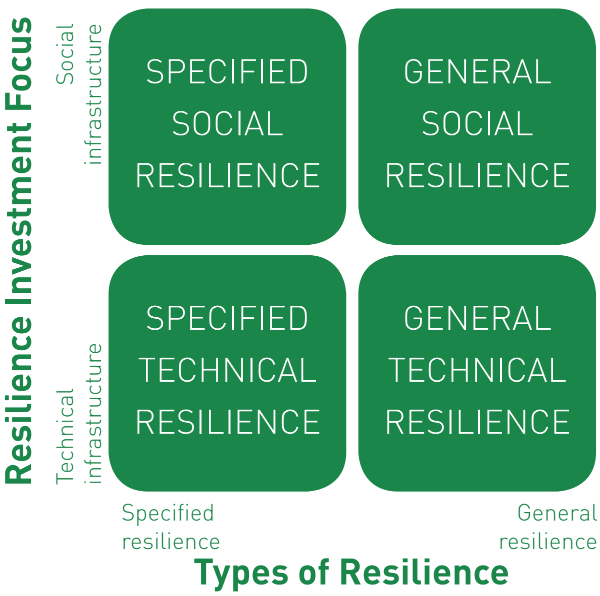
FRAMEWORK FOR RESILIENT ESSENTIAL SERVICES

CST POLICY BRIEF 2019 | LIZA VAN DER MERWE, REINETTE BIGGS, RIKA PREISER

Essential services, like water and electricity, underpin modern life. Disruption in service delivery exposes critical inter-dependency, ranging from community level to the national economy. Therefore essential service providers, such as energy utilities, have a duty of care to ensure resilient service delivery. Resilience is the ability of people, institutions and systems to adapt, survive, and thrive despite acute shocks or chronic stresses. Policy can promote pre-emptive and holistic resilience practices among essential service providers.

FRAMEWORK FOR CONCEPTUALIZING, ASSESSING, AND BUILDING THE RESILIENCE OF ESSENTIAL SERVICES

Building resilience requires attention to multiple aspects of the socio-technical systems that produce essential services. We have developed a framework that highlights the different domains of resilience in terms of a focus on investments in social versus technical infrastructure, and a focus on general versus specified resilience. Specified resilience focuses on building resilience to foreseeable eventualities through best practice approaches, while general resilience uses complexity-based approaches to build resilience to unpredictable and unprecedented disruptions. Investments in all four quadrants are required to build resilience of essential services.



Specified social resilience focuses on specific skills, response capabilities and preparedness to build resilience through processes and institutions that enhance the ability of people to deal with known hazards (e.g. business disruptions).

Specified technical resilience focuses on robust technical infrastructure, building resilience into components to ensure they are adequate, reliable and secure to known hazards (e.g. storms).

General social resilience focuses on collective human agency, agility, and volition to build resilience of people and processes to unknown and novel systemic changes and disruptions.

General technical resilience focuses on systems-level flexibility and adaptability to build resilience of the overall system through adaptive technologies and tools that offer systems-level flexibility to enable effective responses to uncertain and novel situations.

RESILIENCE ROLES AT DIFFERENT ORGANIZATIONAL LEVELS

A complex adaptive system is resilient if it can persist, adapt and transform at different levels and scales. Resilience can be operationalized by assigning responsibilities at the **operational**, **tactical** and **strategic** levels in an organization.

Strategic leadership takes a long-term perspective to timeously transform the organisation through emergent strategic planning to survive and thrive amid uncertainty, while navigating disruptive change, to intentionally transform its identity towards a more sustainable trajectory of development

Tactical leadership establishes adaptability through management control, continuous improvement, integrated response capabilities and scenario-based exercises, to enable the organisation to adaptively manage risk, bounce back better, and embrace opportunities for bouncing forward.

Operational leadership fosters persistence through operational control in daily operations to ensure that the system has the day-to-day ability to absorb a magnitude of disturbances and to anchor essential services with minimum disruption.

OPERATIONALIZING THE FRAMEWORK

Holistic resilience capabilities can be established by addressing each domain within each organizational level. An array of resilience indicators can be developed to operationalize this framework in building resilience. The indicators in the table below apply to electricity as an example of how the framework can be applied to Eskom, the South African national electrical utility.

	INDICATORS OF PERSISTENCE AT OPERATIONAL LEVEL	INDICATORS OF ADAPTABILITY AT TACTICAL LEVEL	INDICATORS OF TRANSFORMABILITY AT STRATEGIC LEVEL
SPECIFIED SOCIAL RESILIENCE	• Competent in decisions that require attention to detail and precision across multiple recurring iterations. • Competent in execution of standard operating procedures, emergency roles and responsibilities, ability to execute pre-approved response plans and ability to effectively participate in simulation exercises.	• Competent in semi-structured decisions and ensuring efficient and effective use of resources through business planning, logistics coordination and operational improvements. • Contingency arrangements, response plans, and risk reduction strategies are systematically reviewed and adaptively revised to incorporate learning. • Response structures effectively integrate across functions.	• Competent in unstructured decisions that are complex, ambiguous and far-reaching in scope, entail high levels of uncertainty and often pertain to non-linear risks in the external environment. • Commitment to resilience through visible leadership in good-practice disciplines such as emergency preparedness and business continuity management. • Ownership of contingency arrangements, knowing and testing established plans and actively participating in emergency simulation exercises. • The ability to anticipate and avoid foreseeable, predictable, avoidable surprises.
SPECIFIED TECHNICAL RESILIENCE	• Infrastructure and assets well managed to required standards, including regular maintenance and tests of back-up technologies. • Deploy standardized redundancy criteria, have redundant equipment available and have efficient access to operational spares to restore network disruptions.	• Technical standards are adaptively revised to incorporate learning. Adaptive assessment approaches are applied and a portfolio of technical investments exist for disaster risk reduction. • Strategic spares are available for contingencies and response. • Engineers consider build-back-better and fail-to-safe design philosophies.	• Strategic commitment to invest in resilience, reserve margins and smart grid self-healing capabilities. • Decision-making considers impact of decisions on resilience of critical processes. • Adopt a modular substation design strategy; although initial cost is higher, it can standardize on spares and speeds up recovery.
GENERAL SOCIAL RESILIENCE	• People feel empowered to act in the interest of safety and resilience if events occur contrary to what is expected. • Follow intuition based on deep experience in situations that necessitate that the rules be broken. • Be comfortable to apply an incident command system to perform emergency operations during extreme events, even under great pressure. • Employ safe-to-fail scenarios in emergency exercises that stretch people beyond the plan.	• Network and mobilize support through strong social networks, third-party agreements and memorandums of understanding that have been established. • Monitor for signs of restorative or retributive justice exercised in supervision. • Identify heuristics used on the frontline, verify their validity and spread guiding heuristics to be used in crises. • Be comfortable to coordinate planning, and integrate situational awareness during the extreme event incidents to provide a common operational picture of unfolding events, execute tactical command, mobilize resources and coordinate logistics to support operations.	• Actively build a culture of resilience and safety, with restorative justice in word and deed. The ability to anticipate and avoid predictable surprises. • Evidence of valuing and actively building social and psychological capital, practice adaptive management and encourage decentralized self-organisation during disruption. • Strengthen external and internal connections in functions, across disciplines and with other sectors. • Be comfortable to fulfil the incident commander role during extreme events, be able to see the big picture, prioritize objectives, take decisions in spite of incomplete information and recognize when a regime shift has taken place.
GENERAL TECHNICAL RESILIENCE	• Be able to operate adaptive technology under pressure and maintain back-up and contingent systems components. • Technical capabilities that allow operational flexibility often beyond the infrastructure itself, for example, demand response contracts.	• Review asset condition monitoring practices and test results of deployed technologies that provide adaptive capacity and strengthen systems flexibility, for example, unit islanding schemes and black-start tests performed. • Consider technology solutions beyond the infrastructure system.	• Proactive investment in systems flexibility (in electricity supply these include smart metering, smart grid, containerized mobile substations, demand-side products and supply-side mix).

ASSESSING AND BUILDING RESILIENCE

The domains of resilience in this framework are different in kind. Different approaches are required to build and assess resilience in each. The portfolio of resilience building interventions has to balance these objectives. A focus on one may erode resilience in the others.

SUMMARY OF APPROACHES TO BUILD AND ASSESS RESILIENCE IN THE FOUR DOMAINS	
SPECIFIED SOCIAL RESILIENCE Resilience of critical components to specific risks (e.g. business process disruption due to cyber-attack) through people, plans and preparedness. **To build** Establish specific skills, response capabilities and preparedness in people, processes and institutions. **To assess** Verify established preparedness against predefined objectives contained in contingency arrangements, plans and procedures.	**GENERAL SOCIAL RESILIENCE** Resilience of the overall system to novel and unknown risks, through people, processes and institutions. **To build** Establish collective human agency, agility and volition of people and processes, along with enabling institutions to withstand unknown hazards. **To assess** Make sense of levels of social capital, the collective sense of coherence, the nature of the safety culture, adaptive management practices, and resilience leadership employed.
SPECIFIED TECHNICAL RESILIENCE Resilience of technical infrastructure to specific risks (e.g. substation due to storm) to ensure it is adequate, reliable, and secure. **To build** Build robustness into technical infrastructure components to be adequate, reliable, and secure. **To assess** Employ quantitative measures, test compliance to engineering standards, and controls applied throughout the asset life-cycle.	**GENERAL TECHNICAL RESILIENCE** Resilience of the technical system to novel and unknown risks, through network topology and adaptive technologies, which offer systems-level flexibility to enable an agile response across the system in dealing with uncertainty. **To build** Strengthen systems-level flexibility and connectivity through adaptive tools and technologies, to support and enable effective response in dealing with uncertainty. . **To assess** Test flexibility of the overall system under strain and failure conditions; evaluate complex network topology & system dynamics for resilience.

Socio-technical systems that deliver essential services need ambidexterity to persist, adapt and transform in the face of acute shocks, chronic stress and discontinuous change. These capabilities can also enable utilities to better navigate local and global energy transitions.

FURTHER READING

Dahlberg, R. 2015. 'Resilience and complexity: conjoining the discourses of two contested concepts', Culture Unbound: Journal of Current Cultural Research. Linköping University Electronic Press, 7(3), pp. 541–557. doi: 10.3384/cu.2000.1525.1572541.

Folke, C., S. R. Carpenter, B. Walker, M. Scheffer, T. Chapin, and J. Rockström. 2010. 'Resilience thinking: Integrating resilience, adaptability and transformability', Ecology and Society, 15(4). doi: 10.5751/ES-03610-150420.

National Academies of Sciences, Engineering, and Medicine (NAS). 2017. Enhancing the resilience of the nation's electricity system. National Academies Press, Washington, D.C., USA. [online] URL: https://doi.org/10.17226/24836

National Infrastructure Advisory Council (NIAC) 2010. A Framework for Establishing Critical Infrastructure Resilience Goals. National Infrastructure Advisory Council. Available at: https://www.dhs.gov/national-infrastructure-advisory-council.

Panteli, M., and P. Mancarella. 2015. The grid: stronger, bigger, smarter?: Presenting a conceptual framework of power system resilience. IEEE Power and Energy Magazine 13(3):58-66. http://dx.doi.org/10.1109/MPE.2015.2397334

Poli, R. 2013. A note on the difference between complicated and complex social systems. Cadmus 2(1):142-147. [online] URL: http://cadmusjournal.org/article/volume-2/issue-1-part-3/note-differencebetween-complicated-and-complex-social-systems

Van der Merwe, S. E., Biggs, R. and Preiser, R. 2018. 'A framework for conceptualizing and assessing the resilience of essential services produced by socio-technical systems', Ecology and Society, 23(2). Available online: https://doi.org/10.5751/ES-09623-230212

FOR FURTHER INFORMATION PLEASE CONTACT:

CENTRE FOR COMPLEX SYSTEMS IN TRANSITION
Stellenbosch University, Private Bag X1, The Stables at 19 Jonkershoek Road, Stellenbosch, South Africa
Tel: +27 21 808 9607 | Website: www.sun.ac.za/cst