

Certificado Não é Evidência:

Classes de evidência e avaliação de argumento de segurança na aquisição de sistemas de armazenamento

Eduardo Mayer Fagundes, M.Sc.

Engenheiro Eletricista | Energia e Sistemas Inteligentes

nMentors Engenharia

São Paulo, Brasil

eduardo.mayer@nMentors.com.br

Resumo — Em 13 de agosto de 2026, o recurso da Clearstone Energy para um sistema de armazenamento de 150 MW em Axminster, Inglaterra, foi indeferido porque a inspetora não se convenceu de que as estratégias de mitigação de deflagração funcionariam com gabinetes separados por 10 cm. Distância de separação está entre os parâmetros que o ensaio em escala de instalação do UL 9540A permite avaliar. A recusa não decorreu de descumprimento normativo: decorreu de a evidência disponível não cobrir a configuração implantada. Artigo anterior deste autor sustentou que a capacidade de sustentar um argumento de segurança é propriedade da arquitetura de controle e traduziu esse argumento em itens de especificação técnica. Este artigo trata da pergunta seguinte, que a habilitação técnica do LRCAP de 2026 e os leilões de 2 e 4 de dezembro colocam diante de desenvolvedores, seguradoras, financiadores e órgãos licenciadores: recebida a resposta do fornecedor, como se avalia se ela demonstra alguma coisa? A proposição central é que **não existe evidência forte em abstrato — existe evidência adequada ou inadequada a uma determinada asserção, configuração e regime operacional**. Dela decorrem três teses. Epistemicamente, cada asserção admite apenas certas classes de evidência, e a maior parte das disputas de aquisição nasce de aceitar classe inferior à exigida. Estruturalmente, a ausência de um ensaio de nível superior não é por si sinal favorável nem desfavorável: seu significado depende de por que o ensaio parou onde parou. Temporalmente, evidência possui escopo de validade delimitado pela edição do método, pela identidade da configuração ensaiada e pelo regime operacional pressuposto. O artigo propõe sete classes de evidência ordenadas por informação recuperável e diferenciadas, no topo, por dois eixos independentes; um critério explícito de suficiência probatória; uma regra de correspondência entre asserção e classe mínima requerida; uma classe de asserção sobre arbitragem de autoridade entre controladores; e uma taxonomia de cinco modos de não-resposta. Aplica os instrumentos à leitura de um dossiê construído e declara explicitamente o que não demonstra.

Palavras-chave — sistemas de armazenamento de energia em baterias; argumento de segurança; classes de evidência; UL 9540A; NFPA 855; arbitragem de autoridade; especificação técnica; devida diligência; LRCAP 2026.

Abstract — On 13 August 2026, Clearstone Energy's appeal for a 150 MW storage system in Axminster, England, was dismissed because the inspector was not persuaded that deflagration mitigation strategies would work effectively for cabinets spaced 10 cm apart. Separation distance is among the parameters that UL 9540A installation-scale testing allows to be assessed. The refusal did not follow from any breach of standards: it followed from available evidence failing to cover the deployed configuration. A previous paper by this author argued that the capacity to sustain a safety argument is a property of the control architecture, and translated that argument into technical specification items. This paper addresses the next question, which Brazil's LRCAP 2026 technical qualification and the December auctions place before developers, insurers, lenders and licensing authorities: once the vendor has answered, how does one assess whether the answer demonstrates anything? The central proposition is that **there is no strong evidence in the abstract — there is evidence adequate or inadequate to a given claim, configuration and operating regime**. Three theses follow. Epistemically, each claim admits only certain classes of evidence, and most procurement disputes arise from accepting a class below what the claim requires. Structurally, the absence of a higher-level test is in itself neither favourable nor unfavourable: its meaning depends on why testing stopped where it did. Temporally, evidence has a scope of validity bounded by the edition of the method, the identity of the tested configuration, and the presumed operating regime. The paper proposes seven evidence classes ordered by recoverable information and differentiated, at the upper end, along two independent axes; an explicit sufficiency criterion; a correspondence rule between claim and minimum required class; a claim class concerning authority arbitration among controllers; and a taxonomy of five modes of non-response. It applies these instruments to a constructed dossier and states explicitly what it does not demonstrate.

Index Terms — battery energy storage systems, safety case, evidence classes, UL 9540A, NFPA 855, authority arbitration, technical specification, technical due diligence.

I. INTRODUÇÃO

A Empresa de Pesquisa Energética encerrou o cadastramento dos Leilões de Reserva de Capacidade por meio de sistemas de armazenamento em baterias com 6.091 projetos, somando 296,8 GW, para certames marcados para 2 e 4 de dezembro de 2026 que contratarão uma fração desse volume (EPE, 2026). Entre o cadastramento e o leilão está a habilitação técnica conduzida pela EPE. Entre a habilitação e a operação estão o licenciamento ambiental, a contratação de fornecimento, a subscrição de seguro e a estruturação de financiamento. Em cada uma dessas passagens, alguém precisa ler um conjunto de documentos e decidir se ele demonstra o que afirma.

Artigo anterior deste autor sustentou que conformidade normativa cumprida e argumento de segurança demonstrável são coisas distintas, que apenas a segunda sustenta licença, financiamento e apólice, e que a capacidade de sustentá-la é propriedade da arquitetura de controle e não do equipamento (FAGUNDES, 2026). Aquele texto encerrou com itens de especificação e com uma observação que ficou sem desenvolvimento: um certificado transfere ao comprador a conclusão de um ensaio, não a competência para avaliar seu escopo.

Este artigo desenvolve essa observação. A pergunta não é mais o que exigir. É o que fazer com o que se recebe.

O caso que motivou o artigo anterior admite releitura sob esse ângulo, e a releitura é instrutiva. A Clearstone Energy apresentou o projeto Axminster Energy Hub à East Devon District Council no início de 2024, sob a aplicação 24/0096/MFUL, tendo obtido conexão na subestação de Axminster, da National Grid. A autarquia indeferiu em maio de 2025. No curso do recurso, a própria autarquia retirou sua oposição, em reunião de 14 de janeiro de 2026, restando a oposição a cargo de grupos locais admitidos como Rule 6 Party. Em 13 de agosto de 2026, a inspetora de planejamento Helen Heward indeferiu o recurso em decisão de dezessete páginas, apesar de o desenvolvedor empregar tecnologia de fabricante de primeira linha e ter seguido a orientação aplicável de segurança contra incêndio.

O fundamento é o que interessa. A inspetora registrou não estar persuadida de que houvesse evidência robusta suficiente para demonstrar que as estratégias de mitigação de deflagração e explosão funcionariam eficazmente, e que os riscos de explosão seriam satisfatoriamente controlados para gabinetes separados por 10 cm. Como a evidência de

controle de poluição estava predicada na evidência de segurança contra incêndio, a insuficiência da primeira arrastou a segunda.

Distância de separação entre unidades está entre os parâmetros que o ensaio em escala de instalação do UL 9540A permite avaliar. A Seção V mostra por que a evidência tipicamente disponível não cobre esse parâmetro, e por que a lacuna é estrutural ao método, e não falha de um fornecedor específico.

Há ainda um precedente próximo que expõe a questão em sua forma mais pura. No recurso relativo ao empreendimento de Pound Road, em Hawkchurch, o corpo de bombeiros não apresentou objeção, e a inspetoria indeferiu assim mesmo, consignando que não havia sido demonstrado que a proposta não representaria risco significativo para residentes e para o meio ambiente. A autoridade tecnicamente competente não se opôs; a autoridade probatória não se convenceu. **Ausência de objeção não é presença de evidência.**

A proposição central deste artigo é que não existe evidência forte em abstrato. Existe evidência adequada ou inadequada a uma determinada asserção, sob uma determinada configuração e um determinado regime operacional. Disso decorrem as três teses enunciadas no resumo — epistêmica, estrutural e temporal — e a estrutura do texto.

A Seção II situa o trabalho na literatura de argumentação de segurança. A Seção III caracteriza a assimetria de competência probatória. A Seção IV propõe as classes de evidência e o critério de suficiência. A Seção V desenvolve o caso do UL 9540A. A Seção VI estabelece a regra de correspondência. A Seção VII acrescenta uma classe de asserção ausente do artigo anterior: a arbitragem de autoridade entre controladores. A Seção VIII apresenta a taxonomia da não-resposta. A Seção IX trata do escopo de validade. A Seção X aplica os instrumentos a um dossiê construído. A Seção XI discute o uso institucional. A Seção XII declara o que esta análise não demonstra.

II. TRABALHOS RELACIONADOS

A noção de que segurança se demonstra por argumento estruturado, e não por lista de conformidade, não é nova. Ela consolidou-se no Reino Unido após o desastre de Piper Alpha e o relatório Cullen, migrando para a regulação nuclear, ferroviária e de defesa — notadamente pela Def Stan 00-56, que substituiu prescrição por exigência de argumento de segurança. Kelly e McDermid formalizaram

a representação desse argumento na Goal Structuring Notation (GSN) (KELLY; MCDERMID, 1997), posteriormente mantida como padrão comunitário pelo Assurance Case Working Group, e a tradição paralela de Claim–Argument–Evidence estabeleceu vocabulário equivalente. A ISO/IEC 15026 normalizou a estrutura de *assurance case* para sistemas e software, e a ISO 26262 incorporou o argumento de segurança ao ciclo de vida automotivo.

Esse arcabouço já foi estendido a sistemas com componentes de aprendizado. A metodologia AMLAS organiza a produção de evidência de garantia para aprendizado de máquina em sistemas autônomos (HAWKINS et al., 2021); a UL 4600 adota explicitamente abordagem baseada em argumento de segurança, em vez de requisitos prescritivos, para veículos autônomos; e a ISO/IEC TR 5469 trata das propriedades, fatores de risco e métodos do uso de inteligência artificial em funções relacionadas à segurança, do uso de funções não baseadas em IA para assegurar equipamentos controlados por IA, e do uso de IA no desenvolvimento de funções de segurança (ISO/IEC, 2024). No domínio do armazenamento, a aplicação de análise de processo baseada em teoria de sistemas (STPA) proposta por Sandia trata falhas de sistema de gerenciamento de baterias, gases inflamáveis, arco elétrico, incêndio e explosão como problema de controle inadequado, e não de falha de componente isolado (SANDIA, 2016).

Há ainda literatura específica sobre a **suficiência** do argumento, e não apenas sobre sua forma. Bloomfield e Rushby discutem confiança em *assurance cases* (BLOOMFIELD; RUSHBY, 2020); Goodenough, Weinstock e Klein propõem argumentação eliminativa, na qual a força do argumento decorre da eliminação sistemática de *defeaters* — razões pelas quais a conclusão poderia não se sustentar (GOODENOUGH; WEINSTOCK; KLEIN, 2013). Essa linha é o antecedente mais próximo da taxonomia proposta na Seção VIII deste artigo: os modos de substituição ali descritos podem ser lidos como *defeaters* não eliminados, e o reconhecimento dessa filiação é devido.

Este trabalho difere do conjunto acima em quatro aspectos, que delimitam sua contribuição.

Perspectiva. GSN, CAE, AMLAS e UL 4600 são instrumentos do produtor: quem projeta o sistema constrói o argumento e o submete. O problema tratado aqui é o do **avaliador** — licenciador, segurador, financiador ou comprador — que precisa julgar um argumento que não

construiu, sobre um sistema que não projetou, com competência assimétrica e sob incentivo comercial adverso da contraparte.

Acesso. Metodologias de *assurance case* pressupõem acesso aos artefatos de desenvolvimento. Em aquisição, o avaliador dispõe apenas do que o fornecedor divulga, tipicamente em formato que descarta as premissas — daí a centralidade, neste artigo, da distinção entre certificado e relatório.

Granularidade da evidência. Nas notações existentes, a evidência é nó terminal do argumento, tratada como dada. Este artigo propõe classificá-la por informação recuperável e por dois eixos de aplicabilidade — fidelidade de configuração e realismo da condição —, e mostra, no caso do UL 9540A, que um mesmo documento pode ser evidência favorável quanto a um nível e ausência de evidência quanto a outro.

Janela temporal. A literatura de *assurance case* trata do ciclo de vida do sistema. A aquisição tem prazo: a alavanca contratual que torna a evidência exigível extingue-se na assinatura, o que converte a classificação de evidência em decisão de especificação, e não de auditoria.

III. A ASSIMETRIA DE COMPETÊNCIA PROBATÓRIA

O mercado de aquisição de sistemas de armazenamento opera sob assimetrias de várias naturezas: de informação, de acesso à evidência e de incentivos. Este artigo trata de outra, que subsiste às demais: **mesmo quando a informação existe e é disponibilizada, permanece uma assimetria de competência probatória**. O documento entregue exige, para ser avaliado, conhecimento que o comprador tipicamente não possui e que o próprio documento não transfere.

Um certificado é o exemplo canônico. Ele comunica que um objeto foi submetido a um procedimento e obteve resultado conforme. Identifica, em geral, o modelo ou família, a edição da norma e o laboratório. Não comunica com granularidade suficiente sob que condições o ensaio ocorreu, contra que critérios, com que configuração detalhada, nem o que permaneceu fora do escopo. Essas informações existem — estão no relatório de ensaio, que não circula com a proposta comercial. O certificado é a conclusão destacada de suas premissas.

A resposta reflexa do comprador é exigir mais certificados. Isso agrava o problema em vez de resolvê-lo, por duas razões. Primeiro, porque multiplica conclusões sem

recuperar premissas, aumentando o volume documental sem aumentar a capacidade de julgamento. Segundo, porque desloca o critério de decisão para uma métrica — quantidade de certificações — ortogonal à pergunta relevante e que fornecedores otimizam com facilidade.

A distinção entre norma de produto e método de ensaio ilustra bem a confusão. O UL 9540 é a norma de segurança de produto para sistemas de armazenamento e seus equipamentos. O UL 9540A não é norma de certificação: é método padronizado de ensaio que gera dados sobre comportamento de propagação térmica sob condições extremas (UL SOLUTIONS, 2026a). Dizer que um sistema "tem UL 9540A" é categoricamente equivalente a dizer que uma amostra "tem cromatografia". O método foi aplicado; o resultado é outra coisa, e é o resultado que responde à pergunta.

Essa assimetria não se resolve com mais documentos. Resolve-se com um critério de leitura — o que exige, minimamente, uma tipologia de classes de evidência e uma regra que associe cada asserção à classe mínima capaz de sustentá-la.

IV. CLASSES DE EVIDÊNCIA E CRITÉRIO DE SUFICIÊNCIA

Tabela I — Classes de evidência.

Classe	Descrição	O que autoriza a concluir
E0	Declaração do fornecedor: folheto, resposta a questionário, apresentação comercial	Que o fornecedor afirma. Nada sobre o sistema.
E1a	Certificação organizacional ou de sistema de gestão	Que a organização mantém processos documentados. Nada sobre o produto ofertado.
E1b	Certificação de produto ou de subsistema	Que um objeto foi avaliado contra requisitos de produto e obteve resultado conforme. Escopo apenas parcialmente recuperável: condições, configuração detalhada e resultados permanecem no relatório.
E2	Relatório de ensaio sem declaração de nível, edição e configuração	Que houve medição. Transferibilidade ao objeto entregue indeterminada.
E3	Relatório de ensaio com nível, edição, configuração e critérios declarados	Que o objeto identificado, sob as condições identificadas, apresentou o comportamento medido.

Classe	Descrição	O que autoriza a concluir
E4	Ensaio em laço fechado com o componente real sob condição de projeto: C-HIL; pior caso de tempo de execução sob estrangulamento térmico	Que o componente que será entregue, com seu firmware e seu envelope térmico, comporta-se conforme medido sob a condição especificada.
E5	Registro operacional instrumentado ou investigação forense de ocorrência em ativo comparável	Que o comportamento ocorreu em operação real, sob condições não antecipadas pelo projetista.

A. A escala é ordinal apenas até E3

De E0 a E3 a progressão é estritamente ordinal, porque cada classe recupera informação que a anterior descartou sobre o mesmo objeto: da afirmação à avaliação, da avaliação ao dado, do dado ao dado com escopo. Nenhuma asserção é mais bem sustentada por E1b do que por E3 do mesmo objeto.

Acima de E3 a ordenação deixa de valer, e é preciso enunciar isso com clareza para não induzir a leitura de que classe superior é sempre melhor. E4 e E5 diferenciam-se por dois eixos independentes:

- **Fidelidade de configuração** — proximidade entre o objeto observado e o objeto que será entregue: química, configuração de módulo, PCS, BMS, versão de firmware, invólucro, sistema de supressão.
- **Realismo da condição** — proximidade entre a condição de observação e a condição de operação adversa não antecipada.

E4 é forte no primeiro eixo e fraca no segundo: mede o componente que será entregue, sob condições que alguém precisou imaginar. E5 é o inverso: registra o que efetivamente ocorreu, mas em outro ativo, com outra química, outro firmware, outro clima e outra época.

Um relatório forense de um sistema NMC de 2019 em clima temperado é insumo valioso para identificar modos de falha, e não é evidência superior a um ensaio C-HIL específico do sistema LFP que será entregue em 2028. **As classes não estabelecem dominância absoluta entre si; a força probatória final depende da correspondência entre a evidência e a asserção.** Um dossiê que apresenta apenas E4 e outro que apresenta apenas E5 têm lacunas diferentes, não graus diferentes da mesma lacuna.

B. Critério de suficiência probatória

A classe é condição necessária e não suficiente. Enuncia-se o critério na forma predicativa:

Uma evidência *e* sustenta uma asserção *a* se, e somente se: (i) a classe de *e* atende à classe mínima requerida por *a*; e (ii) a configuração ensaiada em *e* corresponde à configuração ofertada; e (iii) o regime operacional pressuposto em *e* cobre o regime contratado.

Duas consequências merecem enunciado explícito, porque são frequentemente violadas na prática: **classe igual ou superior à mínima não implica suficiência**. Uma evidência E4 obtida sobre outra versão de firmware não satisfaz a asserção, ainda que sua classe seja alta. Um relatório E3 relativo a outro arranjo de módulos tampouco a satisfaz. A condição (i) é a mais fácil de verificar e a menos decisiva; as condições (ii) e (iii) são onde as asserções efetivamente se rompem, e são tratadas na Seção IX.

C. Três propriedades adicionais

Disponibilidade não acompanha força. E5 depende, por construção, de que algo tenha acontecido. Como argumentado no artigo anterior, o Brasil não possui casuística forense própria em armazenamento em rede, o que torna E5 acessível apenas por importação de relatórios estrangeiros — precisamente a classe cuja fidelidade de configuração é mais baixa (FAGUNDES, 2026).

A força de um conjunto é limitada pelo elo mais fraco da cadeia de sustentação. Em Axminster, a evidência de controle de poluição estava predicada na de segurança contra incêndio; a insuficiência da segunda invalidou a primeira independentemente da qualidade desta. Cadeias probatórias herdam a força de seu antecedente.

O salto de E1b para E3 normalmente não exige novo ensaio. O relatório existe; o certificado deriva dele. Pode exigir acordo de confidencialidade ou controle de acesso, e em alguns casos esbarra em restrições do laboratório ou em proteção de propriedade intelectual — mas recupera evidência já produzida, sem impor nova campanha experimental. É a intervenção de melhor relação entre custo e ganho probatório em todo o processo de aquisição.

V. ANATOMIA DE UM MÉTODO DE ENSAIO: O UL 9540A E A LÓGICA DE PARADA

O UL 9540A é o único método de ensaio consensual explicitamente citado pela NFPA 855 para ensaio de incêndio em larga escala, e o método especificado tanto pela edição de 2026 da NFPA 855 quanto pela edição de 2024 do International Fire Code (UL SOLUTIONS, 2026a; NFPA, 2026). Ele progride em quatro níveis, cada um alimentando o seguinte com parâmetros medidos.

Tabela II — Níveis do UL 9540A e o que cada um demonstra.

Nível	Objeto	O que a passagem demonstra	O que permanece fora
Célula	Célula individual forçada a disparada térmica em vaso pressurizado	Características de disparada; composição e inflamabilidade dos gases; limite inferior de inflamabilidade, pressão máxima e velocidade de queima	Interação entre células
Módulo	Módulo em configuração de produção	Tendência de propagação entre células; taxa de liberação de calor e gás; potencial de ignição ou deflagração	Propagação entre módulos e comportamento da unidade
Unidade	Sistema completo, com supressão desabilitada	Propagação entre módulos; taxas de liberação da unidade; potencial de deflagração e reignição	Propagação entre unidades; afastamentos; eficácia da supressão instalada
Instalação	Configuração implantada, com supressão ativa	Que a disparada em uma unidade não se propaga às adjacentes na disposição ensaiada; evidência para avaliar afastamentos e proteção ativa	Condições fora do cenário ensaiado

A propriedade que interessa é a **lógica de parada**: o ensaio começa no menor nível possível e não prossegue quando os critérios de desempenho são atendidos (TELGIAN ENGINEERING & CONSULTING, 2025). Se o ensaio de módulo passa, os de unidade e instalação não são requeridos.

Disso decorre a inversão que este artigo deseja tornar explícita. **Um dossiê contendo apenas ensaios de célula e módulo relata um bom resultado — o sistema parou ali porque passou. E, exatamente por isso, nada informa sobre propagação entre unidades, sobre afastamentos ou sobre a eficácia da supressão na disposição implantada.** O mesmo documento é, simultaneamente, evidência favorável quanto ao comportamento do módulo e ausência de evidência quanto à instalação.

A leitura ingênua é a de que mais níveis ensaiados significam sistema mais seguro. A leitura correta é a de que mais níveis ensaiados significam que os níveis anteriores exibiram comportamento que exigiu prosseguir — e que, ao mesmo tempo, existe informação sobre a escala em que o ativo será efetivamente instalado.

Essa lacuna não é interpretação deste autor. Ela foi reconhecida normativamente e corrigida. A justificativa técnica publicada para as revisões de 2026 é explícita: como o método pode encerrar cedo quando um nível é aprovado, alguns sistemas de grande porte nunca chegaram a ser ensaiados como um todo (TELGIAN ENGINEERING & CONSULTING, 2025). A edição de 2026 da NFPA 855 passou a exigir o ensaio de incêndio em larga escala em conjunto com o UL 9540A, introduzindo o Anexo G.11, que orienta sobre iniciação de condição de incêndio desenvolvido, avaliação de distâncias de separação e papel dos sistemas ativos de proteção (NFPA, 2026). A 6ª edição do UL 9540A, publicada em 13 de março de 2026, revisou a Seção 10 para incorporar método de ensaio em larga escala alinhado ao Anexo G.11, deixou de exigir o ensaio de nível de unidade para sistemas não residenciais — que passam do nível de módulo diretamente ao de instalação — e acrescentou o Anexo C, para ensaio de deflagração em larga escala de invólucros (UL SOLUTIONS, 2026a).

Três consequências para quem lê evidência no Brasil.

A primeira é temporal. Relatórios emitidos sob edições anteriores foram produzidos sob um método que permitia precisamente a lacuna que a edição de 2026 fechou. Um dossiê de 2024 pode ser tecnicamente impecável e ainda assim silente sobre a escala de instalação, e a data do relatório é o indicador dessa condição.

A segunda é de escopo geográfico. A exigência de ensaio em larga escala decorre de código norte-americano. O arcabouço brasileiro não possui equivalente. A lacuna que a NFPA 855 fechou permanece aberta aqui, e o comprador brasileiro que não a especificar contratualmente não a terá.

A terceira devolve o argumento a Axminster. A recusa incidiu sobre mitigação de deflagração em gabinetes separados por 10 cm — parâmetro de disposição, portanto de escala de instalação. O desenvolvedor tinha conformidade e tinha equipamento de fabricante reconhecido. O que não tinha era evidência no nível em que a pergunta foi feita. Não há indicação de má-fé nem de deficiência de produto; há incompatibilidade entre a classe de evidência disponível e a asserção que precisava ser sustentada.

Registre-se, por fim, que a NFPA 855 de 2026 passou a tratar em seção própria os sistemas ativos de prevenção de propagação de disparada térmica, definidos como sistemas automáticos que detectam precursores — desprendimento de gases ou temperatura anômala — e acionam meio dirigido de supressão ou resfriamento, sendo as medidas passivas complementares e insuficientes, isoladamente, para constituí-los (TELGIAN ENGINEERING & CONSULTING, 2025). É a camada de percepção descrita no artigo anterior (FAGUNDES, 2026) aparecendo como requisito de código, o que amplia o conjunto de asserções sobre as quais o comprador precisará exigir evidência de classe E3 ou superior.

VI. REGRA DE CORRESPONDÊNCIA ENTRE ASSERÇÃO E EVIDÊNCIA

A tipologia da Seção IV só opera quando associada a uma regra que determine, para cada asserção, a classe mínima requerida. A Tabela III aplica a regra aos itens de especificação propostos no artigo anterior (FAGUNDES, 2026), com uma correção: a primeira asserção decompõe-se em duas, porque projeto e efetividade sob falha exigem classes distintas. As colunas de classe indicam o piso; a suficiência permanece condicionada aos critérios (ii) e (iii) da Seção IV-B.

Tabela III — Classe mínima requerida por asserção.

Asserção do fornecedor	Classe mínima	Observação
A segregação entre função de segurança e componente de aprendizado foi projetada	E3	Descrição arquitetural com identificação do hardware segregado e mapeamento dos princípios adotados aos riscos e métodos descritos na ISO/IEC TR 5469:2024

Asserção do fornecedor	Classe mínima	Observação
Essa segregação permanece efetiva sob falha da camada de aprendizado	E4	Descrição de projeto não demonstra independência sob falha; exige ensaio com injeção de falha na camada de inferência
A malha rápida cumpre o envelope temporal	E4	Pior caso de tempo de execução sob condição térmica de projeto
A detecção de precursores é eficaz	E3	Taxa de falsos negativos na região de operação, latência de detecção e comportamento sob falha de sensor
A propagação térmica é contida	E3; em escala de instalação quando a asserção envolver afastamento ou supressão	O nível do ensaio delimita a asserção sustentável
A função de segurança não pode ser desabilitada	E3	Declaração de inexistência de modo operacional, de serviço ou de comissionamento que a remova, e procedimento de manutenção correspondente
A arbitragem entre controladores é determinística e rastreável	E4	Propriedade emergente da integração; ver Seção VII
As decisões são rastreáveis	E4	Demonstração em ensaio de registro de restrição ativa e de ação bloqueada, com retenção definida
O sistema opera com autonomia sem conectividade	E4	Ensaio de aceitação com duração, estado e comportamento de reconexão declarados
As interfaces são abertas e os dados são do proprietário	E3	Especificação de interface por ponto de integração; declaração contratual isolada é E0

Duas leituras decorrem da tabela.

A primeira é que **cinco das dez asserções admitem sustentação em E3** — segregação projetada, detecção de precursores, contenção de propagação, impossibilidade de desabilitação e interfaces —, ou seja, com documentos que já existem e cuja obtenção não impõe nova campanha

experimental. O obstáculo, nesses casos, é de prática de aquisição e não de custo de ensaio.

A segunda é que **as cinco asserções que exigem E4 são exatamente as que dizem respeito ao comportamento sob falha ou sob integração** — efetividade da segregação, envelope temporal, arbitragem, rastreabilidade e autonomia. São também as que mais frequentemente recebem resposta de classe inferior, porque exigem ensaio com o componente real e não podem ser satisfeitas por documento de produto.

VII. A CADEIA DE AUTORIDADE ENTRE CONTROLADORES

O artigo anterior propôs arquitetura de referência em quatro camadas, com autoridade exclusiva de atuação concentrada na camada de blindagem (FAGUNDES, 2026). Aquela formulação enuncia uma regra de projeto correta e é, ao mesmo tempo, incompleta como descrição de um ativo real: em um sistema utility-scale, **a autoridade para comandar, limitar, bloquear ou interromper a operação está distribuída entre subsistemas de fornecedores distintos**, e o argumento de segurança precisa cobrir as fronteiras entre eles. Adota-se aqui essa formulação, mais ampla que a de "autoridade de escrita" empregada em Fagundes (2026), porque relés de proteção, intertravamentos e sistemas de detecção e combate a incêndio exercem autoridade por saída física, sem necessariamente escrever no mesmo domínio de controle.

A cadeia efetiva aproxima-se de: sensoriamento de célula → BMS de módulo → BMS de rack → BMS mestre → controlador do PCS → EMS e controlador de planta (PPC) → SCADA → proteção elétrica → sistemas de HVAC, incêndio e detecção de gases → telecomunicações → operador. Cada fronteira é um ponto de integração, e é nas fronteiras que se concentram os modos de falha que nenhum ensaio de componente revela.

O caso elementar é o conflito de comando. O EMS solicita potência; o controlador do PCS aceita; o BMS detecta que a taxa C solicitada excede o limite térmico admissível para o estado de saúde corrente. As perguntas que o comprador precisa fazer são:

1. Qual comando prevalece, e por que regra?
2. Em quanto tempo a arbitragem se resolve, e qual o pior caso desse tempo?

3. Que variável bloqueou o comando, e isso foi registrado de forma recuperável?
4. O comando bloqueado é reapresentado automaticamente, e com que frequência?
5. O controlador de planta pode sobrescrever o bloqueio? Sob que condição e com que registro?
6. Existe modo degradado definido, e qual o comportamento em cada degradação?
7. O que ocorre na perda e na retomada de comunicação entre dois elos da cadeia?
8. Como se evita a execução de comando obsoleto (*stale command*) após a reconexão?

Nenhuma dessas perguntas é respondida por certificação de produto, porque nenhuma é propriedade de um produto. **São propriedades emergentes da integração**, e a classe mínima que as sustenta é E4 — ensaio em laço fechado com os controladores reais, incluindo injeção de falha de comunicação e de sensor.

Essa é também a razão pela qual a resposta "o sistema opera localmente em caso de perda de comunicação" é insuficiente. As perguntas subsequentes são: por quanto tempo; com qual setpoint; a partir de qual estado; com quais funções degradadas; e o que acontece na reconexão. A ausência dessas cinco informações converte uma asserção operacional em declaração comercial.

A implicação para a especificação é direta: **a matriz de autoridade e o comportamento de arbitragem devem ser documentos contratuais, produzidos antes da definição do arranjo de fornecimento**. Depois da integração, alterá-los envolve interfaces de BMS, PCS, EMS, proteção e supervisão simultaneamente, convertendo decisão arquitetural em retrofit.

VIII. TAXONOMIA DA NÃO-RESPOSTA

Resposta que não sustenta a asserção raramente é recusa explícita. É substituição. Distinguem-se cinco modos, cada um revelando algo sobre a arquitetura ou sobre o processo de engenharia por trás da proposta. Na terminologia de argumentação eliminativa (GOODENOUGH; WEINSTOCK; KLEIN, 2013), cada modo corresponde a um *defeater* que permanece não eliminado.

Substituição de métrica. Responde-se com grandeza correlata mas insuficiente: latência média no lugar de tempo de execução no pior caso; acurácia agregada de

detecção no lugar de taxa de falsos negativos na região de operação; disponibilidade contratual no lugar de comportamento sob falha.

O caso da latência merece demonstração, porque é o mais frequente e o mais facilmente aceito. Considere uma malha com requisito determinístico de 10 ms cujo controlador apresente latência média de 4 ms, percentil 99 de 8 ms e máximo observado de 47 ms. Pela média, o sistema opera com folga de 60%. Pelo requisito, o sistema viola o prazo. As duas afirmações são simultaneamente verdadeiras, e apenas a segunda descreve o comportamento do controle. **Latência média é insuficiente, por construção, para demonstrar atendimento a requisito temporal de pior caso** — e, quando apresentada como se o demonstrasse, é declaração ocupando o lugar de medição. Como argumentado no artigo anterior, um estimador cuja inferência ocasionalmente leva várias vezes o tempo típico não é um estimador lento: é um estimador que quebra a malha de forma intermitente e difícil de diagnosticar (FAGUNDES, 2026).

Substituição de artefato. Responde-se com certificado quando se pediu relatório, com declaração de conformidade quando se pediu dado, com apresentação comercial quando se pediu procedimento. O que o modo revela: o relatório pode existir e não ter sido lido internamente, ou pode conter delimitações de escopo que o fornecedor prefere não expor.

Substituição de nível. Responde-se com evidência de nível inferior a uma pergunta de nível superior — ensaio de módulo respondendo pergunta sobre propagação entre unidades ou sobre afastamento. É o modo mais difícil de detectar, porque a resposta é tecnicamente verdadeira e formalmente pertinente. É o modo que produziu Axminster.

Substituição de configuração. Responde-se com evidência sobre variante da mesma família de produtos — outra química, outra configuração de módulo, outro invólucro, outro sistema de supressão, outra versão de firmware. Qualquer alteração de química da célula, de configuração do módulo, de material do invólucro ou do sistema de supressão posterior à data do ensaio original demanda novo ensaio, independentemente da edição vigente (UL SOLUTIONS, 2026b). É a violação da condição (ii) do critério de suficiência.

Substituição de regime. Responde-se com evidência obtida sob regime operacional distinto do contratado — dados de clima temperado para operação tropical, de despacho sazonal para ciclagem contínua, de operação

neutra quanto a arbitragem para operação multiserviço, de distribuição de treinamento para operação fora dela. É a violação da condição (iii), e o modo mais relevante para o parque brasileiro que entra em operação a partir de 2028, pelas razões desenvolvidas em Fagundes (2026): experiência acumulada em um regime não transfere automaticamente para outro, e o modo de falha do Victorian Big Battery ocorreu precisamente na transição entre regimes (ENERGY SAFE VICTORIA, 2021).

A regra prática que decorre da taxonomia é simples de enunciar e desconfortável de aplicar: **a não-resposta é informação, e deve ser registrada como tal na avaliação, e não tratada como pendência documental a ser sanada depois.** Pendência sanada depois da assinatura já não dispõe da alavanca contratual que a tornaria sanável.

IX. ESCOPO DE VALIDADE DA EVIDÊNCIA

As condições (ii) e (iii) do critério de suficiência desdobram-se em três dimensões que delimitam o que um documento sustenta.

Edição do método. O procedimento sob o qual a medição ocorreu define o que foi medido. No caso do UL 9540A, relatórios anteriores à 6ª edição foram produzidos sob método que admitia o encerramento precoce discutido na Seção V, e a vigência da nova edição foi estabelecida para 1º de janeiro de 2027 (UL SOLUTIONS, 2026a). Existe inclusive proposta para que a edição do UL 9540A conste da placa de marcação e das instruções do sistema, o que indica que o próprio ecossistema normativo reconhece a edição como informação de identificação, e não como detalhe bibliográfico.

Identidade de configuração. O objeto ensaiado precisa ser o objeto entregue. Alterações de química, configuração de módulo, invólucro, supressão ou firmware rompem a identidade e invalidam a transferência (UL SOLUTIONS, 2026b). Na prática de aquisição, isso significa vincular a evidência à lista de materiais e à revisão de projeto da proposta, e não ao nome comercial do produto.

Regime operacional pressuposto. Toda medição incorpora hipóteses sobre a condição de uso. O achado do Victorian Big Battery quanto à lacuna entre o envelope de ensaio de queima — que contempla ventos da ordem de 12 mph — e as rajadas de até 35 mph registradas no dia do evento é a ilustração canônica (FAGUNDES, 2026; ENERGY SAFE VICTORIA, 2021). Para o Brasil, a dimensão crítica é térmica: a margem entre temperatura de

junção e ambiente, que governa o estrangulamento térmico da inferência embarcada, é comprimida pelo clima local justamente nas horas de maior solicitação do ativo.

Segue daí uma exigência de especificação que não aparece na lista do artigo anterior e que este artigo acrescenta: **a evidência deve vir acompanhada de declaração de escopo de validade** — edição do método, identificação da configuração ensaiada e regime operacional pressuposto. Sem essas três informações, as condições (ii) e (iii) não são verificáveis, e o documento não é avaliável, qualquer que seja sua qualidade intrínseca.

X. APLICAÇÃO: LEITURA DE UM DOSSIÊ CONSTRUÍDO

O dossiê a seguir é construído por este autor para fins de ilustração. Não corresponde a fornecedor, produto ou processo real, e não deve ser lido como avaliação de qualquer participante de mercado. As respostas foram redigidas para representar padrões plausíveis, não para caricaturar.

Contexto. Comprador especifica sistema de 60 MW / 120 MWh, química LFP, conexão à rede básica com requisito de formação de rede, regime multiserviço com exposição a mercado.

Segregação projetada. *"O sistema emprega algoritmos avançados de inteligência artificial integrados ao BMS, com arquitetura redundante e certificação ISO 9001."* — Classe E1a. A pergunta era sobre fronteira de autoridade; a resposta descreve capacidade e apresenta certificação de sistema de gestão, que nada informa sobre arquitetura de controle. Substituição de artefato combinada com substituição de métrica. A ausência de mapeamento aos métodos da ISO/IEC TR 5469:2024 sugere que a fronteira foi herdada da plataforma do fornecedor, não projetada para este ativo.

Envelope temporal. *"Latência típica de resposta do controlador inferior a 5 ms."* — Classe E0. Substituição de métrica em sua forma pura, e exatamente o caso demonstrado na Seção VIII. "Típica" é média; a asserção exige pior caso sob condição térmica de projeto.

Ponto de operação da detecção. *"Acurácia de detecção superior a 98% em base de validação."* — Classe E2. Houve medição, sobre a grandeza errada. Não há taxa de falsos negativos na região de operação, nem latência de detecção, nem comportamento sob falha de sensor. Dado o custo assimétrico entre falso negativo e falso positivo, e dado o precedente de Moss Landing, em que o falso

positivo produziu o próprio dano (FAGUNDES, 2026), acurácia agregada é irrelevante para a decisão.

Contenção. *"Sistema testado conforme UL 9540A, relatório de ensaio disponível mediante acordo de confidencialidade."* — Classe E1b na forma apresentada, potencialmente E3 quando o relatório for lido. É a resposta mais promissora do dossiê e a que o comprador deve perseguir. As perguntas a fazer são três: em que nível o ensaio parou; sob que edição foi conduzido; e se a configuração ensaiada corresponde à ofertada. Se parou em módulo, o dossiê nada sustenta sobre os afastamentos propostos.

Não desabilitação. *"As funções de segurança seguem as melhores práticas do setor e só podem ser alteradas por pessoal autorizado."* — Classe E0, e a resposta mais preocupante do conjunto. "Só por pessoal autorizado" não nega a existência de modo de desabilitação: afirma controle de acesso a ele. A pergunta era se o modo existe. É exatamente a configuração que produziu o evento do Victorian Big Battery, em que a proteção foi removida por comutação para modo de serviço e a falha permaneceu não detectada por treze horas (FAGUNDES, 2026; ENERGY SAFE VICTORIA, 2021).

Arbitragem entre controladores. *"O BMS possui prioridade sobre o EMS em condições de limite."* — Classe E0. A resposta enuncia uma regra de precedência sem informar tempo de resolução, registro da variável bloqueadora, comportamento de reapresentação do comando, possibilidade de sobrescrita pelo PPC ou definição de modo degradado. Das oito perguntas da Seção VII, responde parcialmente a uma.

Rastreabilidade. *"O sistema registra eventos e alarmes com carimbo de tempo, exportáveis via API."* — Classe E2. Registro de evento não é registro de restrição ativa e de ação bloqueada. A distinção importa sob o regime de penalidades da REN nº 1.162/2026 (ANEEL, 2026): o que precisa ser demonstrável é por que o sistema não executou determinada ação, e isso exige o registro da restrição que a barrou, não do alarme que a acompanhou.

Autonomia sem conectividade. *"Operação local garantida em caso de perda de comunicação."* — Classe E0. Sem duração declarada, sem setpoint, sem estado de partida, sem funções degradadas identificadas, sem comportamento de reconexão e sem tratamento de comando obsoleto.

Interoperabilidade. *"Interfaces padronizadas Modbus TCP e IEC 61850; dados operacionais acessíveis pelo*

portal do fornecedor." — Classe E3 quanto ao protocolo, E0 quanto à propriedade dos dados. Acesso por portal do fornecedor não é propriedade de dado, e a resposta não trata do ponto de integração do controlador, que é onde a dependência efetivamente se forma.

Leitura consolidada. O dossiê responde a nove das dez asserções da Tabela III: a efetividade da segregação sob falha não recebe resposta específica. Das nove respostas, uma é certificação organizacional sem relação com o produto ofertado, quatro são declarações sem evidência, duas apresentam medição sobre grandeza inadequada, uma é parcial e uma é potencialmente sustentável mediante documento já existente.

Nenhuma resposta alcança E4. Das cinco asserções que exigem E4 pela Tabela III, quatro são explicitamente tratadas no dossiê e permanecem sem sustentação; a quinta — efetividade da segregação sob falha — sequer recebe resposta. O dossiê não permite formar juízo sobre comportamento sob falha.

O ponto metodológico é que essa conclusão foi obtida **sem avaliar o produto**. Não se afirmou que o sistema é inseguro; afirmou-se que o dossiê não demonstra que é seguro. São proposições distintas, e apenas a segunda está ao alcance de quem lê documentos.

XI. USO INSTITUCIONAL: TRÊS AVALIADORES, TRÊS FUNÇÕES DE PERDA

Licenciador, segurador e financiador leem o mesmo dossiê com funções de perda distintas, e o desalinhamento entre elas é um risco de projeto pouco reconhecido.

O **licenciador** decide sob incerteza com perda assimétrica e irreversível: autorizar um empreendimento que falha é dano público, enquanto indeferir é custo privado. Sua racionalidade favorece exigir classe alta e, na dúvida, indeferir. Axminster e Pound Road exemplificam o padrão — em ambos, a decisão não afirmou que o sistema falharia, e sim que não fora demonstrado que não falharia.

O **segurador** decide sob perda quantificável e recorrente, com leitura atuarial. O levantamento da QBE junto a 49 corpos de bombeiros britânicos apurou 212 incêndios ligados a sistemas fotovoltaicos em 2025, contra 91 em 2022 — alta de 133% —, enquanto o número de instalações cresceu 52%, com a propagação para além da instalação de origem subindo de 33 para 88 casos no mesmo período (QBE, 2026). A incidência observada

cresceu mais rapidamente do que o número de instalações, sinal que merece consideração na modelagem de risco — embora os dados agregados não permitam inferir diretamente uma taxa causal de falha por instalação, uma vez que não normalizam idade do parque, tipologia, exposição, qualidade de instalação nem eventuais mudanças de critério de notificação. O que a série sustenta é que a hipótese de estabilidade da sinistralidade por unidade não pode ser assumida sem verificação, o que empurra a subscrição em direção a evidência de classe superior ou a prêmio que a substitua.

O **financiador** decide sobre fluxo de caixa em horizonte contratado, com exposição dupla: o evento de segurança e a incapacidade de empilhar receitas. No ativo de 30 MW/60 MWh do sistema de transmissão paulista, o estudo publicado indica que a extensão para determinados serviços adicionais pode exigir alterações de ajustes de proteção, de algoritmos de controle e de sistemas auxiliares de software e hardware (TORRES et al., 2025), o que demonstra que capacidade nominal, isoladamente, não define a aptidão funcional do ativo. A arquitetura de controle é, portanto, variável de modelagem financeira, e não apenas de segurança.

O risco de desalinhamento é concreto: um dossiê suficiente para a habilitação técnica pode ser insuficiente para o licenciamento ambiental, e um dossiê suficiente para ambos pode não sustentar a hipótese de receita que fundamenta o financiamento. Como as três avaliações ocorrem em momentos distintos e a alavanca contratual sobre o fornecedor se extingue na assinatura, **a classe de evidência a especificar é a exigida pelo avaliador mais rigoroso da cadeia, e não pela primeira barreira a ser transposta.**

XII. O QUE ESTA ANÁLISE NÃO DEMONSTRA

Esta análise sustenta que a distinção entre classes de evidência é operacionalizável; que a suficiência probatória exige simultaneamente classe adequada, identidade de configuração e aplicabilidade de regime; que a lógica de parada do UL 9540A produz, por construção, dossiês silentes sobre a escala de instalação, e que essa lacuna foi reconhecida e corrigida normativamente em 2026 nos Estados Unidos e permanece aberta no arcabouço brasileiro; que a arbitragem de autoridade entre controladores é asserção distinta das demais e exige classe própria de evidência; e que a não-resposta admite classificação e é informativa.

Ela **não** é metodologia validada, e esta é a limitação principal do trabalho. O dossiê da Seção X foi construído por este autor, com respostas selecionadas para ilustrar modos de substituição definidos pelo próprio autor. Esse exercício demonstra que os instrumentos produzem leitura internamente consistente; não demonstra que produzem leitura correta, nem que discriminam adequadamente entre dossiês de qualidade distinta. A validação exigiria aplicação a um conjunto de dossiês reais anonimizados, com avaliação independente dos resultados — trabalho que não foi realizado e que constitui a continuação natural desta linha.

A tipologia da Tabela I é proposta conceitual, sem calibração quantitativa. As classes E0 a E3 são ordenadas por informação recuperável; acima de E3, a comparação depende dos dois eixos descritos na Seção IV-A e não admite ordenação única. Não se propõe métrica de força relativa entre E4 e E5.

A taxonomia da Seção VIII não é exaustiva nem foi derivada de amostra sistemática de respostas de mercado. Modos adicionais provavelmente existem, e a distribuição relativa entre eles é desconhecida.

Esta análise tampouco constitui avaliação de fornecedor, produto ou tecnologia, nem substitui análise de risco de projeto, análise de mitigação de perigos ou parecer de conformidade emitido por profissional habilitado. Não trata de aspectos jurídicos ou contratuais da aquisição, que exigem competência distinta.

Por fim, os instrumentos aqui propostos endereçam a leitura de evidência apresentada. Eles não resolvem o caso em que a evidência necessária não existe — situação que, para a caracterização de tempo de execução no pior caso sob estrangulamento térmico em contêiner operando em clima tropical, permanece sendo a lacuna experimental mais relevante para o parque brasileiro que entra em operação a partir de 2028 (FAGUNDES, 2026).

XIII. CONCLUSÃO

O artigo anterior encerrou observando que a janela para especificar corretamente os ativos do parque brasileiro de armazenamento fecha antes de eles existirem. Este acrescenta que especificar sem saber ler produz a mesma exposição, com mais papel.

A assimetria que separa comprador e fornecedor subsiste mesmo quando a informação existe e é disponibilizada: é de competência para avaliar escopo. Ela não se resolve exigindo mais certificados, porque certificado é conclusão

destacada de premissa. Resolve-se com quatro instrumentos, todos de aplicação imediata: uma tipologia de classes de evidência; um critério de suficiência que exige simultaneamente classe adequada, configuração compatível e regime aplicável; uma matriz explícita de autoridade e arbitragem entre controladores; e o hábito de registrar a não-resposta como informação, e não como pendência.

A proposição que os organiza é que não existe evidência forte em abstrato. Existe correspondência, ou ausência de correspondência, entre a asserção que se precisa sustentar e a evidência de que se dispõe — correspondência que depende simultaneamente da fidelidade de configuração e do realismo da condição sob a qual a observação foi feita.

A intervenção de melhor relação entre custo e ganho probatório é modesta e quase nunca praticada: pedir o relatório em vez do certificado, e exigir que ele venha com nível, edição e configuração declarados. Não impõe nova campanha experimental; recupera evidência já produzida, ainda que possa demandar acordo de confidencialidade.

Axminster demonstrou que conformidade cumprida não licencia. Pound Road demonstrou algo mais duro: nem mesmo a ausência de objeção da autoridade tecnicamente competente licencia, se a demonstração não for feita. Entre a habilitação técnica de novembro, os leilões de dezembro e o início de suprimento em agosto de 2028, cada dossiê lido no Brasil estará sujeito ao mesmo critério — com a diferença de que aqui a lacuna normativa que a NFPA 855 fechou em 2026 continua aberta, e o que não for exigido em contrato não será obtido depois.

REFERÊNCIAS

AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA (ANEEL). **Resolução Normativa nº 1.162, de 2 de junho de 2026**. Altera a Resolução Normativa nº 1.000, de 7 de dezembro de 2021, para disciplinar o faturamento e o enquadramento regulatório de sistemas de armazenamento de energia elétrica. Brasília, DF: ANEEL, 2026. Publicada no DOU de 24 jun. 2026.

ASSURANCE CASE WORKING GROUP. **Goal Structuring Notation community standard**. Bristol: Safety-Critical Systems Club, [20--?].

BLOOMFIELD, R.; RUSHBY, J. **Assurance of AI systems and the confidence in assurance cases**. Relatório técnico. [S.l.: s.n.], 2020.

BRASIL. Ministério de Minas e Energia. **Portaria Normativa nº 136, de 1º de junho de 2026**. Estabelece as diretrizes e a sistemática para a realização do Leilão de Reserva de

Capacidade na forma de Potência por meio de novos sistemas de armazenamento de energia em baterias — LRCAP de 2026. Brasília, DF: Diário Oficial da União, 2026.

EMPRESA DE PESQUISA ENERGÉTICA (EPE). **Resultado do cadastramento — LRCAP de 2026 Armazenamento**. Rio de Janeiro: EPE, ago. 2026.

ENERGY SAFE VICTORIA. **Statement of technical findings: fire at the Victorian Big Battery**. Melbourne: ESV, 28 set. 2021.

FAGUNDES, E. M. **Conformidade não é segurança: argumento de segurança demonstrável em sistemas de armazenamento de energia e a arquitetura de controle que o sustenta**. Zenodo, set. 2026. DOI 10.5281/zenodo.22310318.

GOODENOUGH, J. B.; WEINSTOCK, C. B.; KLEIN, A. Z. Eliminate induction: a basis for arguing system confidence. In: **INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING (ICSE)**, 35., 2013, San Francisco. Proceedings [...]. [S.l.: s.n.], 2013.

HAWKINS, R.; PATERSON, C.; PICARDI, C.; JIA, Y.; CALINESCU, R.; HABLI, I. **Guidance on the assurance of machine learning in autonomous systems (AMLAS)**. York, UK: Assuring Autonomy International Programme, University of York, 2021.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 15026: systems and software engineering — systems and software assurance**. Genebra: ISO/IEC.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC TR 5469:2024: artificial intelligence — functional safety and AI systems**. Genebra: ISO/IEC, 2024.

KELLY, T. P.; MCDERMID, J. A. Safety case construction and reuse using patterns. In: **INTERNATIONAL CONFERENCE ON COMPUTER SAFETY, RELIABILITY AND SECURITY (SAFECOMP)**, 16., 1997, York. Proceedings [...]. [S.l.: s.n.], 1997.

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA). **NFPA 855: standard for the installation of stationary energy storage systems**, ed. 2026, Anexo G.11. Quincy, MA: NFPA, 2026.

QBE INSURANCE. **Solar panel fires increasing at more than double the rate of installations**. Londres: QBE European Operations, ago. 2026.

SANDIA NATIONAL LABORATORIES. **Analyzing system safety in lithium-ion grid energy storage**. Albuquerque, NM: Sandia National Laboratories, 2016. Disponível em: <https://www.osti.gov/servlets/purl/1257985>.

TELGIAN ENGINEERING & CONSULTING. **NFPA 855 changes in the 2026 edition**. [S.l.]: Telgian Engineering & Consulting, 2025.

TORRES, P. F.; MANITO, A. R. A.; FIGUEIREDO, G.; ALMEIDA, M. P.; ALMEIDA NETO, J. C. S.; CAVALCANTE, R. L.; SILVA, C. C. V. F. A.; ZILLES, R. Energy storage as a transmission asset — assessing the multiple uses of a utility-scale battery energy storage system in Brazil. **Energies**, v. 18, n. 4, art. 902, 2025. DOI 10.3390/en18040902.

UL SOLUTIONS. **UL 9540A test method for battery energy storage systems e Understanding UL 9540A, NFPA 855 and large-scale fire testing for battery energy storage systems**. Northbrook, IL: UL Solutions, 2026a.

UL SOLUTIONS. **Installation codes and requirements for energy storage systems (ESS) — FAQs**. [S.l.]: UL Solutions, 2026b.

UL STANDARDS & ENGAGEMENT (ULSE). **UL 4600: standard for safety for the evaluation of autonomous products**. Northbrook, IL: ULSE.

UNITED KINGDOM. Ministry of Defence. **Defence Standard 00-56: safety management requirements for defence systems**. Glasgow: MoD.