Survivability Evaluation of Gas, Water and Electricity Infrastructures

Alberto Avritzer[a,1] Laura Carnevali[b,3] Lucia Happe[c,5]
Boudewijn R. Haverkort[f,8] Anne Koziolek[c,4]
Daniel Menasche[d,6] Anne Remke [f,9] Sahra Sedigh Sarvestani[e,7]
Enrico Vicario[b,2]

[a] *Siemens Corporation, CT R US*
Princeton, NJ 08540, USA

[b] *University of Florence*
Florence, Italy

[c] *Karlsruhe Institute of Technology (KIT)*
Karlsruhe, Germany

[d] *Federal University of Rio de Janeiro (UFRJ)*
Rio de Janeiro, Brazil

[e] *Missouri University of Science and Technology (S&T)*
Rolla, MO 65401, USA

[f] *University of Twente*
Enschede, Netherlands

Abstract

The infrastructures used in cities to supply power, water and gas are consistently becoming more automated. As society depends critically on these cyber-physical infrastructures, their survivability assessment deserves more attention. In this overview, we first touch upon a taxonomy on survivability of cyber-physical infrastructures, before we focus on three classes of infrastructures (gas, water and electricity) and discuss recent modelling and evaluation approaches and challenges.

Keywords: Survivability, critical infrastructures, cyber-physical systems, gas distribution networks, water distribution networks, smart grids, hybrid models.

[1] Email: alberto.avritzer@siemens.com
[2] Email: enrico.vicario@unifi.it
[3] Email: laura.carnevali@unifi.it
[4] Email: lucia.kapova@kit.edu
[5] Email: koziolek@kit.edu
[6] Email: sadoc@dcc.ufrj.br
[7] Email: sedighs@mst.edu
[8] Email: b.r.h.m.haverkort@utwente.nl
[9] Email: a.k.i.remke@utwente.nl

1 Introduction

More and more aspects of our daily life depend heavily on large-scale infrastructural systems, think of rail and road networks, but also about telecommunication networks (internet, wired and wireless telephony). Many governments have recently issued reports on the importance (and vulnerability) of their so-called critical infrastructures, e.g., [1,2,3]; an overview can be found in [4]. Over the last few years, the infrastructure systems and networks that provide gas, water and electricity have become much more "ICT-based", implying that their well-operation is becoming dependent on the correct operation of the supporting ICT. And although the embedded ICT does provide more functionality, it is also often a source of failures, or the victim of attacks. Nevertheless, it is essential for all these critical infrastructural systems to survive catastrophic events. In this paper we address approaches towards so-called "survivability evaluation" of infrastructural systems; our focus thereby lies on water, gas and electricity infrastructures, infrastructures that used to be run by municipalities, but now are mostly run by large internationally operating companies.

We note here that the concept of survivability is not restricted to just this class of infrastructural systems. It is also known for military devices, for example, aircraft combat survivability, and even in agriculture [5]. The literature is abundant with different definitions of survivability. For an overview see for example [6,7]. Distinct definitions stress different aspects of survivability, be it the detection of faults, the defence against attacks or the recovery from various types of disasters. We will focus on the behaviour of a system *after* a disaster has occurred. Note that we do not introduce a new definition of survivability but state a slightly generalised version of the one in [8]; it reflects an intuitively appealing view on survivability of systems but is therefore also quite informal:

> *Survivability is the ability of a system to* ***recover*** *predefined* ***service*** *levels in a* ***timely manner*** *after the occurrence of* ***disasters****.*

A disaster might be any kind of severe disturbance of the infrastructural system, for example, a power breakdown, a complete or partial cut of communication lines, a flood, heavy rain or a thunderstorm. The possible causes are manifold and include purposeful attacks as well as natural disasters like earthquakes or thunderstorms.

A system is survivable if it includes mechanisms to return to normal service within an acceptable time even though a disaster occurred. What kind of mechanisms are used and how they are implemented is not part of the survivability definition. One possible mechanism to achieve survivability is fault tolerance or any other form of redundancy [9].

The above definition of survivability does not give at all a precise recipe how to decide whether a system is survivable or not. To overcome this, many approaches have been followed in the literature for the quantitative determination of survivability [10,11,7,12,13]. Most of them are model-based and suggest some measure on the system (model) behaviour and study its evolution after the occurrence of a disaster. It, thus, is the deliberate decision of the person performing the survivability evaluation to choose an appropriate measure.

Note that the definition of survivability in essence addresses the evolution of the system of interest *after* the occurrence of a disaster. This implies that the

process leading to a disaster, does not have to be included in the evaluation of the survivability. This is actually very favourable, as the exact occurrence process and probabilities are mostly very difficult to establish. In this context, we speak of so-called *GOOD models for survivability*, for *Given the Occurrence Of Disasters* [13]. In contrast, models in which the disaster occurrence is explicitly modelled, are called *ROOD models*, for *Random Occurrence Of Disasters*.

What is typical for the approaches [10] presented in this paper, is that the application field requires some form of hybrid model, taking into account discrete state components (e.g., for the up/down state of various components, or their mode of operation), continuous state components (e.g., for the physical issues playing a role), in combination with both deterministic (e.g., fixed time-outs or deterministic system evolution) and stochastic behaviour (e.g., for restoration or repair actives with random length). This combination makes analytical approaches very challenging, however, there is a clear need for these, as purely simulation-based approaches are very costly, sometimes even overly costly, to use in practice. In the remaining part of the paper, we give a brief introduction into recent approaches on survivability evaluation of infrastructures for smart water, gas and electricity networks.

The three approaches have quite a lot in common, however, also have remarkable differences. Two of them (that for gas and electricity) are based on a form of behavioural decomposition [27] in which the failure (or disaster) handling process is modelled separately from the performance of the system, through a combination of a stochastic process describing the failure handling mechanism and steady-state performance measures of interest, much the same as done in performability evaluation using Markov-reward models [26]. In contrast, in the approach taken for the water system is truly hybrid, in that the failure handling process and the water transportation and storage are combined in a single integrated model.

2 Water infrastructure

2.1 Water

Water infrastructures include the production and distribution of drinking water, as well as the collection and cleaning of sewage water. The main goal of drink water companies is the reliable supply of high quality water, whereas sewage facilities have to guarantee that a predefined maximum amount of water can be taken from the community sewage system and be cleaned and released with acceptable quality.

SCADA (Supervisory Control and Data Analysis) systems are used to remotely manage treatment and distribution facilities in all phases of operation [65]. They are used for real-time monitoring and control of the substance (water) quality, optimising pumps, maintaining reservoir levels, managing distribution systems pressures, detection of leakages and to ensure the security of facilities. Improperly managed water networks can result in increased cost and insufficient supply of drinking water. Currently, water cleaning facilities are migrating towards unmanned operation, as human operation can not be guaranteed due to labor laws. The trend towards

[10] Since this paper has an overview character, more details and mathematical background on these approaches can be found in other (cited) papers.

unmanned operation requires even more dependable and survivable systems.

2.2 Modelling approaches

To make the above more concrete, we now focus wastewater-management systems. Such systems clean water in several chemical and physical cleaning steps, before it is released. A suitable modelling formalism for such systems needs to take into account continuous (water tanks, pumps, etc.) and discrete (the setting of valves, the state of the SCADa system, etc.) quantities, as well as random events (failure occurrences, repair times, etc.). So-called stochastic hybrid models (SHMs) combine discrete and continuous variables with stochastics, hence, allow to model water treatment facilities in a natural way. However, the water treatment plants we want to consider are by far too large for state-of-the-art approaches that feature general SHMs. Several formalisms supporting SHMs have been defined [19,25,28], where each of them is suitable only in some very specific domain, and suffers from limitations that prevent it from being used in other applications.

Water management systems are characterised by deterministic fluid transportation, however, with rates that change according to a stochastic process. Hence, Fluid Stochastic Petri Nets (FSPNs) [25,28] and Piece-wise Deterministic Markov Processes (PDMPs) [19] appear to be suitable. However, the memory of continuous variables in PDMPs is lost upon stochastic transitions. Hence, they are not suitable to model the physical behaviour of fluid critical infrastructures. First and second order Fluid stochastic Petri nets (FSPNs), cf.[25,29], have a sound mathematical basis allowing for a completely formalised characterisation of the state-evolution in terms of differential equations. However, such equations can be solved only when there are at most one or two continuous variables. Simulation is the only available alternative when considering larger models [17,24].

2.3 Hybrid Petri-nets with General one-shot Transitions

To tackle the issue of scalability, a new approach based on Hybrid Petri nets [18] has recently been proposed, where the deterministic evolution is separated from the stochastic evolution of the system [23], by exploiting the quasi-deterministic behaviour of the system under study, given that failure and repair events are stochastic. Therefore, there are relatively few stochastic transitions, which allows for separating the deterministic from the stochastic evolution of the system, using a conditioning-deconditioning argument. This will speed up the reachability analysis and will allow for a large number of continuous variables in the model, as opposed to previous approaches.

The Hybrid Petri Net formalism with General one-shot transitions (HPNG) as proposed in [23] is specifically tailored towards fluid critical infrastructures. It allows for an arbitrary number of continuous variables ("tanks") that can be connected via fluid transitions ("pumps"). These transitions can be controlled by discrete places that can be connected via deterministic and generally distributed transitions; these can be used to model the ICT part of the system. Generally distributed transitions must respect the constraint that they can fire only once during the evolution of the model: for this reason we call them one-shot transitions. They can be used well to

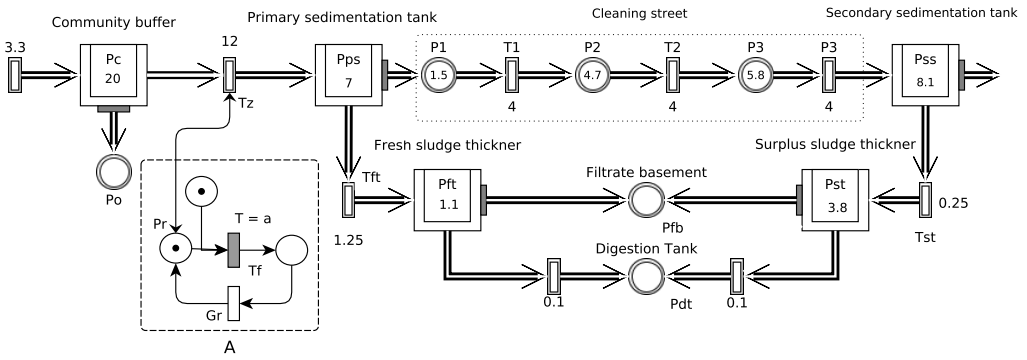

Fig. 1. The simplified HPnG model of the sewage system in the city of Enschede

model one-time disasters, or repairs.

[22] introduces a new and efficient algorithm that maps the underlying state-space onto a plane for all possible firing times of the general transition s and for all possible system times t. The key idea of the proposed method is that instead of dealing with infinitely many points in the so-called $t - s$ plane, we can partition the state space into several regions, such that all points inside one region are associated with the same system state. To compute the probability to be in a specific system state at time τ, it suffices to find all regions intersecting the line $t = \tau$ and decondition the firing time over the intersections.

To compute more complex measures of interest over time, the so-called Stochastic Time Logic (STL) has been proposed in [21], together with efficient model checking procedures that recursively traverse the underlying state space of the hybrid Petri net model. STL allows to formulate intricate state-based and time-bounded-until-based properties; the notion of *survivability* can easily be expressed using the until operator. Even though the current analysis approach is limited to a single general one-shot transition, it has been shown in [20] that one can effectively model and analyse a real sewage treatment facility, as will be shown next.

2.4 Case study

Waste water treatment facilities clean sewage water from households and industry in several cleaning steps. Such facilities are dimensioned to accommodate a maximum intake. However, in the case of very bad weather conditions or failures of system components the system might not suffice to accommodate all waste water. We show the model of a real waste water treatment facility, situated in the city of Enschede, the Netherlands, as HPNG and analyse under which circumstances the existing infrastructure will overflow.

Figure 1 models the various stages of the sewage treatment process in a simplified manner. We are mainly interested in the capacity of each phase and the average amount of time the waste water stays in the different phases. We, however, do not aim at modelling the physical, chemical and biological processes in detail. Then, for a given failure of the system (at a certain time), we analyse the survivability of the system for changing weather conditions. Fixing the failure to a specific time of the day results in a so-called "*Given the Occurrence Of Disaster*" (GOOD)

model, allows us to model the repair of the system with the single general one-shot transition. Since the evaluation method at hand is so quick, it is easily possible to parametrize the failure time and hence analyse the system thoroughly.

The capacity of the community sewerage system is modelled by an overflow place denoted P_c (the leftmost "box" in Figure 1), of which the input rate may differ, depending on the weather conditions. From this tank the water is pumped into the treatment facility with a maximum rate 12 (transition T_z); in case the input exceeds the capacity of the place and the intake of the treatment facility, waste water flows into place P_o which models the amount of water in the streets. The primary stage of the sewage treatment consists of two phases, namely the sand interceptor and the primary sedimentation tank. The sand interceptor is responsible for filtering solids like sand from the water. After that, the sewage flows into a large tank, which is used to settle the sludge, while the lighter material rises to the surface and is removed, and the remaining water overflows. In the model the sand interceptor is abstracted by the pump T_z, and the primary sedimentation tank is modelled by the overflow place P_{ps}.

A sedimentation tank physically separates suspended solids from water using gravity [16]. While the dirt settles at the ground, cleaned water is forwarded to the second cleaning stage. This stage consists of several phases for removing chemical and biological contaminations, modelled by a sequence of continuous transitions and places, before a secondary sedimentation tank separates the biological material from the now environment friendly sewage water, that can safely be disposed to surface water. The second sedimentation tank is modelled by overflow place P_{ss}. The sludge that settles at the primary and secondary sedimentation tank is accumulated and forwarded to the sludge treatment stage. There it is thickened to reduce its volume for easier off-site transport. The sludge from the primary tank is pumped out and forwarded to the fresh sludge thickener. This is also modelled by an overflow place, denoted P_{ft}. Sludge is pumped out of the place with a small rate and discharged to the digestion tank which is considered a very large tank. The overflow is directed to the filtrate basement. The same procedure is repeated for the accumulated sludge in the second sedimentation tank.

We now consider a failure in the sand interceptor, T_z, modelled by the deterministic transition T_f, firing at deterministic time α (which again could be parametrized for any value). After the occurrence of a failure, a repair crew will repair the pump, which takes, on average 2 hours (but that actually follows an exponential distribution). For this case we now investigate the following survivability property Φ (expressed in the logic STL):

$$\Phi = (x_{P_o} < 0.01)\ \mathcal{U}^{[\alpha,\alpha+30]}\ (m_{P_r} = 1), \tag{1}$$

where, $m_{P_r} = 1$, means that the sand interceptor pump is repaired. This equation expresses the probability that the overflow tank P_o will have a very low level, that is, there is no overflow, during the 30 hours following the failure, or until it is repaired, whichever comes first. Here, we have chosen the time bound $[\alpha, \alpha + 30]$ for the Until operator, since the pump is supposed to be repaired within 30 hours after its failure. The above formula (1) is typical for a wide variety of survivability measures of interest. The first term, before the Until operator is called the *safety condition*, whereas the one after the Until operator is called the*recovery condition*.

For this scenario, we consider two parameters, the time of failure and the intake rate. The result is shown in Figure 2. On the x-axis the overall intake rate (leftmost transition) is varied from 6 to 13, and the y-axis represents different failure occurrence times, from $\alpha = 30$ minutes (0.5 hours) to $\alpha = 5$ hours (after model start). As expected, for larger intake rates, the probability for Φ to hold decreases. However, it is interesting that for a late occurrence of the failure, the probability is lower, especially for high intake rates. The reason for this is that the effective capacity of the system is equal to the sum of the cleaning street rate (rate 4), and the fresh sludge thickener pump rate (rate 1.25), that is, 5.25 in total. Initially, the buffer P_c is fully filled (capacity 20). Therefore, the buffer is filling up for intake rates greater than 5.25, hence, a late failure will cause a quicker violation of the safety condition. For intake rates smaller than 5.25, the buffer P_c is actually emptied with effective rate On the other hand, for early failures, we have a non-zero survivability probability, even for high intake rates.

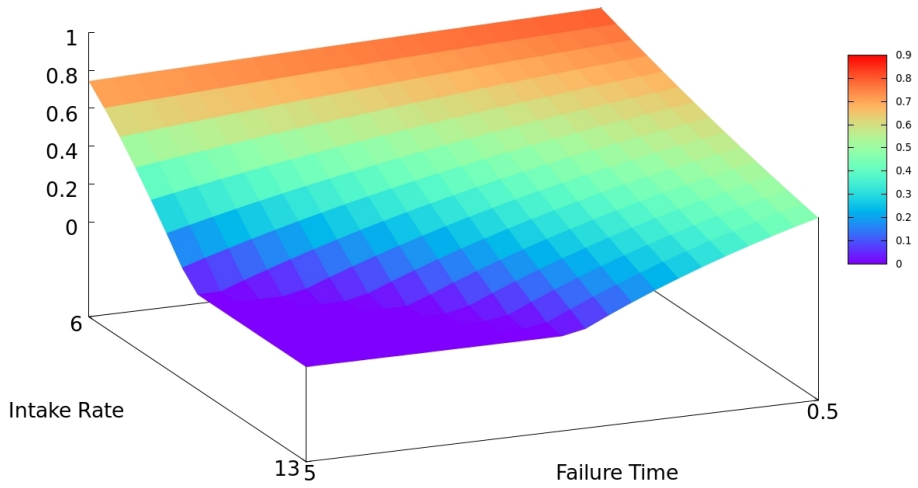

Fig. 2. Probability of holding Φ by parametrizing two factors: intake rate (x-axis) and failure time (y-axis).

2.5 Conclusions

The case study clearly shows the strength of HPNGs in both modelling capabilities and efficiency of computations, for the application field of critical water infrastructures, even with the current restriction to a single general one-shot transition. Using the underlying stochastic time diagram and the new algorithms for model checking the logic STL, it is possible to analyse the survivability of the system very quickly, so that full parametric studies can easily be performed.

3 Gas infrastructure

3.1 Gas

Long-range gas transportation is performed through transmission networks (publicly-owned in some countries), which operate at high-pressure and usually feature redundancy and storage capacity (pipeline, underground, liquefied natural gas) to make

shortage a very unlikely event. Gas delivery to customers is mostly achieved by distribution networks (owned by municipalities or private investors), which operate at lower pressure due to safety issues and leakage control.

In the past, gas transmission, distribution, and retail were usually performed by a single "vertical" company. Nowadays, the liberalised regulation has produced a number of independent companies which manage customer service but have no role in network operation. Hence, the new role of a gas network operator includes the calculation and publication of technical and available capacity, the allocation of capacity rights, and the contractual and physical congestion management.

Survivability evaluation has been less investigated for gas networks compared to electric and telecommunication network systems. However, recently, the subject is receiving increased attention due to competitive challenges raised by demand-response control applications, smart monitoring and actuation devices, novel industrial organisation of utilities, and an emphasis on homeland security and serviceability [30].

3.2 Modelling approaches

Most of the literature on the analysis of gas networks focuses on the fluid-dynamics perspective, mainly oriented to assess flow rates and pressures across network elements [31,32,33]. Optimisation of operations has been addressed in various ways, notably to favour efficient integration within multi-carrier systems combining provisioning of electric and gas power [35,36,37,38]. Stochastic modelling has been applied in [39] to consider different rates of leakage that may occur in a pipe fault and thus predict the impact on pressures and flow rates, supporting the planning of appropriate actions to mitigate risks. In [40], fluid-dynamic analysis of a section of a real gas network is repeated for different configurations of demand, thus reflecting the statistics of usage at different hours of the day and in different seasons. The effects of sequential restoration and constrained network capacity are considered in [41] to support reliability assessment by deriving average measures of interruption rate and outage time experienced by end-users, exemplifying the approach on a small-sized gas network.

3.3 An approach for derivation of transient survivability metrics

The recently proposed approach in [42] addresses quantitative evaluation of the transient behaviour of a gas distribution networks *after* the failure of a network element, i.e., again addressing a so-called GOOD model. Notice that the HPNG model cannot directly be used in the context of gas networks; the HPNG model does only address the fluid volume, and (piecewise) constant pump rates; for gas networks, next to the volume also the pressure should betaken into account. Based on pressure, also the pumps speeds can change. Temperature is taken to be constant. Overall, a more advanced modelling and analysis approach is needed for modelling gas distribution networks.

As a relevant assumption, changes of the operating conditions of the network due to daily and seasonal demand variations or demand-response mechanisms are considered independent of the actions taken in reaction to a component failure.

This permits a decoupling of the fluid dynamic behaviour of gas from the stochastic temporal behaviour of recovery actions, yielding two distinct models, while allowing their separate analyses to provide feedback to each other ("co-modelling"). On the one hand, the fluid dynamics model follows a relatively conventional graph-theoretical representation of the network topology, supporting well-known techniques for the evaluation of pressures and flow rates under a given configuration of components and parameters. On the other hand, the failure management model provides a representation of the different functional behaviours that may occur when a network component fails.

The fluid dynamic analysis consists of solving a system of non-linear equations that describes the gas behaviour across the network in terms of pressures at nodes and mass flow rates in pipes. This is performed through an iterative procedure based on the Newton-Raphson method, cf. [34]. Setting up and solving such system of equations has a complexity of $O(N+M)$ and $O(N^3)$, respectively, where N is the number of nodes and M is the number of pipes. The number of sectioning valves does not affect fluid dynamic analysis. The failure management and recovery process model is defined as a so-called *stochastic Time Petri Net* (sTPN) [44] extended with enabling and flush functions [45] (see Figure 3, lower part), which augment the modelling convenience without changing the model expressivity nor disrupting the subsequent analysis. As shown in Figure 3 (upper part), the model structure can be visualised using the UML activity diagram of recovery actions and turns out to be independent of the network topology, which makes the model general and almost guarantees a constant level of complexity of stochastic analysis. In contrast, stochastic distributions associated with temporal parameters of the model depend on the specific network under analysis, notably on the failure localisation and the consequent pressure regulation within the network.

The failure management and recovery process model describes the successive steps to be taken to recover from a disaster (or failure), in Figure 3 (lower part) visualised as an sTPN. This model may include concurrently enabled transitions with non-exponential distributions (possibly with bounded support), which goes well beyond the limits of the so-called enabling restriction and motivates the use of the solution technique proposed in [46] to perform transient stochastic analysis. The analysis method yields the transient probability of each logical state of the model, which actually corresponds to a specific operating condition of the network. The complexity of the analysis largely depends on the number of concurrent timers and on the length of paths between subsequent regenerations. As the structure of the survivability model is independent of the network topology, also the complexity of stochastic analysis turns out to be independent of the network topology. Subsequently, these probabilities are aggregated on the basis of the results of fluid dynamic analysis, which is in fact repeated under different boundary conditions to assess the service level experienced by each load node in each operating condition of the network, i.e., after each step of the failure management and recovery process that either changes the network topology or the pressure at the supply node. Hence, for each tangible state in the failure management and recovery process, a fluid dynamic analysis has to be performed; the results of these are combined with the transient state probabilities, in much the same way as done for performabil-

ity evaluation using Markov-reward models [26]. This finally allows us to derive transient and average availability measures for end-users.

3.4 Case study

To provide a proof of concept of the overall methodology, the approach has been applied on a small-sized network taken from the literature and shown in Figure 4(a) [41]. The network is made of a supply node, four load nodes (marked as A through D) and nine pipes (numbered from 4 to 12). The gas is provided by the supply node, while the sectioning valve belonging to pipe 9 is kept closed in ordinary operating conditions. According to this, the gas is supplied radially, so that load nodes A and B are served by pipes 4 and 6, and 4, 7 and 8, respectively (the "*upper branch*"), while load nodes C and D are served by pipes 5, 11 and 12, and 5 and 10, respectively (the "*lower branch*"). Without loss of generality, we now focus on failures of pipe 5, as failures of pipes belonging to the so-called network ring leave more load nodes not served than failures of radial pipes. Table 1 illustrates the results of fluid dynamic analysis, whereas Figures 4(b,c,d) show the transient metrics derived for each end-user. Although not reported here, the stochastic analysis also supports the derivation of the average outage time experienced by load nodes after a pipe failure. If failure statistics are known, such average availability measures could also be derived over a longer period of time.

failure management step	**online served nodes**	**online not served nodes**	**offline nodes**
automated detection	A,B	-	C,D
network reconfiguration	-	A,B,C,D	-
pressure regulation step 1	A	B,C,D	-
pressure regulation step 2	A	B,C,D	-
pressure regulation step 3	A,B	C,D	-
pressure regulation step 4	A,B,C,D	-	-

Table 1
Service level of each load node after each step of the failure management procedure, that changes either the network topology or the pressure at the supply node, after a failure of pipe 5.

3.5 Conclusions

The approach of [42] supports modelling and evaluation of the transient behaviour of a gas distribution network after a pipe failure. As a salient feature, the approach allows the use of non-Markovian transitions that overcome the limits of previous modelling approaches. This section only shows a small example, however, larger cases have been addressed in [46,43]. Future work includes relaxing the assumption that recovery actions do not overlap with variations of the network operating conditions.

4 Smart Grid infrastructure

4.1 Smart Grid

The Smart Grid vision for the generation and distribution of electric power is sustained by favourable tradeoff between the ratio of the increasing power generation,

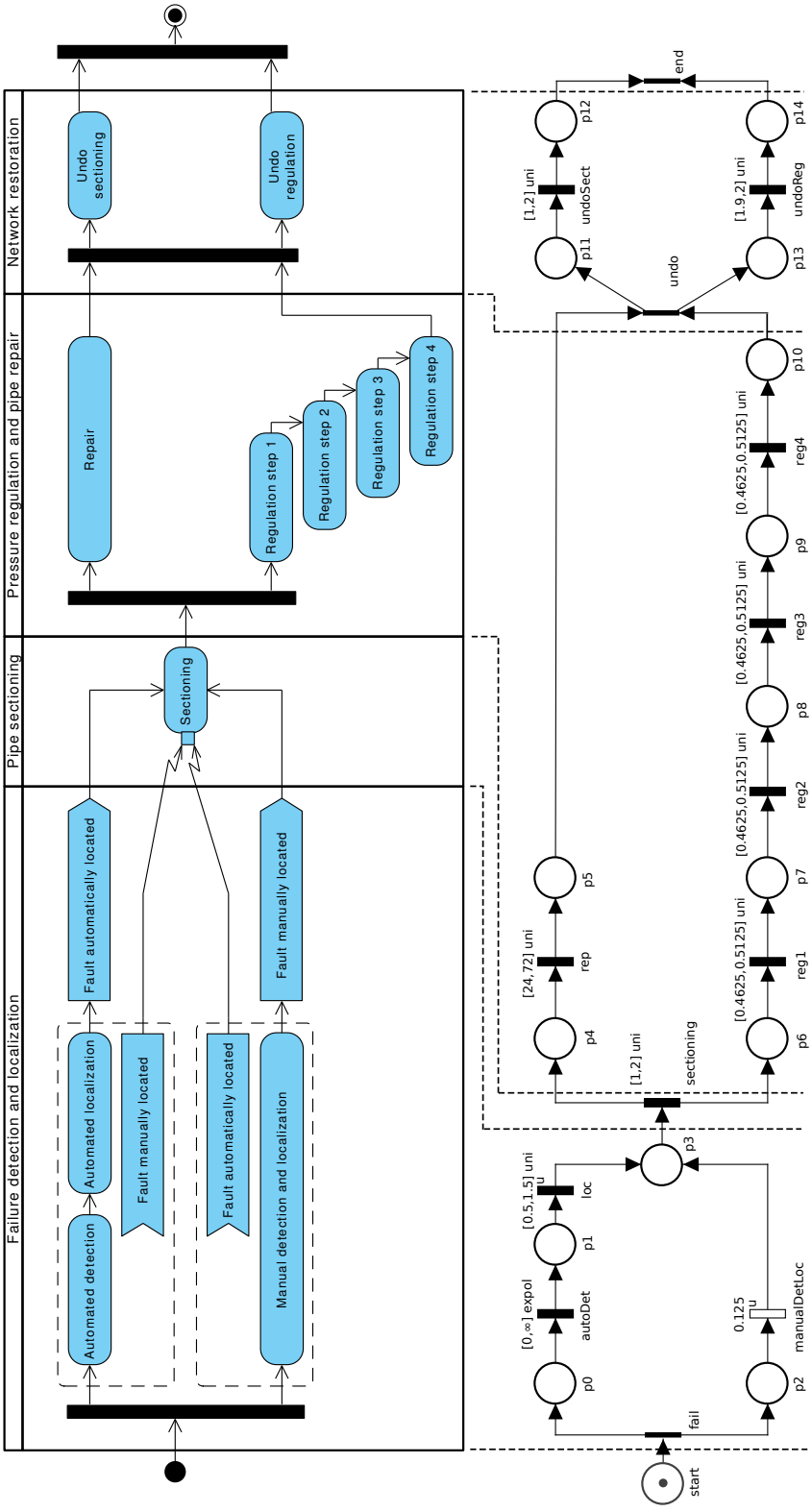

Fig. 3. The UML activity diagram of failure management actions (upper) and the corresponding sTPN specification (lower). In the sTPN, distributions associated with timed transitions refer to the example discussed in 3.4 (immediate, exponential, and general transitions are represented by thin bars, thick empty bars, and thick black bars, respectively).

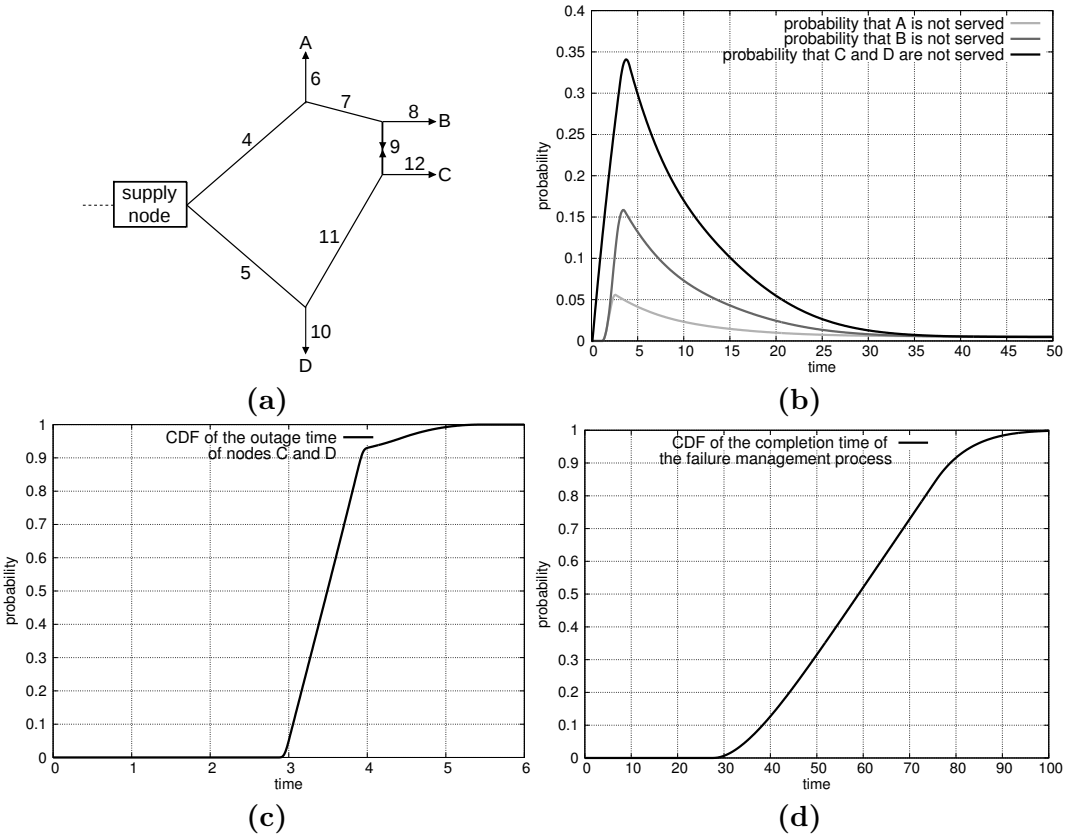

Fig. 4. **(a)** The example gas distribution network; **(b)** probability that nodes A, B, C, and D are not served after a failure of pipe 5; **(c)** CDF of the time during which nodes C and D are not served; **(d)** completion time distribution of the failure management process. All times are expressed in hours.

transmission and distribution costs to the decreasing costs of deploying computer and communication technologies. Therefore, utilities are embarking onto capital investments that deploy computer and communication technologies to the power grid with the objective of increasing the overall reliability of power systems. One objective of these investments is fortification of the grid against inevitable disruptions caused by weather, as, for instance, exemplified by the very large storm (Sandy) that recently hit the northeast coast of the United States. Regardless of the source of disruptions, which could also be the result of attacks, the goal is to mitigate the effects of failure and prevent cascading blackouts.

Smart grids aim to deploy proven ICT and internet services to the power system. For example, one approach to power reliability improvement is to dynamically route power. This is equivalent to dynamic routing protocols in the internet that detect failed links and automatically re-route over them. This is referred to in smart grid terminology as failure detection, isolation and restoration *(FDIR)*, whereby faulty sections of a feeder line are located and isolated, and power is restored to sections outside the faulty region. Dynamic routing protocols in the Internet are complemented by dynamic flow control algorithms. In power systems, flow control is referred to as *demand/response*. The *demand/response* feature in power systems are activated to manage transient variations in the supply-demand power balance or as a failure recovery mechanism.

Therefore, the opportunity for improvement of the reliability of power systems by the deployment of computer and communication technologies has been a topic of interest to system dependability researchers, see, e.g., [49,51,62,58,52,55]. The survivability assessment of power grids was first performed in [48,53,57].

4.2 Modelling approaches

Most existing approaches focus on steady-state analysis of power distribution systems. For example, Brown *et al.* [49] use an hierarchical Markovian model to derive classical metrics such as the *system average interruption duration index (SAIDI)*. Pievatolo *et al.* [59] presents a model where the components fail according to independent semi-Markov processes and the restoration times can follow non-exponential distributions. Using the model, the authors obtain the steady-state outage duration distribution. Elmakias [51] reviews available applications of Markov models in power system reliability assessment, focused on steady-state metrics.

Several studies [62,64,60,63] study the impact of adding Distributed Generation (DG) as a backup source in a power system on reliability metrics such as SAIDI. Martins and Borges [56] present a model for active distribution systems expansion planning and assess expansion alternatives using steady state metrics such as SAIDI. Chopade and Bikdash use graph-theoretic techniques to carry out structural and functional vulnerability analysis for a smart grid [50]. This study indirectly addresses survivability through the analysis of vulnerability. On the communication technology side, Wang *et al.* [61] evaluate the reliability of wide-area measurement systems (as part of the monitoring infrastructure of the smart grid) using Markovian models. However, none of these approaches considers transient measures for survivability. Resilience, defined as the ability of a system to bounce back from a failure, is a quantitative metric related to survivability. Decision support for phased recovery of a power grid, based on an analysis of the resilience of the grid throughout restoration efforts, has been presented in [47].

4.3 A phased-recovery model

Our recently introduced approach [48,57] targets assessment of transient properties of the power systems accounting for the implications of electro-mechanical and computer-based strategies to address failures in an integrated manner. In this approach, we quantify the effect of FDIR behaviour and demand/response functionality on survivability metrics, based on extended SAIDI metrics. We assume a topology as shown in Figure 5, where a feeder line between two substations is partitioned into sections that can be isolated by opening recloser devices. In case of a failure, parts of the feeder line can be powered by the backup substation by opening the tie switch.

The assessment of complex systems such as the smart grid with numerous elements and many possible states is highly challenging. The key steps to make our analysis feasible have been: (i) *initial state conditioning:* considering survivability instead of overall reliability metrics, thus conditioning the initial state of our model to be a failure state, i.e., the use of GOOD models; (ii) *state space factorisation:* modelling the system behaviour after the failure of a single given section; and (iii)

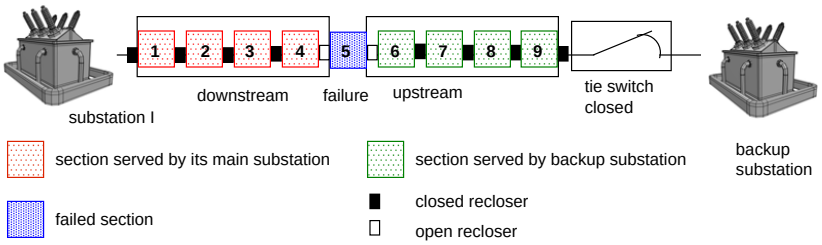

Fig. 5. Failed section ($i = 5$; blue) and its upstream sections ($i+$; green) and downstream ($i-$; red) (from [48]).

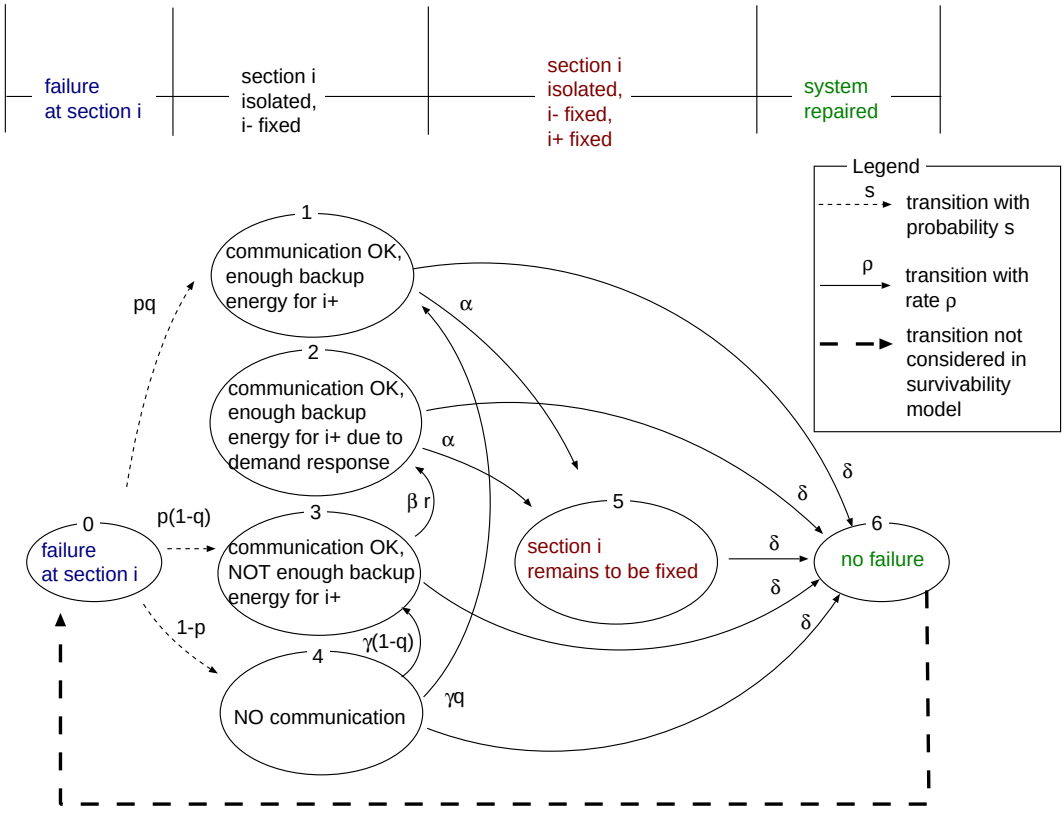

Fig. 6. Phased recovery model (adapted from [48])

state aggregation: aggregating the state of the sections outside the faulty section.

Figure 5 visualises the state aggregation principle. Consider a failure in section $i = 5$. Then, sections 1 to 4 are treated together as *the downstream sections* (denoted as $i-$) and sections 6 to 9 are considered together as *the upstream sections* (denoted as $i+$).

Our approach models the recovery of the system as a Markov chain with reward rates as illustrated in Figure 6. The states of the model correspond to the different recovery phases, indicated in the upper part of the figure: failure at section i (blue), isolation of section i and automated restoration of downstream sections $i-$ (black), automated restoration of upstream sections $i+$, and full repair. Each state has a reward rate, which models the survivability metric of interest. In the following, we use *energy not supplied per hour* as reward rate.

Parameters of our model are p, the probability that the communication network

state	0 – 1	2	3 – 4	5	6
ENS/h	542.27	509.94	542.27	49.50	0.00

Table 2
Choice of reward rates: lower bound on energy not supplied per hour (ENS/h) (from [57]).

is still operational after a section failure; q, the probability that there is sufficient backup power to supply energy for sections $i+$; and r, the probability that load can be successfully reduced in case of insufficient backup power. The time-related parameters in our model are α, the time to restore the upstream sections, β, the time to call for demand/response; δ, the time to manually repair the faulty section, and γ, the time to restore communication.

Finally, we denote with ϵ the mean time to detect the failure and isolate the faulty section. Because ϵ is an order of magnitude smaller than the other intervals of time considered in this paper, we assume its value to be $\epsilon = 0$. The average time spend in state 0 (cf. Figure 6) is therefore also 0; the initial probabilities for states 1,3 and 4 are then equal to pq, $p(1-q)$ and $1-p$, respectively.

A final assumption in our model is that the failure of communication and the load in the sections are independent of the failed section. Additionally, the model presented here supports a single faulty section only. In ongoing work [57], we are extending this to multiple failures.

4.4 Case study

In the following, we show a typical case study of applying our method taken from [57]. The load per section in the topology (cf. Figure 5, based on a feeder line in Virginia, USA [62]) is input to compute the values of the reward rates at the different model states, as shown in Table 2. The reward rates are computed based on data provided by the engineers of the power grid about its topology, taking into account the load and supply at each section. As the worst-case scenario, we consider a situation in which section 1 fails, i.e., $i = 1$, thereby maximising the demand placed on the backup substation to supply the $i+$ sections.

Figure 7 (cf. [48]) shows the expected accumulated energy not supplied (EAENS) by time t, for two cases, namely the case when demand-response is not enabled (left graphs; $r = 0$) and demand-response being enabled (right graph; $r = 1$). Using our method, changes in different parts of the system, i.e., due to investments, can be assessed. In the following, we analyse the relation between q and r, as an example. If $q = 0.9$, that is, there is a high probability that the backup power suffices for sections $i+$, demand response does not have a significant impact on EAENS. In contrast, if $q = 0.1$, demand response does play a key role, because sections $i+$ can be automatically restored when demand response is effective. The corresponding plots in Figure 7 (left and right) also demonstrate the significant impact of integrated demand response on EAENS.

The presented method allows us to quantify how various input parameters affect the EAENS. In other work, cf. [54,53], we show how these input parameters can be derived for existing power grids and how investments can be optimised. We have also applied the approach to a distribution automation benchmark derived from a

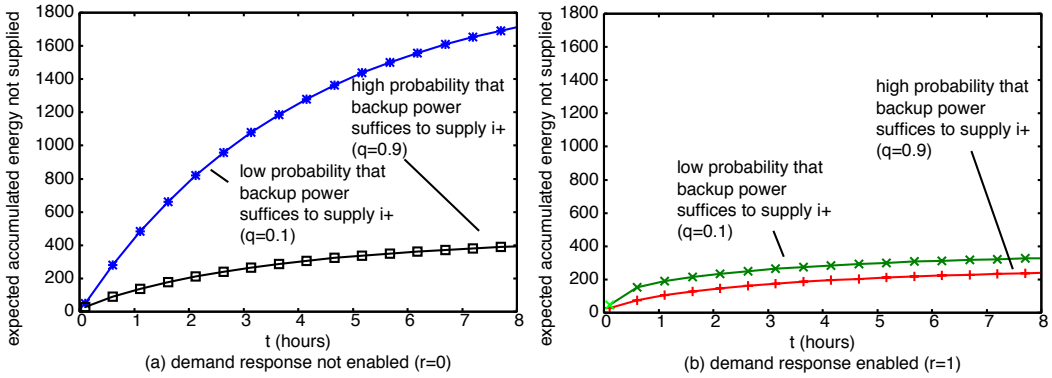

Fig. 7. Expected accumulated energy not supplied until time t, computed using uniformisation (from [48]).

German medium voltage distribution network [53].

4.5 Conclusions

The presented method supports the evaluation of different investment alternatives to improve survivability in distribution automation power grids.

The results obtained in the case study indicate that the integration of demand response with failure recovery results in a significant reduction in the amount of energy not supplied after a failure. In the future our models can serve to quantify the trade-offs between investment cost and reliability gains. The presented method is a step towards an holistic approach to guide investment decisions on different parts of a smart grid infrastructure.

5 Summary and future work

In this paper we provide an overview of three approaches towards the modelling and analysis of the survivability of smart infrastructures, in particular, gas, water and electricity networks. As more and more citizens rely on such infrastructures, adequate means to address such infrastructures, in an efficient model-based way, become more important. Such means help to make important design trade-offs and to see whether and where investments are needed to guarantee continuous operation.

From a modelling and analysis perspective, the challenges to tackle lie in:

- handling of discrete and continuous quantities, next to deterministic and random behaviour;
- dealing with large-scale systems, that is, the ability to deal with large models, large state spaces, and still provide computationally attractive numerical procedures;
- bridging the gap between the viewpoint of an application-engineer (who focusses on the application, that is, the gas, water or electricity network), and that of the modeller and analyser of the models.

The three presented approaches have quite a lot in common, however, also have remarkable differences. The approaches for smart gas and electricity infrastructures are based on a form of behavioural decomposition [27] in which the failure (or dis-

aster) handling process is modelled separately from the performance of the system, much the same as done in performability evaluation using Markov-reward models [26]. In contrast, in the approach taken for the water system is truly hybrid, in that the failure handling process and the water transportation and storage are combined in a single integrated model. This fully integrated approach has the advantage of avoiding the approximation due to the behavioural decomposition, however, this comes at the price of a more limited use of stochastic variables (only one general stochastic event can be modelled).

In this paper we have only shown small-scale applications of the three recently developed methods for survivability evaluation. A practical challenge is to team up with true application engineers, that is, from gas, water and electricity operators, to come to models for real systems. The final proof of the pudding is in the eating!

Acknowledgement
This paper is the result from the interaction between the authors at the recent Dagstuhl seminar on *Randomized Timed and Hybrid Models for Critical Infrastructures*, January 12–17, 2014, organised by Erika Ábrahám (RWTH Aachen), Alberto Avritzer (Siemens, Princeton), Anne Remke (University of Twente), and Bill Sanders (University of Illinois, Urbana Champaign). We thank these organisers for inviting us; we thank Dagstuhl for facilitating this seminar.

References

[1] Ministry of the Interior and Kingdom Relations, the Netherlands. *Rapport Bescherming Vitale Infrastructuur*. Technical report (in Dutch), 2005.

[2] Federal Ministry of the Interior, Germany. *National Strategy for Critical Infrastructure Protection*. Technical report, 2009.

[3] National Infrastructure Advisory Council. *Critical infrastructure resilience: Final report and recommendations*. Technical report, Department of Homeland Security, United States of America, 2009.

[4] A. Avritzer, F. Di Giandomenico, A.K.I. Remke, M. Riedl, "Assessing dependability and resilience in critical infrastructures: challenges and opportunities". In: *Resilience assessment and evaluation of computing systems*. Springer, Berlin, pp.41–63, 2012.

[5] S. Ling, Z. Zesheng, and G. Hengshen, "A GIS-based agricultural disaster evaluation system," *ESRI International User Conference*, 1998.

[6] J.C. Knight, E.A. Strunk, and K.J. Sullivan, "Towards a rigorous definition of information system survivability," *3rd DARPA Information Survivability Conference and Exposition (DISCEX 2003)*. IEEE Press, 2003, pp. 78–89.

[7] Y. Liu and K.S. Trivedi, "A general framework for network survivability quantification," *12th GI/ITG Conference on Measuring, Modelling and Evaluation of Computer and Communication Systems together with 3rd Polish-German Teletraffic Symposium (MMB & PGTS 2004)*. VDE Verlag, 2004, pp. 369–378.

[8] B. Ellison, D.A. Fisher, R.C. Linger, H.F. Lipson, T. Longstaff, and N.R. Mead, "Survivable network systems: An emerging discipline," Carnegie Mellon Software Engineering Institute, Tech. Rep. CMU/SEI-97-TR-013, 1997.

[9] D. Pradhan (editor) *Fault-tolerant and dependable computer system design*, 2nd ed. Prentice Hall, 2003.

[10] S.C. Liew and K.W. Lu, "A framework for characterizing disaster-based network survivability," *IEEE J. Selected Areas in Communications* **12**(1): 52–58, 1994.

[11] Y. Liu, V.B. Mediratta, and K.S. Trivedi, "Survivability analysis of telephone access network," *5th IEEE International Symposium on Software Engineering (ISSRE 2004)*, 2004, pp. 367–378.

[12] D. Medhi, "A unified approach to network survivability for teletraffic networks: Models, algorithms and analysis," *IEEE Trans. Comm.* **42**(2/3/4): 534–548, 1994.

[13] A. Zolfaghari and F.J. Kaudel, "Framework for network survivability performance," *IEEE J. Selected Areas in Communications* **12**(1): 46–51, 1994.

[14] K.S. Trivedi, *Probability and Statistics with Reliability, Queuing, and Computer Science Applications*, 2nd ed. John Wiley & Sons, 2001.

[15] M.L. Shooman, *Reliability of Computer Systems and Networks. Fault Tolerance, Analysis and Design.* John Wiley & Sons, 2002.

[16] Primer for municipal wastewater treatment systems, 'http://www.epa.gov/npdes/pubs/primer.pdf'. 2004.

[17] G. Ciardo, D.M. Nicol, and K.S. Trivedi. "Discrete-event simulation of fluid stochastic Petri nets", *IEEE Transactions on Software Engineering* **25**(2):207 –217, 1999.

[18] R. David and H. Alla. "On hybrid Petri nets", *Discrete Event Dynamic Systems* **11**: 9–40, 2001.

[19] M.H.A. Davis. "Piecewise-deterministic Markov processes: A general class of non-diffusion stochastic models", *Journal of the Royal Statistical Society. Series B (Methodological)* **46**(3): 353–388, 1984.

[20] H. Ghasemieh, A. Remke, and B.R. Haverkort. "Analysis of a sewage treatment facility using hybrid Petri nets", *Proceedings 7th International Conference on Performance Evaluation Methodologies and Tools*, ACM Press 2013.

[21] H. Ghasemieh, A. Remke, and B.R. Haverkort. "Survivability evaluation of fluid critical infrastructures using hybrid Petri nets" *Proceedings 19th IEEE Pacific Rim International Symposium on Dependable Computing*, 2013.

[22] H. Ghasemieh, A. Remke, B.R. Haverkort, and M. Gribaudo. "Region-Based Analysis of Hybrid Petri Nets with a Single General One-Shot Transition", *Formal Modeling and Analysis of Timed Systems*, *Lecture Notes in Computer Science* **7595**: 139–154, 2012.

[23] M. Gribaudo and A. Remke. "Hybrid petri nets with general one-shot transitions for dependability evaluation of fluid critical infrastructures", *Proceedings of the 2010 IEEE 12th International Symposium on High-Assurance Systems Engineering*, pp.84–93, IEEE Computer Society, 2010.

[24] M. Gribaudo and M. Sereno. "Simulation of fluid stochastic Petri nets", *Proceedings of the 8th International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems*, MASCOTS 2000, pp.231–239, IEEE Computer Society.

[25] M. Gribaudo and M. Telek. "Fluid models in performance analysis", *Proceedings of the 7th international conference on Formal methods for performance evaluation*, pp.271–317, Berlin, Heidelberg, 2007. Springer-Verlag.

[26] B.R. Haverkort, R. Marie, G. Rubino, K.S. Trivedi (Editors), *Performability Modelling: Techniques and Tools*, John Wiley & Sons, 2001.

[27] K.S. Trivedi, R.M. Geist, "Decomposition in reliability analysis of fault-tolerant systems", *IEEE Transactions of Reliability* **32**: 463–468, 1983.

[28] G. Horton, V.G. Kulkarni, D.M. Nicol, and K.S. Trivedi. "Fluid stochastic Petri nets: Theory, applications, and solution techniques", *European Journal of Operational Research* **105**(1): 184–201, 1998.

[29] K. Wolter, G. Horton, R. German. "Non-Markovian fluid stochastic Petri nets", Technical Report 13, Technical University of Berlin, 1996.

[30] Smart Grids Task Force of the European Commission, *Mission and work programme*, 2012.

[31] A. Herrán-González and J.M. De La Cruz and B. De Andrés-Toro and J.L. Risco-Martín. "Modeling and simulation of a gas distribution pipeline networks", *Applied Math. Modelling* **33**(3): 1584–1600, 2009.

[32] A.L.H. Costa, J.L. de Medeiros, F.L.P. Pessoa. "Steady-state modeling and simulation of pipeline networks for compressible fluids", *Brazilian Journal of Chemical Engineering* **15**: 344–357, 1998.

[33] B.R. Munson, D.F. Young, T.H. Okiishi, and W.W. Huebsch. *Fundamentals of Fluid Mechanics*, 2010.

[34] C. Colebrook, "Turbulent flow in pipes, with particular reference to the transition region between smooth and rough pipe laws", *Journal of the Institution of Civil Engineers*, paper number 5204, pp.133–156, 1939.

[35] , J. Munoz, N. Jimenez-Redondo, J. Perez-Ruiz, and J. Barquin, "Natural gas network modeling for power systems reliability studies", *Proceedings of the IEEE Bologna Power Tech Conference* **4**, 2003.

[36] T. Li, M. Eremia, M. Shahidehpour, "Interdependency of Natural Gas Network and Power System Security", *IEEE Transactions on Power Systems* **23**(4): 1817–1824, 2008.

[37] G. Koeppel, G. Andersson, "Reliability modeling of multi-carrier energy systems", *Energy* **34**(3): 235–244, 2009.

[38] A. Martinez-Mares, C.R. Fuerte-Esquivel, "Integrated energy flow analysis in natural gas and electricity coupled systems", *Proc. North American Power Symposium*, pp. 1–7, 2011.

[39] A.J. Brito, A.T. de Almeida, C.M.M. Mota, "A multicriteria model for risk sorting of natural gas pipelines based on ELECTRE TRI integrating Utility Theory", *European Journal of Operational Research* **200**(3): 812–821, 2010.

[40] J. Szoplik, "The Gas Transportation in a Pipeline Network, Advances in Natural Gas Technology", Dr. Hamid Al-Megren (Ed.), 2012.

[41] A. Helseth, A.T. Holen, "Reliability modeling of gas and electric power distribution systems; similarities and differences", *Intl. Conference on Probabilistic Methods Applied to Power Systems*, pp. 1–5, 2006.

[42] L. Carnevali, M. Paolieri, F. Tarani, E. Vicario, "Quantitative evaluation of availability measures of gas distribution networks", *Proc. Int. Conf. on Perf. Eval. Methodologies and Tools*, ACM, 2013.

[43] L. Carnevali, M. Paolieri, K. Tadano, E. Vicario, "Towards the Quantitative Evaluation of Phased Maintenance Procedures Using Non-Markovian Regenerative Analysis", *Proc. European Workshop on Performance Engineering*, *Lectures Notes in Computer Science* **8168**: 176190, 2013.

[44] E. Vicario, L. Sassoli, L. Carnevali, "Using Stochastic State Classes in Quantitative Evaluation of Dense-Time Reactive Systems", *IEEE Transactions on Software Engineering* **35**(5):703–719, 2009.

[45] K.S. Trivedi, *Probability and statistics with reliability, queuing, and computer science applications*, John Wiley and Sons, New York, 2001.

[46] A. Horváth, M. Paolieri, L. Ridi, E. Vicario, "Transient analysis of non-Markovian models using stochastic state classes", Performance Evaluation **69**(7): 315–335, 2012.

[47] M. Al-Basrawi, N. Jarus, K. Joshi and S. Sedigh Sarvestani, "Analysis of reliability and resilience for smart grids", *Proc. 38th Intl. Computers, Software & Applications Conference (COMPSAC)*, Västerås, Sweden, 2014, submitted for publication.

[48] A. Avritzer, S. Suresh, D. S. Menasché, R.M.M. Leão, E. de Souza e Silva, M. C. Diniz, K.S. Trivedi, L. Happe and A. Koziolek, "Survivability models for the assessment of smart grid distribution automation network designs", *Proceedings of the ACM/SPEC international conference on performance engineering*, ACM, 2013, pp.241–252.

[49] E.R. Brown, *Electric Power Distribution Reliability*. CRC Press, 2002, 2nd edition.

[50] P. Chopade, M. Bikdash, "Structural and functional vulnerability analysis for survivability of Smart Grid and SCADA network under severe emergencies and WMD attacks", *Proc. IEEE Intl. Conf. on Technologies for Homeland Security (HST)*, 2013.

[51] D.E. Elmakias, *New Computational Methods in Power System Reliability*, Springer, 2010.

[52] A.Z. Faza, S. Sedigh and B.M. McMillin, "Integrated cyber-physical fault injection for reliability analysis of the smart grid", *Proc. 29th Int. Conf. Computer Safety, Reliability and Security (SAFECOMP)*, 2010, pp. 277–290.

[53] A. Koziolek, A. Avritzer, S. Suresh, D. S. Menasche, K.S. Trivedi and L. Happe, "Design of distribution automation networks using survivability modelling and power flow equations". *IEEE 24th International Symposium on Software Reliability Engineering*, pp. 41–50, 2013.

[54] A. Koziolek, L. Happe, A. Avritzer and S. Suresh, "A common analysis framework for smart distribution networks applied to survivability analysis of distribution automation". *International Workshop on Software Engineering for the Smart Grid (SE4SG)*, 2012, pp. 23 –29.

[55] K. Marashi, S. Sedigh Sarvestani,"Towards comprehensive modeling of reliability for smart grids: Requirements and challenges". *Proc. 15th IEEE Int'l. High Assurance Systems Engineering Symposium*, Miami, USA, 2014, pp.105–112.

[56] V. Martins, C. Borges, *Active distribution network integrated planning incorporating distributed generation and load response uncertainties*. IEEE Transactions on Power Systems **26** (2011), pp. 2164 –2172.

[57] D.S. Menasche, A. Avritzer, S. Suresh, R. M. Leao, E. de Souza e Silva, M. Diniz, K.S. Trivedi, L. Happe and A. Koziolek. "Assessing survivability of smart grid distribution network designs accounting for multiple failures", *Concurrency and Computation: Practice and Experience* (2014), to appear.

[58] K. Moslehi, R. Kumar, "A reliability perspective of the smart grid", *IEEE Transactions on Smart Grid*, 2010, pp. 57–64.

[59] A. Pievatolo, E. Tironi and I. Valade, "Semi-Markov processes for power system reliability assessment with application to uninterruptible power supply", *IEEE Transactions on Power Systems* **19(3)**, 2004.

[60] S. Wang, W. Zhao and Y. Chen, *Distribution system reliability evaluation considering DG impacts. Int. Conf. Electric Utility Deregulation and Restructuring and Power Technologies*, 2008, pp. 2603–2607.

[61] Y. Wang, W. Li and J. Lu, "Reliability analysis of wide-area measurement system", *IEEE Transactions on Power Delivery* **25**: 1483–1491, 2010.

[62] I. Waseem, *Impacts of Distributed Generation on the Residential Distributed Network Operation*, M.Sc. Thesis, Virginia Polytechnic Institute, 2008, 92 pp.

[63] J. Zhang, Z. Bo, "Research of the impact of distribution generation on distribution network loss". *Universities Power Engineering Conference 2010*, 2010, pp.1–4.

[64] K. Zou, W. Keerthipala and S. Perera,"SAIDI minimisation of a remote distribution feeder", *Proceedings AUPEC 2007*, pp. 1–5, 2007.

[65] K. Stouffer, J. Falco, K. Kent, "Guide to supervisory control and data acquisition (SCADA) and industrial control systems security", *NIST Special Publications*, number 800-82, 2006.