Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p26573-cd

Resilience Assurance for Critical Systems: Lessons from the 2025 Interlock Whole-of-State Infrastructure and Public Safety Summit

Vincent P. Paglioni

Risk, Reliability, & Resiliency Characterization (R3C) Lab, Department of Systems Engineering, Colorado State University. Fort Collins, CO, USA. Vincent.paglioni@colostate.edu

Graeme W. Troxell

Blue Green Decisions Lab, Department of Systems Engineering, Colorado State University. Fort Collins, CO, USA. G.troxell@colostate.edu

Critical infrastructure systems, spanning domains including water, electricity, transportation, and communications, are the centerpiece of modern quality of life, national and international security. Traditionally, reliability has been used as a primary measurand of system health and functionality, facilitating the development of robust methods for evaluating systems. However, novel threat vectors, increasing system complexity, and deeper cross-domain interconnections reinforce a growing interest in *resilience*, rather than reliability, as the principal measurement of system safety. The recent "Interlock: Whole-of-State Infrastructure and Public Safety Summit," held in Denver, Colorado in September 2025, brought together experts from across infrastructure domains to discuss the achievement of resilience. This work presents the lessons learned from those discussions regarding the apparent roadblocks to achieving system resilience, and outlines potential strategies to implementing system resilience approaches. Infrastructure systems across the globe are becoming more complex, more tightly coupled, and subject to expanding natural and anthropogenic threats. While it is increasingly clear that resilience is a critical system characteristic, gaps in resilience theory and application have hindered the development of resilience-centered approaches to systems engineering. This work provides the foundations to overcome some of these barriers, and suggests continued areas of research for establishing resilience engineering as a coherent science.

Keywords: Resiliency, Systems Engineering, Critical Infrastructure

1. Introduction

Critical infrastructure systems are the core of the global economy and serve fundamental roles for national and international security. As a result, the ability of these systems to withstand and/or overcome failures is absolutely necessary. As system complexity increases, e.g., with the introduction/proliferation of hyperconnectivity through the "Internet of Things" (IoT), the failure behaviors of these systems also grow in complexity, and it becomes increasingly difficult to ensure and verify the non-occurrence of failure – i.e., the system reliability. As a result, there are some who now advocate that resiliency, rather than reliability, be viewed as the key metric of system success (Paglioni et al. 2025). That is, as the non-occurrence of failure (reliability) becomes less achievable, the focus of engineers should shift to the ability to overcome failure.

However, there are real challenges associated with the shift from reliability to resiliency. These challenges were highlighted at the 2025 Interlock Whole-of-State Infrastructure and Public Safety Summit ("Interlock"), held in Denver Colorado in September 2025. Interlock was a collaborative, multidomain exercise designed to coalesce expertise from across infrastructure domains and strengthen critical connections between domains and civil government. Discussions held at Interlock elucidated the current pressing demands and challenges facing critical systems for ensuring resiliency.

This paper presents a brief background of resiliency as a concept for critical infrastructure and its growing importance. Then, we discuss the lessons learned from the 2025 Interlock summit. Finally, we present critical areas of further

research that will enable actionable resiliency approaches for critical infrastructure.

2. Resiliency

Despite the importance of resiliency to modern systems, resiliency remains a fuzzily-defined concept in engineering (Paglioni 2024; Paglioni et al. 2026). This fuzzy definition is, at least in part, at the root of challenges related to promoting resiliency across system domains. Resiliency is closely related to other system characteristics or "ilities," most notably reliability. However, resiliency is a distinct concept.

The *reliability* of a system is the probability that the system operates (fulfils some mission) without failure for a given amount of time under assumed conditions. Thus, reliability is concerned chiefly with the avoidance of failure. Under this perspective, reliability is intimately related to *risk*, which captures the probability (and consequences) of failure (Modarres and Groth 2023). While these are critical system characteristics, neither risk nor reliability considers post-failure actions/events that could have significant impact on the system's overall state.

Resiliency, which can be broadly defined as the ability of systems to withstand or cope with stressors, encompasses *proactive* and *reactive* elements. Systems incorporate proactive resiliency by anticipating and planning for stressors. Reactive resiliency entails responding to and learning from stressors. Resiliency is thus concerned with both pre- and post-failure system behaviors. Resiliency thus encompasses and expands risk and reliability to include the post-failure regime.

2.1. *Ecological vs. engineering resiliency*

Resiliency in practice is often distinguished into *engineering* and *ecological* approaches. The distinction relates to the assumptions of system behaviors. In the classical conceptualization of resiliency (Neubert and Caswell 1997), the system is assumed to possess a single stable equilibrium, to which it ideally returns following a shock. While engineering resiliency allows for system evolution, it ultimately rests on the concept of a single stable equilibrium (Hollnagel et al. 2006; Yodo and Wang 2016). In the engineering perspective, resiliency is measured by the time required to return to the single point of stability (Bodin and Wiman 2004).

Ecological resiliency is rooted in Holling's (1973) initial conceptualization of evolution around multiple stable equilibria and embraces the ability of systems to evolve. In this view, systems can be stable in multiple configurations and go through *panarchy cycles* of growth, conservation, collapse, and ultimate reorganization (Gunderson and Holling 2003).

Both ecological and engineering resiliency perspectives have advantages – principally, realism and modelability, respectively. That is, ecological resiliency comports more closely to real system behaviors. Engineering systems, like natural systems, undergo evolution as components age, get replaced/upgraded, the mission changes, and/or the environment changes. After each evolution (e.g., each maintenance period), the system enters a new stable regime. Thus, capturing system behaviors realistically requires recognizing these multiple equilibria, and so aligns with the ecological perspective of resiliency. Where the engineering resiliency perspective has an advantage is in the practical modelling of systems. The evolutionary processes that govern the system, and the resulting multiple equilibria, are difficult to capture in a tractable system model.

Resiliency engineering, which naturally assumes the engineering perspective, is a growing discipline (Hollnagel 2009; Hollnagel et al. 2011). However, interest in this discipline and the concept of resiliency have not translated into generally usable principles of resiliency practice.

2.2. *Gaps in resiliency*

There are both theoretical and practical roadblocks to the effective implementation of resiliency for engineering systems. At the root of the issue is the lack of a coherent, cohesive definition of resiliency itself. In addition to this, there is the growing issue of system complexity

There are multiple definitions of resiliency available in academic and professional literature. These range from relatively simple and concise statements like "maintaining capability in the face of an adversity" (Brtis et al. 2025) to robust, but clumsy multi-faceted definitions (Paglioni 2024). Despite the obvious similarities across definitions (e.g., the emphasis on proactive and reactive capabilities, the necessity of recovery, etc.), no single comprehensive definition has been offered. This uncertainty of definition complicates the practice of resiliency engineering; in the absence of

robust resiliency standards (which also require a consistent definition), practices have developed inconsistently across domains and organizations.

A related, but distinct, gap in the foundations of resiliency practice relates to the measurement and quantification of resiliency. There is currently no widely-accepted quantitative resiliency metric, although some have been proposed (Mejia-Giraldo et al. 2012; Panteli et al. 2017; Paglioni et al. 2026). Being able to compare resiliency metrics is necessary to enable decision-making both within and across systems. In the absence of a coherent metric, resiliency-enforcing decisions are difficult to validate and defend.

The foundational issues associated with the definition and quantification of resiliency are compounded by practical complications, namely growing complexity and interconnectedness. The separate pursuit of reliability and resiliency as system goals leads to tension as the pursuit of reliability can result in decreased resiliency (via brittleness to unexpected events) or vice-versa (as redundancy complicates system analysis). However, these two concepts are not necessarily at odds, as displayed through high reliability organizations (HRO) which value resiliency and reliability as interconnected characteristics (Sutcliffe 2011).

The issues associated with resiliency in practice are not new, but are taking on new urgency as more, and more severe, threat vectors emerge to endanger critical systems. As critical infrastructure systems become more interconnected, threats can propagate through systems faster and become more damaging. As a result, it is imperative that industry professionals and governance organizations prioritize resiliency in critical infrastructure and develop the means to realize it.

3. Interlock 2025 and Lessons Learned

Resiliency was the major theme of "Interlock 2025: Whole of State Infrastructure and Public Safety Summit," held in Denver, Colorado in September. The event brought together experts from across critical/lifeline infrastructure domains including water, transportation, energy and communications to discuss threats, vulnerabilities, and collaborative solutions.

3.1. *Whole-of-State approach*

The state of Colorado is piloting a *whole-of-state* (WoS) approach to infrastructure safety and security, with the goal of building more resilient infrastructure systems while also reducing the time, talent and effort required from any one organization to ensure resiliency. The focus on interfaces and information sharing brings to bear multidomain expertise to solving infrastructure resiliency issues. The end goal of the WoS approach is to establish a unified, coherent infrastructure protection strategy that works across state, local, tribal and federal agencies.

The WoS approach models the binary nature of resiliency by providing both proactive and reactive capabilities. Cross-domain partnerships feed a centralized data fusion approach that can identify possible failure cascades. This allows all stakeholders to remain cognizant of scenarios and facilitates effective decision-making. The WoS approach facilitates effective responses (reactive resiliency) with a tactical operations center that coordinates emergency response across government agencies and industry partners.

While the WoS approach is certainly a model for success, and is being replicated across the U.S. and elsewhere, there are still issues with its implementation. The lessons shared by partners within the WoS approach point to several concerns going forward.

3.2. *Lessons learned*

The early operation of the WoS approach has resulted in several lessons that can be replicated by any organization interested in taking a similar robust approach to infrastructure resiliency. These lessons relate principally to the broad need for a focused strategic/proactive philosophy and strong governance.

3.2.1. *Proactive strength*

As discussed, one of the hallmarks of the WoS approach mirrors the dual nature of resiliency. However, simply recognizing the need for proactive and reactive approaches is not sufficient to promoting effective behaviors. The WoS approach features clear distinctions between personnel and resources responsible for strategic (proactive) and tactical (reactive) system actions. This helps to ensure that the system – including response personnel – is adequately prepared for shocks/stressors, and that a response can be effectively mounted without delay.

A significant amount of effort is devoted to the strategic/proactive functions of the WoS

approach. This effort starts with a culture of preparedness among participants. Regular training and awareness campaigns (such as Interlock itself) ensure all stakeholders remain situationally aware. The partnerships established by the WoS are fostered and strengthened with advanced planning exercises.

3.2.2. *Governance and organization*

The partnerships established and maintained as part of the WoS approach must exist within a strong governance structure to minimize conflict. The WoS approach establishes clear leadership roles and accountability processes across stakeholders. The governance plans are aligned with higher-level (federal and state) priorities and responsive to funding, which ensures continuity and cohesiveness with other activities.

3.2.3. *Reactive strength*

The final class of replicable lessons offered by WoS is the importance of strong reactive resiliency approaches. A system-wide database with real-time, secure information sharing, the WoS approach ensures that tactical decisions can be made with the best available information and without delay. This is bolstered with the increasing use of predictive analytics to anticipate and mitigate cascading failures. Enabled by the proactive activities of the WoS approach, the reactive approaches ensure that system stressors can be identified, handled, and learned from in a timely and effective manner.

4. Challenges to Resiliency

Beyond the actionable lessons learned from the WoS approach, the Interlock summit elucidated the ongoing challenges with infrastructure resilience. The cross-cutting (across infrastructure domains) challenges identified at Interlock define the risks and critical needs of infrastructure in the current era.

4.1. *Cybersecurity*

One of the most widely-discussed challenges across infrastructure domains was exposure to cyber intrusion and attacks. The era of cybersecurity as a discrete or niche technical concern is over as infrastructure systems are increasingly subject to "smart" control. Further, because infrastructure systems are becoming more interconnected, the cybersecurity risks of one domain quickly become risks to all other domains. In the digital age, as physical infrastructure has become increasingly tied to the digital/cyber domain, cybersecurity has been recognized as a critical piece of resiliency (Hutschenreuter et al. 2021).

The necessity of cybersecurity as a critical concern for physical infrastructure is evidenced by recent events from multiple domains. In 2025, the maritime industry identified cybersecurity as a serious concern following the cyber-induced grounding of the MSC Antonia (Pordham 2025). In August, 2025, a ransomware attack disrupted transportation services in the Maryland Transit Administration (Ng 2025). Power grids and energy infrastructure have long been recognized targets for cyber attacks (Knake 2017), with the latest evidence coming from Sweden (Priya 2025) and potentially Venezuela (Miller 2026).

The cyber realm is no longer separate from the physical, placing many systems – particularly "old fashioned" infrastructure like power and water – at serious risk. These threats are less predictable and less isolable than purely physical threats. Cybersecurity is one of the highest concerns for infrastructure resiliency moving forward.

4.2. *Water-energy nexus*

The vulnerabilities associated with domain interfaces were widely discussed at Interlock. These interfaces serve as blind spots for many practitioners – points where cognizance and situational awareness transition between organizations and threats can more easily materialize and/or propagate.

The water-energy nexus was repeatedly discussed as a concerning fragility and progenitor of systemic risk. These infrastructure systems provide the most basic functions (at least of those typically presented as lifeline infrastructure), and thus present the biggest societal risks if interrupted. Further, the deep interconnections between these systems (water infrastructure needs power, energy infrastructure needs water) enforces tight coupling and fast shock/stress propagation.

The water-energy nexus produces not only technical/infrastructure risks but climate and societal risks. There is growing recognition of the importance of this interface to both infrastructure and climate concerns (Jackson 2025). However,

current practice remains relatively siloed, even for critical concerns like water quality. A WoS approach, however, bridges the practical divide and treats these domains as inherently interconnected. This improves visibility of the interface itself and the ability to respond to threats that propagate across the interface.

4.3. *Building capacity and partnerships*

In addition to technical improvements within and across domains, participants highlighted the need to build trust and coordination between agencies. In most definitions, resiliency encompasses both technical and organizational elements. Thus, building inter-agency partnerships and cross-domain expertise will improve resiliency of the overall infrastructure.

In Colorado's WoS approach, the Colorado Information Analysis Center (CIAC), facilitates information fusion, agency coordination, and communication with the private sector. These are critical capabilities for total system resiliency and ensure that stakeholders have the data necessary to make decisions and effectively communicate.

4.4. *Operationalizing resilience*

The concept of resilience motivated much of the discussion at the Interlock summit as participants recognized the importance of responding to, rather than merely avoiding, shocks. However, conversations largely mirrored the discussion in Section 2 and highlighted the lack of a shared definition for resiliency. Resiliency definitions and processes vary across energy, water, communications and transportation domains.

This variance manifests in the inability to share methodologies across domains, and thus to operationalize cross-domain resilience. Cross-domain interdependencies can introduce vulnerabilities by allowing shocks to propagate quickly, but can also provide system resilience through, e.g., redundancy. However, unleashing this potential requires a common understanding of resiliency and compatible practices so that domain experts can effectively work together.

5. Discussion and Conclusion

Critical infrastructure – whether in the energy, water, transportation or communications domain – is under increasing threats from both cyber and physical sources. As a result, the concept of resiliency is critical to ensuring the continuity of our quality of life and global security. The 2025 Interlock Summit brought together experts from across infrastructure domains and government agencies to discuss the threats facing infrastructure and solutions to build resiliency. This paper summarized the main lessons learned at this summit, which established the foundation for future work that will facilitate infrastructure resiliency.

Infrastructure systems continue to grow in complexity, while at the same time cross-domain interdependencies are becoming more common and more important to system function. This situation presents both complications and unprecedented opportunities for the science and engineering of resiliency.

One of the biggest areas of need for resilience engineering is the establishment of common definitions and processes. There is ongoing work to establish domain-agnostic, quantitative approaches to resilience (Barcelos et al. 2025; Paglioni et al. 2026). As the theory is developed, there needs to be a similar concerted effort to establish practical implementation policies. Additionally, there must be a focus on establishing cross-agency connections and cohesion. The organization is a critical piece of system resilience, and as systems grow in size and complexity, the organization must be seen to encompass multiple agencies and cross traditional domain boundaries.

References

, and 2004. "Resilience and Other Stability Concepts in Ecology: Notes on Their Origin, Validity and Usefulness." *The ESS Bulletin* 2 (2).

Brtis, John, Ken Cureton, Scott Jackson, and Ivan Taylor. 2025. "System Resilience." In *The Systems Engineering Body of Knowledge (SEBoK)*, 2.12, edited by Nicole Hutchison. The Trustees of the Stevens Institute of Technology. https://sebokwiki.org/w/index.php?title=System_Resilience&oldid=71441.

Gunderson, Lance, and Crawford Holling. 2003. "Panarchy: Understanding Transformations In Human And Natural Systems." *Bibliovault OAI Repository, the University of Chicago Press* 114 (December). https://doi.org/10.1016/S0006-3207(03)00041-7.

Holling, C. S. 1973. "Resilience and Stability of Ecological Systems." *Annual Review of Ecology, Evolution, and Systematics* 4 (Volume 4, 1973): 1–23. https://doi.org/10.1146/annurev.es.04.110173.000245.

Hollnagel, Erik. 2009. “The Four Cornerstones of Resilience Engineering.” In *Resilience Engineering Perspectives, Volume 2*. CRC Press.

Hollnagel, Erik, Jean Paries, David D. Woods, and John Wreathall, eds. 2011. *Resilience Engineering in Practice*. 1st ed. Taylor & Francis Group: CRC Press.

Hollnagel, Erik, David D. Woods, and Nancy Leveson, eds. 2006. *Resilience Engineering: Concepts and Precepts*. CRC Press Taylor & Francis Group.

Hutschenreuter, Helmar, Salva Çakmakçı, Christian Maeder, and Thomas Kemmerich. 2021. “Ontology-Based Cybersecurity and Resilience Framework:” *Proceedings of the 7th International Conference on Information Systems Security and Privacy*, 458–66. https://doi.org/10.5220/0010233604580466.

Jackson, Felicia. 2025. “The Water-Energy Nexus: The Hidden Infrastructure Of Resilience.” News. Forbes, October 27. https://www.forbes.com/sites/feliciajackson/2025/10/27/the-waterenergy-nexus-the-hidden-infrastructure-of-resilience/.

Knake, Robert K. 2017. *Contingency Planning Memorandum No. 31: A Cyberattack on the U.S. Power Grid*. Contingency Planning Memorandum. Council on Foreign Relations.

Mejia-Giraldo, Diego, Jose Villarreal-Marimon, Yang Gu, Yanyi He, Zhaoyang Duan, and Lizhi Wang. 2012. “Sustainability and Resiliency Measures for Long-Term Investment Planning in Integrated Energy and Transportation Infrastructures.” *Journal of Energy Engineering* 138 (2): 87–94. https://doi.org/10.1061/(asce)ey.1943-7897.0000067.

Miller, Maggie. 2026. “Trump Suggests US Used Cyberattacks to Turn off Lights in Venezuela during Strikes.” News. POLITICO, January 3. https://www.politico.com/news/2026/01/03/trump-venezuela-cyber-operation-maduro-00709816.

Modarres, Mohammad, and Katrina M. Groth. 2023. *Reliability and Risk Analysis*. 2nd ed. CRC Press, Taylor & Francis Group.

Neubert, Michael G., and Hal Caswell. 1997. “Alternatives to Resilience for Measuring the Responses of Ecological Systems to Perturbations.” *Ecology* 78 (3): 653–65.

Ng, Greg. 2025. “MTA: ‘Cybersecurity Incident’ Affecting Mobility Paratransit Services, Real-Time Tracking Information.” News. WBAL, August 25. https://www.wbal.com/mta-cybersecurity-incident-affecting-mobility-paratransit-services-real-time-tracking-information.

Paglioni, Vincent. 2024. “A System Objectives-Based Proposal for Modeling Resilience in Nuclear Power Plant Operations.” Paper presented at Pacific Basin Nuclear Conference 2024, Idaho Falls. October.

Paglioni, Vincent P., Steven Conrad, and Aaron Brown. 2025. “Reliability to Resiliency: Exploring Interconnected Metrics of System Performance.” Paper presented at INCOSE Western States Regional Conference (WSRC), Seattle, WA. *Proceedings of the 8th Western States Regional Conference*, September.

Paglioni, Vincent P., Graeme Troxell, Aaron Brown, Steve Conrad, and Mazdak Arabi. 2026. “Developing a Quantitative Resiliency Approach.” arXiv:2601.03452. Preprint, arXiv, January 6. https://doi.org/10.48550/arXiv.2601.03452.

Panteli, Mathaios, Pierluigi Mancarella, Dimitris N. Trakas, Elias Kyriakides, and Nikos D. Hatziargyriou. 2017. “Metrics and Quantification of Operational and Infrastructure Resilience in Power Systems.” *IEEE Transactions on Power Systems* 32 (6): 4732–42. https://doi.org/10.1109/TPWRS.2017.2664141.

Pordham, Luke. 2025. “Cyber-Physical Risk in the Marine Sector: A Wake-up Call from the MSC Antonia.” Industry. Lockton, May 27. https://global.lockton.com/news-insights/cyber-physical-risk-in-the-marine-sector-a-wake-up-call-from-the-msc-antonia.

Priya, Any. 2025. “Swedish Power Grid Operator Confirms Breach After Everest Ransomware Claim.” News. Cyber Press, October 28. https://cyberpress.org/swedish-power-grid-breach/.

Sutcliffe, Kathleen M. 2011. “High Reliability Organizations (HROs).” *Best Practice & Research Clinical Anaesthesiology*, Safety in Anaesthesia, vol. 25 (2): 133–44. https://doi.org/10.1016/j.bpa.2011.03.001.

Yodo, Nita, and Pingfeng Wang. 2016. “Engineering Resilience Quantification and System Design Implications: A Literature Survey.” *Journal of Mechanical Design* 138 (111408). https://doi.org/10.1115/1.4034223.