Editorial: Games and Decisions in Reliability and Risk

Refik Soyer, Suleyman Ozekici

PII: S0951-8320(18)30885-8
DOI: 10.1016/j.ress.2018.07.019
Reference: RESS 6218

To appear in: *Reliability Engineering and System Safety*

Please cite this article as: Refik Soyer, Suleyman Ozekici, Editorial: Games and Decisions in Reliability and Risk, *Reliability Engineering and System Safety* (2018), doi: 10.1016/j.ress.2018.07.019

Editorial: Games and Decisions in Reliability and Risk

Refik Soyer
Department of Decision Sciences
George Washington University, USA

Suleyman Ozekici
Department of Industrial Engineering
Koc University, Turkey

The aim of this special issue is to bring together recent advances in the use of game and decision theoretic methods in reliability and risk analysis. Due to the interdisciplinary nature of the theme, the special issue involves novel applied and methodological research from diverse disciplines such as economics, engineering, mathematics, national security, probability, and statistics. The special issue contains nine papers. Three of these papers were presented at the Fourth Symposium on Games and Decisions in Reliability and Risk which was held in Istanbul, Turkey on June 17-19, 2015.

The first article, "A graphical method for simplifying Bayesian games" by Thwaites and Smith shows how chain event graphs (CEGs) can be used in representing and solving Bayesian games. The authors point out that CEGs, which were introduced recently for Bayesian learning and model selection, provide an effective alternative to multi-agent influence diagrams for games with highly asymmetric trees.

The next three papers deal with issues of national security involving multiple decision makers (agents) who have an adversarial relationship. The paper by Shan and Zhuang is on "Modeling cumulative defensive resource allocation against a strategic attacker in a multi-period multi-target game". The authors consider an extension of sequential defender-attacker games, which have been previously analyzed for a single target, by allowing for multiple targets. In so doing, they develop optimal allocations for the defender under different scenarios and present numerical illustrations using real data. The second paper is by Quijano, Ros-Insua and Cano on "Critical networked infrastructure protection from adversaries". The authors present a new perspective using the adversarial risk analysis (ARA) framework to deal with the protection of critical networked infrastructures. The ARA framework relaxes the "common knowledge" assumption of the game-theoretic approaches which have been considered for protection of infrastructure networks. The authors illustrate their approach by