

Utility-Grade Cyber-Physical Red Team

Validating Grid Resilience Against Physics-Aware Adversaries — EMS / PCS / BMS

One of the few red teams validating attacks at the grid-physics layer — not just the IT perimeter.

For utilities and grid-scale BESS operators, the consequential threat is not data theft — it is grid instability, equipment damage, and cascading loss of availability. We validate whether a cyber compromise can cross into the **physical layer** of your energy assets — proven safely on a range that mirrors your operations, never your production estate.

THE ENGAGEMENT MODEL

- **We build a digital twin of your operations.** A containerised cyber-range replicates your specific EMS/PCS/BMS architecture, communication protocols, and control logic.
- **We run the destructive tests on our range — not yours.** Every high-consequence scenario is executed in a fully isolated environment, so nothing touches live grid assets.
- **We hand you the controls.** You receive prioritised, engineering-grade mitigations mapped to each validated weakness — not a generic best-practice binder.
- **Physics-aware, not perimeter-only.** We assess whether an IT-layer foothold can be pivoted into a genuine cyber-physical consequence.
- **Detection-ready output.** Every scenario ships with the forensic artefacts your SOC needs to build detection rules. Optional hardware-in-the-loop — bring your own PCS/BMS units for non-destructive lab validation.

ATTACK CLASSES WE VALIDATE

PLL / Phase-Mismatch & Grid-Sync Manipulation

Whether power-conversion sync integrity can be disturbed via the control path — and whether your SOC would see it as a cyber indicator rather than a grid fault.

False State-of-Charge (SoC) Injection

Whether manipulated battery telemetry can drive unsafe dispatch decisions at the EMS, affecting reserve integrity and pack health.

BMS Firmware-Downgrade & Integrity

Whether battery-management safety firmware can be rolled back or tampered with, and whether your fleet can detect an unsigned or downgraded image.

EMS Ransomware & Operational Blindness

Whether loss of EMS visibility during a peak event leaves operators without a safe manual dispatch path.

BLE / CAN Trust-Boundary Weaknesses

Whether local control-bus and wireless interfaces accept commands they should reject — unknown devices, unauthenticated writes.

IT-to-OT Pivot & Kill-Chain Validation

Whether a low-impact web/EMS foothold can be chained toward high-impact grid consequence — the pivot NERC CIP is designed to prevent.

HOW WE WORK

- 1 Scoping Workshop**
Map your EMS/PCS/BMS estate & risk priorities
- 2 Range Build**
Digital twin of your ops & protocols
- 3 Validation**
Destructive tests, safely, on our range
- 4 Risk Heatmap**
Likelihood vs impact, per scenario
- 5 Controls Handover**
Engineering fixes & SOC watchlist

STANDARDS ALIGNMENT

NERC CIP-002 / 007

Demonstrates how impact classification must account for IT-to-grid pivots.

IEEE 1547 / UL 1741

Validates grid-interconnection safety-parameter integrity.

CISA / DOE — CIE

Aligned to Cyber-Informed Engineering principles.

LEADERSHIP

Rahul Modak

Co-Founder & CEO · Technical Lead

30+ years in applied Bayesian statistics across capital markets and retail; co-developer of the MW Framework.

Dr. Rahul Walawalkar

Co-Founder & Executive Chairman

20+ years in energy storage research and commercialisation; CMU faculty affiliation; co-developer of the MW Framework.

WHAT YOU RECEIVE

- **Cyber-Physical Risk Heatmap** — every scenario rated on likelihood vs impact; and a **Mitigation Playbook** of specific engineering controls for EMS, PCS, and BMS.
- **SOC Watchlist** — forensic artefacts to hunt in your SIEM; and an **Executive & Engineering Debrief** for both board and control room.

Book a scoping workshop.

We'll map your architecture, agree the validation scope, and stand up a range that mirrors your operations — so you know how your assets behave under attack before an adversary finds out for you.

Rahul Modak

rahul.modak@bayesiananalytics.in
+91 91674 72453