Work Group #4

Infrastructure and Service Resilience for Smart Society

Takuro YONEZAWA

Chrysostomos STYLIOS

Teaser: Building resilient smart societies through integrated approaches to infrastructure, human factors, and cybersecurity.

Executive Summary

Following the ERCIM/JST Joint Workshop 2024, this white paper outlines the key challenges and research directions identified by the Infrastructure and Service Resilience for Smart Society working group. The collaboration between European and Japanese researchers focused on addressing the increasing vulnerability of urban environments to disruptions caused by climate change, digital threats, and evolving societal needs.

The group identified three critical areas requiring coordinated research efforts: infrastructure resilience, people's resilience, and Security and Privacy. The paper describes how these areas interconnect and proposes key research directions related to the applications of Artificial Intelligence, the adoption of immersive technologies, the development of human-centered design approaches, and the necessary policy frameworks required for standards and interoperability.

The document concludes with a call for multi-stakeholder engagement through research partnerships, pilot implementations, policy development, funding collaborations, and educational initiatives to address these shared challenges.

Identified Challenges

In today's rapidly evolving urban landscape, cities worldwide face unconventional challenges to their infrastructure and service resilience. The convergence of aging physical systems, climate change impact, digital vulnerabilities, and evolving societal needs creates a complex environment where traditional approaches to resilience are no longer sufficient. For this white paper, a 'smart society' is defined as an urban and social environment where advanced digital technologies, including the Internet of Things (IoT), big data analytics, and Artificial Intelligence, are deeply integrated with physical infrastructure and public services. The objective of such a society is to enhance the quality of life, operational efficiency, and sustainability. However, this profound integration also introduces novel complexities and vulnerabilities, forming the core challenge this paper addresses. Europe and Japan share many of these challenges: both regions have increased natural disaster frequency, cybersecurity threats, and the need to maintain essential services under diverse disruption scenarios.

The integration of emerging technologies into urban environments presents both opportunities and risks. While innovative systems can enhance efficiency and adaptability, they also introduce new vulnerabilities that must be addressed through coordinated research and innovation efforts. However, the interdependencies between physical infrastructure, digital systems, and human communities further complicate the resilience landscape, necessitating holistic approaches that transcend traditional disciplinary boundaries.

In this white paper, we synthesize insights from the Infrastructure and Service Resilience for Smart Society working group, established under the auspices of the European Research Consortium for Informatics and Mathematics (ERCIM) and the Japan Science and Technology Agency (JST). Through collaborative discussions, the working group has identified three complementary pillars for enhancing the resilience of smart societies: *1)* Infrastructure's Resilience, *2)* People's Resilience, and *3)* Security and Privacy.

Pillars for Resilience Enhancement

Infrastructure's Resilience

As urban infrastructures mature, the systems designed and built decades ago are becoming increasingly vulnerable to failures and external threats. Climate change exacerbates these challenges by increasing the frequency and severity of natural disasters that can damage critical infrastructure. Traditional reactive approaches to infrastructure management—i.e., repairing systems after failure—are no longer sufficient in this context. Proactive resilience necessitates a paradigm shift toward systems that can anticipate, prevent, and respond rapidly to potential failures. Recent advances in sensor technologies, Artificial Intelligence, and autonomous systems are creating new possibilities in this domain, including:

- Early Warning Systems that utilise distributed sensor networks and advanced analytics to provide actionable intelligence to infrastructure managers before critical thresholds are reached.
- Predictive Maintenance Algorithms that optimise intervention timing based on real-time condition assessments, historical data, and contextual factors such as weather forecasts and usage patterns.

The working group identified several research challenges in these domains, including the development of integrated approaches to monitoring interdependent infrastructure systems, balancing resilience with sustainability objectives, and creating cost-effective methods for upgrading existing infrastructure. Such methods could include, for instance, the targeted reinforcement of critical nodes identified through digital twin simulations or the deployment of modular, scalable sensor packages for monitoring aging assets.

People's Resilience

As social systems become more complex and interconnected, communities face new challenges in preparing for, responding to, and recovering from disruptions. Traditional approaches to community resilience, which rely primarily on physical infrastructure and top-down emergency management, are insufficient to address the human dimensions of crisis response and recovery. The Metaverse—encompassing Virtual, Augmented, and Mixed Reality technologies—offers a transformative potential for enhancing community resilience. By

creating immersive digital environments that integrate real-world data, it provides a wide range of opportunities for simulation, training, and service continuity focused on human dimensions of resilience, including:

- Immersive Training Environments for emergency responders and community members that simulate complex disaster scenarios and develop adaptive response capabilities through realistic yet safe experiences.
- Virtual Service Continuity Platforms that maintain essential public services during physical disruptions, including virtual classrooms, telemedicine systems, and digital government interfaces that function even when physical infrastructure is compromised.
- Collaborative Planning Tools that engage diverse stakeholders in resilience strategy development through visualisation and simulation capabilities that make complex technical concepts accessible to non-specialists.

The working group identified several challenges in these domains, including the integration of computational social science with virtual environments, the need to address privacy and data concerns in human behaviour modelling, and the facilitation of equitable access to these technologies across diverse communities with varying resources and capabilities. Furthermore, while the Metaverse offers powerful tools, it is crucial to recognise that People's Resilience is a multifaceted concept that extends beyond technological solutions. A genuinely holistic approach must also encompass strengthening community bonds through local engagement programs, enhancing digital and information literacy to combat misinformation during crises, and providing accessible psychological support frameworks to help individuals cope with the stress of disruptive events. These socio-psychological factors are foundational to the effective adoption and use of any technological system.

Security and Privacy

As digital technologies become increasingly embedded in critical infrastructure and services, cybersecurity has emerged as a fundamental dimension of resilience. The integrity, availability, and confidentiality of digital systems are essential for maintaining societal functions during both normal operations and crisis scenarios. Traditional approaches to security, which focus primarily on perimeter defense, are inadequate for today’s interconnected systems. Proactive security requires comprehensive strategies that address vulnerabilities across the entire digital

ecosystem. Recent advances in cryptography, distributed systems, and Artificial Intelligence are creating new possibilities in this domain, including:

- Federated Learning Systems that enable privacy-preserving machine learning approaches for collaborative model development without exposing sensitive data.
- Supply Chain Transparency Technologies that utilise cryptographic and blockchain-based systems for verifying the integrity and provenance of software and hardware components throughout supply chains.
- AI-Based Threat Detection that employs advanced machine learning systems capable of identifying novel attack patterns and anomalous behaviors across complex networks.

The working group identified several research challenges in these domains, including protecting digital supply chains with multiple entry points for malicious actors, securing the proliferation of IoT devices in urban environments, and developing enhanced governance frameworks for protecting critical infrastructure in increasingly connected systems.

The Resilience Framework

While each pillar addresses distinct aspects of resilience, their true power emerges through integration. The working group has developed a conceptual framework that illustrates the interdependencies between **infrastructure's resilience, people's resilience, and Security and Privacy**, highlighting how these elements must work together to create truly resilient smart societies (Fig. 1).

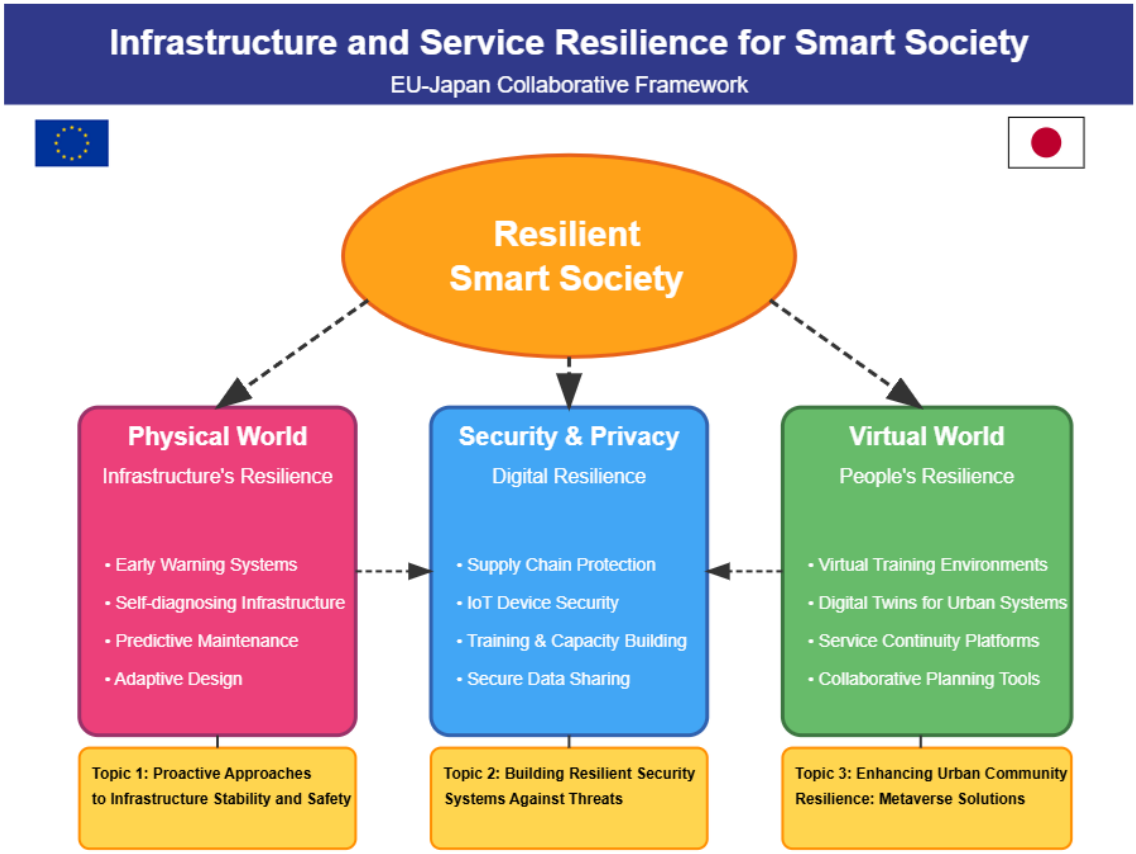

Figure 1. Conceptual framework for resilience.

At the core of the framework is the recognition that **digital resilience** emerges from the interactions between **physical systems**, **virtual environments**, and **human communities**. Physical infrastructure provides the foundation for essential services, while virtual systems enable simulation, monitoring, and service continuity. Finally, security and privacy protections ensure the integrity of these interconnected systems. Key integration points include:

- Physical-Digital Interfaces: The boundaries between physical infrastructure and digital systems are increasingly blurred as embedded sensors, actuators, and control systems become ubiquitous.
- Human-Technology Interaction: The effectiveness of resilience technologies ultimately depends on how humans interact with them, both during normal operations and crisis scenarios. User-centered design approaches that accommodate diverse needs and capabilities are essential for resilience in practice.
- Data Flows Across Domains: Information sharing between physical infrastructure systems, virtual environments, and security mechanisms is essential for integrated resilience but raises complex privacy and interoperability challenges that must be addressed through both technological and governance innovations.
- Cross-Scale Coordination: Resilience requires coordination across different spatial and temporal scales, from individual buildings to regional infrastructure networks, and from immediate emergency response to long-term adaptation strategies. Integrated approaches must facilitate this coordination through appropriate technological and institutional mechanisms.

Research Directions

The working group has identified several key technological enablers that can support integrated resilience across all three pillars.

Artificial Intelligence and Machine Learning

Artificial Intelligence technologies offer powerful capabilities for pattern recognition, prediction, and automated decision support across resilience domains. Priority research areas include:

- Explainable AI to provide transparent justifications for recommended actions in high-stakes contexts.
- Transfer of learning approaches to allow models trained in one context to be applied effectively in others.
- Federated learning systems to enable collaborative model development while preserving data privacy and security.

Immersive Technologies

Virtual, augmented, and Mixed Reality technologies create new possibilities for training, simulation, and service delivery across resilience applications. Key research directions include:

- Low-resource VR/AR systems that can function on widely available hardware to enhance accessibility across different socioeconomic contexts.
- Haptic (multi-sensory) interfaces to create more realistic training environments for complex tasks.
- Collaborative virtual environments to enable coordination among distributed teams during both planning and response phases.
- Adaptive interfaces to accommodate diverse user needs and capabilities, such as simplified modes for elderly users, voice-activated controls for first responders, or multi-lingual support in multicultural communities, as a means of ensuring inclusive access to resilience tools.

Human-Centered Design

Technical capabilities alone are insufficient for effective resilience; systems must be designed with a deep understanding of human factors. Key research areas include:

- Crisis decision-making patterns to reveal how individuals and organisations make choices under extreme stress and uncertainty.
- Inclusive design methodologies to ensure that resilience technologies are accessible and usable across diverse populations.
- Trust-building mechanisms for automated and AI-driven systems involved in critical decision processes.
- Risk communication approaches capable of translating complex technical information into actionable insights for different stakeholders.

Policy and Governance Considerations (Standards and Interoperability)

Appropriate policy and governance frameworks must also accompany research and innovation in resilience technologies. Key areas for consideration include:

- Common data formats and exchange protocols to facilitate information sharing across systems and jurisdictions.
- Resilience assessment methodologies to provide consistent evaluation approaches across different contexts.
- Interoperable emergency communication systems to enable coordination among diverse responders.
- Open standards for critical interfaces to prevent vendor lock-in for essential resilience technologies.

The Path Forward

In line with the above, the work group members would like to substantive call to action for researchers, policymakers, industry partners, and community stakeholders. The complex resilience challenges facing smart societies demand coordinated responses that transcend traditional disciplinary boundaries, sectoral divisions, and national frameworks. As such, we invite interested parties to join this collaborative initiative. To catalyse this effort, the working group proposes a series of immediate next steps:

- **Establish a Joint EU-Japan Task Force:** To coordinate research efforts, share best practices, and guide the development of the integrated resilience framework.
- **Launch Thematic Workshops:** To delve deeper into the specific research challenges outlined in this paper, bringing together experts from academia, industry, and government.
- **Identify and Develop Pilot Implementations:** To test integrated approaches in real-world contexts, selecting candidate cities in both Europe and Japan to serve as living laboratories.
- **Secure Joint Funding Collaborations:** To create a dedicated funding stream that supports multinational, interdisciplinary research projects addressing these shared challenges.
- **Develop a Shared Educational Curriculum:** To build future capacity by creating educational modules and exchange programs for students and professionals in resilience-related disciplines.

End of Document