11TH INTERNATIONAL CONFERENCE
ON CRITICAL INFORMATION
INFRASTRUCTURES
SECURITY

10-12 October 2016
UIC HQ Paris

CRITIS
2016

Integrated Safety and Security Risk Assessment Methods: A Survey of Key Characteristics and Applications

Sabarathinam Chockalingam[a], Dina Hadžiosmanović[b], Wolter Pieters[a], André Teixeira[a], and Pieter van Gelder[a]

[a] *Faculty of Technology, Policy and Management, Delft University of Technology, The Netherlands*

[b] *Deloitte, The Netherlands*

TUDelft Deloitte. NWO
Netherlands Organisation for Scientific Research

Presentation Outline

- Safety vs. Security
- Safety and Security Interactions
- Risk Management Process
- Research Question and Research Objectives
- Observations
- Key Takeaways

Safety

Fukushima Daiichi Nuclear Disaster (2011)

Northeast Blackout (2003)

Security

German Steel Mill Hack (2014)

Lodz City Tram Hack (2008)

Safety and Security Interactions (1/2)

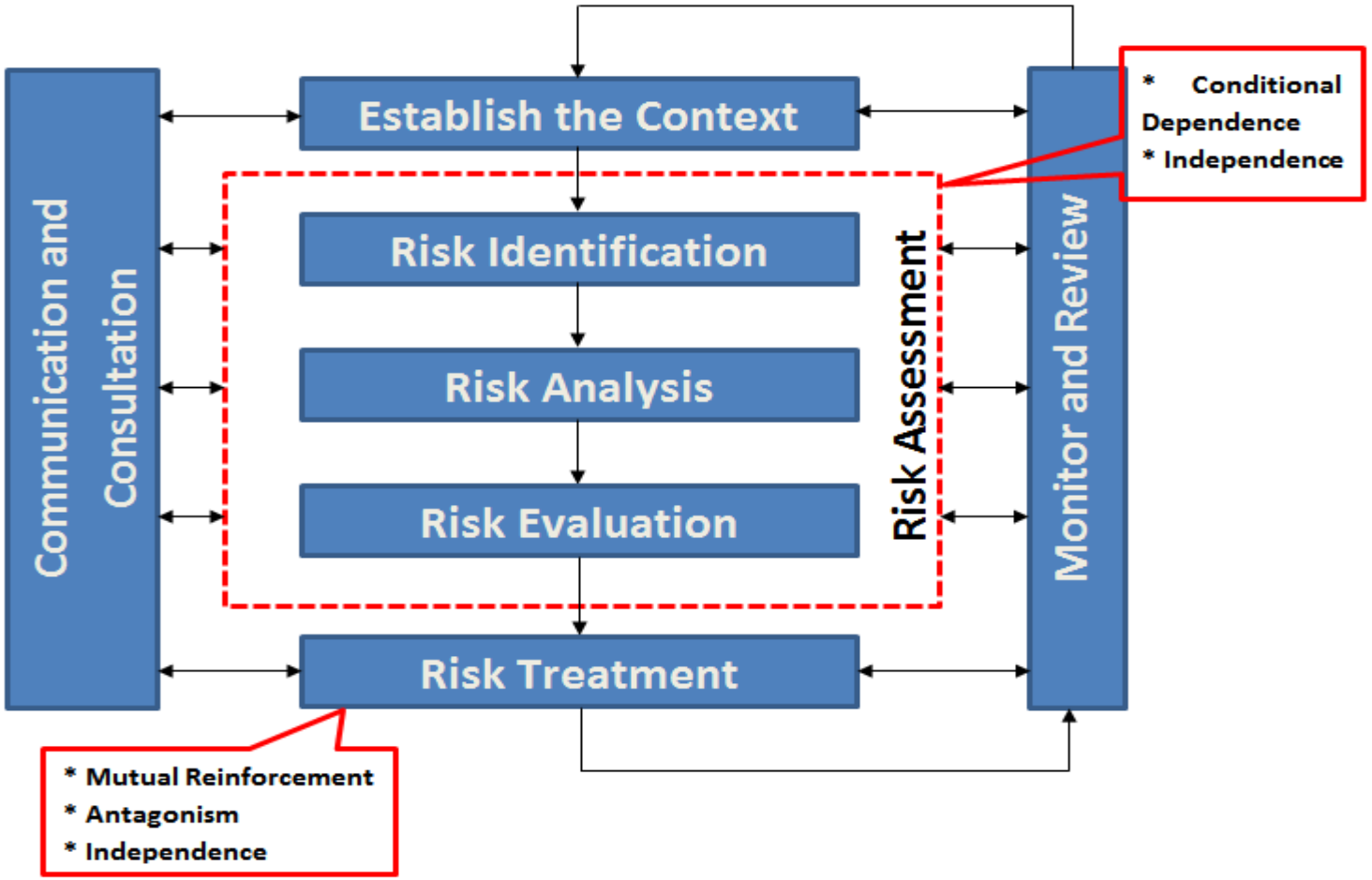
- Conditional Dependence
- Mutual Reinforcement
- Antagonism
- Independence (No Interaction)

Source: Pietre-Cambacedes, L., Bouissou, M.: Modeling Safety and Security Interdependencies with BDMP (Boolean Logic Driven Markov Processes). In: Proceedings of the IEEE International Conference on Systems Man and Cybernetics (SMC). pp. 2852 – 2861. (2010)

Safety and Security Interactions (2/2)

- This research was conducted as part of the project entitled "**Secure Our Safety: Building Cyber Security for Flood Management (SOS4Flood)**".

Risk Management Process (Based on ISO 31000)



Research Question and Research Objectives

RQ. What are the key characteristics of integrated safety and security risk assessment methods, and their applications?

RO1. To identify integrated safety and security risk assessment methods.

RO2. To identify key characteristics and applications of integrated safety and security risk assessment methods based on the analysis of identified methods.

Integrated Safety and Security Risk Assessment Methods

- Security-Aware Hazard Analysis and Risk Assessment (SAHARA)
- Combined Harm Assessment of Safety and Security for Information Systems (CHASSIS)
- Failure-Attack-CounTermeasure (FACT) Graph
- Failure Mode, Vulnerabilities, and Effect Analysis (FMVEA)
- Unified Security and Safety Risk Assessment
- Extended Component Fault Tree (CFT)
- Extended Fault Tree (EFT)

Sequential vs. Non-sequential

- **Sequential Integrated Safety and Security Risk Assessment Method:** SAHARA, FACT Graph, Unified Security and Safety Risk Assessment, Extended CFT, and EFT.
  - Partially addressed 'Conditional Dependencies'.
  - Addressed 'Independence'.
  - Bias involved in the sequential methods as importance placed on either 'Safety' or 'Security'.

- **Non-sequential Integrated Safety and Security Risk Assessment Method:** FMVEA, and CHASSIS.
  - Only addressed 'Independence'.

Integration Methodology (1/2)

Security RA / Safety RA	Variation of Conventional Safety Risk Assessment Method	Conventional Security Risk Assessment Method	Others
Conventional Safety Risk Assessment Method	I. SAHARA II. FMVEA	I. FACT Graph II. Extended CFT III. EFT	
Variation of Conventional Security Risk Assessment Method		I. Unified Security and Safety Risk Assessment	
Others			I. CHASSIS

Integration Methodology (2/2)

- These methods did not take into account **real-time system information** to perform **dynamic risk assessment**.

- The list of combinations of safety, and security risk assessment methods provided in this study would act as a base to investigate the other **combinations that are more effective**.

Stages of Risk Assessment Addressed

Integrated Safety and Security Risk Assessment Method	Risk Identification	Risk Analysis	Risk Evaluation
SAHARA	✓	✓	×
CHASSIS	✓	×	×
FACT Graph	✓	×	×
FMVEA	✓	✓	×
Unified Security and Safety Risk Assessment	✓	✓	✓
Extended CFT	✓	✓	×
EFT	✓	✓	×

- How 'Unified Security and Safety Risk Assessment' method addressed Risk Evaluation?
- **Research Gaps:** How to address safety and security interactions especially 'Mutual Reinforcement', and 'Antagonism' in Risk Treatment?; How to use the results of integrated safety and security risk assessment in risk treatment?

Key Takeaways

- Identified 7 Integrated Safety and Security Risk Assessment Methods.
- Sequential (Bias) vs. Non-sequential (Independence).
- 4 combinations were used to develop these methods.
- 3 Existing Domains of Application: Transportation, Power and Utilities, and Chemical.

- Investigate the other combinations that are more effective.
- Evaluate the applicability of these methods in the other domains.
- How to use the results of integrated safety and security risk assessment in risk treatment?
- How to address safety and security interactions in Risk Treatment?

Saba Chockalingam

S.Chockalingam@tudelft.nl

Project - Secure Our Safety: Building Cyber Security for Flood Management (SOS4Flood)