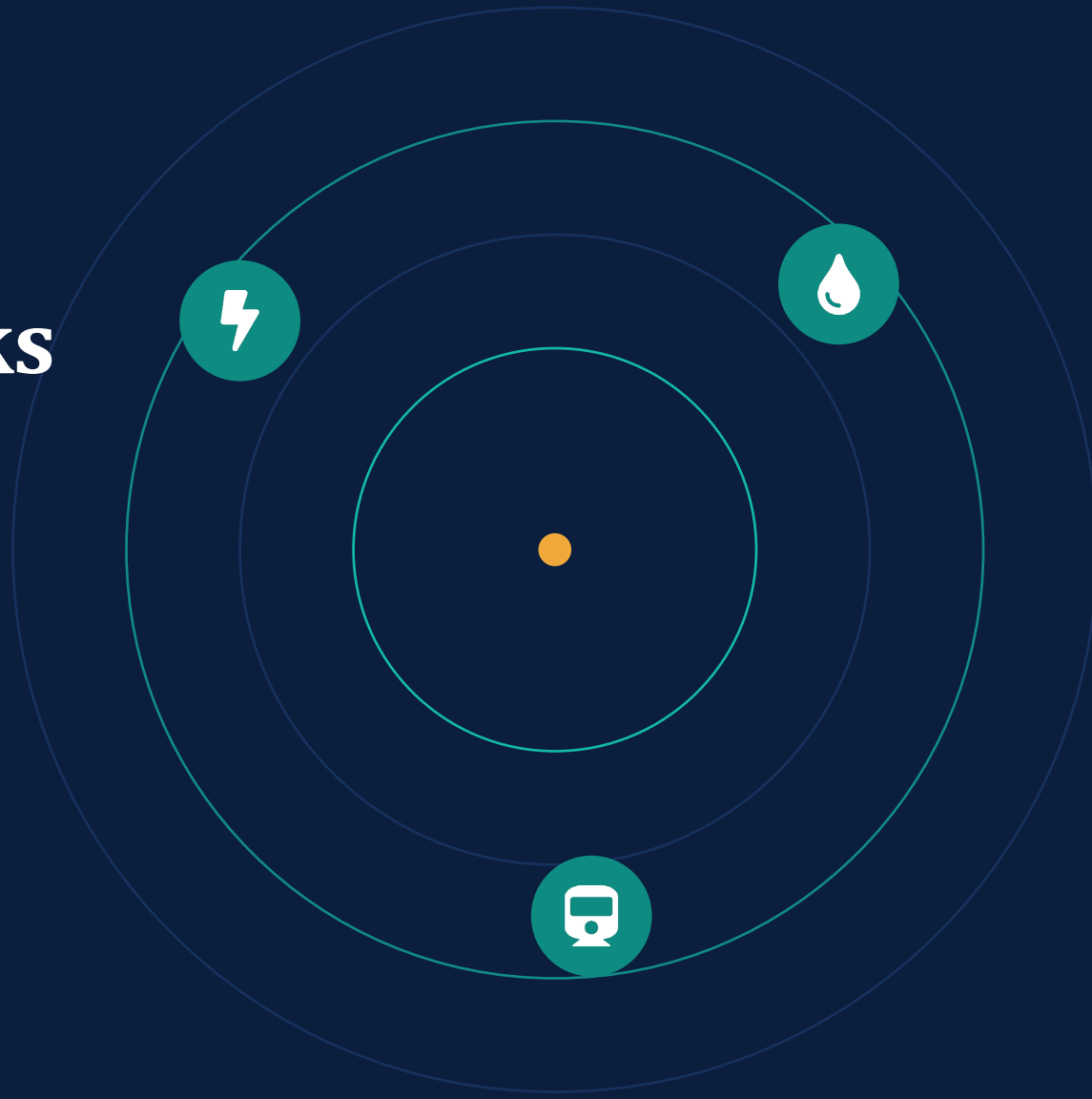
TRUE NORTH
PROGNOSTICS

AI-MSET FOR SCADA OPERATIONS

Catch the intrusion that looks like normal operations

Behavior-based anomaly detection for electric utilities, water systems, and railroad operations



Zero-day
no signature needed

Ultra-low
false and missed alarms

Passive
no scanning of live OT

THE PROBLEM

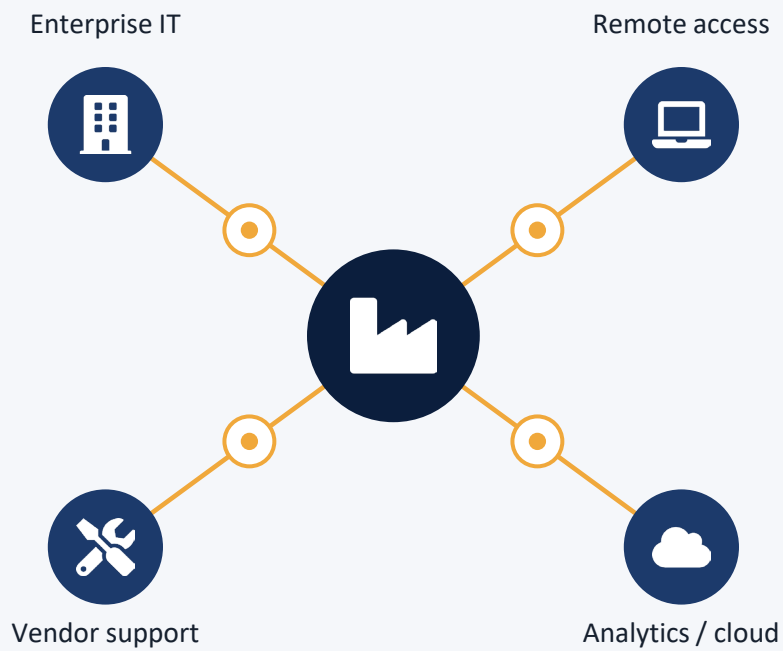
Control systems built for isolation are now connected

Rail and utility control systems were designed decades ago, when separation from outside networks was assumed. That assumption no longer holds.

THEN

Isolated by design

NOW



Attackers blend in

The most dangerous intrusions change behavior slowly and stay inside normal-looking ranges.

IT tools do not fit

OT cannot tolerate frequent scanning, intrusive agents, or a steady stream of nuisance alarms.

Speed decides outcomes

How fast abnormal behavior is noticed determines whether a problem stays manageable or becomes a safety event.

WHERE AI-MSET FITS

Signatures catch known attacks. Behavior catches the rest.

Intrusion detection falls into three families. Each has a blind spot; together they give defense in depth.

Dictionary-based

Signature matching

Compares traffic and logs against a library of known attack signatures.

Strength Few false alarms, simple to run

Gap Blind to zero-day attacks; library needs constant updates

Specification-based

Expert-written rules

Security staff define allowed behavior and policies in advance.

Strength Low false alarms, no profiling stage

Gap Only as good as the rules; gaps and errors are manual

Behavior-based

AI-MSET + SPRT

Learns how the system behaves when healthy, then flags statistically significant departures.

Strength Detects zero-day, malicious intrusion activity from outside, and insider (disgruntled employee, etc) activity; no signature updates

Gap Needs good training data and disciplined tuning, which AI-MSET provides

Complement, not replace. AI-MSET adds a layer alongside signature IDS, segmentation, access control, and incident response.

HOW IT WORKS

From raw telemetry to an alert operators can trust

01

Collect

Network, host, and process signals already produced by the system

02

Condition

IDP and DeQuantize clean, synchronize, and restore signal fidelity

03

Estimate

AI-MSET predicts each signal from its learned correlation relationships with all the others

04

Test

SPRT tests the residuals against preset false- and missed-alarm rates

05

Alert + replay

Actionable alert; Software Black Box Recorder lets analysts scroll back for fast, accurate, deterministic Traceback Root Cause Analysis (RCA)

CONVENTIONAL LOGIC ASKS

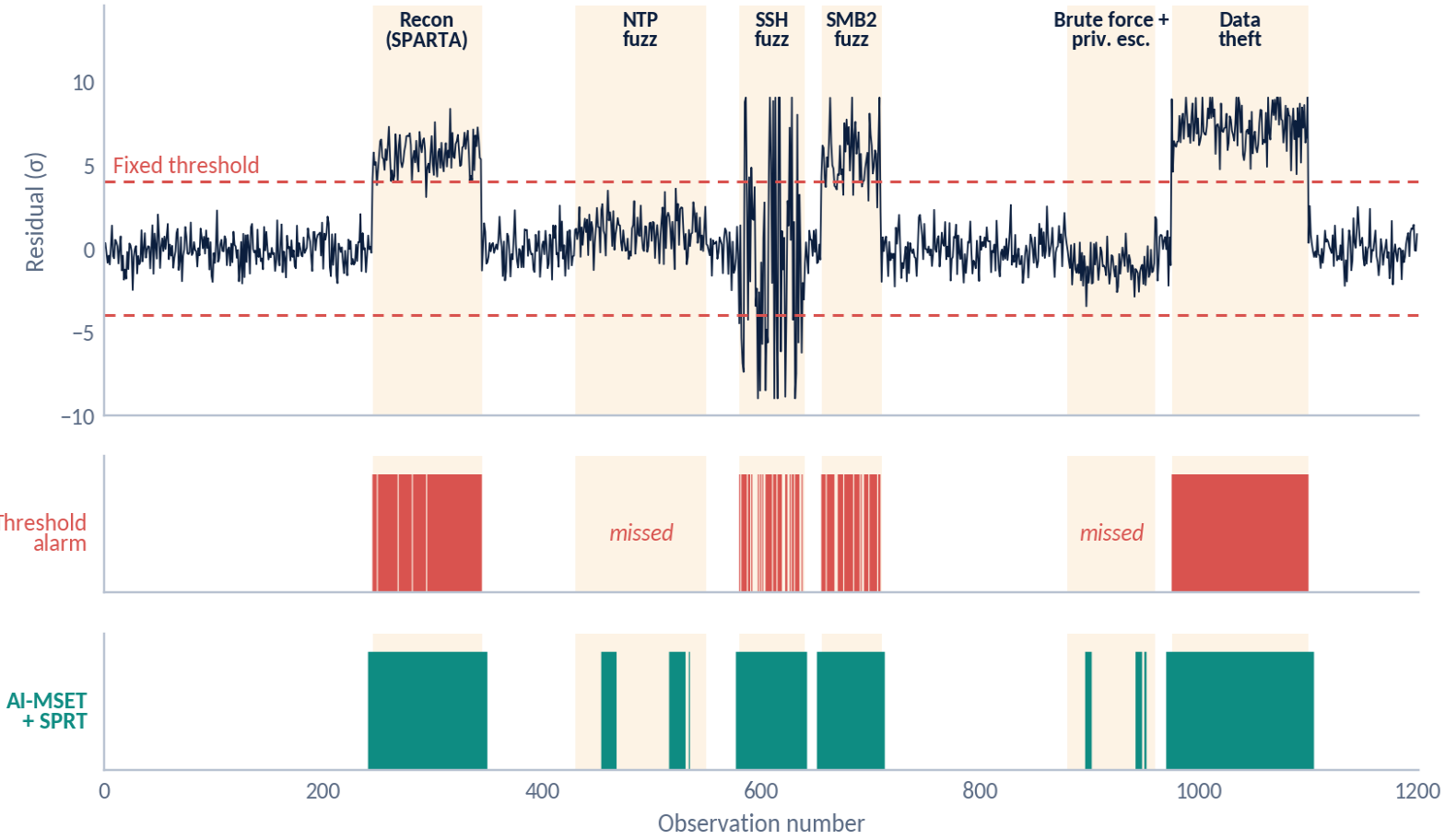
Has any single value crossed its limit?

AI-MSET ASKS

Are the dynamic correlation relationships among signals departing from normal, even while every value is still within limits?

CORRELATION BEATS THRESHOLDS

Quiet attacks slip under a fixed limit. SPRT still sees them.



Illustrative residual patterned on the University of Tennessee Nuclear Analysis Linux Cluster testbed attack sequence (shaded windows).

Attacks detected in this sequence

4 / 6 fixed threshold

6 / 6 AI-MSET + SPRT

Magnitudes differ by orders

In the testbed, the largest residuals were far bigger than the fuzzer and brute-force signatures. A limit set for one misses the other.

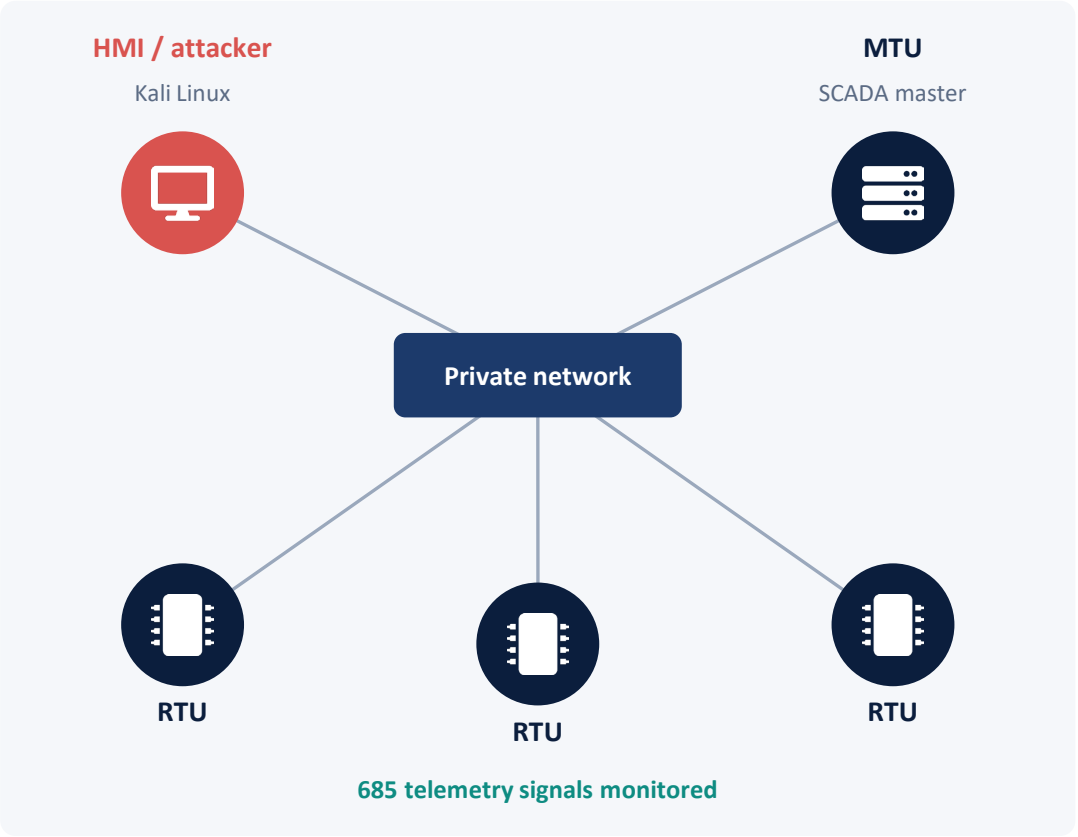
Error rates are set, not guessed

SPRT fixes ultra-low false- and missed-alarm probabilities up front and gives the (mathematically provable) earliest-warning malicious-activity alerts for anomalous patterns (even those “below the noise floor” that are impossible to detect with threshold rules).

EVIDENCE

Tested against real attack tools on a simulated SCADA network

University of Tennessee Nuclear Engineering with Oracle (Jeffries, Hines, Gross). Isolated servers in UT's HPC Nuclear Analysis Linux Cluster emulate the SCADA roles.



ATTACK SEQUENCE

Reconnaissance
SPARTA network and host discovery (Nmap, Nikto, others)

Denial of service
SSH, SMB2, and NTP protocol fuzzers from Metasploit

Brute-force login
SSH password attack until a shell is obtained

Privilege escalation
Meterpreter upgrade to root on a new port

Exfiltration
Files of 100 KB to 50 MB copied off the target

RESULTS

Every intrusion that disturbed the SCADA telemetry patterns was detected

Share of signals in each model group that flagged all six intrusions

Memory / CPU only: just 2 signals caught all six. These metrics still sharpen predictions for the rest of the model.

6 / 6

intrusion types detected by both AAKR and AAMSET model families

4.5–5.1%

average per-signal prediction uncertainty across monitored telemetry

11 of 20

exploits changed telemetry. The other 9 left no trace and belong to signature IDS

Source: Jeffries, Hines, Gross, NPIC&HMIT 2017; UT conference draft. Models were built with UT's PEM toolbox, a non-proprietary MSET-class method. SPRT α = β = 1%.

SCADA for ELECTRIC UTILITIES

Early warning across generation, transmission, and grid control

Small deviations in these systems can escalate quickly. The goal is to see them while there is still time to isolate and respond.

Generation
Turbines, generators, exciters

Transmission
Lines, breakers, relays

Substations
Protection and control, RTUs

Distribution
Feeders, reclosers, switching

Control center
EMS / SCADA, historians

WHAT AI-MSET CORRELATES

- Control commands against the physical response they should produce
- Relay and breaker states against measured currents and voltages
- Polling timing and traffic between master and RTUs
- Host and network metrics on the servers running SCADA itself

WHY IT MATTERS

Abnormal control actions, unexpected responses, and emerging instability show up as broken relationships before a protection trip or an operator notices.

Supports proactive monitoring expectations under NERC CIP without altering required controls.

SCADA for WATER AND WASTEWATER DISTRICTS

Protect treatment chemistry and pumping without adding staff

Many water systems run lean. Behavior-based monitoring gives them continuous watch without a signature team to maintain it.

Intake
Raw water pumps, screens

Treatment
Chemical dosing, filtration

Storage
Tanks, reservoirs, levels

Distribution
Booster pumps, valves, pressure

Control room
SCADA, HMI, historian

WHAT AI-MSET CORRELATES

- Chemical dosing rate against flow and measured residuals
- Pump commands against flow, pressure, and motor power
- Tank levels against pump and valve states
- RTU and PLC communication timing across remote sites

WHY IT MATTERS

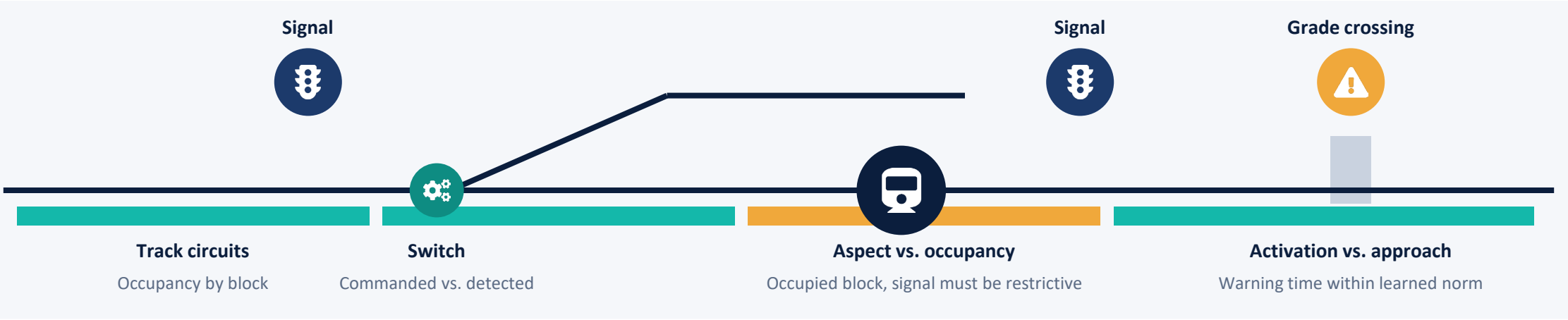
A setpoint change can stay inside every individual limit and still break the physics between dosing, flow, and water quality. That broken relationship is what AI-MSET detects.

Complements AWIA risk and resilience planning and existing utility controls.

SCADA PROGNOSTIC CYBER SECURITY FOR RAILROAD “SWITCH and CROSSING” (S&C) OPERATIONS

Guard the timing and logic that keep train movements safe

Switching, signaling, interlocking, and grade-crossing systems depend on deterministic timing. AI-MSET learns their normal interplay.



Unauthorized control actions

Switch or signal commands that do not match the traffic plan or occupancy state.

Timing anomalies

Crossing warnings, interlocking responses, or comms latency drifting from learned norms.

One engine, two jobs

The same AI-MSET engine also supports rail asset prognostics: locomotive DPUs, Railroad Positive Train Control (PTC) infrastructure, wayside detectors (HBD and Acoustics), bridge structural integrity assurance.

WHY AI-MSET

Built for the constraints of operational technology

Passive

Reads telemetry the system already produces. No scanning or agents on controllers.

No signature treadmill

Complements conventional “dictionary based” security. Proactively detects departures from normal telemetry dynamics, so zero-day attacks do not need a prior entry.

Error rates you choose

SPRT runs with ultra-low preset false- and missed-alarm probabilities, so alerts stay credible.

Light compute

Runs at the edge with far lower overhead than neural-network anomaly detectors.

Deterministic and explainable

Per-signal residuals show which relationships broke, and repeat runs give the same answer. Deterministic traceback root cause analysis (RCA) speeds NTSB and FRA post-event analyses, and Lloyds-of-London (and other) fault attribution.

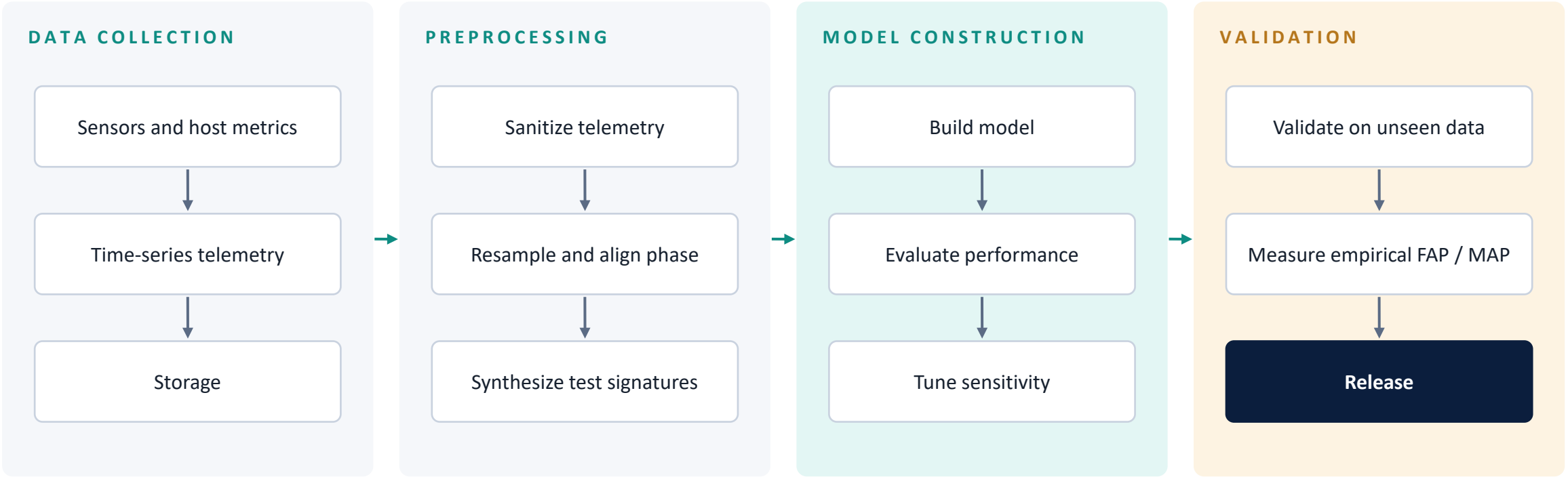
Forensic replay

Software Black Box Recorder with TNP’s proprietary “Zeno’s Circular File” statistical-compression structure keeps a lifetime of telemetry history in a compact storage footprint for fast, accurate, and auditable root cause analyses.

DISCIPLINE

A rigorous path from raw data to a validated model

Detection performance is specified before deployment and measured on held-out data, not assumed.

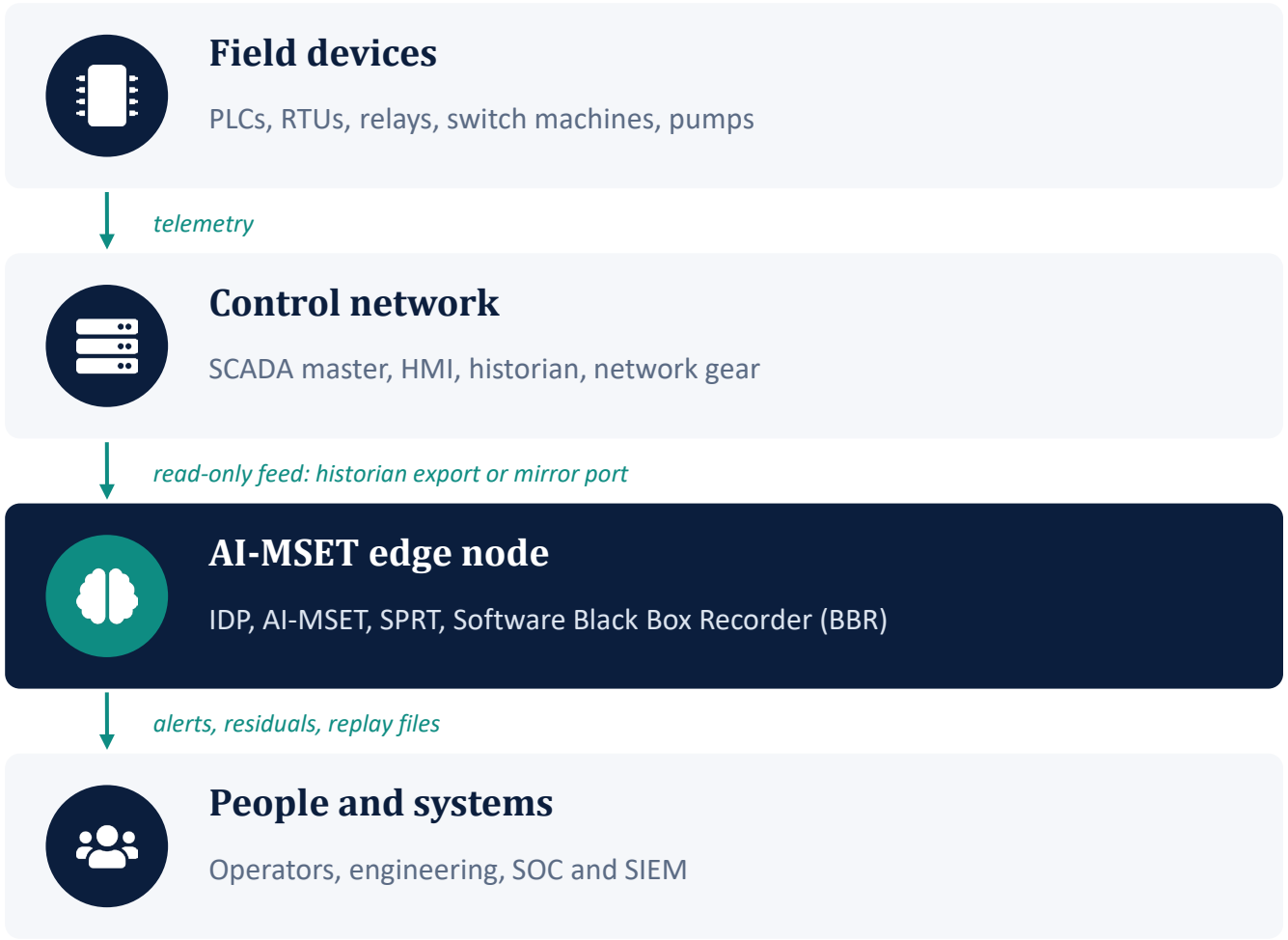


↺ Autonomously iterates optimal sensitivity tuning per empirical signal-to-noise ratios … no subjective human judgment needed

Rigorously and autonomously assures that pre-specified false-alarm and missed-alarm probability Functional Requirements are met↺

DEPLOYMENT

Runs beside existing controls, not in place of them



DESIGN PRINCIPLES

No write path to control

AI-MSET observes; it never issues commands.

Data stays on site

Models run at the edge under customer control.

Fits existing workflows

Alerts flow to the tools operators and the SOC already use.

Supports compliance

Adds evidence for NERC CIP, AWIA, and rail security programs without changing required controls.

NEXT STEP

Prove value in weeks from data you already keep

The fastest proof uses existing data-historian archives. A live pilot is needed only where no telemetry has been saved.

IF: ARCHIVE INCLUDES PAST FAILURES

Paper POC

Weeks no site access needed

YOU SEND

Data from assets that never had problems, plus one or more assets that suffered any undetected event [e.g. malicious intrusion of SCADA systems & networks]

WE SHOW

False-alarm rate measured on the healthy fleet, and how many weeks or months before the event AI-MSET would have flagged the small precursor faults

IF: ARCHIVE, BUT NO FAILURES

Fault-injection POC

Weeks no site access needed

WE DO

Train on archived data, then analytically insert many types of subtle anomalies at controlled sizes

WE SHOW

False-alarm rate on clean data, plus missed-alarm rate and time-to-detect for each anomaly type and size

IF: NO HISTORIAN ARCHIVE

Live pilot

90+ days read-only, on site

WE DO

Collect telemetry read-only, learn normal operation, then challenge with red-team injections in a replica

WE SHOW

Time-to-detect and false- and missed-alarm rates against the tools the operator runs today

Why the archives usually exist. Insurers of high-liability rail and utility assets often require operators to keep historian telemetry, so a major loss can be attributed: e.g. act of nature, maintenance lapse, manufacturing defects, software update errors, human error, or malicious activity. That same record lets AI-MSET prove itself retrospectively.

TRUE NORTH
PROGNOSTICS

THE TAKEAWAY

AI-MSET SCADA Prognostic Cyber Security: Detect abnormal behavior early. Act deliberately, not reactively.

AI-MSET turns cybersecurity for electric, water, and rail SCADA control systems into an operational resilience capability, aligned with the safety and reliability goals operators already have.

Electric **Water** **Rail**