An Information Flow Modelling Approach for Critical Infrastructure Simulation

Denise Gall, Christian Luidold, Gregor Langner,
Thomas Schaberreiter, Gerald Quirchmayr

`Contact email: denise.gall@univie.ac.at`

Research Group Multimedia Information Systems,
Faculty of Computer Science, University of Vienna

SECURWARE 2020 November 21, 2020 to November 25, 2020
Valencia, Spain

About the Lead Author

Denise Gall is currently working in the Research Group Multimedia Information Systems at the Faculty of Computer Science at the University of Vienna, where her contributions focus on the development of an information flow model within the ODYSSEUS project. She also works on a Master Thesis related to the project.

Acknowledgment

This work was partially funded by the Austrian FFG research program KIRAS in course of the project ODYSSEUS ("Simulation und Analyse kritischer Netzwerk-Infrastrukturen in Städten") under Grant No. 873539.

Overview

- Introduction
- Modelling Approach
- Case Study
- Discussion of results
- Conclusion

Introduction

- Critical infrastructures need to be resilient against a multitude of threats to maintain public interests.
- Cascading effects due to failures in other critical infrastructures are often unknown.
- Communication and collaboration among dependent critical infrastructures support identifying dependencies between the infrastructures.
- Identified dependencies enables providers to prepare themselves from cascading failures.

This approach is intended to support critical infrastructure providers and first responders through a customized information flow model.

Introduction

Goals of the modelling approach:

- Modelling cascading effects in critical infrastructures in a structured form
- Establishing a basis for subsequent simulation
- Supporting discussion with and between critical infrastructure providers and first responders

The modelling approach was applied in the ongoing ODYSSEUS project.

Modelling Approach

The modelling approach comprises:

- Analyzing modelling prerequisites including textually defined threat scenarios.
- Establishing activity diagrams based on the previous defined threat scenarios.
- Establishing object diagrams including objects, parameters and information flows.
- Further refining diagrams in multiple workshop settings.

Critical infrastructures are multi-stakeholder domains, which this modelling approach is designed for.

Modelling Approach 1/4

Modelling prerequisites

- The basis for later designed diagrams are textually composed threat scenarios.
- Various information sources on threats were collected and analyzed to create realistic scenarios for critical infrastructures. The focus was on threats and possible attacks.
- Based on the information, first drafts of threat scenarios were developed.
- The main stakeholders are:
  - Critical infrastructure providers
  - First responders
  - Critical infrastructure security experts
  - Simulation experts
- The model drafts were validated and refined in a series of workshops with experts from critical infrastructures.

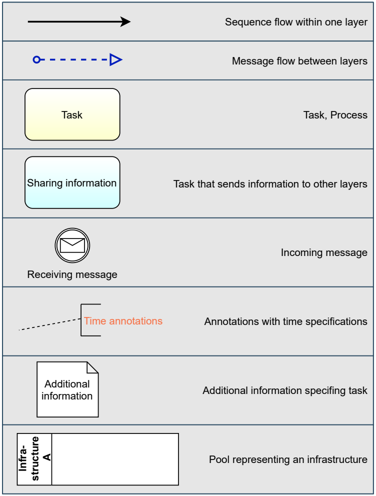
Modelling Approach 2/4

Modelling scenario behavior in activity diagrams

- The designed activity diagram represents a process view of events and impacts occurring in the defined threat scenarios.
- Advantages:
  - Structured form of sequences including information flows
  - Basis for subsequent simulations
  - Facilitate evaluation by end-users
- Transformation of textual descriptions into activity diagrams:
  - Extract all affected infrastructures from the textual description
  - Identify activities that can influence the state of an infrastructure
  - Identify information flows between infrastructures, especially between stakeholders
- The visual representation is based on BPMN, as it is a common accepted notation.

Modelling Approach 2/4

Modelling scenario behavior in activity diagrams



→	Sequence flow within one layer
○- - - - - -▷	Message flow between layers
Task	Task, Process
Sharing information	Task that sends information to other layers
Receiving message	Incoming message
Time annotations	Annotations with time specifications
Additional information	Additional information specifing task
Infra-structure A	Pool representing an infrastructure

Figure: Notation used in Activity Diagrams.

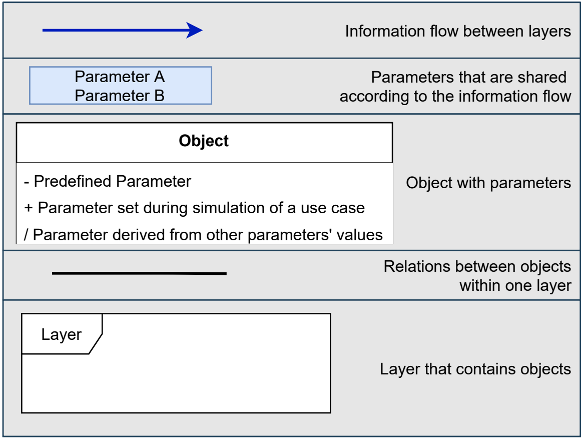
Modelling Approach 3/4

Modelling scenario parameters in object diagrams

- Object diagrams visualize objects and parameters needed for simulating behaviors and information flows.
- Close cooperation with simulation experts is required for this step, to cover their requirements and limitations.
- Identification steps for developing an object diagram:
  - Identify objects relevant for representing the threat scenario
  - Identify parameters for each object
  - Identify information flows between infrastructures
  - Identify parameters shared with information flows
- UML class diagrams were chosen as representation, because it is an established standard.

Modelling Approach 3/4

Modelling scenario parameters in object diagrams



Information flow between layers

Parameter A
Parameter B

Parameters that are shared according to the information flow

Object

- Predefined Parameter

+ Parameter set during simulation of a use case

/ Parameter derived from other parameters' values

Object with parameters

Relations between objects within one layer

Layer

Layer that contains objects

Figure: Notation used in Object Diagrams.

Modelling Approach 4/4

Iterative refinement of modelling results

- A series of consecutive workshops needs to be held to gather feedback from domain experts.
- Workshops help to identify inaccuracies and wrong representations of events and information flows.
- The major goal of the workshops is to collect the following additional information:
  - Information regarding every-day processes
  - Threats which can lead to failures in infrastructures
  - How would such failures impact other infrastructures
  - Information on communication and collaboration with and between infrastructures and outside stakeholders
- The newly obtained information is used to update diagrams and textual descriptions.

Case Study

- A Case Study was conducted in the context of the ODYSSEUS project.
- Project goal: Identify and simulate cascading effects between critical infrastructures in an urban area to improve procedures and reactions in case of a threat scenario materializing.
- Main end-users:
  - Critical infrastructure providers
  - First responders
  - Experts in response capacity planning
- Multiple workshops with the stakeholders are a core component in the project:
  - During the initial workshop use cases were identified based on their relevance.
  - Follow up workshops with experts of each area of critical infrastructures were performed individually.

Case Study

Power failure

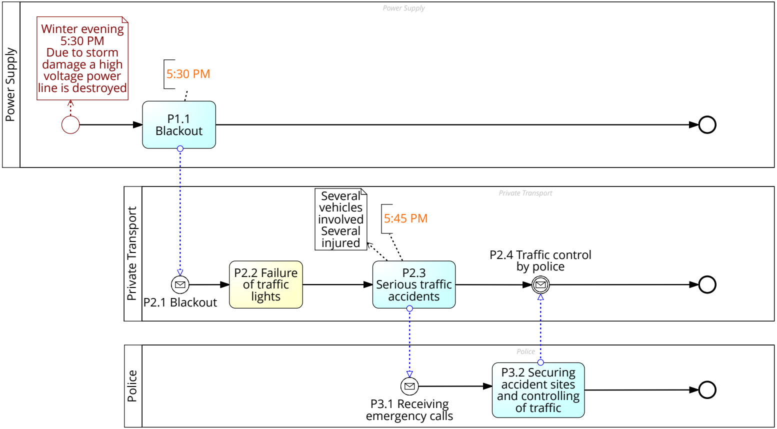
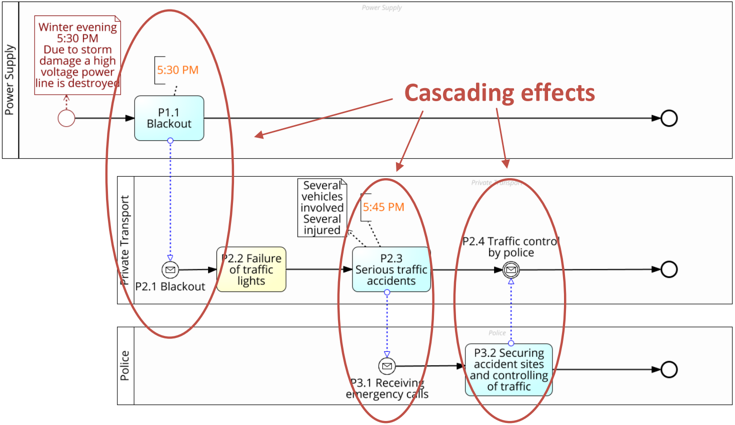

Power Supply
Power Supply
Winter evening 5:30 PM Due to storm damage a high voltage power line is destroyed
5:30 PM
P1.1 Blackout
Private Transport
Private Transport
Several vehicles involved Several injured
5:45 PM
P2.1 Blackout
P2.2 Failure of traffic lights
P2.3 Serious traffic accidents
P2.4 Traffic control by police
Police
Police
P3.1 Receiving emergency calls
P3.2 Securing accident sites and controlling of traffic

Figure: ODYSSEUS Activity Diagram Power Failure - Snapshot.

Case Study

Power failure



Power Supply
Power Supply
Winter evening 5:30 PM Due to storm damage a high voltage power line is destroyed
5:30 PM
P1.1 Blackout
Cascading effects
Private Transport
Private Transport
P2.1 Blackout
P2.2 Failure of traffic lights
Several vehicles involved Several injured
5:45 PM
P2.3 Serious traffic accidents
P2.4 Traffic control by police
Police
Police
P3.1 Receiving emergency calls
P3.2 Securing accident sites and controlling of traffic

Figure: ODYSSEUS Activity Diagram Power Failure - Snapshot.

Case Study

Power failure

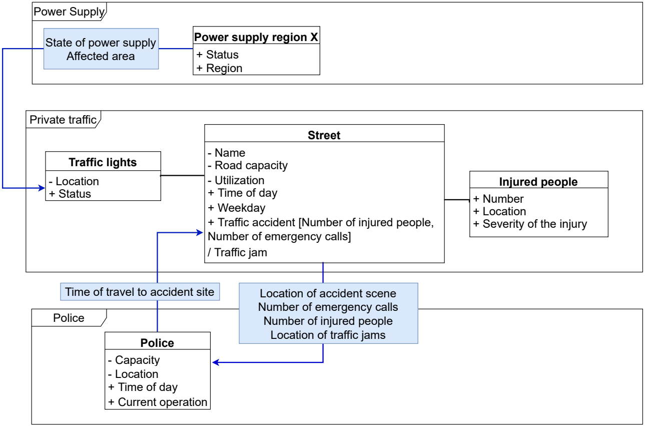


Figure: ODYSSEUS Object Diagram Power Failure - Snapshot.

Case Study
Power failure

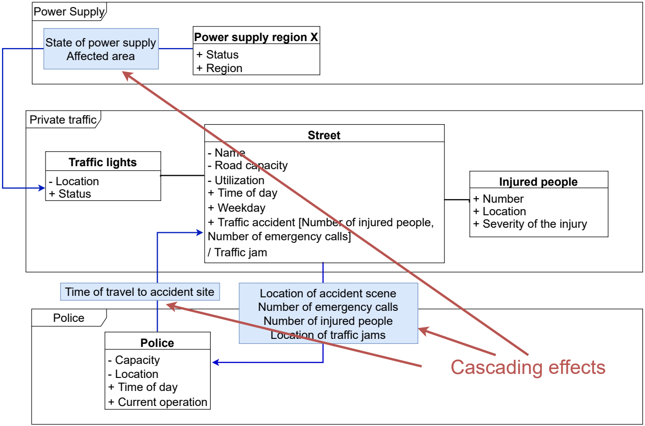
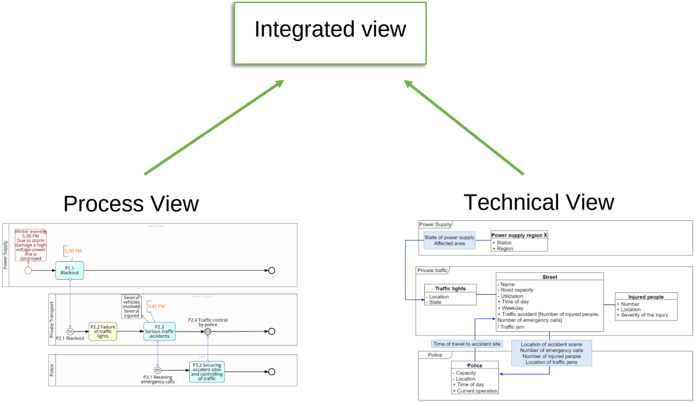


Figure: ODYSSEUS Object Diagram Power Failure - Snapshot.

Viewpoint integration

towards supporting situational awareness



Integrated view

Process View

Technical View

Power Supply
Winter evening 5:30 PM Due to storm damage a high voltage power line is destroyed
5:30 PM
P1.1 Blackout
Private Transport
P2.1 Blackout
P2.2 Failure of traffic lights
Several vehicles involved Several injured
5:45 PM
P2.3 Serious traffic accidents
P2.4 Traffic control by police
Police
P3.1 Receving emergency calls
P3.2 Securing accident sites and controlling of traffic
Power Supply
State of power supply Affected area
Power supply region X
+ Status
+ Region
Private traffic
Traffic lights
- Location
- State
Street
- Name
- Road capacity
- Utilization
+ Time of day
+ Weekday
+ Traffic accident [Number of injured people, Number of emergency calls]
/ Traffic jam
Injured people
+ Number
+ Location
+ Severity of the injury
Time of travel to accident site
Location of accident scene Number of emergency calls Number of injured people Location of traffic jams
Police
Police
- Capacity
- Location
+ Time of day
+ Current operation

Figure: Viewpoint integration

Discussion of results

- *Modelling cascading effects in critical infrastructures in a structured form*
  - Textual threat scenarios can be transformed into a structured visual form.
  - The model is helpful for outlining the potential cause and effect relationships of cascading failures.
  - The model supports the validation with experts during workshops.
- *Establishing a basis for subsequent simulation*
  - The model has shown to be a valid basis for subsequent simulation.
  - The model provides a process view of the threat scenarios and a technical view.
- *Supporting discussion with and between critical infrastructure providers and first responders*
  - The activity diagram supports stakeholders in better understanding the activities observed during a threat scenario.
  - Stakeholders have shown a high interest in understanding procedures in other critical infrastructures.

Summary

- The modelling approach demonstrates how textual threat scenarios can be transformed into activity diagrams and object diagrams.
- The diagrams serve as a basis for subsequent simulations by providing a process view and a technical view.
- The modelling approach offers a method to model cascading effects in critical infrastructures in a structured form, which supports evaluation in end-user workshops.
- The approach was evaluated in the context of the ODYSSEUS project.
- Future work includes obtaining values for objects' parameters and further evaluation with end-users within the ODYSSEUS project.

Major Conclusion

Information flow models have demonstrated their value for improving situational awareness and for supporting collaborative scenario analysis during the project.

Thank you for your attention!

An Information Flow Modelling Approach for Critical Infrastructure Simulation

Contact email: denise.gall@univie.ac.at

This work was partially funded by the Austrian FFG research program KIRAS in course of the project ODYSSEUS (”Simulation und Analyse kritischer Netzwerk-Infrastrukturen in Städten”) under Grant No. 873539.