Risk Analysis
AN INTERNATIONAL JOURNAL
An Official Publication of the Society for Risk Analysis

CALL FOR PAPERS

Special Issue of *Risk Analysis* on

Resilience Analytics for Cyber-Physical-Social Networks

Guest editors:

- Kash Barker, University of Oklahoma
- Jose E. Ramirez-Marquez, Stevens Institute of Technology
- Giovanni Sansavini, ETH Zurich

The US government has increasingly emphasized resilience planning for critical infrastructure networks. Presidential Policy Directive 21 [White House 2013] states that these networks "must be secure and able to withstand and rapidly recover from all hazards," where the combination of "withstanding" and "recovering" from disruptions constitutes *resilience*, a definition with which many agree [e.g., Haimes 2009, Aven 2011, Ayyub 2014]. According to the US Department of Homeland Security [2013], the resilient operation of critical infrastructure networks is "essential to the Nation's security, public health and safety, economic vitality, and way of life." Governments across the globe have followed suit. Further, the resilience of communities after a disruptive event has become an important topic, acknowledging that infrastructures do not exist for their own sake but serve society (e.g., citizens, industries) [NIST 2015].

As such, three important (and interdependent) cyber-physical-social networks include [Barker et al. 2017]: (i) *Infrastructure networks* that are the engineered cyber-physical systems that enable essential "lifeline" services for society, (ii) *Service networks* that are engaged in a disruption to enable the function of other networks, and (iii) *Community networks* that represent the interconnected society that the other networks support. Infrastructure networks and service networks connect communities, enable economic prosperity, and provide for societal interactivity.

Data describing the performance of such cyber-physical-social networks are particularly important before, during, and after a large disruption because of the central role these networks play in supporting the society's resilience. These data may come from sensors embedded in the physical infrastructure, or from cameras which monitor system performance, but they also may be generated at the service network level in such forms as data feeds from emergency services operations, or at the community network level in such forms as social media posts. This availability of data has the potential to inform decisions through the application of advanced analytical methods, or *analytics*, thereby improving resilience. *Descriptive analytics* refers to techniques that effectively describe and possibly help visualize

the performance of the interdependent networks before, during, and after a disruptive event. *Predictive analytics* involves models that help determine complex patterns and relationships among variables to quantify the likelihood and the impact of future events and thus reduce the associated uncertainty. While descriptive analytics relate to the current or historic states of system, and predictive analytics attempt to quantify future states, *prescriptive analytics* provides guidance on how to achieve desirable resilience outcomes and combines with system modeling for estimating the benefits of resilience-improving strategies. Further, learning analytics addresses how we adapt with new information, and evaluation analytics assesses the effectiveness of data-driven policies.

To address the increasingly important area of modeling the resilience of cyber-physical-social networks, *Risk Analysis* calls for papers to be published in a special issue with the topic **Resilience Analytics for Cyber-Physical-Social Networks**. Topics of the special issue can include, but are not limited to, the following specific issues:

- Models of reliability, vulnerability, and/or recovery of cyber-physical-social networks
- Measures of resilience driven by descriptive, predictive, and/or prescriptive analytics
- Interdependencies among cyber-physical-social networks
- Community resilience to physical infrastructure disruption
- Emergency response and/or humanitarian logistics integrated with physical infrastructure disruption

Manuscript submission:

Please submit your papers via the online submission portal at: http://manuscriptcentral.com/riskanalysis. Please be prepared with a list of three keywords and suggested names and e-mail addresses for three potential reviewers.

Please be sure to indicate in your cover letter that you are submitting the paper for this special series. Submitted articles must not have been previously published or currently submitted for journal publication elsewhere. As an author, you are responsible for understanding and adhering to submission guidelines, which can be accessed at http://sra.org/sra-journal or http://manuscriptcentral.com/riskanalysis. Each submitted manuscript will undergo a rigorous review process.

Important dates:
Submission deadline: November 1, 2017
First reviews (target): March 1, 2018
Special issue published: Late 2018 or early 2019

References:

Aven, T. 2011. On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience. *Risk Analysis*, **31**(4): 515-522.

Ayyub, B.M. 2014. Systems Resilience for Multihazard Environments: Definition, Metrics, and Valuation for Decision Making. *Risk Analysis*, **34**(2): 340-355.

Barker, K., J.H. Lambert, C.W. Zobel, A.H. Tapia, J.E. Ramirez-Marquez, L. Albert, C.D. Nicholson, and C. Caragea. 2016. Defining Resilience Analytics for Interdependent Cyber-Physical-Social Networks. *Sustainable and Resilient Infrastructure*, **2**(2): 59-67.

Department of Homeland Security. 2013. *National Infrastructure Protection Plan*. Washington, DC: Office of the Secretary of Homeland Security.

Haimes, Y.Y. 2009. On the Definition of Resilience in Systems. *Risk Analysis*, **29**(4): 498-501.

White House. 2013. *Presidential Policy Directive 21 -- Critical Infrastructure Security and Resilience*. Office of the Press Secretary: Washington, DC.