Creating a Cross-Domain Simulation Framework for Risk Analyses of Cities

Stefan Schauer, Stefan Rass

Chapter 1

APPROACH TOWARDS A CROSS-DOMAIN SIMULATION MODEL TO SUPPORT RISK ANALYSIS IN CITIES

Stefan Schauer, Stefan Rass

Abstract Cities and their agglomerations are home to a large number of critical infrastructures 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 one infrastructure can have an impact on the entire system. 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. In this article, we want to show a general approach on how to create a cross-domain simulation model, which can describe the major critical infrastructure networks within a large city up to a certain level of abstraction. In contrast to existing solutions, this approach focuses mainly on the dynamic relationships between networks and integrates mathematical models from stochastics for a realistic representation. The central output is a framework that supports 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.

Keywords: cross-domain simulation interdependencies stochastic model machine learning critical infrastructures.

1. Introduction

Critical infrastructures (CIs) are generally defined as organizations or systems (or parts thereof) that are responsible for the maintenance of essential economic and societal functions and whose disruption or failure would have a significant impact on the economic and social well-being of the population [5]. Large cities and their agglomerations are

home to a large number of such CIs that provide central societal processes such as the supply of essential goods and services in a confined space. This creates a number of geographical, physical as well as logical (information-related) dependencies among them, resulting in a highly interrelated and sensitive network of organizations and connections [29]. In particular, CIs in the areas of general utilities (electricity, gas, water, etc.), information and communication technologies (ICT), distribution of goods (food, fuel, etc.) and transportation (road, rail, etc.) operate extensive networks which have special requirements in terms of security measures. Due to such strongly connected interrelations and dependencies, it is clear that an impairment or even the total failure of a critical supply network does not only affect the network itself but can also have direct or indirect (cascading) effects on a number of other critical networks as well as on the economic and social well-being of the population. Especially in the context of the Network and Information Security (NIS) Directive in Europe [4], a detailed risk analysis with a strong focus on the interaction of these networks and potential cascading effects for the population is a central aspect for the protection of these critical infrastructures.

Currently used systems and tools (see Section 1.2) that can simulate the function of the supply networks within a city (and thus can serve operators and administrative institutions as a basis for a risk analysis) have some disadvantages which make it difficult to fully assess the effects on the overall system of a city. First of all, the simulation approaches represent isolated solutions, i.e., they only depict one supply network at a time. These simulations are designed for the physical characteristics and technical conditions of the networks and therefore only allow a close examination of an individual network. In a way, we can think of these to provide a *local view only*, whereas a defense against cascading effects on a larger scale calls for a bird's eye perspective, i.e., a *global view* on a network of interdependent CI. This calls for cross-domain simulation, for which models are far less available. However, the dependencies on other networks are usually ignored, which means that a detailed understanding of the dynamics in the overall system of all networks within a city is missing. Additionally, the mainly proprietary systems used by most supply network operators do not necessarily provide the option of exchanging data or connecting to systems of other operators to allow a cross-domain analysis of an incident. Thus, although the effects within a particular network can be analyzed by respectively specialized simulations,, a cross-domain view is generally not possible. As a consequence, the effects of potential threats cannot be assessed precisely,

since cascading effects in the multi-network infrastructure of a city and the associated effects on social life are not considered.

In this article, we will show a general concept how to develop a cross-domain simulation model, which describes the networks of the central utility infrastructures electricity, gas, water, food and telecommunications (including ICT) as well as the transport networks (road and rail) within a large city. The model is developed as part of the currently running project ODYSSEUS[1] and aims at simulating potential threats (both natural disasters and man-made incidents) with a strong focus on the dynamic relationships between the networks. Therefore, ODYSSEUS applies probabilistic models (e.g. Markov chains, probabilistic automata) to achieve a flexible yet realistic representation of the networks. The core output of the ODYSSEUS project is a framework that allows a detailed assessment of both the impact of threats on individual CIs and the possible cascading effects within the entire network of critical supply infrastructures. The simulation describes which potential compensation and displacement mechanisms can be expected within the multi-domain network of supply infrastructures in case of an incident. From this knowledge, targeted preventive safety measures can be derived, presented and evaluated, the implementation of which will help to minimize the effects in the event of an incident.

2. Existing Approaches in the Literature

2.1 Simulation of Supply Networks

A detailed overview of the critical supply networks and their behavior in the event of an incident can be achieved on the one hand by continuously monitoring the network (collecting data from different components in the network) and on the other hand by simulating the behavior of this network on the basis of mathematical models. The combination of these two approaches allows both an up-to-date picture of the network and a good estimation of its behavior in future situations. The underlying mathematical models are often specific to the respective domain and are therefore based on various physical approaches, as shown in Table 1. The given list of models (which is not an exhaustive list) already underlines the enormous diversity of existing simulation approaches. Similarly, a subdivision of different approaches according to the underlying methodology is possible, e.g., empirical, agent-based, system dynamics-based, economic aspects, or network-based.

A central shortcoming of the approaches mentioned in Table 1 is that they can only represent a single network or a single domain, the dependencies between the networks are typically not represented in the

Table 1. Overview on different model-based simulation approaches applied in various CI domains.

Domain	**Physical Models (selection)**
Traffic	Granular flows (macroscopic model, e.g. [11]), agent-based simulation (microscopic model, e.g. [38]), or variants thereof; cf. for example [12].
Water	Incompressible fluids or similar; cf. for example [24][22] [2][33].
Gas	Compressible liquids/gases or similar; cf. for example [7] [25].
Communication	Stochastic models (waiting lines, e.g. [27]) or similar; cf. for example [14][36].
Power	Ohm's laws and alternating current technology, Maxwell equations, induction law, etc.; cf. for example [14][32]

model. Although this allows simulations and risk analyses to be carried out for a single network, it does not allow a view beyond the boundaries of the network, such as a holistic view of all supply networks within a city. In order to achieve such a coupling of different simulation systems into an overall system, so-called co- or cross-domain simulation methods [14][36][32] are used. In these methods, however, usually only two domains can be "interwoven" into a common model, such as energy and communication [23] in the context of Smart Grids.

2.2 Interdependency Graphs

Dependencies between critical infrastructures or parts thereof have been extensively investigated in recent years. Various approaches to categorize these dependencies can be found in the literature (cf. for example [29][28]), which basically propose five categories: physical, informational, spatial, procedural and social dependencies ([29][28]). Such categorization can contribute to a better understanding of the interaction between infrastructures, e.g., by visualization in the form of an interdependency graph and supports the assessment of the probability that an incident will have an impact on related infrastructures. In real scenarios, however, the interdependencies are much more complex and the definition of these categories, as contained in the literature, is often too general to be applied directly in practice.

Refined approaches to categorize and describe the interrelationships between critical infrastructures include the Hierarchical Holographic Model (HHM), the Input-Output Interoperability Model (IIM), and the Hierarchical Coordinated Bayesian Model (HCBM) (see [8] for more details on these models). In this context, the HHM [9] provides a taxonomy that explains the various possible interdependencies between critical infrastructures in more detail than described in [29]. This makes it possible to get a more precise idea of the existing interdependencies. The IIM [10] also provides a detailed overview of the interdependencies between critical infrastructures (or more generally between economic sectors) and describes the impact of incidents based on linear equations. However, it focuses heavily on economic aspects that may not always be the appropriate context for considering critical infrastructures. Rather, extreme events are of low probability but with serious consequences of particular interest, although generally little data on such events is available. Therefore, HCBMs [37] allow the combination of data on extreme events from different sources in order to improve the accuracy and variance in impact assessment.

One interesting approach to identify and assess the interdependencies among critical infrastructures is the Preliminary Interdependency Analysis (PIA) [1]. The PIA provides a methodology to inspect different types of dependencies (e.g., functional dependencies, similar components or common environment) and refine the findings in an iterative way. This then leads to a High Level Service Model and a Detailed Service Behaviour Model, which provide an overview on the abstract services of the critical infrastructures and the operation of those services. In this way, the PIA is similar to the ODYSSEUS approach we will present below, since it manages to connect services from different domains and also describe the operational states of those services in case of an incident.

Another effective way to model partly unknown dynamics and relations between events are stochastic processes. By using probability distributions, these models can take into account the intrinsic randomness and uncertainty inherent in the interaction between critical infrastructures. A prominent example of this is percolation theory [15][30], but has rarely been used in the areas of security and risk management. For example, percolation theory was used in [16] to model the spreading of malware within a heterogeneous network. In addition, techniques based on Bayesian networks are also used to describe interdependencies between critical infrastructures [31].

2.3 Cascading Effects

Interdependency graphs are also frequently used as a basis for simulation methods to describe cascading effects (as mentioned above). A first approach in this direction was the Cross Impact Analysis (CIA), which allows to describe how the relationships between individual events will affect future events (for a more detailed examination of CIA for cascading effects, see [34] and the references contained therein). In a more general approach, Interdependent Markov Chains (IDMCs) are used to describe the propagation of cascading effects within a utility infrastructure [26]. Initially, IDMCs were used in the energy sector to describe the dynamics of the system in order to analyze overload scenarios and estimate the probability of a blackout. This model was later extended to be applicable among critical infrastructures [26]. However, Bayesian models and Markov chains are more difficult to apply compared to percolation theory because of the large amount of data required to analyze the system and understand the interplay. In addition to the above-mentioned approaches, various other stochastic models for the description of cascading effects are available, which in particular specify dependencies between different networks (cf. [13][8][21]) and can be simulated using percolation theory (cf. [20]).

However, such models are sometimes difficult for end users to instantiate (parameterize), since the specification of probabilities for the behavior of network nodes is often an essential part of the model building. Software support (e.g. [35]), and process-oriented procedure models for data collection (e.g. [3]) exist, but may be difficult to implement in practice due to the diversity of the domains involved. In [17][18], a stochastic model has been developed that not only identifies potential cascading effects within a network of interconnected critical infrastructures, but also supports the assessment of these cascading effects. Therefore, existing methods from the fields of percolation theory and Markov chains (see details above) were combined and extended to determine the possible consequences of certain scenarios, e.g., when an infrastructure has to reduce its capacity or fails completely, by means of simulations [6]. In a similar approach, the concept of Markov chains is extended by probabilistic Mealy automatons [19], which allows a simulation of cascading effects within a critical infrastructure.

3. ODYSSEUS Simulation Approach

The cross-domain analysis framework that is going to be developed in ODYSSEUS is based on the simulation of the effects of different threats to supply networks within a city, which are essentially determined by the

interdependencies of these networks. This typically means a "parallel" simulation of different networks taking into account the current state of the another network, e.g., between electricity $\leftrightarrow$ ICT). The framework in ODYSSEUS is based on a construction that is equally applicable to all domains and is based on a representation as a directed graph consisting of a set of nodes and edges. A node is not fixed in its physical characteristics and can, depending on the type of simulation, represent a node in the power grid, a distribution point in the water network etc., while edges represent the connections between these nodes in various forms (physical, logical, ...). Accordingly, an edge can represent a connection between two nodes in the same domain or between different domains [2]. Therefore, the model is divided into an intra-domain and an inter-domain (or cross-domain) level.

3.1 Simulation on the Intra-Domain Level

The intra-domain level focuses on the simulation of one individual network, e.g., the power network, and therefore pursues two basic approaches: on the one hand, the dynamics within the network are described on the basis of the underlying and proven physical models (see Table 1). In this way, each individual network can be simulated using well-established models from the literature, which are instantiated using existing information on the individual networks. Therefore, existing theoretical and practical tools (theories and software) implementing these domain-specific models can be used. However, there is one drawback to this approach: since utility networks are only considered up to a certain level of abstraction (e.g., due to complexity of the overall network or the available information), these physical models may not always be fully applicable.

In cases where such an "exact" model-based simulation is unavailable or infeasible, the second approach focuses on the approximation of the dynamics by generic models. More precisely, the behavior of a node A is simulated by an artificial neural network (ANN). Abstractly speaking, this ANN is represented as a function f_A with n input parameters and m output values, which can be flexibly designed by training data (cf. Figure 1). The same procedure is used for edges $A \to B$, whose behavior is also represented by a (analogously constructed) function $f_{A \to B}$. In particular, this form of modelling allows an abstraction of physical processes in a purely qualitative way, such that it can be applied for any physical quantities (such as electrical power, water pressure, traffic density, etc.) used in the respective network.

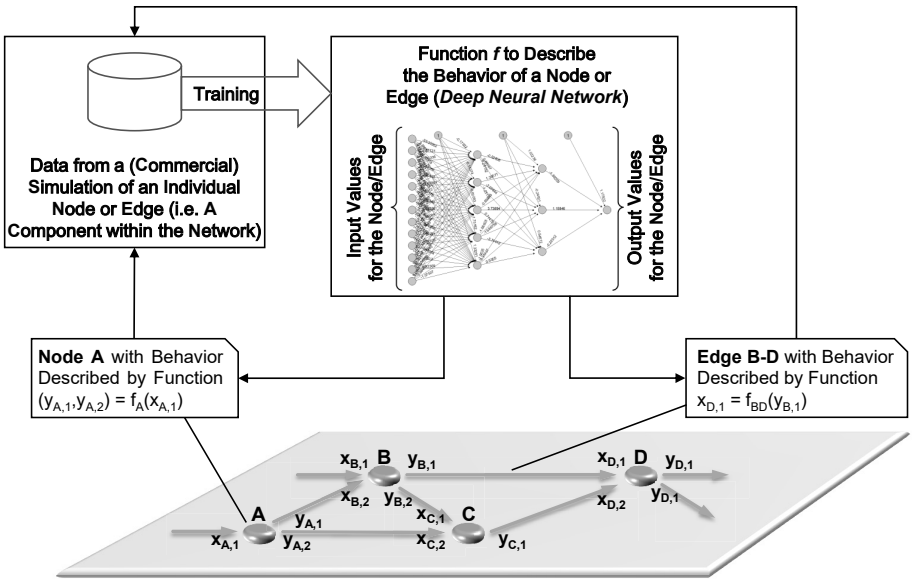

Figure 1. Illustration of the intra-domain view of the model.

This machine learning approach can approximate single physical systems (e.g., incompressible fluids for water networks, compressible gases for gas networks, granular flows for traffic networks, etc.), if there is not enough information available for a complete simulation (e.g., due to the chosen level of abstraction). To achieve that, the participation of stakeholders and network operators is required to supply a sufficient amount of training data for the ANN (or more precisely the function f_A) described above. If such data is available, the ANN can simulate the physical behavior of a node or an edge with sufficient accuracy. This results in a network of nodes and edges which can be seen (mathematically and for the simulation) as a series of different function blocks whose individual behavior can be adapted to the conditions of the simulation (see Figure 1 for a graphical illustration).

3.2 Simulation on the Inter-Domain Level

The inter- or cross-domain level focuses on the simulation of the overall system, i.e., the dynamics between the individual networks. Therein, the behavior of a node is characterized by its reaction to external influences, i.e., by a change in the operational state of its neighboring (dependent) nodes. These interdependencies are subject to complex dynamics,

which can be determined by technical relations as well as organizational (i.e. non-technical or non-physical) mechanisms, such as emergency supply systems, insurances for the failure of individual suppliers or similar. To describe these dependencies, we are relying on a formalization of stochastic dependencies, which has already been developed in [17][18][6] [19].

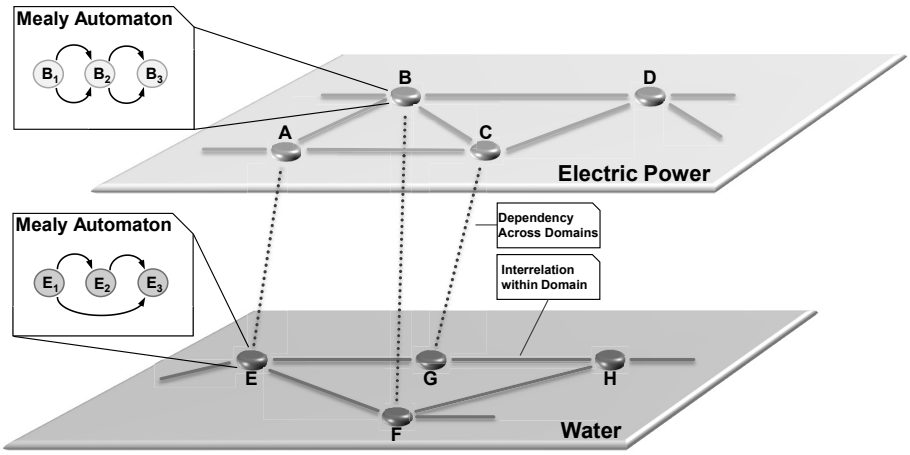

Figure 2. Illustration of the inter-domain view of the model.

In detail, to find a more abstract way of representing the general condition of a node separately from its respective domain, each node is characterized by different operational states, which can range, for example, from "undisturbed operation" to the "total failure" of a node. In this way, the effects of an incident on a node E in one domain (for example in the power network) can be represented by the change of its operational state. Furthermore, due to the existing dependencies across different domains, the change of the operational state of node E can affect the node A in another domain (e.g., in the water network, cf. Figure 2). Hence, this external event in the power network triggers a transition of node A from one operational state to another. From a theoretical perspective, each node can be understood as a probabilistic Mealy automaton, since such an automaton is described using different states and can emit symbols to model the effects influencing other nodes [19]. An additional advantage of this representation is that state transitions are probabilistic, i.e., the inherent uncertainty about the influences between different domains can be represented in this process. In other words, the

node A may or may not react onto a state change of the connected node E in the other domain depending on some probability.

This prior method provides a basis for the description of the connections between different infrastructure networks. However, in ODYSSEUS the approach is extended and further developed for a cross-domain and generic use in order to better represent these dynamic aspects of the individual networks. For this purpose, the information flow between the individual components (both technical and organizational) of the different domains is analyzed and their interplay and interactions are considered to make use of domain expertise about the dependencies between the nodes. This information flow between the networks is used to define the transitions of the operational states of each node.

In a similar way, the state transitions are also depending on the node's behavior according to the intra-domain model. Hence, the output of the ANNs from the intra-domain model described in the previous Section 1.3.1 are mapped onto the operational states of the automaton representation of the node. In this way, the machine learning approach is applied to model the physical part of a node and mimic its behavior according to concrete physical processes whereas the Mealy automaton representation integrates more abstract and informal knowledge about the interdependencies and the interplay across domains (cf. also Figure 3).

By jointly simulating the intra- and inter-domain levels, the simulation framework envisaged in ODYSSEUS can provide a holistic understanding of the impact of potential threats across multiple interrelated networks. Hence, this approach allows to characterize these interrelations between the individual domains in a structured, systematic and empirically underpinned way.

4. Applications and Limitations

4.1 Application Fields

Due to the constantly growing dependencies and interconnections among the CIs located within a large city, the complexity of those networks can hardly be grasped anymore. Therefore, it has become more and more important to understand the potential cascading effects an incident might have on specific infrastructures but also the social life within a city. The main application of the simulation model presented here lies in this context with the aim to support regional risk analyses carried out by different bodies. This can be achieved by using the cross-domain simulation approach as part of the impact assessment during the the classical risk management process. Besides the results coming from

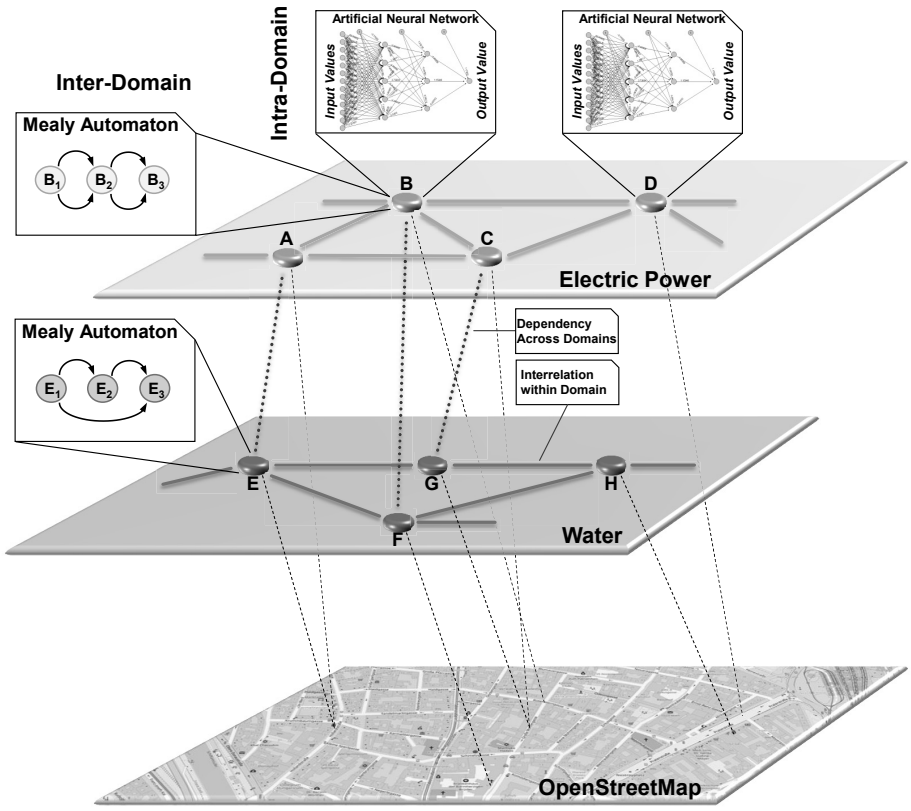

Figure 3. Illustration of the combination of the intra- and inter-domain model with information from a publicly available GIS-based platform (e.g., OpenStreetMap).

the analysis of the risks for an individual CI network, the simulation approach will provide a more general and holistic view. This will allow risk managers within the CI operators as well as on a higher administrative or political level to make better estimations on the potential consequences of an incident. This information will further facilitate a more comprehensive risk analysis and support decision makers on multiple levels. Especially against the background of the recently established "Network and Information System Security Act" in Austria such a cross-domain risk analysis is a central enabler for the protection of these critical supply infrastructures. Accordingly, we envision three potential users groups:

- *Infrastructure operators* running the various supply networks within a city would benefit from a simulation model as proposed here,

since it would provide much more accurate assessment of the consequences of an incident within their own network. Furthermore, by considering cascading effects on other networks, existing risk analyses can be complemented and refined with additional information.

- *Central administrative bodies* responsible for risk and disaster control within a city would benefit greatly from a holistic overview on the various supply networks within the city. A comprehensive simulation of the entire network will enable such institutions to better assess the complex effects of an incident on the individual infrastructures as well as on the population and thus to plan preventive measures more effectively.
- *National authorities* responsible for the protection of critical infrastructures would also gain an improved insight to the analysis of difficult to assess events, especially intentional hazards and attacks on soft targets, through such a holistic simulation model. This would allow the identification of potential cascading effects at multiple levels and support the planning of preventive measures and emergency response plans to mitigate the effects.

4.2 Limitations

The core limitation of the presented approach is the availability and handling of the required data, as already mentioned in the previous Section 1.3. This manifests itself in threefold way; firstly, the information about the individual network infrastructures. Whereas some of those are rather easy to acquire (e.g., the road and rail network), some others (e.g., power or telecommunication networks) are more difficult to get, in particular, when it comes to the "last mile", i.e., information about the final connection to the consumer. This is highly sensitive data that infrastructure operators won't (and shouldn't) be giving out easily. Secondly, with regards to the intra-domain simulation, the machine learning approach requires a large amount of training data to produce a sufficient model of one component in the respective network. For the same reasons as just mentioned above, it might be difficult to obtain this data from infrastructure operators. This, however, is where *domain-specific simulation models* may become an unlimited source of data to train our ANNs. Thirdly, with regards to the inter-domain simulation, a lot of knowledge about the interrelations between networks is necessary to instantiate the model. Whereas this information, to some degree, might not be too sensitive, it can be difficult to obtain since a lot of it might be implicit knowledge.

In our project, we plan on tackling all three parts mentioned above. On the one hand, we will strongly rely on openly available data on infrastructure networks, e.g., from OpenStreetMap, OpenInfrastructureMap or others (cf. the bottom domain in Figure 3). These maps provide a good overview on existing infrastructure networks down to a certain level of detail, which should be sufficient building a simulation model for each network. On the other hand, we will heavily involve experts from the infrastructure operators to obtain first-hand data and information upon the networks. In particular, we will be developing the information on dependencies and relations between infrastructure networks in interdisciplinary workshops with the operators' experts. This will allow us to obtain sufficient information on the interdependencies and also extract implicit knowledge from the experts. With regards to the machine learning approach, we will also investigate the option that the ANN can be trained by the operators themselves within their security domain. In this way, neither interfaces to the systems of the network operators nor the exchange of sensitive information will be necessary.

Another critical limitation to the presented approach is the already mentioned complexity of the CI systems and networks within a city. Each individual network consists of numerous physical and cyber assets as well as multiple kinds of connections (e.g., cables, pipe etc.) between them. Hence, it is not only almost infeasible to model every detail of each network but it is also inefficient. At a certain point, the amount of work required to make the model more detailed and precise does not correspond to the increase of insights gained by this effort. In our project, we will take up this challenge by introducing a specific level of abstraction. We will only model the individual CI networks down to this level of abstraction and not go into further detail. This will allow us to keep the modelling process feasible without losing too much information and insight about the operation and behavior of the network. For choosing this level of abstraction, we will have in-depth discussions with the CI operators to identify the right point below which the overall model does not provide a significant increase of information about the system.

5. Conclusion

In this article, we presented a conceptual approach towards a holistic simulation model combining multiple critical infrastructure networks within a large city that is going to be developed in the Austrian funded research project ODYSSEUS. Our approach mainly builds upon a two-level structure, an intra-domain level and an inter-domain level. On the

intra-domain level, the individual infrastructure network is simulated either based upon the underlying physical model of the respective domain or using a machine learning approach, where individual components of a network are represented by a neural network which is trained based on existing data. Further, the inter-domain level models the interdependencies among the networks and simulates cross-domain effects using a stochastic approach, where each component in a network is modeled as a Mealy automaton with probabilistic state transitions. Hence, this holistic simulation provides infrastructure operators with a concise overview on potential cascading effects, which can range from one domain to another. In this way, the simulation results can be used in a risk analysis of an entire city to inspect the effects of threats on the complex network of critical infrastructure networks.

Acknowledgement

The authors would like to thank Sandra König for invaluable feedback during her reviews. This work was supported by the research Project ODYSSEUS ("Simulation und Analyse kritischer Netzwerk-Infra- strukturen in Städten") funded by the Austrian Research Promotion Agency under Grant No. 873539.

Notes

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

2. We leave the more general concept of hyperedges (and resulting hypergraphs) that connect three or more entities aside in this work.

References

[1] R. Bloomfield, P. Popov, K. Salako, V. Stankovic and D. Wright, Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment, *Reliability Engineering and System Safety*, vol. 167, pp. 198–217, 2017.

[2] M. Chaudhary, S. Mishra and A. Kumar, Estimation of water pollution and probability of health risk due to imbalanced nutrients in River Ganga, India, *International Journal of River Basin Management*, vol. 15(1), pp. 53–60, 2017.

[3] F. Dietrich and C. List, Probabilistic opinion pooling generalized. Part one: general agendas, *Social Choice and Welfare*, vol. 48, pp. 747–786, 2017.

[4] European Commission, 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, *Official Journal of the European Union*, Brussels, Belgium, 2016.

[5] European Commission, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, *Official Journal of the European Union*, Brussels, Belgium, 2008.

[6] T. Grafenauer, S. König, S. Rass and S. Schauer, A simulation tool for cascading effects in interdependent critical infrastructures, *Proceedings of the Thirteenth International Conference on Availability, Reliability and Security*, 2018.

[7] S. Grundel, N. Hornung, B. Klaassen, P. Benner and T. Clees, Computing surrogates for gas network simulation using model order reduction, in *Surrogate-Based Modeling and Optimization*, S. Koziel and L. Leifsson (Eds.), Springer, New York, New York, USA, pp. 189–212, 2013.

[8] Y. Haimes, J. Santos, K. Crowther, M. Henry, C. Lian and Z. Yan, risk analysis in interdependent infrastructures, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 297–310, 2007.

[9] Y. Haimes, Hierarchical holographic modeling, *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 11(9), pp. 606–617, 1981.

[10] Y. Haimes and P. Jiang, Leontief-based model of risk in complex interconnected infrastructures, *Journal of Infrastructure Systems*, vol. 7(1), 2001.

[11] B. Haut, G. Bastin and Y. Chitour, A macroscopic traffic model for road networks with a representation of the capacity drop phenomenon at the junctions, *IFAC Proceedings Volumes* vol. 38(1), pp. 114–119, 2005.

[12] M. Herty, *Mathematics of traffic flow networks: Modeling, simulation and optimization*, Logos Verlag, Berlin, Germany, 2004.

[13] A. Kelic, D. Warren and L. Phillips, Cyber and Physical Infrastructure Interdependencies, SAND2008-6192, Sandia National Laboratories, Albuquerque, New Mexico, 2008.

[14] B. Kelley, P. Top, S. Smith, C. Woodward and L. Min, A federated simulation toolkit for electric power grid and communication network co-simulation, *Proceedings of the Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, 2015.

[15] E. Kenah and J. Robins, Second look at spread of epidemics on networks, *Physical Review E*, Vol. 76(3), 2007.

[16] S. König, A. Gouglidis, B. Green and A. Solar, Assessing the impact of malware attacks in utility networks, in *Game Theory for Security and Risk Management*, S. Rass and S. Schauer (Eds.), Birkhäuser, Cham, Switzerland, pp. 335–351, 2018.

[17] S. König and S. Rass, Stochastic dependencies between critical infrastructures, *Proceedings of the Eleventh International Conference on Emerging Security Information, Systems and Technologies*, pp. 106–110, 2017.

[18] S. König and S. Rass, Investigating stochastic dependencies between critical infrastructures, *International Journal on Advances in Systems and Measurements*, vol. 11(3-4), pp. 250–258 2018.

[19] S. König, S. Rass, B. Rainer and S. Schauer, Hybrid dependencies between cyber and physical systems, in *Intelligent Computing*, K. Arai, R. Bhatia and S. Kapoor (Eds.), Springer, Cham, Switzerland, pp. 550–565, 2019.

[20] S. König, S. Schauer and S. Rass, A stochastic framework for prediction of malware spreading in heterogeneous networks, in *Secure IT Systems*, B. Brumley and J. Röning (Eds.), Springer, Cham, Switzerland, pp. 67–81, 2016.

[21] P. Kotzanikolaou, M. Theoharidou and D. Gritzalis, Interdependencies between critical infrastructures: Analyzing the risk of cascading effects, in *Critical Information Infrastructure Security*, S. Bologna, B. Hämmerli, D. Gritzalis and S. Wolthusen (Eds.), Springer, Berlin Heidelberg, Germany, pp. 104–115, 2013.

[22] H. Krieg, D. Nowak and M. Bortz, Surrogate models for the simulation of complex water supply networks, *Proceedings of First International WDSA / CCWI Joint Conference Joint Conference*, 2018.

[23] H. Lin, S. Sambamoorthy, S. Shukla, J. Thorp and L. Mili, Power system and communication network co-simulation for smart grid applications, *Proceedings of the IEEE PES Conference on Innovative Smart Grid Technologies*, 2011.

[24] D. Paluszczyszyn, Advanced modelling and simulation of water distribution systems with discontinuous control elements, Ph.D. Thesis, School of Engineering and Sustainable Development, De Montfort University, Leicester, UK, 2015.

[25] Y. Qiu, S. Grundel, M. Stoll and P. Benner, Efficient numerical methods for gas network modeling and simulation, arXiv:1807.07142 (`arxiv.org/abs/1807.07142`), 2018

[26] M. Rahnamay-Naeini and M. Hayat, Cascading failures in interdependent infrastructures: An interdependent Markov-Chain approach, *IEEE Transactions on Smart Grid*, vol. 7(4), pp. 1997–2006, 2016.

[27] M. Reiser, A queueing network analysis of computer communication networks with window flow control, *IEEE Transactions on Communications*, vol. 27(8), pp. 1199–1209, 1979.

[28] S. Rinaldi, Modeling and simulating critical infrastructures and their interdependencies, *Proceedings of the Thirty-Seventh Annual Hawaii International Conference on System Sciences*, 2004.

[29] S. Rinaldi, J.P. Peerenboom and T.K. Kelly, Identifying, understanding, and analyzing critical infrastructure interdependencies, *IEEE Control Systems Magazine*, vol. 21(6), pp. 11–25, 2001.

[30] M. Salathé and J. Jones, Dynamics and control of diseases in networks with community structure, *PLOS Computational Biology*, vol. 6(4), 2010.

[31] T. Schaberreiter, K. Kittilä, K. Halunen, J. Röning and D. Khadraoui, Risk assessment in critical infrastructure security modelling based on dependency analysis, in *Critical Information Infrastructure Security*, S. Bologna, B. Hämmerli, D. Gritzalis and S. Wolthusen (Eds.), Springer, Berlin, Germany, pp. 213–217, 2013.

[32] F. Schloegl, S. Rohjans, S. Lehnhoff, J. Velasquez, C. Steinbrink and P. Palensky, Towards a classification scheme for co-simulation approaches in energy systems, *Proceedings of the IEEE International Symposium on Smart Electric Distribution System and Technologies*, pp. 516–521, 2015.

[33] M. Sunela and R. Puust, Real time water supply system hydraulic and quality modeling – A case study, *Procedia Engineering*, vol. 119, pp. 744–752, 2015.

[34] M. Turoff, V. Bañuls, L. Plotnick, S. Hiltz and M. Ramírez de la Huerga, A collaborative dynamic scenario model for the interaction of critical infrastructures, *Futures*, vol. 84, pp. 23–42, 2016.

[35] J. Wachter, T. Grafenauer and S. Rass, Visual risk specification and aggregation, *Proceedings of the Eleventh International Conference on Emerging Security Information, Systems and Technologies*, pp. 93–98, 2017.

[36] T. Wen, X. Lyu, D. Kirkwood, L. Chen, C. Constantinou and C. Roberts, *Proceedings of the IEEE Eighteenth International Conference on Intelligent Transportation Systems*, pp. 2665–2670, 2015.

[37] Z. Yan, Y. Haimes and M. Wallner, Hierarchical coordinated Bayesian model for risk analysis with sparse data, presented at the *Society of Risk Analysis Annual Meeting*, 2006.

[38] N. Yuhara and J. Tajima, Multi-driver agent-based traffic simulation systems for evaluating the effects of advanced driver assistance systems on road traffic accidents, *Cognition, Technology and Work*, vol. 8(4), pp. 283–300, 2006.