International Journal of Recent Advances in Multidisciplinary Topics
Volume 7, Issue 2, February 2026
www.ijramt.com | E-ISSN: 2582-7839 | RESAIM Publishing | www.resaim.com

Beyond a Threshold: Diminishing Resilience Gains from Additional Fiber Exit Paths Under Correlated Weather Disturbances

Huneef Mohammad Sofi*
Jio, India

***Abstract*: Telecommunication network resilience strategies frequently assume that increasing the number of geographically diverse terrestrial fiber exit paths proportionally improves availability and survivability. This assumption breaks down under correlated weather disturbances such as basin-wide floods, cloudbursts, landslides, cyclonic envelopes, and heat-driven failures, which can impair multiple routes simultaneously and constrain restoration access. This paper introduces an orthogonal risk-domain framing: resilience gains depend less on the number of terrestrial paths and more on the number of decorrelated Orthogonal Spatial Risk Zones (OSRZ) a geography can realistically support. Once OSRZ saturates—often around 4 in mountainous regions and 5 in well-connected central regions—additional terrestrial exits largely replicate existing risk domains and provide negligible improvement under widespread events. We conclude that seamless continuity of globally distributed Internet services requires a layered approach: (i) adding orthogonal risk domains such as OPGW/power corridors and satellite as an emergency layer, and (ii) weather hardening ("bulletproofing") of both terrestrial and OPGW routes, since redundancy alone is limited by common-cause failures and correlated regional hazards.**

***Keywords*: Network resilience, correlated failures, climate risk, fiber diversity, OSRZ, OPGW, satellite backup, hardening, redundancy saturation.**

1. Introduction

Extreme weather events increasingly disrupt telecom infrastructure through physical damage to outside plant (OSP), prolonged power failures, and access limitations that extend restoration times. A common resilience response is adding more terrestrial fiber exits under the assumption that more routes reduce isolation probability. Yet severe outages frequently show multi-route simultaneous failures because routes share correlated exposure (basins, slope systems, bridges, tunnels, and shared access corridors), defeating classical independence assumptions. This paper argues that the true design goal is not "more paths," but "more orthogonal risk domains," followed by hardening of those domains to survive widespread hazards while maintaining global Internet reachability.

2. Background and Related Work

Regional failure modeling in communication networks emphasizes geographically correlated failure events and shared-risk structures (e.g., SRLG and probabilistic SRLG), highlighting that disasters can remove multiple links within a geographic region. Reliability theory warns that common-cause failures can defeat redundancy, placing a practical ceiling on reliability gains achievable purely by adding redundant elements. Practitioner resilience guidance stresses that redundancy must be complemented by customized hardening measures, disaster recovery, and service continuity planning under climate-driven hazards.

3. Conceptual Framework

A. Correlated Failure Domains (CFDs)

A Correlated Failure Domain (CFD) is a spatial-temporal region in which a single disturbance can simultaneously impair multiple infrastructure elements (ducts, aerial spans, crossings, access roads, and power feeds). Regional hazards—flood basins, landslide belts, cyclone envelopes—create correlated disruptions across multiple "diverse" paths.

B. Orthogonal Spatial Risk Zones (OSRZ)

OSRZ represent the effective number of decorrelated spatial hazard corridors available for routing exits from a geography. OSRZ depends on the N–S/E–W spread of feasible exits, corridor topology (valleys, ridges, roads, rail, power), and whether separation is large relative to hazard footprints. Mountainous geographies typically constrain OSRZ to ~4, while well-connected central regions may approach ~5.

C. Resilience Saturation Threshold (RST)

RST is the exit-path count beyond which adding another terrestrial path no longer increases OSRZ, meaning the new route mostly replicates an existing risk domain. Beyond RST, widespread events dominate failure outcomes and marginal gains diminish sharply.

*Corresponding author: huneef111@gmail.com

4. Results

A. OSRZ Saturation (Mountain vs Central)

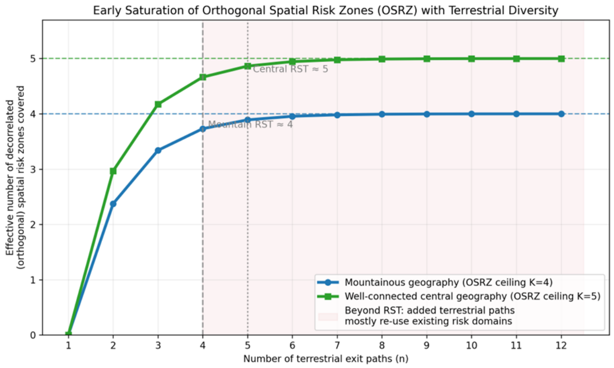

Fig. 1. Early saturation of OSRZ with terrestrial diversity. Mountainous geographies typically saturate around K≈4; well-connected central geographies may saturate around K≈5. Beyond these thresholds (RST), additional terrestrial exits reuse existing spatial risk domains and do not meaningfully add decorrelated resilience

B. CFD-Wide Floor and Isolation Plateau (Illustrative)

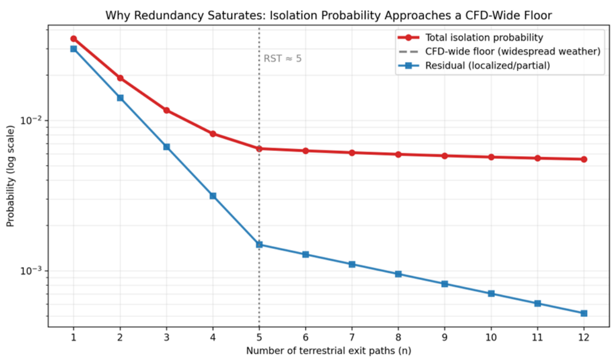

Fig. 2. Conceptual decomposition: total isolation probability approaches a CFD-wide floor during widespread weather events, while the residual (localized/partial) component decays with added diversity. After RST, the CFD-wide term dominates, explaining diminishing returns. (Illustrative decision-support plot.)

C. Post-RST Investment Priorities (Illustrative)

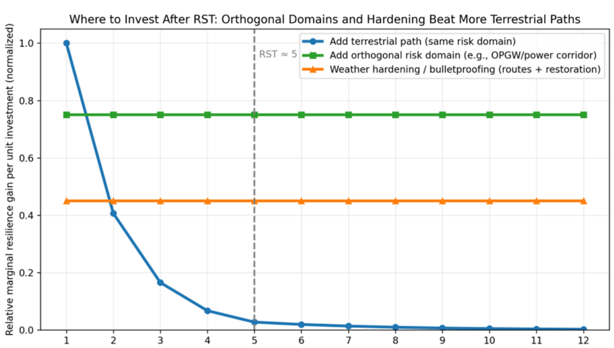

Fig. 3. Relative marginal resilience gain per unit investment (conceptual). Beyond RST, an additional terrestrial exit in the same risk domain yields low benefit compared to adding an orthogonal risk domain (e.g., OPGW/power corridor) and weather hardening (bulletproofing routes + restoration readiness). (Illustrative decision-support plot.)

5. Design Principle: Stop Replicating Domains—Add Orthogonal Domains

Once OSRZ saturates, additional terrestrial paths tend to replicate the same corridor class (same basin, slope system, shared crossings/access). Regional and common-cause events can disable all "redundant" copies if they share the same external stressor. Therefore, design reviews should explicitly ask whether a new path adds a new decorrelated domain or only adds another instance inside an existing domain.

6. Weather Hardening ("Bulletproofing") and Orthogonal Domains

A. Why Hardening is Required for Seamless Internet Continuity

Telecommunications underpin critical services and disaster response; widespread outages can halt access to data applications and disrupt emergency operations. Because Internet services are globally distributed (cloud, content, DNS, peering), maintaining continuity requires robust upstream interconnection; redundancy without hardening can still fail under wide-area hazards and access constraints.

B. Terrestrial Fiber Hardening Measures (Engineering + Operations)

- Civil/route hardening: ducting/conduit and appropriate burial depth on vulnerable stretches; detectable markers and accurate as-builts to reduce accidental digs and shorten restoration time.
- Resilient crossings: trenchless crossings (HDD/boring) for roads/rivers and flood-prone structures; prioritize river approaches and washout-prone sections.
- Hotspot hardening and micro-segmentation: identify landslide belts, bridge/tunnel approaches, and heat-stressed duct segments; reinforce and segment for faster isolation and repair.
- Cable/closure hardening: water-blocked designs, sealed closures, bend-radius discipline; armored/reinforced solutions in high mechanical-risk/rodent-risk zones.
- Restoration velocity: pre-stage spares, closures, tools, and workforce plans; maintain monitoring, fault localization, and access playbooks for monsoon windows.

C. OPGW as an Orthogonal Domain (and Why it Also Must Be Hardened)

OPGW integrates optical fibers within the overhead ground wire of power transmission lines and often follows a right-of-way structurally different from road/valley telecom ducts. This makes OPGW a strong orthogonal risk domain, but it must be engineered and maintained for wind/ice loading, tower integrity, corrosion, and maintainable splice access.

- Mechanical integrity: fittings, vibration control, tension management, and periodic inspections/testing.
- Environmental durability: corrosion-resistant

materials and inspection cycles suited to the local environment.

- Maintainable splicing strategy: splice points and joint boxes placed for accessibility during adverse weather; spares and restoration planning aligned with power-corridor access.

D. Satellite as a Separate Orthogonal Risk Domain (Emergency Layer)

Satellite-based connectivity (GEO/MEO/LEO) represents a separate orthogonal risk domain because it is not co-located with terrestrial corridors and therefore remains available when floods, landslides, or corridor washouts sever multiple ground routes. However, satellite is not yet engineered to replace terrestrial or OPGW transport for high-volume Internet backhaul at scale: aggregate capacity is shared across wide coverage cells and depends on spectrum reuse constraints, and the satellite network typically relies on ground stations to tie into the Internet backbone. As a result, satellite is best positioned today as an emergency-grade continuity layer (lifeline connectivity, control-plane reachability, limited essential services) rather than a full replacement for the multi-Tbps terrestrial transport required for modern broadband demand and economic return on investment.

7. Conclusion

Resilience gains from terrestrial fiber exit paths saturate once a geography's orthogonal spatial risk zones are exhausted—often around 4 in mountainous regions and 5 in well-connected central regions. Beyond RST, additional terrestrial exits mostly replicate existing risk domains and deliver limited incremental benefit under widespread weather events. Seamless continuity for globally distributed Internet services requires adding orthogonal risk domains (e.g., OPGW/power corridors and satellite as an emergency layer) and weather hardening of terrestrial and OPGW corridors, since correlated hazards and common-cause failures can defeat redundancy unless infrastructure and restoration are engineered for climate stress.

References

[1] World Bank, Resilient Telecommunications Infrastructure: A Practitioner's Guide, 2024.
[2] Nokia (Bell Labs Consulting), *Making Networks Resilient to Climate Change*, white paper.
[3] U.S. Department of Homeland Security, Implications of Extreme Weather Events on U.S. Telecommunications Infrastructure, 2024.
[4] The Fiber Optic Association (FOA), Outside Plant Construction Guide: Underground Construction.
[5] Corning Inc., Direct-Buried Installation of Fiber Optic Cable, Recommended Procedure.
[6] H. W. Jones, Common Cause Failures and Ultra Reliability, NASA Technical Report.
[7] B. Vass et al., How to Model and Enumerate Geographically Correlated Failure Events in Communication Networks, Springer.
[8] International Telecommunication Union (ITU), *Emergency Telecommunications*, backgrounder.
[9] Fiber Broadband Association, "Technical Assessment of LEO Satellite Broadband," *Broadband Technologies Review*, public-domain model, Nov. 2024.
[10] Satellite Industry Association, *Satellite Communications in Disaster Relief*, 2019.