TESTUDO

HORIZON-CL3-2022-INFRA-01- Grant Agreement No. 101121258

AUTONOMOUS SWARM OF HETEROGENEOUS RESOURCES IN
INFRASTRUCTURE PROTECTION VIA THREAT PREDICTION AND PREVENTION

1st Policy Brief

"Advancing Critical Infrastructure Resilience through Technological Innovation"

Summary: *The TESTUDO project pioneers the integration of AI, predictive analytics, and autonomous systems to enhance the resilience of critical infrastructure. TESTUDO strengthens infrastructure protection through real-time threat detection and response mechanisms by addressing emerging threats such as cyber-attacks and climate-induced disasters. The project aligns with key EU policies, including the Artificial Intelligence Act and GDPR, ensuring responsible and legally compliant technological advancements. With a focus on interoperability, ethical AI deployment, and cross-sector collaboration, TESTUDO is a strategic model for safeguarding Europe's critical infrastructure against evolving security challenges.*

TESTUDO is a project funded by the European Commission under the Horizon Europe Programme (HORIZON-CL3-2022-INFRA-01) under Grant Agreement No. 101121258.

1. Introduction

1.1. Why Critical Infrastructures Matter

Critical infrastructures (CIs) are essential systems and assets that support the functioning of society and the economy. Their importance cannot be overstated, as they provide vital services crucial for public health, safety, and economic stability. The failure or disruption of these infrastructures can lead to significant societal and financial consequences, underscoring their critical role in modern life.

CIs encompass many sectors, including energy, transportation, water supply, telecommunications, and healthcare. For instance, water networks are a prime example of critical infrastructure, as they are essential for providing clean drinking water, sanitation, and irrigation. The aging infrastructure of water utilities, coupled with integrating new technologies such as supervisory control and water quality tracking in treatment and distribution processes, introduces additional vulnerabilities and risks (Moraitis et al., 2023). Disruptions in water supply can lead to public health crises, economic losses, and social unrest (Назарова et al., 2024; Stock et al., 2022; Wahab et al., 2023). The interdependence of various infrastructures means that a failure in one sector can cascade into others, amplifying the overall impact on society (Oliver et al., 2022; Ouyang & Fang, 2017). For example, a power outage can disrupt water treatment facilities, leading to water supply issues, which can affect public health and safety (Stock et al., 2022; Oliver et al., 2022).

The economic implications of critical infrastructure failures are profound. Research indicates that businesses reliant on these infrastructures can suffer significant financial losses, potentially jeopardizing their future existence (Strelcová et al., 2015; Krupa & Wiśniewski, 2015). The economic security of enterprises is closely tied to the reliability of CIs; thus, ensuring their resilience is paramount for maintaining economic stability (Strelcová et al., 2015). Moreover, the societal impacts of infrastructure disruptions can exacerbate existing inequalities, as vulnerable populations may be disproportionately affected by service outages (Barquet et al., 2023; Badolo, 2024).

The societal importance of CIs extends beyond mere functionality; they are integral to the quality of life and the overall well-being of communities. Providing reliable infrastructure services enhances social cohesion and trust in public institutions (Dolan et al., 2016). Furthermore, the resilience of critical infrastructures is essential for disaster preparedness and response, as they play a pivotal role in emergency management (Sfetsos et al., 2021). For instance, during natural disasters, adequate transportation and communication networks are vital for coordinating relief efforts and ensuring public safety (Williams et al., 2019).

1.2. Emerging Threats

The increasing frequency and intensity of natural disasters, particularly wildfires and floods exacerbated by climate change, pose significant threats to critical infrastructure. These threats are compounded by the interconnectedness of modern infrastructure systems, which can lead to cascading failures across multiple sectors. This synthesis will explore the implications of climate change on infrastructure resilience, the risks associated with wildfires, and the emerging threats from cyber-attacks and physical vulnerabilities.

Ulibarrí and Han highlight that the long-term resilience of infrastructure projects is compromised by anticipated changes in climate variables, including precipitation patterns and the frequency of natural hazards like hurricanes and wildfires (Ulibarrí & Han, 2022). Verschuur et al. further emphasize that infrastructure systems are particularly vulnerable to climate hazards, necessitating quantitative analyses to inform resilience and adaptation strategies (Verschuur et al., 2024). The increasing severity of these climate-related events underscores the urgent need for infrastructure to adapt to changing conditions, as evidenced by the rising risks associated with wildfires, which can lead to extensive damage to critical infrastructure such as power lines and water systems (Severino et al., 2024; Pan et al., 2024).

Wildfires present a multifaceted threat to infrastructure. The aftermath of wildfires can result in significant post-fire hazards, including contamination of water supplies and damage to building infrastructure, which can persist long after the initial event (Belongia et al., 2023). For instance, the destruction of vegetation can lead to increased sediment runoff, adversely affecting water quality and infrastructure integrity (Wibbenmeyer et al., 2023). Moreover, the wild-and-urban interface (WUI) is increasingly at risk as urban development encroaches on fire-prone areas, heightening the potential for catastrophic losses (Balch et al., 2017). The economic impacts of wildfires are substantial, with estimates indicating that the costs associated with wildfire damage to infrastructure and ecosystems are likely to escalate as climate change progresses (Wang et al., 2020).

In addition to natural disasters, the interconnected nature of modern infrastructure systems introduces vulnerabilities to cyber-attacks. The potential for cyber threats grows as infrastructure becomes increasingly digitized and reliant on interconnected networks. For instance, the evolution of power grids has been accompanied by new challenges, including the risk of cyber-attacks that can disrupt service and compromise infrastructure resilience (Hu et al., 2023). This highlights the need for integrated approaches considering physical and cyber vulnerabilities in infrastructure planning and management.

Furthermore, socio-economic factors compound infrastructure systems' physical vulnerabilities to climate change and natural disasters. Already, socially vulnerable communities may face exacerbated risks from wildfires and flooding, necessitating targeted interventions to enhance resilience (Zhang et al., 2024). The interplay between environmental hazards and social vulnerability underscores the importance of incorporating equity considerations into infrastructure planning and disaster response strategies (Amil et al., 2022).

1.3. TESTUDO’s Role

The TESTUDO project is pivotal in advancing the resilience of critical infrastructure (CI) through technological innovation, aligning closely with the EU's broader security and resilience strategies. As a Horizon Europe initiative, TESTUDO integrates state-of-the-art AI, predictive analytics, and autonomous systems to enhance real-time threat detection, response coordination, and infrastructure protection.

The European Union recognizes the increasing complexity of CI threats, ranging from cyberattacks to physical disruptions caused by natural disasters and human-made incidents. The EU Security Union Strategy (2020-2025) and Directive (EU) 2022/2557 on the resilience of critical entities highlight the need for a proactive, technology-driven approach to safeguarding essential services. TESTUDO directly contributes to these objectives by developing an autonomous swarm of heterogeneous unmanned resources—comprising aerial, ground, and cyber assets—that operate collaboratively to predict and prevent threats dynamically and adaptively.

A key innovation within TESTUDO is its integration of AI-driven surveillance, digital twins, and cybersecurity tools to create a holistic situational awareness framework. The project's ability to autonomously detect, analyze, and respond to threats reduces reliance on human operators, ensuring a faster and more coordinated response to potential disruptions. By leveraging multispectral detection, cyber threat analysis, and real-time data fusion, TESTUDO enhances the predictive capabilities of CI operators, minimizing downtime and mitigating risks before they escalate into full-scale crises.

Moreover, TESTUDO's commitment to interoperability ensures seamless integration with existing security frameworks, making it a scalable solution for diverse Critical Infrastructure (CI) sectors, including energy, transportation, and water supply networks. The project aligns with the European Union's regulatory landscape, embedding compliance with key directives such as the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)[1] for data protection, the AI Act for ethical and transparent AI deployment, and the Cybersecurity Act (Regulation (EU) 2019/881)[2] for certification of ICT security products. Additionally, TESTUDO directly addresses Directive (EU) 2022/2557[3] on the resilience of critical entities (CER Directive) by enhancing the security posture and operational continuity of essential services through predictive threat intelligence and autonomous monitoring. The project also integrates cybersecurity safeguards with Directive (EU) 2022/2555 (NIS2 Directive)[4], ensuring robust incident detection and response mechanisms against cyber threats targeting critical infrastructure. Furthermore, TESTUDO adheres to Directive 2012/18/EU (Seveso-III Directive)[5] to mitigate industrial risks, incorporating real-time hazard detection and risk assessment features that support compliance with EU-wide industrial safety regulations. By embedding these legal and ethical considerations, TESTUDO provides a resilient and future-proof solution for CI protection following the evolving European regulatory framework.

From an exploitation perspective, TESTUDO's impact extends beyond research, focusing on commercialization pathways, stakeholder engagement, and regulatory alignment. Its structured approach to market adoption, intellectual property management, and standardization facilitates its integration into real-world security operations. By aligning with the EU's strategic priorities, TESTUDO strengthens Europe's resilience against evolving threats, reinforcing the Security Union Strategy's vision of a safer, more secure European infrastructure landscape

[1] European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation - GDPR)*. Official Journal of the European Union, L 119, 1-88.

[2] European Parliament & Council of the European Union. (2019). *Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act)*. Official Journal of the European Union, L 151, 15-69.

[3] European Parliament & Council of the European Union. (2022). *Directive (EU) 2022/2557 on the resilience of critical entities*. Official Journal of the European Union, L 333, 1-30.

[4] European Parliament & Council of the European Union. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Official Journal of the European Union, L 333, 80-152.

[5] European Parliament & Council of the European Union. (2012). *Directive 2012/18/EU on the control of major-accident hazards involving dangerous substances (Seveso-III Directive)*. Official Journal of the European Union, L 197, 1-37.

2. Key Findings

2.1. Research Highlights

TESTUDO is at the forefront of technological innovation in critical infrastructure (CI) protection, leveraging advanced tools and methodologies to enhance resilience and security. The project integrates cutting-edge technologies, including artificial intelligence (AI), predictive analytics, digital twins, and autonomous systems, to develop a comprehensive security framework capable of addressing emerging threats in dynamic and complex environments.

One of TESTUDO's primary innovations is its deployment of an autonomous swarm of heterogeneous resources, combining unmanned aerial and ground vehicles (UAVs and UGVs) with sophisticated sensing and data fusion capabilities. These autonomous assets operate in a coordinated fashion, utilizing AI-driven algorithms to detect anomalies, assess threats, and respond effectively to potential incidents. Integrating multispectral detection technologies further enhances the system's ability to identify various threats, from environmental hazards to terrorist attacks.

The project also pioneers the use of digital twin technology, enabling real-time simulation and threat modeling for CI operators. TESTUDO allows stakeholders to anticipate vulnerabilities, optimize responses, and refine security measures in a controlled environment by creating a virtual representation of physical assets and infrastructure. This predictive capability, powered by advanced machine learning techniques, significantly improves situational awareness and decision-making processes.

Cybersecurity is critical in TESTUDO's framework, with robust threat detection modules designed to identify and mitigate cyber risks. The system leverages AI-enhanced anomaly detection to recognize suspicious activity, reinforcing the security of interconnected infrastructure networks. Additionally, implementing privacy-preserving AI ensures that these capabilities align with European data protection and cybersecurity regulations.

To ensure the reliability and effectiveness of these technologies, TESTUDO employs a rigorous validation process through large-scale and cross-sectorial pilots conducted in real-world operational environments. These pilots are crucial testbeds for refining AI models, optimizing sensor integrations, and validating autonomous decision-making mechanisms. By involving end-users and infrastructure operators throughout the project, the project ensures that its solutions are practical and scalable, capable of addressing the diverse security needs of different CI sectors.

Through this combination of advanced technologies and real-world validation, TESTUDO establishes itself as a leading initiative in CI resilience. The project's approach enhances immediate threat detection and response and contributes to the long-term sustainability and adaptability of Europe's critical infrastructure systems.

2.2. Strategic Alignment with EU Policies

TESTUDO is committed to aligning its technological advancements with the European Union's regulatory frameworks, particularly the Artificial Intelligence Act and the General Data Protection Regulation (GDPR). By adhering to these directives, TESTUDO ensures that its critical infrastructure protection innovations are effective and compliant with EU standards.

The Artificial Intelligence Act establishes harmonized rules for developing and deploying AI within the EU, emphasizing the importance of trustworthy and human-centric AI systems. TESTUDO's AI-driven solutions are designed with these principles, incorporating robust risk management and transparency measures to meet the Act's requirements. This includes implementing explainable AI models and ensuring human oversight in decision-making processes, fostering trust and accountability in AI applications.

In parallel, the GDPR sets stringent guidelines for processing personal data, safeguarding individual privacy rights. TESTUDO integrates privacy-by-design principles into its systems, ensuring data collection, storage, and analysis comply with GDPR standards. This involves minimizing data usage, anonymizing personal information, and establishing clear data governance protocols to protect individuals' privacy.

Recent discussions at the Paris AI summit[6] have highlighted the EU's commitment to balancing innovation with regulation. Leaders emphasized the need to streamline regulatory processes to foster technological advancement while maintaining ethical standards. TESTUDO's approach reflects this balance by advancing cutting-edge technologies aligned with EU policies, ensuring that innovation proceeds responsibly and sustainably.

TESTUDO complies with current EU directives by proactively engaging with these regulatory frameworks and shapes a secure and ethical AI landscape within Europe. This strategic alignment underscores TESTUDO's dedication to responsible innovation and its role in enhancing the resilience of critical infrastructure across the EU.

3. Policy Recommendations

Policies that accelerate the adoption of AI-driven solutions, strengthen regulatory frameworks, and foster cross-sector collaboration are essential to enhancing the resilience of critical infrastructure across the EU. These recommendations align with the EU’s broader security and digital transformation goals, ensuring technological advancements contribute to a safer and more resilient infrastructure landscape.

Accelerating the Adoption of AI and Emerging Technologies

Encouraging member states to invest in AI-based solutions for early threat detection is crucial in modernizing critical infrastructure protection. By leveraging predictive analytics and autonomous surveillance systems, operators can proactively identify and mitigate risks before they escalate into large-scale disruptions. To support this transition, the EU should promote the development of AI training and education programs tailored to stakeholders involved in infrastructure management. Such initiatives

[6] Reuters. (2025, February 10). *Paris AI summit draws world leaders, CEOs eager for technology wave*. Reuters. Retrieved from https://www.reuters.com/technology/artificial-intelligence/paris-ai-summit-draws-world-leaders-ceos-eager-technology-wave-2025-02-10/.

would equip security professionals, policymakers, and operators with the necessary skills to integrate AI technologies into their operational workflows effectively.

Strengthening Regulatory Frameworks

A robust regulatory framework is fundamental to ensuring AI's safe and ethical deployment in infrastructure security. The EU should advocate for standardized security measures that define AI applications' roles and limitations within critical infrastructure protection. Establishing clear EU-wide guidelines would help harmonize security standards, prevent regulatory fragmentation, and promote compliance among member states. Additionally, integrating digital security technologies into national and local policies would strengthen overall infrastructure resilience by embedding cybersecurity and AI-driven risk management into governance structures.

Encouraging Collaboration Across Sectors

Cross-sector collaboration is essential to addressing critical infrastructure's complex and evolving threats. Establishing cross-border platforms for information sharing and joint action would enable stakeholders to exchange intelligence on security threats, vulnerabilities, and best practices. This collaborative approach would facilitate a more coordinated response to infrastructure risks and enhance collective security efforts across the EU. Furthermore, incentivizing public-private partnerships is key to co-developing innovative security solutions. By encouraging joint investment in AI-driven infrastructure protection technologies, the EU can bridge the gap between industry expertise and public sector needs, fostering a more adaptive and resilient security ecosystem.

4. Ethical and Legal Considerations

Ensuring that AI-driven solutions for critical infrastructure protection align with ethical principles and legal requirements is a cornerstone of the TESTUDO project. Maintaining public trust, accountability, and compliance with legal frameworks is essential as AI and autonomous systems become more integrated into security operations. TESTUDO is committed to upholding ethical AI deployment and data privacy standards, following EU regulations and global best practices.

Ethics in AI and Autonomous Systems

AI and autonomous systems are crucial in TESTUDO’s ability to predict, detect, and mitigate threats in critical infrastructure environments. However, their deployment must be guided by transparency, fairness, and accountability principles. TESTUDO aligns with the Ethics Guidelines for Trustworthy AI[7], which ensures that AI models are explainable, auditable, and free from biases that could lead to unintended discrimination or security vulnerabilities. The project integrates human-in-the-loop decision-making, reinforcing oversight mechanisms to prevent overreliance on automated processes. This approach corresponds to the guidance from the European Commission and the EU High-level expert group on AI, which emphasize human-centric design principles and the preservation of meaningful human

[7] European Commission. (2019). *Ethics guidelines for trustworthy AI. High-Level Expert Group on Artificial Intelligence*. Retrieved from https://ec.europa.eu/futurium/en/ai-alliance-consultation.

agency in AI-human interactions. By embedding ethical AI principles into system design, TESTUDO fosters trust among stakeholders by ensuring that AI-driven security applications remain aligned with European values of transparency, fairness, accountability, and human oversight. This commitment enhances public confidence in AI's role in critical infrastructure protection, ensuring compliance with EU ethical frameworks, such as the Ethics Guidelines for Trustworthy AI developed by the High-Level Expert Group on AI (AI HLEG)[8], which emphasize explainability, robustness, and the avoidance of bias in automated decision-making. Furthermore, this approach reflects the strategic vision outlined in the European Commission's White Paper on Artificial Intelligence[9], which advocates for a risk-based regulatory framework that promotes excellence and trust in AI systems while safeguarding fundamental rights. By integrating these principles, TESTUDO strengthens the resilience of security applications. It reinforces its alignment with EU-wide AI governance frameworks, ensuring that emerging technologies serve both security imperatives and ethical responsibilities..

Privacy and Data Security

TESTUDO places data privacy and security at the core of its technological framework, ensuring strict compliance with the General Data Protection Regulation (GDPR). All AI-driven surveillance, monitoring, and threat detection systems are designed with privacy-by-design principles, incorporating robust encryption, anonymization, and access control measures. The project emphasizes the need to balance technological innovation with citizens' rights, ensuring that personal and sensitive data are handled with the highest security and ethical responsibility. TESTUDO's approach also aligns with evolving EU data protection regulations, addressing challenges posed by the increasing digitalization of security systems while maintaining a clear commitment to fundamental rights.

As AI governance and privacy regulations evolve, TESTUDO proactively engages with legal and ethical experts to anticipate potential regulatory changes and ensure ongoing compliance. The project's framework is a model for responsible AI implementation in critical infrastructure protection, demonstrating how innovation can advance security while upholding ethical integrity and legal accountability.

5. Conclusions

The TESTUDO project represents a significant advancement in the protection and resilience of critical infrastructure through technological innovation. TESTUDO enhances real-time threat detection, response coordination, and long-term infrastructure security by integrating AI-driven surveillance, predictive analytics, digital twins, and autonomous systems. The project's alignment with key EU policies, including

[8] EU High-Level Expert Group on AI (AI HLEG). (2019). *Policy and Investment Recommendations for Trustworthy Artificial Intelligence*. European Commission. Retrieved from https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence; EU High-Level Expert Group on AI (AI HLEG). (2019). *Ethics Guidelines for Trustworthy AI. European Commission*. Retrieved from https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

[9] European Commission. (2020). *White Paper on Artificial Intelligence: A European Approach to Excellence and Trust*. Retrieved from https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

the Artificial Intelligence Act and GDPR, ensures its solutions are legally compliant and ethically responsible. Additionally, TESTUDO's emphasis on large-scale cross-sectorial trials and real-world validation reinforces its commitment to practical implementation and scalability.

To fully realize the potential of these innovations, EU policymakers should prioritize the acceleration of AI adoption, the strengthening of regulatory frameworks, and the enhancement of cross-sector collaboration. By fostering investment in AI-based security measures, standardizing security protocols, and promoting partnerships between public and private entities, the EU can further bolster the resilience of its critical infrastructure. As emerging threats evolve, TESTUDO serves as a model for responsible innovation, demonstrating how cutting-edge technology can safeguard essential services while upholding ethical standards and regulatory compliance.

Key Message to Take Away from the Brief

Critical infrastructure resilience is fundamental to society's stability and security. TESTUDO demonstrates how AI, predictive analytics, and autonomous systems can revolutionize infrastructure protection by enabling real-time threat detection, proactive risk mitigation, and coordinated response mechanisms. By aligning with EU policies such as the Artificial Intelligence Act and GDPR, TESTUDO ensures that innovation is implemented responsibly, balancing technological advancement with ethical considerations and data privacy. To maximize impact, EU policymakers, industry leaders, and stakeholders must prioritize investment in AI-driven security solutions, establish robust regulatory frameworks, and foster cross-sector collaboration. In doing so, TESTUDO serves as a blueprint for the future of critical infrastructure protection in an increasingly complex and interconnected world.

6. References

Amil, M., Nogueira-Moure, E., Prestemon, J., & Touza, J. (2022). Spatial patterns of social vulnerability in relation to wildfire risk and wildland-urban interface presence. Landscape and Urban Planning, 228, 104577. https://doi.org/10.1016/j.landurbplan.2022.104577.

Balch, J., Bradley, B., Abatzoglou, J., Nagy, R., Fusco, E., & Mahood, A. (2017). Human-started wildfires expand the fire niche across the United States. Proceedings of the National Academy of Sciences, 114(11), 2946–2951. https://doi.org/10.1073/pnas.1617394114.

Badolo, M. (2024). Modeling and planning interdependent critical urban infrastructures resilience to extreme events: the Badolo Cires model. https://doi.org/10.22541/au.171148942.23175536/v1.

Barquet, K., Englund, M., Inga, K., André, K., & Segnestam, L. (2023). Conceptualising multiple hazards and cascading effects on critical infrastructures. Disasters, 48(1). https://doi.org/10.1111/disa.12591.

Belongia, M., Wagner, C., Quesnel, K., & Ajami, N. (2023). Building water resilience in the face of cascading wildfire risks. Science Advances, 9(37). https://doi.org/10.1126/sciadv.adf9534.

Dolan, T., Walsh, C., Bouch, C., & Carhart, N. (2016). A conceptual approach to strategic performance indicators. Infrastructure Asset Management, 3(4), 132–142. https://doi.org/10.1680/jinam.16.00015.

Назарова, К., Hordopolov, V., Lositska, T., Nezhyva, M., & Mysiuk, V. (2024). Comparative analysis of critical infrastructure and public significance enterprises. Multidisciplinary Reviews, 7(6), 2024108. https://doi.org/10.31893/multirev.2024108.

Hu, H., Yu, S., & Trinh, H. (2023). A review of uncertainties in power systems - modelling, impact, and mitigation. https://doi.org/10.20944/preprints202312.1585.v1.

Krupa, T. and Wiśniewski, M. (2015). Situational management of critical infrastructure resources under threat. Foundations of Management, 7(1), 93-104. https://doi.org/10.1515/fman-2015-0028.

Moraitis G, Sakki G-K, Karavokiros G, Nikolopoulos D, Tsoukalas I, Kossieris P, Makropoulos C. Exploring the Cyber-Physical Threat Landscape of Water Systems: A Socio-Technical Modelling Approach. Water. 2023; 15(9):1687. https://doi.org/10.3390/w15091687.

Oliver, E., Mazzuchi, T., & Sarkani, S. (2022). A resilience systemic model for assessing critical supply chain disruptions. Systems Engineering, 25(5), 510-533. https://doi.org/10.1002/sys.21633.

Ouyang, M. and Fang, Y. (2017). A mathematical framework to optimize critical infrastructure resilience against intentional attacks. Computer-Aided Civil and Infrastructure Engineering, 32(11), 909-929. https://doi.org/10.1111/mice.12252.

Pan, W., Li, Y., Guo, Z., & Zhang, Y. (2024). Interdependent expansion planning for resilient electricity and natural gas networks. Processes, 12(4), 775. https://doi.org/10.3390/pr12040775.

Severino, G., Fuentes, A., Valdivia, A., Cheein, F., & Reszka, P. (2024). Assessing wildfire risk to critical infrastructure in central Chile: application to an electrical substation. International Journal of Wildland Fire, 33(4). https://doi.org/10.1071/wf22113.

Sfetsos, A., Giroud, F., Clemencau, A., Varela, V., Freissinet, C., Lecroart, J., … & Hahmann, S. (2021). Assessing the effects of forest fires on interconnected critical infrastructures under climate change. Evidence from South France. Infrastructures, 6(2), 16. https://doi.org/10.3390/infrastructures6020016.

Stock, A., Davidson, R., Kendra, J., Martins, V., Ewing, B., Nozick, L., … & León-Corwin, M. (2022). Household impacts of interruption to electric power and water services. Natural Hazards, 115(3), 2279-2306. https://doi.org/10.1007/s11069-022-05638-8.

Strelcová, S., Řehák, D., & Johnson, D. (2015). Influence of critical infrastructure on enterprise economic security. Communications - Scientific Letters of the University of Zilina, 17(1), 105-110. https://doi.org/10.26552/com.c.2015.1.105-110.

Ulibarrí, N. and Han, D. (2022). Nepa and climate change: consideration of climate mitigation and adaptation in infrastructure review processes. Environmental Research Infrastructure and Sustainability, 2(1), 015004. https://doi.org/10.1088/2634-4505/ac5006.

Verschuur, J., Fernández, A., Mühlhofer, E., Nirandjan, S., Borgomeo, E., Becher, O., … & Hall, J. (2024). Quantifying climate risks to infrastructure systems: a comparative review of developments across infrastructure sectors. Plos Climate, 3(4), e0000331. https://doi.org/10.1371/journal.pclm.0000331.

Wahab, Y., Alias, N., Anuar, A., Taib, S., Bashah, K., & Baslan, N. (2023). Critical infrastructure (ci) protection for flood risk assessment and flood vulnerability index in Sungai Pinang, Pulau Pinang. Malaysian Journal of Civil Engineering, 35(1), 47-52. https://doi.org/10.11113/mjce.v35.19946.

Wang, D., Guan, D., Zhu, S., Kinnon, M., Geng, G., Zhang, Q., … & Davis, S. (2020). Economic footprint of California wildfires in 2018. Nature Sustainability, 4(3), 252–260. https://doi.org/10.1038/s41893-020-00646-7.

Wibbenmeyer, M., Sloggy, M., & Sánchez, J. (2023). Economic analysis of wildfire impacts to water quality: a review. Journal of Forestry, 121(4), 374–382. https://doi.org/10.1093/jofore/fvad012.

Williams, J., Wilson, T., Horspool, N., Lane, E., Hughes, M., Davies, T., … & Scheele, F. (2019). Tsunami impact assessment: development of vulnerability matrix for critical infrastructure and application to Christchurch, New Zealand. Natural Hazards, 96(3), 1167–1211. https://doi.org/10.1007/s11069-019-03603-6.

Zhang, T., Wang, D., & Lu, Y. (2024). A dynamic spatiotemporal understanding of changes in social vulnerability to wildfires at local scale. Fire, 7(7), 251. https://doi.org/10.3390/fire7070251.