# Editorial

Adrian V. Gheorghe* and
Polinpapilinho F. Katina

Department of Engineering Management and Systems Engineering,
National Centers for System of Systems Engineering,
Old Dominion University,
2101 Systems Research and Academic Building,
Norfolk, VA 23508, USA
Email: agheorgh@odu.edu
Email: pkatina@odu.edu
*Corresponding author

**Biographical notes:** Adrian V. Gheorghe holds an MSc in Electrical Engineering from the Faculty of Power Engineering, Bucharest Polytechnic Institute in 1968, Bucharest, Romania; PhD in Systems Science/Systems Engineering from City University, London, UK in 1975; an MBA from Academy of Economic Studies, Bucharest, Romania in 1985; and MSc Engineering-Economics, Bucharest Polytechnic Institute, Bucharest, Romania. He serves as a Senior Scientist with the European Institute for Risk and Communication Management (EURISC), Bucharest, Romania and Vice President, World Security Forum (WSF), Langenthal, Switzerland. He is a Professor of Engineering Management and Systems Engineering and Batten Endowed Chair on System of Systems Engineering with the Department of Engineering Management and Systems Engineering at Old Dominion University (ODU) in Norfolk, Virginia, USA.

Polinpapilinho F. Katina is a PhD candidate in the Department of Engineering Management and Systems Engineering at Old Dominion University (ODU) in Norfolk, Virginia, USA. He holds an MEng in Systems Engineering in 2011 and BSc in Engineering Technology in 2009. He serves as a Graduate Research Assistant at National Centers for System of Systems Engineering (NCSOSE). His areas of research include critical infrastructure protection, decision-making under uncertainty, complex system governance, infranomics, systems engineering, systems of systems engineering and systems theory. He recently co-edited a critical textbook on *Infranomics*. His research has been published in the *International Journal of Critical Infrastructures*, *International Journal of Critical Infrastructure Protection*, *International Journal of System of Systems Engineering*, and the *Journal of Requirements Engineering*.

## 1 Introduction

In 1983, the US Congressional Budget Office (USCBO) (1983) stipulated that long-term economic growth was intrinsically linked with functioning of public works infrastructures such as highways, public transits systems, wastewater treatment plants, water resources, air traffic control, air ports, and municipal water supplies. In the last two centuries, growing concerns in infrastructure deterioration – wear and tear, technological

obsolescence, and decreasing capacity to serve future population, continue to persist (USCBO, 1983; Vaughan and Pollard, 1984). Remarkably, issues confronted in the 21st century – enabling, maintaining, and sustaining public well-being through protection of infrastructures, continue to challenge policy-makers, infrastructure operators, and scientists alike (Clinton, 1996; Gheorghe, 2006; Thissen and Herder, 2003). Moreover, overtime, new threats have emerged from a changing landscape of rapid technological and institutional changes, increasing complexity steaming from trans-national interdependencies, and increasing concerns of a more sustainable society that can meet demand for quality services. These concerns form a nexus of challenges for research in the domain of critical infrastructures.

The domain of critical infrastructures, at a very basic level, addresses elements of assessment, remediation, indications and warnings, mitigation, response, and reconstruction pertaining to hazards, risks, and threats from natural and manmade events affecting public well-being – public safety, economic vitality, and security. The frequency of occurrences and increasing loss of lives and property associated with natural and man-made events leads us to question effectiveness and applicability of traditional scientific methods. In this special issue, we contribute to a wider body of knowledge calling for a (re)thinking of critical infrastructures and suggesting viewing infrastructures as interconnected complex systems. In this paper, basic concepts of dependency and interdependency, resiliency, and risk governance take precedence (Katina and Hester, 2013).

Infrastructure dependency connotes a reliance on services and products of a given infrastructure system. This concept addresses how much an infrastructure is a part of people's daily lives, and thus, critical to people's well-being. A review of literature reveals that economic performance, infrastructure effects, criticality, community awareness, importance, satisfaction, critical quality, scope, magnitude of failure, system user impact, political relevancy, and cost to repair provides important measures for infrastructure dependency (Katina and Hester, 2013).

Critical infrastructures do not operate in isolation. They exhibit interconnectedness behaviour such that the output of a given infrastructure is contingent on input from other interconnected infrastructures. This suggests that the goal of maintaining and sustaining public well-being depends on inputs and outputs from multiple *interconnected infrastructures*. Thus, to sufficiently address issues in this domain, an analysts needs to understand interdependencies among infrastructure systems. This is especially critical since a seemingly isolated event (i.e., a failure) could have the ability to cascade and cause major failures far beyond its point of origin (Weil and Apostolakis, 2001; Kröger and Zio, 2011).

The nature of infrastructure dependency and interdependency suggests that we have to (re)formulate *risk*. Traditionally, we have defined risk in terms of probability of occurrence of an event and its consequences (ASCE, 2009). However, risk governance for interdependent infrastructure systems must also consider elements beyond system of interest. Katina and Hester (2013) suggest infrastructure vulnerability, likelihood of failure, threat, exclusivity, environmental factors, frequency, intent, physical property damage, safety, and fragility as variables for quantifying risk in infrastructure systems.

Natural systems have an intrinsic ability and tendency to bounce back after an event (e.g., a failure, an attack). This tendency is what Martin-Breen and Anderies (2011, p.7) refer to as *resilience* and define it as "the ability to withstand, recover from, and reorganize in response to crises". Our question becomes, *could this be said of man-made*

*infrastructure systems*? Disruptions ranging from uncertainty of natural (e.g., hurricanes) to man-made (e.g., terrorism) events, suggest that policy-makers, infrastructure operators, and scientists must address infrastructures in terms of resiliency to known and unknown risk-events. To mimic natural systems, infrastructure systems must be designed with the capability for quick recovery and survive despite the 21st century 'wicked' landscape of terrorism and global warming (Martin-Breen and Anderies, 2011). Important measures for infrastructure resiliency include system defensive characteristics (e.g., deterrence, detection, delay, response, time to recovery; system defensive properties (e.g., physical barriers), maintenance capability to resist attacks; susceptibility, adaptive capacity, time to repair, availability of warning systems, and critical time (Katina and Hester, 2013; Martin-Breen and Anderies, 2011).

Meeting the grand challenge of ensuing public well-being in the domain of critical infrastructure largely depends on:

1 viewing the world at the metasystem level

2 addressing the high degree of social-technical complexity.

A metasystem provides a view of a higher logical order than any constituent system. The nature of infrastructure dependency coupled with interdependencies and the associated risks, suggests a need for holistic view that must draw on variety of fields to support the "analysis and decision-making regarding the Metasystem" [Gheorghe and Masera, (2014), p.3]. This is in the opposition to viewing infrastructures closed and isolated systems. When we engage in research at the metasystem level of critical infrastructures, we draw upon knowledge on a variety theories, assumptions, models, and methods that enable conceptualising, design, development, operation, transformation, and maintenance of interdependent complex systems – or rather as Gheorghe and Masara (2014) posit, *infranomics*. Under this paradigm, the analysis is not limited to technical elements of system of interest; rather, the analyst must address internal as well as external technical and social elements beyond any one system of interest (Hughes, 1998).

Ultimately, the domain of critical infrastructure deals with engineering systems – "a class of systems characterized by a high degree of technical complexity, social intricacy, and elaborate processes, aimed at fulfilling important functions in society" [De Weck et al., (2011), p.31]. Critical infrastructures are made of parts (elements) that serve a particular function – perhaps via a series of processes – in the society and thus meet a basic characterisation of 'system' (Gibson et al., 2007). Moreover, engineering systems are characterised by existing in the real world, artificiality, dynamic, hybrid state, and involvement of human control (De Weck et al., 2011). Table 1 is drawn to elaborate on implications of engineering systems for the critical infrastructure domain.

Clearly, the domain of critical infrastructures deals with engineering systems. However, the dwindling applicability of 'old' methods and tools cannot be expected to address increasing 21st century concerns. There is need to (re)think such issues as infrastructure protection, deterioration, assessment, remediation, indications and warnings, mitigation, response, and reconstruction. Again, drawing on current societal changes, it is increasingly clear that we must continuously evolve our views on basic concepts of maintain and sustaining public well-being by combining policy, technology, and science. This special issue presents an initial outlook of recent development emphasising theory and practice of resiliency in engineering systems. In all, the ten articles contribute to our contemporary understanding of how resiliency might be used to

address different systems in the domain of critical engineering systems within the purview of natural and man-made events.

**Table 1** Relating engineering systems to critical infrastructures

| *Characteristic of engineering systems* | *Description of characteristic* | *Implication for critical infrastructures* |
|---|---|---|
| Exists in the real world | Engineering systems always have some physical reality among their components (De Weck et al., 2011). | Critical infrastructures include physical systems (e.g., highways and hospitals) as well as virtual systems (e.g., supervisory control and data acquisition, SCADA). Virtual systems cannot exists without physical components (e.g., routers and servers). |
| Artificiality | Engineering systems exists by virtue of some human intervention. A deliberate process that involves human design and implementation is required (De Weck et al., 2011). | As modern society evolves, creating new social changes (e.g., demand for quality goods and services); human interventions (e.g., policing and management) provide means to meeting contemporary challenges in the domain. |
| Dynamical | The state and configuration of engineering systems including properties, elements, and interrelationships are always fluid and changing with time (De Weck et al., 2011). | Critical infrastructures operate in a changing environmental flux and evolve to accommodate shifting needs of the public – largely influenced by evolving research, technology, social, and policy changes. |
| Hybrid state | Engineering systems operate at a mixture of states such that some states are continuous (e.g., water levels at a dam for electricity generation) while other are discrete (e.g., on/off power network) (De Weck et al., 2011). | Not only must critical infrastructures operate in a mixture of hybrid states – continuous and discrete, they also exists in a failure mode state and must be restored as part of their resiliency capability. |
| Some human control | Engineering systems always require human involvement such as designers, operators, or policy-makers (De Weck et al., 2011). | Infrastructure owners, operators, consumers, and policy-makers play a major role the socio-technical operations as well as performance of infrastructures. |

## 2 The contents of the special issue

The first paper, by Yannick Hémond and Benoît Robert, focuses on resilience assessment. Rather than seeing assessment as a one-and-done activity, resilience assessment is presented as a dynamic continuous process that increases one's ability to management infrastructure within a changing environment. Authors provide a set of measures that can be used for assessment for the infrastructure resiliency. The promising

theoretical methodology has ability to assess resilience – ranging from a firm to a regional scale.

The second paper is written by Eric Vugrin, Mark Turnquist, and Nathanael Brown focuses on enhancing resilience in transportation systems. In this paper, the authors draw on the traditional concept of resilience – physical protection and asset hardening to include ability to withstand and rapidly recover from disruptions. Specifically, the authors use a project-oriented perspective to propose a general optimisation methodology that considers sequencing a set of repair tasks that must be undertaken to enhance recovery response – a specific component of resilience in a networked transportation system.

The third paper, by Michael Kalinski, L. Sebastian Bryson, Alex Krumenacher, Bryan Phillips, Zack Ethington and Benjamin Webster, reviews the current security landscape for protecting dams as critical infrastructures. The paper focuses on the enhancing resilience of dams through an integrated approach of detection and surveillance technologies. Authors suggest that resilience of dams is intrinsically related to detection, deterrence, and defeat systems. Moreover, Kalinski et al. suggest that the maintaining public well-being is a complexity issue that might require examination of technology while considering social and political aspects.

The fourth paper, by William Hurst, Madjid Merabti, and Paul Fergus, is a continuation of previous research promoting critical infrastructure security through use of behavioural observation for critical infrastructure security support (BOCISS). Using a simulated nuclear power plant to generate datasets based on observable behaviours of system components (normal and attack mode), authors suggest that it is possible to enhance plant security.

The fifth paper, by Antonio Di Pietro and Stefano Panzieri, focuses on securing SCADA systems. This paper describes a reference model for a SCADA security testbed and its constituent elements. The model can be used in the virtual control system environment for the purpose of testing security standards aimed at prevent and reducing impact of cyber-attacks on physical processes of critical infrastructures.

In the sixth paper, Hosny Abbas suggests a range of challenges associated with SCADA systems. To meet the articulated challenges, Abbas suggest use of multi-agent systems to (re)think software engineering and architecture design. A first generation methodology supporting multi-agent systems design is provided along with possible applications in critical industrial systems.

Toshiyuki Yasui, Seiko Shirasaka, and Takashi Maeno's paper reminds us of the value of incorporating values of the general public in developing policy aimed at elevating social concerns related to engineering systems. Using a case of Fukushima, Japan, the authors propose a participatory and collaborative systems analysis model for public policy design. The model is then implemented to (re)discover problems and potential intervention points.

The work of Boris Petrenj and Paolo Trucco proposes a simulation-based approach to enhance resilience in critical infrastructures. While suggesting that the concept of resilience might be modified based on system of interest, they offer new measures for resilience and apply their approach to transportation infrastructure in the Milan metropolitan area.

The ninth paper, by Berna Eren Tokgoz and Adrian Gheorghe, explores 'probabilistic resilience of structures' that are exposed to natural elements. The authors develop and

implement a new methodology for quantification of resilience using probabilistic resilience measures of structural loss of estimation function, wind speed probability, recovery function, and loss of use function along with a geographic information system-based natural hazard loss estimation software package (i.e., HAZUS) to establish resilience of buildings. The approach might be used to identify the most vulnerable buildings in a natural disaster-prone area along with facilitating development of mitigation strategies for vulnerable buildings.

The final paper, by Tanya Le Sage, Hervé Borrion, and Sonia Toubaline, is focused on constraints of contemporary modelling and simulation of terroristic attacks. Specifically, the authors develop a user-layered approach that allows multiple stakeholders to interface with a single modelling environment. The research in this paper is concerned with modelling different user groups who have different requirements and addressing means for reducing vulnerability in such an environment.

From this limited set of papers, we can see limitations of current approaches and the need to expand our view of critical engineered systems by considering environment, catastrophe planning, and technological innovation.

## Acknowledgements

Many thanks to all the people who helped us in making this special issue possible. First, we would like to acknowledge the help of our reviewers whose help transformed these papers and tremendously improved the quality of the papers. We would also like to extend our appreciation to Miss Liz Harris whose assistance and persistence provided encouragement for completion of this special issue. Finally, our thanks to the authors who were willing to transform their manuscripts in a moment's notice!

## References

American Society of Civil Engineers (ASCE) (2009) *Guiding Principles for the Nation's Critical Infrastructure*, Reston, VA [online] http://www.asce.org/uploadedFiles/Infrastructure_-_New/GuidingPrinciplesFinalReport.pdf (accessed 17 October 2013).

Clinton, W.J. (1996) 'Executive Order 13010: critical infrastructure protection', *Federal Register*, Vol. 61, No. 138, pp.37345–37350.

De Weck, O.L., Roos, D. and Magee, C.L. (2011) *Engineering Systems: Meeting Human Needs in a Complex Technological World*, MIT Press, Cambridge, MA.

Gheorghe, A.V. (2006) *Critical Infrastructures at Risk: Securing the European Electric Power System*, Vol. 9, Springer, Dordrecht, The Netherlands.

Gheorghe, A.V. and Masera, M. (2014) 'Infranomics: a discipline-of-disciplines for the XXIst century', in Gheorghe, A.V., Masera, M. and Katina, P.F. (Eds.): *Infranomics*, pp.1–7, Springer International Publishing.

Gibson, J.E., Scherer, W.T. and Gibson, W.F. (2007) *How to do Systems Analysis*, Wiley-Interscience, Hoboken, NJ.

Hughes, T.P. (1998) *Rescuing Prometheus*, Pantheon Books, New York, NY.

Katina, P.F. and Hester, P.T. (2013) 'Systemic determination of infrastructure criticality', *International Journal of Critical Infrastructures*, Vol. 9, No. 3, pp.211–225.

Kröger, W. and Zio, E. (2011) *Vulnerable Systems*, Springer-Verlag, London, UK.

Martin-Breen, P. and Anderies, J.M. (2011) *Resilience: A Literature Review*, p.64, The Rockefeller Foundation, New York, NY [online] http://www.rockefellerfoundation.org/blog/resilience-literature-review (accessed 5 August 2014).

Thissen, W.A. and Herder, P.M. (2003) *Critical Infrastructures: State of the Art in Research and Application*, Kluwer Academic Publishers, Boston.

US Congressional Budget Office (USCBO) (1983) *Public Works Infrastructure: Policy Considerations for the 1980s*, US Congressional Budget Office, Washington, DC [online] http://www.cbo.gov/sites/default/files/cbofiles/ftpdocs/50xx/doc5046/doc20-entire.pdf (accessed 20 August 2014).

Vaughan, R. and Pollard, R. (1984) *Rebuilding America's infrastructure: an agenda for the 1980s*, Vol. 1, Council of State Planning Agencies, Washington, DC.

Weil, R. and Apostolakis, G. (2001) 'A methodology for the prioritization of operating experience in nuclear power plants', *Reliability Engineering & System Safety*, Vol. 74, No. 1, pp.23–42.