

ORIGINAL RESEARCH

Open access

A Conceptual Framework for Liability-Aware Autonomous Smart Grids Linking Algorithmic Decisions, Operator Oversight, and Regulatory Auditability

Noah Williams^{1*}, Liam Johnson¹, Grace Collins², Ethan Brooks¹

Abstract

Autonomous smart grids increasingly rely on AI-driven decisions, yet legal frameworks have not kept pace. Liability for autonomous actions remains ambiguous, threatening both innovation and accountability. No existing conceptual framework systematically links the algorithmic decision layer, operator oversight, and regulatory auditability to address the liability gap in autonomous grid operations. This creates uncertainty when harmful outcomes arise from distributed interactions among software, operators, vendors, and regulated utilities. This article develops a conceptual framework that connects these three layers into a coherent liability-aware governance architecture for autonomous smart grids. The aim is to clarify how responsibility could be assigned, reviewed, and operationalized before and after autonomous grid actions occur. The framework is built through conceptual synthesis of AI law, human-in-the-loop research, and regulatory governance literature. No experiments are conducted, and no quantitative data are presented. The framework defines the roles and interactions of algorithmic decisions, operator oversight, and auditability mechanisms, and derives eight testable propositions. Two tables summarize the decision-liability mapping and the framework logic. The liability-aware framework provides a foundation for designing accountable autonomous grid systems and for future interdisciplinary legal-technical research. It supports legal clarity while preserving the operational benefits of intelligent grid automation.

Keywords Conceptual framework, Liability, Autonomous smart grids, Algorithmic decisions, Operator oversight, Regulatory auditability

*Correspondence:

Noah Williams

noah.williams@gmail.com

¹ Department of Smart Grid Technologies, Faculty of Engineering, University of Melbourne, Melbourne, Australia

² Department of Energy Data Science, Faculty of Engineering, University of Sydney, Sydney, Australia

Introduction

Autonomous smart grids are increasingly shaped by AI systems that forecast demand, schedule flexible resources, manage distributed energy assets, and recommend or execute control actions in real time. Reinforcement learning and related machine-learning approaches have become prominent in demand response and operational decision-making because they can adapt to dynamic grid conditions [1]. Yet as these systems become more autonomous, responsibility for harmful grid outcomes could become distributed across algorithms, operators, data providers, utilities, and technology vendors.

The legal difficulty is not merely that AI systems are technically complex, but that their decisions may sit between traditional categories of human agency and machine operation. Legal scholarship on AI liability has warned that

automated systems can create responsibility gaps when harm cannot be clearly attributed to a human actor, manufacturer, deployer, or software provider [2]. In autonomous grid contexts, this problem is intensified because operational decisions can affect safety, reliability, consumer access, and market fairness at the same time.

Existing energy governance research has emphasized that smart grid transitions are sociotechnical rather than purely technical processes, requiring attention to institutional design, justice, accountability, and public legitimacy [3]. AI governance scholarship similarly argues that regulatory systems must move beyond broad ethical aspirations toward enforceable arrangements that identify duties, risks, and review mechanisms [4]. A liability-aware framework for autonomous grids therefore needs to connect technical control, human supervision, and regulatory auditability in a single conceptual architecture.

This article contributes such a framework by linking three governance layers: the algorithmic decision layer, the operator oversight layer, and the regulatory auditability layer. The proposed framework treats liability as a relational governance problem rather than as a purely post-hoc legal question, drawing on work on AI service responsibility, transparency, and human control [5]. It argues that liability for autonomous grid actions would be more systematically assignable when algorithmic decisions are traceable, operator authority is defined, and regulatory audit trails are designed before deployment.

Liability Problem

Liability diffusion in autonomous systems

Liability diffusion arises when multiple actors contribute to an autonomous decision without any single actor appearing to exercise complete control. AI-as-a-service arrangements are especially relevant because grid operators may rely on models, platforms, or decision-support tools developed and maintained by external providers [5]. In such cases, liability would be difficult to assign unless contractual, operational, and technical responsibilities are linked to the specific decision points where harm could occur.

Legal doctrines and their limits

Traditional tort doctrines can address negligence, defective products, and failures to warn, but AI systems complicate these categories when conduct emerges from learning, adaptation, and opaque decision pathways. Legal analyses of AI injury have questioned whether existing tort doctrines are adequate when the relevant causal chain includes automated inference, data-driven adaptation, and human reliance on machine recommendations [6]. The framework proposed here therefore treats legal doctrine as necessary but insufficient unless supported by operational records and governance structures.

The energy-sector specificity

The energy sector has distinctive liability features because grid actions can simultaneously involve reliability obligations, consumer protection, cybersecurity exposure, environmental performance, and public-service duties. Research on AI in sustainable energy systems shows that algorithmic tools are spreading across forecasting, optimization, control, and asset management, creating governance challenges beyond ordinary software deployment [7]. Liability-aware smart grid governance must therefore reflect the critical-infrastructure character of electricity systems rather than importing generic AI accountability models without adaptation.

Autonomous Smart Grid Background

Levels of autonomy in grid control

Autonomy in grid control can range from advisory analytics to automated control actions that require little or no immediate human approval. Reviews of AI in power systems indicate a progression from predictive tools toward systems that can support or execute operational decisions across supply, demand, storage, and network management [8]. The legal relevance of autonomy lies in whether the system merely informs a human decision or materially determines the action that creates risk.

Examples of autonomous decisions

Autonomous grid decisions may include electric vehicle charging schedules, storage dispatch, demand response activation, microgrid control, and renewable integration management. Deep reinforcement learning has been applied to real-time electric vehicle charging, illustrating how algorithmic agents can allocate resources under grid constraints and user needs [9]. Similar applications in energy storage arbitrage show that autonomous decisions may affect both economic outcomes and asset degradation, making liability analysis dependent on the decision's operational context [10].

Current oversight practices

Current oversight practices often rely on operators, engineers, and compliance teams to monitor automated recommendations, intervene when needed, and review failures after incidents. Human factors research warns that such arrangements can be fragile when operators are asked to supervise highly automated systems without clear authority, situational awareness, or intervention protocols [11]. In smart grids, oversight would therefore need to be designed as an accountable governance function rather than as an informal expectation that humans will notice and correct algorithmic failures.

Algorithmic Decision Layer

Types of algorithmic decisions

The algorithmic decision layer includes predictive, prescriptive, and autonomous control functions that influence grid operations. Demand-side response systems, for example, may predict flexibility, recommend load shifting, or directly trigger automated adjustments across distributed resources [12]. The framework proposes that liability analysis should begin by classifying the decision type because predictive advice, optimization recommendations, and autonomous execution generate different expectations of human review and vendor responsibility.

Opacity and traceability issues

Opacity becomes a liability problem when affected parties, operators, or regulators cannot reconstruct why a particular grid action occurred. Explainable AI research in energy and power systems identifies transparency, interpretability, and post-hoc explanation as central challenges for deploying machine-learning systems in operational contexts [13]. In this framework, traceability would not require full exposure of proprietary model internals in every case, but it would require enough decision reconstruction to support responsibility attribution and compliance review.

Liability-triggering scenarios

Liability-triggering scenarios could include unsafe switching, unjustified curtailment, discriminatory demand response, battery degradation from automated dispatch, or failure to prevent cascading operational risk. Safe reinforcement learning work on electric vehicle charging shows that constraints can be embedded into autonomous scheduling, but the legal question remains who is responsible when such constraints are insufficient, incorrectly specified, or ignored by the deployed system [14]. The framework therefore treats liability triggers as events where algorithmic action, foreseeable risk, and governance failure intersect.

Data and logging requirements

Data and logging requirements are foundational because liability cannot be assigned reliably without records of inputs, model outputs, confidence indicators, constraints, operator actions, and system state. Research on algorithmic inscrutability emphasizes that accountability depends less on whether systems are intuitively understandable and more on whether they can be examined, tested, and challenged through appropriate procedures [15]. **Table 1** summarizes how different algorithmic decision types would create distinct liability triggers and oversight requirements.

Table 1. Classification of Algorithmic Decision Types, Associated Liability Triggers, Oversight Functions, and Required Audit Records in Grid Operations

Algorithmic decision type	Grid function	Potential liability trigger	Required oversight function	Audit record needed
Predictive recommendation	Forecasting demand, renewable output, congestion, or flexibility	Harmful reliance on inaccurate forecast or failure to flag uncertainty	Operator review of forecast confidence, boundary conditions, and operational relevance	Input data provenance, forecast timestamp, uncertainty statement, model version, and operator acknowledgement
Prescriptive optimization	Scheduling storage, demand response, or electric vehicle charging	Optimization objective prioritizes cost or efficiency over safety, equity, or reliability	Human approval of objective hierarchy and constraint selection before execution	Objective function description in plain language, constraint set, rejected alternatives, approval record, and exception log
Autonomous execution	Direct control of devices, switches, loads, or distributed resources	Automated action causes outage, equipment damage, unfair curtailment, or safety risk	Predefined intervention thresholds and real-time override authority	Control command, system state, trigger condition, execution pathway, override availability, and post-action review
Adaptive learning update	Model updates based on new operational data or feedback	Model drift produces unsafe or legally non-compliant behavior	Periodic validation and suspension authority when drift indicators exceed acceptable limits	Training data window, update rationale, validation result, drift signal, deployment approval, and rollback record
Emergency automation	Rapid response to faults, instability, or cyber-physical disturbance	System escalates or suppresses emergency action without sufficient justification	Ex-ante certification of emergency logic and ex-post incident review	Emergency trigger, decision latency, alternatives considered, operator notification, system constraints, and incident reconstruction

Figure 1 maps how different autonomous smart-grid decision types create distinct liability triggers, oversight requirements, and audit evidence needs.



Figure 1. Decision-to-Liability Mapping Across Autonomous Smart-Grid Functions

Operator Oversight Layer

Models of human-in-the-loop

The operator oversight layer defines how humans remain meaningfully involved in autonomous grid governance. Meaningful human control scholarship argues that human involvement must be more than symbolic; it must include the ability to understand, influence, and take responsibility for system behavior [16]. In the proposed framework, human-in-the-loop, human-on-the-loop, and human-over-the-loop arrangements would each carry different liability implications depending on timing, authority, and access to information.

Oversight responsibilities and authority

Oversight responsibilities should specify who may approve, pause, override, or escalate algorithmic actions under ordinary, abnormal, and emergency conditions. Variable autonomy research suggests that control can shift between humans and automated systems depending on context, risk, and operational needs [17]. Liability would be assigned more coherently when those shifts are predefined, legally recognized, and logged rather than improvised during incidents.

Training and trust calibration

Training is necessary because operators may either over-trust automated recommendations or reject useful automation without clear reasons. Human-automation research shows that effective oversight requires calibrated trust, situational awareness, and awareness of automation limitations [11]. In autonomous grids, operator training should therefore include not only technical interface use but also legal awareness of when reliance, override, and escalation could affect responsibility attribution.

Legal status of operator override

The legal status of operator override is central because an override can either prevent harm, create new harm, or reveal that the system's automated pathway was not adequately governed. AI liability scholarship has emphasized that regulatory approaches must define responsibilities across developers, deployers, and users rather than assuming that a human supervisor automatically absorbs responsibility [18]. Under this framework, an operator override would be legally meaningful only if the operator had sufficient authority, timely information, feasible alternatives, and a documented basis for intervention.

Regulatory Auditability Layer

Audit trail specifications

The regulatory auditability layer specifies what must be recorded so that autonomous grid actions could be reconstructed after incidents, disputes, or compliance reviews. AI-enabled microgrid control illustrates why audit trails must capture not only final actions but also the control environment, operating mode, data sources, and intervention opportunities surrounding the action [19]. In this framework, audit trails would serve as legal infrastructure by preserving the evidence needed to distinguish algorithmic error, operator omission, vendor defect, and unforeseeable system disturbance.

Explainability for compliance

Explainability for compliance differs from explainability for engineering optimization because regulators need decision accounts that are reviewable, contestable, and connected to legal duties. Research on transparency requirements for AI emphasizes that trustworthy transparency must be contextual, meaning that the form of explanation should match the affected stakeholder, institutional setting, and accountability purpose [20]. For autonomous smart grids, the framework proposes that compliance explanations should translate algorithmic actions into operational reasons, risk controls, and responsibility-relevant decision points.

Regulatory review and enforcement

Regulatory review would examine whether autonomous grid systems were designed, deployed, supervised, and updated consistently with legally recognized obligations. Risk-management analysis of the Artificial Intelligence Act shows that AI regulation increasingly relies on ex-ante risk controls, documentation, monitoring, and post-market governance rather than only post-hoc liability claims [21]. In the proposed framework, enforcement would be strengthened when regulators can compare audit records with declared system functions, operator protocols, and approved operational boundaries.

Standards and certification

Standards and certification can reduce liability uncertainty by defining minimum expectations for traceability, oversight, testing, documentation, and incident reporting. Research on AI-powered renewable integration in multi-energy systems shows that large-scale automation creates cross-sector reliability and governance challenges that cannot be managed through isolated technical optimization alone [22]. Certification under this framework would not eliminate liability, but it could clarify whether a utility, vendor, or operator complied with recognized governance duties before harm occurred.

Framework Logic

Linking the three layers

The framework links the algorithmic decision layer, operator oversight layer, and regulatory auditability layer through a sequential but interactive logic. Methods integrating AI, big data, internet of things, and blockchain in smart energy management demonstrate that autonomous energy governance increasingly depends on interconnected technical infrastructures rather than single decision tools [23]. The framework therefore proposes that liability-aware governance must follow the decision across its full pathway: from algorithmic generation, to human oversight, to regulatory review.

Figure 2 presents the proposed liability-aware governance architecture linking algorithmic decision generation, operator oversight, regulatory auditability, and responsibility attribution in autonomous smart-grid operations.

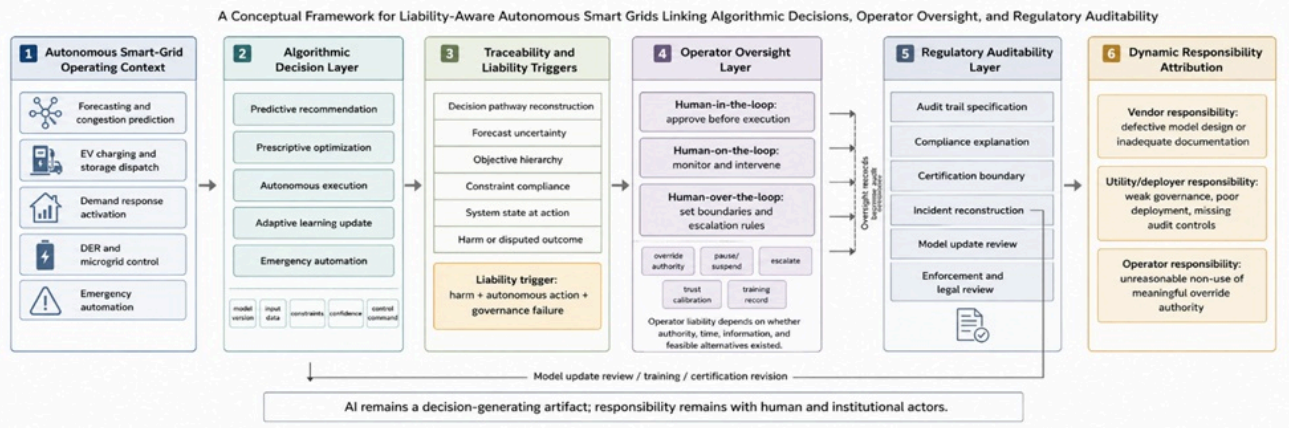


Figure 2. Liability-Aware Governance Architecture for Autonomous Smart Grids

Information flows and feedback

Information flows are central because operators cannot supervise what they cannot see, and regulators cannot audit what systems fail to record. Research on electricity supply-chain automation shows that AI can coordinate multiple operational activities, but such coordination also increases dependence on reliable information exchange among actors and systems [24]. The framework proposes feedback loops in which audit findings inform operator training, operator interventions inform model governance, and algorithmic failures inform regulatory certification requirements.

Dynamic liability assignment

Dynamic liability assignment means that responsibility would be allocated according to the role each actor played at the relevant decision point rather than fixed in advance to a single party. Theories of sociotechnical change show that governance frameworks must account for interactions among technology, institutions, organizational routines, and social expectations [25]. In autonomous grids, liability could therefore shift toward the vendor when the model design is defective, toward the utility when deployment governance is inadequate, or toward the operator when a legally meaningful override was available but unreasonably unused.

Boundary conditions and assumptions

The framework assumes that autonomous smart grid systems operate within regulated electricity environments where public-interest obligations, technical reliability, and legal accountability are inseparable. Debates on AI legal personhood show why the framework does not assign responsibility to the AI system itself, but instead treats AI as a decision-generating artifact embedded within human and institutional governance arrangements [26]. Table 2 maps the constructs, relationships, and liability pathways across the three layers.

Table 2. Multi-layer governance framework mapping algorithmic decision constructs, oversight relationships, and associated liability pathways with corresponding indicators for empirical validation in future research

Framework construct	Primary governance question	Relationship to other constructs	Liability pathway	Testable indicator for future research
Algorithmic decision classification	What type of decision did the AI system make or recommend?	Determines the level of operator review and the audit detail required	Misclassification may shift responsibility toward deployers that failed to recognize the system's autonomy level	Presence of formal decision taxonomy in deployment documentation

Traceability mechanism	Can the decision pathway be reconstructed after the event?	Enables operator explanation and regulatory review	Weak traceability increases uncertainty and may indicate governance negligence	Completeness of logs linking inputs, outputs, constraints, and system state
Operator authority design	Did a human actor have meaningful power to intervene?	Converts oversight from symbolic monitoring into legally relevant supervision	Responsibility may attach to operators only when authority, time, and information were sufficient	Existence of role-specific override rights and escalation rules
Trust calibration process	Were operators trained to rely on or challenge automation appropriately?	Shapes whether oversight can correct algorithmic error	Poor calibration may indicate organizational failure rather than individual operator fault	Training records addressing automation limits, uncertainty, and legal duties
Compliance explanation	Can the action be explained in terms regulators can assess?	Translates technical behavior into legal and operational justification	Inadequate explanation may shift responsibility toward deployers or vendors	Availability of stakeholder-specific explanations for disputed actions
Regulatory audit protocol	Can an external authority review the decision and governance pathway?	Connects logs, explanations, and oversight records into enforceable review	Missing audit protocol weakens legal certainty and enforcement capacity	Formal audit procedure covering incidents, model updates, and overrides
Certification boundary	What system functions were approved for autonomous operation?	Defines the lawful operating envelope for algorithmic and human action	Liability may arise when systems operate outside certified boundaries	Documented certification scope and evidence of boundary monitoring
Feedback and correction loop	Are failures converted into system, training, or regulatory improvements?	Links post-hoc review to future prevention	Failure to learn from incidents may support claims of organizational negligence	Recorded changes to models, procedures, or compliance controls after review

Propositions

Propositions on algorithmic transparency and liability

The first proposition is that higher decision traceability would reduce liability ambiguity in autonomous smart grid incidents. This proposition follows from the idea that inscrutability is not only a technical property but also a governance problem when affected parties cannot challenge or reconstruct automated decisions [15]. The second proposition is that transparency mechanisms would have stronger liability-reducing effects when they are tailored to the specific decision type rather than applied uniformly across all autonomous grid functions.

Propositions on operator oversight strength

The third proposition is that operator oversight would reduce liability diffusion only when operators possess authority, timely information, and feasible intervention options. Meaningful human control research supports this claim because human involvement is normatively significant only when it enables genuine influence over autonomous system behavior [16]. The fourth proposition is that variable autonomy protocols would improve responsibility attribution by clarifying when control shifts from algorithmic execution to human intervention [17].

Propositions on auditability and legal certainty

The fifth proposition is that stronger regulatory auditability would increase legal certainty by allowing regulators and courts to distinguish design failure, deployment failure, supervision failure, and unforeseeable disturbance. Contemporary AI liability analysis emphasizes that responsibility across developers, deployers, and users must be institutionally specified rather than inferred after harm occurs [18]. The sixth proposition is that certification and audit protocols would have greater liability-reducing effects when they include post-deployment monitoring rather than relying only on pre-deployment approval.

Propositions on interaction effects

The seventh proposition is that algorithmic transparency, operator oversight, and regulatory auditability would reinforce one another rather than operate as independent safeguards. Sector-specific reviews of AI in power systems show that key matters of concern include technical performance, governance, human reliance, and institutional responsibility, making isolated safeguards insufficient [27]. The eighth proposition is that liability-aware autonomous grid governance would be strongest where transparent decisions, meaningful oversight, and enforceable audit trails are designed together before deployment.

Figure 3 illustrates how integrated transparency, meaningful operator oversight, and enforceable auditability convert liability diffusion into stronger legal certainty and continuous governance improvement.

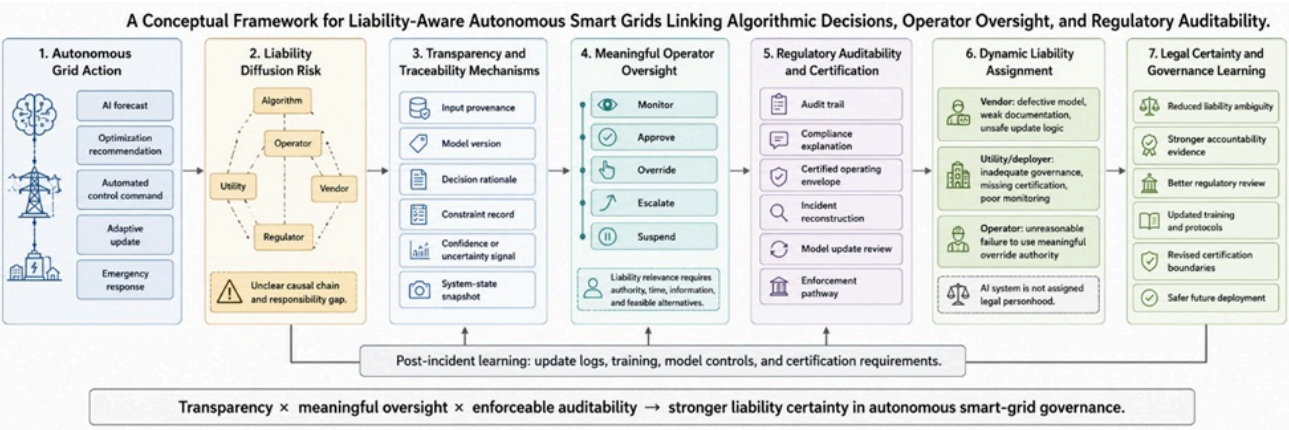


Figure 3. From Liability Diffusion to Legal Certainty: Auditability and Feedback Pathway

Implications

Implications for system designers

For system designers, the framework implies that liability awareness should be embedded into autonomous grid architecture rather than added after deployment. AI applications in sustainable energy systems already span forecasting, control, optimization, and management, so design teams should treat documentation, explainability, and override interfaces as core system features rather than compliance accessories [7]. Designers would therefore need to build systems that can support legal reconstruction as well as operational performance.

Implications for regulators and lawmakers

For regulators and lawmakers, the framework suggests that autonomous grid regulation should define evidence duties, oversight duties, and audit duties in relation to specific classes of algorithmic decision. Research on intelligent AI regulation argues that legal systems should adopt risk-sensitive and adaptive governance mechanisms rather than rely

on static rules that cannot keep pace with technical change [4]. In energy regulation, this means that auditability standards, certification boundaries, and liability presumptions could be coordinated before autonomous grid systems become widespread.

Implications for future research

For future research, the framework provides a conceptual basis for empirical, doctrinal, and design-oriented studies of liability-aware autonomous grids. Legal scholarship on AI liability in financial services shows that sectoral application matters because general AI liability principles must be translated into the institutional structure of the regulated domain [28]. Future studies could therefore examine how utilities, vendors, operators, regulators, and courts interpret the proposed constructs in real incidents, simulations, regulatory sandboxes, or comparative legal settings.

Conclusion

This article has developed a conceptual governance framework for liability-aware autonomous smart grids. The framework links algorithmic decision-making, operator oversight, and regulatory auditability as three interdependent layers of accountability.

The central argument is that liability for autonomous grid actions should not be treated only as a question for courts after harm occurs. It should also be designed into the technical, organizational, and regulatory architecture of autonomous grid systems before deployment.

The framework shows how algorithmic decisions could be classified, how operator authority could be structured, and how audit records could support post-hoc review. It also clarifies why responsibility should remain attached to human and institutional actors rather than displaced onto the autonomous system itself.

The proposed propositions offer a path for future empirical and legal research. By testing the relationships among transparency, oversight, auditability, and liability certainty, future work can refine the framework and support the responsible adoption of autonomous smart grids.

Acknowledgements

None

Conflict of interest

None

Financial support

None

Ethics statement

None

Rights and permissions

Open Access The author(s) retain copyright. This article is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. It may be shared and adapted for non-commercial purposes with appropriate attribution, an indication of changes, and distribution of adaptations under the same license. Third-party material may be subject to separate terms identified in its credit line. View the license at <https://creativecommons.org/licenses/by-nc-sa/4.0/>.

References

- Vázquez-Canteli JR, Nagy Z. Reinforcement learning for demand response: A review of algorithms and modeling techniques. *Appl Energy*. 2019;235:1072-89.
- Santoni de Sio F, Mecacci G. Four responsibility gaps with artificial intelligence: Why they matter and how to address them. *Philos Technol*. 2021;34(4):1057-84.
- Milchram C, Hillerbrand R, van de Kaa G, Doorn N, Künneke R. Energy justice and smart grid systems: Evidence from the Netherlands and the United Kingdom. *Appl Energy*. 2018;229:1244-59.
- Buiten MC. Towards intelligent regulation of artificial intelligence. *Eur J Risk Regul*. 2019;10(1):41-59.
- Cobbe J, Singh J. Artificial intelligence as a service: Legal responsibilities, liabilities, and policy challenges. *Comput Law Secur Rev*. 2021;42:105573.
- Sullivan HR, Schweikart SJ. Are current tort liability doctrines adequate for addressing injury caused by AI?. *AMA J Ethics*. 2019;21(2):160-6.
- Ahmad T, Zhang D, Huang C, Zhang H, Dai N, Song Y, et al. Artificial intelligence in sustainable energy industry: Status Quo, challenges and opportunities. *J Clean Prod*. 2021;289:125834.
- Heymann F, Quest H, Garcia TL, Ballif C, Galus M. Reviewing 40 years of artificial intelligence applied to power systems—A taxonomic perspective. *Energy AI*. 2024;15:100322.
- Wan Z, Li H, He H, Prokhorov D. Model-free real-time EV charging scheduling based on deep reinforcement learning. *IEEE Trans Smart Grid*. 2018;10(5):5246-57.
- Cao J, Harrold D, Fan Z, Morstyn T, Healey D, Li K. Deep reinforcement learning-based energy storage arbitrage with accurate lithium-ion battery degradation model. *IEEE Trans Smart Grid*. 2020;11(5):4513-21.
- Endsley MR. From here to autonomy: lessons learned from human–automation research. *Hum Factors*. 2017;59(1):5-27.
- Antonopoulos I, Robu V, Couraud B, Kirli D, Norbu S, Kiprakis A, et al. Artificial intelligence and machine learning approaches to energy demand-side response: A systematic review. *Renew Sustain Energy Rev*. 2020;130:109899.
- Machlev R, Heistrene L, Perl M, Levy KY, Belikov J, Mannor S, et al. Explainable Artificial Intelligence (XAI) techniques for energy and power systems: Review, challenges and opportunities. *Energy AI*. 2022;9:100169.
- Li H, Wan Z, He H. Constrained EV charging scheduling based on safe deep reinforcement learning. *IEEE Trans Smart Grid*. 2019;11(3):2427-39.
- Kroll JA. The fallacy of inscrutability. *Philos Trans R Soc A Math Phys Eng Sci*. 2018;376(2133):20180084.
- Santoni de Sio F, Van den Hoven J. Meaningful human control over autonomous systems: A philosophical account. *Front Robot AI*. 2018;5:323836.

Methnani L, Aler Tubella A, Dignum V, Theodorou A. Let me take over: Variable autonomy for meaningful human control. *Front Artif Intell.* 2021;4:737072.

Bertolini A, Episcopo F. The expert group's report on liability for artificial intelligence and other emerging digital technologies: A critical assessment. *Eur J Risk Regul.* 2021;12(3):644-59.

Trivedi R, Khadem S. Implementation of artificial intelligence techniques in microgrid control environment: Current progress and future scopes. *Energy AI.* 2022 1;8:100147.

Felzmann H, Villaronga EF, Lutz C, Tamò-Larrieux A. Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data Soc.* 2019;6(1):2053951719860542.

Schuett J. Risk management in the artificial intelligence act. *European Journal of Risk Regul.* 2024;15(2):367-85.

Liu Z, Sun Y, Xing C, Liu J, He Y, Zhou Y, et al. Artificial intelligence powered large-scale renewable integrations in multi-energy systems for carbon neutrality transition: Challenges and future perspectives. *Energy AI.* 2022;10:100195.

Li J, Herdem MS, Nathwani J, Wen JZ. Methods and applications for artificial intelligence, big data, internet of things, and blockchain in smart energy management. *Energy AI.* 2023;11:100208.

Richter L, Lehna M, Marchand S, Scholz C, Dreher A, Klaiber S, et al. Artificial intelligence for electricity supply chain automation. *Renew Sustain Energy Rev.* 2022;163:112459.

Sovacool BK, Hess DJ. Ordering theories: Typologies and conceptual frameworks for sociotechnical change. *Soc Stud Sci.* 2017;47(5):703-50.

Pagallo U. Vital, Sophia, and Co.—the quest for the legal personhood of robots. *Information.* 2018;9(9):230.

Henao F, Edgell R, Sharma A, Olney J. AI in power systems: A systematic review of key matters of concern. *Energy Inform.* 2025;8(1):76.

Montagnani ML, Najjar MC, Davola A. The EU Regulatory approach (es) to AI liability, and its Application to the financial services market. *Comput Law Secur Rev.* 2024;53:105984.