Chapter 21
Smart Technologies as a Thread for Critical Infrastructures

Tobias Koch, Dietmar P. F. Möller and Andreas Deutschmann

21.1 Critical Infrastructures Within a Smart Environment

Critical infrastructures (CI) play an important role within our everyday life supplying us with resources such as electrical power, water, heating, communication and financial services, transportation, or even health care. They are named 'critical,' as a dysfunction of the infrastructure results in a large impairment of our society. Therefore, the US government (U.S. GAO 2004) as well as the European Union (EPC 2013) initiated programs treating the topic of critical infrastructure protection (CIP). Besides human failures (Bundesnetzagentur 2007) and environmental threats to CIs such as geomagnetic storms (Kappenman et al. 1997), earthquakes, tsunamis, floods, or storms (Urlainis et al. 2014), the digital control systems assisting with operational control make the CIs even more vulnerable to dysfunctions of the information and communication technology (ICT). In addition to the safety threats named beforehand, CIs are also target of third-party attacks due to the high impact on society in case of a successful attack. Though, in the past, terrorism has been the primary thread and still is threading CIs (Zoli et al. 2018), the continuing digitalization results in an increasing vulnerability toward cybercrime via, e.g., Supervisory Control and Data Acquisition (SCADA) Systems (Stamp et al. 2009). The consequences of successful cyberattacks are very diverse reaching from train signal (Hancock 2003) and traf-

T. Koch (✉) · A. Deutschmann
German Aerospace Center (DLR), Brunswick, Germany
e-mail: tobias.koch@dlr.de

A. Deutschmann
e-mail: andreas.deutschmann@dlr.de

D. P. F. Möller
Institute of Applied Stochastics and Operations Research, Clausthal University of Technology (TUC), Clausthal-Zellerfeld, Germany
e-mail: dietmar.moeller@tu-clausthal.de

K. B. Akhilesh and D. P. F. Möller (eds.), *Smart Technologies*,
https://doi.org/10.1007/978-981-13-7139-4_21

fic light manipulation (McMillan 2007) over hijacked water service control systems (Abrams and Weiss 2008) up to disrupting nuclear power plants (Kesler 2011).

The concept for tomorrow's smart cities (European Commission 2011) leads to an inevitable increase of interconnectedness within the infrastructures (Batty et al. 2012). Though there is no official definition of a 'smart city' by now, most approaches of planning a smart city contain the idea of smart grids and intelligent mobility. The term smart grid refers to an adaption of electricity production with respect to its consumer in a decentralized grid with short reaction times, which enables an efficient, environmental-friendly use of electricity without a high amount of losses. For this purpose, smart meters have to measure and regulate energy consumption and communicate with each other (Palensky and Dietrich 2011), leading to an increased exposure to cyberattacks not only within the CIs, but also within the smart homes of population (Anwar and Mahmood 2014; Möller and Vakilzadian 2014; Eckert and Kraüs 2011). The idea of intelligent mobility, i.e., the use of ICT systems, to optimize transfer, waiting and door-to-door times, leads to a further collection of sensitive data and increased interconnectedness.

For safety and security analysis, CIs have to be considered as cyber-physical systems (Möller 2016), due to the high number of interconnected embedded systems within modern CIs and its rising trend, as both the ICT systems and the physical systems are exposed to safety and security threats. Within the context of Industry 4.0 (Hermann et al. 2016), i.e., with periodic conditions and a low amount of unpredictable factors, data-driven approaches are used to detect uncommon or conspicuous system behavior (Niggemann et al. 2016). However, this approach is not possible if smart technologies interact with or depend on human behavior as it is, e.g., in the transport sector the case. Therefore, we propose here a classical, two-layered, process-oriented approach to model CIs as a cyber-physical system at the example of an airport structure (Koch et al. 2017, 2018).

21.2 Airports as a Cyber-Physical System

Airports are a junction point within our modern travel chain like metro or train stations, but even more complex due to their higher safety and security requirements. Furthermore, the importance of aviation within this travel chain will increase in the future (EUROCONTROL 2013). Incidents at airports have shown in the past that the consequences of these incidents have been unpredictable (Hope 2015; Macdonald and Bartunek 2016; Gurzu 2017). Thus, they are a perfect example to explain the process-coupling of our modeling approach. Figure 21.1 (top) shows a passengers' way through the departure area of the Suvarnabhumi International Airport in Bangkok starting at the escalators/elevators (blue), which connect the terminal to public transport, and ending at the boarding area (purple) waiting for the plane. On this path (orange dashed line in Fig. 21.1), the passenger has to check-in (brown) and/or drop his luggage and continue through the security checks (dark green) to the gate area. At all steps, either the passenger or the staff interact with electrical devices and ICT systems such as the elevator and its control unit, the

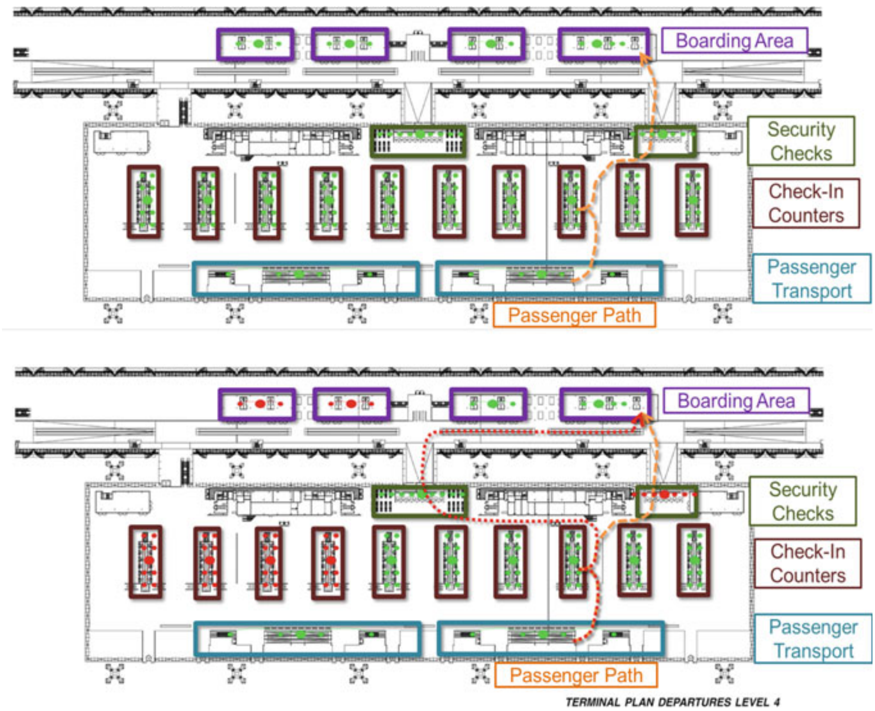

Fig. 21.1 Passenger trajectory through an airport terminal under full performance (left) and power shortage conditions (right). Green and red dots represent operating and non-operating objects within the CI. Rectangles represent groups of objects connected to a certain process

computers and luggage conveyor belts at the check-in counter, the body scanners and screening devices at the security checks and the boarding card scanners at the gate. Within Fig. 21.1, such electrical devices or ICT systems are depicted as dots with its color indicating its operating status, where green refers to on and red dots refer to off. Figure 21.1 (bottom) shows the same process steps under disturbed conditions, i.e., some of the devices are out of order. Possible scenarios causing these conditions could be power shortages or outage of some ICT systems. For the passenger, this results in a detour (red-dotted line) due to the outage of the next-by security checks. Moreover, the extended walking distance and a possible bottleneck effect to the increasing number of passengers per available security check result in a delayed arrival at the boarding area, which might lead to missing the flight.

This example shows the tight coupling between the airports infrastructure and the processes taking place including human behavior. Until the coupling between infrastructure and processes is not fully understood, data-driven approaches cannot be applied, as they would not be able to distinguish between normal and conspicuous states. Hence, a classical two-layered modeling approach is used to understand the coupling between the infrastructure and the ongoing processes. The term two-layered corresponds to two sets of properties corresponding to the electrical properties and the

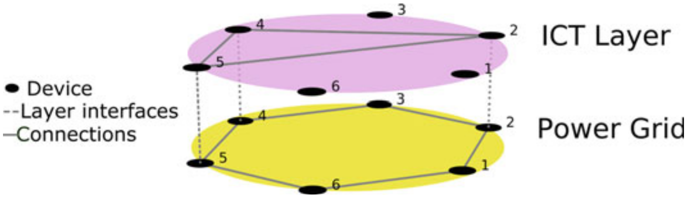

Fig. 21.2 Example of a two-layer network structure showing the devices (dots) and their interconnections (solid lines) within the ICT (light purple) and power grid layer (yellow). Device having properties on both layers build the layer interfaces (dashed lines)

ICT properties of a device. As the ICT network does not coincide with the electrical grid of the infrastructure, two layers of networks exist. In the smart, automated infrastructures, all devices rely on power supply, i.e., they are all connected to the power grid. Furthermore, some of these devices also need ICT systems and therefore build the interface of both networks. Figure 21.2 visualizes such a multilayer network at the example of six devices (dots) being interconnected (solid lines) by ICT (light purple) and the power grid (yellow). While all devices need power and therefore are connected via the power grid, only devices 2, 4, and 5 also use ICT and build the interfaces between the layers (dashed lines).

21.3 Two-Layered Simulation Model

Since the layers are only connected through the interface devices, the interaction between the devices within both layers can be analyzed separately. Thus, for a working simulation model three modules need to be developed, starting with a dynamic power-flow model for the power grid, continuing with an ICT network flow model and concluding with a logic combining the outcomes of both layers to a final result. As the overall goal is to understand the coupling between infrastructure and processes, the output of the simulation has to be the operability status of each device over time t_k, which can be used as resource management for process simulations such as passenger flow simulation for the airport terminal example depicted in Fig. 21.1.

21.3.1 Dynamic Power-Flow Model

Modern censoring and smart meters enable a continuous supply with information about the power demand at the devices, i.e., loads of the power grid and the state of our power supply. Each load i demands at each time t_k for a certain demand of electrical power $S_{\mathrm{d};i}(t_k)$ that is injected into the grid by a power source with the voltage $U_{\mathrm{supply}}(t_k)$ and a frequency $f_{\mathrm{supply}}(t_k)$, which can be assumed as nearly

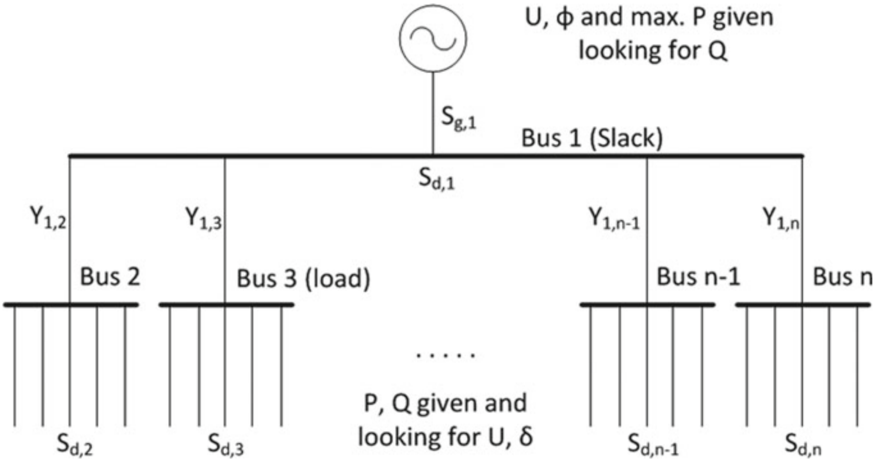

Fig. 21.3 Self-similar bus system structure assuming one power supply injecting into the main bus, which is connected to $n - 1$ distribution buses representing grouped loads

constant throughout a microgrid. From circuit schematics of the infrastructure, the admittance matrix entries Y_{ij} can be deduced, containing cable properties of the connection between the buses i and j. Figure 21.3 shows an example of a self-similar bus system architecture consisting of a slack bus connected to a power source and to subtree bus systems, distributing the power to the consumer loads. In application, one has to distinguish between the power sources types such as the power grid (primary supply), an emergency supply (secondary supply), and the uninterrupted power supply (UPS). The term secondary supply might also refer to other self-operated power sources as thermal power plants or solar panels directly connected to the CI grid. In all cases, the amount of real power supply is limited to a real power of $P_{\text{supply;max}}(t_k)$: In addition, electrical devices need an input voltage within a specific voltage range at a predefined frequency leading to the following constraints at a load i:

$$\begin{aligned} U_{\min} < U_i < U_{\max} \\ f_{\min} < f_i < f_{\max} \\ P_{g;\text{supply}} < P_{\text{supply};\max} \end{aligned} \tag{21.1}$$

Therefore, the goal of the dynamic power-flow model approach is first to determine the voltages U_i applied to the load and then determine its working state by checking whether the voltage maintains within the permitted voltage range.

The static power-flow analysis (Tinney and Hart 1967; Ilic and Zaborsky 2000; Grainger and Stevenson 1994) is a well-known tool in electrical engineering to calculate bus voltages within a grid and mathematically expressed as solving n - m number of power balance equations

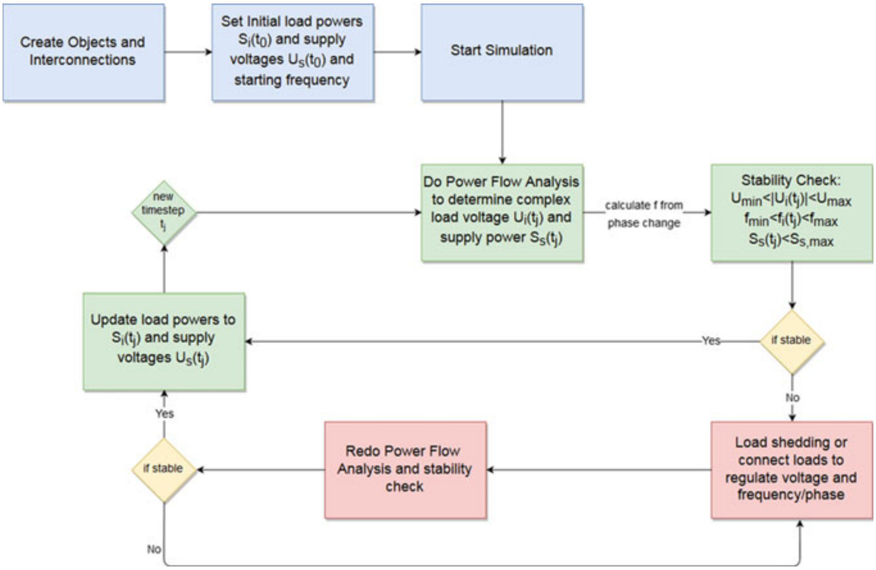
Create Objects and Interconnections
Set Initial load powers $S_i(t_0)$ and supply voltages $U_S(t_0)$ and starting frequency
Start Simulation
new timestep t_j
Do Power Flow Analysis to determine complex load voltage $U_i(t_j)$ and supply power $S_S(t_j)$
calculate f from phase change
Stability Check: $U_{min}<|U_i(t_j)|<U_{max}$ $f_{min}<f_i(t_j)<f_{max}$ $S_S(t_j)<S_{S,max}$
Update load powers to $S_i(t_j)$ and supply voltages $U_S(t_j)$
Yes
if stable
No
Yes
if stable
Redo Power Flow Analysis and stability check
Load shedding or connect loads to regulate voltage and frequency/phase
No

Fig. 21.4 Flow chart of the dynamic power flow analysis approach: After completion of the setup stage (blue), a first power flow analysis is conducted and grid stability is checked. Under stable conditions (green), the new timestep is introduced by updating input values. If instabilities (red) occur, reactions regulation processes like load shedding/adding loads are started and the power flow analysis and stability check is repeated. Decision points are marked as yellow if-statements

$$P_i - jQ_i = U_i^* \sum_{k=1}^{n} Y_{ik} U_k$$

with P_i being the real power, Q_i the reactive power of a bus i, n the number of buses, m the number of power supplies, and * denoting the complex conjugate. As the power demand of all loads vary over time and therefore leads to a variation in the applied voltages, the power-flow analysis is looped as shown in Fig. 21.4. Updating the input conditions after each timestep leads to a power flow loop driven by dynamic boundary conditions (Koch et al. 2017). The constraints defined in 1 are checked after each iteration resulting in a control feedback loop, enabling reactions if grid instabilities occur. These reactions can be planned beforehand by creating a digital emergency plan that will further described in Sect. 21.4.

21.3.2 *ICT Network Flow Model*

The purpose of the ICT network flow model is to describe how possible malware infections spread throughout the network and therefore affect process operations based on network structure and a priori knowledge about the embedded systems and

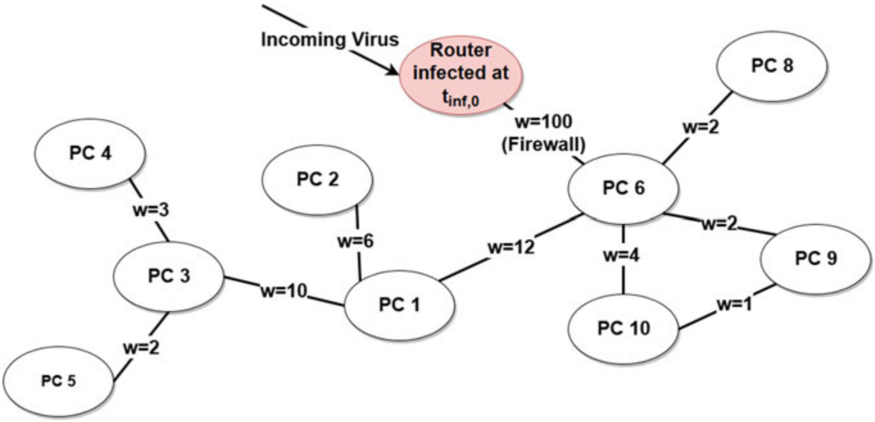

Fig. 21.5 ICT layer structure represented as a graph with objects as nodes and infection time as edges under conditions of a cyberattack, shortly after infecting the router (red) and starting to propagate through the network

malware properties. Real-time detection is excluded in the approach, but might be done in the future by comparing normal state to measured state conditions. Differential equation-based approaches as they are commonly used in epidemic modeling (Martcheva 2015), do not include network topology. Thus, a graph-based network flow (Ahuja et al. 1999) approach based on weighted edges similar to the ones explained in (Chen and Carley 2001) and (Lloyd and Valeika 2007) is used. The edge weights w_{ij} represent infection times (here we use a general time unit t.u.) between the devices i and j. While the propagation time is affected by many factors such as malware properties, the OS, computer architecture, data transfer rate, type of connection, used protocols, and encryptions or security precautions, the edge weights combine these factors to one macroscopic value. Furthermore, an infection probability is added to the nodes since not every attack on an ICT system is successful.

Figure 21.5 shows an example for an ICT network structure consisting of ten personal computers using one router to access the Internet via a router, that gets infected at a time $t_{\mathrm{inf};0}$ (red). As only PC 6 is directly connected to the router, the firewall between the router and PC 6 is attacked first. After a successful infection of PC 6, the malware spreads to every neighbor at once, i.e., at $t = t_{\mathrm{inf};0} + 100$ t.u. the infection spreads toward PCs 1, 8, 9, 10. In this example, the router is predefined as the point of attack. In real networks, attack vectors are not limited to one point of attack. Hence, many points of attack can be predefined. With the help of shortest-path algorithms such as Dijkstra or Floyd–Warshal algorithms (Dijkstra 1959; Cormen et al. 2001), the infection time of each node is calculated and assigned to each node. After time evolves beyond the node's infection time, the device is considered as infected.

By varying weight edges, points of attack, and infection probabilities, we are able to simulate a manifold of different types of cyberattacks. Whereas e-mail-based attacks might have a low probability to infect a computer, but many points of attack at once, a virus has only one or few points of attack and is more dependent on propagation behavior. In the first case, the probability is highly depended on user behavior and their knowledge about cybersecurity. Due to this, companies are highly advised to teach their staff how to detect suspicious e-mails, webpages, etc.

Moreover, an infected device is not equal to a dysfunctional device, because in some cases only certain software is affected by the infection. Thus, the devices need to be added a list of software being used on this device, and a list of affected programs is given as a malware property. As an example serves the ransomware WannaCry, which targeted the Deutsch Bahn AG but only shut down some screens and ticket vending machines without affecting traffic (Karabasz et al. 2017).

21.3.3 Model Output

Summarizing the two-layered approach yields the power demands $S_{\mathrm{d};i}(t_k)$, supply voltage $U_{\mathrm{supply}}(t_k)$, supply frequency $f_{\mathrm{supply}}(t_k)$, and admittances Y_{ij} as input parameters for the power grid layer and the edge weights w_{ij} and affected application lists of the devices for the ICT layer as it is shown in Fig. 21.6. Apart from those initial and boundary conditions, the simulation is triggered by events, i.e., (partial) blackouts or cyberattacks containing the information about power shortages and malware properties such as infection probabilities and points of attack.

Applying the mathematical tools of the dynamic power flow analysis to the electrical layer and the network flow analysis to the ICT layer then results in the load voltages $U_i(t_k)$, load frequencies $f_i(t_k)$, and needed supply power $S_{\mathrm{supply}}(t_k)$ on the one hand and the ICT infection state at time t_k on the other hand. As we are interested in the operability state at this time t_k, we have to apply the logic depicted in Fig. 21.7. The operability state depends on three decisive questions (rectangles) asking whether the power constraints (see Eq. 21.1) are fulfilled, if there is an infection of the ICT systems and if so, does it affect the process related to the device. If the electrical properties are within the constraints, if the device is not infected or at least the process not affected, the device is considered to be operable, otherwise not.

The conduction of a process relies in most cases on several devices. Therefore, to finally determine the availability of the process, the devices are grouped and assigned to process tasks. As seen in Fig. 21.1 inside one brown rectangle, several devices are located belonging to the check-in counter, which by itself is dedicated to the process of check-in. Whereas in the undisturbed case ten check-in counters are available for the check-in process, in the disturbed case only six of these are available. Thus, the resource availability can be concluded from the device grouping and process assignment.

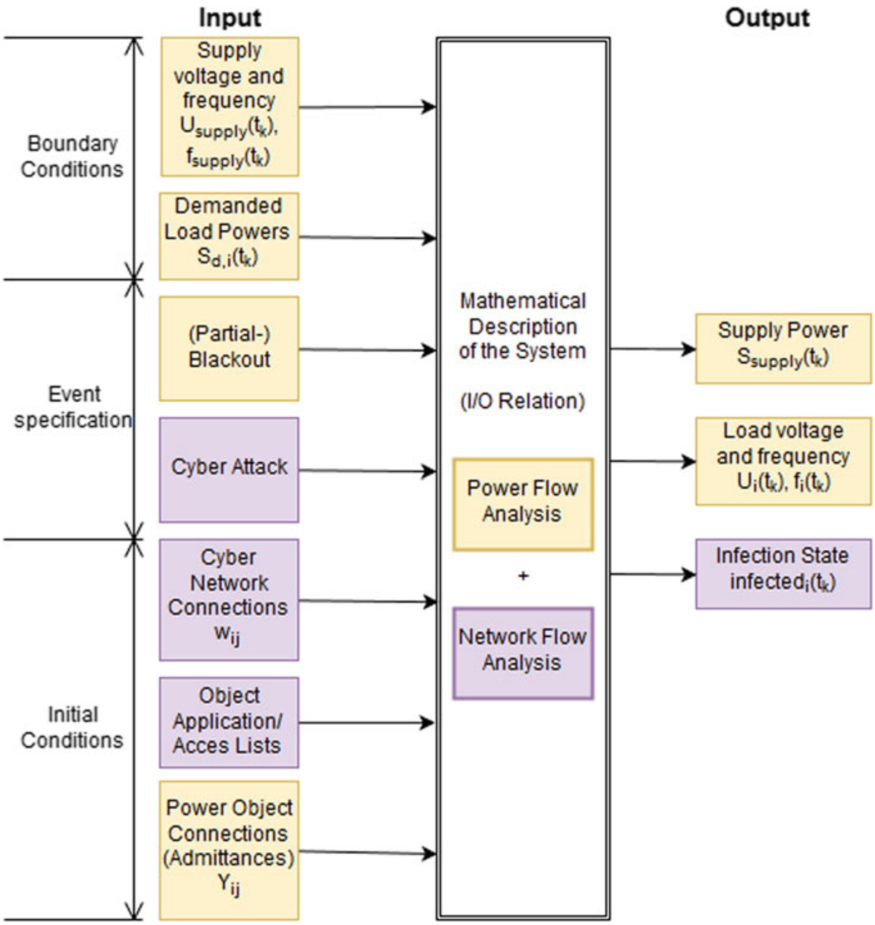
Input
Output
Boundary Conditions
Event specification
Initial Conditions
Supply voltage and frequency $U_{supply}(t_k)$, $f_{supply}(t_k)$
Demanded Load Powers $S_{d,i}(t_k)$
(Partial-) Blackout
Cyber Attack
Cyber Network Connections w_{ij}
Object Application/ Acces Lists
Power Object Connections (Admittances) Y_{ij}
Mathematical Description of the System
(I/O Relation)
Power Flow Analysis
+
Network Flow Analysis
Supply Power $S_{supply}(t_k)$
Load voltage and frequency $U_i(t_k)$, $f_i(t_k)$
Infection State $infected_i(t_k)$

Fig. 21.6 Model input and output parameters of the simulation model for the power grid (yellow) and ICT layer (light purple) connected by a power flow and network flow analysis

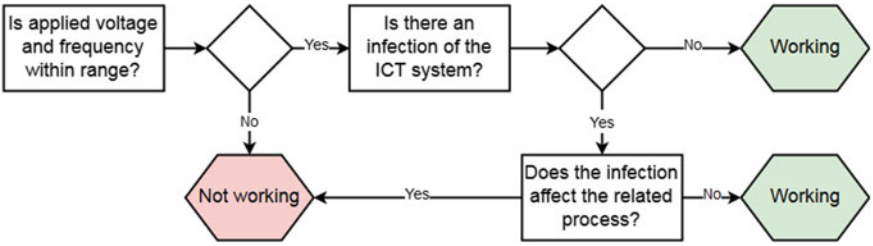
Is applied voltage and frequency within range?
Yes
No
Is there an infection of the ICT system?
No
Working
Yes
Not working
Yes
Does the infection affect the related process?
No
Working

Fig. 21.7 Visualized logic to determine working state from output parameters. Rectangles pose questions handled by yes/no logical operators (diamonds) to determine operability states (hexagons)

21.4 Digital Emergency Planning and Automated Emergency Management

During the simulation grid, instabilities might occur due to higher power demands or power shortages. Thus, in these situations steps have to be taken to stabilize the grid. Additionally, if malware infections are detected the operator might disconnect systems to prevent further spreading. Ilic and Zaborsky (2000) divide this decision and control procedure in a decision and control phase. First step is to analyze the actual grid state, determine the degree of abnormality, and categorize it within the decision phase. They propose the six categories reaching from normal and expected state over light structural or security defects and crisis situations to total system failure. Based on the categorization, the situation is assigned to a control regime proposing a list of measures. This scheme for operation and control is depicted in Fig. 21.8, where additionally to the version of (Ilic and Zaborsky 2000), the degree of abnormality is shown in the color gradient reaching from low (green) to high (red).

The increasing complexity of the CI complicates manual decision making and causes a demand for automated decision making. Combining this model for operation by decision and control with our CI model enables testing automated emergency managements by forecasting its performance. The feedback control loop within the dynamic power flow analysis is the interface to the decision and control model as it includes reactions in case of grid instabilities or infections. Using the categories defined by (Ilic and Zaborsky 2000), grid instabilities are categorized as stability or viability crisis and therefore result in control measures from the emergency control regime (dark yellow to red). Thus, in the following we need to create a digital emergency plan. System failures are explicitly excluded from this digital emergency plan since the goals are very different. While within the emergency control regime, the operator aims to keep the system viable under optimized performance, the goal of a restorative plan is to increase the resilience with a step by step solution for minimizing booting times.

For large grid structures, Ilic and Zaborsky (2000) propose a manifold of measures to be taken into account within the emergency control regime. Within a CI, measures such as increasing power injection by frequency reduction or demand for power at neighboring areas are not feasible.

The amount of measures can be reduced to four key measures within a digital emergency plan:

- Load shedding
- Control generated power
- Reschedule power demand
- Restructuring the network.

For automated control, the measures have to be expressed in a machine-readable form. Hence, a prioritization list is used to enable automated load shedding or connection of loads by pop and push operations in case of power shortages or power reserves, respectively. Considering the control of generated power, a dictionary con-

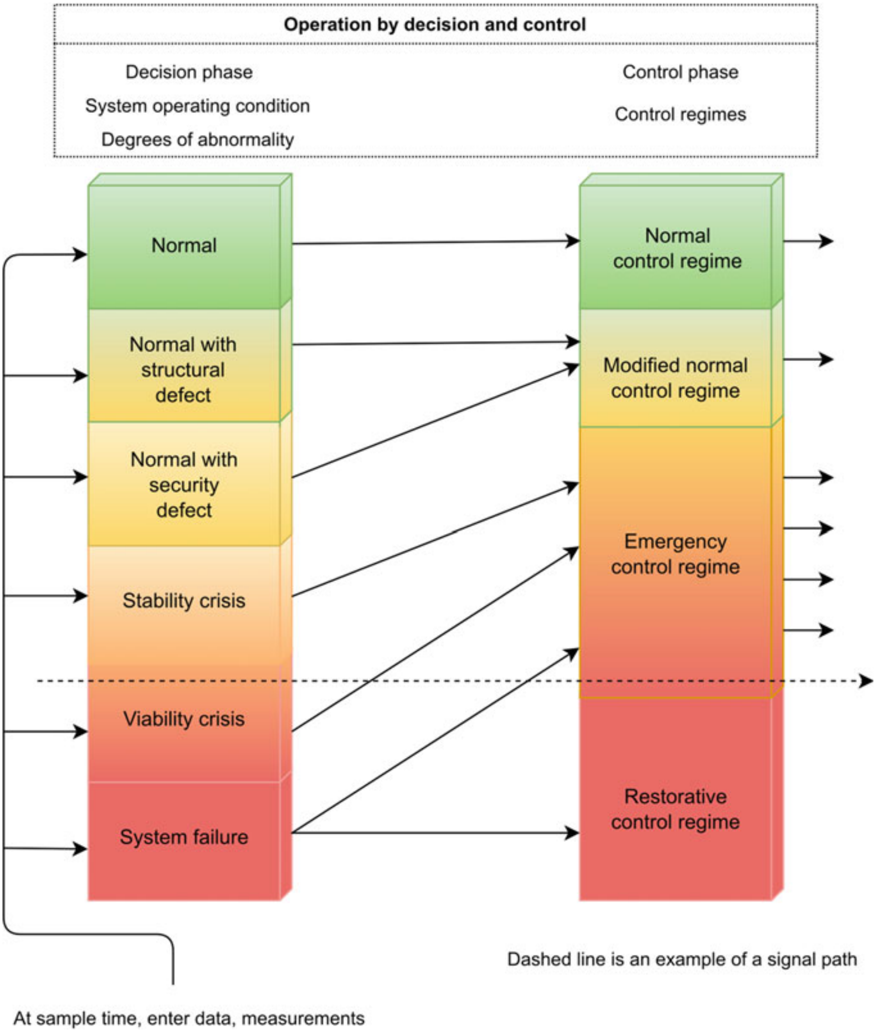
Operation by decision and control
Decision phase
System operating condition
Degrees of abnormality
Control phase
Control regimes
Normal
Normal with structural defect
Normal with security defect
Stability crisis
Viability crisis
System failure
Normal control regime
Modified normal control regime
Emergency control regime
Restorative control regime
Dashed line is an example of a signal path
At sample time, enter data, measurements

Fig. 21.8 Decision and control scheme for infrastructure operation after Ilic and Zaborsky (2000) via categorization in the decision phase determining the reaction procedures

taining available reserves, their range of power generation, and whether power generation is adjustable or not enables adaption of power injection. An application example for such a reserve within a CI is a diesel generator that might be connected to the grid, if the public power grid undergoes a power shortage. While on the ICT layer, the network structure is defined by the adjacency matrix of the graph; the admittance matrix expresses the cabling of the CI. Thus, alternating matrix entries represent a restructuring of the network. Restructuring possibilities and the respective indices have to be identified beforehand and recorded in a list for both layers each. However, the sequence of disconnection or re-connection has to be additionally determined. Therefore, we propose identifying the instability/infection source and search for the closest neighbors and whether a possibility of disconnection exists for the connection between the source and its neighbor. To automate rescheduling of processes is the most complex measure, as it should be based on the current performance of the CI and experience from the past. Thus, before the coupling between processes and infrastructure is fully understood, rescheduling of processes should be avoided. In the future, machine learning techniques might be used for this purpose. Overall, load shedding or control of the generated power should be preferred as reactive measures for power grid instabilities and insulation via restructuring the network in case of malware infections within the ICT network.

21.5 Discussion and Outlook

As the application of smart technologies exposes critical infrastructures to a wider range of threads, there is a demand for new methods ensuring the safety and security of the infrastructure. Furthermore, the introduction of smart systems makes the infrastructure system more complex due to the interfaces between physical and ICT properties. Moreover, data-driven technologies are not applicable in environments with unpredictable factors such as human behavior. Therefore, a new model was introduced that enables investigation of process-infrastructure coupling and simulating the operating state of the infrastructure throughout time. The model consists of two network layers interfering with each other, which represents the dependency of the ICT and electrical properties of the devices within the infrastructure. Within those layers, a power flow and network flow analysis is used to describe the behavior of the electrical power grid and ICT network, respectively. Whereas cyberattack, power shortages, or similar incidents can be portrayed by a triggering event, a digital emergency plan allows automated control of the system response through a feedback control loop.

The static power flow analysis was enhanced to a dynamic power flow analysis driven by dynamic boundary conditions, which enables the determination of grid stability state over time. Though the discrete approach has disadvantages compared to continuous simulations such as not being able to portray charging effects or realistic generator starting behavior, it perfectly detects instability states.

Previous graph-based approaches from Chen and Carley (2001), Lloyd and Valeika (2007), or Kephart and White (1993) describing virus propagation though concentrated on the impact of topology on propagation, but did not include any information about single systems. Thus, introducing propagation times as a macroscopic measure is a novel approach to introduce time dependencies going beyond the assumption of exponential spreading. In the context of security, reaction time is the most decisive factor for damage mitigation. As a lot of information about the malware properties has to be predefined, the technique is not able to portray real-time cyberattacks. Nevertheless, if the scenarios are set up in the right manner, the consequences of a broad range of cyberattacks can be forecasted.

Smart infrastructures are required to be able to control themselves in a secure way. Therefore, an automated emergency management system is integrated by combining the analysis results for the system operation state with a decision and control approach proposed by Ilić and Zaborsky (2000). This approach was adapted to the limitations of critical infrastructures yielding in a digitized emergency plan. As manipulations of such a digitized emergency plan might result in crucial failures, automated infrastructure control introduces a new vulnerability by creating an attack point for possible cyberattacks. However, considering critical infrastructures as highly interconnected cyber-physical systems and adapting the security precautions to this property are inevitable.

Future research needs to include infrastructure specific simulations of the related processes such as passenger flow or freight traffic to introduce assessment criteria for the digital emergency plans by evaluating infrastructure performance. If a quantitative value, rating the emergency plan, is determined, parameter studies will gain further knowledge about relations between reactive measures and infrastructure performance.

Though the overall approach is specified on improving preparedness and response until now, the model might be enhanced to restorative measures. In addition, simulation results for normal state behavior might be used as input for data-driven approaches such as machine learning to progressively improve the detection of abnormal system behavior.

References

Abrams, M., & Weiss, J. (2008). Malicious control system cyber security attack case study—Maroochy Water Services, Australia. Tech. rep., The MITRE Corporation Applied Control Solutions.

Ahuja, R. K., Magnanti, T. L., & Orlin, J. B. (1999). *Network flows—Theory, algorithms, and applications*. Upper Saddle River: Prentice Hall.

Anwar, A., & Mahmood, A. N. (2014). *Cyber security of smart grid infrastructure* (pp. 449–472). Boca Raton: CRC Press.

Batty, M., Axhausen, K. W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., et al. (2012). Smart cities of the future. *The European Physical Journal Special Topics, 214*(1), 481–518. https://doi.org/10.1140/epjst/e2012-01703-3, URL https://doi.org/10.1140/epjst/e2012-01703-3.

Bundesnetzagentur. (2007). Report by the Federal Network Agency for electricity, gas, telecommunications, post and railways on the disturbance in the German and European power system on the 4th of November 2006. Tech. rep., Bundesnetzagentur.

Chen, L. C., & Carley, K. M. (2001). A computational model of computer virus propagation. In T. H. Cormen, C. E. Leiserson, R. L. Rivest, & C. Stein (Eds.), *Introduction to algorithms* (2nd ed.). Cambridge: MIT Press.

Cormen, T. H., Leiserson, C. E., Rivest, R. L. & Stein, C. (2001). *Introduction to algorithms*, (2nd ed.). MIT Press.

Dijkstra, E. W. (1959). A note on two problems in connexion with graphs. *Numerische Mathematik, 1*(1), 269–271.

Eckert, C., & Kraüs, C. (2011). Sicherheit im Smart Grid - Herausforderungen und Handlungsempfehlungen. *DuD: Datenschutz und Datensicherheit, 35*(8), 535–541.

EUROCONTROL. (2013). Challenges of growth 2013—task 4: European Air Traffic in 2035. Tech. rep., European Organisation for the Safety of Air Navigation (EUROCONTROL).

European Commission. (2013). On a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure.

European Commission DGfRP. (2011). Cities of tomorrow—Challenges, visions, ways forward. Tech. rep., European Union. https://doi.org/10.2776/41803, URL http://ec.europa.eu/regional_policy/sources/docgener/studies/pdf/citiesoftomorrow/citiesoftomorrow_final.pdf.

Grainger, J. J., & Stevenson, W. D., Jr. (1994). *Power system analysis* (1st ed.). McGraw-Hill Education: Electrical and Computer Engineering.

Gurzu, A. (2017). Blackout at Brussels Airport delays flights. URL https://www.politico.eu/article/blackout-at-brussels-airport-delays-flights/.

Hancock, D. (2003). *Virus disrupts train signals*. The Associated Press. URL https://www.cbsnews.com/news/virus-disrupts-train-signals/.

Hermann, M., Pentek, T., & Otto, B. (2016). Design principles for Industrie 4.0 scenarios. In *49th Hawaii International Conference on System Sciences (HICSS)*. IEEE. https://doi.org/10.1109/hicss.2016.488.

Hope, A. (2015). Brussels Airport downed by power cut, 23,000 passengers stranded. URL http://www.flanderstoday.eu/business/brussels-airport-downed-power-cut-23000-passengers-stranded.

Ilić, M. D., & Zaborsky, J. (2000). *Dynamics and control of large electric power systems*. Hoboken: Wiley Interscience.

Kappenman, J. G., Zanetti, L. J., & Radasky, W. A. (1997). Geomagnetic storms can threaten electric power grids. *Earth in Space, 9*(7), 9–11.

Karabasz, I., Louven, S., & Kerkmann, C. (2017). Germans don't WannaCry. URL https://global.handelsblatt.com/companies/germans-dont-wannacry-765291.

Kephart, J. O., & White, S. R. (1993). Measuring and modeling computer virus prevalences. In *IEEE Computer Society Symposium on Research in Security and Privacy*. IEEE. https://doi.org/10.1109/risp.1993.287647.

Kesler, B. (2011). The vulnerability of nuclear facilities to cyber attack. Tech. rep., Strategic Insights.

Koch, T., Möller, D. P. F., & Deutschmann, A. (2017). Model-based airport security analysis in case of blackouts or cyber-attacks. In *16th IEEE Conference on Electro Information Technology*. https://doi.org/10.1109/eit.2017.8053346.

Koch, T., Möller, D. P. F., & Deutschmann, A. (2018). A python-based simulation software for monitoring the operability state of critical infrastructures under emergency conditions. In *17th IEEE Conference on Electro Information Technology.*

Lloyd, A. L., & Valeika, S. (2007). Network models in epidemiology: An overview. In *Complex population dynamics: Nonlinear modeling in ecology, epidemiology and genetics*. https://doi.org/10.1142/9789812771582_0008.

Macdonald, A., & Bartunek, R. J. (2016). Power cut disrupts brussels airport. URL https://uk.reuters.com/article/uk-belgium-airport-powercut/power-cut-disrupts-brussels-airport-idUKKCN0YW0DQ.

Martcheva, M. (2015). Introduction to epidemic modeling. In *An introduction to mathematical epidemiology. Texts in applied mathematics* (pp. 9–31). Berlin: Springer. https://doi.org/10.1007/978-1-4899-7612-3_2.

McMillan, R. (2007). Two charged with hacking la traffic lights. IDG News Serivce. URL https://www.computerworld.com/article/2549204/security0/two-charged-with-hacking-la-traffic-lights.html.

Möller, D. P. F. (2016). *Guide to computing fundamentals in cyber-physical systems*. Springer Publ. https://doi.org/10.1007/978-3-319-25178-3.

Möller, D. P. F., & Vakilzadian, H. (2014). Ubiquitous networks: Power line communication and internet of things in smart home environments.

Niggemann, O., Biswas, G., Kinnebrew, J. S., Khorasgani, H., Volgmann, S., & Bunte, A. (2016). Data-driven monitoring of cyber-physical systems leveraging on big data and the internet-of-things for diagnosis and control. In: *International Workshop on Principles of Diagnosis*.

Palensky, P., & Dietrich, D. (2011). Demand side management: Demand response, intelligent energy systems, and smart loads. *IEEE Transactions on Industrial Informatics, 7*(3).

Stamp, J. E., Laviolette, R. A., Phillips, L. R., & Richardson, B. T. (2009). Final report: Impacts analysis for cyber attack on electric power systems (national scada test bed fy08). Tech. rep., Sandia National Laboratories.

Tinney, W. F., & Hart, C. E. (1967). Power flow solution by Newton's method. *IEEE Transactions on Power Apparatus and Systems*.

Urlainis, A., Shohet, I. M., Levy, R., Ornai, D., & Vilnay, O. (2014). Damage in critical infrastructures due to natural and man-made extreme events—A critical review. *Procedia Engineering*, *85*, 529–535. https://doi.org/10.1016/j.proeng.2014.10.580, URL http://www.sciencedirect.com/science/article/pii/S1877705814019468, selected papers from Creative Construction Conference 2014.

US GAO. (2004). Critical infrastructure protection—Challenges and efforts to secure control systems. Tech. rep., U.S. Government Accountability Office.

Zoli, C., Steinberg, L. J., Grabowski, M., & Hermann, M. (2018). Terrorist critical infrastructures, organizational capacity and security risk. *Safety Science*. https://doi.org/10.1016/j.ssci.2018.05.021, URL http://www.sciencedirect.com/science/article/pii/S0925753517305994.