Preface

Frédéric Petit*, Julia Phillips and David Brannegan

Argonne National Laboratory,
Risk and Infrastructure Science Center (RISC),
Global Security Sciences Division,
9700 South Cass Avenue, Bldg. 221,
Argonne, IL 60439, USA
Email: fpetit@anl.gov
Email: phillipsj@anl.gov
Email: dbrannegan@anl.gov
*Corresponding author.

Biographical notes: Frédéric Petit is a Research Scientist specialising in critical infrastructure interdependencies and resilience at Argonne National Laboratory. He leads methodology development to assess preparedness, mitigation, response, recovery, and overall resilience capabilities of facilities, communities, and regions. He applies his expertise to assess the overall risk, vulnerability of, and threats to critical infrastructure. He received his PhD from the École Polytechnique de Montreal in Civil Engineering, where he focused on vulnerability analysis techniques for critical infrastructure and dependencies on cybernetics. After an initial education in earth sciences and environmental sciences, he has specialised in risk management and business continuity since 2002.

Julia Phillips is the Deputy Director of Methodology for RISC at Argonne National Laboratory. She has considerable experience in the application of operations research methods in a number of different disciplines, including decision analysis, modelling and simulation, and statistical analysis. She is currently assisting with the development and implementation of risk methodologies with respect to critical infrastructure with special focus on capturing system-level resilience and the impacts of dependencies and interdependencies between critical infrastructure assets and systems. Prior to joining RISC, she spent 13 years as an active duty Air Force Officer as a Scientific Analyst. She received her PhD in Operations Research from the Colorado School of Mines in Golden, Colorado.

David Brannegan is the Director of RISC at Argonne National Laboratory. RISC is a multidisciplinary applied research centre that delivers risk and resilience capabilities to inform stakeholder decision-making. Prior to his position with Argonne National Laboratory, he was a Branch Chief at the US Department of Homeland Security. He also held previous positions conducting international counter-proliferation analysis for Computer Sciences Corporation, as well as assessment of multilateral export control and US-European relations for the Henry L. Stimson Center, a Washington DC-based think tank. He received his Bachelor's in Political Science from the College of the Holy Cross and Master's in International Relations from the Maxwell School of Citizenship and Public Affairs at Syracuse University.

Efforts to enhance the protection and overall resilience of a facility must consider all dependencies (e.g., physical, cybernetic, geographic, and logical). Such an all-encompassing assessment accounts for potential vulnerabilities that may exist outside traditional facility 'boundaries'. The degradation of the supply of resources from one facility in support of another facility can cause direct and potentially severe impacts. However, it is also important to consider the fact that bidirectional relationships between facilities may exist. A situation in which two infrastructures are dependent on each other is called interdependency.

Dependencies and interdependencies are complex elements to consider in risk assessments, risk management, and business continuity procedures as they are dynamic and multidimensional. Although it may be obvious that there exists a need to identify and mitigate potential dependencies and interdependencies, they tend to be extremely difficult to capture and understand in totality due to their complexity.

The presence of multiple interconnected sets of infrastructure across multiple jurisdictions adds a system of systems dimension to the interdependency discussion. Vulnerabilities resulting from infrastructure interdependencies are generally not as well understood as other vulnerabilities. A single-point of failure can lead to multiple infrastructure disruptions in multiple geographic locations. Though there is no single solution as to how to analyse interdependencies, it is clear that enhancing capabilities and innovations in that field is critical.

The main purpose of this special issue is to present recent advancements related to the assessment of infrastructure dependencies and interdependencies, the modelling of complex critical infrastructure systems, and the consideration of these elements in risk assessment and management methodologies to support decision-making. This special issue contains three papers that represent the diversity of problems and approaches when considering complex systems dependencies and interdependencies.

The first paper, 'Tightly coupled governance for loosely coupled wicked problems: the train explosion in Lac-Mégantic case', presents and analyses governance components and the complexity and interdependencies of actors at a macro level by studying the Lac-Mégantic disaster that occurred in Quebec on July 6, 2013.

The second paper, 'Dependencies in enterprise networks and its influence on a focal company's global strategy: a theoretical analysis', focuses on dependencies and interdependencies at a micro level by addressing dependency relationships between a focal company and its partners at the early stages of a project. The goal of the report is to understand the behaviour and influence of stakeholders on the strategy, tactics, and operational actions of different firms.

The third paper, 'Modelling and analysis of availability for critical interdependent infrastructures', offers an analysis at an intermediate level between macro and micro approaches. This paper proposes an analysis framework for critical interdependent infrastructures exposed to disruptions caused by equipment failures, cascading errors from neighbouring infrastructures, and the damages resulting from natural catastrophes.

Dependencies and interdependencies influence all components of risk (threat/hazard, vulnerability, resilience, and consequence), can themselves be a threat or hazard, can affect the resilience and protection performance of critical infrastructure, and can lead to the propagation of cascading and escalating failures. Dependencies and interdependencies must be integrated into risk and resilience methodologies. A data-driven capability that operationalises the analysis of dependencies and interdependencies would not only provide an unprecedented level of situational awareness, but also enable decision makers

to anticipate disruptions. To achieve this ultimate goal, the development of a comprehensive and interactive assessment of critical infrastructure dependencies and interdependencies requires multidisciplinary or 'socio-technical' approaches combining multiple areas of expertise (e.g., engineering, social sciences, business continuity, and emergency management) in an adaptive and flexible assessment framework.

We would like to thank all the researchers who submitted papers and all those who were involved in the review process. We hope that readers will enjoy this special issue of the *International Journal of Risk Assessment and Management*, and that it will generate further discussion and support future research in the field of dependencies and interdependencies.