Old Dominion University
ODU Digital Commons

Modeling, Simulation and Visualization Student Capstone Conference

Apr 14th, 12:00 AM - 12:00 AM

Risk-and-Resiliency-Intelligent Supply Chain (RRiSC)

Ahmad A. Abdelnabi
Old Dominion University

Ahmed M. Abdelmagid
Old Dominion University

Ghaith Rabadi
Old Dominion University

Andres Sousa-Poza
Old Dominion University

C. Ariel Pinto
Old Dominion University

Follow this and additional works at: https://digitalcommons.odu.edu/msvcapstone

 Part of the Operations and Supply Chain Management Commons, and the Systems Engineering Commons

Recommended Citation

Abdelnabi, Ahmad A.; Abdelmagid, Ahmed M.; Rabadi, Ghaith; Sousa-Poza, Andres; and Pinto, C. Ariel, "Risk-and-Resiliency-Intelligent Supply Chain (RRiSC)" (2022). Modeling, Simulation and Visualization Student Capstone Conference. 2. DOI:10.25776/87sm-cf37 https://digitalcommons.odu.edu/msvcapstone/2022/transbusindustry/2

This Paper is brought to you for free and open access by ODU Digital Commons. It has been accepted for inclusion in Modeling, Simulation and Visualization Student Capstone Conference by an authorized administrator of ODU Digital Commons. For more information, please contact digitalcommons@odu.edu.

RISK-AND-RESILIENCY-INTELLIGENT SUPPLY CHAIN (RRiSC)

Ahmad A. Bany Abdelnabi
Ahmed M Abdelmagid
Ghaith Rabadi, Ph.D.
Andres Sousa-Poza, Ph.D.
C. Ariel Pinto, Ph.D.

Engineering Management & Systems Engineering, Old Dominion University
Engineering Systems Building, Norfolk, VA 23529

abany001@odu.edu, aabde005@odu.edu, grabadi@odu.edu, asousapo@odu.edu, cpinto@odu.edu

ABSTRACT

This work proposes a risk-and-resiliency-intelligent supply chain (RRiSC) tool which is an SC risk management framework that leverages cutting-edge technologies in Artificial Intelligence (AI), Big Data Analytics (BDA), and Digital Twins (DT) to develop specific capabilities for SC risk management. RRiSC is a convergence of mature tools and techniques embedded in three modules: Modeling, Simulation, and Visualization – all together integrate the optimization, simulation, and data analytics to test the performance of the whole supply network under different scenarios through measuring the vital KPIs, identifying the vulnerabilities, and setting proactive plans to diminish risks consequences.

Keywords: supply chain, risk, resilience, modeling, simulation, visualization, digital twin, FDNA.

1 INTRODUCTION

The resiliency of the supply chain (or more accurately, network) could be defined as its ability to endure, cope, and recover from unexpected events (i.e., disruptions) that may occur and have negative effects on delivering the demand to customers (Pinto, McShane et al. 2012). Risk events include natural disasters like hurricanes and pandemics, as well as manmade disasters like wars – all of which can cause an interruption in meeting society's various needs. As various technologies emerge and adapt towards Industry 4.0, it is now becoming possible to analyze complex systems in ways that were not possible a decade ago. The objective of this work is to build the RRiSC tool which is capable to assess SC risks and dynamically monitor supplier relationships while hierarchically accumulating risk throughout the SC.

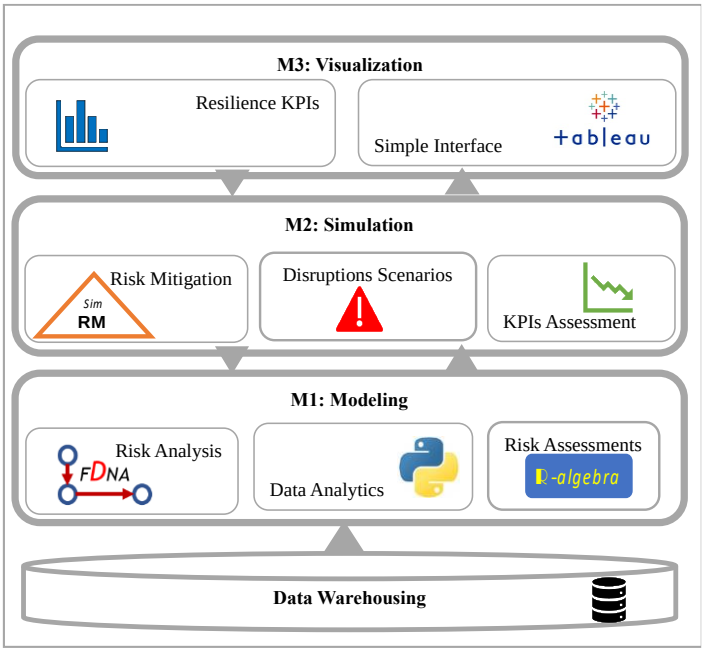
2 PROPOSED METHODOLOGY

RRiSC is a convergence of mature tools and techniques embedded in three modules.: Modeling, Simulation, and Visualization, as illustrated in Figure 1. M1 Modeling: this module includes data analytics and risk analysis. Data analytics include building suppliers' risk profiles based on a set of risk archetypes. The risk analysis will be implemented using Functional Dependency Network Analysis (FDNA), (Garvey et al., 2014), to manage the potential propagation of risk through the network. Also used is Enterprise Risk algebra (R-algebra) to measure enterprise capability risk (Pinto & Garvey, 2012). M2. Simulation: a simulation model will be designed to assess and mitigate the risk of disruptions in supply chain networks based on

©2021 Society for Modeling and Simulation (SCS) International

Sim-RM, as well as to measure its impact on the supply network KPIs (Seck et al., 2015) under various disruption scenarios. M3. Visualization: this module simplifies the interface for the end-user and allows controlling and monitoring of resilience KPIs (which are dependent on each company or system in terms of functional context, responsibilities, and goals (Karl, Micheluzzi et al. 2018)) for the supply network.

Figure 1. RRiSC Architecture



3 EXPECTED RESULTS

RRiSC will leverage the BDA approaches to assess each supplier based on historical data. The integration between optimization, simulation, and data analytics will confer a powerful tool for stakeholders to test the performance of the whole supply network under different scenarios by measuring the vital KPIs identifying the vulnerabilities, and setting proactive plans to diminish risks and consequences. Furthermore, RRiSC can be used to optimize the overall supply network's resiliency by controlling the ripple effect of risks in the supply network, such as sales, stock returns, and costs. Eventually, the Risks visualization module delivers a rich feedback loop through which managers can identify, mitigate, and monitor risks events to enhance supply network resiliency.

REFERENCES

Garvey, P. R., Pinto, C. A., & Santos, J. R. (2014). Modelling and measuring the operability of interdependent systems and systems of systems: advances in methods and applications. International Journal of System of Systems Engineering, 5(1), 1-24.

Karl, A. A., et al. (2018). "Supply chain resilience and key performance indicators: a systematic literature review." Production **28**.

Pinto, C. A., & Garvey, P. R. (2012). Advanced risk analysis in engineering enterprise systems. CRC Press.

Pinto, C. A., et al. (2012). "System of systems perspective on risk: towards a unified concept." International Journal of System of Systems Engineering 3(1): 33-46.

Seck, M., Rabadi, G., & Koestler, C. (2015). A simulation-based approach to risk assessment and mitigation in supply chain networks. Procedia Computer Science, 61, 98-104.