International Journal of Disaster Risk Reduction 133 (2026) 106009

Contents lists available at ScienceDirect

International Journal of Disaster Risk Reduction

journal homepage: www.elsevier.com/locate/ijdrr

A self-organized criticality model of extreme events and cascading disasters of hub-and-spoke air traffic networks

Mary Lai O. Salvaña [a,b,*], Harold Jay M. Bolingot [b], Gregory L. Tangonan [b]

[a] Department of Statistics, University of Connecticut, 215 Glenbrook Rd., Storrs, CT, 06269, USA
[b] Ateneo Innovation Center, Ateneo de Manila University, Quezon City, Metro Manila, 1108, Philippines

ARTICLE INFO

Keywords:
Air traffic disasters
Cascading disasters
Critical infrastructures
Early warning systems
Disaster risk reduction
Self-organized criticality

ABSTRACT

Critical infrastructure networks, such as transportation, power grids, and communication systems, exhibit complex interdependencies that can lead to cascading failures with catastrophic consequences. These cascading disasters often originate from failures at critical points in the network, where single-node disruptions can propagate rapidly due to structural dependencies and high-impact linkages. Such vulnerabilities are exacerbated in systems that have been highly optimized for efficiency or have self-organized into fragile configurations over time. The air transportation system in the United States, built on a hub-and-spoke model, exemplifies this type of critical infrastructure. Its reliance on a limited number of high-throughput hubs means that even localized disruptions — particularly those triggered by increasingly frequent and extreme weather events — can initiate cascades with nationwide impacts. We introduce a novel application of the theory of Self-Organized Criticality (SOC) to model and analyze cascading failures in such networks. Through a detailed case study of U.S. airline operations, we show how the SOC model exhibits the power-law distribution of disruptions and the long-tail risk of systemic failures, reflecting the real-world interplay between structural fragility and external shocks. Our approach enables quantitative assessment of network vulnerability, identification of critical nodes, and evaluation of proactive intervention strategies for disaster risk reduction. The results demonstrate that the SOC model successfully replicates the observed statistical patterns of disruption sizes — characterized by frequent small events and rare but severe cascading failures — offering a powerful systems-level framework for infrastructure resilience planning and emergency management. The model provides practitioners with actionable insights for anticipating and mitigating systemic risks in complex, interdependent systems.

1. Introduction

The catastrophic failures that have increasingly plagued modern air transportation networks reveal a fundamental vulnerability in our interconnected world. When Southwest Airlines canceled over 16,000 flights during the December 2022 winter storm [1], the Federal Aviation Administration's (FAA) Notice to Airmen (NOTAM) system failure grounded all domestic flights in January 2023 [2], and Hurricane Ian's impact cascaded through the entire national aviation network despite affecting only a handful of airports [3], they exposed a troubling reality: the air transportation infrastructure has evolved into a system poised on the edge of chaos [4,5].

* Corresponding author at: Department of Statistics, University of Connecticut, 215 Glenbrook Rd., Storrs, CT, 06269, USA.
E-mail addresses: marylai.salvana@uconn.edu (M.L.O. Salvaña), harrybo@ateneoinnovation.org (H.J.M. Bolingot), goriot@mac.com (G.L. Tangonan).
URL: https://marylaisalvana.com (M.L.O. Salvaña).

https://doi.org/10.1016/j.ijdrr.2026.106009
Received 19 June 2025; Received in revised form 5 January 2026; Accepted 9 January 2026
Available online 12 January 2026

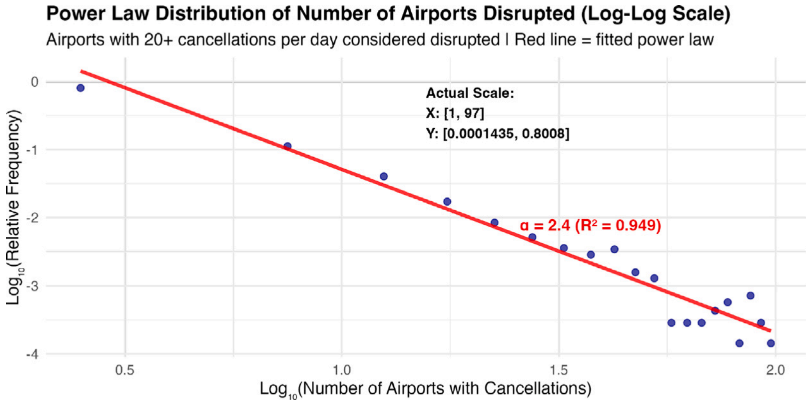


Fig. 1. Power-law distribution of airport disruptions in the U.S. air traffic network, exhibiting characteristics of self-organized criticality (SOC). The log–log plot shows a power-law exponent of $\alpha = 2.4$ with high goodness-of-fit ($R^2 = 0.949$), indicating that while small disruptions are common, large system-wide failures are rare but statistically expected.

Modern aviation relies on a hub-and-spoke architecture that is remarkably efficient under normal conditions. However, this structure exhibits hallmarks of self-organized criticality (SOC)—a regime where small perturbations can trigger avalanche-like cascading failures [6]. This architecture concentrates the vast majority of air traffic through a limited number of high-throughput hubs such as ATL (Atlanta), ORD (Chicago O'Hare), DFW (Dallas–Fort Worth), and DEN (Denver). Each of these hubs processes thousands of connecting flights daily, creating a tightly coupled system in which the failure of a single hub can rapidly propagate disruptions across the entire network.

Our empirical analysis of comprehensive flight operations data from the Bureau of Transportation Statistics [7] shows that the U.S. air traffic network operates in an SOC state. Fig. 1 demonstrates that airport disruptions follow a power-law distribution — a signature of SOC systems — where small disruptions occur frequently while large systemic failures, though rare, emerge as inevitable consequences of the network's structure. This behavior persists across decades of data, as Fig. 2 illustrates.

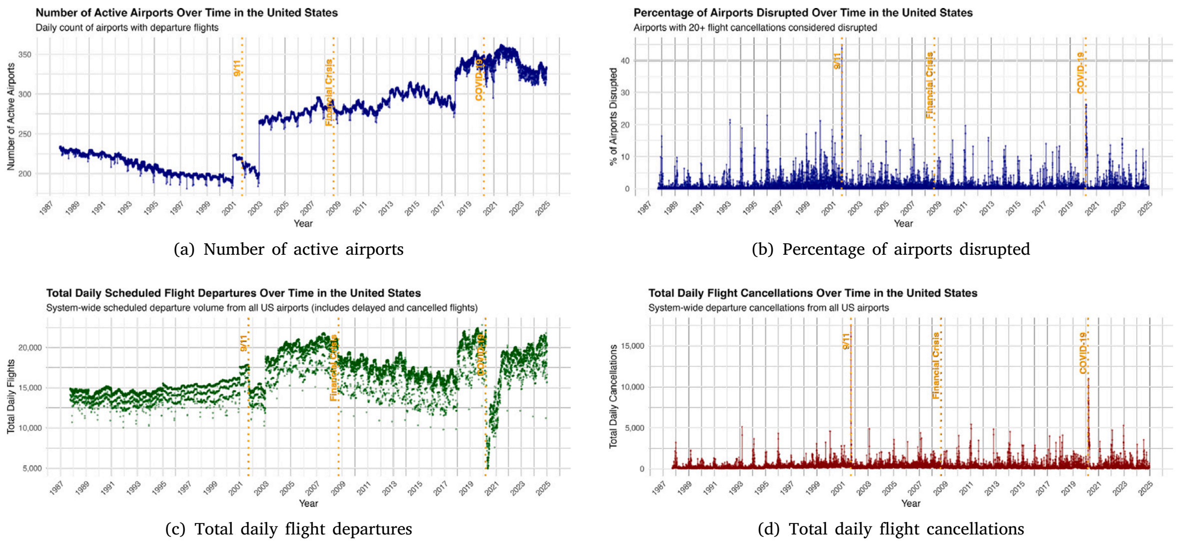
The evolution toward criticality reflects two reinforcing trends: the relentless optimization of air traffic for business efficiency and the climate-driven intensification of extreme weather. Together, these forces have created systemic vulnerability—efficiency optimization has eliminated redundancy precisely as weather shocks have become more severe. The four panels of Fig. 2 illustrate this transformation: (a) airport network expansion followed by saturation and crisis-driven contraction, (b) disruption patterns exhibiting SOC behavior, (c) operations nearing fundamental capacity limits, and (d) cancellation severity surpassing historical norms. These trends have positioned the aviation system at the edge of chaos — a pattern echoed in power grid failure analysis [8] — and suggest that cascading failures are now structural features rather than preventable anomalies.

This empirical evidence of SOC behavior in aviation networks reflects a broader pattern of systemic vulnerability emerging across complex systems. Cascading disasters — where initial disruptions propagate through interdependent networks — have drawn increasing attention for their disproportionate and unexpected impacts. In contrast to compound events involving multiple independent hazards, cascading failures originate in tightly coupled, efficiency-optimized systems, where local perturbations rapidly escalate across sectors [9–11]. This systems perspective has been applied to multi-hazard interactions, which reveal latent vulnerabilities often overlooked in single-event analyses. [12–17]. These dynamics are further amplified by institutional fragilities and coordination gaps [11,18–20].

Cascading failure dynamics have been extensively studied in digital networks and global supply chains, offering valuable cross-domain insights. In digital infrastructure, cascading failures manifest through routing table corruption, distributed denial-of-service amplification, and software dependency chains—where a single library vulnerability can propagate across millions of systems [21,22]. The 2021 Fastly outage demonstrated how a single configuration error could simultaneously disable major websites worldwide [23]. Similarly, global supply chains exhibit SOC-like behavior: the 2021 semiconductor shortage cascaded from initial chip fabrication disruptions to automobile production halts and broader economic impacts [24,25]. The 2021 Suez Canal blockage revealed how a single chokepoint failure could propagate through global trade networks [26,27]. These cross-domain parallels underscore the universality of SOC dynamics and highlight transferable resilience strategies — including redundancy investment, modular design, and real-time monitoring — that inform our aviation network analysis.

Climate change intensifies these risks by increasing the frequency and severity of extreme events, while aging infrastructure, brittle supply chains, and algorithmic complexity push systems closer to failure [24,28–30]. Compound extremes — such as wildfire–heatwave–drought linkages — have highlighted the inadequacy of scenario-based planning and underscored the need for systemic models that can capture emergent, network-wide failure patterns [31–36]. Yet dominant modeling frameworks remain static and rule-based, lacking the capacity to simulate the nonlinear, evolving dynamics that unfold across space and time [37–43].

In contrast, SOC dynamics are fundamentally emergent. Large-scale failures can arise not from a single extreme event but from the gradual accumulation and redistribution of stress across interconnected components. For example, a bridge may appear structurally



(a) Number of active airports

(b) Percentage of airports disrupted

(c) Total daily flight departures

(d) Total daily flight cancellations

Fig. 2. Evolution of the U.S. aviation system from 1987 to 2025 across four key operational metrics. Vertical dotted lines denote major crisis events: 9/11 (2001), the Financial Crisis (2008), and COVID-19 (2020).

sound under normal traffic but collapse after repeated minor stresses exceed a threshold. Because tipping points depend on evolving system states — not just observable shocks — models based solely on past events may overlook future vulnerabilities. This limitation is especially acute in dense, interconnected environments, where complexity and fragility grow in tandem [44–49].

This paper addresses these challenges by introducing a novel application of SOC theory to model cascading failures as emergent outcomes of complex system dynamics. Rather than viewing large-scale disruptions as isolated anomalies, SOC frames them as inevitable outcomes of stress accumulation and structural fragility—offering a systems-level framework for anticipating, diagnosing, and mitigating cascading failures in critical infrastructure networks.

Traditional stress-testing approaches for aviation networks rely on scenario enumeration: analysts design discrete disruption scenarios — a hurricane at Miami, a blizzard at O'Hare, a system outage at Atlanta — simulate each one, and measure the response. This paradigm, while intuitive, suffers from a fundamental limitation: real aviation systems do not face neatly defined scenarios. They face continuous, random, unpredictable friction—small pressures arriving everywhere, all the time. A crew scheduling delay here. A maintenance backlog there. A ground equipment shortage somewhere else. The system adapts, redistributes load, absorbs some shocks and buckles under others. This emergent behavior cannot be captured by enumerating individual failure scenarios, no matter how comprehensive the scenario library.

The SOC framework offers a fundamentally different paradigm. Rather than asking "What happens if Disruption X hits Airport Y?" — which requires exhaustive scenario enumeration — the model asks: "Given the network's topology, operational rules, and current stress levels, is this system inherently fragile or inherently resilient?" The simulation applies continuous random stress accumulation, letting the system evolve through its own dynamics: absorbing pressure below thresholds, redistributing load when thresholds are exceeded, and cascading when redistribution overwhelms neighboring capacity. The emergent power-law distribution reveals whether the architecture is poised for catastrophic failure—a structural property invisible to scenario-based tools.

This study makes three primary contributions. *First*, we present the first systematic application of SOC theory to model cascading failures in air traffic networks, demonstrating that power-law distributed disruptions emerge from network topology and operational rules rather than external shocks alone. *Second*, we develop a novel early warning system (EWS) framework with operationally interpretable metrics — contagion risk and susceptibility risk — that enable proactive identification of vulnerable airports and can be calibrated using existing FAA and airline data. *Third*, we introduce a climate stress-testing methodology that quantifies how extreme weather amplifies cascade risk under future climate scenarios, providing actionable guidance for infrastructure resilience planning.

The rest of the paper is organized as follows: Section 2 reviews the theoretical foundations of SOC. Section 3 presents the SOC model for the U.S. air traffic network. Section 4 reports simulation experiments. Section 5 develops the early warning system. Section 6 applies SOC to climate stress-testing. Section 7 concludes and identifies future research directions.

2. Theoretical foundations of self-organized criticality

SOC represents a major theoretical breakthrough in complex systems science, offering a unified framework for understanding how large-scale catastrophic events can emerge naturally from the intrinsic dynamics of interconnected systems. Unlike traditional approaches that treat major disruptions as exogenous shocks or rare anomalies, SOC theory reveals that catastrophic failures are often structural features of systems operating near critical thresholds. This perspective shifts the focus of infrastructure resilience from preventing isolated failures to managing the dynamics of criticality itself—particularly in systems optimized for efficiency and operating under constant stress.

2.1. Systems on the edge of chaos

The theoretical foundation of SOC emerged from the seminal work of Bak et al. [6], who showed that complex systems can spontaneously evolve toward critical states without external tuning. The canonical sandpile model illustrates this: grains of sand accumulate until a critical slope is reached, after which a single grain can trigger avalanches of all sizes. This balance between slow buildup and fast relaxation produces three defining characteristics: scale invariance, where statistical patterns persist across scales; universality, where outcomes are independent of micro-level details; and long-range correlations, where local perturbations can affect distant parts of the system. These features produce power-law distributions of event sizes, offering a theoretical basis for why catastrophic failures occur with statistical regularity across domains such as evolution [50], solar flares [51], earthquakes [52–54], landslides [55], financial markets [56,57], economic cycles [58], neural dynamics [59,60], psychological phenomena [61], ecosystems [62], wildfires [63], and power grids [8,64,65].

2.2. The mathematics of criticality

The mathematical foundation of SOC is its scale-invariant behavior, expressed through a power-law distribution: $P(s) \sim s^{-\alpha}$, where s is the event size and α is the critical exponent. This distribution implies the absence of a typical event size—unlike normal distributions centered on averages, power laws exhibit heavy tails where extreme events are far more probable than intuition suggests. The value of α governs the system's risk profile: smaller exponents increase the likelihood of large cascades, while larger exponents favor smaller, more frequent events.

2.3. SOC in complex systems

SOC theory provides a powerful explanation for cascading failures in complex systems. The 2003 Northeast blackout exemplifies this behavior: a line failure in Ohio cascaded across regional networks, affecting over 50 million people and causing an estimated $10 billion in damages [66,67]. More recently, Salvaña and Tangonan [8] demonstrated that monitoring changes in the exponent α could forecast the 2021 Texas power crisis 6–12 months in advance.

Building on this foundation, we present a framework that models critical infrastructures as SOC systems. This marks a paradigm shift from conventional risk assessments — focused on isolated failure modes — toward a systems-level view where criticality is an emergent property of the system itself. Hub-and-spoke architectures concentrate stress at central nodes, making them natural cascade triggers. SOC theory suggests that catastrophic failures are statistically expected outcomes driven by network topology, load conditions, and proximity to criticality.

3. The SOC model of the U.S. air traffic network

Our modeling framework extends the Bak–Tang–Wiesenfeld (BTW) sandpile model [6] to network-based critical infrastructure systems. In the original BTW model, sand grains accumulate on a lattice until a critical slope is exceeded, triggering avalanches where grains redistribute to neighboring sites. We adapt this framework by treating airports as lattice sites, operational stress as accumulated grains, and capacity thresholds as critical slopes. A key extension is the introduction of a tunable redistribution parameter $\beta \in [0, 1]$ that controls what fraction of stress propagates to neighbors upon failure. When $\beta = 0$, stress is fully dissipated locally; when $\beta = 1$, stress is perfectly conserved and redistributed; intermediate values produce the partial redistribution dynamics characteristic of SOC.

Our framework formalizes five core elements that collectively determine the system's critical behavior:

1. **Network Configuration**: Defines the pathways through which failures propagate. Fig. 3 depicts the hierarchical hub-and-spoke structure of U.S. aviation.
2. **Stress Accumulation Rule**: Describes how operational pressure builds up over time, reflecting the slow progression toward criticality. In aviation, stress arises from operational bottlenecks, environmental hazards, and workforce dynamics.
3. **Failure Condition**: Specifies the threshold at which individual nodes become unstable and trigger redistributive events, capturing capacity constraints.
4. **Stress Redistribution Rule**: Determines how stress released by failed nodes transfers to neighbors. The parameter β controls the fraction transferred, ranging from full dissipation ($\beta = 0$) to perfect conservation ($\beta = 1$).
5. **Cascade Propagation**: Describes how failures recursively trigger other failures until the system reaches a stable state.

These five elements jointly shape the system's emergent behavior. Fig. 4 illustrates the progression from a stable subcritical state to supercritical conditions where minor shocks trigger widespread disruptions.

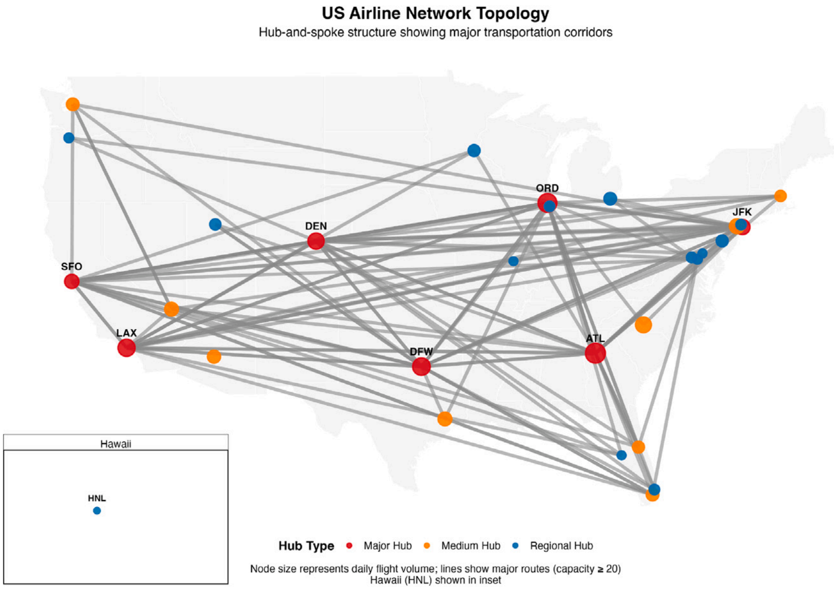


Fig. 3. Topology of the U.S. airline network. Major hubs (red), medium hubs (orange), and regional hubs (blue) are distinguished by node color; node size reflects hub strength, and edge thickness indicates route capacity.

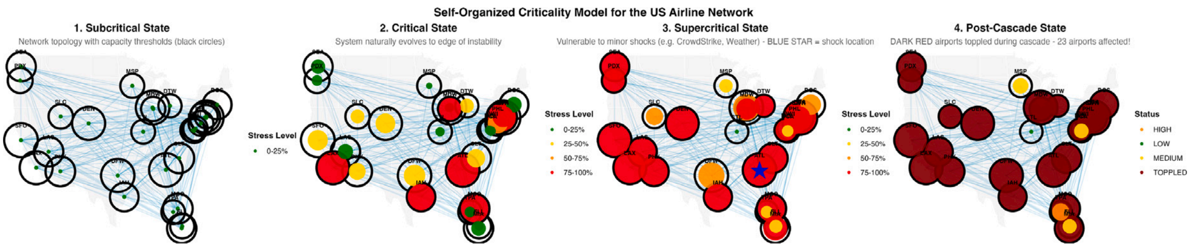


Fig. 4. Progression of the U.S. airline network through four phases of SOC: (1) Subcritical State, (2) Critical State, (3) Supercritical State with cascading failures, and (4) Post-Cascade State with partial recovery.

4. Simulation study

We conduct simulation experiments to investigate how structural and operational factors shape SOC behavior and the distribution of cascading failures. A key objective is to examine how the emergent power-law exponent α varies across network configurations and to establish the relationship between α and systemic risk outcomes.

4.1. Network topologies

We simulate three network configurations representing distinct organizational paradigms (Fig. 5):

- *Hub-and-Spoke*: Centralized around major hubs, with regional airports dependent on hub connectivity. This reflects the dominant structure of legacy carriers.
- *Point-to-Point*: Decentralized with dense interconnectivity and no dominant hubs. This approximates the operational model of low-cost carriers.
- *Fragmented Regional*: Organized into semi-autonomous regional clusters with sparse inter-regional connections.

4.2. Operational scenarios

For each topology, we define three operational scenarios (Table 1). Rather than calibrating β to specific historical events — which would require granular propagation data not currently available — we adopt a scenario-based approach spanning the operationally meaningful range.

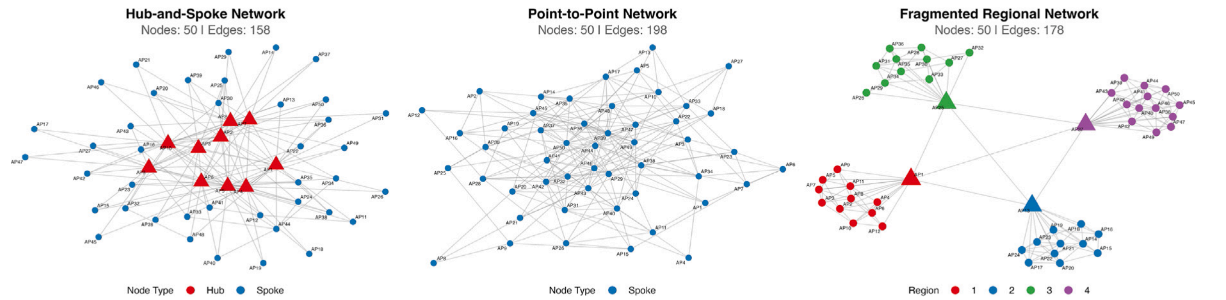


Fig. 5. Three network topologies used in simulation experiments. **Left:** Hub-and-Spoke. **Center:** Point-to-Point. **Right:** Fragmented Regional.

Table 1
Network scenarios across three topologies (n = 50 airports). β controls stress redistribution, θ represents failure thresholds, α is the emergent power-law exponent, and Max Affected measures cascade impact.

Topology	Scenario	β	θ_{hub}	θ_{spoke}	α	Max	Real-world analog
Hub-and-Spoke	Baseline	0.50	1.0	1.0	3.24	18	Normal operations
Hub-and-Spoke	Critical	0.90	0.7	1.0	2.03	47	Holiday peak + storm
Hub-and-Spoke	Resilient	0.35	1.3	1.0	3.95	14	Post-crisis reforms
Point-to-Point	Baseline	0.50	1.0	1.0	3.38	19	Normal operations
Point-to-Point	Critical	0.90	0.8	0.8	2.10	50	System-wide congestion
Point-to-Point	Resilient	0.35	1.2	1.2	3.52	10	Distributed buffers
Fragmented	Baseline	0.50	1.0	1.0	3.58	17	Normal operations
Fragmented	Critical	0.90	0.7	0.9	2.62	46	Regional storm clustering
Fragmented	Resilient	0.35	1.3	1.1	3.77	10	Regional autonomy

- *Baseline*: Normal operations with moderate stress redistribution ($\beta = 0.50$) and uniform failure thresholds ($\theta = 1.0$). At $\beta = 0.50$, half of the stress from a failed node propagates to neighbors, representing a system with adequate operational buffers.
- *Critical*: The system operates near its critical threshold. High redistribution efficiency ($\beta = 0.90$) reflects saturated capacity—nearly all stress transfers to neighbors because local absorption mechanisms are exhausted. Reduced hub thresholds capture weather-induced capacity constraints.
- *Resilient*: Post-crisis reforms with enhanced buffer capacity. Low redistribution ($\beta = 0.35$) reflects operational slack—most disruption impact is contained locally through reserve resources. Elevated thresholds represent infrastructure investments.

The empirically observed $\alpha \approx 2.4$ (Fig. 1) falls between our baseline ($\alpha \approx 3.2$–3.6) and critical ($\alpha \approx 2.0$–2.6) scenarios, suggesting the real system operates with effective β in the range 0.5–0.9. This provides indirect empirical grounding for our parameter choices.

4.3. Results

The simulation results reveal a systematic relationship between α and cascade severity:

- *Critical scenarios produce dangerous power-law signatures:* Under critical conditions, all topologies exhibit α values between 2.03 and 2.62, with near-complete system failures (46–50 airports affected). The Hub-and-Spoke network under critical stress produces $\alpha = 2.03$, with cascades affecting 94% of the network.
- *Resilient configurations shift the system toward safer regimes:* Resilient scenarios consistently produce α values between 3.52 and 3.95, with maximum cascade sizes limited to 20%–28% of the network.
- *Topology modulates risk through distinct mechanisms:* The Point-to-Point network achieves complete system failure (50/50 airports) under critical conditions, outpacing even the Hub-and-Spoke network (47/50). This arises from connection density: Point-to-Point networks provide more pathways for stress propagation. When β is high, each failed node distributes stress across numerous highly connected neighbors, creating rapid chain reactions. In contrast, Hub-and-Spoke concentrates risk at hubs, but spoke nodes' limited connectivity slows cascade propagation at the periphery. The Fragmented Regional network exhibits the highest α under critical conditions (2.62 vs. 2.03–2.10), demonstrating that modular structure provides inherent protection. Sparse inter-regional connections act as natural firebreaks, creating bottlenecks that limit propagation.

Fig. 6 illustrates the inverse relationship between α and maximum cascade size. The empirically observed $\alpha \approx 2.4$ falls between baseline and critical scenarios, suggesting the real system operates in an intermediate risk regime susceptible to transitioning toward criticality under stress.

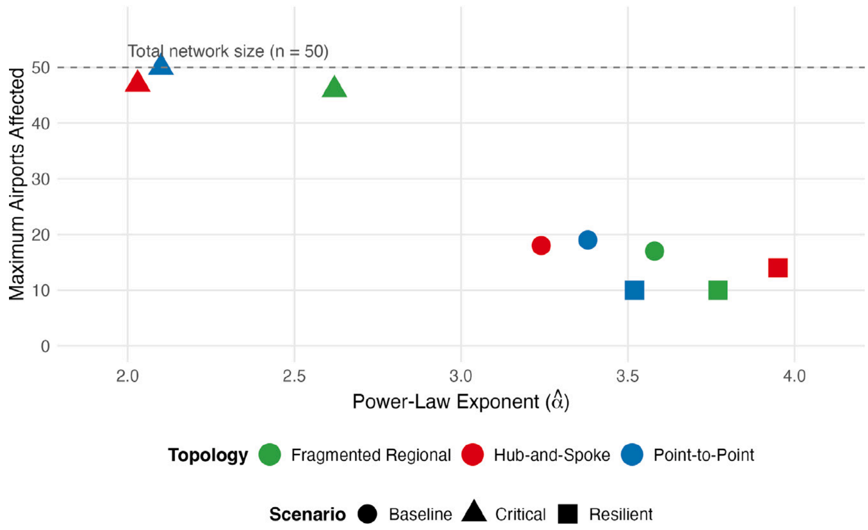


Fig. 6. Relationship between the emergent power-law exponent α and maximum cascade size. Critical scenarios cluster in the high-risk region ($\alpha < 2.7$, >90% affected), while resilient scenarios remain in the contained-risk region ($\alpha > 3.5$, <30% affected).

5. SOC-based early warning system

5.1. Monte Carlo shock testing framework

We develop an early warning system using Monte Carlo shock testing to quantify airport risk along two dimensions. For each airport, we simulate forced failures across multiple independent system states primed to criticality and track cascade propagation.

Contagion risk measures the average number of secondary failures triggered when airport i fails:

$$R_i^{\text{out}} = \frac{1}{N_{\text{tests}}} \sum_{t=1}^{N_{\text{tests}}} |V_i^{(t)}| \tag{1}$$

where $V_i^{(t)}$ is the set of downstream victims in trial t. *Susceptibility risk* counts the unique trigger airports whose failure causes airport j to fail:

$$R_j^{\text{in}} = \left| \left\{ i : \exists\, t \text{ s.t. } j \in V_i^{(t)} \right\} \right| \tag{2}$$

These metrics define four intervention quadrants (Fig. 7): **Full Protection** (high contagion and susceptibility), **Pre-position Resources** (high contagion, low susceptibility), **Rerouting Caution** (low contagion, high susceptibility), and **Standard Monitoring** (low both).

The results reveal an asymmetric risk structure. Susceptibility rankings (Fig. 8(b)) confirm that mega-hubs are the most vulnerable—ATL, ORD, DFW, and DEN each fail in response to failures at 38–39 other airports. Their high connectivity exposes them to stress propagation from across the network. Contagion rankings (Fig. 8(a)), however, show that spoke airports generate the largest cascades. Connection-dependent spokes (SNA, MCI, CMH) and origin-heavy spokes (RDU, TPA, SAN) top the rankings because their failures redirect traffic to already-stressed hubs, triggering secondary hub failures that propagate system-wide. The quadrant classification reflects this asymmetry: mega-hubs cluster in Rerouting Caution (vulnerable but contained), while many spokes fall into Pre-position Resources (high cascade potential but structurally insulated). This suggests that interventions should prioritize monitoring spoke airports as cascade triggers, not just protecting hubs.

5.2. Operational integration

For the EWS to deliver practical value, aviation operations centers must implement and calibrate the SOC model using existing data infrastructure.

- *Model calibration.* Centers can calibrate the framework using historical disruption data: (1) construct network topology from published route schedules, (2) estimate β by fitting simulated cascade distributions to historical patterns, and (3) set airport-specific thresholds based on observed capacity utilization. This requires no novel data collection—only systematic analysis of records maintained by FAA and airline systems.

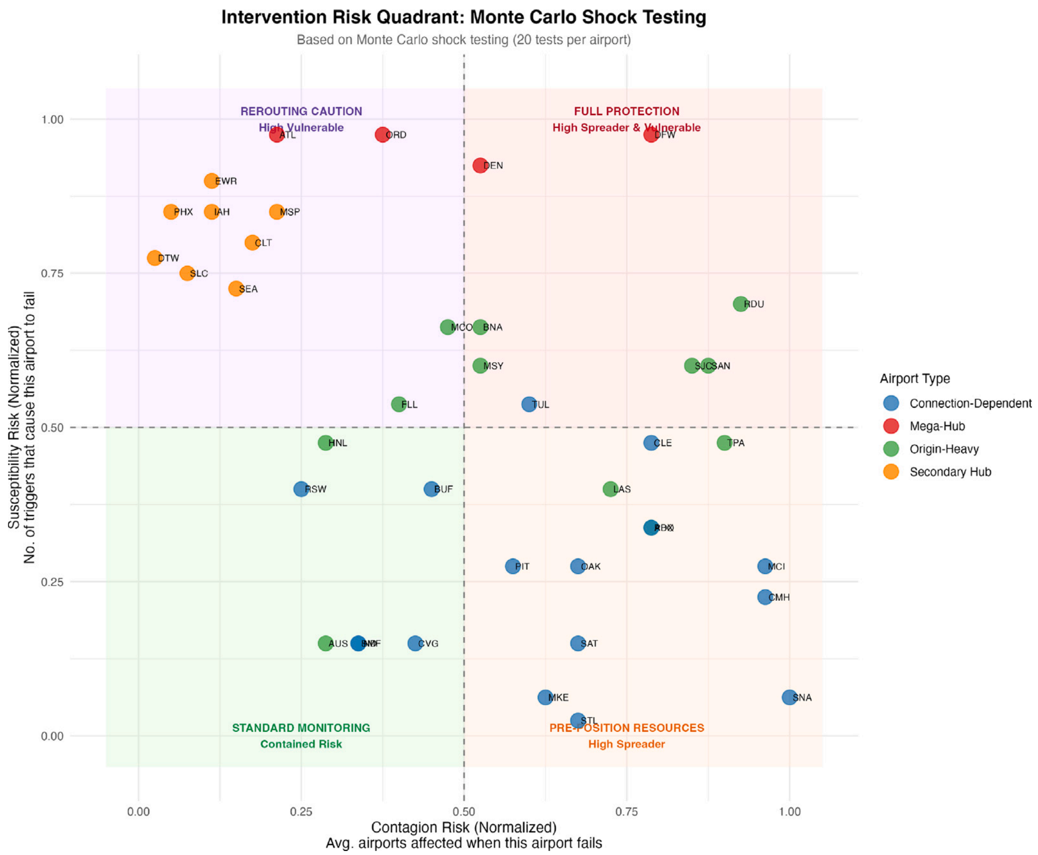
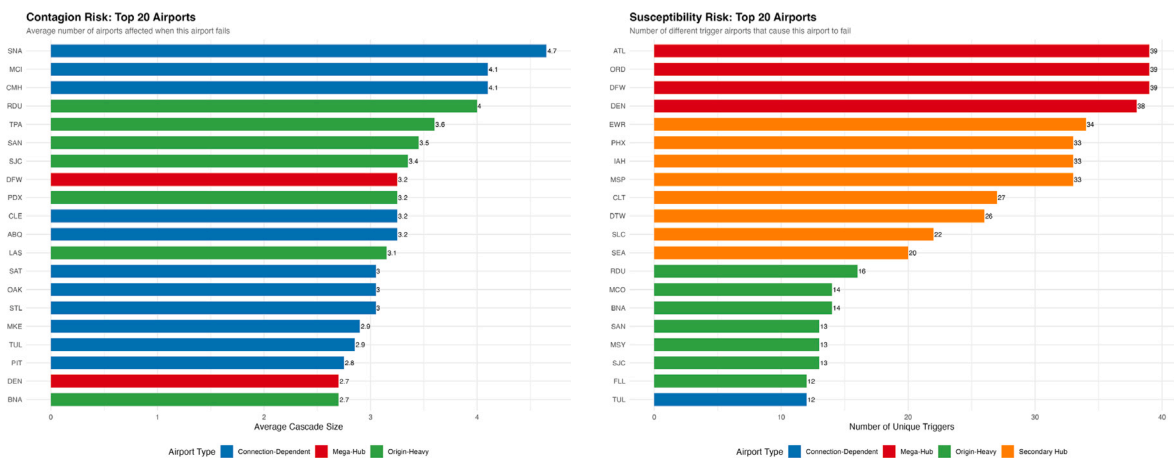
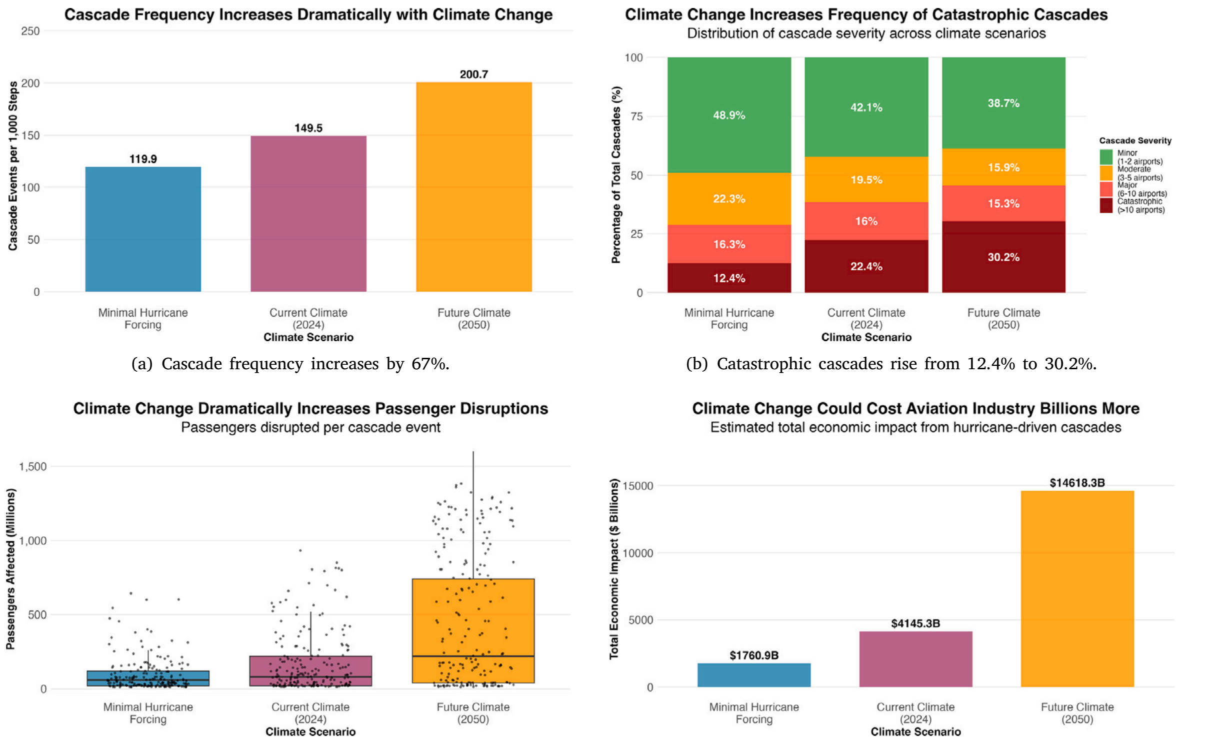


Fig. 7. Intervention risk quadrant from Monte Carlo shock testing. Node colors indicate tier: mega-hubs (red), secondary hubs (orange), origin-heavy (green), and connection-dependent spokes (blue).



(a) Contagion risk ranking (b) Susceptibility risk ranking

Fig. 8. Top 20 airports by (a) contagion risk and (b) susceptibility risk.



(a) Cascade frequency increases by 67%.

(b) Catastrophic cascades rise from 12.4% to 30.2%.

(c) Passenger disruptions increase dramatically.

(d) Economic losses increase 8.3×.

Fig. 9. Climate-driven cascade amplification across four impact dimensions under increasing hurricane intensity.

- *Anticipatory resource allocation.* With a calibrated model, centers can conduct shock testing to identify vulnerable airports *before* disruptions occur, enabling pre-positioning of crews, equipment, and rebooking capacity at high-risk nodes.
- *Real-time decision support.* The risk quadrant classification provides actionable guidance: prioritize ground delay programs at Full Protection airports, activate standby resources at Pre-position nodes, and exercise caution when rerouting to Rerouting Caution airports. These protocols integrate directly with existing Traffic Management Initiatives.

6. Climate vulnerability assessment

The EWS identifies which airports are most vulnerable under current conditions. However, a complete framework must address how vulnerabilities evolve as external stressors intensify. Climate change poses a particular challenge: as extreme weather events become more frequent, systems already near criticality will experience amplified cascade dynamics—not merely proportional increases, but nonlinear shifts in failure size distributions.

To quantify this, we extend our SOC model to incorporate hurricane intensity I_h as a stress-testing parameter. Simulations reveal nonlinear responses to forcing. As shown in Fig. 9(a), cascade frequency climbs from 119.9 under minimal forcing to 149.5 under current climate (+25%) and 200.7 under future conditions (+67%).

Beyond frequency, the size distribution undergoes a regime shift. Under future climate conditions, catastrophic cascades (affecting > 10 airports) rise to 30.2% of all events—2.4× more than under baseline forcing. Economic impacts escalate from $1.76 trillion to $14.6 trillion, an 8.3× increase driven by systemic instability rather than storm severity alone.

The SOC model enables identification of critical nodes by mapping spatially heterogeneous risk:

$$V_{\text{airport}}(I_h) = \begin{cases} 10 \cdot I_h \cdot f_{\text{cascade}} & \text{if hurricane-prone} \\ 2 \cdot I_h \cdot f_{\text{cascade}} & \text{otherwise} \end{cases} \tag{3}$$

Fig. 10 reveals dramatic bifurcation between coastal and inland airports. Key coastal hubs — including ATL, MIA, JFK, MCO, TPA, and IAH — exhibit sharp increases in cascade involvement under future conditions. The five-fold differential between coastal and inland nodes illustrates where targeted resilience investments yield the highest marginal benefit.

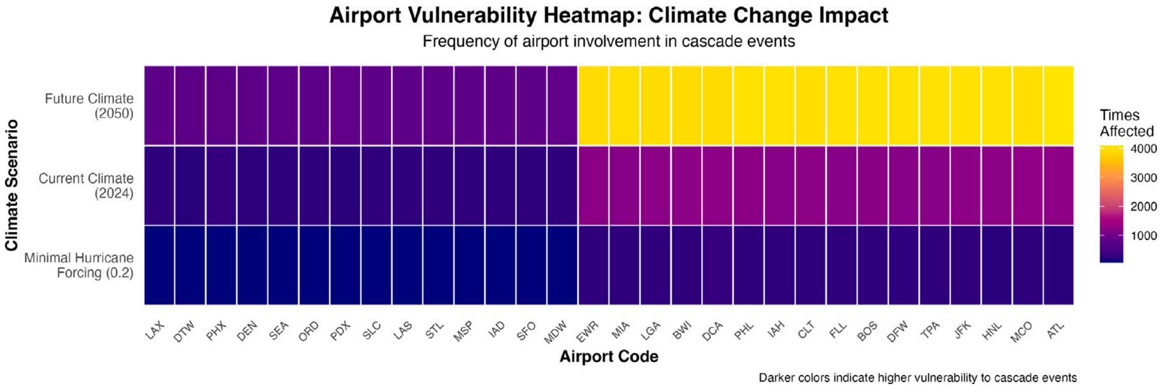


Fig. 10. Airport vulnerability heatmap showing frequency of cascade involvement across climate scenarios. Coastal airports show sharply increasing vulnerability under future conditions.

7. Conclusion

This study demonstrates that modern aviation networks, optimized for efficiency, naturally evolve toward self-organized criticality—a regime where small disruptions can trigger cascading failures with systemic consequences. This *efficiency–resilience paradox* reveals that design choices improving day-to-day performance can undermine shock absorption. Our analysis shows that network structure and operational rules jointly determine disruption scale. Dense interconnectivity and centralized hubs can amplify failures, while modular architectures contain them. Across all simulations, we observe universal power-law behavior: while specific cascades remain unpredictable, the statistical structure of risk is not.

7.1. Managerial insights

The SOC framework provides practitioners with a fundamentally different lens for understanding and managing systemic risk in aviation networks. Unlike scenario-based tools that evaluate specific disruption events, the SOC approach reveals whether a system's architecture makes it inherently fragile or resilient—a distinction that determines outcomes regardless of which specific shock triggers a cascade. For practitioners, the findings translate into actionable guidance:

- *Hub resilience yields system-wide benefits*: Resilience investments at major hubs propagate stability throughout the network. Because mega-hubs sit at the intersection of multiple cascade pathways, improving their capacity buffers reduces β (the fraction of stress redistributed to neighbors), shifting the entire system toward safer power-law regimes.
- *Monitor power-law exponents as early warning indicators*: Declining α values signal approaching criticality and should trigger preemptive interventions. Our analysis shows that the transition from $\alpha \approx 3.5$ (resilient) to $\alpha \approx 2.0$ (critical) corresponds to a shift from contained failures (affecting <30% of airports) to system-wide cascades (affecting >90%). Regular estimation of α from operational disruption data provides a leading indicator that conventional metrics miss.
- *Plan for systemic climate impacts*: Climate adaptation must account for cascade amplification, not just isolated storm damage. Our stress-testing shows that a linear increase in hurricane intensity produces an 8.3× increase in economic losses through nonlinear cascade dynamics. Infrastructure investments should target cascade pathways, not just storm-exposed airports.
- *Target coastal hubs*: Hurricane-prone coastal airports dominate cascade pathways and warrant geographically targeted investment. The five-fold vulnerability differential between coastal and inland airports (Fig. 10) identifies where marginal resilience investments yield the highest systemic returns.
- *Design for containment*: Modular architectures with sparse inter-regional links limit cascade propagation. The fragmented regional topology achieves $\alpha = 2.62$ under critical conditions versus $\alpha = 2.03$ for hub-and-spoke—demonstrating that network structure can be deliberately designed to contain cascades through architectural choices, not just operational buffers.

These insights represent a paradigm shift from reactive crisis management to proactive architectural resilience. The goal is not to prevent all failures — an impossibility in complex systems — but to ensure the network operates in a regime where failures remain contained rather than cascading.

7.2. Limitations and future directions

Several limitations motivate future research:

- *Static network assumption*: Real aviation systems adapt dynamically through rerouting and capacity reallocation. Adaptive SOC extensions would enable simulation of real-time mitigation.

- *Human and organizational factors*: Crew decisions, ATC interventions, and airline policies can mitigate or exacerbate cascades. Agent-based extensions could address this gap.
- *Infrastructure interdependencies*: Aviation depends on IT systems, fuel logistics, and ground transportation. Multi-layer network models represent a promising direction.
- *Empirical validation*: While $\alpha \approx 2.4$ provides indirect calibration, granular propagation data would enable direct parameter estimation.

Despite these limitations, the SOC framework provides a rigorous foundation for understanding systemic risk. The goal is not to prevent all failures, but to understand how risk emerges, where it concentrates, and how systems can be made robust to the unpredictable dynamics of an interconnected world.

CRediT authorship contribution statement

Mary Lai O. Salvaña: Writing – review & editing, Writing – original draft, Visualization, Methodology, Formal analysis, Data curation, Conceptualization. **Harold Jay M. Bolingot:** Methodology, Investigation, Conceptualization. **Gregory L. Tangonan:** Writing – review & editing, Writing – original draft, Methodology, Investigation, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

[1] A.B.C. News, Southwest Airlines Holiday Meltdown Will Cost Company up to $825 Million, ABC News, 2023, URL: https://abcnews.go.com/Business/southwest-airlines-holiday-meltdown-cost-company-825-million/story?id=96261607.
[2] C.N.N. Travel, FAA System Outage Causes Thousands of Flight Delays and Cancellations Across the US, CNN, 2023, URL: https://www.cnn.com/travel/article/faa-computer-outage-flights-grounded.
[3] The Washington Post, Threat of Hurricane Ian cancels more than 3000 flights in Florida, 2022, The Washington Post, URL: https://www.washingtonpost.com/travel/2022/09/28/hurricane-ian-flight-cancellations/.
[4] C. Perrow, Normal Accidents: Living with High-Risk Technologies, Basic Books, New York, USA, 1984.
[5] L.K. Comfort, Shared Risk: Complex Systems in Seismic Response, Pergamon, New York, USA, 1999.
[6] P. Bak, C. Tang, K. Wiesenfeld, Self-organized criticality: An explanation of the 1/f noise, Phys. Rev. Lett. 59 (4) (1987) 381–384.
[7] Bureau of Transportation Statistics, TranStats, 2025, URL: https://www.transtats.bts.gov/.
[8] M.L.O. Salvaña, G.L. Tangonan, Predicting power grid failures using self-organized criticality: A case study of the Texas grid (2014–2022), 2025, arXiv preprint arXiv:2504.10675.
[9] D. Alexander, A magnitude scale for cascading disasters, Int. J. Disaster Risk Reduct. 30 (2018) 180–185.
[10] G. Pescaroli, D. Alexander, A definition of cascading disasters and cascading effects: Going beyond the "toppling dominos" metaphor, Planet@ Risk 3 (1) (2015) 58–67.
[11] G. Pescaroli, D. Alexander, Understanding compound, interconnected, interacting, and cascading risks: a holistic framework, Risk Anal. 38 (11) (2018) 2245–2257.
[12] J.C. Gill, B.D. Malamud, Hazard interactions and interaction networks (cascades) within multi-hazard methodologies, Earth Syst. Dyn. 7 (3) (2016) 659–679.
[13] S.L. Cutter, Compound, cascading, or complex disasters: What's in a name? Environ.: Sci. Policy Sustain. Dev. 60 (6) (2018) 16–25.
[14] M.C. De Ruiter, A. Couasnon, M.J. van den Homberg, J.E. Daniell, J.C. Gill, P.J. Ward, Why we can no longer ignore consecutive disasters, Earth's Futur. 8 (3) (2020) e2019EF001425.
[15] J. Lawrence, P. Blackett, N.A. Cradock-Henry, Cascading climate change impacts and implications, Clim. Risk Manag. 29 (2020) 100234.
[16] O. Ilalokhoin, R. Pant, J.W. Hall, A model and methodology for resilience assessment of interdependent rail networks–case study of Great Britain's rail network, Reliab. Eng. Syst. Saf. 229 (2023) 108895.
[17] G. Pescaroli, A. Suppasri, L. Galbusera, Progressing the research on systemic risk, cascading disasters, and compound events, Prog. Disaster Sci. 22 (2024) 100319.
[18] J. Cuartas, T. Frazier, E. Wood, The application of cascading consequences for emergency management operations, Nat. Hazards 108 (3) (2021) 2919–2938.
[19] S. Huang, C. Li, Coordination of preventive, emergency and restoration dispatch against cascading failures for resilience enhancement, Int. J. Electr. Power Energy Syst. 160 (2024) 110136.
[20] C. Leppold, H. Morrice, K. Brady, L. Reifels, S. Abeysinghe, P. Quinn, L. Gibbs, Recovery work in cascading and compounding disasters: A qualitative study of community recovery workers in Australia, Int. J. Disaster Risk Reduct. 116 (2025) 105152.
[21] S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, S. Havlin, Catastrophic cascade of failures in interdependent networks, Nature 464 (7291) (2010) 1025–1028.
[22] J. Gao, S.V. Buldyrev, H.E. Stanley, S. Havlin, Networks formed from interdependent networks, Nat. Phys. 8 (1) (2012) 40–48.
[23] D.D. Woods, D.L. Alderson, Progress toward resilient infrastructures: Are we falling behind the pace of events and changing threats? J. Crit. Infrastruct. Policy 2 (2) (2021) 5–18.
[24] J. Verschuur, E.E. Koks, J.W. Hall, Systemic risks from climate-related disruptions at ports, Nat. Clim. Chang. 13 (8) (2023) 804–806.
[25] H. Inoue, Y. Todo, Firm-level propagation of shocks through supply-chain networks, Nat. Sustain. 2 (9) (2019) 841–847.
[26] T. Notteboom, T. Pallis, J.-P. Rodrigue, Disruptions and resilience in global container shipping and ports: the COVID-19 pandemic versus the 2008–2009 financial crisis, Marit. Econ. Logist. 23 (2) (2021) 179.

[27] T. Notteboom, H. Haralambides, K. Cullinane, The Red Sea Crisis: ramifications for vessel operations, shipping networks, and maritime supply chains, Marit. Econ. Logist. 26 (1) (2024) 1–20.

[28] G.B. Gratton, P.D. Williams, A. Padhra, S. Rapsomanikis, Reviewing the impacts of climate change on air transport operations, Aeronaut. J. 126 (1295) (2022) 209–221.

[29] R.G. Little, Managing the Risk of Aging Infrastructure, IRGC, Public Sector Governance of Emerging Risks Council, Infrastructure Case, 2012.

[30] Y. Guo, F. Liu, J.-S. Song, S. Wang, Supply chain resilience: A review from the inventory management perspective, Fundam. Res. 5 (2) (2025) 450–463.

[31] S.J. Sutanto, C. Vitolo, C. Di Napoli, M. D'Andrea, H.A. Van Lanen, Heatwaves, droughts, and fires: Exploring compound and cascading dry hazards at the pan-European scale, Environ. Int. 134 (2020) 105276.

[32] A. AghaKouchak, L.S. Huning, F. Chiang, M. Sadegh, F. Vahedifard, O. Mazdiyasni, H. Moftakhari, I. Mallakpour, How do natural hazards cascade to cause disasters? Nature, 2018, URL: https://www.nature.com/articles/d41586-018-06783-6.

[33] A. AghaKouchak, F. Chiang, L.S. Huning, C.A. Love, I. Mallakpour, O. Mazdiyasni, H. Moftakhari, S.M. Papalexiou, E. Ragno, M. Sadegh, Climate extremes and compound hazards in a warming world, Annu. Rev. Earth Planet. Sci. 48 (1) (2020) 519–548.

[34] K. Barquet, M. Englund, K. Inga, K. André, L. Segnestam, Conceptualising multiple hazards and cascading effects on critical infrastructures, Disasters 48 (1) (2024) e12591.

[35] R. Hoff, R. Sparks, M. Chester, A. Mustafa, N. Johnson, A. Birchfield, T. McPhearson, R. Li, N. Ahmad, I. Searles, Cascading failure propagation and perfect storms in interdependent infrastructures, ASCE OPEN: Multidiscip. J. Civ. Eng. 3 (1) (2025) 04025001.

[36] M. Shimizu, A.L. Clark, Interconnected risks, cascading disasters and disaster management policy: a gap analysis, Planet@ Risk 3 (2) (2015).

[37] Z. Gong, Y. Wang, G. Wei, L. Li, W. Guo, Cascading disasters risk modeling based on linear uncertainty distributions, Int. J. Disaster Risk Reduct. 43 (2020) 101385.

[38] E. Mühlhofer, E.E. Koks, C.M. Kropf, G. Sansavini, D.N. Bresch, A generalized natural hazard risk modelling framework for infrastructure failure cascades, Reliab. Eng. Syst. Saf. 234 (2023) 109194.

[39] P. Tang, W. Zhong, J. Wen, S. Shao, D. Zhou, S. Huang, Developing and understanding cascading effects scenario of typhoons in coastal mega-cities from system perspectives for disaster risk reduction: A case study of Shenzhen, China, Int. J. Disaster Risk Reduct. 92 (2023) 103691.

[40] F. Chen, H. Jia, E. Du, Y. Chen, L. Wang, Modeling of the cascading impacts of drought and forest fire based on a Bayesian network, Int. J. Disaster Risk Reduct. 111 (2024) 104716.

[41] M. Gordan, D.A. Kountche, D. McCrum, S. Schauer, S. König, S. Delannoy, L. Connolly, M. Iacob, N.G. Durante, Y. Shekhawat, C. Carrasco, T. Katsoulakos, P. Carroll, Protecting critical infrastructure against cascading effects: The PRECINCT approach, Resilient Cities Struct. 3 (3) (2024) 1–19.

[42] M. Diakakis, A. Sarantopoulou, M. Gogou, C. Filis, P. Nastos, I. Kapris, E. Vassilakis, A. Konsolaki, E. Lekkas, Cascade effects induced by extreme storms and floods: The case of Storm Daniel (2023) in Greece, Water 17 (7) (2025) 912.

[43] P. Liu, P. Liu, Y. Yang, J. Wu, G. Tian, Z. Zhang, L. Chai, Risk analysis and mitigation strategy of power system cascading failure under the background of weather disaster, Processes 13 (1) (2025) 45.

[44] L.G. Brunner, R. Peer, C. Zorn, R. Paulik, T. Logan, Understanding cascading risks through real-world interdependent urban infrastructure, Reliab. Eng. Syst. Saf. 241 (2024) 109653.

[45] R. Lee, C.J. White, M.S.G. Adnan, J. Douglas, M.D. Mahecha, F.E. O'Loughlin, E. Patelli, A.M. Ramos, M.J. Roberts, O. Martius, E. Tubaldi, B. van den Hurk, P.J. Ward, J. Zscheischler, Reclassifying historical disasters: From single to multi-hazards, Sci. Total Environ. 912 (2024) 169120.

[46] M. Kumasaki, M. King, M. Arai, L. Yang, Anatomy of cascading natural disasters in Japan: main modes and linkages, Nat. Hazards 80 (2016) 1425–1441.

[47] T.J. Huggins, F. E, K. Chen, W. Gong, L. Yang, Infrastructural aspects of rain-related cascading disasters: a systematic literature review, Int. J. Environ. Res. Public Health 17 (14) (2020) 5175.

[48] B. Li, C. Liu, Y. Yin, Q. Jiang, Y. Zhang, T. Liu, Study on power system resilience assessment considering cascading failures during wildfire disasters, Energy Rep. 13 (2025) 1819–1833.

[49] D. Purwar, J. Flacke, E.A. Guzman, R. Sliuzas, A qualitative analysis of cascading effects of critical infrastructure service failure post torrential floods in formal & informal settlement: the study-case of Medellin city, Colombia, Sustain. Resilient Infrastruct. 9 (5) (2024) 496–512.

[50] C. Adami, Self-organized criticality in living systems, Phys. Lett. A 203 (1) (1995) 29–32.

[51] M.J. Aschwanden, N.B. Crosby, M. Dimitropoulou, M.K. Georgoulis, S. Hergarten, J. McAteer, A.V. Milovanov, S. Mineshige, L. Morales, N. Nishizuka, G. Pruessner, R. Sanchez, A.S. Sharma, A. Strugarek, V. Uritsky, 25 years of self-organized criticality: solar and astrophysics, Space Sci. Rev. 198 (2016) 47–166.

[52] K. Bhattacharya, S. Manna, Self-organized critical models of earthquakes, Phys. A 384 (1) (2007) 15–20.

[53] K. Chen, P. Bak, S. Obukhov, Self-organized criticality in a crack-propagation model of earthquakes, Phys. Rev. A 43 (2) (1991) 625.

[54] A. Sornette, D. Sornette, Self-organized criticality and earthquakes, Europhys. Lett. 9 (3) (1989) 197.

[55] S. Hergarten, H.J. Neugebauer, Self-organized criticality in a landslide model, Geophys. Res. Lett. 25 (6) (1998) 801–804.

[56] A.E. Biondo, A. Pluchino, A. Rapisarda, Modeling financial markets by self-organized criticality, Phys. Rev. E 92 (4) (2015) 042814.

[57] J.-P. Bouchaud, The self-organized criticality paradigm in economics & finance, 2024, arXiv preprint arXiv:2407.10284.

[58] J.A. Scheinkman, M. Woodford, Self-organized criticality and economic fluctuations, Am. Econ. Rev. 84 (2) (1994) 417–421.

[59] J. Hesse, T. Gross, Self-organized criticality as a fundamental property of neural systems, Front. Syst. Neurosci. 8 (2014) 166.

[60] D. Plenz, T.L. Ribeiro, S.R. Miller, P.A. Kells, A. Vakili, E.L. Capek, Self-organized criticality in the brain, Front. Phys. 9 (2021) 639389.

[61] R. Ramos, R. Sassi, J.R.C. Piqueira, Self-organized criticality and the predictability of human behavior, New Ideas Psychol. 29 (1) (2011) 38–48.

[62] S.A. Levin, Self-organization and the emergence of complexity in ecological systems, BioScience 55 (12) (2005) 1075–1079.

[63] J.E. Gang, W. Jia, I.A. Herniter, Sand and fire: applying the sandpile model of self-organised criticality to wildfire mitigation, Int. J. Wildland Fire 31 (9) (2022) 847–856.

[64] B.A. Carreras, D.E. Newman, I. Dobson, A.B. Poole, Evidence for self-organized criticality in a time series of electric power system blackouts, IEEE Trans. Circuits Syst. I. Regul. Pap. 51 (9) (2004) 1733–1740.

[65] I. Dobson, B.A. Carreras, V.E. Lynch, D.E. Newman, Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization, Chaos Interdiscip. J. Nonlinear Sci. 17 (2) (2007).

[66] CNN, Major power outage hits New York, other large cities, 2003, URL: https://www.cnn.com/2003/US/08/14/power.outage/.

[67] New York Independent System Operator, A look back at the Northeast blackout of 2003 and lessons learned, 2023, URL: https://www.nyiso.com/-/a-look-back-at-the-northeast-blackout-of-2003-and-lessons-learned.

Mary Lai O. Salvaña is an Assistant Professor of Statistics at the University of Connecticut (UConn). Prior to joining UConn, she was a Postdoctoral Fellow at the Department of Mathematics at University of Houston. She received her Ph.D. in Statistics at the King Abdullah University of Science and Technology (KAUST), Saudi Arabia. She obtained her BS and MS degrees in Applied Mathematics from Ateneo de Manila University, Philippines, in 2015 and 2016, respectively. Her research interests include extreme and catastrophic events, risks, disasters, spatial and spatio-temporal statistics, environmental statistics, computational statistics, large-scale data science, and high-performance computing.

Harold Jay M. Bolingot holds a Bachelor of Science in Computer Engineering from Ateneo de Manila University, Philippines, and a Master of Engineering in Assistive Robotics from Kyushu Institute of Technology, Japan. His research expertise lies in machine learning, with a focus on convolutional neural networks, computer vision, and biomedical signal processing.

Gregory L. Tangonan graduated in Physics from Ateneo de Manila University and earned his PhD in Applied Physics from the California Institute of Technology. He spent 32 years at Hughes Research Laboratories in Malibu, California, retiring as Lab Director of the Communications Laboratory. His expertise spans fiber optics, wireless communications, materials science, and complex systems science. He has published over 200 papers and holds 49 U.S. patents. After retiring, he returned to his alma mater and founded the Ateneo Innovation Center (AIC), which is actively engaged in disaster risk and resilience research. AIC has developed Resilience Hubs for nationwide deployment in the Philippines and has been at the forefront of research on cascaded disasters and risk assessment.