

Scaling Safety at the Heavy Frontier

Why Battery Safety Breaks at Scale – and What to Do About It





EXECUTIVE SUMMARY

Lithium-ion battery systems have historically been designed and validated for use in relatively controlled environments, including consumer electronics, automotive applications, and static energy storage. As these systems scale into multi-megawatt-hour applications and are deployed into sectors such as heavy industry and mining, the assumptions underpinning those approaches are increasingly misaligned with operational reality.

In these environments, systems are exposed to harsh conditions, limited access, and constrained response capability. This leads to a shift in how risk manifests. Environmental degradation becomes a dominant driver of failure, fire may not be operationally manageable at scale, and maintenance constraints allow faults to persist in service for longer than design assumptions account for.

These challenges are not independent. They interact at a system level, amplifying risk in ways that are not always captured by existing design and validation approaches.

As a result, safety cannot be considered solely a function of design. It must be actively managed across the full lifecycle, with approaches that reflect the environments in which systems actually operate.

This paper outlines a shift towards active lifecycle safety management, including:

- ❖ System-level design thinking that accounts for real-world environments and operational interfaces
- ❖ Condition awareness that extends beyond cell behaviour to capture system-level and environmental inputs
- ❖ Validation and testing approaches aligned with actual operating conditions, rather than inherited assumptions
- ❖ Maintenance-aware engineering that considers containment, recovery, and transport of damaged systems at scale.

INTRODUCTION



Lithium-ion battery systems are increasingly being deployed in applications that extend beyond the environments in which their design and validation approaches were originally developed.

Rather than re-examining the fundamentals of battery safety, this paper focuses on how those existing approaches interact with the realities of large-scale operational deployment. In particular, it considers how environmental conditions, system scale, and operational constraints introduce different failure drivers.

This paper does not attempt to redefine existing safety standards or prescribe specific design solutions. Instead, it aims to explore how these factors influence how risk develops, where assumptions in current approaches may not fully reflect operational reality, and what that means for safety over time.

The paper begins by outlining the origins of common design assumptions, before examining how these assumptions are challenged in real-world deployment. It then explores three interacting areas of risk: environmental degradation, fire, and maintenance. It concludes by proposing a shift towards actively managing safety across the lifecycle.



ORIGIN OF DESIGN ASSUMPTIONS

The majority of lithium-ion battery design and safety approaches have been developed within applications such as consumer electronics, automotive systems, and static energy storage. These contexts have shaped both the technical solutions used and the assumptions underpinning how safety is assessed and managed.

While these applications differ in scale and complexity, they share several common characteristics. Operating environments are generally bounded and well understood, with limited exposure to contamination or external influences. Systems are accessible for inspection and maintenance, and failures can typically be managed through established response mechanisms.

These conditions influence how systems are designed and validated. Testing is often conducted under controlled laboratory conditions, with defined inputs and expected outcomes. Safety approaches are typically built around demonstrating compliance with established standards, with the expectation that behaviour observed under test conditions is representative of behaviour in operation, despite significant differences in environmental conditions such as humidity, contamination, and exposure. These approaches are also influenced by the domains in which many engineers develop their experience, where exposure to more variable or severe operating environments may be limited.

This does not mean that these approaches are flawed. In many cases, they are entirely appropriate for the environments in which they were developed. The issue is not that current approaches are wrong, but that they are often applied beyond the contexts in which their assumptions hold. As a result, assumptions about operating conditions, system accessibility, and response capability can break down when systems are deployed in more complex or less controlled environments.

Key Point:

Battery safety approaches developed for controlled environments can fail to account for the realities of large-scale operational deployment.

WHEN ASSUMPTIONS MEET OPERATIONAL REALITY

Lithium-ion battery safety approaches are underpinned by assumptions about environment, accessibility, and response capability. As systems are deployed into more complex and less controlled environments, these assumptions are increasingly challenged in practice.

The result is not just an increase in risk, but a shift in how risk develops and is managed over time. In particular, environmental degradation, fire behaviour, and maintenance constraints introduce dynamics that are not always fully captured by approaches developed for more controlled contexts.

Environmental Degradation

Lithium-ion battery systems are typically designed for applications such as automotive and other controlled environments, where operating conditions are bounded and reasonably well characterised. Environmental conditions such as temperature, humidity, and exposure to contaminants are generally treated as defined inputs, within which system behaviour can be predicted and managed.

In large-scale industrial deployments, these conditions are often more variable and less controlled. Systems may be exposed to conductive dust, saline moisture, vibration, and aggressive washdown processes, often in combination and over extended periods. These exposures are not always intermittent, but can form part of normal operation, introducing environmental stressors that differ from those assumed during design and validation. These environments are also less well characterised, with far less operational data available compared to domains such as automotive, where large volumes of field data inform design assumptions.

These conditions can introduce different degradation mechanisms, or accelerate those already understood. Contamination and moisture can contribute to insulation breakdown and tracking, while repeated mechanical and thermal loading can affect structural integrity over time. The interaction between these factors can be difficult to characterise, particularly where they are not explicitly exercised during validation.

As a result, degradation behaviour observed in operation may not align with expectations derived from testing approaches including transport-focused testing such as UN38.3, which do not fully reflect the conditions experienced in large-scale operational deployment. This can affect both the rate at which systems degrade and the way in which faults develop, reducing the predictability of system behaviour over time. In this context, environmental degradation becomes a primary driver of risk, rather than a secondary consideration.



High-pressure washdown and contamination exposure in heavy industrial environments

Fire

Lithium-ion battery fire behaviour is often considered within the context of applications such as automotive systems, where operating environments are relatively controlled and response capability is well established. Fire is typically treated as a rare but bounded event, with mitigation strategies focused on detection, containment, and controlled escalation. These approaches assume that systems are accessible, that surrounding conditions remain stable, and that external response can be applied in a timely and effective manner.

In large-scale operational deployments, these assumptions become less reliable. The energy contained within multi-megawatt-hour battery systems introduces a different scale of consequence, while operating environments may be remote, variable, and less predictable. Detection may be delayed, escalation pathways may not follow expected patterns, and interactions with the surrounding environment can influence how a fire develops and spreads. Conditions that are treated as boundary cases in controlled applications can become part of normal operation.



Fire response at scale is constrained by access, suppression capability, and operating conditions

The ability to respond to fire is not only constrained, but in some cases fundamentally misaligned with the scale and operational reality of these systems. While a range of battery fire suppression approaches exist, there is limited evidence of their effectiveness at the scale of multi-megawatt-hour systems in real-world deployment, and some may introduce additional risks if they do not fully extinguish the event or alter its progression. In many operational environments, access to sufficient volumes of water or appropriate suppression agents cannot be assumed, and the logistics of delivering sustained intervention may be impractical. Physical access to the system may also be restricted, particularly where systems are integrated into large equipment or remote infrastructure.

In addition, the act of suppression can introduce further consequences. Combustion products from lithium-ion battery fires may be toxic, and the use of water or other agents can result in contaminated runoff, creating potential risks to soil and groundwater. In these contexts, response is not simply a question of extinguishment, but of managing competing safety, environmental, and operational considerations under constrained conditions.

As a result, fire behaviour in these systems cannot be considered solely as a design case to be mitigated. It becomes an operational risk that affects not only safety, but also system availability, environmental impact, and recovery strategy. In many deployments, battery systems are tightly coupled to operational capability, for example through charging infrastructure or critical equipment, meaning that a fire event can disrupt or halt operations, with consequential impacts on production, logistics, and asset availability. The impact is therefore not limited to the asset itself, but can propagate across the wider system, introducing secondary risks and constraints.



As a result, approaches that assume containment and intervention may not reflect how these events develop in practice. This requires a shift towards managing fire risk across the full lifecycle, rather than being addressed at a single point in design.

These challenges do not end with the event itself. They extend into how systems are inspected, repaired, and returned to service.

Maintenance

Lithium-ion battery systems are typically designed on the basis that faults can be identified and addressed through planned inspection and maintenance activities. These approaches assume that systems are accessible, that appropriate diagnostic information is available, and that intervention can be carried out in a timely and controlled manner. Maintenance is therefore treated as a mechanism for restoring systems to a known state, with the expectation that degradation and emerging faults can be managed before they materially affect safety or performance.

In large-scale industrial deployments, these assumptions are often challenged. Systems may be integrated into heavy equipment or remote infrastructure where access is limited, inspection intervals are extended, and specialist skills or tooling are not always available. Maintenance personnel may be highly experienced in mechanical systems but have limited exposure to high-voltage battery systems, creating a gap between system design assumptions and operational capability. Operational conditions can further constrain effective intervention, with contamination, confined access, and harsh working environments making inspection and repair more difficult to perform safely and consistently.

Operational pressures can compound these challenges, with downtime carrying significant cost or production impact. As a result, systems may continue to operate with known faults, allowing faults or degraded conditions to persist in service for longer than design assumptions typically allow, increasing the likelihood of escalation or secondary failure. In many cases, deployments are located significant distances from dedicated repair facilities, sometimes requiring transport over thousands of miles, making timely intervention impractical. Diagnostic information may also be less reliable or harder to interpret in context, particularly where environmental effects introduce behaviours not captured during validation.

Rather than faults being detected and removed, they may persist and evolve within the system, interacting with environmental stressors and operational loading. Degradation becomes cumulative rather than reset through intervention, and conditions that would be treated as precursors to failure in controlled contexts can become part of normal operation.

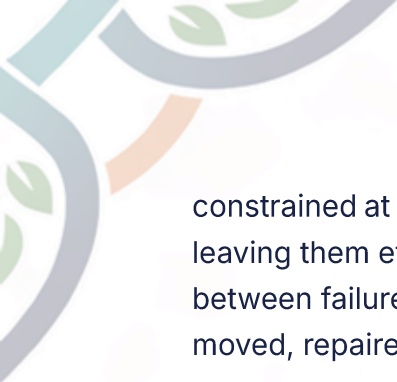
This reduces predictability of system behaviour and increases the potential for failure mechanisms to develop in ways that are not fully anticipated during design and validation. These constraints make timely intervention impractical and allow faults or degraded conditions to persist in service, changing how risk develops over time.

Maintenance cannot be considered solely a support function, but as a key factor in how safety is realised in practice. The ability to inspect, repair, isolate, or recover systems becomes integral to the overall safety approach, particularly at the scale of multi-megawatt-hour deployments. In many cases, this extends beyond routine maintenance to include the handling, containment, and transportation of damaged systems under constrained conditions.



Even in workshop environments, maintenance of large-scale systems is constrained by access, infrastructure, and the realities of scale

However, the movement of damaged lithium-ion battery systems presents a fundamental challenge. Systems that have experienced faults or damage may no longer be suitable for transport under standard requirements, while leaving them in place may not be viable or safe. At the same time, clear and consistent approaches for transporting large, damaged battery systems remain poorly defined and operationally



constrained at this scale. In some cases, systems cannot be safely transported, leaving them effectively stranded in a degraded or uncertain state. This creates a gap between failure occurrence and recovery capability, where systems cannot be easily moved, repaired, or safely returned to a controlled environment.

In this context, systems may remain in degraded or uncertain states for extended periods, with limited options for intervention or removal. This demands consideration of maintenance capability, logistics, and operational context as part of a lifecycle approach to safety, rather than assuming that risks can be fully addressed at the point of design.

Maintenance is not a downstream activity. It is a defining constraint on how safety is achieved in practice.

Key Points:

- ❖ Safety approaches derived from controlled and well characterised environments do not account for the realities of large-scale operational deployment.
- ❖ Environmental degradation, fire behaviour, and maintenance constraints are not independent challenges. They interact to shape how risk develops over time.
- ❖ Conditions treated as boundary cases in design, such as contamination, limited access, or delayed response, can become part of normal operation.
- ❖ Assumptions about detection, intervention, and recovery often break down in practice, particularly where systems are remote, access is constrained, or infrastructure is limited.
- ❖ Maintenance constraints play a defining role in how safety is achieved in practice, particularly where access, logistics, and recovery pathways are limited.
- ❖ As a result, risk cannot be fully understood or managed at the point of design alone, but must be considered across the full operational lifecycle.

CONCLUSION

Lithium-ion battery safety has been shaped by the environments in which these systems were first developed and deployed. As systems scale into large industrial applications, the assumptions that underpin those approaches are increasingly misaligned with operational reality. Environmental conditions are more variable and less well characterised, access is constrained, and response capability cannot be assumed. As a result, risk does not behave in the way design and validation processes assume.

In this context, safety cannot be treated solely as a design outcome. It must be understood as a function of how systems operate over time, shaped by degradation, intervention constraints, and the environments in which they are deployed. Approaches that focus on demonstrating compliance at a single point in the lifecycle risk overlooking how conditions evolve in service, and how those changes influence failure behaviour and consequence.

Addressing this requires a shift in how safety is considered. Design, validation, and operational planning must be more tightly integrated, with explicit consideration of environmental exposure, fire response capability, and maintenance constraints from the outset. Testing strategies should reflect real operating conditions, and system level monitoring and condition awareness should be used to inform decision making throughout the lifecycle. Equally, maintenance capability, logistics, and recovery pathways must be treated as fundamental components of the safety case, rather than downstream considerations.

What Needs to Change

Addressing these challenges requires a shift not only in how risk is understood, but in how systems are designed, validated, and supported in practice.

❖ **Validation aligned to operational environments**

Testing and validation approaches must reflect the environments in which systems actually operate, rather than relying solely on automotive or transport focused standards. This includes drawing on practices from other domains, such as defence and heavy equipment, where exposure to harsh and variable conditions is explicitly considered.

❖ **Expanded condition awareness and monitoring**

Monitoring strategies should extend beyond internal battery parameters such as state of charge, temperature, and current, to include environmental and operational conditions. These inputs are critical to understanding degradation behaviour and should inform damage models and predictions of system health over time.

❖ **Fire response capability at scale**

Greater consideration must be given to how fire is managed in large scale and industrial applications. This includes the availability and effectiveness of suppression approaches, as well as the constraints imposed by access, infrastructure, and environmental impact. Where appropriate, greater emphasis should be placed on cell and system architectures that reduce susceptibility to thermal runaway and limit propagation.

❖ **Maintenance and recovery as design inputs**

Maintenance capability, logistics, and recovery pathways must be considered from the outset. This includes how systems are inspected, repaired, isolated, and, where necessary, transported following damage. At present, there is limited clarity and consistency in guidance for the handling and transportation of damaged lithium-ion batteries at scale, particularly where systems may no longer meet standard transport requirements, which can leave them effectively stranded in degraded or unsafe states within operational environments. Clear, practical frameworks are needed to enable safe recovery and movement of damaged systems without leaving them stranded in operational environments.

❖ **Cross domain engineering awareness**

Engineers working across domains must be equipped to recognise differences in environmental exposure, operational constraints, and failure behaviour. Without this awareness, assumptions derived from one domain can be inadvertently applied to another, introducing risk at the point of design.

This is not a question of improving individual techniques, but of aligning safety approaches with the realities of large-scale deployment. As lithium-ion systems continue to scale, the ability to manage risk will depend on recognising that safety is not achieved at the point of design, but through how systems are operated, monitored, maintained, and supported in practice.