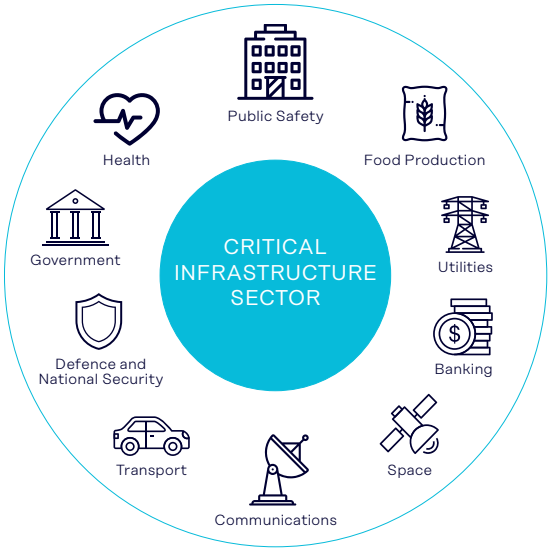
Critical Infrastructure Resilience

CRITICAL INFRASTRUCTURE RESILIENCE

According to EU COM (2006) 786, a Critical Infrastructure is an asset or system essential for the maintenance of vital societal functions. Damage to Critical Infrastructure, their destruction or disruption by natural disasters, terrorism, criminal activity or malicious behavior, has a significant negative impact on the security of our society and the well-being of its citizens.

Moreover, due to their networked character and mutual dependencies failures in one part of the network of critical infrastructure can cause problems in other parts of the network, potentially causing cascading impact across society that is difficult to predict.



Critical Infrastructure Sectors

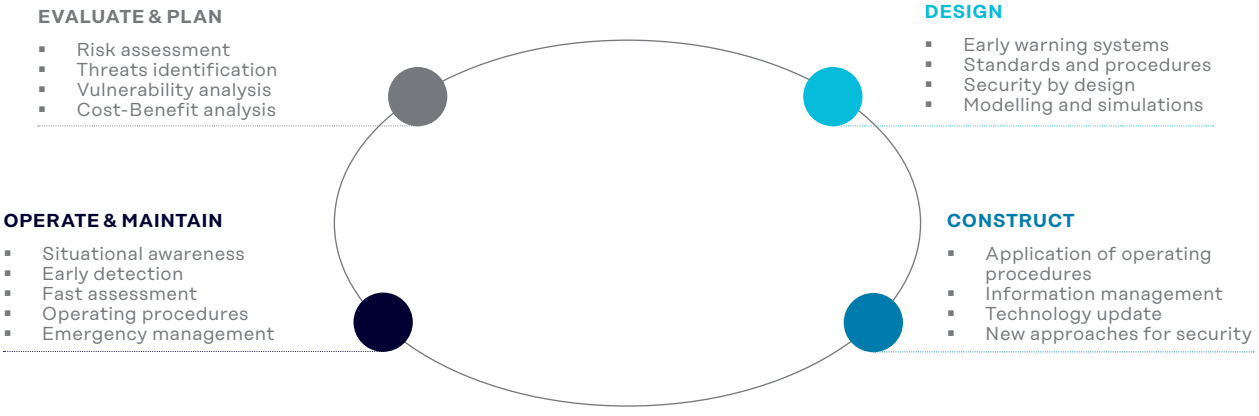
Linking Resilience to Asset Management

Traditionally, Critical Infrastructure activities have been focused on the protection and reliability of infrastructure systems against known threats (mainly physical one). Given the networked character of the infrastructure, their complexity, mutual dependencies on one side and new, complex and emerging threats on the other side, an approach looking solely to the protection of Critical Infrastructure is not viable nor efficient anymore. To this end it is therefore fundamental to link Resilience to Asset Management so that to support the implementation of proper governance strategies that incorporate and make operational resilient approaches.

Indeed, integrating resilient approaches into Asset Management, allows the Owner, Operator or Manager of a Critical Infrastructure to build a more pragmatic approach towards an optimal Governance of an Asset, improving the integration across different disciplines and cross-functional coordination. RINA is pursuing, adopting and promoting a paradigm shift aimed at implementing Resilience of Critical Infrastructure across all phases of the life-cycle, from design to construction, to normal operations and emergency, embedded into the Asset Management process.

In this sense RINA can support the user by the definition of an Operational Resilience Plan (ORP) that:

- Complies with the resilience capabilities (plan/prepare, absorb, recover and adapt), taking into account reliability (low susceptibility), resistance (robustness), redundancy, as well as better response and recovery (rapidity and resourcefulness)
- Include the mapping and analysis of interdependencies among Infrastructure
- Is based on user defined most likely scenarios
- Encapsulates business continuity plan

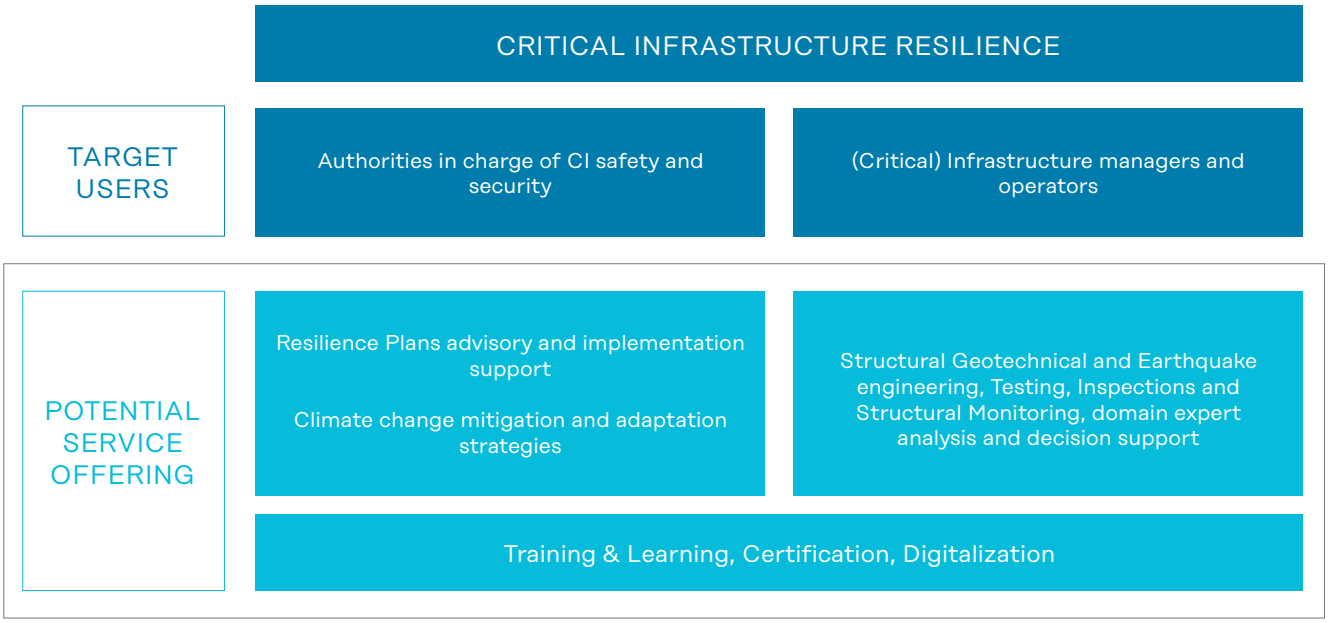


Linking Resilience to Asset Management

Users and Service offering

To strengthen our service offering and the delivery of added-value services to our clients (managers and operators of Critical Infrastructure, Authority in charge of their safety and security, companies providing services to CI owners), RINA has built its own digital platform, RINACube, that provides our clients with a complete level of services and a holistic view of RINA's digital services through a single sign-on.

The platform is open, to allow for data integration from various sources, and is capable of machine learning driven powerful analytics to correlate data and provide valuable business insights.



Users and service offering

In the area of Resilience Engineering, the digitalization process can support the transition towards more robust and integrated services that are spanning from Prevention to Mitigation, following a risk management cycle, across the various phases of the life-cycle of an infrastructure (from design to emergency operations). This includes the development of methodologies to assess risks from current and emerging threats and of tools to support decision making to enhance security and resilience and to mitigate environmental, economics and material damage impacts that may arise.

(Critical) Infrastructure Owner/Manager/Operator		Phases			
		Prevention	Detection	Response	Mitigation
Relevant phases across the life-cycle	Desing	●	●	●	●
	Construction	●	●		●
	Normal Operations	●	●	●	●
	Emergency Operations	●	●	●	●

As such, RINA can support the clients in:

- Planning ahead during the design phase (understanding future scenarios)
- Adapting and controlling (analysing cascading effects and their propagation)
- Recovering quickly from the minimum performance level (optimizing the recovery process)
- Restoring effectively (combining restoration strategies)

Areas of expertise

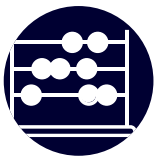

Risk Engineering


Geotechnical Engineering


Structural Engineering

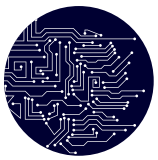

Earthquake Engineering


Climate Change


Asset Management


Testing & Inspection


Structural Monitoring


Software Engineering


Decision Support


Training & Learning

- Risk engineering, including the implementation of an all-hazards approach
- Geotechnical and geophysical engineering; structural and earthquake engineering
- Climate change adaptation, mitigation, assessment and policy advisory
- Asset management, including the implementation of performance-based approaches
- Non-destructive inspections and controls, Structural Health Monitoring (SHM)
- Software engineering, including tools for security risks management
- Decision support in securing resilience against combined physical and cyber threats
- Training and learning for awareness, preparedness and planning

Key Benefits

- Added value tools and services delivered via the corporate RINACube platform
- A resilient approach that integrate the various capabilities of Resilience (robustness, redundancy, resourcefulness, rapidity) into the Infrastructure Asset Management processes
- A bespoke decision support for infrastructure operators/ managers across all phases of the infrastructure life-cycle, from planning and decision, to design and construction, to operation and maintenance, up to crisis management
- A consolidated methodology for risk-based assessments (all-hazards, including emerging threats) and the identification of associated contingencies plans
- Strong competences in software and system development, integration and operation, supporting the implementation of joint security and privacy by design mechanisms
- Deep knowledge of cyber-physical risks and related mitigation actions, to ensure continuity plans and loss minimization, for various sectors and applications
- Deep understanding of the impact of climate change risks from design to operation and provision of a structured approach to their mitigation and identification of alternative strategies
- An integrated approach in earthquake and geotechnical engineering ranging from hazard identification, design specifications up to the adoption of mitigation actions
- Planning, designing and operating Structural Health Monitoring (SHM) strategies for loss prevention, remaining lifetime estimation, optimization of inspection and maintenance activities
- Comprehensive and systematic training services, provided by means of a rigorous analysis of organisational training requirements and the development of bespoke training solutions

---

info@rina.org
rina.org

jun19_eng