

BESS Cyber-Physical Red Team Range

A controlled, fully instrumented environment where your team watches real cyber-physical attacks play out against Battery Energy Storage operational technology — the Battery Management System (BMS), Power Conversion System (PCS) and Energy Management System (EMS). Everything runs safely on our range, so you learn how these attacks behave **before** an adversary attempts them against a live plant.

SEE THE CHAIN

Watch a cyber intrusion turn into a physical consequence, stage by stage.

TEST CONTROLS

Check whether your controls detect and contain each stage — or miss it.

BENCHMARK READINESS

An honest read on detection and response times under pressure.

PRIORITISE FIXES

Leave with a ranked view of gaps and the controls that close them.

THE NINE DEMONSTRATIONS

Each maps to a control your regulator already expects — the CEA power-sector cyber rules, plus CERT-In for detect-and-report.

#	DEMONSTRATION	LAYER	WEAKNESS EXERCISED	CONSEQUENCE ON THE RANGE	MAPS TO (CEA / CERT-IN)
01	Control-bus command injection	BMS	No authentication on control bus	Forced overcharge / discharge; thermal risk	CEA · logins & access
02	False state-of-charge injection	BMS	No validation of critical parameters	Over-discharge; accelerated ageing	CEA · data accuracy
03	Phase-offset via session hijack	PCS	Weak OT web-session control	Grid-sync instability; inverter stress	CEA · access + OT
04	Firmware downgrade	BMS	Weak update governance; no rollback	Safety limits removed; old flaws return	CEA · firmware & vendors
05	Operations-server ransomware	EMS	Weak access control; stolen creds	Operator lockout; plant runs blind	CEA · access + CERT-In
06	Credential brute-force / spray	EMS	Weak passwords; no lockout	Full admin compromise of the EMS	CEA · logins & access
07	Command replay	BMS	No sequence / freshness check	Valid command amplified into unsafe	CEA · OT commands
08	Firmware corruption	BMS	No firmware integrity check	Controller bricked; safety off	CEA · firmware & vendors
09	Operator-facing data deception	EMS	No input validation / cross-check	Misinformed dispatch; stealth degradation	CEA · data accuracy

Under all nine — CERT-In. You must detect the incident, report it within 6 hours, and keep 180 days of logs to prove what happened. Where the logs weren't kept, cause cannot be shown — the range tests whether you would have the evidence.

Controls validated

Evidence of which existing defences actually fired against each scenario, and which stayed silent.

Preparedness benchmark

A measured baseline of how quickly your people and tooling detect, decide and respond.

Remediation roadmap

A prioritised set of fixes, mapped to the layer, the weakness, and the CEA control each addresses.

Grounded, not hypothetical. Every scenario in the suite corresponds to a documented real-world incident or peer-reviewed research. All demonstrations are reproduced in isolation on our range — never executed against production assets, and delivered as a defensive readiness exercise.

Mapping is indicative, in plain language. CEA Cyber Security Guidelines (2021, in force) and the draft Cyber Security in Power Sector Regulations (2024); grid storage is Critical Information Infrastructure under Indian law.