SAFETY: THE OVERLOOKED METRIC IN BESS LTSA AVAILABILITY

Advanced Energy and Environmental Solutions / Adam Han, Rasheedah Ladd

ESS Safety and Reliability Forum June 2-4, 2026

EXECUTIVE SUMMARY

Availability in battery energy storage systems is typically discussed through equipment performance and contractual metrics, especially under long-term service agreements (LTSAs). Field audits suggest an important additional layer: safety-related conditions often appear before reported availability losses, even when standard dashboards and monthly reporting do not yet show a clear problem.

This poster presents anonymized, audit-based observations from operating BESS sites. The emphasis is not on rare catastrophic failures, but on conditions visible during normal operations that can increase outage likelihood or extend recovery duration once an abnormal condition occurs. These include gaps in maintenance verification, hazard controls, emergency-plan control, documentation quality, and interfaces between owner, operator, and vendor.

METHODS / AUDIT APPROACH

This poster synthesizes field-audit observations from operating BESS sites using an operational evidence lens. Evidence inputs include maintenance records, monthly performance reports, corrective-action closure, emergency-plan and training records, and system-interface documentation. The method is observational rather than failure-forensic: the aim is to identify precursor conditions that may increase outage likelihood or extend recovery duration before those conditions become visible in standard availability reporting. This poster does not present a legal opinion and does not claim a site-specific root cause unless explicitly documented elsewhere.

AVAILABILITY / LIABILITY / SYSTEM-EXIT STATE

A severe thermal event is not merely another low-availability month. It is a **system-exit condition**: availability can collapse to zero, the asset may be partially or fully unrecoverable, and routine performance accounting gives way to incident response, contractual resolution, of organizational and individual duty of care. In that setting, prior maintenance evidence, emergency-planning records, training logs, and escalation history can matter far beyond the monthly

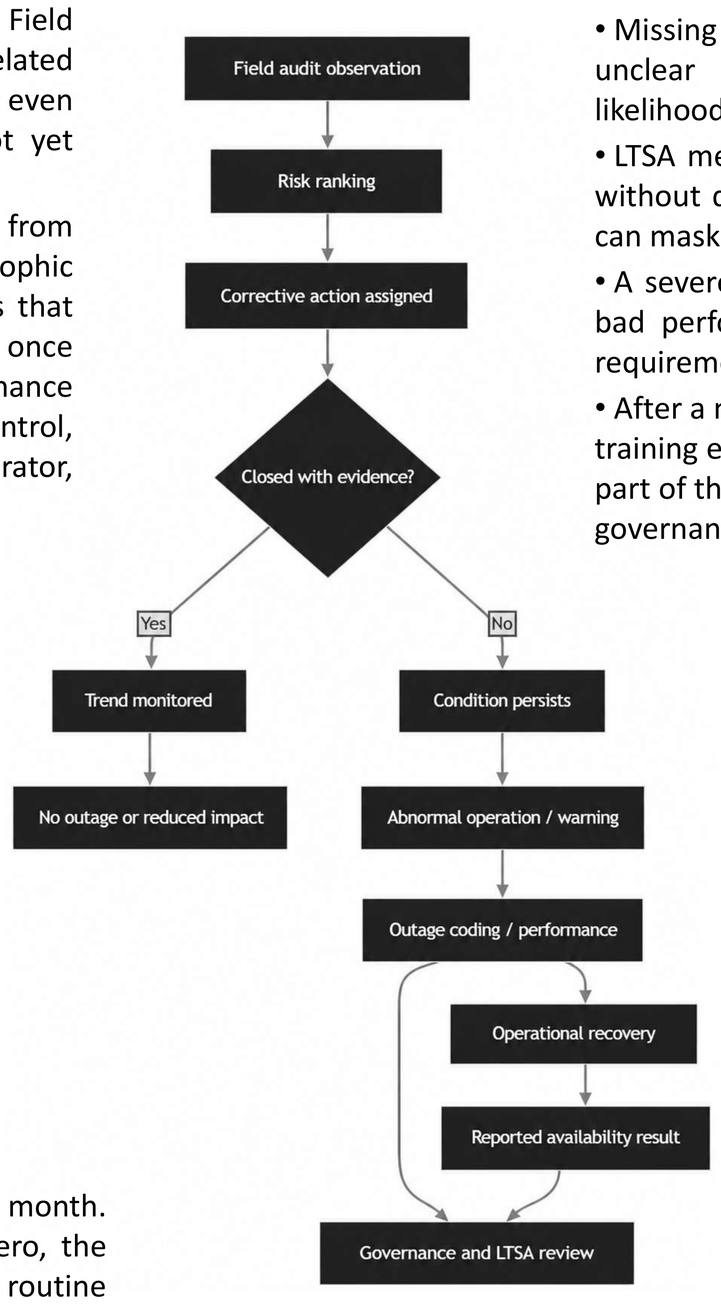

Fig 1. Audit-to-Outage Relay

The Audit–Outage Relay illustrates how audit-observed conditions build into conditions that ultimately drive outages.

KEY TAKEAWAYS

- Safety-related precursor conditions can appear before availability losses are formally counted or explained.
- Missing maintenance evidence, weak monthly-report review, and unclear owner-vendor interfaces can increase both outage likelihood and recovery duration.
- LTSA metrics and LD calculations are necessary but incomplete; without documented review and attribution, the reported metric can mask operational debt.
- A severe thermal event is a system-exit condition, not simply a bad performance month. Fire, emergency action, and recovery requirements move the case into a different governance regime.
- After a major event, maintenance records, emergency plans, training evidence, and escalation history may be scrutinized as part of the evidentiary record. This is an operational and governance point, not a legal opinion.

CASE OBSERVATIONS

- **Thermal Event informed composite-** A site shows significant underperformance against its availability guarantee, the LD review method is not formally documented, and monthly maintenance descriptions are incomplete. Presented as a composite, this illustrates how performance stress, incomplete evidence, and weak governance can coexist before escalation.
- **Maintenance evidence gap-** Scheduled battery or fire-suppression work appears on plan, but inspection reports are missing or do not clearly describe what was done. The problem is not clerical; it reduces confidence in actual asset condition and in whether corrective actions were truly closed.
- **Emergency-plan and responder interface gap-** Training or response materials exist, but version control, external responder documentation, or role clarity are incomplete. In an abnormal event, that kind of gap can extend restoration even if the initiating technical fault was manageable.

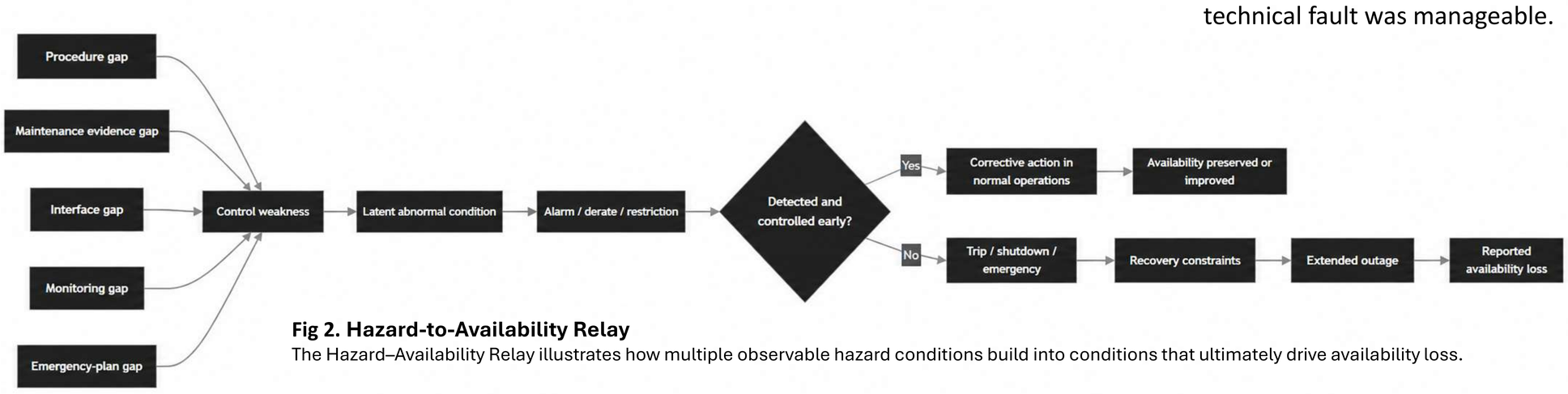

Fig 2. Hazard-to-Availability Relay

The Hazard–Availability Relay illustrates how multiple observable hazard conditions build into conditions that ultimately drive availability loss.

POTENTIAL CATASTROPHIC FAILURE ASSESSMENT

Degradation and control conditions can increase proximity to catastrophic failure pathways. Emergency readiness influences outcome severity.

SITE	OPERATIONAL CONDITIONS AND CONTROLS (0 = Best / Low Exposure, 1 = Worst / High Exposure)				POTENTIAL FIRE EXPOSURE
	L — LD / Unexplained Capacity Loss / Unavailability	D — Detection / Monitoring Sensitivity	C — Control / Escalation / Verification	E — Emergency Readiness / ERP Accessibility / Responder Coordination	
El Cajara	1.0	0.7	0.8	0.6	4.16
Vista Verde	1.0	0.7	0.8	0.6	4.16
Stonegate	0.6	0.7	0.8	1.0	3.67
Highmont	0.6	0.6	0.6	1.0	3.07
Elliridge	0.6	0.6	0.6	1.0	3.07
Eastvale Channel	0.6	0.6	0.6	1.0	3.07
Miravale	0.8	0.5	0.8	0.6	2.94
Tortuga	0.6	0.6	0.6	0.8	2.52
Northvale	0.6	0.6	0.8	0.6	2.35
Fairbridge	0.6	0.6	0.8	0.6	2.35
Migara	0.4	0.4	0.6	0.6	1.22

EXPOSURE LEGEND	LOW EXPOSURE	MODERATE-LOW EXPOSURE	MODERATE-HIGH EXPOSURE	HIGH EXPOSURE	VERY HIGH EXPOSURE
	0.00 – 1.49	1.50 – 2.49	2.50 – 3.49	3.50 – 4.00	≥ 4.01
	Lower exposure to catastrophic failure	Some exposure; monitor and manage	Elevated exposure; take action to reduce risk	High exposure; prioritize risk mitigation	Very high exposure; immediate attention required

PRACTICAL RECOMMENDATIONS FOR ASSET MANAGERS

- Track precursor conditions separately from reportable outages: unresolved alarms, incomplete maintenance evidence, open corrective actions, emergency-document defects, and *interface-control* gaps.
- Require evidence-based closure of maintenance and corrective work, not status-only closure. Reconcile CMMS status, vendor reports, punch lists, and operating restrictions.
- Add formal monthly review procedures for performance reports and LD calculations to LTSA governance.
- Maintain one controlled emergency-action and response package, with version control, responder distribution, and a documented training log.
- Run recovery-readiness drills that test restart authority, alarm clearance, escalation ownership, and return-to-service evidence.
- Treat severe thermal events as **system-exit scenarios** in risk governance. Predefine who owns technical facts, external communications, regulatory interface, and document preservation.