# Security of Electricity Supply in 2030

Wolfgang Raskob, Valentin Bertsch, Manuel Ruppert, Misha Strittmatter,
Lucia Happe, Brandon Broadnax, Stefan Wandler, Evgenia Deines
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
wolfgang.raskob@kit.edu

***Abstract*—The stability and well-operation of a future electricity grid which includes numerous components of smart grid technology is becoming much more dependent on the correct operation of the supporting IT, and in this respect may become more attractive to malicious attacks. To understand the vulnerabilities, interdependencies between the electrical distribution grid and IT components as well as critical infrastructures such as water supply and health care will be simulated and evaluated. Aim of the research activity is to develop a holistic analysis framework to quantify and evaluate requirements and design decisions of the many players in such complex infrastructures. Planning methods and tools will be introduced that provide guidance at the design-time of smart grid infrastructures, allowing for a high level of security even under unfavorable conditions.**

**This paper presents the framework focusing on the methods envisaged and an application scenario dealing with potential threats to and impact of a large-scale and longer-lasting power outage.**

## Disclaimer

This paper was accepted and presented at the Critical Infrastructure Protection and Resilience Europe (CIPRE) conference in March 2015. It was never officially published by the organizers.

## I. Introduction

Critical Infrastructures (CIs) are facilities and organizations, which ensure essential services and goods. A disruption of a CI may have severe impacts for society, economy, and industry. Critical Infrastructure Protection (CIP) covers all activities that ensure a continued supply of vital services and products for the population. This includes all coping measures to mitigate and to minimize the consequences of CI disruptions before and during disasters as well as to recover from the effects back to satisfying living conditions.

Most critical are disruptions in information technology (e.g. STUXNET [Geekheim, 2010]) and power blackouts (e.g. Münsterland 2005 [Menski and Gardemann, 2008], USA 2012 [Mühr et al., 2012]) as they can easily affect further critical infrastructures.

In 2012, the German Helmholtz research organization initiated a research line on security. Three large Helmholtz centers, the German aeronautics and space research centre (DLR), the Research Center Jülich (FZJ) and the Karlsruhe Institute of Technology (KIT), formed a consortium, combining their vast knowledge in cyber security, sensors and platforms, emergency management and security of critical infrastructures in one project. The central activity so far focuses on CI. In particular, the project aims at establishing a platform that serves as focal point related to CIP activities for CI owners, operators, local emergency management organizations and research. To demonstrate the developed methodologies, a common scenario was defined that allows combining the experience of the three research centers and demonstrating the benefit of the simulation approaches selected. This scenario focuses on a malicious attack on the ICT components of a future power grid in 2030, investigating the consequences and possible measures to mitigate or prevent a longer lasting power blackout.

This paper is organized as follows. First the methodological approaches applied will be presented, followed by a used case. In further sections, preliminary results of the use case will be discussed and first conclusions as well as future research activities will be highlighted.

## II. Model Description

As described above, modern societies increasingly depend on critical infrastructures (CIs), which are characterised by an increasing interdependency between the different CI sectors as well as between CIs and further socioeconomic systems [Wang et al., 2012], [Rinaldi et al., 2001]. The evolution of CIs and their interconnectedness imply that understanding and predicting the consequences of disruptions has become extremely difficult. The impact of any triggering event causing CI disruptions has two components. The direct impact on the CI itself, and the indirect impacts that propagate through the network. To understand the importance of CIs and the far-reaching consequences of their failure, modelling individual CIs is not sufficient any longer [Comes et al., 2013]. Thus, the need arises for integrated approaches.

Focusing on the CI sectors energy supply, ICT, health care and water supply, the developed integrated approach includes a critical infrastructure model (for health care and water supply), a power flow optimization model, an ICT grid model as well as an ICT security assessment model (see Figure 1). The ultimate target of our approach is the provision of decision support for designing resilient CIs. As a major input to reach this target, the focus in this paper is the analysis of consequences of CI disruptions (focus on electricity outages through malicious attacks) as a basis for evaluating measures to increase the CI's resilience.

Figure 1 illustrates the connections and interfaces between the individual submodels. Based on cost functions for lost electrical load (provided by the critical infrastructure model,

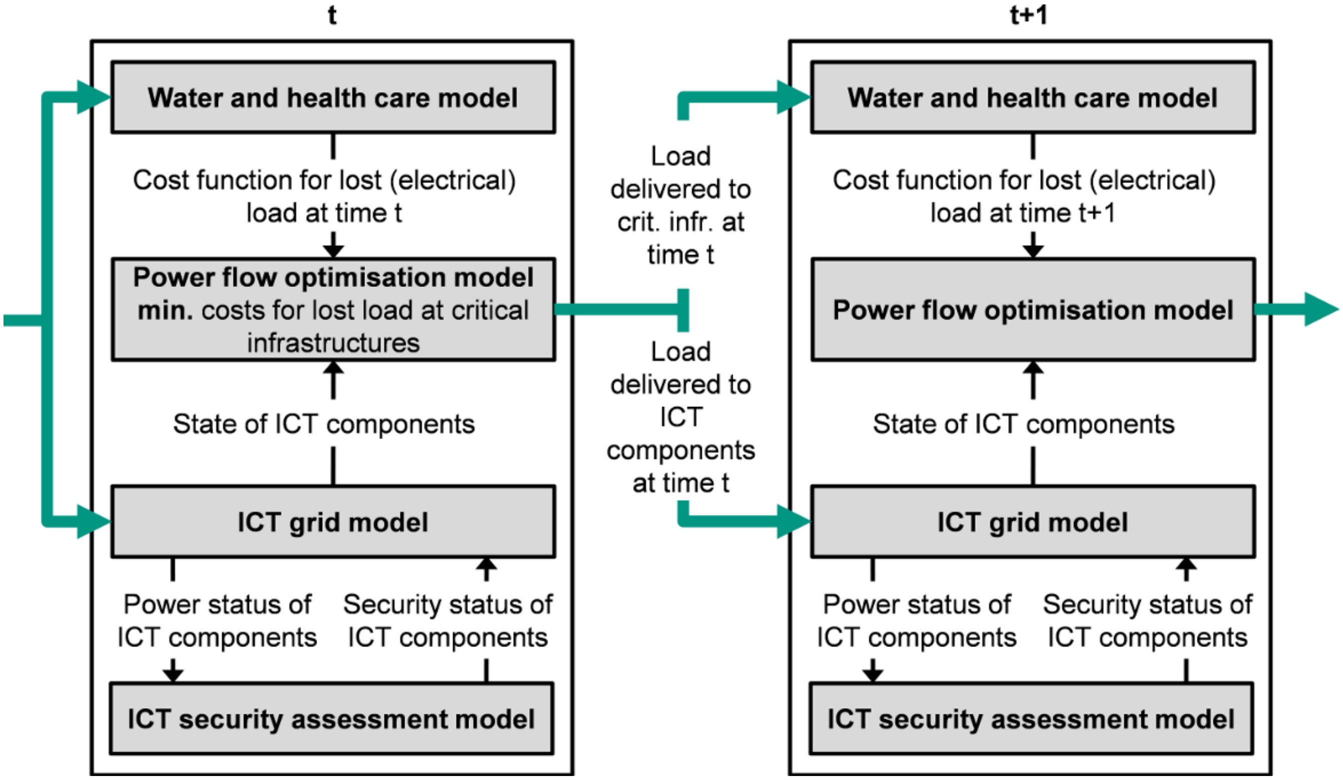
t
t+1
Water and health care model
Cost function for lost (electrical) load at time t
Power flow optimisation model min. costs for lost load at critical infrastructures
State of ICT components
ICT grid model
Power status of ICT components
Security status of ICT components
ICT security assessment model
Load delivered to crit. infr. at time t
Load delivered to ICT components at time t
Water and health care model
Cost function for lost (electrical) load at time t+1
Power flow optimisation model
State of ICT components
ICT grid model
Power status of ICT components
Security status of ICT components
ICT security assessment model

Fig. 1. Model Interaction

see Section II-A) and a static evaluation of the ICT grid (see Section II-B), the power flow optimization model conducts a static optimization of the power grid in each time step (see Section II-C). As an important input for the evaluation of the ICT grid, the ICT security assessment model provides an analysis of the security objectives depending on the power status of the individual ICT components. The dynamic characteristics of CIs over time are mainly reflected by changing cost functions for increasing outage or shortage durations.

### A. *Critical Infrastructure Modelling: Example with Water and Health Care*

To describe complex interdependencies of CIs, different simulation approaches exist and one of them is the multi agent based approach. It allows to introduce distributed problem solving and considers trade-offs between the interests of all parties involved (e.g. [Shoham and Leyton-Brown, 2008]). All parties of interest, e.g. various critical infrastructures, population, crisis management organizations, resources can be represented by one or more individual agents. Any agent interacts with others and the relevant environment. This interaction is based on a set of rules, which represent the interaction in reality. In this way, CI components are represented by individual agents which can interact with each other and also negotiate about resources needed. However, the CI model contains, besides the simulation part, also a data model. The data model contains the properties and attributes of the CIs and describes the relations between them. The Simulation tool comprises the behaviors and the decisions of CIs' elements. As we decided to use the agent based modelling (ABM), the next step was to select a suitable simulation environment. There exist several simulation frameworks that can be used to set up agent based simulations. For example NetLogo [Tisue and Wilensky, 2004], Power TAC [Ketter et al., 2013], AnyLogic [Borshchev and Filippov, 2004] and REPAST [Collier et al., 2003] are representatives of commonly used simulation environments. In this project the REPAST platform is used as it is open source, has a strong user community and can be easily combined with GIS systems and other external tools. As a starting point, agents are defined for the health care system (e.g. hospitals, elderly care and pharmacies) and water supply. In a second step, households, emergency management organizations with their crisis teams and first responders will be also set up. Key parameters representing a CI are the resources needed for operation and this defines to some extent the decencies and the self-help capabilities of each individual CI realization. Furthermore, the power and water consumption of hospitals have been analyzed and the appropriated functions derived. They will be recalculated at each iteration step during the simulation. In order to consider the practical applicability of our approach, agents are equipped with real data. The data search refers preliminary to health care facilities, water supply facilities and households. Of interest are characteristics of these facilities for example in the area of hospitals the number of beds, operation theatres, patients or water consumption, etc. It also includes coping capacities such as the number and performance of emergency generators or food stocks. Furthermore it is important to collect all relevant measures for these agents, which they can use to mitigate consequences of the blackout. To estimate the resilience in case of a longer lasting power blackout, the emergency power supply capacity is important. For hospitals this is typically 24 hours in Germany. This duration may differ for other CIs. To allow the agents negotiating about the energy needed, a cost function is under development which comprises all relevant attributes such as the energy consumption, importance for the society, importance for other CIs and others. The cost function is of exponential nature with a gentle slope as long as self-help capabilities exist and with a steep slope when the functionality is no longer guaranteed. This allows negotiating how to distribute remaining resources between all parties involved, including the normal household.

### *B. ICT Grid Model*

The resilience of the future power grids ICT (information and communications technology) infrastructure is an emerging field of research. Some related work deals with the assessment of the interplay between the IT and physical aspects. In 2010 Kundur et al. present an approach which expresses the IT and electrical aspects as two graphs which are interconnected [Kundur et al., 2010]. However, their approach is very detailed and targets at modelling the internals systems, while our approach aims at expressing the topologies of whole cities. In 2014, Menasch et al. present an approach, which aims to predict the impact of natural disasters and assess the effect of countermeasures like undergrounding of power lines or tree pruning [Menasché et al., 2014]. However, IT and communication is not in the focus of their approach. Thus, cyber-security is not covered. In 2011, Lin et al. coupled a power system dynamics simulation with an event-based network communication simulation. However, their approach focusses on detailed communications and does not explicitly consider cyber-threads [Lin et al., 2011]. The ICT grid model assesses the consequences such threats can have on the ICT infrastructure of the future power grid. As input, this analysis gets data specifying the topology of the ICT infrastructure, as well as a scenario specification. Within the scenario specification, it is defined which points are still supplied by power as well as which elements are corrupted or damaged. The scenario specification either can be created manually or is computed by the power flow model and an (cyber) attacker simulation. As output, the ICT grid model determines which systems are still able to perform demand side management and which elements are still able to communicate with each other. This output can in turn be used as input for the power flow model and attacker simulations. The intended use of the ICT grid model is within the design time of the power grid's ICT infrastructure. The goal is to fulfil the engineering mantra: assess the properties of a system early, as well as identify critical points in the system and fix problems as soon as possible. The topology of the power grid's ICT infrastructure is captured within a graph. The vertices of the graph represent either IT components (e.g., smart meters, controllers within small power plants, SCADA servers) or network nodes (e.g., routers, switches, multiplexers). There are two kinds of edges. Edges that represent physical communication connections as well as optional edges that restrict logical communication. Further, the vertices can be connected to multiple power supply spots. These power supply spots are the incoming interface from the power flow model. Based on the input scenario, which specifies which power supply spots can be powered as well as which nodes are defect, clusters of IT components are determined which are still physically connected. If the logical communication is constrained, the logical clusters are identified within the physical clusters. The determination of clusters is done using a modified version of Tarjan's algorithm [Tarjan, 1972]. Depending on the communication paradigm which should be investigated and if there is a supervisory component within the cluster, the smart meters can exert demand side management of differing effectiveness. This information serves in turn as input for the power flow model. Within the ICT grid model, varying types of cyber-attacks can be simulated. These may or may not be restricted by information from the ICT security model. As input, these attacker simulations get information specifying the communication clusters from the ICT grid model. The attacker simulation tracks information of the corruption states of the IT components in the ICT infrastructure. This information can be used by the power flow model to determine the grids remaining demand side management capabilities, as well as margins of malevolent manipulations. E.g., a bot net of controllers simultaneously turning consumption or production to a maximum. Examples of attacker simulations are virus propagation and local hacker. Both are specified by a spread rate. In each time step, each node corrupted by a virus can corrupt as many new as specified by the spread rate. Viruses can still spread within their communication cluster, even if they are severed from their source by the outage of a communication line. A hacker on the other hand has a fixed point of access within the ICT infrastructure. Per time step, he is able to corrupt node within his reach in the amount of the spread rate. If corrupted nodes are severed from the hacker by communication outages, he loses control over these nodes.

### *C. Power Flow Optimization Model*

Prospectively, the introduction of smart grid techniques in electrical grids will increase control possibilities for system operators on the one hand, but also lead to a significant increase of complexity in the lower voltage levels. In order to incorporate power supply into the combined approach and to simulate interdependencies of the electrical grid at the distribution grid level and other CIs, a nonlinear model for the alternate current Optimal Power Flow (OPF) problem using IPOPT [Wächter and Biegler, 2006] is formulated as described in [Torres and Quintana, 1998]. OPF models are widely used in electrical engineering with a widely diversified field of applications [Momoh et al., 1999]. The generalised formulation of the OPF approach is shown in Equation 1.

$$\begin{aligned} min\ f(x), s.t. \\ G(x) = 0 \\ H(x) \leq 0 \\ x_{min} \leq x \leq x_{max} \end{aligned} \qquad (1)$$

The equality constraints of the problem are given by the power balance equations on every node of the system whereas the inequality equations are given set by voltage limits and maximum current flows on transmission lines and cables. During each timestep t, information from the CI model and the ICT grid model are used for the generation of the electricity network state. Whereas most OPF models focus on minimization of generation cost in a system without malfunctions, in this approach the optimal supply of critical infrastructures requires a goal function which minimizes cost of load shedding. In order to optimise utilisation of the system consisting of the i CIs simulated by the approach described in the above subsection, the target function of the problem is formulated as the minimisation of occurring cost for lost load $P_{i,t}$ at every CI (see Equation 2).

$$min \sum_{i \in CI} c_{i,t} * P_{i,t} \qquad (2)$$

## III. Use Case

### A. Scenario Description

In the considered scenario, we assume a future based on the German Renewable Energy Act (German: Erneuerbare-Energien-Gesetz, EEG), according to which the share of electricity generation from renewable energy sources (RES) in the overall generation shall amount to 50% until the year 2030. The expansion of RES is accompanied by a decentralization of the energy system. In order to efficiently maintain today's security of supply in the course of the expansion of fluctuating RES, we assume that the power grid is not only restructured and strengthened by conventional grid technologies but also by smart grid technologies providing the basis for an energy information and control network with distributed system intelligence. As consumers also become producers, a decentralized way of control is needed. Through smart meters (that have the ability to regulate producing or consuming devices) or similar controllers, demand side management is enabled. When assessing the stability of the power supply of the CIs, the ICT is an important aspect. In our future scenario, ICT becomes ubiquitous within the power grid [Beckert et al., 2011]. But not only the energy system, also other (critical) infrastructures are assumed to heavily depend on ICT. In particular, software will control essential components of the physical infrastructures as well as the communication between these and their maintenance. Since modern societies depend on the functioning performance of the physical infrastructures and the services provided through these, a safe and secure operation of the ICT system becomes more and more vital while, at the same time, the risk exposure, e.g. to malicious attacks, increases with the rising ICT penetration.

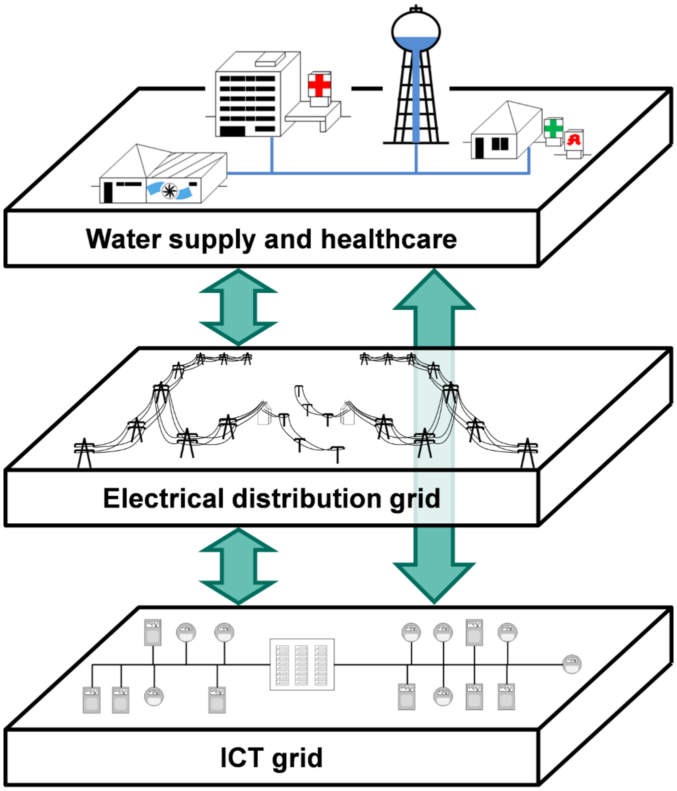

Fig. 2. Scenario Levels

In order to provide a platform on which to demonstrate the developed methodology within the scenario described above, we construct a hypothetical city with its own topography, urbanisation, critical infrastructures and economy. We chose to use a hypothetical region so that there are no security or data access issues. We shall ensure that natural hazards, such as earthquakes, floods or windstorms on a broad range of intensity levels, duration, and spatial extent, are plausible within the region and that it reflects the characteristics of a real site in Germany. However, the major risk we focus on within the use case in this paper is that of a malicious attack to the ICT components within the decentralised energy system (e.g. smart meters and controllers). The major question in the considered use case is whether the malicious attack infects the ICT components and under which circumstances such infections my lead to a power outage. Besides this consequence analysis itself, our goal is the evaluation of different measures to prevent a power outage. The city's simulated levels of data acquisition are shown in Figure 2. The simulated area includes approximately 180,000 households with about 300,000 inhabitants, connected to the low voltage electricity grid, and about 2,000 transformer substations connecting the low voltage grids to the medium voltage level. For the healthcare and water supply CI, 138 relevant elements have been identified and data have been collected. This comprises mainly the size, the number of patients, number of surgeries, power consumption, self-help capabilities and production capacities (for water works).

### B. Selected Results

So far the simulation models described above are under development and interfaces are defined but not realized. In this respect, no results of coupled simulation are available at the time of writing this paper. However, first assessments can be reported.

Having set up the 138 elements of the two CI structures healthcare and water supply, we have performed simulations for selected power blackout scenarios. Figure 3 shows the time dependent status of seven main hospitals assuming a power blackout for 24 hours. This demonstrated on the one hand site that a collapse of the CI is not immediate and allows to identify those elements which requires support in the first hours. The low number of hospitals on EPU (emergency power generators) is the result of the assumption that diesel is available only for some hours and that due to the power blackout no further diesel can be obtained gasoline stations do not have an EPU. These simulations are valuable for planning purposes, on the basis of which the emergency management organizations can set up contingency plans for the most important power blackout scenarios.

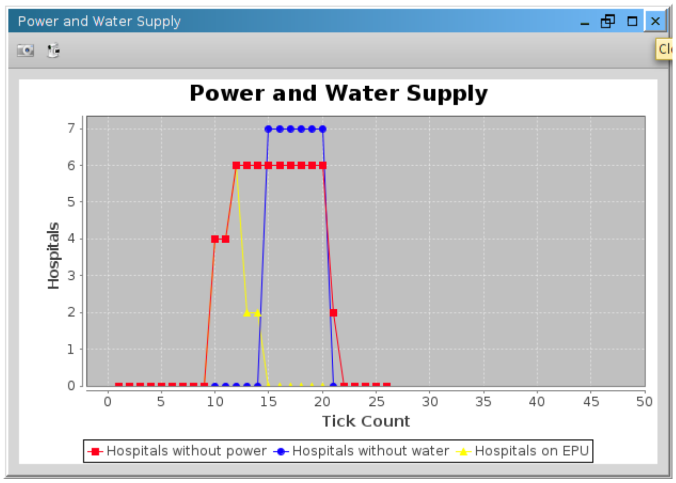

Fig. 3. Time dependent status of hospitals (EPU = emergency power generators), red means the number of hospitals without power, blue without water and yellow number of hospitals where the emergency power is on

To simulate potential countermeasures a first version of a cost function has been defined. Figure 4 shows an example for one CI element. Depending on the nature of the CI and its associated parameters defined in Section II-A, the cost function will vary. This allows the power gird module to set priorities in providing energy if still available to those CIs with the highest cost functions.

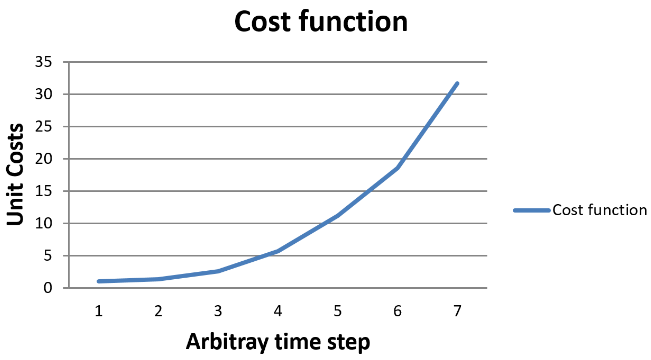

Fig. 4. Example cost function for one selected hospital with self-help capabilities for the first two time steps

## IV. Conclusions and Outlook

Individual simulation models and approaches for critical infrastructures, ICT and power flow have been developed and customized to the simulated city. Data collection for the simulation models is critical and partly difficult to realize. However, dealing with the power grid of 2030 allows for some flexibility in defining particular parameters. This also allows performing parameter variations in the simulation to identify components or approaches which are not at all suitable in such a future grid. The next step will be the coupling of the individual simulation models as indicated in Figure 1. For this purpose, the time-dependent cost function resulting from the water and health care model will be connected to the grid and ICT model. The integrated simulation approach will allow an estimation of the optimized electricity supply of these critical infrastructures in case of emergency situations. Interfaces between the modelling approaches, which connect the system's components based on geographical areas of electricity grid substations, have been defined and realization has started. In a second step, sensible countermeasures have to be defined which will become part of the simulation models. For the CI, a workshop has been conducted in 2014 with emergency managers of local communities from southern Germany. As a result, 12 management options were defined for water supply, ranging from the use of additional power generators up to use of tanks and construction of new pipelines. For hospitals, only 8 measures were identified including the use of mobile surgery components from outside up to a complete evacuation of all patients. To decide between such measures, specific agents will be developed and equipped with additional negotiation facilities such as Multi Criteria Decision Making (e.g. [Belton and Stewart, 2002]) or knowledge data bases with case based reasoning approaches to learn from historic events (e.g. [Aamodt and Plaza, 1994]). This will allow testing attack scenarios with potential countermeasures to define those which can be applied by the emergency management organizations under the constraint of cost, manpower and resources.

## Acknowledgment

This work was funded by the Helmholtz Association of German Research Centers.

## References

[Aamodt and Plaza, 1994] Aamodt, A. and Plaza, E. (1994). Case-based reasoning: Foundational issues, methodological variations, and system approaches. *AI communications*, 7(1):39–59.

[Beckert et al., 2011] Beckert, B., Hofheinz, D., Müller-Quade, J., Pretschner, A., and Snelting, G. (2011). Software security in virtualized infrastructures – the smart meter example. *it-Information Technology Methoden und innovative Anwendungen der Informatik und Informationstechnik*, 53(3):142–150.

[Belton and Stewart, 2002] Belton, V. and Stewart, T. (2002). *Multiple criteria decision analysis: an integrated approach*. Springer Science & Business Media.

[Borshchev and Filippov, 2004] Borshchev, A. and Filippov, A. (2004). From system dynamics and discrete event to practical agent based modeling: reasons, techniques, tools. In *Proceedings of the 22nd international conference of the system dynamics society*, volume 22. Citeseer.

[Collier et al., 2003] Collier, N., Howe, T., and North, M. (2003). Onward and upward: The transition to repast 2.0. In *Proc. First Annual North American Association for Computational Social and Organizational Science Conference*.

[Comes et al., 2013] Comes, T., Bertsch, V., and French, S. (2013). Designing dynamic stress tests for improved critical infrastructure resilience. In *Proceedings of the 10th international ISCRAM conference, Baden-Baden*.

[Geekheim, 2010] Geekheim (2010). Stuxnet: targeting the iranian enrichment centrifuges in natanz? http://frank.geekheim.de/?p=1189. Accessed: 12.01.2015.

[Ketter et al., 2013] Ketter, W., Collins, J., and Reddy, P. (2013). Power tac: A competitive economic simulation of the smart grid. *Energy Economics*, 39:262–270.

[Kundur et al., 2010] Kundur, D., Feng, X., Liu, S., Zourntos, T., and Butler-Purry, K. L. (2010). Towards a framework for cyber attack impact analysis of the electric smart grid. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 244–249. IEEE.

[Lin et al., 2011] Lin, H., Sambamoorthy, S., Shukla, S., Thorp, J., and Mili, L. (2011). Power system and communication network co-simulation for smart grid applications. In *Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES*, pages 1–6. IEEE.

[Menasché et al., 2014] Menasché, D. S., Avritzer, A., Suresh, S., Leo, R. M., de Souza e Silva, E., Diniz, M., Trivedi, K., Happe, L., and Koziolek, A. (2014). Assessing survivability of smart grid distribution network designs accounting for multiple failures. *Concurrency and Computation: Practice and Experience*, 26(12):1949–1974.

[Menski and Gardemann, 2008] Menski, U. and Gardemann, J. (2008). Auswirkungen des Ausfalls Kritischer Infrastrukturen auf den Ernährungssektor am Beispiel des Stromausfalls im Münsterland im Herbst 2005. *Empirische Untersuchung im Auftrag der Bundesanstalt für Landwirtschaft und Ernährung (BLE). Hrsg.: Fachhochschule Münster, Fachbereich Oecotrophologie, Kompetenzzentrum Humanitäre Hilfe*.

[Momoh et al., 1999] Momoh, J. A., El-Hawary, M., and Adapa, R. (1999). A review of selected optimal power flow literature to 1993. part i: Nonlinear and quadratic programming approaches. *IEEE transactions on power systems*, 14(1):96–104.

[Mühr et al., 2012] Mühr, B., Kunz, M., Khazai, B., Kunz-Plapp, T., Comes, T., Vannieuwenhuyse, M., Schröter, K., Elmer, F., Leyser, A., and Zschau, J. (2012). CEDIM FDA - report no. 1 on hurricane sandy. CEDIM Research Reports Series.

[Rinaldi et al., 2001] Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems, IEEE*, 21(6):11–25.

[Shoham and Leyton-Brown, 2008] Shoham, Y. and Leyton-Brown, K. (2008). *Multiagent systems: Algorithmic, game-theoretic, and logical foundations*. Cambridge University Press.

[Tarjan, 1972] Tarjan, R. (1972). Depth-first search and linear graph algorithms. *SIAM journal on computing*, 1(2):146–160.

[Tisue and Wilensky, 2004] Tisue, S. and Wilensky, U. (2004). Netlogo: A simple environment for modeling complexity. In *International conference on complex systems*, volume 21. Boston, MA.

[Torres and Quintana, 1998] Torres, G. L. and Quintana, V. H. (1998). An interior-point method for nonlinear optimal power flow using voltage rectangular coordinates. *Power Systems, IEEE Transactions on*, 13(4):1211–1218.

[Wächter and Biegler, 2006] Wächter, A. and Biegler, L. T. (2006). On the implementation of an interior-point filter line-search algorithm for large-scale nonlinear programming. *Mathematical programming*, 106(1):25–57.

[Wang et al., 2012] Wang, S., Hong, L., and Chen, X. (2012). Vulnerability analysis of interdependent infrastructure systems: a methodological framework. *Physica A: Statistical Mechanics and its applications*, 391(11):3323–3335.