Regulatory-Grade Compliance Telemetry for Distributed Renewable Portfolios: A Secure Event-Sourced Fabric for Policy-Constrained Operation

Karim Bensalem[1] and Rachid Meziane[2]

[1]University of Ghardaia, Department of Environmental Economics and Natural Resource Management, BP 455, Noumerate Road, Ghardaia 47000, Algeria
[2]University of El Oued, Department of Environmental Policy and Sustainable Development, Chott Road 12, El Oued 39000, Algeria

Abstract

As electricity systems absorb large volumes of inverter-based generation, governance increasingly depends on the ability to observe, interpret, and verify operational behavior across many heterogeneous assets. Traditional compliance approaches rely on periodic reporting, document-heavy audits, and post hoc investigations, which do not scale well when operational decisions are automated and conditions change quickly. At the same time, higher penetration elevates the sensitivity of power-quality constraints, reliability services, and environmental or community operating limits, creating a need for oversight mechanisms that can be both technically rigorous and administratively workable. This paper proposes a regulatory-grade compliance telemetry fabric that treats compliance as a continuously maintained, event-sourced record of policy-constrained decisions rather than as a static checklist. The core contribution is an architecture that binds policy obligations to a tamper-evident stream of signed operational events, supports verifiable attribution across delegated operators and intermediaries, and enables low-latency auditing without forcing universal data disclosure. The design specifies interoperable compliance objects, runtime checkers that evaluate obligations against observed actions, and dispute-resolution workflows that reconstruct the provenance of contested outcomes. The approach is engineered for environments where fleets are controlled by aggregators, grid operators require fast assurance about constraint adherence, and regulators must manage both confidentiality and accountability. The paper details the fabric's threat model, data-plane primitives, policy compilation workflow, and practical deployment considerations, and proposes an evaluation methodology centered on stress scenarios, audit-time measurements, and robustness under policy updates.

1 Introduction

High-penetration renewable deployment is often framed as an engineering challenge of capacity expansion, interconnection studies, and balancing variability [1]. In practice, it is equally a challenge of operational governance: who is allowed to do what, under which conditions, with what evidence, and with what recourse when outcomes are contested. Distributed energy resources, utility-scale plants, storage, and demand response are increasingly orchestrated by software-defined controllers that can change behavior rapidly in response to prices, forecasts, and grid signals. This creates a mismatch between legacy compliance regimes, which assume slow-changing, human-interpretable operations, and modern control regimes, which produce decisions at machine speed and at scale [2]. When regulators, grid operators, and communities cannot reliably verify that operational constraints are being respected, they compensate with conservative limits, redundant procedures, and prolonged disputes, all of which reduce effective capacity and slow deployment.

The governance burden grows when renewable infrastructure is expected to serve not only mitigation but also resilience and adaptation objectives. Policy discourse and planning tools still often emphasize emissions reduction, while the system-level value of decentralization, diversification, and distributed robustness is treated as secondary. Comparative policy analysis has noted that national adaptation policies can acknowledge renewable energy's resilience potential while deployment in practice remains oriented toward mitigation rather than toward adaptation needs such as geographic and technological diversification [3]. This asymmetry matters for compliance design because adaptation-oriented operation introduces additional constraints, such as heatwave-driven derating,

wildfire safety shutoffs, and islanded microgrid behavior, all of which require auditable control decisions that are not easily reduced to static permit conditions [4].

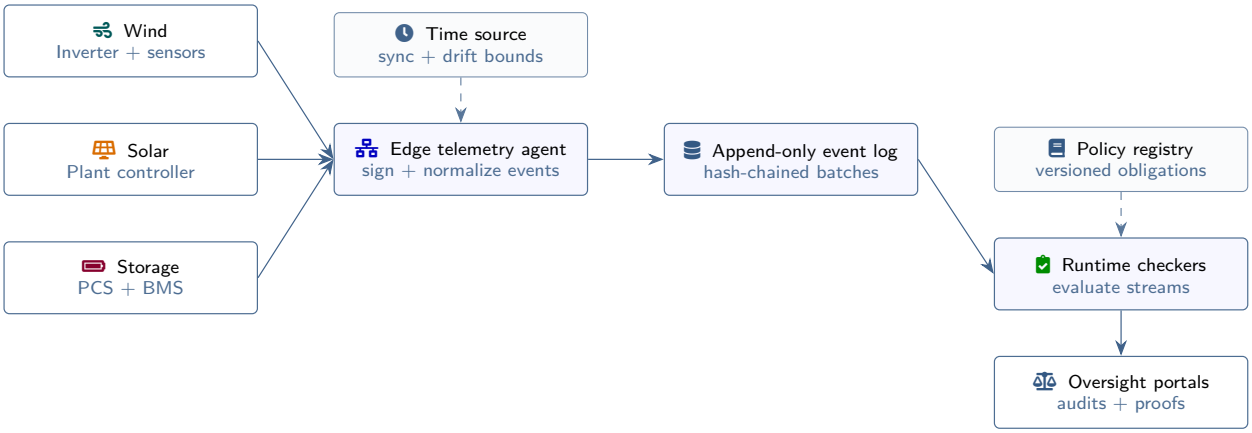

Figure 1: End-to-end compliance telemetry fabric for distributed renewable portfolios: heterogeneous assets emit signed operational events via an edge agent into an append-only log. Versioned policy objects feed runtime checkers that generate auditable compliance assertions and bounded disclosures for oversight stakeholders.

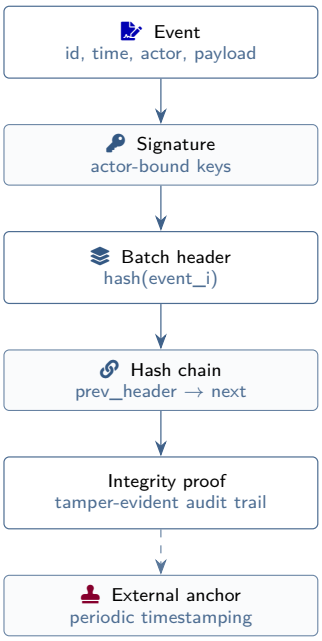

Figure 2: Evidence-grade event sourcing: operational events are signed, grouped into batch headers, and chained by hashes to make omission or modification detectable. Periodic anchoring strengthens timestamp assurance without requiring public-chain dependence.

This paper advances an independent technical thesis: scalable oversight for distributed renewable portfolios requires compliance to be represented as an event-sourced, cryptographically attributable record of policy-constrained decisions, paired with machine-checkable policy semantics that can be revised without rewriting history. The central idea is to shift from compliance as periodic reporting to compliance as a verifiable telemetry fabric that is continuously produced by operational systems themselves. Under this model, regulators do not merely receive summaries; they can verify that the summaries are consistent with an immutable stream of signed events, and they can reconstruct the causal chain when outcomes are challenged [5]. Grid operators can obtain low-latency assurance that a fleet respected a constraint at the moment it mattered, without needing full access to proprietary control code. Communities and environmental authorities can obtain bounded disclosures that confirm adherence to agreed operating windows or curtailment commitments, without exposing sensitive site-level telemetry beyond what is necessary for accountability.

The contribution is not a proposal to automate regulation wholesale. Policy choices remain normative, and enforcement remains institutional [6]. The contribution is a technical substrate that makes compliance claims verifiable across fragmented operational ecosystems. The substrate has three design goals that are rarely satisfied

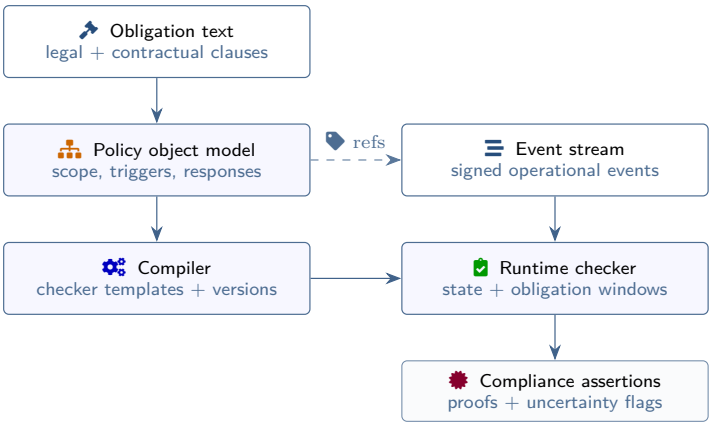

Figure 3: Policy compilation and checking: obligations are transformed into versioned policy objects and compiled into runtime checkers. Checkers consume signed event streams to emit attributable compliance assertions, including explicit handling of incomplete evidence.

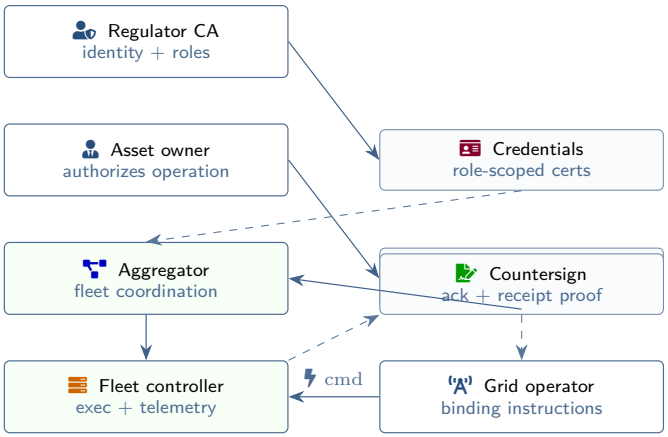

Figure 4: Delegation and accountability boundaries: roles are bound to identities via credentials, while operation authority is expressed through delegation tokens. Critical instruction workflows can be strengthened by bilateral receipts (countersigned acknowledgments) to reduce attribution disputes.

simultaneously. It must be scalable across thousands to millions of assets and events; it must be auditable and resistant to tampering or selective disclosure; and it must be deployable in settings where control is delegated to aggregators, consultants, and private intermediaries, and where data confidentiality is a real constraint.

The remainder of the paper introduces a system model and threat model for compliance telemetry in cyber-physical energy systems, then specifies the architecture of the proposed fabric, including its data-plane primitives and its event schemas [7]. It then describes how policy obligations can be compiled into runtime checkers that evaluate event streams, and how policy updates can be handled without compromising evidentiary continuity. It next addresses delegation, intermediary roles, accountability boundaries, and privacy-preserving disclosure strategies. It then proposes an evaluation methodology based on stress scenarios that couple grid contingencies with policy constraints and audit workloads [8]. The conclusion summarizes implications and limitations and outlines pathways for incremental adoption.

2 Compliance Telemetry as a Cyber-Physical Oversight Problem

Renewable portfolio operation is a cyber-physical process whose governance depends on both physical observables and institutional semantics. On the physical side, compliance-relevant signals include power injection, voltage and frequency excursions, ramp rates, inverter mode changes, protection trips, and availability of flexibility services such as reactive power or fast frequency response. On the cyber side, compliance-relevant artifacts include dispatch instructions, curtailment commands, constraint activation flags, controller configuration updates, and acknowledgments exchanged between operators and fleets [9]. On the institutional side, compliance-relevant obligations include interconnection agreements, market participation rules, environmental operating windows, noise or shadow-flicker constraints, and emergency protocols that can supersede normal operation. The key observation is that the decisive compliance evidence is often not a single measurement but the linkage between intent, instruction, action, and

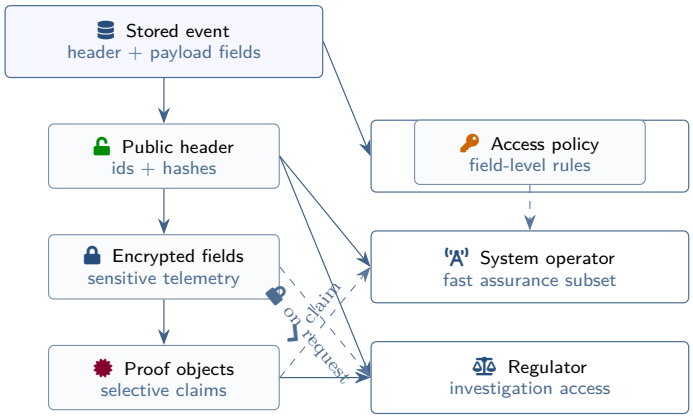

Figure 5: Bounded disclosure over the same evidence record: a public header enables integrity verification, encrypted fields protect sensitive telemetry, and proof objects support limited-purpose compliance claims. Access policy governs which stakeholders can decrypt which fields during routine assurance versus escalated investigations.

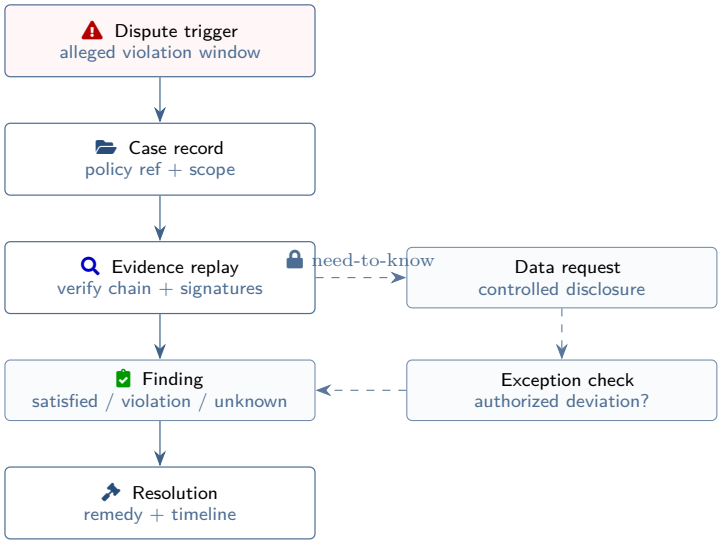

Figure 6: Dispute-resolution workflow over an immutable event record: a case is opened on a contested time window, evidence is replayed to reconstruct instruction–action–measurement provenance, and findings incorporate exception authorization and (when needed) logged data requests under controlled disclosure.

context, including who issued a command, what constraint justified it, and what the system observed at the time.

Legacy compliance approaches typically emphasize document-based artifacts because they are legible to human reviewers. Environmental and planning processes may require assessments, mitigation plans, and monitoring reports, while grid compliance may rely on periodic performance tests and incident reports [10]. These practices remain important, but at high penetration they suffer from two scaling failures. The first is temporal mismatch. Many violations and near-violations are transient and context-dependent, occurring within seconds or minutes of disturbances [11]. The second is attribution mismatch. Modern operations are distributed across many entities, and responsibility for an outcome is often contested, especially when automated systems react to signals from multiple authorities. When audits cannot reliably reconstruct attribution, institutions tend to respond by narrowing permissible operating modes or by demanding redundant oversight steps that slow operations.

A compliance telemetry fabric addresses these failures by elevating operational event provenance into a first-class governance object [12]. Event provenance includes who issued an instruction, which controller executed it, what data inputs were used, and what constraint semantics were applied. This provenance is not intended to expose proprietary algorithms; it is intended to expose the minimal verifiable structure that supports accountability. For example, a fleet may be obligated to curtail when a grid operator issues a binding constraint signal, and it may be obligated to avoid certain operating modes during sensitive ecological periods. The fabric provides a way to prove that curtailment occurred in response to a valid signal and within the allowed time window, and to prove that the fleet did not operate in a prohibited mode during the restricted period, while still allowing the fleet operator to keep internal forecasting models private [13].

The threat model for compliance telemetry is broader than adversarial hacking. It includes strategic behavior

Domain	Signals / artifacts	Compliance question
Physical	Power injection, voltage/frequency excursions, ramp rates, inverter mode changes, protection trips, flexibility availability	Were physical envelopes and power-quality constraints respected at relevant timescales?
Cyber	Dispatch instructions, curtailment commands, constraint flags, controller configuration updates, acknowledgments	Were digital instructions and configurations consistent with authorized control logic and received in time?
Institutional	Interconnection agreements, market rules, environmental operating windows, emergency protocols	Were actions justified by applicable contracts, permits, and exceptional procedures?
Provenance	Linked intent–instruction–action chains, actor identities, clock sources, asset identifiers	Can responsibility for specific outcomes be reconstructed across actors and platforms?

Table 1: Compliance-relevant observables across physical, cyber, institutional, and provenance dimensions.

by actors who may benefit from selective disclosure, ambiguous attribution, or delayed reporting. It includes unintentional error, such as misconfigured controllers, clock drift, or inconsistent identifiers across systems [14]. It includes institutional threats, such as conflicts of interest when monitoring is performed by parties aligned with developers or operators. It also includes political and governance volatility, where constraints can change due to policy updates or negotiated revisions, and where compliance claims must remain interpretable under the updated semantics.

Regulatory systems also face a legitimacy problem when constraints are contested, especially in contexts where renewable infrastructure generates local opposition. In wind governance, for example, environmental regulators can be pulled between climate objectives and ecological protection, and the stance of a regulator can evolve toward stronger opposition and heightened scrutiny under sustained stakeholder pressure, even when formal authority is limited [15]. This kind of dynamic affects compliance telemetry requirements because heightened scrutiny typically demands stronger evidence, tighter attribution, and clearer delineation of responsibility across agencies and private operators [16]. A telemetry fabric does not resolve the value conflict, but it reduces the ambiguity that often amplifies conflict by making operational behavior and decision justifications more reconstructable.

The final premise of this section is that compliance must be resilient to negotiation and change. Constraints are rarely stable for decades. They evolve with new technical standards, new ecological baselines, market redesigns, and shifts in public tolerance [17]. Oversight mechanisms that assume stability tend to break under updates because they cannot reconcile old evidence with new semantics. A compliance telemetry fabric therefore needs explicit versioning, interpretability guarantees, and the ability to replay event streams against updated policy checkers without rewriting what happened.

3 A Secure Event-Sourced Compliance Fabric

The proposed compliance telemetry fabric is an interoperability layer that sits between operational control systems and oversight institutions [18]. It does not replace dispatch or market platforms. Instead, it provides an evidence-grade stream of operational events and accompanying attestations that can be verified independently. The fabric is designed around the principle of event sourcing: the authoritative record is a time-ordered sequence of signed events. State is derived from events, rather than being reported as an ungrounded snapshot [19]. This design allows audits to replay history, to test alternative interpretations, and to detect inconsistencies between reported summaries and underlying events.

At the center of the fabric is a canonical event schema. Each event carries an event identifier, a timestamp with an explicit clock source, an actor identity, an asset or fleet identity, an event type, and an event payload. Event types include instruction issuance, instruction acknowledgment, instruction execution, measurement sampling, constraint activation, constraint deactivation, configuration change, and exception declaration [20]. The payload is typed, with fields appropriate to the event type. For example, an instruction execution event includes the requested

Aspect	Legacy compliance practice	Event-sourced telemetry fabric	Oversight effect
Temporal granularity	Periodic reports, after-the-fact incident summaries	Continuous, time-ordered streams of signed events	Captures transient and context-dependent behavior.
Attribution	Informal logs, mixed responsibilities, narrative reconstruction	Actor-signed events, explicit delegation tokens, linked instruction chains	Reduces ambiguity over "who did what, when, and under which authority".
Data disclosure	Broad raw-data requests, document-heavy audits	Selective field-level disclosure, aggregated proofs, role-specific views	Enables bounded transparency with targeted evidence.
Policy evolution	Static checklists, manual reinterpretation of old records	Versioned policy objects, replay against new checkers	Preserves evidentiary continuity under changing rules.
Exception handling	Ad hoc justifications after disturbances	Structured exception events with scope, authority, and justification references	Distinguishes violations from authorized deviations.

Table 2: Contrasting legacy compliance approaches with an event-sourced telemetry fabric.

setpoint, the achieved setpoint, the relevant control mode, and a pointer to the instruction issuance event. A measurement sampling event includes the measured quantity, units, sampling interval, and a calibration reference [21]. A configuration change event includes the identifier of the configuration artifact, its version, and a hash reference that can be used to retrieve the artifact through access-controlled channels if needed for an investigation.

Cryptographic attribution is achieved through signing. Each event is signed by the entity that generated it, using keys bound to an identity framework. Identity binding is not assumed to be a global public-key infrastructure; it can be implemented through regulator-issued certificates, utility-issued certificates, or sectoral trust frameworks [22]. The crucial property is that verifiers can check that events were produced by authorized entities and were not modified after the fact. The fabric also supports countersigning for critical workflows. For example, when a grid operator issues a constraint instruction, the operator signs the issuance event, and the fleet controller signs an acknowledgment event that references the issuance. This produces a bilateral record that reduces disputes about whether an instruction was received and when [23].

Tamper-evidence is strengthened through append-only logging. Events are grouped into batches that are chained by hash references. Each batch includes a batch header that summarizes included events and references the previous batch header, producing a verifiable chain [24]. The chain can be anchored periodically to an external timestamping service or institutional registry, but the design does not require a public blockchain. The goal is practical immutability: once an event is published to the fabric, removing or altering it becomes detectable to verifiers who have access to the chain headers.

The fabric separates storage from access. Oversight stakeholders do not necessarily gain access to all event payloads [25]. Instead, the fabric supports multiple disclosure levels. A regulator may be permitted to access full payloads for enforcement investigations, while a market monitor may access only market-relevant event subsets, and a community oversight body may access only aggregate compliance proofs. This separation is achieved through field-level encryption and selective disclosure policies. In the simplest deployment, events are stored in an access-controlled repository and verifiers obtain the subset they are authorized to view [26]. In more advanced deployments, events can be accompanied by disclosure tokens that allow certain fields to be revealed without revealing others, enabling bounded transparency.

A key design issue is how the fabric represents policy constraints. Rather than embedding policy text in events, the fabric uses constraint references [27]. A constraint reference is an identifier for a policy object defined elsewhere, such as an interconnection requirement, a market rule, or an environmental operating window. The event payload includes the constraint reference when an action is taken to satisfy or enforce a constraint. This is essential for interpretability because constraints can be revised. The fabric maintains a versioned registry of policy objects so

Event type	Description	Key payload elements
Instruction issuance	Grid operator or market platform sends a binding command to a fleet or asset	Issuer identity, target asset/fleet, setpoint or mode, constraint reference, validity window.
Instruction acknowledgment	Fleet or asset confirms reception and intent to execute	Recipient identity, reference to issuance event, timestamp/clock source, acceptance status.
Instruction execution	Controller applies a command in the field	Requested vs achieved setpoint, control mode, asset identity, linkage to issuance and acknowledgment events.
Measurement sampling	Telemetry observation of system state or behavior	Quantity and units, sampling interval, calibration reference, measurement context (e.g., pre/post-event).
Constraint activation / deactivation	A reliability, market, or environmental constraint becomes active or is cleared	Constraint identifier and version, activation trigger, affected scope, deactivation cause.
Configuration change	Update to controller parameters or operating logic	Configuration artifact ID, version, hash reference, actor identity, rationale code.
Exception declaration	Authorized deviation from normal policy (e.g., emergency, safety)	Exception type, declaring authority, scope and duration, justification reference.

Table 3: Canonical event types in the proposed compliance telemetry fabric.

that a verifier can interpret an event against the policy version that was in force at the time, and can also evaluate counterfactuals under updated versions [28].

The fabric is intentionally agnostic to the specific governance domain. It can represent grid reliability constraints, market compliance constraints, and environmental constraints using the same event mechanics. This matters because modern renewable governance is multi-actor and multi-domain, and constraints interact. Solar deployment governance, for instance, can involve ongoing negotiations over market design, land use, regulatory coordination, and stakeholder engagement, shaping both policy design and implementation outcomes over time [29]. When governance is negotiated, constraints may change in response to disputes or performance observations [30]. An event-sourced fabric supports this by keeping the operational record stable while allowing policy checkers to evolve.

Finally, the fabric incorporates exception handling as a formal mechanism rather than as an informal workaround. Exceptions include emergency operations, safety shutoffs, and force majeure conditions [31]. An exception event declares the exception type, the declaring authority, the scope, and the justification reference. Subsequent operational events can reference the exception, allowing auditors to distinguish between violations and authorized deviations. This reduces the ambiguity that often follows extreme events, where operators may claim necessity after the fact but cannot demonstrate what was known and authorized at the time.

4 Policy Compilation and Runtime Compliance Checking

A telemetry fabric is useful only if policy semantics can be evaluated against event streams in a reliable and administratively meaningful way [32]. Policy compilation is the workflow that translates legal, contractual, and negotiated obligations into machine-checkable checkers that can process events and produce compliance claims.

Policy component	Role in compliance semantics	Illustrative example
Scope	Defines which assets, fleets, or regions are covered	All utility-scale solar assets in a congestion-prone zone.
Validity window	Specifies temporal applicability of an obligation	Curtailment rule valid from summer peak season start until end-of-season.
Triggering condition	Describes when an obligation becomes active	Frequency deviation beyond threshold or activation of wildfire risk flag.
Response pattern	Defines required behavior and latency bounds	Acknowledgment within 2 seconds and setpoint achievement within 30 seconds.
Version and supersession	Tracks policy evolution and maintains interpretability of past events	Reactive power requirement updated from version 1.2 to 1.3 after a standard revision.
Checker assignment	Binds obligations to entities that implement runtime evaluation	Market monitor checker assesses dispatch compliance for a given fleet.

Table 4: Core components of machine-checkable policy objects.

The compilation problem is not to eliminate ambiguity entirely, but to identify which parts of an obligation can be checked mechanically, which parts require human judgment, and which parts require structured uncertainty declarations.

The proposed workflow begins with a policy object model that distinguishes obligations, permissions, and prohibitions. Each policy object includes a scope, such as which assets or fleets it applies to, a temporal validity window, a set of triggering conditions, and an expected response pattern that can be checked against events [33]. For example, a response pattern for a curtailment obligation might require that a valid instruction issuance event from an authorized grid entity be followed by an acknowledgment within a defined latency bound and an execution event that reaches an acceptable setpoint band. A response pattern for an environmental operating window might require that, during a restricted period, certain operating modes do not occur, or that curtailment is applied when a monitoring trigger is activated.

Runtime checkers are deployed as verifiers that subscribe to event streams and evaluate them against policy objects [34]. Checkers can be operated by regulators, by system operators, or by independent auditors. The architecture supports redundancy: multiple checkers can evaluate the same events and compare outputs, reducing dependence on a single institutional interpretation. Checker outputs are themselves events, signed by the checker, and appended to the fabric. This creates an auditable trail of compliance assessments over time, including changes when policy versions update [35].

Policy updates are handled through versioning and replay. When a policy object changes, a new version is published to the registry with an explicit supersession relationship. Checkers can then evaluate future events under the new version, while past events remain interpretable under the old version [36]. If an institution requires reassessment, checkers can replay historical event streams under the new version to estimate how compliance would have been judged under the updated semantics, without altering the original record. This capability is important when negotiated commitments are revised after disputes or new information, because it allows institutions to quantify the operational impact of policy changes and to manage transition periods transparently.

A practical obstacle to policy compilation is that regulated entities often seek approval pathways by framing their operations in persuasive narratives that emphasize benefits and downplay uncertainties. In innovation governance, work on the interaction between niche actors and regulators has argued that pitching to regulators can be used to address regulatory uncertainties, including by presenting compliance plans, stakeholder alignment claims, and financial projections as part of the approval-seeking process [37]. For compliance telemetry, the relevance is that policy compilation should not rely on narratives alone [38]. Instead, claims made during approval processes should be translated into explicit policy objects with checkable components and declared non-checkable components. The

Threat category	Example	Fabric-level mitigation
Strategic misreporting	Operator selectively omits curtailment instructions that were ignored	Signed event chains and anchoring make omissions or late insertions detectable.
Selective disclosure	Aggregator shares only favorable subsets of telemetry with auditors	Field-level encryption with role-based access policies; verifiers request complete event sets.
Configuration error	Misconfigured controller violates a ramp-rate constraint unintentionally	Configuration change events with versioning support root-cause analysis and rollback.
Time-base inconsistencies	Clock drift between fleets and operators complicates sequence reconstruction	Explicit clock-source metadata and cross-checks across independent event timelines.
Institutional conflicts	Monitoring performed by entities aligned with project developers	Credential metadata and countersigning requirements expose conflicts of interest.
Policy volatility	Sudden tightening of environmental limits mid-season	Versioned policy objects and replay allow assessing impacts without rewriting history.

Table 5: Threat model categories and corresponding mitigation mechanisms.

fabric then ensures that, where claims are checkable, they remain tied to observable events, and where claims are not checkable, the basis for judgment remains explicit.

Because this paper minimizes mathematical formalism, the checker semantics are described operationally. A checker maintains derived state from events, such as the current operating mode, the active set of constraints, and recent instruction histories [39]. When a new event arrives, the checker updates derived state and evaluates relevant policy triggers. If a trigger condition becomes true, the checker opens an obligation window during which it expects corresponding response events. If the responses occur within the window and satisfy the response pattern, the checker records satisfaction [40]. If responses do not occur, or if they occur with unacceptable parameters, the checker records a potential violation or an unresolved exception. Checker outputs can include confidence annotations when data is incomplete or when events are missing due to communication failures, making uncertainty visible rather than silently ignored.

The compilation workflow also supports hierarchical policies. A regulator may define high-level obligations, while a grid operator defines operationally specific constraints [41]. The fabric can represent this through policy references that form a dependency graph: a high-level obligation references a set of subordinate policy objects that operationalize it. This allows different institutions to own different policy layers while still enabling integrated checking. For example, an environmental authority can own restricted-period definitions, while a grid operator owns the operational control commands that implement curtailment, and the checker can verify that operational commands were consistent with environmental restrictions without requiring the environmental authority to operate grid control systems.

5 Delegation, Intermediaries, and Accountability Boundaries

Renewable portfolio governance is increasingly characterized by delegation [42]. Developers hire consultants to produce assessments, fleet operators outsource monitoring, aggregators operate assets on behalf of owners, and regulators sometimes rely on private entities for compliance monitoring or policy development support. Delegation can improve capacity and specialization, but it creates accountability gaps when evidence production and decision authority diverge. The compliance telemetry fabric is designed to make delegation legible by representing not only operational events but also authority relationships and delegation boundaries [43].

Artifact	Description	Produced by	Typical use
Credential object	Binds an identity to roles and qualifications	Regulator, system operator, or sectoral trust framework	Establishes who may issue instructions, monitor, or certify evidence.
Delegation token	Grants authority to act on behalf of another entity within a scope	Asset owner, regulator, or operator	Authorizes aggregators, consultants, or service providers.
Countersignature	Second party signs an event or batch for joint accountability	Independent auditor or system operator	Confirms that a measurement or instruction is jointly witnessed.
Exception declaration	Formal statement that normal rules are temporarily relaxed	Grid operator or competent authority	Documents emergency operations or safety-driven deviations.
Audit annotation	Structured human judgment attached to an event subset	Auditors, regulators, or committees	Records interpretations, findings, and rationales in dispute processes.

Table 6: Delegation- and accountability-related artifacts in the telemetry fabric.

Authority relationships are represented through credential objects and delegation tokens. A credential object binds an entity identity to roles, such as operator, aggregator, auditor, laboratory, or regulator. A delegation token is a signed artifact that states that one entity authorizes another to perform certain actions or to produce certain evidence, within a scope and time window. Events produced under delegation reference the delegation token, allowing verifiers to determine whether an entity acted within its authorized scope [44]. This is important when disputes arise about whether an intermediary had the right to issue an instruction, to certify a measurement, or to declare an exception.

Delegation is not only technical; it reshapes institutional roles. Environmental governance has been argued to be undergoing a structural shift in which regulators increasingly delegate responsibilities to private actors, expanding capacity while also raising concerns about transparency, accountability, and the independence of public oversight, particularly in compliance monitoring and policy development [45]. A telemetry fabric does not solve these concerns by itself, but it provides technical hooks to operationalize oversight requirements. For example, a regulator can require that certain event types be countersigned by an independent auditor, or that certain measurements be produced by accredited entities whose credentials are verifiable in the fabric [46]. The regulator can also require disclosure of funding relationships as metadata in credential objects, enabling audits to identify conflicts of interest systematically rather than ad hoc.

Accountability boundaries also require careful handling of proprietary control logic. Aggregators may treat forecasting models and dispatch optimization as trade secrets [47]. The fabric therefore focuses on verifiable external behavior and minimal internal assertions. It does not demand that operators reveal optimization code. Instead, it demands that operators produce signed events that record what instructions were received, what actions were taken, and what constraint references justified those actions. When deeper investigation is required, the fabric supports escalation pathways where authorized investigators can request access to configuration artifacts or control logs under controlled confidentiality conditions, and where the access request and response are themselves logged as events to ensure process accountability [48].

Privacy considerations extend beyond proprietary concerns to include sensitive environmental and community data. For instance, exact locations of sensitive habitats or protected species monitoring points may be restricted. The fabric supports privacy by allowing policy objects to reference protected zones without revealing full geometry to all stakeholders, and by allowing checkers to output compliance claims that confirm adherence without disclosing raw telemetry. This is achieved through layered disclosure policies and by separating constraint identifiers from constraint content [49]. In practice, an environmental authority can publish a policy object that includes restricted operational windows tied to a zone identifier, while the zone's detailed definition is accessible only to authorized

Stakeholder	Typical roles in the fabric	Event / field access	Primary assurance need
Regulator	Defines policy objects, approves monitoring regimes, conducts enforcement	Access to full events for targeted investigations; summary proofs for routine oversight	Confidence that obligations are met and violations are provable.
System operator	Issues constraints and dispatch instructions; manages reliability	Near real-time view of relevant instruction and execution events	Assurance that fleets respect reliability constraints when it matters.
Aggregator / fleet operator	Orchestrates distributed assets and interfaces with markets	Full internal telemetry plus regulator-facing event subsets	Ability to demonstrate compliance without exposing proprietary logic.
Community / environmental authority	Monitors local impacts and ecological constraints	Access to bounded proofs about operating windows and curtailment patterns	Evidence that agreed environmental or community limits are respected.
Independent auditor	Provides third-party verification of claims and processes	Read access to extensive event histories and credential metadata	Trustworthy reconstruction of provenance and detection of inconsistencies.

Table 7: Representative stakeholders and their interaction with compliance telemetry.

parties. Operators can then prove that their operational events did not violate the policy without being able to exfiltrate the sensitive zone definition.

Dispute resolution is built into the accountability design [50]. When a stakeholder alleges noncompliance, the dispute is registered as a dispute event that references the contested policy object, the relevant time window, and the claimant identity. The resolution process consists of replaying the relevant event segment, verifying signatures and chain integrity, and applying the relevant checker semantics. If an exception was declared, the dispute process verifies whether the exception declaration was authorized and whether subsequent actions remained within exception scope. If evidence is incomplete, the dispute process can trigger a data request workflow with logged requests and responses, reducing the opportunity for selective disclosure [51]. Importantly, the fabric does not assume that disputes can always be resolved technically; it assumes that technical reconstruction can narrow the disagreement to the remaining normative or interpretive issues.

Finally, the fabric is designed to coexist with human oversight rather than to eliminate it. Many obligations, especially those involving community acceptance or ecological impact, include qualitative judgments. The fabric supports these by allowing structured annotations that record judgments, rationales, and decision authorities as signed events [52]. These annotations are auditable, time-stamped, and attributable, making human judgment visible and reviewable without trying to reduce it to mechanistic rules.

6 Evaluation Methodology for Scalable Oversight

Evaluating a compliance telemetry fabric requires metrics that reflect both technical and institutional objectives. The primary technical objective is verifiability under realistic operational conditions, including high event volumes, intermittent connectivity, and policy updates [53]. The primary institutional objective is auditability with bounded disclosure, enabling oversight without forcing universal transparency. This section proposes an evaluation methodology centered on stress scenarios, audit workload measurements, and robustness tests under delegation and policy change.

Stress scenarios are constructed by combining grid contingencies with policy constraints. One class of scenarios includes frequency events, voltage excursions, congestion constraints, and emergency curtailments [54]. The eval-

Scenario class	Evaluation focus	Representative questions
Grid contingency stress	Frequency events, voltage excursions, congestion and emergency curtailment	Can instruction, acknowledgment, execution, and measurement events support reconstruction and low-latency assurance?
Policy volatility	Mid-stream changes in technical or environmental constraints	Do versioned policies maintain interpretability and support replay without rewriting evidence?
Delegation and intermediaries	Aggregators, consultants, and monitoring providers	Are authority chains and countersigning sufficient to localize responsibility in disputes?
Audit workload	Practical use by auditors and committees	Does structured telemetry reduce time to a defensible answer compared to document-centric audits?
Fault and adversary robustness	Benign faults and strategic manipulation attempts	How reliably are omissions, late events, or clock drift detected and characterized?
Hierarchical aggregation	Multi-layer disclosure strategies	What fidelity and audit power are preserved when only aggregated regulator-facing streams are shared?

Table 8: Proposed evaluation scenario classes for the compliance telemetry fabric.

uation measures whether event streams capture instruction issuance, acknowledgment, execution, and resulting measurements with sufficient integrity to support later reconstruction. It also measures whether the fabric can provide low-latency assurance signals to system operators, such as a signed statement that a fleet complied with a curtailment within a defined latency window, without requiring the operator to ingest full raw telemetry.

A second class of scenarios focuses on policy volatility. Constraints are revised mid-operation due to updated standards, negotiated compromises, or newly identified risks [55]. The evaluation measures whether policy versioning is handled cleanly, whether checkers can switch to new versions without losing interpretability of past events, and whether replay-based reassessments can be performed without rewriting or invalidating prior evidence. A critical property is continuity: institutions should be able to explain what was required at the time and what changed, using the same underlying event record.

A third class of scenarios focuses on delegation and intermediary behavior [56]. Aggregators act on behalf of asset owners, and monitoring functions are performed by third parties. The evaluation measures whether delegation tokens and credentials are sufficient to reconstruct authority chains, and whether countersigning requirements can detect or deter unilateral manipulation. It also measures how disputes propagate when responsibilities overlap, such as when a grid operator claims noncompliance but an aggregator claims a conflicting instruction stream or communication failure.

Institutional effectiveness is evaluated through audit-time experiments [57]. Auditors are asked to answer structured questions, such as whether a specific obligation was satisfied during a time window, and to provide the provenance chain supporting the answer. The evaluation measures time to first defensible answer, completeness of provenance reconstruction, and sensitivity to missing data. This is contrasted with document-centric audits, which often involve manual retrieval and interpretation of heterogeneous logs.

The evaluation also considers the gap between procedural compliance and substantive decision support [58]. In regulatory settings where third-party intermediaries produce assessments, evidence can satisfy formal requirements

Design goal	Supporting mechanisms	Resulting capability
Scalability across fleets	Event sourcing with append-only batching, hierarchical aggregation of streams	Handles high event volumes while enabling tiered, fleet-level summaries.
Auditability and tamper-resistance	Signed events, hash-chained batches, external anchoring	Makes post hoc alteration or selective deletion detectable to verifiers.
Delegation-aware accountability	Credential objects, delegation tokens, countersignatures	Clarifies authority boundaries and supports attribution across intermediaries.
Policy evolution resilience	Versioned policy objects, supersession links, replayable checkers	Allows obligations to change without invalidating historical evidence.
Bounded disclosure and privacy	Field-level encryption, role-based access, constraint references	Enables oversight while protecting proprietary and sensitive environmental data.
Dispute-resolution transparency	Dispute events, exception declarations, structured audit annotations	Supports systematic reconstruction of contested outcomes and remaining value conflicts.

Table 9: Key design goals of the fabric and associated technical mechanisms.

while still being insufficiently trusted for confident decision-making, prompting decision-makers to seek external validation and undermining substantive effectiveness. Analysis of wind-project deliberations has identified this pattern by distinguishing high procedural effectiveness from lower substantive effectiveness when committees do not fully rely on intermediary-produced assessments [59]. For a telemetry fabric, the implication is that evaluation should not only count whether required events exist, but also test whether stakeholders actually find the fabric outputs credible enough to reduce redundant validation. Accordingly, evaluation includes surveys or structured interviews of simulated stakeholders, focusing on whether provenance clarity reduces the perceived need for external corroboration, and on what additional safeguards are required when intermediaries are involved [60].

Robustness is assessed under adversarial and non-adversarial faults. Adversarial tests include attempted event omission, delayed publication, and conflicting countersignatures. Non-adversarial tests include clock drift, identifier mismatches, and intermittent network partitions. The evaluation measures detectability of tampering, the rate of false violation flags under benign faults, and the ability to reconcile partitions without losing integrity guarantees [61]. Because this paper avoids heavy formalism, robustness is reported through empirical properties such as detection rates and reconstruction success under controlled perturbations, rather than through analytic bounds.

Finally, scalability is measured in terms of throughput, storage overhead, and checker computation requirements. The fabric is designed to degrade gracefully by supporting hierarchical aggregation. For instance, a fleet can publish high-frequency internal events privately while publishing a lower-frequency, regulator-facing subset that still supports verifiable summaries, with cryptographic linkage between the public subset and the private superset [62]. Scalability evaluation therefore measures not only raw event handling but also the fidelity loss and audit impact when using hierarchical disclosure strategies.

7 Conclusion

Distributed renewable portfolios increasingly operate through software-defined control and delegated market participation, creating a governance environment where compliance depends on rapid, attributable, and verifiable records of operational behavior. This paper proposed a regulatory-grade compliance telemetry fabric that represents compliance as an event-sourced stream of signed operational events linked to versioned policy objects and evaluated by runtime checkers [63]. The design aims to make accountability legible across aggregators, intermediaries, and regulators while supporting bounded disclosure for confidentiality and sensitive environmental information. It also aims to reduce disputes by enabling replay-based reconstruction of contested outcomes under the policy semantics

that were in force at the time, and by formalizing exceptions and delegation boundaries as auditable artifacts.

The approach is not a substitute for policy judgment or institutional authority. Its role is to provide a technical substrate that reduces ambiguity, improves audit efficiency, and supports adaptive policy updates without erasing evidentiary continuity [64]. Limitations remain, including the organizational effort required to standardize identifiers and credentials, the risk of overburdening smaller operators if event requirements are not tiered, and the continuing need for human judgment for qualitative obligations. Nonetheless, the fabric can be adopted incrementally, beginning with high-stakes event types such as curtailment commands and configuration changes, and expanding as institutions build capacity.

Future work can extend the fabric toward richer privacy-preserving disclosures, broader interoperability across non-electric domains such as land-use monitoring, and governance processes that formally integrate negotiated revisions into policy object versioning while preserving legitimacy and contestability. In the broader context of high-penetration renewable governance, verifiable compliance telemetry can serve as a practical bridge between machine-speed operation and institution-speed oversight [65].

References

[1] G. J. G. Sanchez, "In the name of energy sovereignty," *SSRN Electronic Journal*, Jan. 1, 2022. DOI: 10.2139/ssrn.4037683

[2] M. J. Bambawale and B. K. Sovacool, "Energy security: Insights from a ten country comparison," *Energy & Environment*, vol. 23, no. 4, pp. 559–586, Jun. 1, 2012. DOI: 10.1260/0958-305x.23.4.559

[3] A. Eitan, "Climate change adaptation through renewable energy: The cases of australia, canada, and the united kingdom," *Environments*, vol. 11, no. 9, p. 199, 2024.

[4] T. G. Iliopoulos, "Price support schemes in the service of the eu's low-carbon energy transition," in Edward Elgar Publishing, Jul. 28, 2020. DOI: 10.4337/9781839109911.00011

[5] A. Yimere and E. Assefa, "Assessment of the water-energy nexus under future climate change in the nile river basin," *Climate*, vol. 9, no. 5, pp. 84–, May 18, 2021. DOI: 10.3390/cli9050084

[6] K. Madias and A. Szymkowiak, "Residential sustainable water usage and water management: Systematic review and future research," *Water*, vol. 14, no. 7, pp. 1027–1027, Mar. 24, 2022. DOI: 10.3390/w14071027

[7] E. Karim et al., "Energy revolution for our common future: An evaluation of the emerging international renewable energy law," *Energies*, vol. 11, no. 7, pp. 1769–, Jul. 5, 2018. DOI: 10.3390/en11071769

[8] A. Prontera, *The New Politics of Energy Security in the European Union and Beyond*. Routledge, May 18, 2017. DOI: 10.4324/9781315555126

[9] H. Qudrat-Ullah, "The q-npt: Redefining nuclear energy governance for sustainability," *Energies*, vol. 18, no. 11, pp. 2784–2784, May 27, 2025. DOI: 10.3390/en18112784

[10] M. Peterson, *Unsustainable development: The impact of power sector reform on policy regimes in sub-saharan africa*, Feb. 23, 2022. DOI: 10.21203/rs.3.rs-1304310/v1

[11] A. Asthana, "What determines access to subsidised food by the rural poor?: Evidence from india," *International Development Planning Review*, vol. 31, no. 3, pp. 263–279, 2009.

[12] G. B. R. Lambais and G. Gonçalves, "Innovation and global to local energy governance," in Palgrave Macmillan, Aug. 19, 2013. DOI: 10.1057/9781137006127.0018

[13] R. Leal-Arcas, A. Filis, and E. S. A. Gosh, "Energy and law of the sea: Eastern mediterranean basin scenarios," in Edward Elgar Publishing, Nov. 28, 2014. DOI: 10.4337/9781784711504.00013

[14] A. Schapper, "Book review: Climate and energy governance for the uk low carbon transition: The climate change act 2008," *Environmental Law Review*, vol. 22, no. 2, pp. 159–161, Jul. 2, 2020. DOI: 10.1177/1461452920932685

[15] A. Eitan, "Navigating sustainability trade-offs in wind energy governance: The role of environmental regulators," *Energy Policy*, vol. 203, p. 114 645, 2025.

[16] S. Low, L. Fritz, C. M. Baum, and B. K. Sovacool, "Public perceptions on carbon removal from focus groups in 22 countries.," *Nature communications*, vol. 15, no. 1, pp. 3453–, Apr. 24, 2024. DOI: 10.1038/s41467-024-47853-w

[17] R. Wyss, S. Mühlemeier, and C. R. Binder, "An indicator-based approach for analysing the resilience of transitions for energy regions. part ii: Empirical application to the case of weiz-gleisdorf, austria," *Energies*, vol. 11, no. 9, pp. 2263–, Aug. 28, 2018. DOI: 10.3390/en11092263

[18] A. Ambole, K. Koranteng, P. Njoroge, and D. L. Luhangala, "A review of energy communities in sub-saharan africa as a transition pathway to energy democracy," *Sustainability*, vol. 13, no. 4, pp. 2128–, Feb. 17, 2021. DOI: 10.3390/su13042128

[19] P. Drysdale, A. Triggs, and J. Wang, "China's new role in the international financial architecture," *Asian Economic Policy Review*, vol. 12, no. 2, pp. 258–277, Jul. 5, 2017. DOI: 10.1111/aepr.12182

[20] M. Kumar, "Reclaiming spaces of energy consumption through rethinking approaches to rural electrification in india," *International Journal of Environmental Sciences & Natural Resources*, vol. 25, no. 4, pp. 154–156, Aug. 31, 2020. DOI: 10.19080/ijesnr.2020.26.556170

[21] A. Urquiza, C. Amigo, M. Billi, and P. Espinosa, "Participatory energy transitions as boundary objects: The case of chile's energía2050," *Frontiers in Energy Research*, vol. 6, Dec. 6, 2018. DOI: 10.3389/fenrg.2018.00134

[22] B. Patil, "Innovations for sustainability: A case of mainstreaming energy access in rural india," *Asian Journal of Innovation and Policy*, vol. 4, no. 2, pp. 154–177, Aug. 31, 2015. DOI: 10.7545/ajip.2015.4.2.154

[23] A. Silvast, M. Jalas, and J. Rinkinen, "Law and time - energy governance, risk and temporality," in Routledge, Sep. 21, 2018, pp. 212–228. DOI: 10.4324/9781315167695-12

[24] H. L. Heubaum, "Studying governance integration," in Routledge, Dec. 13, 2021, pp. 21–47. DOI: 10.4324/9781315661339-2

[25] P. Andrews-Speed and X. Shi, "What role can the g20 play in global energy governance? implications for china's presidency," *Global Policy*, vol. 7, no. 2, pp. 198–206, Dec. 12, 2015. DOI: 10.1111/1758-5899.12288

[26] B. Saerbeck, K. Jörgensen, and M. Jänicke, "Multi-level climate governance: The global system and selected sub-systems," *Environmental Policy and Governance*, vol. 27, no. 2, pp. 105–107, Apr. 18, 2017. DOI: 10.1002/eet.1746

[27] X. Lu, E. Zhu, L. Campbell, M. Hafner, M. Noussan, and P. P. Raimondi, "Comparison between china, the eu and the us's climate and energy governance: How policies are made and implemented at different levels," *SSRN Electronic Journal*, Jan. 1, 2021. DOI: 10.2139/ssrn.4017427

[28] A. Orsini and C. Godet, "Food security and biofuels regulations: The emulsifying effect of international regime complexes," *Journal of Contemporary European Research*, vol. 14, no. 1, pp. 4–22, Mar. 7, 2018. DOI: 10.30950/jcer.v14i1.872

[29] A. Eitan, "Negotiating the energy transition: Governance trade-offs in solar deployment," *Energy Strategy Reviews*, vol. 61, p. 101 854, 2025.

[30] N. Chaban and J. Bain, "Handbook of energy governance in europe - sustainable europe: Narrative potential in the eu's political communication," in Springer International Publishing, Mar. 30, 2021, pp. 1–16. DOI: 10.1007/978-3-319-73526-9_52-1

[31] N. Gunningham, "Confronting the challenge of energy governance," *Transnational Environmental Law*, vol. 1, no. 1, pp. 119–135, Feb. 21, 2012. DOI: 10.1017/s2047102511000124

[32] D. Bjelić, D. N. Markić, D. Prokić, B. N. Malinović, and A. A. Panić, ""waste to energy" as a driver towards a sustainable and circular energy future for the balkan countries," *Energy, Sustainability and Society*, vol. 14, no. 1, Jan. 2, 2024. DOI: 10.1186/s13705-023-00435-y

[33] J. Copley and M. E. Giraudo, "Depoliticizing space: : The politics of governing global finance," *Environment and Planning C: Politics and Space*, vol. 37, no. 3, pp. 442–460, Jul. 4, 2018. DOI: 10.1177/2399654418786249

[34] Y. Ding, W. Qu, S. Niu, M. Liang, W. Qiang, and Z. Hong, "Factors influencing the spatial difference in household energy consumption in china," *Sustainability*, vol. 8, no. 12, pp. 1285–, Dec. 9, 2016. DOI: 10.3390/su8121285

[35] B. Hofmann, D. Kolcava, and P. Thaler, "The role of switzerland in european electricity governance," in Springer International Publishing, Nov. 27, 2021, pp. 67–92. DOI: 10.1007/978-3-030-80787-0_4

[36] E. Contipelli, "Multi-level climate governance: Polycentricity and local innovation," *Revista Catalana de Dret Ambiental*, vol. 9, no. 2, pp. 2–, Dec. 27, 2018. DOI: 10.17345/rcda2149

[37] A. Eitan and I. Fischhendler, "Shaping niche innovations in energy transitions: The role of pitching to regulators," *Energy Research & Social Science*, vol. 126, p. 104 170, 2025.

[38] M. J. Burke, "Shared yet contested: Energy democracy counter-narratives," *Frontiers in Communication*, vol. 3, Jun. 21, 2018. DOI: 10.3389/fcomm.2018.00022

[39] S. Minas, "Eu climate law sans frontières: The extension of the 2030 framework to the energy community contracting parties," *Review of European, Comparative & International Environmental Law*, vol. 29, no. 2, pp. 177–190, Jun. 30, 2020. DOI: 10.1111/reel.12352

[40] M. Knodt and N. Piefer, "South africa-eu energy governance: Tales of path dependency, regional power, and decarbonization," in Routledge, Mar. 3, 2016, pp. 227–246. DOI: 10.4324/9781315571164-23

[41] M. Sheraz, X. Deyi, M. Z. Mumtaz, and A. Ullah, *The dynamic nexus between financial development, renewable energy and carbon emission: Role of globalization and institutional quality across bri countries*, Jul. 23, 2021. DOI: 10.21203/rs.3.rs-669288/v1

[42] M. Knodt, "Multilevel coordination in eu energy policy: A new type of "harder" soft governance?" In Springer International Publishing, Feb. 2, 2019, pp. 173–191. DOI: 10.1007/978-3-030-05511-0_10

[43] T. G. Reames, D. M. Daley, and J. C. Pierce, "Exploring the nexus of energy burden, social capital, and environmental quality in shaping health in us counties.," *International journal of environmental research and public health*, vol. 18, no. 2, pp. 620–, Jan. 13, 2021. DOI: 10.3390/ijerph18020620

[44] D. Chen, P. Mollet, and B. Efird, *Energy governance in china: The structures and processes of government decision-making*, May 15, 2019. DOI: 10.30573/ks--2019-dp56

[45] A. Eitan, "Privatizing environmental governance: The evolving relationship between regulators and private entities," *Journal of Environmental Policy & Planning*, pp. 1–27, 2025.

[46] N. Pirrone, S. Cinnirella, S. Nativi, F. Sprovieri, and I. M. Hedgecock, "Era-planet the european network for observing our changing planet," *ISPRS - International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. XLI-B8, pp. 1349–1355, Jun. 24, 2016. DOI: 10.5194/isprsarchives-xli-b8-1349-2016

[47] Z. He, Z. Chong, Y. Yang, Y. Zhou, and Y. Liu, "Evolutionary investment network and the emerging energy power in central asia: From the perspective of cross-border mergers and acquisitions," *Journal of Geographical Sciences*, vol. 30, no. 11, pp. 1849–1870, Dec. 23, 2020. DOI: 10.1007/s11442-020-1815-7

[48] V. Dobravec, N. Matak, C. Sakulin, and G. Krajačić, "Multilevel governance energy planning and policy: A view on local energy initiatives," *Energy, Sustainability and Society*, vol. 11, no. 1, pp. 1–17, Jan. 6, 2021. DOI: 10.1186/s13705-020-00277-y

[49] M. A. Azni, R. M. Khalid, U. A. Hasran, and S. K. Kamarudin, "Review of the effects of fossil fuels and the need for a hydrogen fuel cell policy in malaysia," *Sustainability*, vol. 15, no. 5, pp. 4033–4033, Feb. 22, 2023. DOI: 10.3390/su15054033

[50] H. Byrd and S. Matthewman, "Renewable energy in new zealand: The reluctance for resilience," in United States: Springer London, Nov. 30, 2013, pp. 137–153. DOI: 10.1007/978-1-4471-5595-9_8

[51] "Copyright," in Edward Elgar Publishing, May 27, 2016. DOI: 10.4337/9781785368462.00002

[52] *2020 Projections of Climate Finance Towards the USD 100 Billion Goal*. OECD, Oct. 24, 2016. DOI: 10.1787/9789264274204-en

[53] K. M. J. Iqbal, N. Akhtar, M. O. Khan, and M. I. Khan, "Mix-method modelling of actors' capacity for environmental sustainability and climate compatible development in energy sector.," *Environmental science and pollution research international*, vol. 29, no. 33, pp. 50 632–50 646, Mar. 2, 2022. DOI: 10.1007/s11356-022-19399-1

[54] "Introduction," in Palgrave Macmillan, Oct. 25, 2013. DOI: 10.1057/9781137320735.0007

[55] M. Kobi, "Chongqing (people's republic of china): The electrification of the urban fabric," in De Gruyter, Jun. 7, 2022, pp. 97–118. DOI: 10.1515/9783035624243-006

[56] N. Chaban and M. Knodt, "International structures and external perceptions: Projecting and receiving the eu as a global energy governance actor in the eyes of emerging powers (brazil, india, china)," in Palgrave Macmillan UK, Sep. 28, 2016, pp. 201–223. DOI: 10.1057/978-1-137-54758-3_10

[57] M. Pellegrino and M. Rupeka, "Intertwined renewable and digital transitions: A study on south australia's hybridized electricity system," *Sustainability Science*, Apr. 12, 2025. DOI: 10.1007/s11625-025-01647-1

[58] S. A. Abdulrahman, "Energy, governance and security in thailand and myanmar (burma): A critical approach to environmental politics in the south," *International Journal of Environmental Studies*, vol. 76, no. 1, pp. 168–178, Sep. 10, 2018. DOI: 10.1080/00207233.2018.1517967

[59] A. Eitan and D. Levi-Faur, "Environmental impact assessments as a mechanism of regulatory intermediation: The case of israeli wind energy," *Policy and Society*, vol. 44, no. 4, pp. 510–534, 2025.

[60] P. E. Carvajal, A. Miketa, N. Goussous, and P. Fulcheri, "Best practice in government use and development of long-term energy transition scenarios," *Energies*, vol. 15, no. 6, pp. 2180–2180, Mar. 16, 2022. DOI: 10.3390/en15062180

[61] J.-A. van Wyk, "Crouching tigers, leaping lions? developmental leadership lesson for south africa from china and malaysia," *African East-Asian Affairs*, vol. 0, no. 1-2, Nov. 22, 2016. DOI: 10.7552/0-1-2-168

[62] A. N. Asthana, "Decentralisation and supply efficiency of rws in india," 2003.

[63] R. Leal-Arcas and S. M. Minas, "Mapping the international and european governance of renewable energy," *Yearbook of European Law*, vol. 35, no. 1, pp. 621–666, Oct. 27, 2016. DOI: 10.1093/yel/yew022

[64] A. Mosavi, M. Salimi, S. Ardabili, T. Rabczuk, S. Shamshirband, and A. R. Várkonyi-Kóczy, "State of the art of machine learning models in energy systems, a systematic review," *Energies*, vol. 12, no. 7, pp. 1301–, Apr. 4, 2019. DOI: 10.3390/en12071301

[65] S. R. Whyte, E. Yates-Doerr, and C. Labuski, *The Ethnographic Case*. Mattering Press, Nov. 1, 2023. DOI: 10.28938/9781912729340