLE OWNER: 14 assets unassigned · Ch. III blocker: 95.9%

CRITICALITY CLASSIFIED: 61 critical · 1 unknown device pending: 95.2%

PURDUE LEVEL ASSIGNED: needed for Ch. IV segmentation proof: 91.4%

VENDOR BOM ON FILE: Ch. VII — 6 OEMs not yet supplied: 41%

Asset Inventory

The Chapter III register as a living object. Accountable owner and criticality are first-class columns because the regulation asks for them — and completeness against each field is tracked, since an incomplete register is a failed control.

Zones & Conduits — Ballari TPS — Unit 3 — architecture validation

Architecture validation — Unit 3
Ballari TPS · target SL-2 · 6 zones · 11 declared conduits · continuously tested against observed flows

2 VIOLATIONS · Declared vs observed · Generate Ch. IV evidence

PURDUE MODEL — DECLARED ZONES vs OBSERVED TRAFFIC

LEVEL 4S — ENTERPRISE: Corporate IT (not in Ch. IV scope)

LEVEL 3S — DMZ: OT DMZ (National replica · jump host)

LEVEL 3 — SITE OPERATIONS: Plant Operations (Historical · MCS · ring station)

LEVEL 2 — SUPERVISORY CONTROL: Unit 3 DCS (Yokogawa CENTUM VP)

LEVEL 1 — BASIC CONTROL: Turbine Control (Closed loop · vendor-tuned) and Boiler Protection (SL-4000 · no remote access)

LEVEL 0 — PROCESS: Sensors, actuators, field instrumentation

Observed flows that do not match a declared conduit

SOURCE	DESTINATION	PROTOCOL	DIRECTION	FLWS	WHY IT MATTERS	VERDICT
ENG-WKS-01 (L3)	10.44.2.0/24 (corporate)	RDP · SMB	bidirectional	1,284	Creates a routable path from enterprise into Unit 3 supervisory control	VIOLATION
HIST-L3-01	PLC-AC500 *7 (L1)	Modbus TCP R-16	write	96	Write function code on a conduit declared read-only	VIOLATION

last 24h · sampled continuously

SEGMENTATION SCORE: 68 (9 of 11 conduits behaving as declared). SL-2 target requires 2 95% with zero critical breaches.

OPEN VIOLATIONS: V-01: Engineering station (dual-homed) ENG-WKS-01 holds routes to both L3 and corporate. Breaks Ch. IV isolation for Unit 3 OCS. 11 days to statutory closure. V-02: Undeclared write path to BOP PLCs. Observed Modbus writes from L3 historian to 7 * AC500 with no matching conduit declaration. 11 days to statutory closure.

CONDUIT REGISTER: C-01 - DMZ: AS DECLARED. C-02 - L3: AS DECLARED. C-03 - L2: AS DECLARED. C-04 - L1: AS DECLARED. C-05 remote access: DRIFT. C-06 vendor VPN: DRIFT. C-07 - BOP: AS DECLARED.

Zones & Conduits

Chapter IV asks an operator to prove trust-level segmentation, not describe it. Declared zones and permitted conduits are continuously tested against observed traffic, and every mismatch becomes a dated finding.

Deciding what to touch first — and asking why

Risk Queue | All sites | Open | Impact-ranked

61 open findings — ordered by operational consequence

Scoring inputs: asset criticality, declared dependencies, load at risk, compliance clock, exploitability

Rank: ASTRICS Impact | CVSS | EPSS | Bulk assign | Open remediation plan

IF WE RANKED BY CVSS	ASTRICS IMPACT RANKING
1. 9.8 CTV-NVR-01 CVSS: 9.8 (critical) - perimeter camera NVR	1. 94 Firmware drift from approved baseline RELAY-102 - Hoskote 220KV
2. 9.4 HMI-SCADA-08 CVSS: 9.4 (critical) - spare HMI, powered down	2. 91 Engineering station dual-homed to corporate ENG-WKS-01 - Ballari TPS
3. 8.8 PRINT-SRV-02 CVSS: 8.8 (high) - office print server in DMZ	3. 78 Unsupported firmware, vendor EOS declared PLC-AC500 x7 - Bidadi CGPP
4. 8.1 PLC-AC500 x7 CVSS: 8.1 (high) - BOP, no CVSS assigned	4. 72 Undeclared Modbus write path from L3 HIST-L3-01 - BOP - Ballari
5. 7.2 RELAY-102 CVSS: 7.2 (medium) - no CVSS assigned	5. 54 14 assets with no accountable owner Peenya 110KV GSS
6. 6.5 ENG-WKS-01 CVSS: 6.5 (medium) - audit fortified roles, costly weaknesses	6. 48 Config backup beyond policy window SIROTEC 7S382 x3 - Yelahanka
	18. 21 RCE in NVR firmware CCTV-NVR-01 - Perimeter
	27. 12 Auth bypass in HMI package HMI-SCADA-08 - spare

Showing 8 of 61 open findings. The two highest CVSS scores in the estate rank 18th and 27th here — because consequence, not severity, decides what an operator should touch first.

SCORING INPUT — ASSET CRITICALITY: 35%
Decided by the accountable owner

SCORING INPUT — DEPENDENCY BLAST RADIUS: 25%
Modelled plant relationships, not guaranteed

SCORING INPUT — REGULATORY CLOCK: 22%
Days to statutory closure under Ch. IX

SCORING INPUT — EXPLOITABILITY: 18%
CVSS - EPSS - reachability from observed flows

Risk Queue

The same vulnerability data everyone has, ordered by what it would cost this operator. The two highest CVSS scores in the estate rank 18th and 27th here — because consequence, not severity, decides the work.

Operational Assistant | Karnataka estate

If the 132KV incoming line at Hoskote trips this week, what am I actually exposed to — and is anything about it going to fail our next audit?

Three things, in order of how much they should worry you.

- 1. Protection on that line is currently degraded.** RELAY-102 in Bay 04 is running firmware v4.2.1 against an approved baseline of v4.1.3, with no change record behind the difference. RELAY-102 - config pool 07-05. It is the sole protection device for TRF-01, so a trip event has no declared backup path. dependency model - declared by R. Iyer.
- 2. The exposure is 42 MW of dispatchable load.** TRF-01 is a 100 MVA unit feeding Bus-01; the 42 MW figure is the current dispatch on the two feeders behind it, not nameplate. SLB - 132KV West - live.
- 3. Yes — it fails two controls today.** The drift is a Chapter VI approved-baseline failure and an IEC 62443-3-3 SR 7.6 failure. Your CERT-In empanelled audit is 14 October, and the Chapter IX closure window on this finding expires in 6 days, which is the earlier deadline. AF-2026-041 - finding ledger.

The fastest closure is a rollback to v4.1.3 in the Sunday outage window — Bay 04 has no scheduled work, and R. Iyer has closed this class of finding twice before within window. closure history - AF-2025-108, AF-2026-402.

Open RELAY-102 | Show the 42 MW calculation | Draft the change request | Start closure workflow

SUGGESTED NEXT QUESTIONS

- Which other relays are drifting from baseline?
- What else does TRF-01 depend on?
- Show every Ch. VI failure across Karnataka
- Who approved the last firmware change here?
- Can we close AF-2026-041 before 14 Oct?

WHAT THE ASSISTANT IS ALLOWED TO DO

CAPABILITY	DEFAULT	HOW IT IS CONSTRAINED	APPROVER
Read context and answer	ENABLED	Scoped to the sites and zones in the user's role; every answer cites its records	none needed
Draft a change request	ENABLED	Produces a request in the workflow queue — never applies it	Asset owner
Update asset metadata	ON REQUEST	Writes are recorded as ENRICH with the prompt attached to the lineage	Asset owner
Write to a control device	BLOCKED	No path exists in the product — Level 01 writes are outside the platform entirely	not available

HOW THIS ANSWER WAS BUILT

- Resolved the question to plant: 132KV incoming line at Hoskote → Bay 04, Hoskote 220KV GSS
- Read 4 asset records: RELAY-102, TRF-01, Bus-01, SW-PROC-A1
- Traversed the dependency model: 2 hops - stopped at declared plant boundary
- Checked 2 compliance frameworks: CEA 2026 Ch. VI - IEC 62443-3-3 SR 7.6
- Ranked by earliest binding deadline: 6-day closure clock beat the 14 Oct audit date

RECORDS CITED

- RELAY-102 config pool: DISC
- Firmware baseline record: DECLARED
- Dependency: protects TRF-01: DECLARED
- Live dispatch on Bus-01: DISC
- Ch. VI control mapping: ENRICH
- Finding ledger AF-2026-041: ENRICH

DATA SOVEREIGNTY

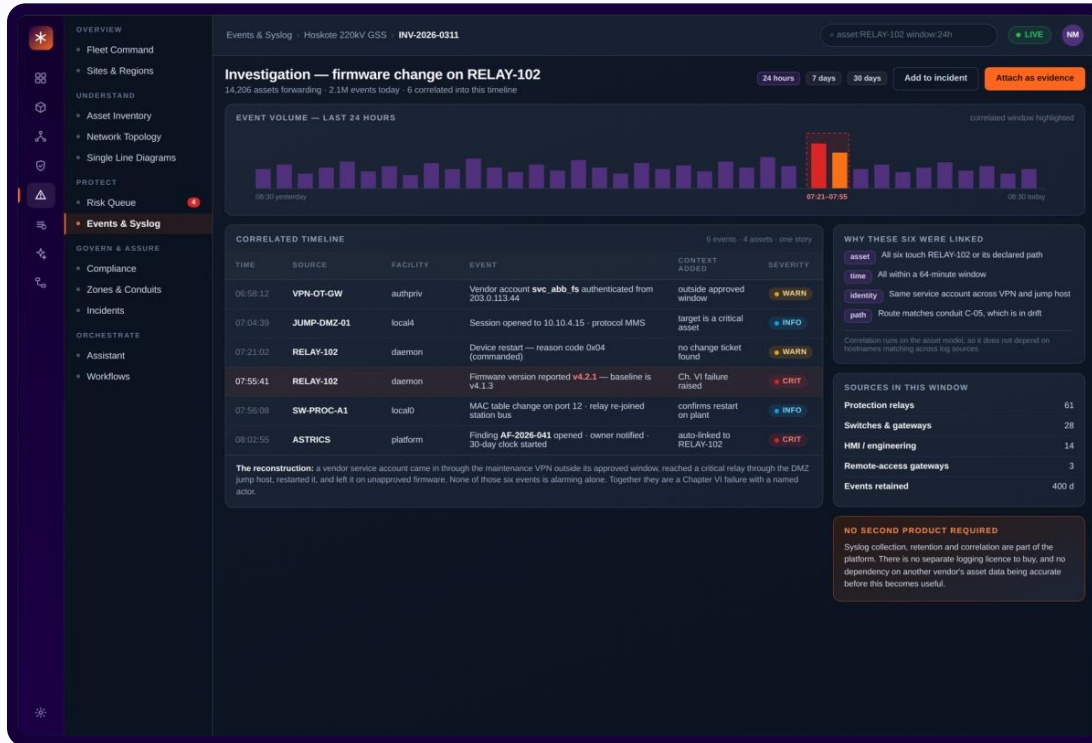
- ON-PREM: Model runs inside the plant network
- NO EGRESS: No asset data leaves the site
- LOGGED: Every query retained for audit

Matters for CEA Ch. IX, which requires remote operation and support to stay within India.

Operational Assistant

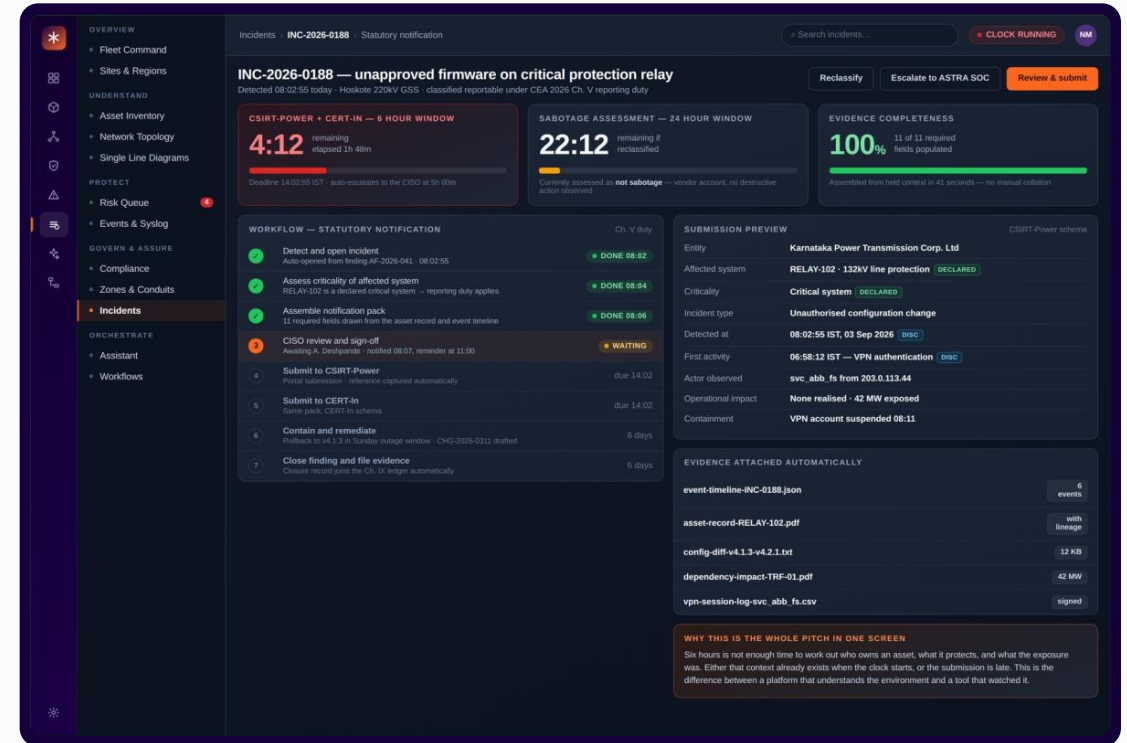
An on-premises assistant that cites the record behind every claim and shows the context it read. Writes to control devices are not a permission it can be granted — that path does not exist in the product.

From six correlated events to a statutory submission



Events & Syslog

Native collection, retention and correlation — no second logging product, and no dependency on another vendor's asset data being right first. Correlation runs on the asset model, not on hostnames matching across log sources.



Statutory Incident Response

CEA 2026 allows six hours to notify CSIRT-Power and CERT-In. The clock, the workflow and the submission all run inside the platform, assembled from context already held.

Deploy it your way. License it simply.

DEPLOYMENT MODELS

- ✓ On-premises
- ✓ Private cloud
- ✓ Hybrid architectures
- ✓ Distributed multi-site, centrally managed

Air-gapped deployment is supported for qualifying environments — ask your ASTRICS team for site-specific guidance.

SIMPLIFIED LICENSING

- ✓ **No feature paywalls**
Understand, Govern, Protect, Orchestrate and Assure travel together as one platform.
- ✓ **No per-tool sprawl**
Built-in Syslog and event analytics replace the need for a separate logging product.
- ✓ **Scales with your estate**
Licensing reflects sites and environments, not artificial technical caps.

Detailed licensing tiers and pricing are provided directly by your ASTRICS account team.

INTEGRATION

Sits alongside your stack — not in place of it.

Open, API-first integration lets ASTRICS share operational intelligence with the SIEM, ITSM and identity platforms your teams already use.

Confirmed integration partners and supported protocols are detailed in the current Technical Integration Guide, available on request.

Understand First. Secure Better.

Built in India. Proven in the field. Designed for the industrial world.

ONE PLATFORM • ONE LANGUAGE • ONE SOURCE OF TRUTH

Industrial cybersecurity isn't just about discovering assets or detecting threats. It's about understanding operations.

See ASTRICS against your own environment. Book a walkthrough with the ASTRICS team and bring one site's worth of questions.

REQUEST A DEMO →

astracyber.one • nikhil@astracyber.one

UNDERSTAND MORE • PROTECT SMARTER • OPERATE BETTER • GOVERN CONTINUOUSLY • SCALE WITH CONFIDENCE