Journal of Polish Safety and Reliability Association
Summer Safety and Reliability Seminars, Volume 6, Number 3, 2015

Alberto Tofani

Antonio Di Pietro

Luisa Lavalle

Maurizio Pollino

Vittorio Rosato
Energy and Sustainable Economic Development (ENEA)
Technical Unit for Energetic and Environmental Modelling, Casaccia Research Centre,
Via Anguillarese 301, 00123 Rome, Italy

Silvio Alessandroni
ACEA S.p.A. Piazzale Ostiense 2, 00154, Rome, Italy

CIPRNet Decision Support System: Modelling Electrical Distribution Grid Internal Dependencies

Keywords

natural hazards, risk analysis, interdependencies, power network, SCADA

Abstract

In this work, we present a peculiar application contained in a Decision Support System for Risk Analysis of (inter)dependent Critical Infrastructures under development within the EU FP7 CIPRNet Project. The application shows the efficacy and the benefits derived from a complete information of the multiple (inter)connected infrastructures (electrical and telecommunication) present in a Crisis Scenario. Electrical Distribution operators use SCADA systems to perform remote operations (tele-control) on the electrical grid such to ensure a constant and efficient energy supply to the consumers. Tele-control operations bi-directionally couple telecommunication and electrical networks: faults in one network produce effects, which then reverberate on the other. The work shows how the DSS, based on the damage estimate occurring on the two systems, may predict the correct tele-control operations needed for the restoring of the electrical grid based on topological properties of the electrical substations and the Telecom nodes.

1. Introduction

In 2009, hurricane Sandy brought high winds and coastal flooding in US, leaving nearly 8 million customers without power. In 2013, a 7.1 magnitude earthquake hit the Philippines causing severe damages to infrastructures. When a specific perturbation hit a system of Critical Infrastructures (CI), system's dependencies propagate faults from one system to another producing cascading effects and thus amplifying impacts of the events.

Prediction and/or a rapid assessment of Critical Scenarios can be thus a major breakthrough for increasing preparedness strategies, for activating mitigation actions by increasing systems resilience. To this end, a major goal could be represented by a correct prediction of the course of events, starting from the prediction of the occurrence of natural hazards and of their strengths, by the connection of event's strength to the expected damages to assets, by the connection of the expected damages to the resulting impacts that they will produce in reducing or destroying supplied Services. If this analysis could also be accompanied by a thorough analysis of the Consequences that reduction or loss of Services might produce on relevant areas of societal life, this could represent an unique and valuable tools for supporting Emergency Managers, CI operators, Public Administration Offices which strong commitment if Crisis Management (Civil Protection, Fire Brigades etc.). The realization of a similar object, cast in the form of a Decision Support System (DSS), is one of the objectives of the CIPRNet project. The designed DSS implementing the above mentioned risk assessment workflow other than predicting the extent of the expected crisis, can also be used to "weigh" the efficacy of the result of the proposed mitigation and healing actions.

The DSS can be logically represented in terms of five functional components (Bn) which leverage on a large Database containing GIS data of CI elements, assets, geographical, social, economic information of the area under control. These are:

Monitoring of natural phenomena (B1): This functional block acquires geo-seismic, meteorological forecasts and nowcasting data, other than sensor field data when available.

Prediction of natural disasters and events detection (B2): This block, based on information of B1, predicts, within an estimated temporal horizon, the strength of a limited set of natural phenomena occurring in the specified area.

Prediction of physical harm scenarios (B3): This block evaluates the probability that each CI element can receive a damage if hit by the predicted natural events and the estimate of its loss of functionality. The association (Event Strength-Damage) of a physical component $\boldsymbol{c_i}$ of the *x-th* CI by a threat manifestation $\boldsymbol{T_j}$ is performed by considering the intrinsic vulnerability of $\boldsymbol{c_i}$ with respect to the intensity of $\boldsymbol{T_j}$ (output of B2). The outcome is a set of affected CI physical components and the extent of the estimated physical damages, the Physical Harms Scenario (PHS) defined as:

$$\boldsymbol{PHS} = (\boldsymbol{c^T}, \boldsymbol{D^T}) \tag{1}$$

where $\boldsymbol{c^T}$ is the set of CI components that are expected to receive an over-threshold probability to be damaged and $\boldsymbol{D^T}$ is the set of the extent of estimated damages for each CI component. The $\boldsymbol{PHS}$ can be provided to CI operators for alerting on the possible damages expected for the physical components of their CI.

Impact and consequences estimate (B4): This block estimates the Impact that Damages will produce on the Services delivered by the CI and the resulting Consequences, i.e. the effects on citizens, services, economy, and the environment (Criteria). European Council Directive 2008/114/EC [1] has, in fact, defined that the relevance of a given Crisis Scenario, produced by disruption or destruction of elements of European (or National) Critical Infrastructure shall be assessed in terms of cross-cutting Criteria weighting all the induced effects on the bases of their costs in terms of casualties other than in economic and other "public" costs.

Support of efficient strategies to cope with crisis scenarios (B5): This block provides Crisis Managers with a decision list of actions in those cases where the DSS can provide further information needed to support a crisis solution.

In Section 2 we describe the objective of this contribution which reports on a specific task for supporting electrical operators in assessing the correct Impact Scenario expected from a $\boldsymbol{PHS}$. This task constitutes the initial stage of the B4 functional block and accounts for the prediction of the short time scale Impacts on the electrical infrastructure, considered to have a major role in crisis management scenarios [3]. Section 3 describes the architecture implemented within the CIPRNet DSS for the B4 functional block. Section 4 describes the electrical distribution grid reconfiguration algorithm. The algorithm plays a central role in the prediction of the short time scale impacts of a $\boldsymbol{PHS}$ on the electrical infrastructure. Section 5 describes a test case for the proposed platform and how the prediction of the short time scale impacts (in particular for large crisis) is useful to improve possible mitigation strategies of crisis due to natural events. The Section 6 draws some conclusions.

2. Assessment of short time scale impacts

In this work, we present how the DSS performs the impacts assessment. In particular, we will focus on the short time scale impacts assessment. Starting from the predicted damages in a test case involving a distribution power network and the relative SCADA system, the proposed module computes the reduction of QoS of the electrical network due to the predicted damage scenario. The Impact evaluation module has been dived into two different phases: in the first, strongly coupled infrastructures (such as the electrical and the telecommunication ones) are considered. Their strong coupling activates dependency mechanisms holding in the short time scale (from a few minutes up to one hour). Coupling of these infrastructures to other CI establishes with a larger latency: during very short times scales, other CI could be considered as "decoupled" from the previously cited infrastructures, in a sort of adiabatic approximation [5]. For this reason, the DSS has divided the Impact evaluation in two stages: for the short time scale the Impacts assessment module resolves the electrical reconfiguration problem described in *Figure 1* as the top of the three steps of Impacts and Consequences estimate.

Modelling the dynamic of a power network and its dependencies with the other systems such as its SCADA system requires a deep knowledge of the electric network model and this task can be extremely complex using mathematical approaches.
Then, we present how our DSS implements an approach to tackle this issue based on simulation of the network topology of the two systems and using forecast results relative to the possible outages of specific substations. We present a procedure that, based on the estimated damages, is able to predict, within a limited time horizon, those substations that, with high probability, may be disconnected from the network due to the possible occurrence of natural threats. In addition, by exploiting the knowledge of the (inter)dependencies between the electrical network and the SCADA system, it detects the electrical substations that can be operated remotely and those that, in turn, would require a manual intervention. The difference in time of the automatic and manual recovery operations required to re-energize specific electrical loads, is used to predict the outage durations of specific substations and ultimately the Consequences of the predicted Crisis Scenario.

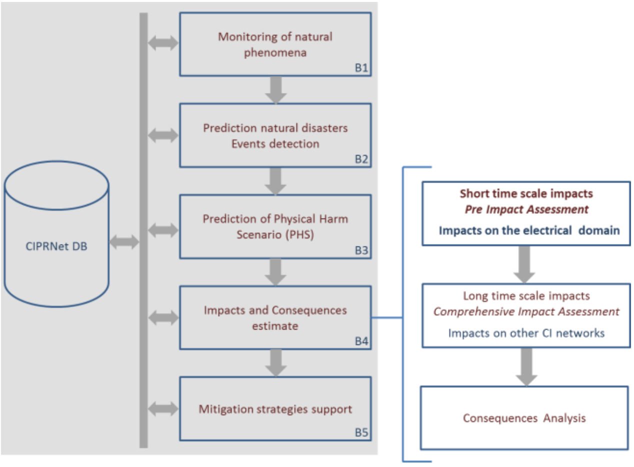

Figure 1. Assessment of short time scale impacts within the CIPRNet DSS

Let us assume to start the analysis from a given PHS, resulting from the B3 block (1). The impact assessment on CI is performed through a two-steps procedure as follows (*Figure 1*):

- Pre Impact Assessment: this procedure analyses the electrical - telecommunication internal dependencies to estimate the availability (or unavailability) of the power network substations depending on the occurrence of threats affecting physical components of the electrical or SCADA system. The outcome of this procedure is the expected outage duration of the electrical distribution substations.
- Comprehensive Impact Assessment: this procedure analyses the dependencies among all the infrastructures (e.g., power grid-water distribution, water distribution-hospital) to have a complete assessment of all the domains considered. This procedure takes as an input the expected outage duration of the distribution substations of the considered scenario calculated in the pre impact assessment block and executes an i2Sim model [2] to evaluate the overall impact on all CI resulting from dependency mechanisms.

The outcome of the impact evaluation is called Impact Scenario (*IS*), defined by a vector containing the set of the variations ΔQ_i of the Quality of Service (QoS) associated to each CI. The *IS* can be generically represented as:

$$\mathrm{IS} = \Delta \mathrm{Q}_1, \dots, \Delta \mathrm{Q}_\mathrm{N} \qquad (2)$$

Based on census data and metrics measuring the vulnerability of the society to the degradation of CI services expressed by the IS, the DSS will estimates the consequences grouped by specific criteria. The outcome of the consequence estimation is called Consequence Estimate (CE). From the electrical grid operator point of view, the CE information can be used in different situations:
1) small crisis scenario,
2) large crisis scenario and
3) electrical gird performance optimization.

A Crisis Scenario can be considered *light* if the available resources to restore the normal network QoS are sufficient and/or the CE values are small. During a light scenario the knowledge of the QoS of the other CI networks and in particular of the other CI components providing services to the electrical infrastructure (as for instance, the fixed and mobile telecommunication network for the electrical infrastructure SCADA system) can be used to further improve the restoration procedures in order to minimize the disconnection time of users and critical loads. During a *severe* crisis scenario, characterized by high values of CE values and/or inadequate available resources for restoration, the DSS output is used to optimize the available resources in order to mitigate the consequences of the crisis. Indeed, in this case, it will not be possible to restore (as in *light* crisis situation) all users and critical loads in an acceptable time. In these cases, the Pre Impact assessment and DSS output in general support the decision-making process. In the end, the CIPRNet DSS can be used as a what-if analysis tool and, in general, CI operators can use the DSS output to drive future network development programs. In this work, we focus on the Pre-Impact Assessment which deals with the short time scale electrical-telecom interaction.

3. Architecture

The aim of the Pre Impact Assessment phase of the risk assessment workflow implemented within the CIPRNet DSS is to obtain the most realistic impacts assessment of a specific PHS on the electrical distribution grid. To this end, it foresees the involvement in the loop of electrical and telecommunication networks operators. This is beneficial for different reasons:

- CI operators have contingency plans to reconfigure their network after failures on one or more CI components;
- Contingency procedures depend on the current configuration of the CI network. Only CI operators have access to the current configuration of their networks;
- Contingency plans and CI network details are considered sensitive data that CI operators would not share and/or distribute.

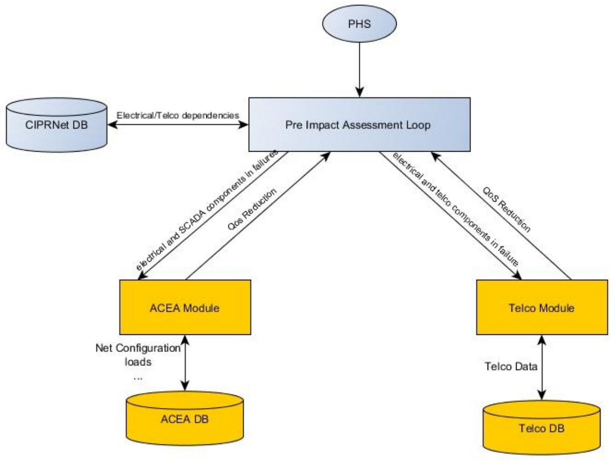

Figure 2. The Pre Impact Assessment Loop

The proposed Pre Impact Assessment Loop (*Figure 2*) starts with the *PHS* data (i.e. the output of B3). Based on the received *PHS*, the application queries the CIPRNet DB containing CI networks dependencies information (the CI network dependencies data represent the minimal requirement for the CIPRNet DB) to find the electrical and telco components directly impacted by the *PHS*. The ACEA and Telco module will then use these information to compute the possible reduction of their QoS. To this end, CI operators will simulate appropriate contingency procedures for the expected networks status. The Pre Impact Assessment Loop will stop once an equilibrium condition is reached (no further variation of networks QoS expected).

The proposed platform for the Pre Impact Assessment phase has been implemented leveraging on the experience gained in the DIESIS [4] project where a federated simulation environment was proposed. In the present work, a simplified version of the isolation and reconfiguration procedures adopted in ACEA and implemented within the ACEA module of *Figure 2* will be described.

4. Implementation

The isolation and reconfiguration algorithm implemented within the electrical module has been developed in collaboration with ACEA. The electrical distribution grid of Rome can be modelled as showed in *Figure 3*.

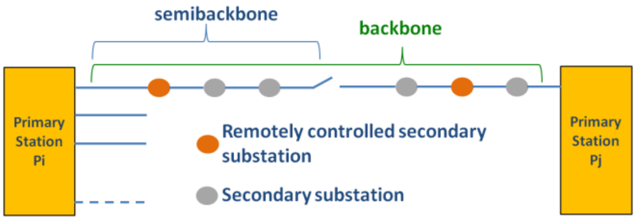

Figure 3. The electrical distribution grid model

The network is composed of a number of *Primary Substations* (*PS*). Each PS originates one (or more) *Medium Tension* (*MT*) semi-backbone(s) ending into a further *PS*. The term "semi" is used as the *MT* line is cut at a certain stage by a switch which decouples the line into two halves, each of them supplied by one of the two overlooking *PS*. Each semi-backbone connects a number of *Secondary Substations (SS)*, some of them being remotely controlled. *SS* on a specific semi-backbone are fed, in the normal configuration, by a specific *PS*. The network can be configured (using the switches showed in *Figure 3*) in a way that the *SS* on a semi-backbone (or a subset of these substations) are fed by the closest *PS* (in *Figure 3*, the PS P_j can be considered the closest primary substation for P_i and vice versa). Each *SS* is modelled as a Finite State Machine as showed in *Figure 4*. In normal condition the SS is in the initial "*FUNCTIONING*" state.
Starting from this state, the secondary substation can move into two different states:

- *FAILURE STATE*: when a failure in the SS occurs, the transition 1 is activated. The SS remains in this state for the expected failure duration (the failure duration is contained in the PHS).
- *NOT FUNCTIONING STATE*: a SS can be in this state after the activation of protection devices. For example, when a SS moves into the *FAILURE STATE* all *SS* on the same semi-backbone move into their *NOT FUNCTIONING STATE*.

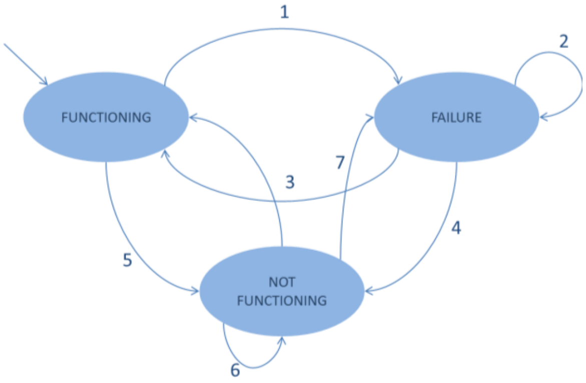

Figure 4 Secondary Substation Finite State model

Figure 5 shows cases that the algorithm needs to consider to compute the *SS* restoration time (the presented cases are not exhaustive).

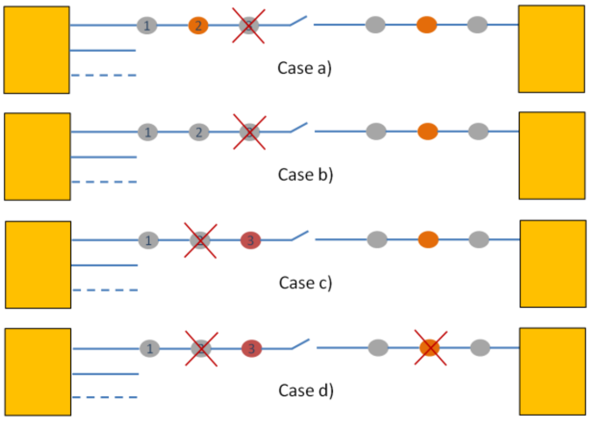

Figure 5. Different cases for the secondary substation restoration

A *SS* remains in this state waiting for restoration. The duration of the restoration can be of a few minutes (about 3-5 minutes) if the *SS* can be tele-controlled or much longer (50-55 minutes to few hours) depending on several factors (e.g., time required by emergency crews to reach the faulted substation and to restore it).

Let us assume that a *t=t1* the electrical substation *SS3* is in *FAILURE STATE*. All *SS* on the same semi-backbone will move into their *NOT FUNCTIONING STATE* starting from *t=t1*.

In *Case a) SS1* and *SS2* can be restored in a few minutes (e.g., 5 minutes): *SS2* can be remotely restored.

In *Case b)* remote control cannot be used so that *SS1* and *SS2* restoration requires a manual procedure performed by emergency crews. The manual restoration of a *SS* would take 50-55 minutes (for real cases, this time can be estimated by historical data of the electric operator), as it could imply the reach of the faulted *SS* (in a complex urban scenario). The other two cases of *Figure 5 - Case c) and Case d)* - require the *closest PS* to restore *SS* on the semi-backbone after the *SS* in failure state. In *Case c) SS3* can be restored using the next *PS*; in addition, considering that as *SS3* is remotely controlled, restoration would take few minutes (e.g., 5). In *Case d)*, the *SS3* cannot be restored using the next primary substation and the restoration duration would depend on the failure duration of the two failures on the backbone.

The implemented algorithm takes into account all possible restoration cases. A simplified sketch of the simulation algorithm of the ACEA restoration procedures is shown in *Figure 6*.

```
1. Read data from DB (Electrical Distribution
   Grid topology, failures)
2. Initialize grid topology data structure
3. Initialize electrical and telco failures data
   structures
4. Initialize simulation constants //start, end
   simulation time, simulation step
5. for (time=0; time<END_SIMULATION_TIME;
   time+=SIMULATION_STEP){
   a. check_telco_failures(time) //check if at
      t=time there are telco components
      entering in the failure state
   b. check_electrical_failure(time) //check if at
      t=time there are  electrical components
      entering in the failure state
   c. update_tlc_status(time)//set tlc status =
      NOT WORKING for those secondary
      substations remotely controlled using a
      BTS that is not functioning (its functioning
      status = NOT WORKING)
   d. update_net(time)//this procedure update
      the state of each secondary substation
 6. }
```

Figure 6. The main simulation loop

The input for the algorithm is constituted by the electrical grid topology, the telecommunication components providing services to the electrical grid SCADA system, mainly Base Transceiver System (BTS) and the *PHS* data. The BTS provides telecommunication services required by the SCADA system of the power distribution stations.

The output is represented by the power profile of the SS during the simulated time slot. After the initialization phase, where the electrical grid topology is loaded from the CIPRNet DB as well as the *PHS* data, the main simulation loop starts. The simulation algorithm introduces a check order of incoming events (i.e. failures).

First, the algorithm checks the state of the BTS. Each BTS is modelled using the model shown in *Figure 7*. In particular a BTS, the procedure *check_telco_failures(time)* (step 5a of *Figure 6*) loops through all BTSs and updates their state accordingly (a BTS in failure moves its status from

FUNCTIONING to FAILURE). The status of the BTSs will influence the functioning status of the electrical grid SCADA system (procedure *update_tlc_status(time)*). Then, (step 5.b of *Figure 6*) the algorithm updates the failure status of the SS. If a SS moves its state from FUNCTIONING to FAILURE the functioning state of the components (e.g. a BTS) powered by the SS will be updated as well.

After the update of the status of the SCADA components (step 5c of *Figure 6*) the simulation loop calls the update_net(time) procedure (step 5d of *Figure 6*). This procedure updates the status of each SS. In particular, the procedure checks if it is possible to restore (i.e. shifts their status to the FUNCTIONING state) all SS that are in the NOT FUNCTIONING state. The update_net(time) procedure takes into account the different possible cases some of them showed in *Figure 5*

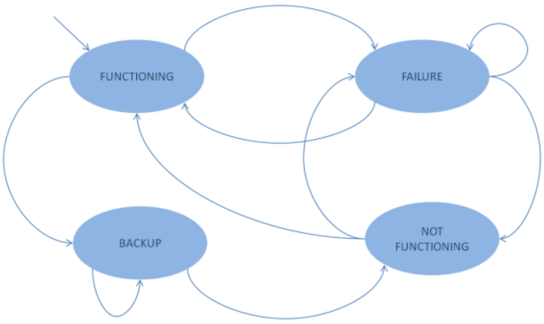

Figure 7. BTS Finite State model

5. The Rome electrical distribution grid test case

A real case study is shown in *Figure 8* where we represented a section of the power distribution grid of an area of the Rome City, consisting of: (i) 9 HT/MT substations (PS); (ii) 154 MT/LT substations (SS); (iii) 6 Telecom BTS and (iv) 3 hospitals. Each PS has a number of backbones consisting of several SS. Some of these may feed Telecom BTS or hospitals in addition to generic users (e.g., households).

The figure shows a possible PHS (all the SS shown in red) i.e., the set of SS estimated to be in failure based on predicted Damages due to the natural events manifestation. Based on the presented reconfiguration procedure, the pre-impact assessment module estimates the IS i.e., the possible evolution of the power network (*Figure 10*) considering the assumption that all the BTS are working properly.

Figure 9 the expected outage duration of the electrical secondary substations that are produced by the pre-impact assessment module.

It can be noticed that, at time t1=0 the DSS estimates that 4 substation will be expected to fail. Then, the algorithm verifies that approximately at time t1=0, 33 substations will be automatically disconnected because of the estimated failures (SS28-SS36, SS49-SS59, SS120-127, SS64-SS68). This behaviour results from the fact that the electrical substations are connected in series configuration.

Considering that some substations can be reconnected through remote operations, the algorithm verifies those BTS that are still receiving power from the secondary substations (we suppose, in the worst case scenario, that BTS do not have electrical backup systems) and that are able to open switches to re-energize the disconnected substations (SS64, SS66-SS68, SS49, SS52, SS56, SS58, SS59, SS120, SS121, SS124, SS125, SS56, SS58, SS59, SS116-SS118, SS114, SS110, SS111, SS107, SS28, SS29).

The algorithm verifies that the failure of the secondary substation SS123 that feeds the Telco BTS07, which, in turn provides remote control to the SS96, has the effect that the semi-backbone SB02 cannot be connected (through the closure of the switch located in SS96) to SS36, leaving several substations in the semi-backbone SB02 in a failure state. This behavior is shown in *Figure 10* at time t=5 where 12 substations cannot be reconnected through remote control (SS30-SS36, SS53-SS55, SS122, SS123, SS65). The figure also shows that, without the dependency information among the substations and the BTS, the decision makers (e.g., an electric operator) receiving only the information of the possible damaged substations may not be able to infer that “additional” substation could be affected due to the failure of the BTS.

In addition, the information provided can also be used to plan an effective intervention of crewmen that be sent to the affected substation in a sequence that minimizes the overall number of the affected substations or the number of affected electric consumers.

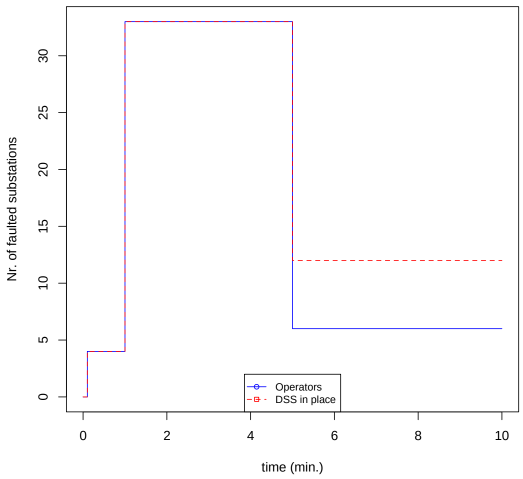

Figure 9. Estimated substations in failure state

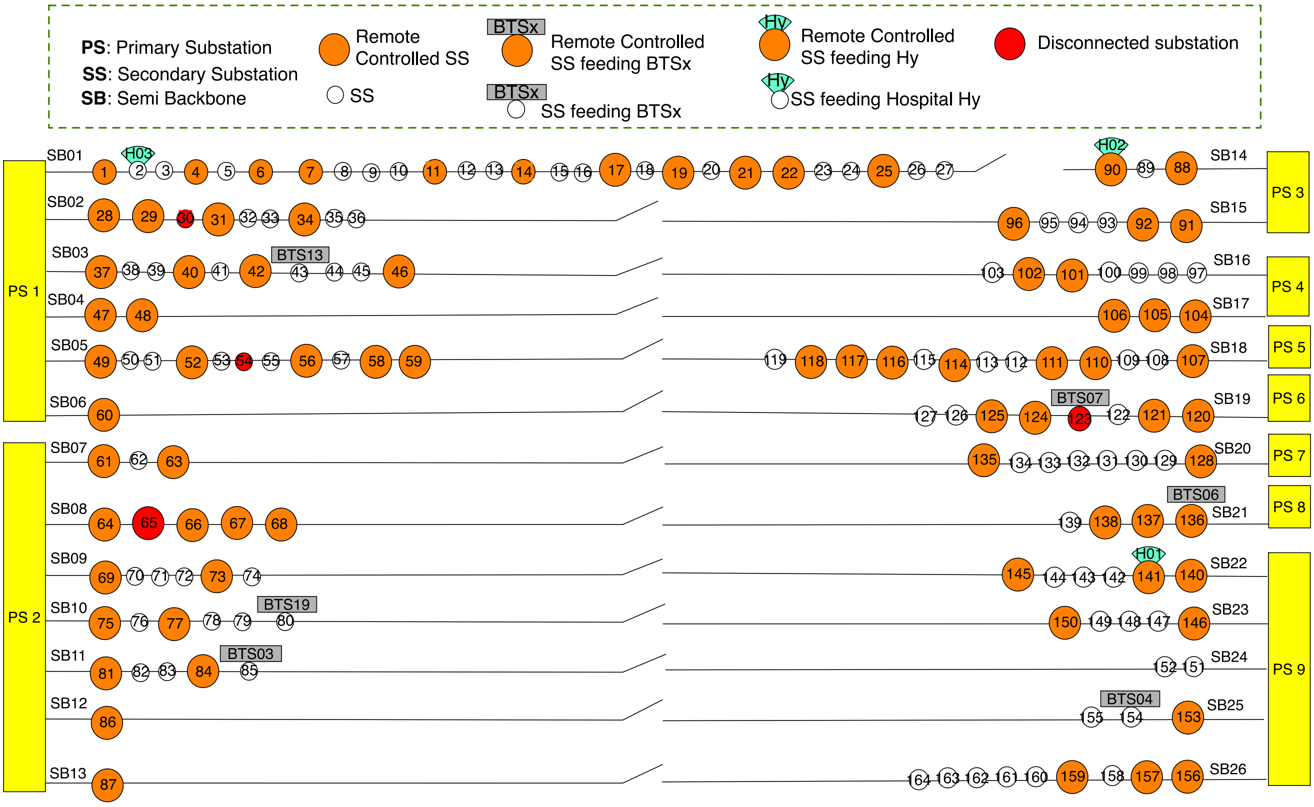

Figure 8. Represtantion of a section of a power distribution grid of Rome. Rome scenario at time t=t1

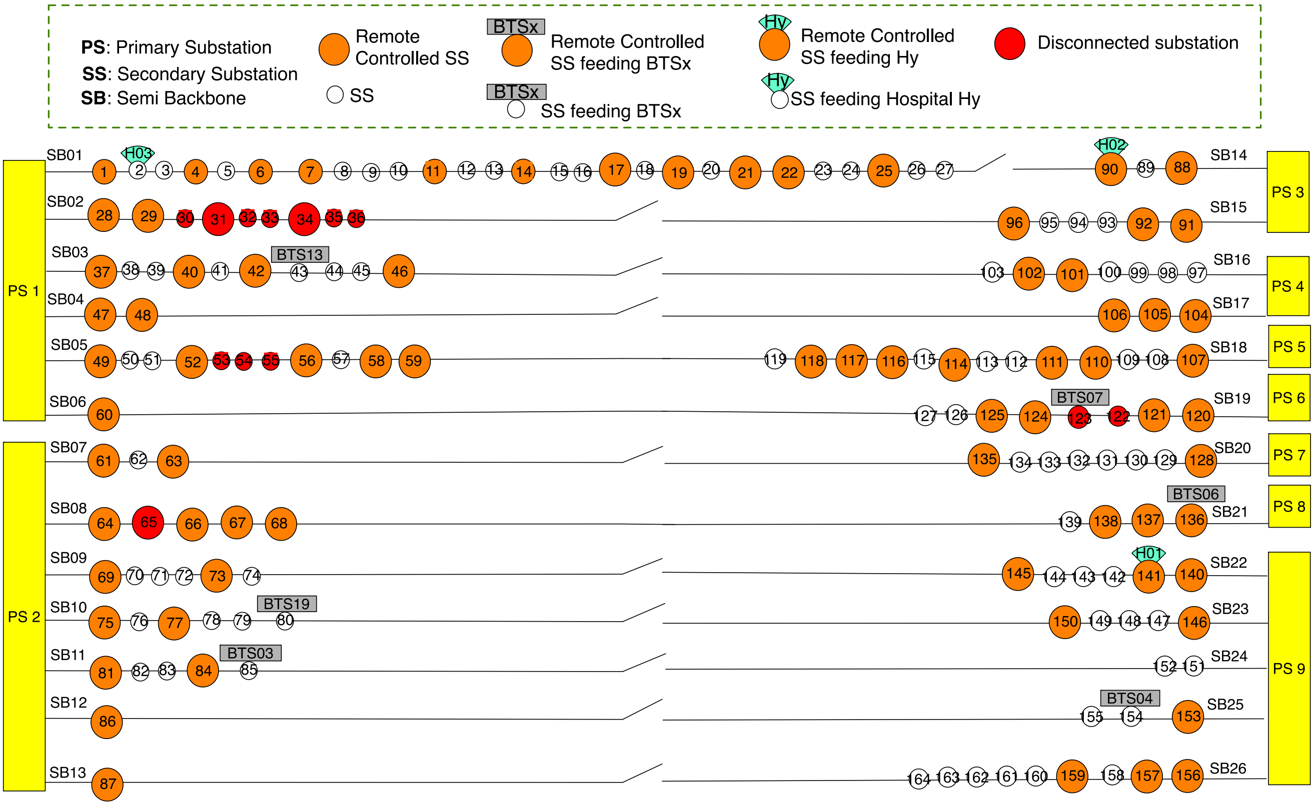

Figure 10. Rome scenario at time t=t2 (hypothesis: BTS are working properly)

The expected outage duration of the electrical secondary substations is provided to the Comprehensive Impact Assessment module based on I2Sim that subsequently evaluates the resulting impacts on the other infrastructures present in the scenario. This outcome, i.e., the Impact Scenario together with census data available for the city of Rome, feeds specific metrics able to estimate the effects on the different societal Criteria to the predicted reduction or loss of Services.

These information may be useful for decision makers to know, during crisis scenarios that in a specific area there might be a high concentration of citizens (e.g., old aged people, disabled people) that may be severely affected by the different outages of primary services (e.g., water, gas) resulting as cascading effects of the unavailability of electric power.

6. Conclusion

This work shows how the DSS, currently under development within the EU FP 7 CIPRNet project, attempts to solve the full risk analysis workflow, from events prediction to impacts and consequences estimation of a Critical Scenario. In this work, we described a core component of this system i.e., the pre-impact assessment module able to estimate the possible effects of specific natural threats to the electrical infrastructure. Indeed, the reduction of the quality of services of the electrical infrastructure may produce negative effects on all human activities and the societal life in general. This module constitutes the bases for a comprehensive impacts and consequences assessment. Moreover, we showed, using a test case, how the electrical grid operators can benefit from the outcome provided by this approach which considers, among others, (inter)dependencies among the electric and SCADA networks. Future works will focus on the application of this approach to estimate the best strategies that minimize the consequences of a crisis.

Acknowledgements

This work was developed within the FP7 Network of Excellence CIPRNet, which is being partly funded by the European Commission under grant number FP7- 312450-CIPRNet. The European Commission support is gratefully acknowledged. The authors wish to thank Prof. Josè Marti (UBC Vancouver) who provided valuable comments and support for the design of the model.

References

[1] European Commission, COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Brussels, December 8, 2008.

[2] Hafiz Abdur Rahman, M. Armstrong, DeTao Mao, and Jose R. Marti. I2sim: A matrix-partition based framework for critical infrastructure interdependencies simulation. In Electric Power Conference, 2008. EPEC 2008. IEEE Canada, pages 1–8, Oct 2008. doi: 10.1109/EPC.2008.4763353.

[3] Petermann, T., Bradke, H., Lallmann, A., Poetzsch, M. & Riehm, U. (2011). What happens during a blackout. Consequences of a prolonged and wide-ranging power outage. Technology Assessment Studies Series – 4. BoD Books on Demand. Norderstedt pp 260.

[4] Tofani, A., Castorini, E., Palazzari, P., Usov, A., Beyel, C., Rome, E. & Servillo, P. (2010). An Ontological Approach to Simulate Critical Infrastructures. *Journal of Computational Science* Volume 1, Issue 4, December 2010, Pages 221-228.

[5] Van Eeten M., Nieuwenhuijs, A., Luiijf, E., Klaver, M., & Cruz, E. (2011). The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports. Public Administration, 89(2): 381–400.