Cognitive-Responsive Risk Communication and Representation for Resilient Energy Supply Chains

White Paper — Phase 1 Report

Muntadher Sallal[1], Gregory Epiphaniou[2], Omar Hamza[3], Yang Lu[4], and Edward Chuah[5]

[1] Bournemouth University
[2] University of Warwick
[3] University of Derby
[4] Loughborough University
[5] University of Aberdeen

April 2026

Project funded by SPRITE+ through EPSRC/UKRI
Grant reference: EP/W020408/1

Table of Contents

Acknowledgements

This work was funded by SPRITE+ through the Engineering and Physical Sciences Research Council (EPSRC), grant reference EP/W020408/1, as part of the project “ResChain: Cognitive-Responsive Risk Communication and Representation for Resilient Energy Supply Chains”.

Reuse of material

The ResChain materials, including figures, tables, workshop outputs, and the Tension Map framework, may be cited or reused for academic, policy, educational, and other non-commercial purposes, provided that appropriate acknowledgement is given. Users should cite this white paper and credit the ResChain project, SPRITE+, and EPSRC/UKRI funding support.

Disclaimer

The views expressed in this white paper are those of the authors and do not necessarily reflect the views of SPRITE+, EPSRC, UKRI, Bournemouth University, or the partner institutions.

The information in this white paper is provided for academic, policy, and general information purposes. It should not be interpreted as legal, regulatory, cybersecurity, engineering, or commercial advice.

Executive Summary

Modern energy systems are increasingly complex, digitalised, and interdependent. They connect critical infrastructure, operational technology, digital control systems, commercial actors, regulators, vendors, and end users. A disruption in one part of this system can propagate across the energy supply chain, affecting continuity of supply, safety, compliance, cost, and public confidence.

Current risk assessment methods are still largely component driven. They focus on assets, threats, and technical vulnerabilities. This remains necessary, but it is not sufficient for complex energy systems. Many risks emerge from the way stakeholders interpret, prioritise, and respond to threats. Different organisations may share the same infrastructure while holding different interests, concerns, duties, and incentives. These differences can create misalignment during both routine risk planning and crisis response.

The research question addressed in Phase 1 of ResChain is therefore:

> *How can we better capture, assess, represent, and communicate diverse stakeholder interests and concerns relating to security and resilience objectives within the energy supply chain?*

To address this question, Phase 1 was organised around four activities: scoping and stakeholder mapping; stakeholder engagement and data collection; analysis of stakeholder tensions and system-level dependencies; and development of recommendations for future research and practice. These activities are summarised in Figure 1.

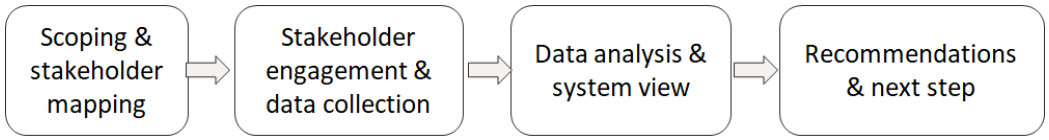

Figure 1: The four activities in ResChain – Phase 1.

The main contribution of Phase 1 is the **Tension Map framework**. This framework represents stakeholder misalignment as a measurable risk factor. It captures differences in stakeholder positions, confidence, and perceived importance across key risk domains, such as cybersecurity, operational continuity, compliance, cost, resilience, transparency, confidentiality, and availability. These tensions are then mapped against stakeholder dependencies to identify latent vulnerabilities that may increase the likelihood or impact of disruption.

Two impact workshops were conducted with participants from the energy and cybersecurity sectors, including energy operators, policy analysts, governance, risk and compliance specialists, SCADA and CPS engineers, cybersecurity researchers, data engineers, digital consultants, asset owners, contractors, vendors, and retailers. The workshops examined stakeholder priorities, risk perception gaps, interdependencies, and responses to a time-pressured energy disruption scenario.

The findings show that compliance, cost, resilience, confidentiality, availability, operational continuity, and transparency were recurring risk domains across stakeholder groups. Compliance was the most widely shared priority, followed by cost and resilience. However, shared priorities did not always imply aligned responses. Several stakeholder pairs showed strong dependencies but different interpretations of what should be prioritised during disruption.

The scenario exercise showed that most groups prioritised restoring control and maintaining supply before establishing root cause. Technical groups tended to emphasise system stabilisation, manual control, and restricted access. Governance and commercial groups placed greater emphasis on compliance, alternative supply, and continuity obligations. This divergence is important because

individually rational actions can become collectively inconsistent when stakeholders act without shared situational awareness or agreed authority.

Vendor-managed remote monitoring emerged as a critical dependency. Participants identified uncertainty around vendor visibility, access rights, authority, and incident responsibilities. This suggests that vendor access is not only a technical or procurement issue; it is a systemic governance risk. During a cyber-physical disruption, the same vendor access used to investigate an incident may also become a point of risk, delay, or disagreement.

Phase 1 also found that stakeholder tensions can be translated into operational vulnerabilities. Examples include delayed patching when cybersecurity conflicts with operational continuity, underinvestment in redundancy when cost conflicts with resilience, and reduced information sharing when transparency conflicts with confidentiality. These vulnerabilities are socio-technical: they arise from interactions between people, processes, technology, and governance arrangements.

The report concludes that energy supply chain risk assessment should move beyond purely technical models. Stakeholder interests, concerns, dependencies, and decision rights should be treated as part of the risk landscape. Tension should be considered a measurable indicator of latent vulnerability, especially where stakeholders share critical assets or depend on each other during disruption.

The next phase of ResChain will refine data-collection methods, pilot case studies that compare calculated tension scores with real or historical incidents, and visualisation techniques will be refined through user testing to ensure clarity and consistency in interpretation. Future work will also examine how tension scores can be integrated into existing risk assessment workflows and used to support more dynamic, continuous, and stakeholder-aware risk management.

1. Introduction

1.1 Background

Energy networks are a critical large-scale infrastructure essential to the functioning of societies and the operation of key economic activities. Over the past decade, energy has played a central role in development plans across all sectors, placing significant demands on the infrastructure that produces, generates, and supplies it. This growing demand places substantial pressure on energy systems, increasing their complexity to unprecedented levels and giving rise to distributed, interdependent supply chains comprising diverse stakeholders with differing socio-technical objectives and business strategies.

The complexity of the energy supply chain directly affects one of the three core objectives of the energy trilemma: security. The energy trilemma comprises ensuring the reliability and security of energy supplies (Security), minimising the cost of energy for consumers (Affordability), and reducing greenhouse gas emissions (Sustainability) [1]. Stakeholders including oil, gas, and renewable energy producers; energy suppliers and generators; and end users, interact through social networks governed by unstable institutional and political structures, each with different objectives. The costs and benefits of low-carbon technologies and energy efficiency measures are uncertain [2]. Robust and successful risk assessment, therefore, requires a comprehensive framework that accounts for the diversity and interdependencies among multiple stakeholders.

Risks in the energy supply chain span operational risks (associated with day-to-day supply chain management) and disruption risks (associated with natural or human-made damage such as

flooding, conflicts [4], or cyberattacks [5]). Geopolitical tensions, economic uncertainty, vulnerabilities in digital systems, and inadequate enforcement of governance regulations cause disruptions. Urciuoli et al. [3] found that piracy at sea, wars, and terrorism are among the most concerning security threats to oil and gas supply chains. Cui et al. [4] showed that the Russia–Ukraine war had a significant macroeconomic impact on European economies and led to a projected 1% reduction in global energy consumption. Hammi et al. [5] highlighted that distributed denial-of-service attacks and malware can severely affect multiple links in the digital supply chain. Colon et al. [6] argued for a top-down governance approach to reduce systemic risks arising from decisions made by individual firms.

Current risk assessment frameworks and methods fail to capture the full diversity and complexity of energy supply chains. Component-driven risk assessment (CD-RA) methods focus on system components such as hardware, software, and services, but do not capture interdependencies among components [7].

1.2 The Problem

Stakeholders in energy supply chains including oil, gas, and renewable energy producers; energy suppliers and generators; end users; and regulatory bodies, have different goals which lead to misaligned priorities. These misalignments arise from competing objectives, the lack of a shared vision, and poor communication. Identifying critical vulnerabilities engendered by these misalignments could significantly improve energy supply chain resilience.

Risk registers are widely used to identify, assess, and track potential risks. However, contemporary risk registers fail to capture hidden vulnerabilities arising from stakeholder misalignment. Holm et al. [9] showed that transitioning from fossil fuels to weather-dependent energy sources introduces new vulnerabilities, and that climatic and non-climatic factors have contributed to rising energy prices. Xexakis et al. [8] showed that model-based electricity supply scenarios in Switzerland relied heavily on fossil fuels and net imports, whereas both informed citizens and energy experts preferred domestically generated renewable energy, illustrating the gap between technical projections and stakeholder preferences.

2. ResChain Project Methodology

This chapter presents the tension mapping framework (Section 2.1), its formal extension from tensions to vulnerabilities and adjusted likelihood (Section 2.2), and the design of the ResChain impact workshops (Section 2.3).

2.1 Tension Mapping Framework

Conventional risk assessment (RA) methodologies, including MAGERIT, are grounded in asset–threat–vulnerability paradigms that prioritise technical system components. While effective for structured environments, these approaches often underrepresent socio-organisational dynamics, which are increasingly recognised as critical determinants of risk in complex systems. Research in socio-technical systems theory and organisational risk theory (e.g., Charles Perrow; Erik Hollnagel) highlights that misalignment among actors can be a latent source of failure. The *Tension Map* framework builds on this foundation by introducing a quantitative mechanism to capture and integrate stakeholder misalignment into probabilistic risk assessment.

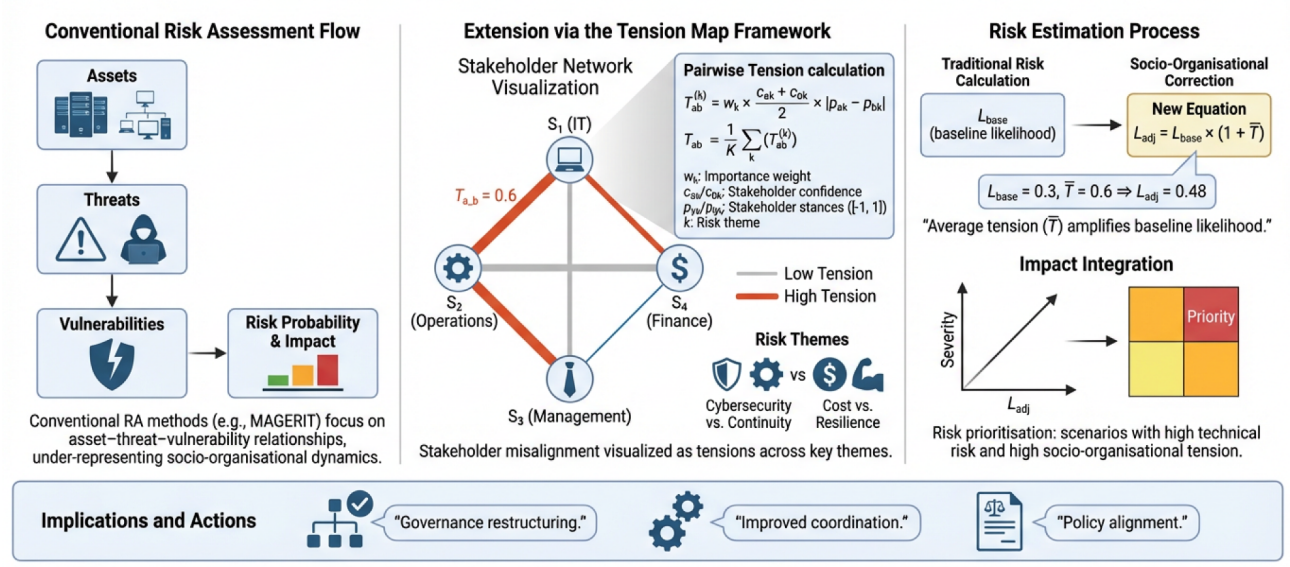

Figure 2: Tension Map Framework: Integrating Socio-organisational tension into probabilistic risk assessment

The framework (Figure 2) begins by defining *risk themes* along which stakeholder perspectives diverge. These themes, such as cybersecurity versus operational continuity or cost versus resilience, reflect trade-offs widely discussed in the cyber risk literature (e.g. Ross Anderson). Each theme is mapped to asset categories, maintaining compatibility with component-based RA models.

Let $S = \{s_1, s_2, \ldots, s_n\}$ denote the set of stakeholders. Their interdependencies are represented through a matrix $D \in [0,1]^{nxn}$, where D_{ab} captures the extent to which stakeholder s_a depends on s_b.

Stakeholder perceptions are elicited for each risk theme t_k using three parameters:

- Position (stance): $p_{ik} \in [-1,1]$
- Confidence: $c_{ik} \in [0,1]$
- Importance weight: $w_k \in [0,1]$

The pairwise tension between stakeholders s_a and s^b under theme t_k is defined as:

$$T_{ab}^{(k)} = w_k \cdot \frac{c_{ak} + c_{bk}}{2} \cdot |p_{ak} - p_{bk}|$$

This formulation extends classical distance metrics by incorporating epistemic confidence and contextual relevance. Aggregating across all K themes yields the overall tension between a pair of stakeholders:

$$T_{ab} = \frac{1}{K} \sum_{k=1} T_{ab}^{(k)}$$

These values define a weighted graph (*Tension Map*) where nodes represent stakeholders and edges encode the intensity of misalignment. Visualisation of such networks supports identification of critical socio-organisational fault lines, consistent with approaches in resilience engineering and system safety.

The central contribution of this framework is the integration of tension into likelihood estimation. Drawing on Bayesian-inspired updating principles, tension acts as a multiplicative adjustment to

baseline risk probabilities. Let L_{base} denote the original likelihood of a given risk scenario. The tension-adjusted likelihood is:

$$L_{adj} = L_{base} \cdot (1 + \underline{T})$$

where $\underline{T} \in [0,1]$ is the normalised average tension among relevant stakeholders. For instance, if $L_{base} = 0.3$ and $\underline{T} = 0.6$, then $L_{adj} = 0.48$, indicating a substantial escalation driven by socio-organisational factors. This model does not replace traditional probabilistic assessments but augments them with a socio-technical correction factor. High tension values are interpreted as *latent vulnerabilities*, echoing James Reason's work on hidden organisational weaknesses that align to produce failure.

2.2 From Tensions to Vulnerabilities, Adjusted Likelihood, and Systemic Insights

A central contribution of the Tension Map framework is the explicit transformation of stakeholder misalignment into *operationally meaningful vulnerabilities* within risk assessment. While traditional approaches, such as MAGERIT, define vulnerabilities primarily as technical weaknesses, this framework extends the concept to include *latent socio-organisational conditions* that increase the likelihood of risk realisation.

2.2.1 Conceptual Foundation

Drawing on socio-technical systems theory, vulnerabilities are not solely embedded in system components but emerge from misalignments between actors, processes, and incentives. In this context, *tension*, quantified divergence in stakeholder stances, serves as a proxy for coordination failure, conflicting priorities, or a communication breakdown. These conditions are well-established precursors to incident propagation in complex systems.

2.2.2 Formal Mapping from Tension to Vulnerability

Let $T_{ab}^{(k)} \in [0,1]$ denote the tension between stakeholders s_a and s^b under risk domain t_k. The corresponding vulnerability factor $V_{ab}^{(k)}$ is defined as:

$$V_{ab}^{(k)} = f\left(T_{ab}^{(k)}\right)$$

where $f(\cdot)$ is a monotonic mapping function. In the simplest case, $V_{ab}^{(k)} = T_{ab}^{(k)}$. However, more expressive formulations may be used to reflect non-linear escalation effects observed in organisational risk literature. For example:

$$V_{ab}^{(k)} = \left(T_{ab}^{(k)}\right)^{\gamma}, \ with\, \gamma > 1$$

This captures the intuition that moderate misalignment may be tolerable, while high tension leads to disproportionately greater vulnerability.

2.2.3 Integration into Risk Likelihood

The adjusted likelihood introduced in Section 2.1 can be generalised by introducing a calibration parameter, α, and an aggregated vulnerability measure, $\underline{V}$. This allows the sensitivity of the risk model to socio-organisational vulnerability to be controlled. The tension-adjusted likelihood becomes:

$$L_{adj} = L_{base} \cdot (1 + \alpha \cdot \underline{V})$$

where L_{base} is the baseline likelihood estimated using an existing risk assessment method, $\underline{V}$ is the aggregated vulnerability across relevant akeholder pairs and themes, and $\alpha \in [0,1]$ is a calibration parameter reflecting the system's sensitivity to socio-organisational factors. This formulation is consistent with Bayesian probabilistic updating principles and remains compatible with existing RA outputs. Importantly, it does not replace baseline estimates but *augments* them to reflect real-world coordination dynamics.

2.2.4 Domain-Specific Interpretation

The transformation from tension to vulnerability is particularly salient in risk domains characterised by, but not limited to, the following trade-offs:

- **Cybersecurity vs Operational Continuity:** High tension between operators and vendors may result in delayed patching, increasing exposure to cyber threats.
- **Cost vs Resilience:** Misalignment may lead to underinvestment in redundancy, elevating system fragility.
- **Transparency vs Confidentiality:** Divergence between regulators and industry actors can hinder information sharing, reducing situational awareness.

In each case, the vulnerability does not arise from a single technical flaw but from an interactional misfit between stakeholders.

2.2.5 Thresholds and Classification

For operational use, vulnerability levels can be categorised based on tension-derived scores. Note that these thresholds are provisional and will be validated empirically against historical incidents in future work (see Section 6):

- $V < 0.3$: Low vulnerability (stable alignment).
- $0.3 \leq V < 0.5$: Moderate vulnerability (requires monitoring).
- $V \geq 0.5$: High vulnerability (priority intervention required).

2.2.6 Implications for Risk Management

By formalising tensions as vulnerabilities, the framework enables:

- Identification of non-technical root causes of risk integrated into component-driven RA processes.
- Prioritisation of interventions targeting governance, communication, and stakeholder alignment.
- Enhanced realism in likelihood estimation for complex socio-technical systems.

Ultimately, our approach operationalises the insight that risk is not only a function of system components, but also of the relationships between the actors who design, operate, and regulate them.

2.3 Impact Workshop Design

The ResChain project team organised two impact workshops in February and March 2026, bringing together stakeholders from the energy and cybersecurity sectors for two days of structured discussion. The aim was to identify new vulnerabilities caused by risk perception misalignments in the energy supply chain. The workshop workflow consists of four steps, illustrated in Figure 3.

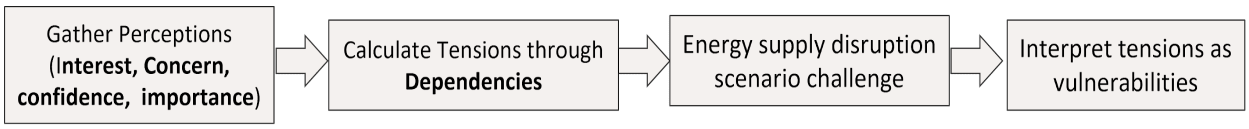

Figure 3: Impact workshop workflow.

The objectives of the workshops were: (1) to identify tensions between stakeholder interests and concerns; (2) to quantify perception gaps engendered by these tensions; (3) to translate tensions into potential vulnerabilities; and (4) to integrate the tension mapping process into a contemporary risk assessment method. All potential vulnerabilities were assigned to asset types defined by MAGERIT [10]: people, process, technology, and information.

There are several key terms using in our impact workshops. These key terms are

- **Dependency:** the degree of correlation between two stakeholders across two distinct risk domains. used consistently throughout the report:
- **Interest:** the level of interest in objectives that must be fulfilled in each risk domain.
- **Concern:** the level of worry about potential negative impacts.
- **Confidence:** the level of confidence in current risk management strategies across risk domains.
- **Importance:** the degree to which a risk domain is important to an organisation's resilience plan.

Numerical values were assigned to each parameter on a five-point scale: 0 (none), 0.25 (low), 0.5 (moderate), 0.75 (high), and 1 (strong). On the other hand, the two workshops were each structured into four sessions, as outlined in Table 1.

Table 1: Workshop sessions.

Session	Title	Purpose & Intended Outcomes
Session 1	Stakeholder perspectives	Collect stakeholders' perspectives in relation to each risk domain. Output: A ranked list of the top risk themes for each stakeholder.
Session 2	Interests and concerns mapping	Identify stakeholders' interests and concerns, with dependencies mapped across diverse risk theme pairs. Output: Tension scores and a list of dependencies between each pair of stakeholders.
Session 3	Scenario challenge	Observe how interests and concerns influence first-priority actions in each disruption scenario. Output: List of first actions taken by stakeholders alongside interest, concern, and dependency ratings.
Session 4	From tensions to vulnerabilities	Translate identified tensions into concrete vulnerabilities. Output: List of vulnerabilities created by stakeholder misalignment, assigned to MAGERIT asset types.

3. Findings

This chapter presents the key findings from the ResChain impact workshops. Section 3.1 introduces the stakeholder participants and their interests, concerns, and top risk domains. Section 3.2 maps interests and concerns to inter-stakeholder dependencies and tension scores. Section 3.3 reports responses to the energy disruption scenario. Section 3.4 describes how identified tensions were translated into concrete vulnerabilities.

3.1 Stakeholders' Perspectives

Representatives from diverse stakeholders in the energy and cybersecurity sectors attended the workshops. These included energy policy analysts, governance, risk, and compliance (GRC) specialists, supervisory control and data acquisition (SCADA) engineers, cybersecurity researchers, cyber-physical systems (CPS) engineers, maintenance and inspection engineers, digital consultants, data engineers, and policymakers, among others. In Session 1, each stakeholder's interests, concerns, and top three risk domains were collected:

- **Multi-service energy retailers:** Interested in profitability, consumer interests, brand awareness, and customer acquisition. Main concerns: slow growth, reduced cash flows due to government regulation, and the energy price cap. Top risk domains: cost, compliance, resilience.
- **Oil and gas producers:** Interested in profit margins and new oil fields. Main concerns: the transition to net zero and renewable energy. Top risk domains: cost, compliance, operational continuity.
- **Digital consultants:** Interested in user engagement, compliance, and organisational disclosure. Main concerns: lack of engagement and of solution adoption. Top risk domains: compliance, resilience, transparency.
- **Asset owners and contractors:** Interested in protecting information assets and organisational reputation. Main concern: compromise of information assets. Top risk domains: confidentiality, integrity, availability.
- **Energy operators:** Interested in the safety, availability, and integrity of software and data. Main concerns: system downtime, zero-day exploits, advanced persistent threats, and insider threats. Top risk domains: resilience, compliance, operational continuity.
- **IoT software vendors:** Interested in revenue growth, intellectual property protection, and scalability. Main concerns: data privacy, supply chain disruption, and vulnerabilities in connected devices. Top risk domains: cost, cybersecurity, confidentiality.
- **Energy policy analysts:** Interested in enforceable and implementable policies. Main concerns: poor policy plans, inadequate data, and unenforceable policies. Top risk domains: compliance, resilience, transparency.
- **Cybersecurity researchers:** Interested in designing trustworthy attack-detection systems and understanding complex cyberattacks. Main concerns: limited research experience and time needed to predict complex attack behaviours. Top risk domains: cost, confidentiality, and availability.
- **Data engineers:** Interested in data transparency, quality assurance, and system interoperability. Main concerns: data privacy compliance and the risk of data mishandling. Top risk domains: transparency, confidentiality, compliance.

Risk domains shared across two or more stakeholders are shown in Figure 4. Compliance (five stakeholders), cost and resilience (four each), and confidentiality (three) emerge as the most widely shared priorities across the energy supply chain.

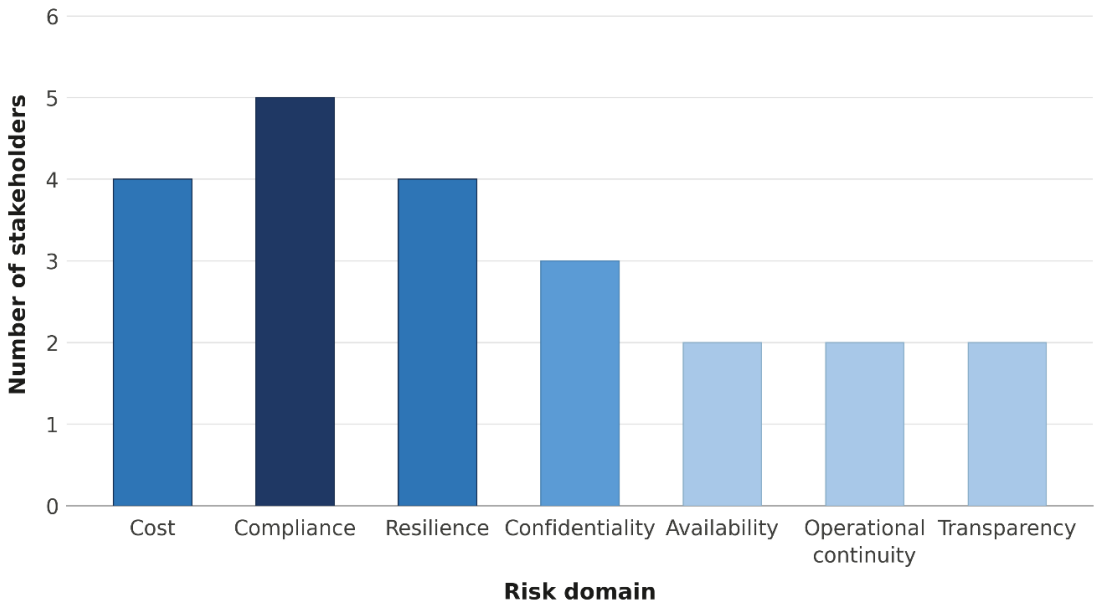

Figure 4: Important risk domains across different stakeholders in the energy supply chain.

From Figure 4, cost is important to four stakeholders (multi-service energy retailers, IoT software vendors, oil and gas producers, and cybersecurity researchers); compliance is important to five (multi-service energy retailers, oil and gas producers, digital consultants, energy operators, and energy policy analysts); resilience is important to four (multi-service energy retailers, digital consultants, energy operators, and energy policy analysts); confidentiality is important to three (asset owners and contractors, cybersecurity researchers, and IoT software vendors); and availability, operational continuity, and transparency are each important to two or more stakeholders.

3.2 Interests and Concerns Mapping

Session 2 asked each stakeholder pair to map their interests and concerns to key tensions. *Tension* refers to misalignment in risk perception across specific areas — termed *risk domains* — where stakeholders view risks differently. These tensions are treated as latent vulnerabilities because they can increase the likelihood of risk realisation. Findings by stakeholder pair are shown in Figure 5. Findings are also summarised below:

- **Asset owner & contractor / SME:** Five strong dependencies were identified, including data protection, service delivery timelines, product and service deliverables, logistics and resources, and compliance with contractual, legal, and regulatory requirements. Despite high interconnection, calculated tension scores were very low across six risk domains, indicating broad alignment.
- **SME / Cybersecurity researchers:** Three high dependencies identified (security services, quality of service, and data availability). However, high tension scores were recorded for the Compliance vs. Cost and Operational Continuity vs. Local Autonomy risk domains.
- **OT/ICS operator / GRC specialist:** Four high dependencies identified (operational continuity, cybersecurity, resilience, and local autonomy), resulting in very low tension scores across Resilience vs. Cybersecurity, Compliance vs. Local Autonomy, and Operational Continuity vs. Local Autonomy, reflecting strong mutual security objectives.

- **Policymaker / GRC specialist:** Strong mutual dependencies around secure data control and coordination, with very low tension scores across Transparency vs. Resilience, Compliance vs. Integrity, and Cost vs. Centralisation. Data-driven, regulatory stakeholders are more likely to achieve coherence in risk management.
- **Oil & gas producer / Cybersecurity researcher:** Three strong dependencies related to cyber defence, regulatory data, and oil field security. Low tension scores recorded for Compliance vs. Confidentiality, Availability vs. Cost, and Resilience vs. Confidentiality.
- **Utilities & retailer / SCADA engineer:** Two high dependencies (digital infrastructure resilience; accurate data for regulatory reporting). High tension scores recorded for Confidentiality vs. Integrity and Compliance vs. Centralisation, reflecting significant misalignment in how these stakeholders prioritise data protection, system control, and regulatory obligations.
- **CPS engineer / Energy operator:** Strong dependencies in unified incident response planning, network and industrial protocols, and critical CPS assets. Moderate tension scores for Compliance vs. Cost and Cybersecurity vs. Operational Continuity, suggesting differences in how cost constraints are balanced against security requirements.

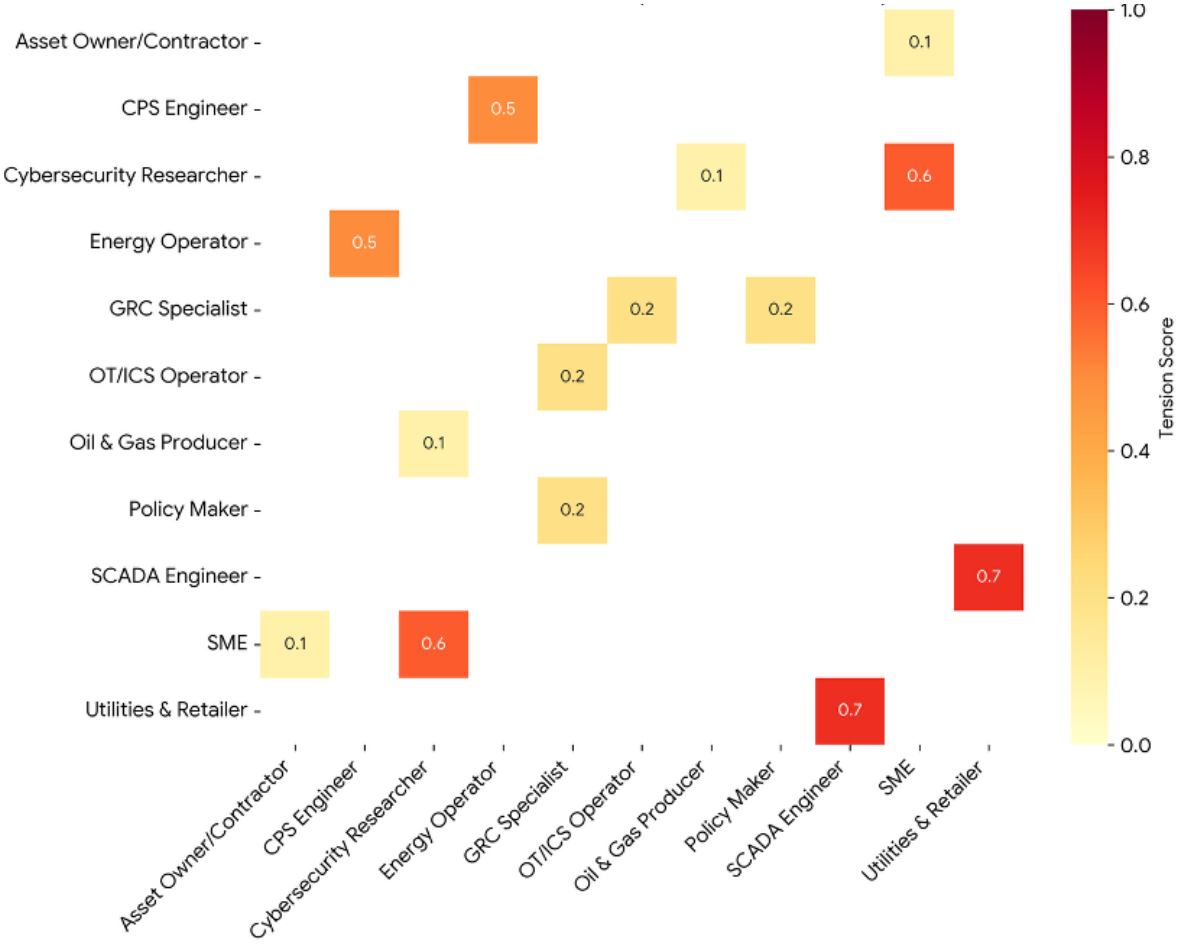

Figure 5: Stakeholder Risk Perception Tension Heatmap.

3.3 Tackling an Energy Disruption Scenario

3.3.1 The Scenario

Session 3 presented participants with a concrete, time-pressured scenario to observe how prior misalignments shaped real-time decision-making. Participants were asked to imagine an 08:30 incident on a weekday: a regional electricity distribution network (supplying power to a major hospital,

a rail signalling system, and a hydrogen production facility) is managed through a SCADA system and a vendor-managed remote monitoring service. Overnight, the monitoring vendor reported abnormal traffic on the SCADA network and a loss of visibility of two substations. Concurrently, voltage instability was detected, control commands were delayed, and hydrogen production was automatically reduced. Within 30 minutes, the hospital had switched to backup generators, rail services had slowed due to signalling delays, and the hydrogen facility reported pressure anomalies. External pressure escalated through media inquiries about a possible cyber attack, a regulator requesting an immediate update, and the vendor requesting full remote access to investigate.

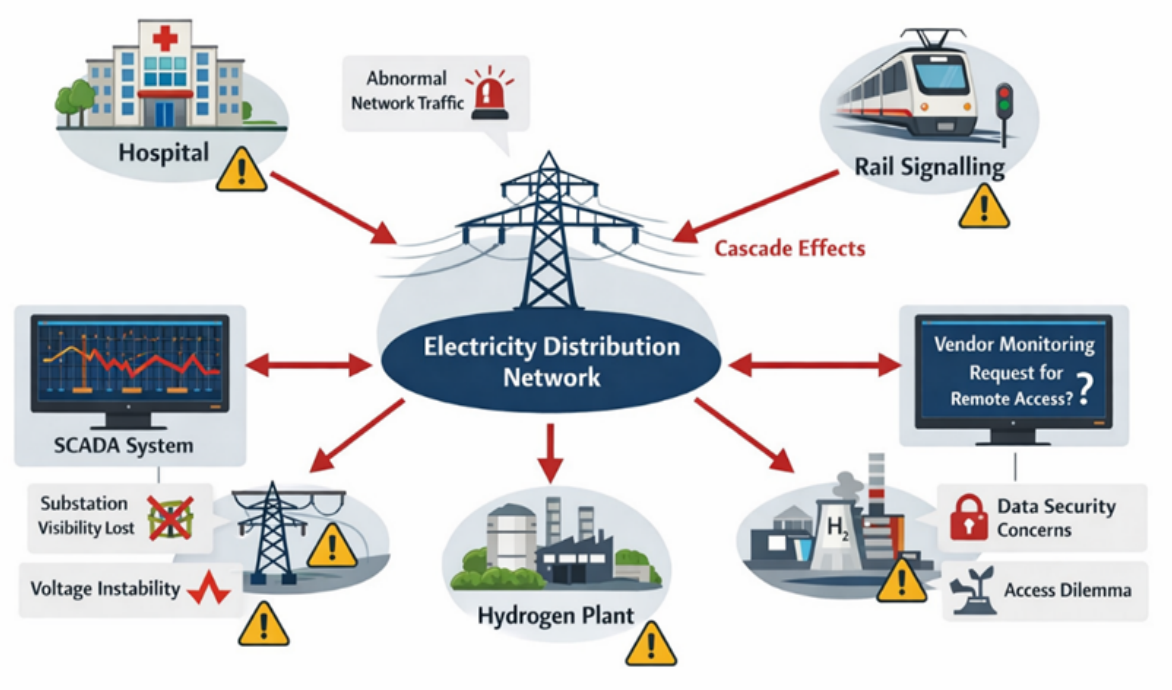

Figure 6: Energy distribution scenario used in Session 3.

3.3.2 Identified Risk Domains

Across all groups, *operational continuity* was the most universally cited risk domain, identified regardless of stakeholder composition. Groups framing the scenario from a technical operations perspective (CPS Engineer / Energy System Operator; OT/ICS Operator / GRC Specialist; SCADA Engineer) emphasised the immediate need to stabilise the system before any investigation could begin — a 'stabilise first, investigate second' logic. Groups with a governance or commercial lens (Oil and Gas Producer / Energy Policy Analyst; Asset Owner / SME) foregrounded compliance and centralisation instead. Cybersecurity and resilience emerged as the second most commonly cited domains; safety was explicitly identified by Group 4 as a primary concern — a framing absent from groups with a more system-engineering orientation.

3.3.3 Prioritised First Actions

Despite identifying different primary risk domains, almost all groups converged on actions centred on restoring control rather than establishing cause:

- CPS/Energy Operator group: switch to manual control and activate a cyber incident response team.
- Oil and gas(O&G) producer / energy policy analyst group: source immediate alternative energy suppliers.
- OT/GRC group: restore the system state to an acceptable level.

- Safety-focused group (Group 4): remain calm, follow the incident protocol, and prioritise operational continuity and safety.
- SCADA-oriented group: assume direct control of the system, deny vendor remote access, and enable retailers to monitor the situation via SCADA.

The SCADA group was the only one to restrict third-party access explicitly rather than request it. This divergence is analytically significant: it reveals that, in a crisis context, the vendor-access dependency identified as a source of high tension in Session 2 becomes an active site of conflicting decisions.

3.3.4 Misalignments and Information Gaps

The SCADA–vendor monitoring dependency surfaced repeatedly as the highest-tension dependency across groups, with participants noting uncertainty about what the vendor could see, what authority they held, and what constituted normal versus abnormal behaviour. One group summarised the contested information neatly: “unsure what this vendor does.” Information gaps were also prominent: groups reported not knowing the current load, the level of voltage instability, or the vendor’s actual capabilities and access permissions. This suggests that vendor access, as a structural dependency, is opaque not only to researchers designing risk frameworks but also to operational stakeholders.

3.3.5 Confidence and Importance Ratings

For their chosen first actions, groups consistently rated both confidence and importance at the highest level (1.0). The one exception was the CPS/Energy Operator group, which rated confidence at 0.5 (moderate) while rating importance at 1.0, linking this asymmetry to the contested nature of vendor-managed monitoring. The overall pattern of high confidence across roles is consistent with Session 2 findings: stakeholders who share strong dependencies tend to exhibit higher confidence in their own planned responses, even when other stakeholders’ responses conflict.

3.3.6 Cross-Group Patterns

Three cross-cutting observations deserve emphasis. First, the scenario consistently collapsed the distinction between technical and governance risk: no group could address operational continuity without also confronting questions of regulatory reporting, vendor authority, and information asymmetry. Second, the most significant dependencies were not between different types of stakeholders (e.g. operators vs regulators) but between stakeholders who share the same critical asset — most notably, the SCADA system. Third, first-mover decisions under crisis conditions were shaped more by role-specific interests than by shared situational awareness, which is itself a systemic vulnerability, since individually rational actions (sourcing alternative supply, restricting vendor access, switching to manual control) can be collectively contradictory at the system level.

3.4 Tensions to Vulnerability

In Session 4, stakeholder pairs worked on risk domains with conflicting objectives and security aims to test whether high tension scores are associated with increased risk likelihood. Key findings are as follows:

- **Cybersecurity researcher / SCADA engineer — Cybersecurity vs Operational Continuity:** Cyberattack detection may require a temporary service shutdown to contain the impact. If unresolved, this tension creates a dependence on manual restart and limited redundancy in operational processes.

- **Cybersecurity engineer / CPS engineer — Speed vs Cost:** Rapid cyber recovery actions can introduce delays that increase operational expenditure. This tension may result in insufficient budget allocation for rapid recovery capability and resource elasticity.
- **SCADA engineer / Utilities & retailer — Resilience vs Availability:** Resilience controls, such as network segmentation and patching, may reduce short-term system availability. The resulting technology vulnerability is an over-centralised architecture with limited failover capacity.
- **Energy operator / CPS engineer — Cost vs Resilience:** Operators demanding resilience investment while CPS engineers resist due to cost constraints creates a technology vulnerability of degraded resilience and decreased supply security. A related tension — Cybersecurity vs Operational Continuity — arises during recovery from an incident, where operators prefer a quicker reconnection while CPS engineers prefer a more secure but slower approach. This can lead to prolonged failure by impeding proper root-cause analysis.
- **Oil and gas producer / Energy policy analyst — Compliance vs Cost:** Producers circumventing environmental regulations (e.g., excess gas flaring) threaten the energy supply chain's ability to meet carbon reduction targets. The resulting process vulnerability is slower progress towards net zero and a just energy transition.
- **Utilities & retailer / Data engineer — Transparency vs Confidentiality:** The data engineer prioritises transparency, while the retailer prioritises confidentiality of commercial and customer data. This information vulnerability increases the likelihood of data leaks or mishandling of sensitive data if the tension is not managed.

4. Implications for Risk Assessment Practice

The findings from the ResChain workshops and the Tension Map framework have direct implications for how risk assessment (RA) is conducted in complex socio-technical systems such as energy supply chains. While existing frameworks, including MAGERIT and other component-driven approaches, provide robust mechanisms for identifying and analysing technical risks, they do not adequately capture the socio-organisational dynamics that influence how risks emerge, propagate, and are managed in practice. The results of this study suggest that incorporating stakeholder misalignment into RA is not an optional enhancement — it is a necessary evolution.

4.1 From Component-Driven to Socio-Technical Risk Assessment

Traditional approaches conceptualise risk as a function of assets, threats, and vulnerabilities, where vulnerabilities are typically defined as weaknesses in technical systems. The workshop findings demonstrate that vulnerabilities also arise from misalignments in stakeholder interests, concerns, and priorities. These misalignments — quantified in this work as *tension* — act as latent conditions that can increase the likelihood of disruption across interconnected systems. RA must therefore evolve towards a socio-technical paradigm in which stakeholder relationships, dependencies, and divergent perceptions are treated as integral elements of the risk landscape. This shift reframes risk assessment from asking solely *"what can fail?"* to also addressing *"where do stakeholders disagree in ways that make failure more likely?"*

4.2 Tension as a Measurable Risk Indicator

The introduction of tension scores provides a structured, repeatable metric for quantifying stakeholder misalignment and incorporating it into RA processes. Unlike qualitative assessments of

organisational risk, tension provides a mechanism that can be systematically applied across different risk domains. In practice, this enables the integration of new artefacts into risk registers, including: tension scores between stakeholder pairs; identification of high-tension risk domains (e.g., compliance versus cost, confidentiality versus transparency); and mapping of dependencies that amplify or mitigate tensions. By treating tension as a leading indicator of risk, organisations can identify latent vulnerabilities before they manifest as incidents — representing a shift from reactive to anticipatory risk management.

4.3 Augmenting Likelihood Estimation in Existing Frameworks

Rather than replacing established approaches, the Tension Map framework introduces a mechanism to augment baseline likelihood estimates using tension-adjusted probabilities. This enables analysts to account for socio-organisational factors that are typically excluded from probabilistic models. For example, a risk scenario that appears to have a low technical likelihood may be significantly elevated when there is high tension among stakeholders responsible for detection, response, or mitigation. Importantly, this approach can be integrated into standard RA workflows without requiring fundamental changes to underlying models, making it suitable for adoption within existing organisational practices.

4.4 Reframing Vulnerabilities as Coordination Failures

The findings from the scenario-based workshop highlight that many critical vulnerabilities are not rooted in technical deficiencies but in coordination failures between stakeholders. During the disruption scenario, different stakeholder groups selected actions that were individually rational but collectively inconsistent, reflecting underlying misalignments in priorities and authority structures. This has significant implications for RA practice: risk scenarios should not only model technical failure modes but also account for potential conflicts in decision-making, unclear responsibilities, and information asymmetries.

4.5 Integration into Risk Assessment Workflows

The Tension Map framework can be integrated into existing RA processes at multiple stages:

- **Risk identification:** Incorporating stakeholder mapping, dependency analysis, and identification of potential tension points.
- **Risk analysis:** Quantifying tensions and translating them into vulnerability factors.
- **Risk evaluation:** Adjusting likelihood estimates using tension-informed models.
- **Risk treatment:** Designing interventions that target alignment, communication, and governance structures, in addition to technical controls.

This layered integration ensures that socio-organisational factors are systematically considered without disrupting established RA practices.

4.6 Expanding the Scope of Risk Mitigation Strategies

Traditional risk mitigation strategies focus on technical solutions such as redundancy, hardening, and detection mechanisms. However, the findings of this study demonstrate that many risks cannot be effectively mitigated solely through technical means. The incorporation of tension into RA highlights the importance of non-technical interventions, including:

- Clarification of roles and decision-making authority.
- Development of shared incident response protocols.

- Improved mechanisms for data sharing and transparency.
- Alignment of incentives across stakeholders.

These measures address the root causes of misalignment and reduce the likelihood of coordination breakdowns during critical events.

4.7 Implications for Decision-Making Under Uncertainty

The workshop findings reveal behavioural patterns that are relevant to RA practice. Stakeholders consistently expressed high confidence in their chosen actions, even when those actions conflicted with other stakeholders' approaches. This suggests that role-specific perspectives and bounded rationality strongly influence decision-making in complex systems. For RA practitioners, this implies that risk models should account for the possibility of divergent decision pathways under uncertainty. Decision-support tools should therefore not only identify optimal actions but also highlight potential conflicts between stakeholder responses and their implications for system-level outcomes.

4.8 Towards Dynamic and Continuous Risk Assessment

Incorporating tension into RA supports a transition from static, periodic assessments to more dynamic, continuous approaches. Stakeholder alignment is not fixed; it evolves over time in response to organisational changes, regulatory pressures, and external events. By monitoring tension as a dynamic variable, organisations can detect emerging misalignments and intervene before they translate into realised risks. This capability enhances resilience by enabling earlier and more targeted responses to changing conditions within the system.

5. Implications for the Energy Sector

The findings from the ResChain workshops, and in particular from the scenario challenge in Session 3, carry implications that extend beyond risk assessment methodology and into the structural conditions of the energy sector itself.

5.1 Operational Risk Cannot Be Separated from Governance Risk

The scenario made visible something that technical risk models routinely suppress: at the moment of disruption, operational decisions are governance decisions. Whether to restrict vendor access, whether to proactively notify the regulator, and whether to prioritise supply restoration over root-cause investigation are not purely technical choices. They are determined by the stakeholders' interests, concerns, and perceived authorities. The energy sector's continued reliance on component-driven risk assessment frameworks that treat these as separable is therefore a structural vulnerability. Risk governance frameworks should be redesigned to treat the operator–vendor interface, the operator–regulator reporting relationship, and the inter-stakeholder information exchange as first-class objects of risk analysis.

5.2 Vendor-Managed Monitoring Is a Systemic Dependency That Is Under-Governed

Across multiple groups and both workshops, the dependency on vendor-managed remote monitoring emerged as the highest-tension dependency in the energy supply chain. This is not merely a contractual or procurement concern. When vendor access can be both the channel through which a threat enters a system and the primary mechanism for investigating that threat, the energy sector faces a principal–agent problem that current risk registers are not designed to capture. This structural condition is reflected across multiple findings (see Figure 7). The ResChain findings suggest that energy sector regulators should consider requiring explicit transparency declarations

for vendor-managed monitoring contracts, including the delineation of access rights, reporting obligations, and escalation authorities in the event of incidents.

5.3 Crisis Response Diverges Across Stakeholder Roles in Ways That Create Systemic Incoherence

The scenario findings showed that individually rational first actions — sourcing alternative supply, restricting remote access, switching to manual control — can be collectively incoherent when enacted simultaneously by different stakeholders without coordination. This is not a training or information-sharing problem alone; it reflects a deeper misalignment in risk priorities documented throughout the workshops. The energy sector needs pre-agreed, multi-stakeholder incident protocols that explicitly define not just what each stakeholder should do, but the sequence and authority under which those actions should be taken, and which actions require inter-stakeholder coordination before they can be implemented.

5.4 Compliance Pressure Under Crisis Conditions Is a Force Multiplier for Misalignment

Groups consistently identified compliance as a risk domain that intensified under scenario conditions, as regulators demanded updates while operators were still trying to stabilise the system. This creates perverse incentives: the stakeholder who pauses to prepare a regulatory report is disadvantaged relative to the one who acts immediately, yet the one who acts without reporting may create legal liability. Sector-level guidance on the sequencing of compliance obligations under active disruption conditions would reduce this tension and improve the coherence of cross-stakeholder responses.

5.5 The Energy Trilemma Is Replicated at the Incident Level

The ResChain workshop findings suggest that the structural tension at the heart of energy policy — between security, affordability, and sustainability — is reproduced at the operational level during incidents. Groups representing O&G producers and energy policy analysts focused on supply restoration and downstream continuity (security and affordability). In contrast, groups representing SCADA engineers and OT operators focused on system integrity and controlled access (security and resilience). Neither orientation is wrong; both are necessary. The implications discussed above are not independent observations but reflect a consistent pattern linking observed stakeholder behaviour to underlying structural conditions in the energy sector. These relationships, and their corresponding implications for practice, are summarised in Figure 7.

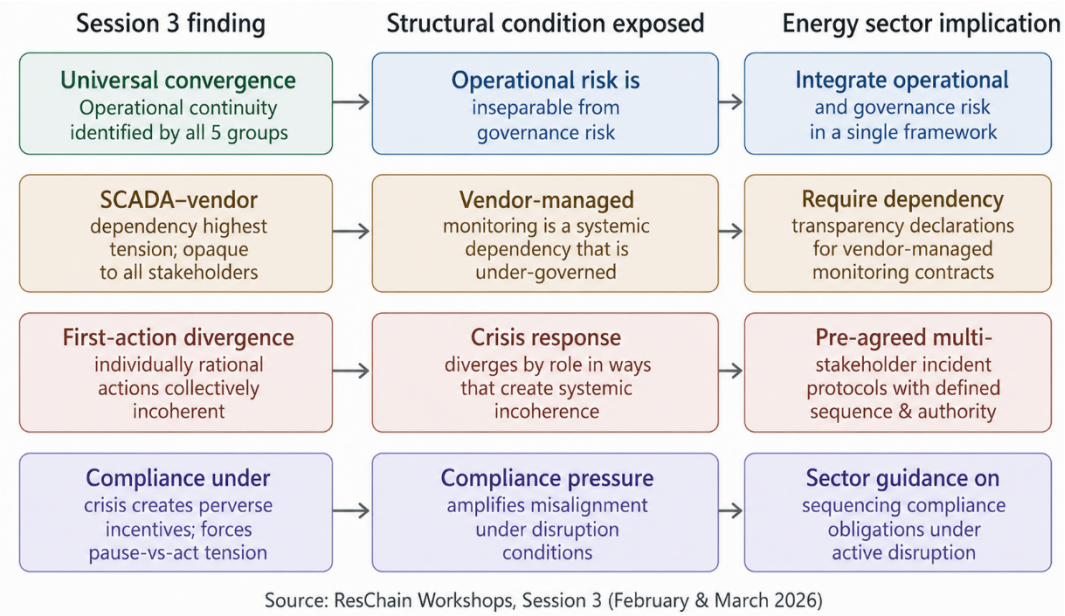

Figure 7: Synthesis of structural conditions identified from Session 3 and their implications for the energy sector.

6. Limitations and Future Work

While the proposed framework provides a structured approach to integrating socio-organisational tensions into risk assessment, several limitations remain that will be systematically addressed in future activities.

A key challenge lies in the reliance on subjective stakeholder perceptions — such as positions, confidence levels, and importance weights — which may introduce bias or inconsistency. To mitigate this, subsequent work will refine data-collection instruments by incorporating calibration techniques and triangulating survey responses with documentary evidence and expert validation.

A further limitation concerns the currently untested assumption that higher tension increases the likelihood of risk. This will be addressed through pilot case studies that compare calculated tension scores with real or historical incidents, enabling empirical validation of the model. The existing tension formulation will also be enhanced by testing alternative approaches that account for non-linear effects, asymmetric relationships, and varying levels of stakeholder dependency.

The vulnerability thresholds presented in Section 2.2.5 ($V < 0.3$, $0.3 \leq V < 0.5$, $V \geq 0.5$) are provisional and will be validated empirically against historical incident data in future work.

Furthermore, the framework's static nature will be extended through longitudinal data collection, enabling the tracking of tensions over time and supporting early identification of emerging risks. Integration challenges with established methodologies, such as MAGERIT, will be addressed by embedding the approach into real-world risk assessment workflows during pilot implementations. Finally, visualisation techniques will be refined through user testing to ensure clarity and consistency in interpretation. Collectively, these activities will strengthen the framework's robustness, usability, and practical relevance.

7. References

[1] Mawhood, B. & Sutherland, N. (2023). Tackling the energy trilemma. House of Commons Library, UK Parliament. Available at: https://commonslibrary.parliament.uk/research-briefings/cdp-2023-0074/

[2] Bale, C. S., Varga, L., & Foxon, T. J. (2015). Energy and complexity: New ways forward. Applied Energy, 138, 150–159. DOI: https://doi.org/10.1016/j.apenergy.2014.10.057

[3] Urciuoli, L., Mohanty, S., Hintsa, J., & Gerine Boekesteijn, E. (2014). The resilience of energy supply chains: a multiple case study approach on oil and gas supply chains to Europe. Supply Chain Management: An International Journal, 19(1), 46–63. DOI: https://doi.org/10.1108/SCM-09-2012-0307

[4] Cui, L., Yue, S., Nghiem, X. H., & Duan, M. (2023). Exploring the risk and economic vulnerability of global energy supply chain interruption in the context of the Russia–Ukraine war. Resources Policy, 81, 103373. DOI: https://doi.org/10.1016/j.resourpol.2023.103373

[5] Hammi, B., Zeadally, S., & Nebhen, J. (2023). Security threats, countermeasures, and challenges of digital supply chains. ACM Computing Surveys, 55(14s), 1–40. DOI: https://doi.org/10.1145/3588999

[6] Colon, C., & Hochrainer-Stigler, S. (2023). Systemic risks in supply chains: a need for system-level governance. Supply Chain Management: An International Journal, 28(4), 682–694. DOI: https://doi.org/10.1108/SCM-03-2022-0101

[7] National Cyber Security Centre (2023). Component driven risk management methods. Risk management. Available at: https://www.ncsc.gov.uk/collection/risk-management/component-driven-risk-management-methods

[8] Xexakis, G., Hansmann, R., Volken, S. P., & Trutnevyte, E. (2020). Models on the wrong track: model-based electricity supply scenarios in Switzerland are not aligned with the perspectives of energy experts and the public. Renewable and Sustainable Energy Reviews, 134, 110297. DOI: https://doi.org/10.1016/j.rser.2020.110297

[9] Holm, T. B., Daloz, A. S., Ma, L., Van Maanen, N., Tamang, R., & Aall, C. (2025). From climatic hazards to systemic vulnerabilities: Evolving perceptions of climate risk in Norway's renewable energy sector. Energy Research & Social Science, 130, 104456. DOI: https://doi.org/10.1016/j.erss.2025.104456

[10] Ministerio de Hacienda y Administraciones Públicas, Spain. *MAGERIT version 3: Methodology for Information Systems Risk Analysis and Management*. Available at: https://interoperable-europe.ec.europa.eu/collection/spain-center-technology-transfer/solution/magerit-v3