# ODYSSEUS

Simulation und Analyse kritischer Netzwerkinfrastrukturen in Städten

| | | | |
|---|---|---|---|
| **Programm / Ausschreibung** | KIRAS, Kooperative F&E-Projekte, KIRAS Kooperative F&E-Projekte 2018 | **Status** | abgeschlossen |
| **Projektstart** | 01.10.2019 | **Projektende** | 31.12.2021 |
| **Zeitraum** | 2019 - 2021 | **Projektlaufzeit** | 27 Monate |
| **Keywords** | Risikomodellierung, Risikomodell, Simulation | | |

## Projektbeschreibung

In Städten und deren Agglomeration ist eine Vielzahl von kritischen Infrastrukturen (KI) angesiedelt, die wesentliche Dienste in einem geographisch engen Raum bereitstellen und dadurch zueinander in physischer und logischer Abhängigkeit stehen. Daraus ergibt sich ein sensibles Geflecht von Organisationen und Verbindungen, in dem Zwischenfälle innerhalb einer einzelnen Infrastruktur Auswirkungen auf das gesamte System haben können. Insbesondere kritische Infrastrukturen aus den Bereichen Versorgung (Strom, Gas, Wasser, etc.), Kommunikation (IKT), Güterverteilung (Lebensmittel, Treibstoff, etc.) und Transport (Straße, Schiene, etc.) betreiben weitläufige Netzwerke, welche besondere Anforderungen im Hinblick auf Sicherheitsmaßnahmen aufweisen. Somit stellt speziell vor dem Hintergrund des Netz- und Informationssystemsicherheitsgesetzes (NISG) eine detaillierte Risikoanalyse mit starkem Fokus auf die Interaktion dieser Netzwerke sowie auf potentielle Kaskadeneffekte für die Bevölkerung einen zentralen Aspekt für den Schutz dieser kritischen Versorgungsinfrastrukturen dar. Aber auch die immer stärker in den Fokus rückenden sogenannten „Soft Targets“, also für Terroranschläge attraktive Ziele im Public Space, hätten im Fall eines Anschlages Auswirkungen auf die oben genannten Netzwerke.

Ziel des Projekts ODYSSEUS ist es, ein mehrschichtiges Risikomodell am Beispiel der Stadt Wien zu erstellen, welches die Netzwerke der zentralen Versorgungsinfrastrukturen (Strom, Gas, Wasser, Lebensmittel und Telekommunikation inkl. IKT) sowie die Transportnetzwerke (Straße und Bahn) bis zu einem bestimmten Abstraktionslevel hin beschreibt. Hierbei sollte dieser Abstraktionslevel so gering wie möglich gehalten werden, um eine möglichst reale Abbildung zu erreichen (abhängig von der verfügbaren Datenquantität und -qualität). Auf Basis dieses Modells werden potentielle Bedrohungen (sowohl Naturkatastrophen als auch durch Menschen verursachte Zwischenfälle) simuliert. Im Gegensatz zu bestehenden Lösungen aus der Literatur und der Praxis wird hierbei in ODYSSEUS auf die dynamischen Zusammenhänge zwischen den Netzwerken fokussiert und es werden mathematische Modelle aus der Stochastik (z.B. Markov-Ketten, probabilistische Automaten) für eine realitätsnahe Darstellung entwickelt.

Zentraler Output von ODYSSEUS ist ein Framework, das eine detaillierte Bewertung sowohl der Auswirkungen von Bedrohungen sowohl auf einzelne kritische Infrastrukturen, als auch der möglichen Kaskadeneffekten innerhalb des

gesamten Netzwerks der kritischen Versorgungsinfrastrukturen unter Berücksichtigung der städtischen Bevölkerung ermöglicht. Die Simulationen beschreiben, welche potentiellen Kompensations- und Verdrängungs-mechanismen innerhalb des mehrschichtigen Netzwerks der Versorgungsinfrastrukturen bzw. auf Public Spaces im Falle eines Ereignisses (intentional, technisch oder Naturgefahr) zu erwarten sind. Aus dieser Erkenntnis können zielgerichtete präventive Sicherheitsmaßnahmen abgeleitet, dargestellt und evaluiert werden, deren Umsetzung die Auswirkungen im Ereignisfall minimieren.

## Abstract

Cities and their agglomerations are home to a large number of critical infrastructures (CI) that provide essential services in a geographically narrow space and are thus physically and logically dependent on one another. This results in a sensitive network of organizations and connections in which incidents within an infrastructure can have an impact on the entire system. In particular, critical infrastructures in the context of utilities (electricity, gas, water, etc.), communication (ICT), distribution (food, fuel, etc.) and transport (road, rail, etc.) operate extensive networks which have special requirements with regard to security measures. Thus, a detailed risk analysis with a strong focus on the interaction of these networks and on potential cascading effects for the population represents a central aspect for the protection of these critical supply infrastructures, especially when considering the Network and Information Security (NIS) Law. Further, also the so-called "soft targets", i.e. attractive targets in public spaces for terrorist attacks, would have an impact on the above mentioned networks in case of an attack.

The goal of the ODYSSEUS project is to create a multi-layered risk model, based on the example of the City of Vienna, which describes the networks of the central supply infrastructures (electricity, gas, water, food and telecommunications, including ICT) as well as the transport networks (road and rail) up to a certain level of abstraction. This level should be kept as low as possible in order to achieve as real a representation as possible (depending on the quantity and quality of data available). Based on this model, potential threats (both natural disasters and man-made incidents) are simulated. In contrast to existing solutions from literature and practice, ODYSSEUS focuses on the dynamic relationships between networks and develops mathematical models from stochastics (e.g. Markov chains, probabilistic automata) for a realistic representation.

The central output of ODYSSEUS is a framework that enables a detailed assessment of the effects of threats both on individual critical infrastructures and on possible cascading effects within the entire network of critical supply infrastructures, taking into account the urban population. The simulations describe which potential compensation and displacement mechanisms can be expected within the multi-layered network of supply infrastructures or on public spaces in the event of an incident (intentional, technical or natural hazard). From this knowledge, targeted preventive safety measures can be derived, presented and evaluated in order to minimize the effects in the event of an incident when implemented.

## Projektkoordinator

- AIT Austrian Institute of Technology GmbH

## Projektpartner

- ACP CUBIDO Digital Solutions GmbH
- Institut für empirische Sozialforschung (IFES) Gesellschaft mbH
- Bundesministerium für Landesverteidigung

- Bundesministerium für Inneres
- Universität Klagenfurt
- Bundeshauptstadt Wien
- Universität Wien