Assessing the Impact of Cascading Failures in Urban Electricity Networks

Leonardo Montecchi, Paolo Lollini, Andrea Ceccarelli
Dipartimento di Matematica e Informatica
Università degli Studi di Firenze
Firenze, Italy
{lmontecchi, lollini, andrea.ceccarelli}@unifi.it

Abstract— **The shape of Critical Infrastructures (CIs) has changed drastically in recent years, leading them to become interconnected systems with complex interactions. This will be especially true for future power grids, known as "Smart Grids". In such complex systems, one of the main challenges consists in understanding the possible impact of failures on the overall system, and avoiding cascading or escalading effects. In this paper we present an extensible framework for the analysis of failures propagation in power networks, based on model templates developed using the Stochastic Activity Networks formalism. The approach is applied to a case study of a power network, derived from a real system. The obtained results demonstrate the effectiveness of the approach in assessing the impact of failures on the network, both when considering random failures and when performing what-if analyses on specific nodes.**

Keywords—Power grid, cascading failures, model-based evaluation, what-if analysis, network analysis, planning.

I. Introduction

The shape of Critical Infrastructures (CIs) has changed drastically in recent years. While they were traditionally closed systems, with dedicated infrastructure and proprietary software and protocols, they are now opening to the external world and increasingly using off-the-shelf components. This will be especially true for future urban electricity networks, known as "Smart Grids" [1], in which complex interactions exist between network nodes.

While one of the main aspects is to secure the CIs and protect them from malicious attacks, it is also necessary – especially in the planning phases – to understand what the effects of failures would be on the health of the system, and its resilience with respect to cascading or escalating failures. Traditional power systems are highly vulnerable to the occurrence of cascades following a node or line failure, as highlighted by large blackouts in different countries [2]. Future urban power grids are expected to minimize these problems; one of the means to achieve this objective is to improve the planning phase, both for the initial planning as well as to future upgrades and extensions of the infrastructure.

In this paper we propose a method to assess the impact of cascading failures in power networks, with the aim to understand bottlenecks and critical nodes in the grid topology. The method is part of the IRENE framework for evaluation and planning [3], [23]. The paper is organized as follows. Section II discusses the related work and introduces the context of our work. Section III introduces the modeling approach and the adopted model of cascading failures. The approach is then applied to a case study in Section IV. Concluding remarks are then reported in Section V.

II. Related Work

Decentralized infrastructures, characterized by a very large scale and independent local growth, are especially interesting to be studied under the perspective of a complex network. The power grid clearly falls in this class of systems, and techniques form complex network analysis has been frequently applied to the analysis of its properties. An interesting survey on this approach can be found in [4].

A common approach is to perform statistical analysis of topological metrics, like the degree of nodes [5], [6] or their betweenness (i.e., how many shortest paths traverse a node) [7], [8], to get an indication of the presence of nodes exposing a critical condition from the perspective of the topology (e.g., having a very high degree). Using such approaches, the resilience of the grid is assessed by evaluating the ability to efficiently guarantee paths between nodes when nodes or edges in the network are removed e.g., due to faults or attacks.

However, analyzing the power grid from a topological perspective only provides a high-level view that may not match the real behavior of the system. Some works combine topological analysis with physical parameters, using models and methods typical of the power engineering tradition, to represent the flow of power that travels through the power lines [9], [10]. Adding physical parameters to the network is beneficial for results, providing a representation of the way networks tend to disrupt and spread failures closer to reality.

Other work specifically focuses on analyzing the propagation of failures. A common approach consists in analyzing how overvoltage and/or overcurrent events are propagated through the grid, possibly leading to cascading failures. In this category, approaches vary from simple propagation models based on topological aspects [11], to the use of precise mathematical models of the physical layer [12], to the use of ad-hoc power grid simulators [13]. These approaches typically analyze the network in a static setting, or under the effect of deterministic failures, thus being particularly tailored to perform what-if analyses.

While those approaches provide a good view of the system response to specific failures, they do not provide indications on the behavior of the system as a whole, that is, how resilient is the nominal grid structure, in terms of node organization and their properties, to the occurrence of random failures under a certain assumed network load. To address this problem, approaches in the literature apply stochastic models (e.g., Stochastic Petri Nets [14]) to represent random occurrence of failures, delays, and probabilistic behavior in general. The work in [15], [16] presents a modeling approach to assess the impact of interdependencies between the Electrical Infrastructure and the controlling Information Infrastructures. The quantification is achieved through the integration of two models: one that concentrates on the structure of the power grid and its physical quantities, and one that concentrates on the behavior of the control system.

In our approach we combine the use of stochastic models with topology-based approaches for modeling the propagation of failures, thus obtaining a generic framework that can be used both to assess nodes criticality in the nominal configuration, and to evaluate the consequence of specific failures (*what-if* analysis). The approach can be used to analyze specific nodes of the grid, to compare the resilience to failures of different grid topologies, and more in general to support the planning and the evolution of the grid.

III. Extensible Modeling Approach

In this paper we present an extensible approach to model failure propagation in power grids. We first introduce the general framework we use for modeling complex systems, and then explain how we apply it to model failure propagation in electricity networks.

A. Framework

The approach we adopted for building the modeling was based on the methodology introduced in [17]: a set of *model templates* are developed for recurrent aspects and/or component of the system, and then composed together to form the global system model. Those templates communicate only through specific, well-defined model *interfaces*.

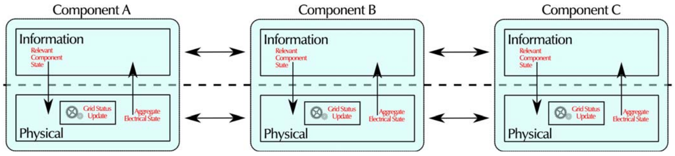

Fig. 1. Overview of the modular modelling approach. The model of each component has precise interfaces to communicate with the others.

In general, each component can be decomposed in a *physical layer* (i.e., electric behavior) and an *information layer* (i.e., control behavior). Those two layers communicate with each other through specific model interfaces (Fig. 1). Changes in the information layer that may have impact on the physical status of the grid (e.g. reconfigurations, failures, recoveries) should be notified to the physical layer, which performs a “Grid Status Update”, i.e., new physical parameters are computed by considering the current system state (e.g., number of connected generators, status of transmission lines, on/off status of loads).

This composition approach facilitates the extensibility and reuse of the model: templates can be modified in isolation, also extending them to include new functionalities. Changes need to be applied only once, and they are reflected to all the instances of that model template. Based on the desired level of detail, both the physical and the information layers can be modeled in different ways, which do not need to be the same across system components. For example, for some components the physical parameters could be obtained by using and external simulator, while for others by using sensors on the real system, or by solving power flow equations.

In the following, we discuss the realization of a *cascading failures propagation model* for the power grid, following this approach. In this instantiation of the proposed framework we only model the physical layer of components, using a simplified model of power flow across components. Section III.B in the following describes the assumptions on which the model is based, while Section III.C describes the implementation of the physical layer of grid components using the SAN formalism.

B. Assumptions and Metrics

As extensively discussed in [19], the literature features a wide range of approaches for modeling cascading failures in power networks. In particular, physical properties can be represented with different levels of detail and assumptions. The model we present in this section abstracts from the details of the power flow equations, in order to focus on failure propagation and the triggering of cascades. As the work in [20], we assume that cascades occur because nodes affected by failures will redistribute part of their load to their neighbors.

More in details, the assumptions of our model can be summarized by the following points:

- The network consists of N identical nodes.
- The initial load of a component, $L_{nominal}$, is uniformly distributed between L_{min} and L_{max}.
- Components have a *hard* limit of operation, L_{fail}, beyond which they immediately fail.
- Components have a *soft* limit of operation, $L_{critical}$, which if exceeded for a duration T_{trip} causes a breaker to trip, and thus the component to fail.
- With a rate λ a component receives an additional load between ΔL_{min} and ΔL_{max}. We are not interested in the cause that generated such overload, which can be natural (e.g., lightning) or accidental (e.g., short circuit).
- Whenever the load of a component is higher than its nominal load, and the component is not failed, the load is reduced by an amount γ with rate μ.
- When a component fails, its load is immediately redistributed among its neighbors.
- Each of the M neighbors of a failed component currently having load L receive L/M additional load.

Under these assumptions, we want to assess the criticality of nodes of a given grid topology. To quantitatively measure the criticality of a node we use the following metrics:

- $N_{fail}(t)$: The number of nodes that have failed by time t.
- $F(t) = N_{fail}(t)/N$: The proportion of nodes that have failed by time t.
- $P_{fail}^{k}(t)$: The probability that node k has failed by time t.

The first metric, $N_{fail}(t)$, is an indication of the resilience of the grid topology as a whole: the higher the number, the weaker the grid topology. By dividing it by the number of nodes in the grid, $N_{fail}(t)/N$, a proportion of the number of failed nodes is obtained. This leads to the second metric, $F(t)$, a relative metric that can be used to compare different grid topologies.

The last metric, N_{fail}(t), is an indication of the criticality of node k: nodes with higher values for this metric have a higher criticality, meaning that they are more subject to fail with respect to others. When performing what-if analysis, assessing this metric for nodes that were not involved in the initial failure gives an indication of the exposition of such nodes to cascading events originated in other nodes in the grid.

C. Realization with Stochastic Activity Networks

The model of the physical layer of components is implemented using a single template model, the *NetworkNode* template, which is replicated and instantiated multiple times to represent the desired network topology. The template has been implemented using the Stochastic Activity Networks (SAN) formalism [18]. A schematic view of the model template is depicted in Fig. 2 and it is described in the following. Dashed boxes highlight the interfaces of the model template.

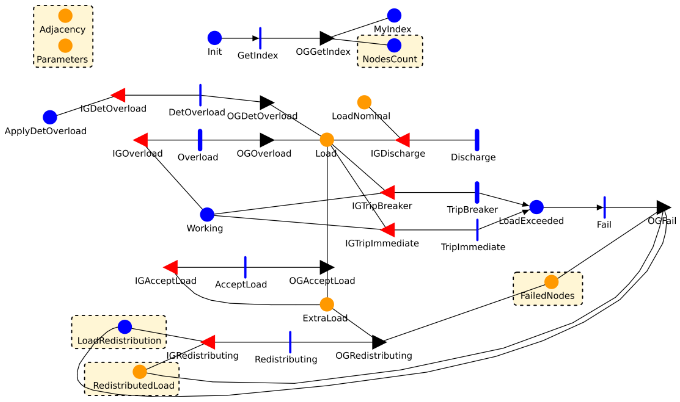

Fig. 2. SAN implementation of the *NetworkNode* model template.

The interfaces of the model template include the *Adjacency*, *Parameters*, *NodesCount*, *FailedNodes*, *LoadRedistribution*, and *RedistributeLoad* places. A unique integer index is automatically assigned to each instance of the model template, thus allowing the different instances to be distinguished. The index is assigned by the firing of activity *GetIndex*, which adds a token in *NodesCount*, and then uses this value as the index, which is then stored in *MyIndex* place. *NodesCount* is shared among all the nodes, so that at the end of the initialization process it contains the total number of nodes in the scenario.

Adjacency is an $N \times N$ array, which contains the adjacency matrix of the topology that needs to be modelled. The value of *Adjacency[i][j]* is 1 if there exist an edge between node *i* and node *j*. The extended place *Parameters* contains the parameters of all the nodes in the scenario, indexed by the node index. *FailedNodes* records which nodes are currently failed, in the form of an array. *RedistributeLoad* and *LoadRedistribution* are used to share the redistributed load between nodes.

During the initialization of the model, a number uniformly distributed between L_{min} and L_{max} is sampled; the resulting values is put in place *LoadNominal*, and then copied to place *Load*. Based on a switch variable, the model can work in two modalities:

- Random failures (*DeterministicOverload=0*)
- Deterministic failures (*DeterministicOverload=1*)

Random overload is modelled by the *Overload* activity, which is enabled only if *DeterministicOverload=0*. The activity fires with rate λ. When it fires, a number uniformly distributed between OL_{min} and OL_{max} is sampled, and the resulting value added to *Load*. Deterministic overload is modelled by the *DetOverload* activity, which instead is enabled only if *DeterministicOverload=1*. If the index of the node is equal to *DeterministicOverloadNode*, then an amount equal to *DeterministicOverloadAmount* is added to *Load*.

If *Load* becomes higher than *LoadNominal* then the activity *Discharge* becomes enabled, and fires with rate μ. Each time it fires, an amount of load γ is removed from *Load*, until the value in *LoadNominal* is restored.

If the value of *Load* exceeds $L_{critical}$ then activity *TripBreaker* is enabled. If it stays enabled for an interval of duration T_{trip} then it fires, removing the token from place *Working*, and adding one to *LoadExceeded*. Similarly, if the value of *Load* exceeds L_{fail} then activity *TripImmediate* is enabled. However, in this case it fires immediately, also removing the token from *Working* place, and adding one to *LoadExceeded*.

When *LoadExceeded* contains a token, activity *Fail* is then enabled and fires, leading to the failure of the node and to the redistribution of the load. The output gate *OGFail* has two main tasks: i) set the current node as failed in the *FailedNodes* array, and ii) compute the number of neighbours of the current node (from *Adjacency*), and consequently the amount of load to be redistributed to each of them (*RedistributeLoad*). Place *LoadRedistribution* signals to the other nodes that load redistribution took place, and thus they need to retrieve the propagated load from *RedistributeLoad* place.

When *LoadRedistribution* contains a number of tokens equal to the index of the node, then activity *Redistributing* is enabled and fires. If there is load to be redistributed for the current node (i.e., *RedistributeLoad[i]>0*), then that amount is added to *Load*, potentially incrementing the load above the critical and/or failure thresholds. This may cause further failures of the other nodes, in a cascading fashion.

The target metrics defined in Section III.B are computed as follows:

- $N_{fail}(t)$: The expected sum of tokens present in place *FailedNodes* at time t.

- $F(t) = N_{fail}(t)/N$.
- $P_{fail}^{k}(t)$: The probability there is a token in place *FailedNodes[k]* at time t.

IV. Analysis and Results

The proposed approach has been applied to a case study derived from a real power grid topology, and some of the defined metrics computed using the simulator provided by the Möbius tool [21]. For all the results shown in the following, values have been computed by running at least 10.000 simulation batches, with a relative confidence half-interval of 0.1, and confidence level 90%.

A. *The Analyzed Scenario*

As a case study we consider an urban power grid composed of 21 interconnected nodes, which can represent for example a neighborhood inside a wider urban area. To obtain a plausible topology, we adopted a modified version of the 30-bus Power Flow Test Case available at [22]. We note that we mainly used the test case from a topological perspective, and thus derived a simplified graph-based representation of it.

The simplified network contains 21 nodes and it is depicted in Fig. 3. With respect to the labels adopted in the original layout [22] some nodes have been joined together for simplicity.

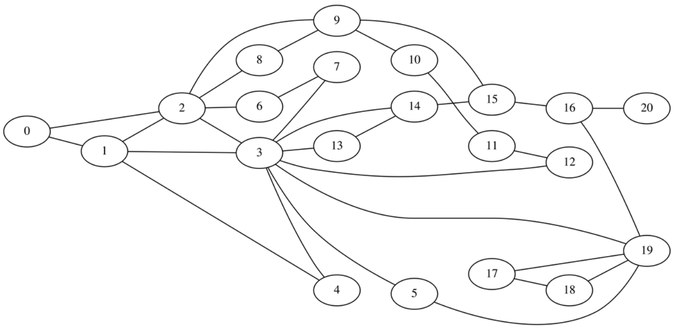

Fig. 3. Simplified network derived from the 30-bus Power Flow Test Case.

The main parameters of the model are reported in Table I, together with the nominal values that will be used in this evaluation. The unit of measurement for time-related quantities is minutes.

B. *Random Failures*

The first evaluation that we describe focuses on analyzing the effects of random failures on the grid. Fig. 4 shows the average number of failed nodes during a month, at varying of the overload rate λ. Note that repairs are not included in the model. Values of λ equal to $5.0 \cdot 10^{-5}$ or higher pose a significant threat for the analyzed grid topology: on the average at least one node will be failed after 30 days. For $\lambda = 5.0 \cdot 10^{-4}$ the system is not manageable anymore: on the average, more than 9 nodes will fail after 30 days. This is clearly a situation where cascading failures occurred, causing a widespread failure of network nodes.

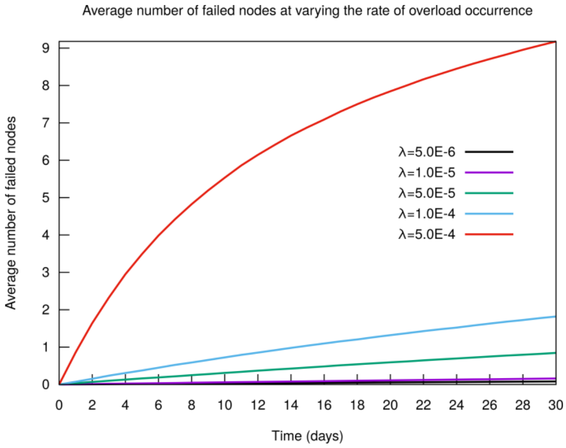

Fig. 4. Average number of failed nodes at varying of the overload rate of individual nodes.

Fig. 5 shows the failure probability of individual nodes after 30 days, in the nominal configuration. From the figure, it is evident that some nodes are more subject to be the target of failure propagation with respect to other nodes. In particular, node 3 is the most critical one, followed by 2, 19, and 9. The least affected ones result to be node 4 and node 5. By comparing these results with the diagram of Fig. 3, the nodes that are deemed most critical are those that have a higher number of neighbors (node degree). The results are explained by the fact that, having more neighbors, they will receive a higher amount of propagated load in case of other nodes' failures.

TABLE I. Model parameters and their default values. Time quantities are in minutes.

Parameter	Symbol	Value	Description
LoadMin	L_{min}	0.2	Minimum initial load
LoadMax	L_{max}	0.6	Maximum initial load
OverloadOccurrenceRate	λ	1.0E-5	Occurrence rate of an overload event
OverloadMin	OL_{min}	0.1	Minimum load amount that is added by a random overload event
OverloadMax	OL_{max}	0.2	Maximum load amount that is added by a random overload event
DeterministicOverloadAmount	–	1.0	Amount of load that is added to a component when in deterministic mode (what-if analysis)
LoadCritical	$L_{critical}$	0.75	Critical load level
LaodFail	L_{fail}	0.99	Maximum load level, beyond which the component immediately fails
BreakerDelay	T_{trip}	20.0	Time after which the component fails if the load remains above $L_{critical}$
OverloadDischargeAmount	γ	0.01	Amount of exceeding load that is absorbed at each discharge
OverloadDischargeRate	μ	0.1	Rate at which discharge of exceeding load occurs

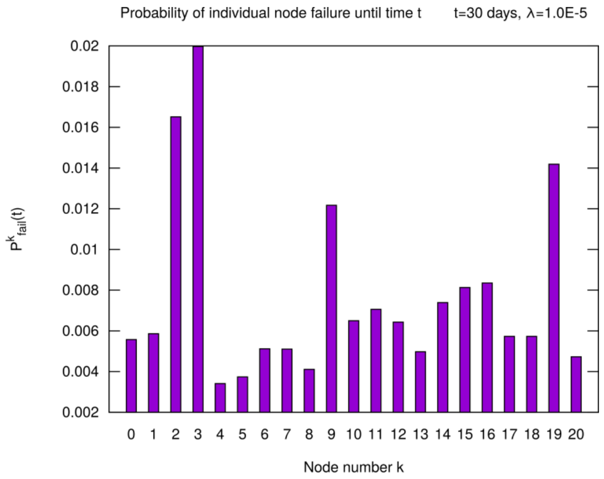

Fig. 5. Failure probability of individual nodes as effect of random faults (node overload) in the network.

C. What-If Analysis

In this section we show how the framework can be used to perform what-if analysis. We assume that a large overload occurs on one of the nodes of the network, causing its failure, and we assess if and how the failure has cascading effects on the other nodes of the grid.

Fig. 6 depicts the effect of a large overload on four different nodes of the network: node 1, node 7, node 9, and node 20. Each graph shows the probability of failure of the other nodes of the network as a consequence of the failure under analysis. The results provide useful insights on the criticality of individual nodes, and on the possible *propagation dynamics* that may arise.

In case of failure of node 1 (top left), its immediate neighbors, nodes 0, 2, 3, and 4, will also fail. However, the cascading effect is limited: for the other nodes the probability of failure is zero or very small. Similarly, the failure of node 7 (top right) has a large impact only on nodes within distance two from it (2, 3, and 6), while it has a limited impact on the others. This is a good indication that the cascading effect will be contained. The interruption of the cascading effect is due to the high degree of both nodes 2 and 3; this allows the excess load to be spread among a large number of nodes, thus being partially absorbed.

Instead, the failures of node 9 (bottom left) or node 20 (bottom right) cause a large cascading effect on many nodes of the network. In the first case, four nodes have a failure probability greater than 50%, and other three greater than 25%. In the second case, three nodes have a failure probability of almost 100%, three near 50%, and other two greater than 25%, some of which are at distance 4 from the failed node.

It should be noted that, under the "random failure" setting (Section 8.3.2), node 9 was found to be one of the nodes more affected by random failures. The what-if analysis performed in this section indicates that a failure of that node would cause

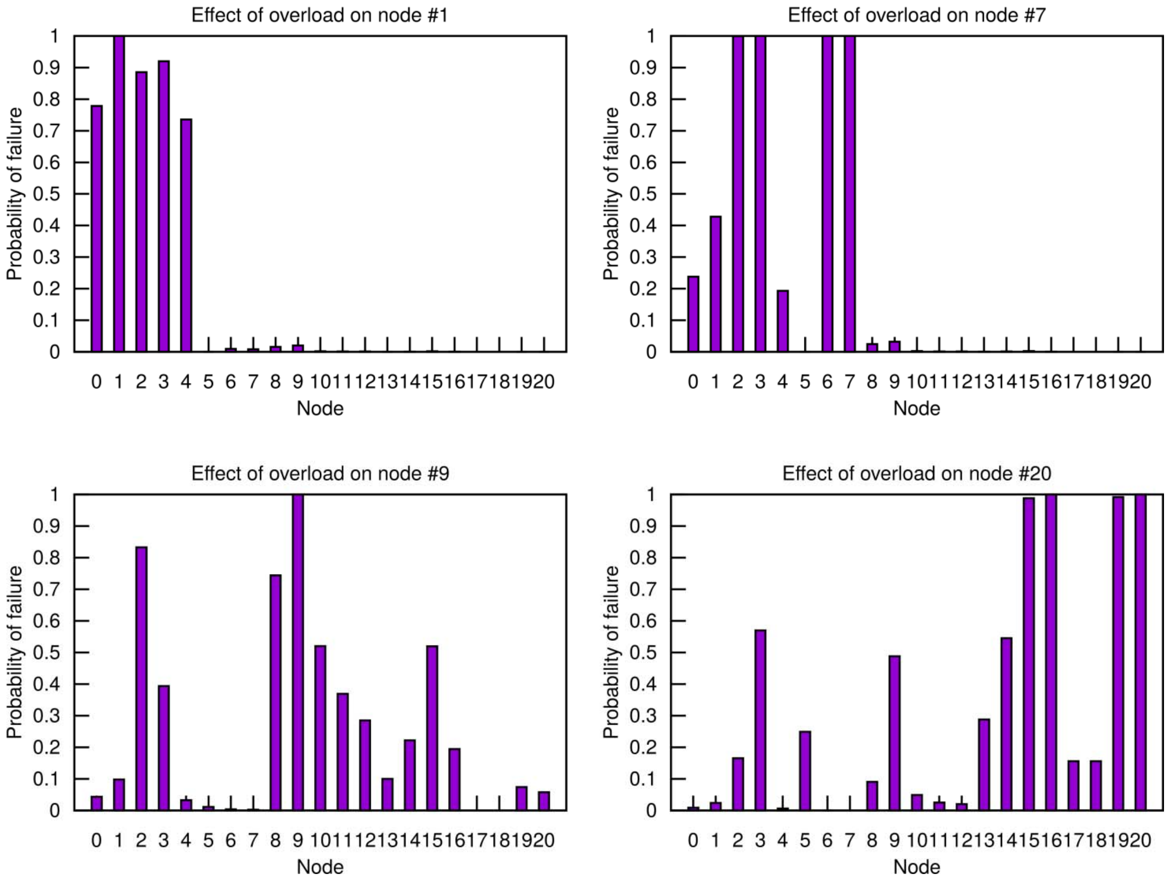

Fig. 6 Effect of a large overload on specific nodes of the network.

severe cascading effects on the whole network. Therefore these results suggest that node 9 is a very critical node, which could require some specific maintenance actions, e.g. for increasing the maximum load level beyond which the component fails (thus increasing the L_{fail} and $L_{critical}$ thresholds).

V. Concluding Remarks

In this paper we presented an approach to analyze, from a quantitative point of view, the impact that failures or attack to nodes have on the global health of the network. The approach can be used to analyze the effect of random failures in the target grid, as well as to perform what-if analyses. The approach we proposed is fit in an extensible framework for modeling complex cyber-physical systems. By using the templates approach, models can be refined and extended, to take into account more complex interactions or lower-level dynamics.

The application of the approach to the presented use case has demonstrated its capabilities to assess the *resilience of the grid topology*, and to identify *most critical paths and nodes* in the grid, which are more vulnerable to cascading failures. These kinds of analyses can be profitably used as support for planning the construction and/or evolution of the network, in order to maximize its resilience to failures.

As a future work, we plan to extend the current approach in different ways. First, we plan to extend the model to include also aspects related to the information layer, e.g., usage profiles and user behavior. The second direction is to formalize the description of model templates according to the TMDL language introduced in [17], and actually develop a library of model templates for the power grid domain. Finally, another direction is towards including a more detailed representation of the physical behavior of nodes, possibly by combining SAN models with a domain-specific simulator, by using an approach similar as the one adopted in [24].

Acknowledgment

This work has been partially supported by the IRENE project “Improving the Robustness of Urban Electricity Networks”, JPI Urban Europe, n°847342 and the Tuscany Region project POR FESR SISTER “Signalling & Sensing Technologies in Railway application”.

References

[1] C. Clastres, “Smart grids: Another step towards competition, energy security and climate change objectives”, Energy Policy, Volume 39, Issue 9, September 2011, Pages 5399-5408, ISSN 0301-4215.

[2] G. Andersson *et al.*, "Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance," in *IEEE Transactions on Power Systems*, vol. 20, no. 4, pp. 1922-1928, Nov. 2005.

[3] “IRENE – Improving the Robustness of Urban Electricity Networks”, JPI Urban Europe, n°847342, http://ireneproject.eu , last accessed 19/04/2017.

[4] G. A. Pagani and M. Aiello, “The power grid as a complex network: a survey,” *Physica A: Statistical Mechanics and its Applications,* vol. 392, no. 11, pp. 2688-2700, 2013.

[5] D. P. Chassin and C. Posse, “Evaluating North American electric grid reliability using the Barabasi Albert Network Model,” Physica A: Statistical Mechanics and its Applications, vol. 355, pp. 667-677, 2005.

[6] Z. Wang, A. Scaglione and R. Thomas, “The node degree distribution in power grid and its topology robustness under random and selective node removals,” in IEEE International COnference on Communications Workshops, ICC, pp. 1-5, 2010.

[7] P. Crucitti, V. Latora and M. Marchiori, “A topological analysis of the Italian electric power grid,” Physica A: Statistical Mechanic and its Applications, vol. 338, pp. 92-97, 2004.

[8] R. Albert, I. Albert and G. L. Nakarado, “Structural vulnerability of the North American power grid,” Phys. Rev. E 69, 025103(R), vol. 69, no. 2, pp. 1-10, 2004.

[9] S. Arianos, E. Bompard, A. Carbone and F. Xue, “Power grid vulnerability: a complex network approach,” Chaos: An Interdisplinary Journal of Nonlinear Science, vol. 013119, no. 19, pp. 1-6, 2009.

[10] E. Bompard, R. Napoli and F. Xue, “Analysis of structural vulnerabilities in power transmission grids,” International Journal of Critical Infrastructure Protection, vol. 2, pp. 5-12, 2009.

[11] S. Hong, B. Wang and J. Wang, “Cascading failure propagation in interconnected networks with tunable load redistribution strategy,” in 2015 Prognostics and System Health Management Conference (PHM), Beijing, China, 2015.

[12] Z. Huang, C. Wang, T. Zhu and A. Nayak, “Cascading failures in smart grid: joint effect of load propagation and interdependence,” IEEE Access, vol. 3, pp. 2520-2530, 2015.

[13] M. Wei and W. Wang, “Combat the disaster. Communications in smart grid alleviate cascading failures,” in 11th Annual High Capacity Optical Networks and Emerging/Enabling Technologies (Photonics for Energy), Charlotte, NC, 2014.

[14] G. Ciardo, R. German and C. Lindemann, “A characterisation of the stochastic process underlying a stochastic Petri net,” IEEE Transactions on Software Engineering , vol. 20, pp. 506-515, 1994.

[15] M. Beccuti, et al., “Quantifications of dependencies in electrical and information infrastructures: the CRUTIAL approach,” in 4th International Conference on Critical Infrastructures (CRIS 2009), 2009.

[16] S. Chiaradonna, P. Lollini and F. Di Giandomenico, “On a modeling framework for the analysis of Interdependencies in elctric power systems dependable systems,” in 37th Annual IEEE/IFIP International Conference, 2007.

[17] L. Montecchi, P. Lollini, and A. Bondavalli. “A DSL-Supported Workflow for the Automated Assembly of Large Stochastic Models”. In: Proceedings of the 10th European Dependable Computing Conference (EDCC’14). Newcastle upon Tyne, UK, May 13–16, 2014, pp. 82–93.

[18] W. H. Sanders and J. F. Meyer, “Stochastic activity networks: formal definitions and concepts,” in Lectures on formal methods and performance analysis, New York, Springer-Verlag, 2002, pp. 315-343.

[19] R. Fitzmaurice, E. Cotilla-Sanchez and P. Himes, “Evaluating the impact of modeling assumptions for cascading failure simulation,” in 2012 IEEE Power and Energy Society General Meeting, San Diego, CA, 2012.

[20] E. Zio and G. Sansavini, “Component criticality in failure cascade processes of network systems,” Risk Analysis, vol. 31, no. 8, pp. 1196-1210, 2011.

[21] T. Courtney, S. Gaonkar, K. Keefe, E. W. D. Rozier and W. H. Sanders, "Möbius 2.3: An extensible tool for dependability, security, and performance evaluation of large and complex system models," *2009 IEEE/IFIP International Conference on Dependable Systems & Networks*, Lisbon, 2009, pp. 353-358.

[22] R. Christie, “30 bus power flow test case,” Power Systems Test Case Archive, August 1993.

[23] O. Jung et al., "Towards a collaborative framework to improve urban grid resilience," 2016 IEEE International Energy Conference (ENERGYCON), Leuven, 2016, pp. 1-6.

[24] A. Bondavalli, P. Lollini, and L. Montecchi. “QoS Perceived by Users of Ubiquitous UMTS: Compositional Models and Thorough Analysis”. In: Journal of Software 4.7 (Sept. 2009), pp. 675–685.

[25] Zoppi, T., et al., A Modeling Framework to Support Resilient Evolution Planning of Smart Grids. In: 2nd EAI International Conference on Smart Grid Inspired Future, Springer Verlag, 2017.