Safety: The Overlooked Metric

in Emerging BESS Reliability

Emerging BESS duty profiles and reliability expectations may expose operational conditions before availability degradation becomes formally visible.

SESSION: Safety Considerations for Emerging Applications — New Duty Profiles, New Reliability Expectations
ADAM HAN RASHEEDAH LADD
AEES

The Shift in BESS

- Higher cycling frequency
- Rapid dispatch requirements
- Extended standby periods
- Faster restart & recovery expectations
- Tighter LTSA availability guarantees

KEY POINT

Traditional availability reporting may lag underlying operational degradation.

Core Thesis

Safety conditions can be leading indicators of reliability degradation.

They are not separate from operations or availability.
They may be the first visible signals that:

Degradation is unresolved

Detection is weak

Escalation is incomplete

Recovery readiness is uncertain

The Reliability Gap

AVAILABILITY METRICS

Everything buried in a single number

LAGGING INDICATOR

- X Missed availability guarantee
- X Unplanned downtime
- X System derates
- X Missed performance guarantee

VS

AUDIT & SAFETY SIGNALS

All records tell a cohesive story

LEADING INDICATOR

- → Unresolved alarms
- → Incomplete maintenance evidence
- → Unclear vendor accountability
- → Weak escalation pathways
- → Emergency-plan gaps
- → Incomplete corrective-action closure

New Duty Profiles Stress More Than Equipment

- Equipment
- Controls
- Procedures
- Operators
- Vendors
- Emergency Response
- Documentation
- Governance

Reliability is no longer only about hardware performance, it is also about whether operational controls can keep up.

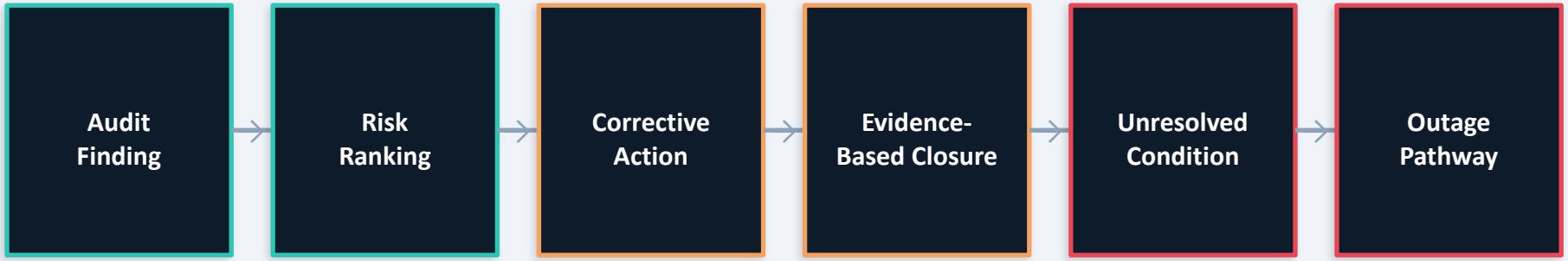
SYSTEM-EXIT CONDITIONS

A severe thermal event is not just another low-availability month.

It is a system-exit condition:

- Availability may collapse to zero
- Asset may be partially or fully unrecoverable
- Recovery becomes uncertain
- Incident response replaces routine performance management
- Records, training, escalation, and maintenance history become critical

Audit-to-Availability Relay



KEY POINT

Reliability degradation often progresses operationally before it becomes obvious in performance metrics.

Deferred Liability Transfer

Unresolved operational conditions can migrate:

FROM

- Maintenance issue
- Vendor issue
- Availability issue

TO

- Outage event
- Emergency response
- Insurance issue
- Governance issue
- Liability exposure

POTENTIAL CATASTROPHIC FAILURE ASSESSMENT

Audit-informed framework evaluating operational conditions and proximity to catastrophic failure pathways.

L

Loss / Degradation

LD penalties, unexplained capacity loss, unavailability

D

Detection

Monitoring sensitivity, alarm coverage, visibility into degradation

C

Control

Escalation pathways, verification protocols, corrective action closure

E

Emergency Readiness

Responder coordination, ERP/EAP currency, recovery preparedness

Audit-informed assessment only — not a site-specific root cause claim.

How to Read the Assessment

The assessment separates two distinct ideas:

OPERATIONAL PATHWAY CONDITIONS

- Degradation (L)
- Detection (D)
- Escalation (C)
- Verification (C)

SEVERITY CONDITIONS

- Emergency readiness (E)
- Responder coordination (E)
- Recovery preparedness (E)

Emergency readiness may not predict whether degradation exists — but it can influence how severe the outcome becomes.

What Stands Out

Highest-exposure sites generally show one of two patterns:

1 DEGRADATION-DRIVEN

- → LDs and unexplained availability loss
- → Capacity loss
- → Unresolved performance stress

2 RESPONSE-DRIVEN

- → Emergency-plan gaps
- → Unclear responder interface
- → Weak recovery readiness

Reliability Governance Is Evolving

GO 167 & Emerging Reliability Expectations

GO 167 reflects a broader industry shift: reliability expectations are becoming more formalized, more operationally auditable, and more evidence-driven.

Portfolio inconsistencies across assets:

- ✕ Documentation standards vary
- ✕ LTSA governance maturity differs
- ✕ Maintenance evidence quality inconsistent
- ✕ Escalation ownership unclear
- ✕ Emergency readiness not standardized

ROLE OF AUDIT

Normalize reliability expectations across inconsistent portfolios by evaluating:

- ✓ Maintenance verification
- ✓ Corrective-action closure
- ✓ Operational escalation
- ✓ Emergency readiness

The question is no longer only whether the asset can perform — but whether the organization can demonstrate consistent operational control.

Practical Recommendations

Asset managers should:

1. Track precursor conditions separately from reportable outages
2. Require evidence-based closure — not status-only closure
3. Reconcile CMMS status, vendor reports, punch lists, and restrictions
4. Formally review performance reports and LD calculations
5. Maintain controlled ERP/EAP documentation
6. Test restart authority and recovery readiness
7. Define document preservation and response ownership before severe events

What This Changes

TRADITIONAL VIEW

Safety Audit
=
Compliance Activity

Periodic, checkbox-driven, backward-looking.

REFRAMED VIEW

Semi-Annual Operational Risk Audit
=
Reliability Intelligence

Proactive, evidence-driven, interrupts the degradation-to-outage pathway.

The audit function should not only document risk, it should interrupt the pathway from degradation to outage, fire exposure, and system exit.

Safety is the overlooked metric in emerging BESS reliability.

- Availability metrics may lag
- Safety signals may appear first
- New duty profiles create new stressors
- Inconsistent portfolio governance creates blind spots

Emerging BESS duty profiles are increasing operational complexity faster than traditional reliability governance models are adapting. Operational Risk Audits are a way to obtain confidence for those requirements.