Cross-Domain Risk Analysis to Strengthen City Resilience: the ODYSSEUS Approach

Stefan Schauer *
AIT Austrian Institute of Technology

Stefan Rass
Alpen-Adria Universität Klagenfurt

Sandra König
AIT Austrian Institute of Technology

Klaus Steinnocher
AIT Austrian Institute of Technology

Thomas Schaberreiter
University of Vienna

Gerald Quirchmayr
University of Vienna

ABSTRACT

In this article, we want to present the concept for a risk management approach to assess the condition of critical infrastructure networks within metropolitan areas, their interdependencies among each other and the potential cascading effects. In contrast to existing solutions, this concept aims at providing a holistic view on the variety of interconnected networks within a city and the complex dependencies among them. Therefore, stochastic models and simulations are integrated into risk management to improve the assessment of cascading effects and support decision makers in crisis situations. This holistic view will allow risk managers at the city administration as well as emergency organizations to understand the full consequences of an incident and plan mitigation actions accordingly. Additionally, the approach will help to further strengthen the resilience of the entire city as well as the individual critical infrastructures in crisis situations.

Keywords

Risk Management, Cross-Domain Networks, Interdependencies, Stochastic Model, City Resilience, Critical Infrastructures.

INTRODUCTION

Nowadays, metropolitan areas are home to a large number of critical infrastructures (CIs) from different domains, which are required to maintain essential services and the social life in these cities. Among them, there are the general utilities like electricity, gas or water, information and communication technologies (ICT), distribution networks for food or as well as road or railway transportation networks. These networks typically span over the entire city area and but are bounded within a geographically narrow space. This leads to manifold physical and logical dependencies among those infrastructure networks (Rinaldi et al. 2001), turning them into a *complex and highly sensitive multi-domain CI network*. Hence, any incident happening at one part of those networks (e.g., an impairment or even the total failure of a system due to external influences) can have far-reaching consequences, i.e., cascading effects, on other domains and thus on the economic and social well-being of the entire city. Consequently, a detailed risk analysis with a strong focus on the interaction of these networks and potential cascading effects for the population, as part of the Network and Information Security (NIS) Directive in Europe European Comission 2016, is a central aspect for the protection and further the resilience of these CIs.

To obtain an overview on the current state and the behavior of their networks, CI operators use simulation tools, which are based on mathematical models and live monitoring data from their networks. However, these tools usually do not provide information on networks from other domains, i.e., *do not take the interdependencies among the*

*corresponding author

networks into account. Thus, despite collecting information from simulations of the individual networks, a detailed understanding of the dynamics in the overall system of all networks within a city is missing. In other words, even though the risk behavior and resilience of a subsystem may be well understood, such a local view is insufficient for an assessment of cascading effects, unless there is also a global view that reveals potential cross-domain effects.

In this article, we conceptually describe a risk management approach for the CI networks located within a metropolitan area to tackle the challenge of systematically gaining a global view on a network of interdependent CIs. This framework is developed as part of the currently running project ODYSSEUS [1] with the goal to provide a *support tool for CI operators as well as city administration and emergency organizations* in (or in preparation of) crisis situations. At the heart of the framework are the *multi-domain CI networks and their interdependencies* as well as the potential cascading effects that can arise from them. These interdependencies are identified and analyzed in close cooperation with CI operators to obtain an extensive CI interdependency graph. Further, a multi-domain simulation tool is developed, which uses stochastic models (e.g., Markov chains and probabilistic automata) to couple the individual domain networks and thus realizes a flexible yet realistic representation of the overall network of networks. This allows simulation of potential threats and evaluates their effects on the entire city. To obtain a realistic assessment of those consequences, the framework integrates a model on the spatial and temporal distribution of the city population.

Based on the output of the framework, risk experts in the city administration as well as within the CI operators will be able to see, which potential compensation and displacement mechanisms can be expected within the multi-domain network of CIs in case of an incident. From this data, targeted preventive safety measures can be derived and evaluated using the framework; their implementation will support minimizing the effects in the event of an incident. Accordingly, this will help to improve the preparation of emergency organizations and further increase the resilience of the entire city as well as the individual CIs in crisis situations.

The remainder of the paper is structured as follows: in the next section, we will provide an overview on existing methodologies and approaches for the core parts of the ODYSSEUS approach. Then, a detailed overview on the specific concepts of the ODYSSEUS framework and their interplay is provided. Finally, we discuss how this framework can support the resilience of CIs within a city as well as the resilience of the entire city itself.

EXISTING APPROACHES IN THE LITERATURE

Modeling Cities and Population Distribution

Many large European cities maintain Geographic Information Systems (GIS), which are used in a wide range of areas in the context of their administration. Much of this data is publicly available within the framework of Open Government Data and can be used for various applications. This includes, on the one hand, basic geometries describing physical objects of the city such as transportation networks or building structure models, and, on the other hand, socio-economic information, such as the use of the buildings or the distribution of the population in the urban space. In general, such information on the spatial distribution of the population within a city is only available in aggregated form for reasons of data protection. It can be given in the form of raster data, which is a representation of the resident population, or at the level of administrative units, where more detailed data on demography is available. Therefore, modelling approaches like spatial disaggregation (Mennis and Hultgren 2006) must be applied to achieve a more precise spatial distribution of the population. This means that the population figures that are available, e.g., per counting district, are distributed to a higher-resolution unit such as buildings (Aubrecht et al. 2009; Widhalm et al. 2015).

In general, this approach is not sufficient to provide a realistic impression of the population distribution of a city. Besides the resident population – i.e., those people who live there and thus also spend the night (”night population”) – but also the so-called ”day population” needs to be modelled (cf. Figure 1). Further, a distinction between the working and non-working population must be made; commuters to and from the urban area also need to be considered (Martin et al. 2015). In this context, time profiles can be helpful, which describe typical spatio-temporal activity patterns of the population and provide a plausible estimate of the population distribution that is sufficiently accurate for applications such as in the event of a disaster. An alternative to modelling the daily population is the analysis of mobile phone data for the spatio-temporal recording of population densities (Deville et al. 2014). The advantage of this method is the worldwide high penetration rate of mobile phones in urban agglomerations. However, it should be noted that in addition to the enormous amounts of data that have to be processed, the spatial accuracy of the data is still limited.

[1]National project funded by the Austrian Research Promotion Agency under grant no. 873539

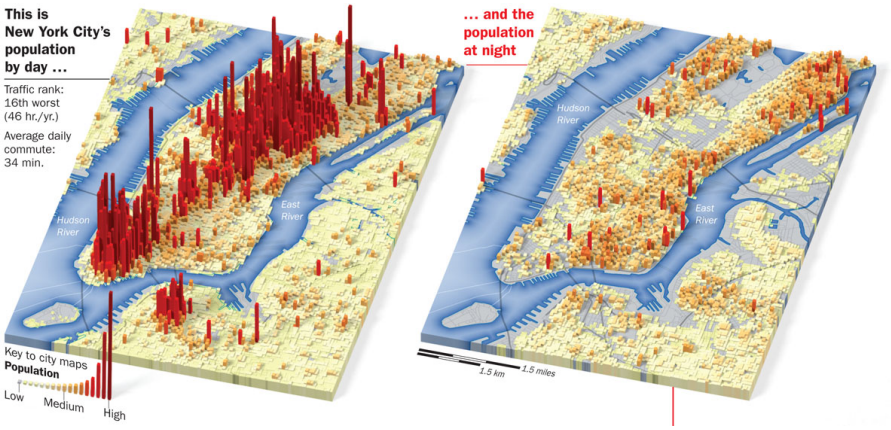

Figure 1. Illustration of the variation between day population and night population of New York

Interdependency Graphs

In the literature, relations and dependencies among CIs are mostly described using graph models, where CIs are represented as nodes and the dependencies, also differentiated in various types (Haimes 1981; Rinaldi et al. 2001), are represented as directed edges. Such a graph model provides a simple overview and a basic understanding of the interactions between CIs and can further be used as a solid basis for investigations and analyses (cf. Figure 2). For example, the Input-Output Interoperability Model (IIM) (Haimes and Pu 2001) uses the structure of interdependency graphs and linear equations to estimate the consequences of incidents on the network of CIs. Moreover, the Hierarchical Coordinated Bayesian Model (HCBM) (Yan et al. 2006) combines the information on interdependencies with incident data from different sources to improve the accuracy and variance in impact assessment and estimate low-probability-high-impact events (also know as "black swans") more precisely.

Other concepts include stochastic processes to improve the modeling of partly unknown dynamics and relations among the CIs. Therefore, the graph structure of the interdependencies among CIs or critical systems within them is used as a starting point for the analysis. Among them, techniques based on Bayesian networks are also applied to describe interdependencies between critical infrastructures (Schaberreiter, Kittilä, et al. 2013; Schaberreiter, Bouvry, et al. 2013). Additionally, percolation theory (Sander et al. 2002; Newman 2002), an approach coming from the field of epidemics, has been applied to analyze the spreading of the effects of an incident in critical communication networks (König, Gouglidis, et al. 2018).

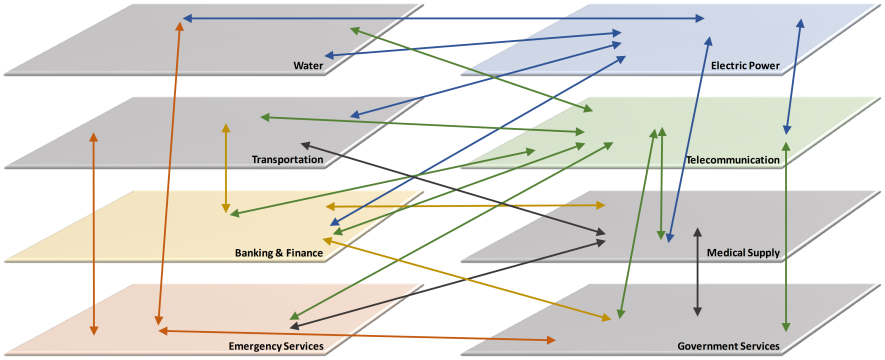

Figure 2. Schematic illustration of the interdependencies among CIs of the different domains (sectors).

Cascading Effects

When looking at the interdependencies among CIs, the question arises on how to identify and assess cascading effects among those infrastructures. The first approaches to solve this were looking at specific events and how they will influence future events (like the Cross Impact Analysis (CIA) (Gordon and Hayward 1968; Turoff 1971)). Currently, more complex concepts are applied to analyze cascading effects within CIs (e.g., Interdependent Markov Chains (IDMCs) (Wang et al. 2012) and their extensions (Rahnamay-Naeini and Hayat 2016)). However, Bayesian

models and Markov chains are more difficult to apply in realistic scenarios compared to percolation theory because of the large amount of data required to analyze and understand the system as well as to instantiate the model.

In (König and Rass 2018), a stochastic model has been developed that not only identifies potential cascading effects within a network of interconnected CIs, but also supports the assessment of such cascading effects. To achieve that, a combination of Markov chains and percolation theory is used, which has been further implemented to simulate the cascading effects among CIs within a region and evaluate their impact (Schauer et al. 2018; Grafenauer et al. 2018). The concept of Markov chains has been further extended to probabilistic Mealy automata (König, Rass, et al. 2019). Such an automaton describes a system which can be in one of finitely many states. Upon receiving an external signal, the Mealy automaton undergoes a state transition with a certain probability (cf. Figure 3). This representation facilitates a more detailed simulation of a CI (or systems therein) together with the cascading effects a specific incident might have on the entire system. Mealy automata are a core aspect of the ODYSSEUS approach, where each automaton describes a critical system within a CI and the signals represent incidents coming from another (dependent) system. Hence, we will describe their application in further detail below.

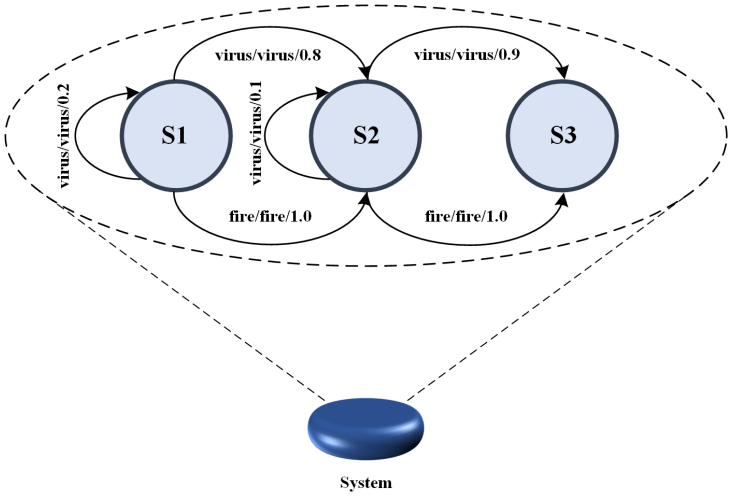

Figure 3. Schematic illustration of a Mealy automaton of some system with three operational states and transitions for the events ”fire” and ”virus”.

Simulation of Sub-Networks of Different Domains

In practice, CI operators usually run simulations of their respective networks to identify the above mentioned (cascading) effects of an incident. Such simulation frameworks are based on a combination of mathematical models of the physical processes and monitoring data gathered from the network itself. Thus, they provide an up-to-date picture of the network and a good estimation of its behavior (e.g., in a crisis situation). Among those mathematical models, various approaches exist (just to name a few): the simulations of power networks are based on Maxwell equations and Ohm's law (cf. for example (Kelley et al. 2015)), communication networks can be modeled using waiting lines (e.g. (Reiser 1979)); granular flows (Haut et al. 2005) or agent-based models (Yuhara and Tajima 2006) are used to simulate traffic within a city, and so forth.

Although these simulation frameworks can represent the behavior of an individual network, the important dependencies and resulting cascading effect across different domains (as discussed in the previous sections) are not considered in those simulations. In other words, incidents originating beyond the boundaries of a CI network as well as their effects are not part of the simulation. In the literature, co-simulation approaches (Lin et al. 2011; Kelley et al. 2015; Wen et al. 2015) can be found, where two domains – most commonly the power and ICT network – are coupled. However, a holistic view of all supply networks within a city is required to be able to perform comprehensive analyses of incidents and their cascading effects on the entire interdependent network of CIs.

Risk Management and Data Processing

The above mentioned results from the infrastructure graphs, cascading effects modelling and simulation are integrated into risk management processes. In classical risk management, and particularly when considering CIs, data preparation mainly focuses on presenting risks in such a way that results can be used as a support for

decision-making. However, in an increasingly dynamic business environment this type of risk management soon reaches its limits due to the large amount of data coming from constant monitoring of critical systems. Additionally, technologies and business processes nowadays have an increasingly fast cycles that require a more dynamic identification and assessment of risks. Hence, risk management needs to adapt to this situation and integrate the benefits coming from this large amount of available data into the decision-making to improve the prevention or mitigation of risks.

In the literature, the concept of dynamic data preparation has been discussed parallel to the increasing relevance of Big Data Analysis and mainly under the umbrella of data-driven management. In this context, a framework has been presented that attempts to overcome the limitations of risk management based on asset management by using big data methods (Middleton 2012). Other innovations in the field of crisis management, which apply Big Data analysis in the general corporate environment, are also examined (Zhang and L. Yang 2017). For Smart Cities, a similar method is discussed, which improves crisis intervention and disaster resilience (C. Yang et al. 2017). Novel risk management approaches for CIs that specifically rely on simulations (Schauer 2018) can apply these methodologies to effectively use the large amount of data. Additionally, more fine-grained data on the behavior of critical systems can help to make alternative concepts for risk minimization much more effective, as for example by applying game theory (Rass et al. 2015).

ODYSSEUS RISK MANAGEMENT APPROACH

GIS Model Development

As a first step towards a GIS model of a city, the relevant data needs to be collected. Therefore, a number of publicly accessible information sources are available (e.g. OpenStreetMap, OpenInfrastructureMap, etc.) to support the geo-referenced modelling of an urban area (cf. Figure 4). These information sources provide data about various different CI networks, e.g., road, railway, electricity. However, this data usually only contains a specific level of detail, i.e., the CI networks will not be displayed in their finest granularity; missing data can be gathered from experts within the CI operators. In this context, it is important to find a *level of abstraction* that remains useful in terms of the amount of data required, but *without revealing sensitive data of the infrastructures*, yet still offers enough detail to provide realistic statements later on in the risk assessment.

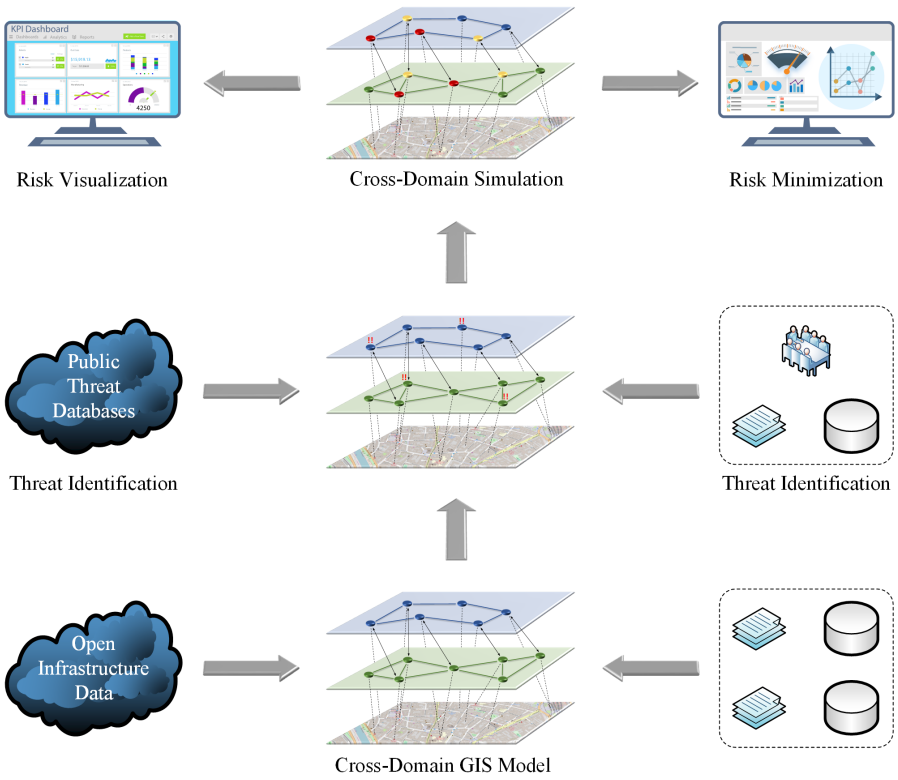

Figure 4. Schematic illustration of the overall ODYSSEUS Risk Management Approach.

The main goal of this step is to create a GIS-based representation of a city, where the different CI domains can be shown as individual layers in the GIS model. All the elements of the different CI networks up to a specific level of abstraction are geo-referenced, which allows an overview of the entire urban area with all the different CI networks located within it. In addition, the population distribution will be modelled in the same representation in a spatial context and under consideration of the time component (details follow below).

Threat Identification

In this step, the threats relevant to urban area in general and to the CIs in particular are identified and compiled in a catalog. As a basis, *domain-specific threat catalogs* as well as *national risk analyses* can be used. The resulting catalog should include *natural and technical* as well as *intentional and non-intentional* threats for the CI networks. The identified threats are backed with reliable data from historical events or current studies. This is achieved using incident databases from the CI operators (e.g., about road accidents, asset malfunctions, hacking, etc.) as well as public threat databases (cf. Figure 4). Subsequently, security controls for the identified threats are derived from publicly available guidelines as well as from best practice approaches from the CI operators.

Based on the resulting threat catalog, *complex threat scenarios* are defined in a next step, which reflect current concerns of the CI operators and thus establish a clear practical relevance. In detail, the prevailing circumstances and the chronological sequence as well as the affected infrastructures and areas of the city are specified for each scenario. To represent a broad spectrum of potential incidents, the scenarios are selected from different threat categories. It should be pointed out that the more information on one scenario is available (and the more precise this information is), the more realistic the outputs will be. Hence, experts from the CI operators are consulted through workshops to formulate the threat scenarios as detailed as possible without revealing any sensitive information on the CI networks.

Cascading Effects Simulation

The simulation of cascading effects which span across the different CI networks is the core feature of the cross-domain risk analysis framework that is going to be developed in ODYSSEUS. In general, this simulation is based on a directed graph model, consisting of nodes and edges, representing the individual assets and links within the CI networks. This is formalized in a generic way such that it can be applied to single domains, e.g., the power or ICT network, as well as to the overall system, i.e., including all CI networks as well as their interdependencies. Accordingly, we speak of two different views or levels of the simulation model, i.e., the *intra-domain* and the *inter-domain* level (cf. Figure 5). In a way, one may think of the intra-domain model as a risk assessment simulation model that is specific for a certain domain (e.g., energy, water, etc.). It describes the *physical behavior* of the CI subnetwork. On top of this, the inter-domain model represents the interdependencies among the individual domain-specific physical networks. The model then operates on abstract information about the operational states of the assets, which is exchanged across those interdependences (cf. Figure 5).

As the name indicates, the intra-domain level focuses on the simulation of one individual network for a specific domain, e.g., the power network. On the one hand, established physical models from the literature can be used to implement the simulation and describe the behavior of a network. Since we are mostly operating on publicly available information and thus often cannot drill down to the last system of a network, there might not be enough data available to instantiate the physical model properly. Hence, a more promising approach for this scenario is finding an approximation for the dynamics of the individual systems in a CI network. Such an approximation can be achieved by using machine learning and building an *artificial neural network* (ANN) for each system. The ANN representing a node is trained based on real-life historic data of that node, or from artificial data obtained from simulation software (the latter may be particularly valuable as a rich source of data, in cases where experts are not available or human domain knowledge is scarce or difficult to obtain). The ANN learns to mimic the physical processes and behavior of a node based on the combination of input and output values coming from log files or other system monitoring tools and can later on simulate the node in a realistic way. Each ANN is thus a *digital twin* for some CI subnetwork. It has to be noted that the monitoring data required for this training needs to come from the CI operators. Since this data is sensitive in most cases, one option is that the CI operator trains the ANN itself without providing the monitoring data to someone else and only gives the resulting ANN to the simulation model.

The inter-domain (or cross-domain) level focuses on the simulation of the overall system, i.e., the dynamics between the individual CI networks. Therefore, the information on the interdependencies between the individual networks are required, i.e., which node in one domain influences a node in another domain. Since these effects are highly complex, including physical as well as organizational mechanisms, we are using Mealy automata as a particular *formalization of stochastic dependencies* to approximate them in an abstract way (cf. (König and Rass 2018;

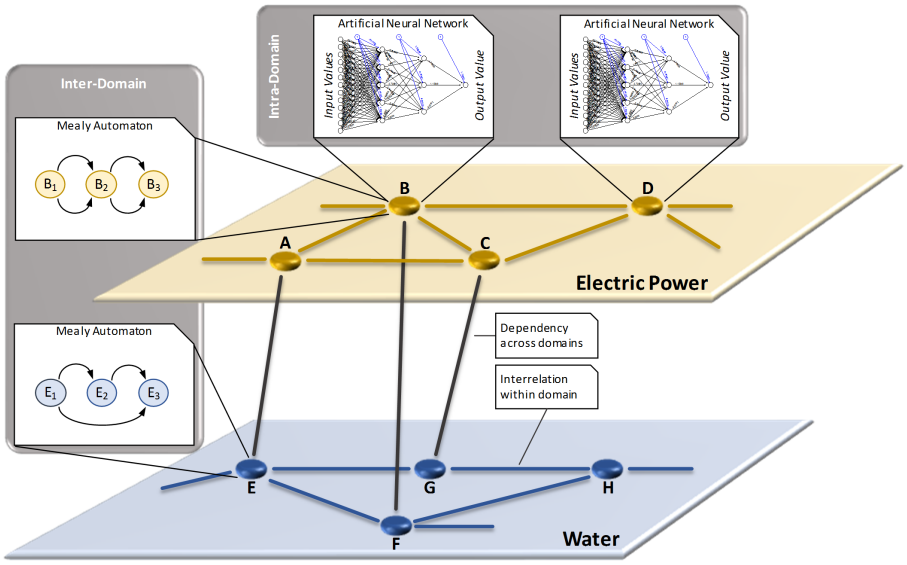

Figure 5. Illustration of the interplay between the intra-domain and inter-domain model.

Grafenauer et al. 2018; König, Rass, et al. 2019) for more details on the approach). In this formalization, a node is taken as a black-box that undergoes changing risk states over its life time, ranging from "undisturbed operation" up to "total failure". A change of state is triggered by external influences, and may result in different new risk states with distinct probabilities (stochastic model). Mealy automata are exactly such state machines that change their internal state, here a risk status, based on external signals and with prescribed probabilities. In our case, an external influence can be an incident happening to the node (e.g., an attack or a technical failure) or the change of the operational state of another node, on which it is depending on. The states represent the current risk level to which a CI is exposed, and the probability is determined by the CI's own resilience or inner dynamics to react on the new situation.

To combine those two levels to form a cross-domain model, the model in (König, Rass, et al. 2019) is extended in ODYSSEUS. In detail, a mapping is introduced from the intra-domain representation of nodes by ANNs to the representation by Mealy automata. Since the ANN reflects the behavior of a node, it can determine the implied risk level and thus the state change of the Mealy automaton. Additionally, both the technical and organizational information flow between depending components of different domains are analyzed using domain-specific expertise from the CI operators. The results then describe the interdependencies and define the cross-domain influence between the Mealy automata. In this way, the individual CI networks are connected and a cross-domain simulation can be implemented, which provides a *holistic understanding of the impact of potential threats across multiple interrelated networks*.

Societal Impact Assessment

The simulation of cascading effects is only one input to risk management; the other one is to assess the impact of those effects. To obtain a valid assessment, highly accurate spatio-temporal information, both on structures within the city and on the affected population, is required. However, demographic data are only available at a rough spatial level and not in a chronologically differentiated manner (as already mentioned above). This results in the need to refine the distribution of the population both in a *spatial and in a temporal context*. To achieve that, we are applying methods of disaggregation in the ODYSSEUS approach, which allow an estimation of the necessary differentiation in the form of quantitative spatio-temporal population models. These models are subsequently used as a basis for impact analyses and assessment of the effects on the population.

To measure the consequences on a diverse and complex ecosystem like a city, several different *impact indicators and impact classes* are defined, which need to cover the broad spectrum of social influencing factors. Such impact classes can be, for example, "people", "economy", "environment" or "society", with indicators measuring the number of wounded people during an incident, the monetary value of the direct and indirect damages, the amount of polluted water or the degree of discontent in the population due to the incident. In this context, the population distribution model of the city provides useful inputs to all these indicators. The final assessment scheme consists of

a function which receives as input the current state of the critical supply networks in the city and calculates an abstract impact measure on this basis.

Integration into Risk Evaluation

The data and results obtained from the simulation and the impact assessment need to be integrated in the risk management process, more specifically into the risk evaluation. Hence, a core focus of this approach is the *dynamic estimation and continuous reassessment* of the risk based on new information. To achieve that, the processing of the results adapts to the changing environment and takes advantage of the additionally available information. This includes the detailed data on the effects of an incident on the overall system coming from the simulations as well as the extensive information from external sources (e.g., from threat intelligence providers or the CI operators themselves). After a reasonable processing, the aim of the approach is to support CI operators with tailored assessments of risks as well as recommendations to prevent or mitigate them, which can significantly speed up corrective actions.

In addition, the results as well as their visualization needs to be *optimally adapted to different personal profiles*. In ODYSSEUS, this is targeted by a methodology for data representation and visualization that builds on the data provided by the project's dynamic risk management approach (cf. Figure 4). Since many roles from within an organization (e.g., managers, technicians, administrators, etc.) need to be involved into the risk management process in one way or another, the aim is to tailor the representation of the results to the different organizational roles. Only in that case, they are able to complete their risk management tasks in an efficient manner and based on a comprehensive understanding of the data presented to them.

Risk Minimization

In order to further support decision-makers in implementing security controls for specific threat scenarios, a *game-theoretical model* is extending the ODYSSEUS approach to identify the optimal allocation of resources (cf. Figure 4). In detail, a CI operator is facing a (intentional or natural) threat and has several security controls (coming from the threat catalog compiled in the beginning) for this specific threat scenario at hand. Using the simulation for cascading effects and the societal impact assessment, the effectiveness of each of these strategies, i.e., to which degree (if at all) they reduce the impacts of an incident, is evaluated.

Based on the methods developed for the dynamic estimation and continuous re-assessment of the threats refine and prepare the data for the game theoretical framework. Accordingly, the framework is designed in such a way that it allows direct integration of simulation results by using distribution-valued payoffs. This eliminates the need of aggregating complex data into a single numbers and thus losing information in that process. Additionally, the approach allows the integration of potentially contradicting expert opinions, i.e., there is no need to find a compromise on the expected impact but rather all views are taken into account. In this way, the game theoretical framework facilitates an *optimal fine-tuning of different variants of security controls* and thus realizes an improved resource allocation for the individual controls, which are then carried out by the CI operators.

EFFECTS ON RESILIENCE

When looking at the resilience of the individual CI networks as well as the entire city, the city administration and the emergency organizations might not be prepared for consequences stemming from cross-domain effects. In case of an incident or during a crisis situation, this might increase the time until all CI networks can be brought back to full operation, i.e., the resilience of the individual CIs and also of the overall city. To reduce that time span, the outputs coming from the ODYSSEUS framework can support the administration and emergency organizations in different ways:

1. the results from the simulation framework, i.e., which assets from the different domains are affected by a specific incident, provide a *holistic view* to the organizations on the potential cascading effects a specific incident might have on individual CI networks as well as on the whole city. This supports them in obtaining a clear impression of the cross-domain effects and avoids missing out on dependencies that are not explicitly visible.

2. the overall impact of an incident (including the cascading effects indicated by the simulations) coming from the risk assessment will give them a *realistic estimation of the damage* a specific incident might have on the entire city, i.e., including consequences to the individual networks as well as to social life in the city (in contrast to the impact on a single network). The usage of different impact indicators allows them to assess the impact in various terms and thus obtain a better insight into multi-domain consequences.

3. the list of security controls coming from the risk minimization will indicate those measures, which should be implemented first since they will reduce the overall impact of the considered incident to a minimum. This enables the organizations to *appropriately prepare to specific incidents* and efficiently react in a crisis situation.

Using this information from the ODYSSEUS framework, the compensation and displacement mechanisms within the multi-domain network of CIs can be better anticipated compared to an analysis which only considers the respective networks individually. Hence, this strengthens the resilience of the CIs and the entire city by reducing the time infrastructures as well as people are affected by the cross-domain effects of an incident.

CONCLUSION

In this paper, we presented a general concept for a risk management approach, which is able to support the assessment of cascading effects among CIs located within a metropolitan area. Therefore, a GIS model of the area is created using open-source data, CIs and their interdependencies are identified therein and a network of CI networks is built. A simulation framework is using this information to simulate cross-domain effects. Those effects are further assessed according to their societal impact; additionally, mitigation actions are evaluated. The output of the framework can then be used by city administration and CI operators to improve their activities in crisis situations in terms of efficiency and effectiveness. This shall ultimately lead to an improvement of the resilience of the individual CIs and accordingly of the entire city.

ACKNOWLEDGEMENT

This work was supported by the research Project ODYSSEUS ("Simulation und Analyse kritischer Netzwerk-Infrastrukturen in Städten") funded by the Austrian Research Promotion Agency under Grant No. 873539.

REFERENCES

Aubrecht, C., Steinnocher, K., Hollaus, M., and Wagner, W. (2009). “Integrating earth observation and GIScience for high resolution spatial and functional modeling of urban land use”. In: *Computers, Environment and Urban Systems* 33.1, pp. 15–25.

Deville, P., Linard, C., Martin, S., Gilbert, M., Stevens, F. R., Gaughan, A. E., Blondel, V. D., and Tatem, A. J. (2014). “Dynamic population mapping using mobile phone data”. In: *Proceedings of the National Academy of Sciences* 111.45, pp. 15888–15893.

European Comission (2016). “DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union”. In: *Official Journal of the European Union*, pp. L 194/1.

Gordon, T. J. and Hayward, H. (1968). “Initial experiments with the cross impact matrix method of forecasting”. In: *Futures* 1.2, pp. 100–116.

Grafenauer, T., König, S., Rass, S., and Schauer, S. (2018). “A Simulation Tool for Cascading Effects in Interdependent Critical Infrastructures”. In: *Proceedings of the 13th International Conference on Availability, Reliability and Security - ARES 2018*. ACM Press, pp. 1–8.

Haimes, Y. Y. (1981). “Hierarchical Holographic Modeling”. In: *IEEE Transactions on Systems, Man, and Cybernetics* 11.9, pp. 606–617.

Haimes, Y. Y. and Pu, J. (2001). “Leontief-Based Model of Risk in Complex Interconnected Infrastructures”. In: *Journal of Infrastructure Systems* 7.1, pp. 1–12.

Haut, B., Bastin, G., and Chitour, Y. (Jan. 2005). “A macroscopic traffic model for road networks with a representation of the capacity drop phenomenon at the junctions”. en. In: *IFAC Proceedings Volumes*. 16th IFAC World Congress 38.1, pp. 114–119.

Kelley, B. M., Top, P., Smith, S. G., Woodward, C. S., and Min, L. (Apr. 2015). “A federated simulation toolkit for electric power grid and communication network co-simulation”. In: *2015 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*. Seattle, WA, USA: IEEE, pp. 1–6.

König, S., Gouglidis, A., Green, B., and Solar, A. (2018). “Assessing the Impact of Malware Attacks in Utility Networks”. In: *Game Theory for Security and Risk Management*. Ed. by S. Rass and S. Schauer. Cham: Springer International Publishing, pp. 335–351.

König, S. and Rass, S. (2018). "Investigating Stochastic Dependencies Between Critical Infrastructures". In: *International Journal on Advances in Systems and Measurements* 11.3, pp. 250–258.

König, S., Rass, S., Rainer, B., and Schauer, S. (2019). "Hybrid Dependencies Between Cyber and Physical Systems". In: *Intelligent Computing*. Ed. by K. Arai, R. Bhatia, and S. Kapoor. Vol. 998. Cham: Springer International Publishing, pp. 550–565.

Lin, H., Sambamoorthy, S., Shukla, S., Thorp, J., and Mili, L. (2011). "Power system and communication network co-simulation for smart grid applications". In: *ISGT 2011*. IEEE, pp. 1–6.

Martin, D., Cockings, S., and Leung, S. (2015). "Developing a Flexible Framework for Spatiotemporal Population Modeling". In: *Annals of the Association of American Geographers* 105.4, pp. 754–772.

Mennis, J. and Hultgren, T. (2006). "Intelligent Asymmetric Mapping and Its Application to Areal Interpolation". In: *Cartography and Geographic Information Science* 33.3, pp. 179–194.

Middleton, B. P. (2012). "The right data drives asset management decision making: a case study of delivering improvements". In: *IET & IAM Asset Management Conference 2012*. IEEE, pp. 1–3.

Newman, M. E. J. (2002). "Spread of epidemic disease on networks". In: *Physical Review E* 66.1, p. 016128.

Rahnamay-Naeini, M. and Hayat, M. M. (July 2016). "Cascading Failures in Interdependent Infrastructures: An Interdependent Markov-Chain Approach". In: *IEEE Transactions on Smart Grid* 7.4, pp. 1997–2006.

Rass, S., König, S., and Schauer, S. (2015). "Uncertainty in Games: Using Probability-Distributions as Payoffs". In: *Decision and Game Theory for Security: 6th International Conference, GameSec 2015, London, UK, November 4-5, 2015, Proceedings*. Ed. by M. Khouzani, E. Panaousis, and G. Theodorakopoulos. Springer International Publishing, pp. 346–357.

Reiser, M. (Aug. 1979). "A Queueing Network Analysis of Computer Communication Networks with Window Flow Control". en. In: *IEEE Transactions on Communications* 27.8, pp. 1199–1209.

Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001). "Identifying, understanding, and analyzing critical infrastructure interdependencies". In: *IEEE Control Systems* 21.6, pp. 11–25.

Sander, L. M., Warren, C. P., Sokolov, I. M., Simon, C., and Koopman, J. (2002). "Percolation on heterogeneous networks as a model for epidemics". In: *Mathematical Biosciences* 180.1, pp. 293–305.

Schaberreiter, T., Bouvry, P., Röning, J., and Khadraoui, D. (2013). "A Bayesian Network Based Critical Infrastructure Risk Model". In: *EVOLVE - A Bridge between Probability, Set Oriented Numerics, and Evolutionary Computation II*. Ed. by O. Schütze, C. A. Coello Coello, A.-A. Tantar, E. Tantar, P. Bouvry, P. Del Moral, and P. Legrand. Vol. 175. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 207–218.

Schaberreiter, T., Kittilä, K., Halunen, K., Röning, J., and Khadraoui, D. (2013). "Risk Assessment in Critical Infrastructure Security Modelling Based on Dependency Analysis". In: *Critical Information Infrastructure Security. CRITIS 2011*. Lecture notes in computer science 6983. Berlin: Springer.

Schauer, S. (2018). "A Risk Management Approach for Highly Interconnected Networks". In: *Game Theory for Security and Risk Management*. Ed. by S. Rass and S. Schauer. Springer International Publishing, pp. 285–311.

Schauer, S., König, S., Latzenhofer, M., Rass, S., and Grafenauer, T. (2018). "Analyzing Cascading Effects among Critical Infrastructures : The CERBERUS Approach". In: *Proceedings of the 15th ISCRAM Conference – Rochester, NY, USA May 2018*. Rochester Institute of Technology, pp. 428–437.

Turoff, M. (1971). "An alternative approach to cross impact analysis". In: *Technological Forecasting and Social Change* 3, pp. 309–339.

Wang, Z., Scaglione, A., and Thomas, R. J. (2012). "A Markov-Transition Model for Cascading Failures in Power Grids". In: *2012 45th Hawaii International Conference on System Sciences*. IEEE, pp. 2115–2124.

Wen, T., Lyu, X., Kirkwood, D., Chen, L., Constantinou, C., and Roberts, C. (Sept. 2015). "Co-simulation Testing of Data Communication System Supporting CBTC". In: *2015 IEEE 18th International Conference on Intelligent Transportation Systems*. Gran Canaria, Spain: IEEE, pp. 2665–2670.

Widhalm, P., Yang, Y., Ulm, M., Athavale, S., and González, M. C. (2015). "Discovering urban activity patterns in cell phone data". In: *Transportation* 42.4, pp. 597–623.

Yan, Z., Haimes, Y. Y., and Wallner, M. G. (2006). "Hierarchical coordinated Bayesian model for risk analysis with sparse data". Baltimore, USA.

Yang, C., Su, G., and Chen, J. (2017). "Using big data to enhance crisis response and disaster resilience for a smart city". In: *2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA)*. IEEE, pp. 504–507.

Yuhara, N. and Tajima, J. (2006). "Multi-driver agent-based traffic simulation systems for evaluating the effects of advanced driver assistance systems on road traffic accidents". In: *Cognition, Technology & Work* 8.4, pp. 283–300.

Zhang, J.-J. and Yang, L. (2017). "A research on enterprise crisis management innovation based on big data technology". In: *2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA)*. IEEE, pp. 406–409.