This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

HyRiM

A Hybrid Risk Management Process for Interconnected Infrastructures

Stefan Schauer

Workshop on Novel Approaches in Risk and Security Management for Critical Infrastructures

Vienna, 19.09.2017

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Contents

- Motivation
- Hybrid Risk Management and the ISO 31000
- HyRiM Process
- Conclusion

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Contents

Motivation

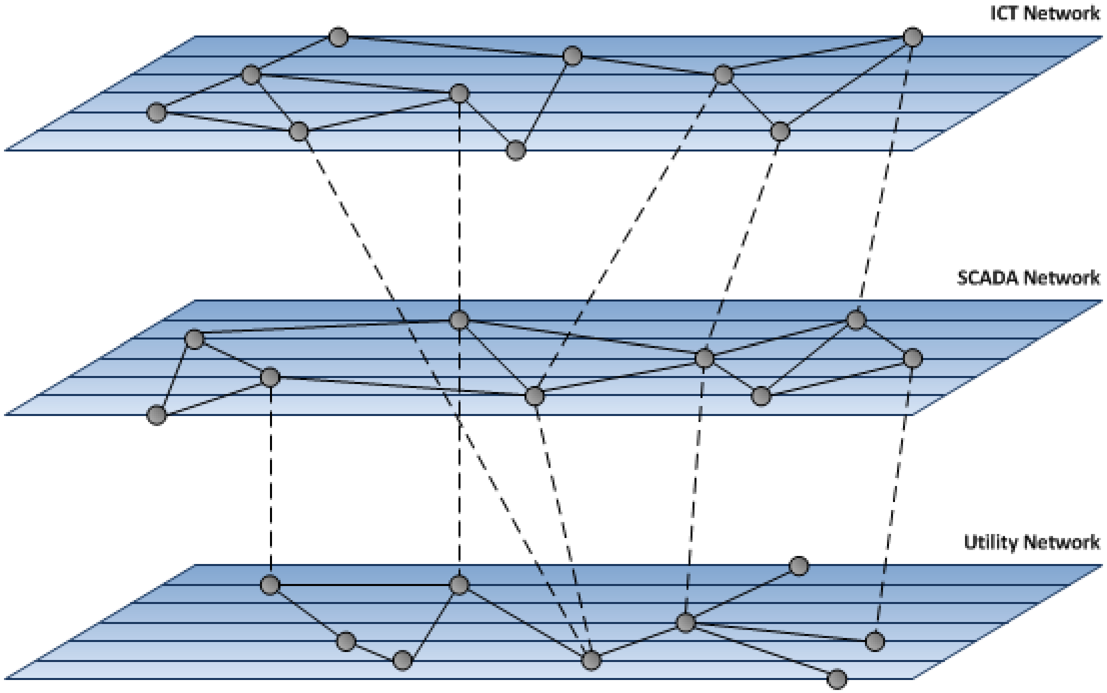
- Risk assessment and risk management is a core duty for utility providers
  - Utility providers operate critical infrastructures
  - Responsible for the supply of large number of people with different goods
  - Incidents within/affecting utility providers might have huge economic and societal impacts

- Numerous risk assessment and risk management tools already exist
  - Based on well-established standards and guidelines (e.g., ISO 31000)
  - Often focusing on a specific field (e.g., IT Security – ISO 27005, Supply Chain Management – ISO 28000, Port Security – ISO 20858)
  - Often designed for businesses and not the special requirements of utility providers or critical infrastructures
  - Mostly a matter of best practices

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Motivation

- Networks operated by utility providers are heavily connected among each other
  - Utility network (e.g., power lines, water pipes, oil pipelines, etc.)
  - Control networks (e.g., SCADA networks, smart grids, etc.)
  - ICT networks (e.g., office networks, communication networks, intranet, etc.)



Contents

- Motivation
- Hybrid Risk Management and the ISO 31000
- HyRiM Risk Management Process
- Conclusion

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

ISO 31000

- World-wide leading standard for risk management is the ISO 31000
  - Follows a very generic approach on risk management
  - Ubiquitously applicable on every kind of organisation
  - More specific standards are building on and extending the ISO 31000 (e.g., ISO 27005, ISO 28000, ISO 20858, etc.)

- ISO 31000 describes a two-tier structure
  - Operative risk management process provides a generic description of the different steps towards risk management
  - Organizational risk management framework required to implement the risk management process within a company

- In HyRiM we extend the ISO 31000 towards a more mathematically-based approach, including concepts and algorithms developed in the project

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Hybrid Risk Management

- Requirements of utility providers have changed
  - Number of cyber-physical systems increases (e.g., SCADA networks, Industrial Control Systems)
  - Threats evolve more rapidly and become more complex (e.g., Advanced Persistent Threats – APT)
  - Intentional threats became more popular in recent years (e.g., terrorism, cyber-terrorism/hacktivists, espionage, etc.)
- Threats affecting one part of a utility provider can propagate through the network and affect other, distant parts, too
  - Malware infection on the ICT network might cause the failure of a SCADA system and thus affect the utility network itself
  - Security issue of a SCADA system might give access to business data handled in the ICT network
- Additionally, utility providers are interconnected and interacting with each other

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Hybrid Risk Management

- Novel approaches towards security and risk management have to be identified to address these issues
  - Solutions for each network level exist and are applied separately
  - "Hybrid" risk management methodologies are required, providing a holistic overview (i.e., looking at several networks simultaneously)
  - Interconnections and the related cascading effects need to be considered

- Sole focus on technical threats and technical solutions is no longer adequate
  - Social engineering is a major aspect in many attack strategies
  - Organizational factors are essential for every security measure or security strategy performed in an organization

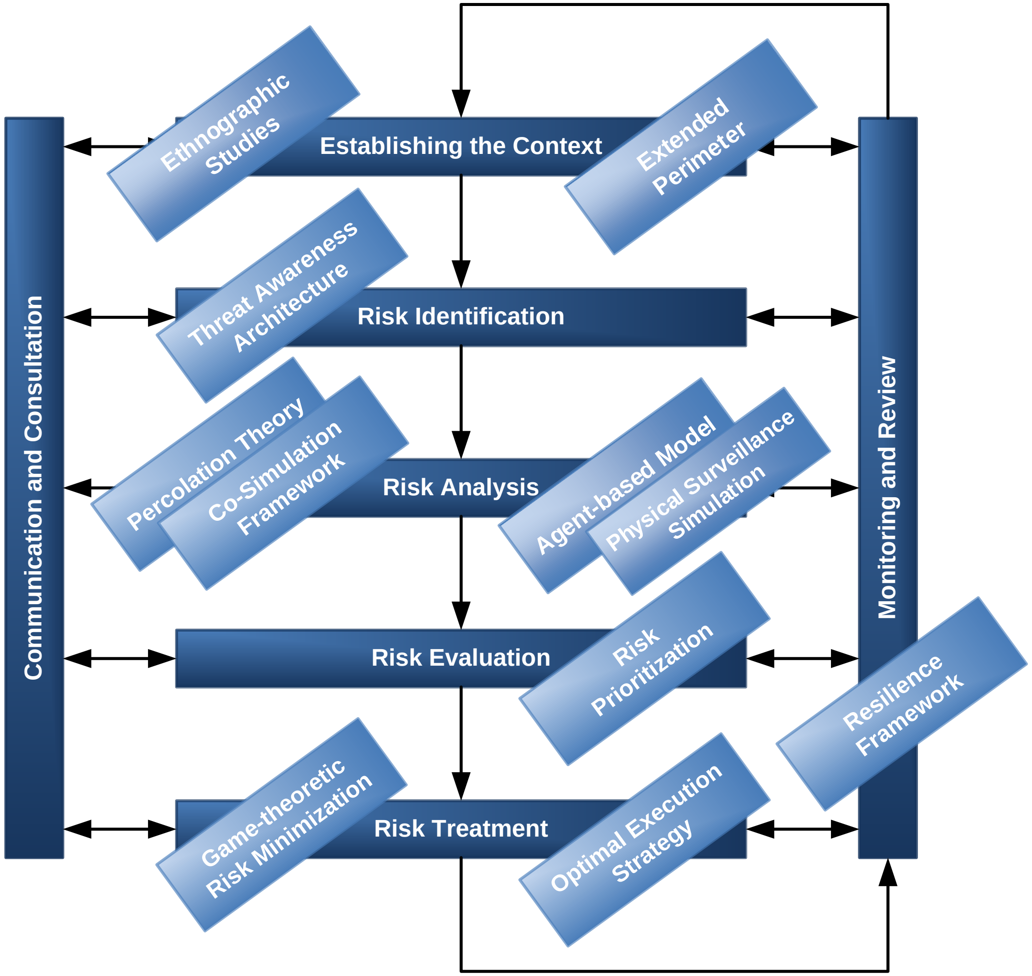
- Security and risk management methodologies explicitly have to take societal factors into account

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

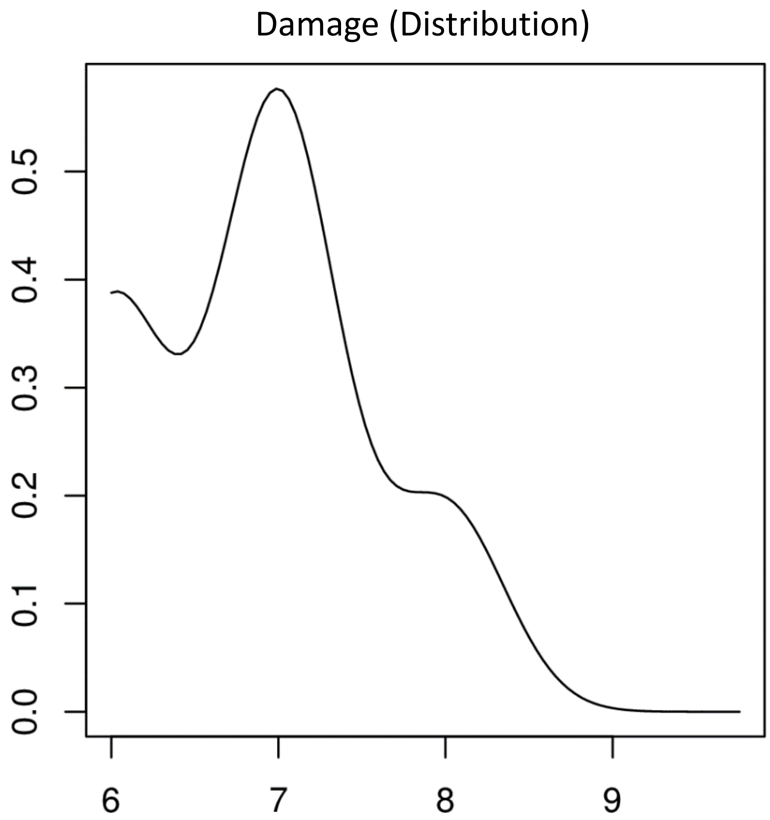
Contents

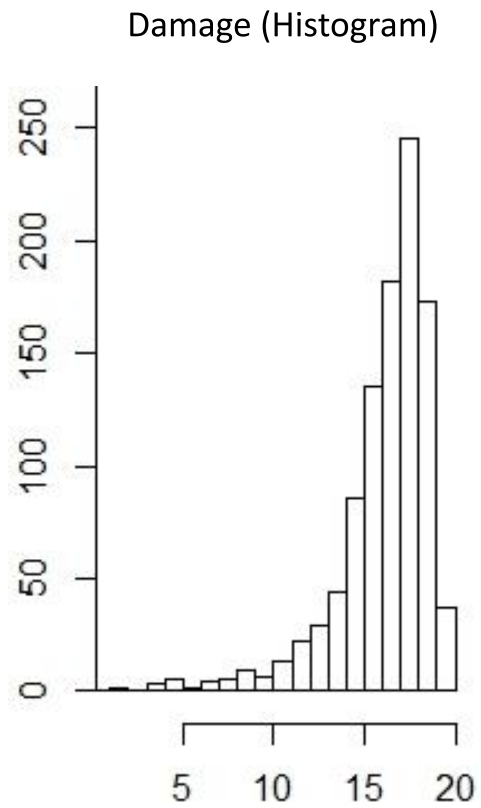
- Motivation
- Hybrid Risk Management and the ISO 31000
- HyRiM Process
- Conclusion

HyRiM Process



Impact and Likelihood



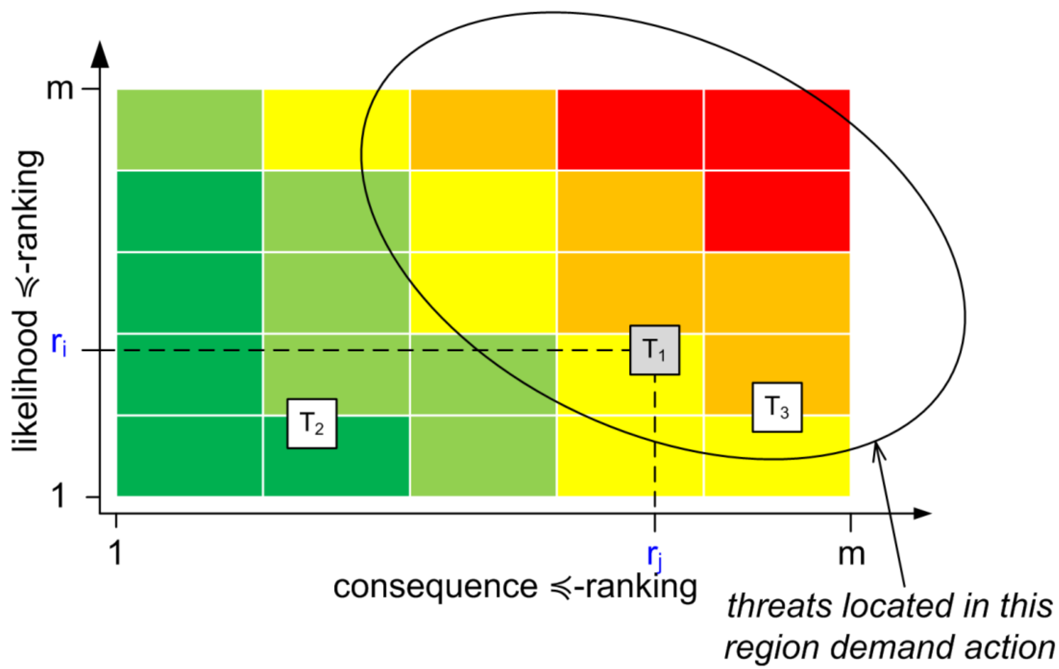


This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

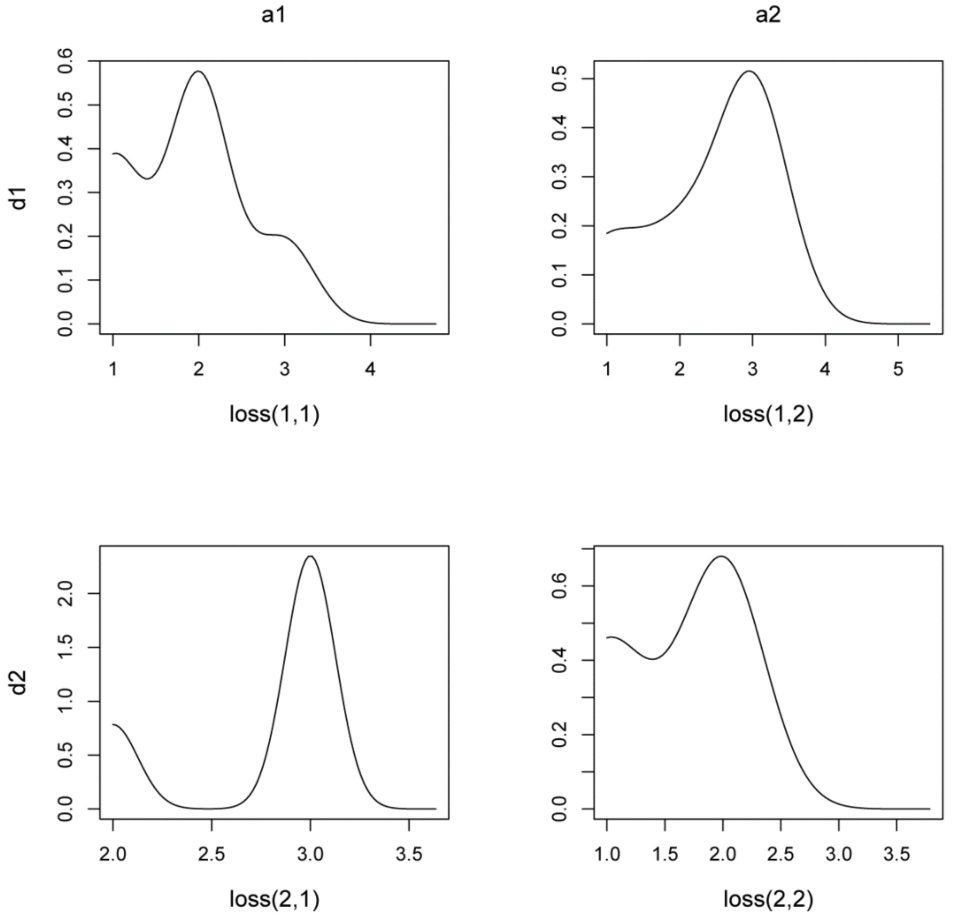
Risk Ranking & Risk Matrix

ranking (w.r.t. $\preccurlyeq$-ascending order)

	1	2	…	r_i	…	r_j	…	m
Consequence:			T_2			T_1	T_3	
Likelihood:			T_2	T_1	T_3			



Payoff Matrix



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Contents

- Motivation
- Hybrid Risk Management and the ISO 31000
- HyRiM Process
- Conclusion

Conclusion

- Utility operators live in a highly uncertain environment
  - More complex and rapidly changing threat landscape
  - Consequences of events are not assessed easily (e.g., cascading effects)

- Standard risk assessment and risk management process are often not enough
- Novel risk management process developed in the HyRiM project
  - Extension of the standard ISO 31000 process
  - Strongly relying on qualitative data/information
  - Application of mathematical tools and structured approaches
  - Implementation of game theory to identify optimal mitigation actions

- Goal is to support the operational and management level to make better decisions

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

HyRiM

Identifying and Managing Risks in Interconnected Utility Networks

Stefan Schauer

stefan.schauer@ait.ac.at
AIT Austrian Institute of Technology
Lakeside B10a
9020 Klagenfurt
Austria

Workshop on Novel Approaches in Risk and Security Management for Critical Infrastructures
Vienna, 19.09.2017

Contents

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Process Overview

Establishing the Context	External Context	Internal Context	Context of the RM Process	Criteria of the RM Process
Risk Identification	Asset Identification	Threat Identification	Vulnerability Identification	
Risk Analysis	Threat Scenario Definition	Consequence Analysis	Likelihood Analysis	
Risk Evaluation	Risk Selection	Risk Ranking	Risk Level Determination	
Risk Treatment	Attack Strategies	Defense Strategies	Mitigation Actions	Implementation Strategy

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Establishing the Context

Establishing the Context → External Context → Internal Context → Context of the RM Process → Criteria of the RM Process

- Identify all interrelations with internal and external stakeholders
  - Internal technical, organizational and social aspects
    (e.g., communication channels, dependencies between different technical and social networks)
  - External interrelations and interdependencies
    (e.g., external organizations as resource providers or regulatory bodies)

- Identify the relevant framework for the risk management process
  - Parts of the organization which are covered in the risk management process
    (e.g., organizational units, depth of the risk assessment process)
  - Criteria to evaluate the significance of a specific risk based on organization’s resources, objectives and goals or general characteristics
    (e.g., definition how the likelihood or the impact of an event is characterized)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Risk Identification

HyRiM

Risk Identification → **Asset Identification** → **Threat Identification** → **Vulnerability Identification**

- Identify the relevant assets of the organization's infrastructure
  - Based on the internal context (cf. "Context Establishment")
  - Focus on the interconnections between assets

- Identify all potential threats and respective vulnerabilities affecting the organization's infrastructure
  - Obtain a structured view on all potential threats and vulnerabilities
  - Application of a specific Threat Awareness Architecture

- Information can/should be collected from different sources
  - External (e.g., existing threat catalogues or online threat databases)
  - Internal (e.g., expert knowledge or information on past incidents)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Risk Analysis

HyRiM

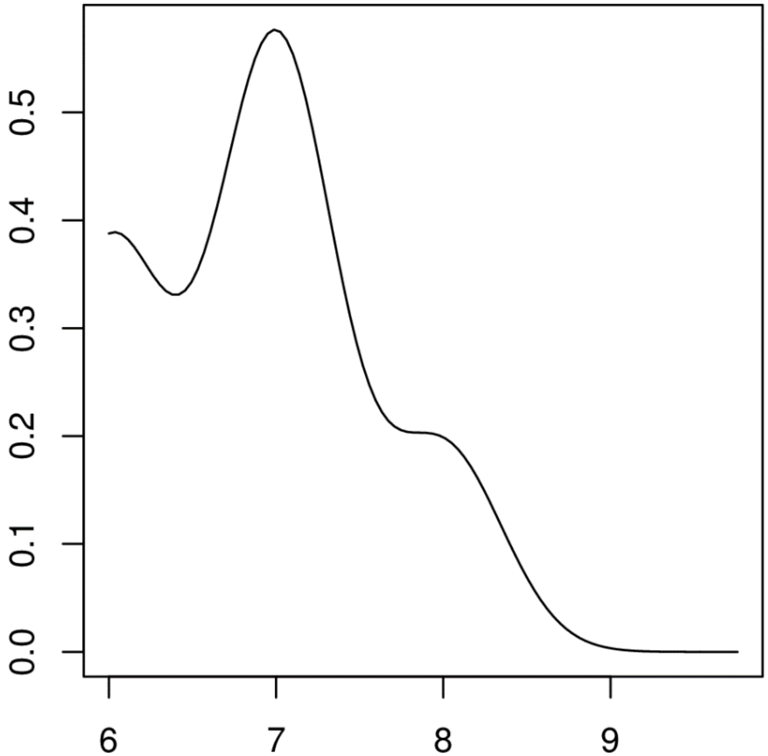
Risk Analysis → **Threat Scenario Definition** → **Consequence Analysis** → **Likelihood Analysis**

- Identify a fine-grained list of potential threat scenarios
- Determine the potential consequences for the manifestation of all threat scenarios
  - Quantitative (e.g., using percolation theory or a co-simulation approach)
  - Qualitative (e.g., by experts from within the organization or external advisors)
- Determine the potential likelihood for the manifestation of all threat scenarios
  - In general fully qualitative estimation supported using information from external sources (e.g., reports containing statistical information on the likelihood of specific events)
- All information is gathered in histograms or distribution functions
  - Capturing of uncertainty and preventing loss of information

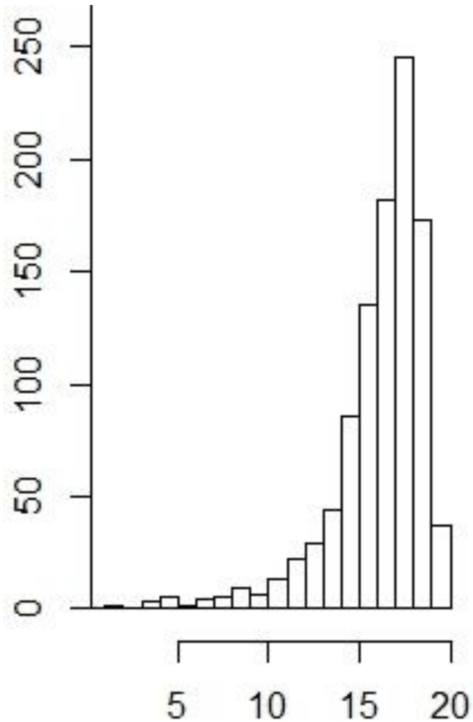
Risk Analysis

Risk Analysis → **Threat Scenario Definition** → **Consequence Analysis** → **Likelihood Analysis**

Damage (Distribution)



Damage (Histogram)



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Risk Evaluation

Risk Evaluation → **Risk Selection** → **Risk Ranking** → **Risk Level Determination**

- Select a list of most relevant risks (based on threat scenarios)
- Determine a ranking of the identified risks
  - Ordering according to their respective consequences and likelihood
  - Comparing histograms is non-trivial (novel approach has bee identified)

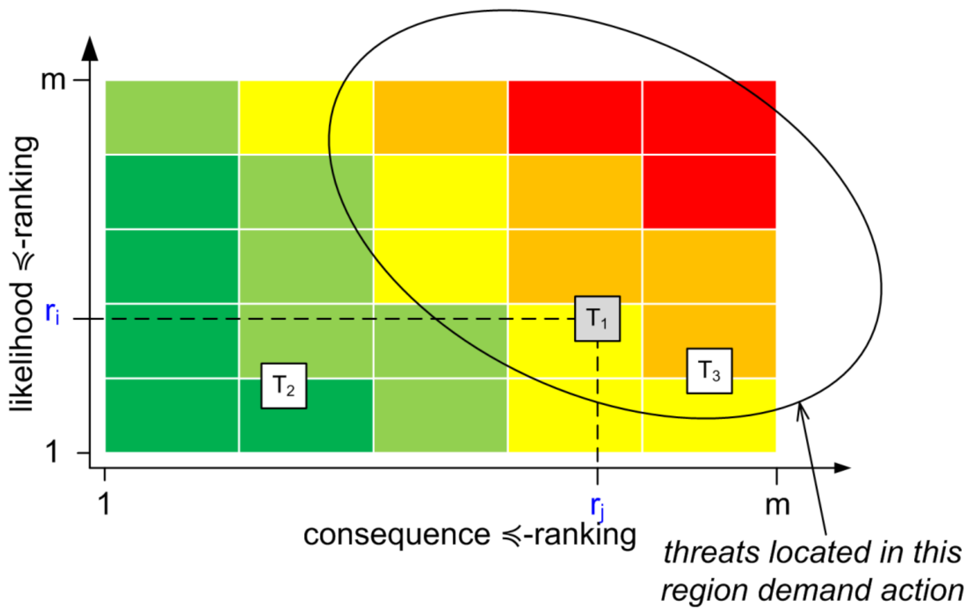
- Create a graphical representation and a priority list of the identified risks
  - Each risk is placed within a risk matrix based on its consequences and likelihood
  - Risks having the most severe consequences together with the highest likelihood are located at the upper right corner of the matrix

Risk Evaluation

Risk Evaluation → Risk Selection → Risk Ranking → Risk Level Determination

ranking (w.r.t. ≼-ascending order)

	1	2	…	r_i	…	r_j	…	m
Consequence:			T_2			T_1	T_3	
Likelihood:			T_2	T_1	T_3			



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Risk Treatment

Risk Treatment → **Attack Strategies** → **Defense Strategies** → **Mitigation Actions** → **Implementation Strategy**

- Identify the risks that need to be mitigated
  - Usually these are the highest-ranked risks
  - Threat scenarios describe potential attack strategies for these risks

- Identify possible mitigation actions (defense strategies) to counter the respective attack strategies
  - Reducing the consequences of the specific risk (e.g., by lowering the number of affected assets)
  - Reducing the likelihood of the specific risk (e.g., by making it harder to exploit specific vulnerabilities)
  - Letting a risk vanish completely (e.g., by closing specific vulnerabilities)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Risk Treatment

HyRiM

Risk Treatment → **Attack Strategies** → **Defense Strategies** → **Mitigation Actions** → **Implementation Strategy**

- Determine the effect of a specific defense strategy on a single attack strategy
  - Rerunning the consequence analysis for the organization's asset structure (assume that the specific defense strategy has been implemented)
  - Evaluate all possible combinations of attack and defense strategies
  - Results are fed into the game-theoretic framework

- Game-theoretic framework provides an optimal security strategy
  - In general a mixture of the single mitigation actions
  - Describes the different frequencies at which these mitigation actions have to be performed
  - Organizational structure (job scheduling) is required to support the correct implementation of the mitigation actions