Accepted for publication in Reliability Engineering and System Safety

Analyzing the topological, electrical and reliability characteristics of a power transmission system for identifying its critical elements

E. Zio[1,2], L.R. Golea[2]

[1]*Ecole Centrale Paris- Supelec, Paris, France*

[2]*Politecnico di Milano, Milano, Italy*

*corresponding author: enrico.zio@ecp.fr, enrico.zio@supelec.fr, enrico.zio@polimi.it

Abstract

The subject of this paper is the analysis of an electrical transmission system with the objective of identifying its most critical elements with respect to failures and attacks. The methodological approach undertaken is based on graph-theoretical (topological) network analysis. Four different perspectives of analysis are considered within the formalism of weighed networks, adding to the purely topological analysis of the system the reliability and electrical characteristics of its components. In each phase of the analysis: i) a graph-theoretical representation is offered to highlight the structure of the most important system connections according to the particular characteristics examined (topological, reliability, electrical or electrical-reliability); ii) the classical degree index of a network node is extended to account for the different characteristics considered. The application of these concepts of analysis to an electrical transmission system of literature confirms the importance of different perspectives of analysis on such a critical infrastructure.

Keywords: critical infrastructures, vulnerability assessment, electrical transmission system, network analysis, reliability, connectivity degree

1. Introduction

Engineered critical infrastructures are the systems of interest in this work. The motivation is that they provide the continuous flow of essential goods (e.g. energy, water, data) and services (e.g. banking, health care, transportation) which the welfare and security of our nations rely on. These critical infrastructures are subject to a set of multiple hazards and threats which must be identified and analyzed for optimal protection.

Among the engineered critical infrastructures, the focus of this work is on the electrical transmission system and its analysis to identify the importance of the individual elements. The motivation is that the infrastructure for electrical transmission of most of the world's countries is aging and failing, with funding often not sufficient to repair or replace it; in this situation, there is a growing demand for a rational, risk-based approach to its operation and maintenance.

A number of recent studies have addressed the assessment of vulnerability in electric power systems, by graph-theoretical topological investigations as in [1]-[5], physics-based models as in [6]-[9], agent-based modeling as in [10]. These studies all refer to the transmission system and are based on different conceptualizations of vulnerability [11]. Also, more sophisticated techniques such as polyhedral dynamics [12] and artificial intelligence-based search methods [13], [14] have been proposed to find critical elements and define vulnerability indices.

The topological approach to vulnerability analysis is quite popular because in spite of its relative simplicity it offers the capability of identifying elements of structural vulnerability, i.e. network edges and nodes whose failure can induce a severe structural damage to the network through the physical disconnection of its parts. However, the methods based on such approach are limited from the point of view of the physical analysis of the electrical transmission systems, which the graphical networks represent; the limitations come from the fact that the analysis focuses only on the topological features of the network, thus neglecting its physical characteristics [15]-[17]. In this respect, it is important to verify the extent of these limitations and possibly overcome them by complementation with more detailed physical analyses on critical parts of the network [18], [19].

In this paper, the formalism of weighed networks is exploited to provide different graph-theoretical representations and analyses of a power transmission system. The aim is to contribute to reducing the gap between the highly conceptualized (and abstract) analyses based purely on considerations of the system topology and the highly detailed (and computationally demanding) simulations of system behavior, in order to render the overall vulnerability assessment more feasible and robust. The "weights" appended to the network elements are intended to capture relevant electrical and reliability properties of the system, so as to overcome the classical simplifying but unrealistic assumption that electrical flow occurs along the shortest and failure-free paths of connections.

The rest of the paper is organized as follows: Section 2 describes the theoretical basis for the proposed perspectives of analysis. In Section 3, the work is presented from a practical point of view with reference to the popular IEEE RTS 96 system [20]. Section 4 contains a critical comparison of the four perspectives of analysis with an outlook on other perspectives. Conclusions are drawn in Section 5.

2. Different perspectives of analysis

In the present study, the system is modeled as a stochastic, weighted, undirected, connected network in which each electric bus is transposed into a node, linked by edges representing the overhead lines connecting consecutive buses. In this respect, this representation focuses on the actual topological structure of the power transmission network.

Mathematically, the topological structure of the network can be represented as an undirected graph $G(V,E)$ where V represents the set of vertexes (or nodes, or components) ($N=\dim(V)$ is the number of nodes) and E represents the set of edges (i,j) ($K=\dim(E)$ is the number of edges).

The connections are specified in an $N \times N$ adjacency matrix $\{a_{ij}\}$ whose entries are 1 if there is an edge joining node i to node j and 0 otherwise.

2.1. Graph-theoretical topological analysis

The transmission network is first analyzed from a purely topological point of view. In the topological representation, no specification of the physical length of the edges is given. Each link is considered having a length equal to one and thus the distance between two nodes i and j is represented solely by the number of edges travelled in the path from i to j. On the basis of $\{a_{ij}\}$, it is possible to compute the matrix of the shortest path lengths $\{d_{ij}\}$ whose generic entry d_{ij} is the number of edges making up the shortest path linking i and j in the network. The fact that G is assumed to be connected implies that d_{ij} is positive and finite $\forall i \neq j$ and that there are $N(N-1)/2$ distinct shortest paths among the N nodes.

From the matrix of shortest path lengths $\left\{d_{ij}\right\}$, a new matrix $\left\{s_{ij}\right\}$ can be computed by considering connected only a number of K_S links with smallest values of shortest path lengths; the generic element s_{ij} is equal to 1 if the shortest distance connecting i and j is one of the K_S smallest values and 0 otherwise.

A synthetic indicator of the topological structure of a complex network is the distribution of the degree (or connectivity) k_i of its nodes $i = 1, 2, ..., N$, the degree being defined as the number of edges incident to the node [21]:

$$k_i = \sum_{j \in N} a_{ij}, \; i = 1, 2, ..., N \tag{1}$$

Intuitively, the degree of a node measures its influence in the graph with respect to the size of its immediate environment.

2.2. Reliability analysis

While some studies witnessed a reasonable association between the topology of the power grids and the robustness and stability of the power transmission systems [1], [22], [23], the relationship between network structure and system reliability is also of relevance. In this respect, the formalism of weighted networks [22] can be undertaken to account for the reliability properties of the transmission network system. More precisely, a reliability matrix $\{p_{ij}\}$ can be introduced to describe the network reliability properties at a local level [24]; the generic element p_{ij} represents the probability of successful transmission along the edge that connects node i and j.

Since the graph is not fully connected, the reliability matrix tends to be sparse (p_{ij}=0 for all pairs of nodes i and j that do not share a direct physical connection). In order to obtain a non-sparse matrix containing the complete information on the reliability of connection between any two pairs of nodes, the reliability $p_{\gamma_{ij}}$ of connection between i and j through any connecting path γ_{ij} is computed by a method based on a combination of cellular automata (CA) and Monte Carlo (MC) sampling [25]. In this method, the reliability $p_{\gamma_{ij}}$, i.e. the probability of a successful connection from i to j, is computed by MC – sampling a large number M of random realizations (MC trials) of the states of the connecting arcs and by CA-computing, for each realization, if a path from i to j exists; the ratio of the number of successful γ_{ij} paths over the total number of realizations computed gives the connection reliability from node i to node j.

As indicator of the importance of the nodes from the reliability point of view, a reliability degree can be introduced as:

$$k_i^r = \sum_{j \in N} p_{\gamma_{ij}}, \; i = 1, 2, ..., N \tag{2}$$

From the reliability analysis, a matrix $\{s_{ij}^r\}$ is computed on the basis of the K_S most reliable paths. The matrix element s_{ij}^r is equal to 1 if the connection from node *i* to *j* is one of the K_S most reliable connections, and 0 otherwise. $\{s_{ij}^r\}$ can be thought of as the reliability equivalent of the topological adjacency matrix $\{a_{ij}\}$.

2.3. Electrical analysis

As mentioned in the Introduction, in the case of electrical transmission networks of interest here, the existing literature on vulnerability analysis largely takes a topological approach to identify the critical components in the network [1], [26], [5]. Even though such analyses are capable of identifying elements of structural vulnerability, they are limited from the point of view of the physical analysis of the electrical transmission system, which the networks represent. These limitations are all related to the fact that the analysis performed focuses only on the topological features of the network, thus neglecting its physical characteristics; this is not realistic for electrical transmission networks in which: i) the "electrical" length of a path differs from the topological length, depending on the difficulty (resistance) of transmission; ii) the electrical power is not necessarily routed through the shortest paths: rather, the transmission of power is determined by physical rules, e.g. Kirchoff's laws, nodal voltages etc.

To practically overcome these limitations, an electrical connectivity metric was introduced within the weighed network formalism to capture the properties of node centrality, relative to metrics based on node-edge connectivity [16].

The electrical characteristics of the individual network elements and their interconnection relationships can be expressed in terms of the bus admittance matrix, Y^{bus}. Inverting the sparse bus admittance matrix ($Y_{ij}^{bus} = 0$ for all pairs of nodes *i* and *j* that do not share a direct physical connection) that incorporates Kirchoff's laws, a non-sparse matrix, known as impedance matrix, can be obtained.

The matrix of electrical distances is then given by the magnitude $\{m_{ij}\}$ of the entries of the matrix Z^{bus}. Admittance is a complete expression of the extent to which a circuit allows a current to flow; as the absolute value of the complex admittance becomes larger, the absolute value of the complex impedance becomes smaller and therefore smaller $m_{ij} = |Z_{ij}^{bus}|$ correspond to shorter electrical distances [16].

The shortest K_S electrical distances, which can be used to define a matrix $\{s_{ij}^e\}$ analogous to the previous matrixes $\{s_{ij}\}$ and $\{s_{ij}^r\}$: the matrix element s_{ij}^e is equal to 1 if the connection from node *i* to *j* is one of the K_S values, and 0 otherwise. The computation of the connection distances between nodes *i* and *j* takes into account all possible paths between nodes, as in the case of the reliability analysis, and not only the shortest paths, as in the topological analysis.

Based on the electrical information contained in the Z^{bus} matrix, an indicator of the importance of the nodes can be introduced as:

$$k_i^e = \frac{1}{\sum_{j \in N} m_{ij}},\ i = 1, 2, ..., N \tag{3}$$

The electrical centrality measure of interest to electrical engineers introduced in [16] and repeated in the paper quantifies that the importance of a substation as being inversely proportional to the Thévenin equivalent circuit seen in the substation. In other words, the electrical equivalent distance (Z Thévenin) between the generation nodes and the substation determines its importance. Thus, the importance of a substation is represented by its maximum level of short circuit power. Choosing

this criterion to identify the importance of a node or substation in a power system implies depending on the number of the operating generators (node admittance). Therefore, the adopted definition of node importance accounts also for the actual generation dispatch.

2.4. Electrical-reliability analysis

As the physical reliability and electrical properties of the transmission network act together in shaping the behavior of the system, an analysis more complete than the previous ones would be one that combines the reliability and electrical characteristics together. In this view, a electrical-reliability distance can be associated to each pair of nodes *ij*, i.e. the product between the reliability $p_{\gamma_{ij}}$ of connection between *i* and *j* and the corresponding electrical distance m_{ij}.

The K_S shortest connections define a matrix $\left\{s_{ij}^{er}\right\}$, where the generic element s_{ij}^{er} is equal to 1 if the connection from node *i* to *j* is one of the K_S values, and 0 otherwise.

As an indicator of the importance of nodes from the electrical and reliability point of view, the electrical- reliability degree can be defined as:

$$k_i^{er} = \frac{1}{\sum_{j \in N}\left(m_{ij}\, p_{\gamma_{ij}}\right)},\ i = 1, 2, ..., N \tag{4}$$

As an alternative to the electrical-reliability degree, the expected electrical distance could be used to evaluate the importance of different network components. This measure is computed as:

$$e_i = \sum_{j \in N}\left(m_{\gamma_{ij}}\, q_{\gamma_{ij}}\right),\ i = 1, 2, ..., N \tag{5}$$

where $q_{\gamma_{ij}}$ is the probability of different combinations of failures when multiple γ_{ij} paths between the pair of nodes *i* and *j* exist, and $m_{\gamma_{ij}}$ is the electrical distance corresponding to the γ_{ij} path.

As previously stated, the measure based on electrical distances is relevant also for dispatching problems aimed at reduction of power losses. In the context of the electrical – reliability analysis where short-term contingencies and supply continuity are the crucial factors, a complementary measure could be obtained by combining the reliability of lines together with the corresponding maximal transmission capacity.

The further development of these indicators is beyond the purpose of this paper.

3. Results and discussion

Let us consider the power transmission network system IEEE RTS 96 of Figure 1 [20]. The network consists of 24 bus locations connected by 38 lines and transformers. Some edges (4 out of 38) are constituted by double physical lines; for the purpose of the analysis, however, they are treated as a single edge of communication so that effectively $K = 34$. The corresponding graph is shown in Figure 2.

3.1. Graph-theoretical topological analysis

Obviously, in the case of $K_S = K = 34$ the smallest values in the matrix of the shortest path lengths are equal to 1, and correspond to the direct physical connections, i.e. $\left\{s_{ij}\right\} \equiv \left\{a_{ij}\right\}$ (Figure 2).

The first column of Table 1 reports the ranking of the nodes based on the values of their degree. As defined in Eq. (1), the most important nodes from a degree point of view have the largest number of connections to other nodes in the network; thus, nodes 9 and 10, characterized by the largest number of incident edges (five) are placed in the first position of the topological ranking; on the contrary, node 7 with only one connection, falls in the last position of the ranking.

3.2. Reliability analysis

Table 2, third column lists the $K_S = 34$ most reliable connections, which can be used to define a matrix $\left\{ s_{ij}^r \right\}$ analogous to $\left\{ s_{ij} \right\}$ defined on the basis of the smallest values of shortest path lengths in the topological analysis. The matrix element s_{ij}^r is 1 if the connection from node *i* to *j* is one of the $K_S = 34$ listed in Table 2, first and second column; it is 0 otherwise. The representation of the connection pattern of the 34 most reliable paths is shown in Figure 3, with the node size proportional to the number of incident edges. It can be seen that the most reliably-connected nodes do not necessarily share a direct physical connection.

The reliability-driven representation of the network connectivity shows a different pattern than the topological one; this is due to the fact that the computation of the reliability of the connection from node *i* to *j* takes into account all the possible paths linking nodes *i* and *j*, not just the shortest topological one. This conceptual representation of the network shows that there are several hubs identified as important from the reliability point of view: they are traversed by the majority of the most reliable paths.

The most reliably connected area is found to be the central part of the network, concentrated around nodes 9, 10, 11 and 12 (which have also the highest degree, as reported in Table 1), due to direct physical connections, i.e. edges 9-11, 10-11, 9-12, and indirect connections, i.e. 9-10 and 11-12. On the other hand, several nodes appear to be disconnected from the network, forming clusters of size one or two. Based on these findings, the network could be made more robust by increasing the reliability of these clusters of critical hubs.

Table 1, third column, provides the ranking of the reliability degree for each node. Nodes 9, 10, 11 and 12 have the most reliable connections. The ranking is similar to the one obtained with the topological degree (Table 1, first column), with nodes 9, 10, 11 and 12 being the most important (reliable), and nodes 7 and 24 the least. This points to a strong correlation between the network structure and the system reliability due to the large values of connection reliability $p_{\gamma_{ij}}$.

3. 3. Electrical analysis

Table 2, column five provides the most important paths with respect to the electrical distance. The edge 7-8 was identified as the most important, i.e. having the shortest electrical distance and therefore a larger propensity for power to flow between its connecting nodes. The tendency of power to flow through this edge is a consequence of the network's structure; as it can be seen from Figure 1, node 7 is a generator connected to the rest of the network only by node 8. As in the reliability case, both direct physical connections, i.e. edges 7-8 and 1-2, and indirect connections, i.e. 18-22 and 17-21 are ranked as the most important connections.

Figure 4 shows the connection pattern realized by the 34 shortest electrical paths. The resulting graph has the same size as the original network in Figure 2 (24 nodes and 34 edges), and the node size is proportional to the number of incident edges. The electrical representation of the network suggests a very different structure with respect to the topological and the reliability perspectives. The most vulnerable area from an electrical perspective is the north-west side of the network, where the power flow concentrates due to Kirchoff's Laws. Indeed, this area contains several important generators (i.e. nodes 15, 16, 18, 21 and 22), and therefore there is a strong exchange of power among the nodes. These electrical hubs appear to be potentially more vulnerable with respect to faults or malicious attacks than the other network nodes.

Table 1, fifth column provides the ranking of the nodes with respect to the electrical degree and shows a different prioritization of the network nodes with respect to the topological and reliability degrees. Nodes 18, 17 and 21 are identified as the most important from an electrical point of view, having the highest degree of electrical connectivity. They are ranked as being the most vulnerable because power is more likely to flow through these electrical hubs. In spite of that, they have small

reliability degrees (Table 1, forth column), which expose the network to potential severe outages. On the contrary, node 7 is among the less critical nodes according to the electrical degree, and consistently, it has the smallest reliability degree.

3.4. Electrical-reliability analysis

The electrical-reliability representation of the connection pattern of the 34 most reliable electrical paths is shown in Figure 5, with the node sizes adjusted according to the number of incident edges. The most important edge from the electrical and reliability point of view is 7-8, which also represents a physical connection of the electrical transmission network analyzed (Figure 1). This edge, ranked as first in Table 2, sixth column is characterized by the smaller electrical distance ($m_{78} = 0.1030$) and a relatively small reliability of 0.7409.

Figure 5 suggests that the majority of the most vulnerable paths are those connecting the south-east and the north sides of the network through nodes 7 and 22; these paths are characterized by small values of the electrical-reliability distance. Some of the $K_S = 34$ connections include also paths with short electrical distance and average reliability, located in the north area of the network system.

Table 1, seventh column provides the ranking of the network nodes with respect to the reliability and electrical properties of the network, which bears resemblance to the reliability ranking (Table 1, third column). This fact suggests that the reliability (and structural) characteristics have a larger influence upon the vulnerability of the network than the electrical characteristics. In this view, node 7 having the smallest reliability degree (Table 1, forth column) and a relatively large electrical degree (Table 1, sixth column) is ranked among the most critical nodes (Table 1, eighth column). Nonetheless, the reliability-electrical analysis highlights criticalities complementary to the electrical analysis. In particular, node 16, characterized by a relatively large reliability degree (Table 1, forth column) and large electrical degree (Table 1, sixth column) is ranked among the critical nodes when combing the two characteristics (Table 1, eighth column).

From this perspective, the core made of nodes 9, 10, 11 and 12, concentrated in the central part of the network, is found to be the most robust, with node 10 having the smallest electrical-reliability degree. On the contrary, the north side of the network appears to be the most vulnerable, with nodes 17, 18 and 22 placed in the first positions of the electrical-reliability ranking.

4. Choosing among the perspectives

The four perspectives on network analysis can be framed into the broader scenario of risk analysis against random failures and malevolent attacks [27]-[30]. In this view, a comparative evaluation is proposed to determine which perspective to choose for a given circumstance. Table 3 provides a starting point for choosing among several perspectives on network analysis based on mutual comparison criteria [31], [32].

The major drawback of the purely topological analysis is that it relies solely on the network structure to assess the connectivity performance and nodes importance, and does not consider any physical properties nor system dynamics (first three columns of Table 3). By considering the connections reliability among the nodes based on the failure probabilities of the edges, the reliability-driven representation highlights the most reliable indirect connections, and the most reliably connected areas of the network.

Nevertheless, the topological and reliability analyses fail to explicitly incorporate the physical laws governing the electrical flow. An electrical- or electrical-reliability-driven representation of the network indeed highlights the electrical hubs that appear to be more vulnerable, due to the smaller electrical- or electrical-reliability distances of the paths that traverse them. The incapacitation of these vulnerable paths causes the electrical flow to be routed along alternative paths, possibly triggering cascades of overloads and extensive blackouts.

The quantification of system vulnerability indicators and the identification of its critical elements are the two main outputs of a vulnerability assessment. While providing complementary information, vulnerability indicators are parameters encompassing the static and/or dynamic characteristics of the whole system, whereas the identification of critical elements comes from their ranking with respect to their individual connectivity efficiency and/or their contributions to the propagation of failures, with their effects, through the system [33].

To properly quantify the importance and criticality of the network components, various weighted indicators can be defined as complements to the topological indicators. From a topological viewpoint, various measures of the importance of a network element (edge or node) can be found in the literature [34]. This centrality measures can be further extended by considering suitable connections weights to identify the critical components with respect to the reliability and the electric features [35] of the networks components. By further considering the 'reliability distances' or the 'electrical-reliability distances' among network nodes in terms of the probabilities of failure of the interconnecting links, or in terms of a combination of the reliability and the electrical properties of the links, vulnerability indicators can be defined for use in the analysis of the robustness of network systems.

The 'data needs' criterion refers to the quantity and quality of input data needed to properly perform the analysis. By associating the high scale to the electrical and electrical- reliability analysis we consider that this approaches strongly depend on a high quantity and quality of input data to provide reasonable outputs. On the contrary, graph-theoretical and reliability analyses rely on a minimum amount of information such as the adjacency matrix and the failure rate of the lines.

The level of maturity of each perspective can be measured by the amount of available literature review [31]. Many application examples are found in scientific literature for the graph-theoretical and the electrical analysis so we assume a high level of maturity. On the contrary, a poor level of maturity is assigned to the electrical-reliability perspective due to the scarce experience in this field. We assume for the reliability analysis a middle level of maturity.

Complexity criteria takes into account the difficulty of the algorithms and programs of the respective methodological approach. Two levels of complexity can be distinguished: a low level of complexity assigned to the graph-theoretical perspective due to the simplicity of the algorithms necessary to perform such an analysis and a medium level of complexity for the remaining perspectives.

The 'requested time' criterion describes the effort employed in developing the algorithms for the analysis, and the simulation speed. A low level can be assigned to the graph-theoretical and reliability analyses because of the relative small amount of time needed to build-in the algorithms and a fast simulation speed, while we assume a medium level for the other two analyses.

A number of alternative approaches for the vulnerability assessment of electrical networks have been reported in Table 3, fifth to eight row [32]. The choice of the suitable approach depends on the type of system, the objective of the analysis, and the available information. For example, statistical analysis [36] is suitable when rich data sets about the system operation and performance are available. It is characterized by a high level of maturity and low level of complexity. However, the structure of the network under analysis may be hidden by the fact that the data are often presented in an aggregate form [37], [38]. Moreover, the effective use of the sets of data is difficult because they come from a variety of past operating conditions that may not fully reflect the situations of interest at present and in the future.

Probabilistic risk assessment is another mature methodology that can be applied for analyzing network systems [39], [23]. It integrates deterministic and stochastic tools to carry out a systematic and structured evaluation of the risk associated with every life cycle aspect of a complex engineered technological system, which may lead to undesired consequences triggered by an accident initiating event. The disadvantages of this methodology arise from its complexity that leads to significant efforts in logic modeling and quantification, and from the limited capability of providing an exhaustive analysis.

Agent-based modeling (ABM) is also a suitable approach, particularly useful for situations with sparse or non-existent macro scale information. ABM is able to use the rich sources of micro-level data to develop interaction forecasts. The main disadvantages of these simulation models lie in the complexity of the computer programs, which tends to obscure the underlying assumptions, and in the inevitable input subjectivity. The high level complexity leads also to a high level of requested time.
Object-oriented modeling offer also an attractive modeling paradigm for describing the dynamic network behavior [40]. One of the major advantages of an object-oriented approach is the possibility to include physical laws into the simulation. The level of modeling detail offered by the object-oriented approach allows analyzing a multitude of time-dependent availability aspects. The main problems are related to the slow simulation speed and the large number of parameters to be input in the analysis [18]. However, by focusing on specific safety aspects, the model can be simplified and the computational burden reduced.
Based on this comparative evaluation, we propose a framework of analysis that incorporates the four perspectives presented in this work to be used as a preliminary screening analysis of the network vulnerabilities. This is reasonable since the first step in a general risk assessment is represented by the system characterization [41], [42]. By performing such an analysis a better comprehension of the system is achieved, and the different criticalities within the network components are highlighted. Such framework could be used as a starting point for a more detailed analysis, focused on the previously identified critical components.

5. Conclusions

In this paper, the analysis of an electrical transmission network system has been undertaken with the objective of identifying the critical components, within a vulnerability assessment frame of work. The electrical transmission network IEEE RTS 96 has been taken as reference to present the development of the analysis from four different perspectives: topological, reliability, electrical and electrical-reliability.
For each perspective, the structure of the most important system connections has been identified, and an extended degree index has been computed for the nodes based on this structure. The three weighted indicators quantify the importance of the network components with reference to the role played by the observed characteristic (topological, reliability, electrical or electrical-reliability).
A comparative evaluation of the four perspectives also with respect to other approaches for the vulnerability assessment was performed and a mechanism for choosing among them was provided.
In particular, we found that the reliability analysis identifies the clusters of critical hubs whose reliabilities have to be enhanced to ensure network robustness against random failures. Moreover, the electrical analysis ranks as vulnerable the buses that are traversed by the greater part of the power flow. These electrical hubs are more vulnerable to faults or malicious attacks because their malfunctions lead to a large redistribution of power to other electrical routes. By comparing the reliability and the electrical analyses, we were able to find inconsistencies in the network design. Namely, nodes with large electrical degree have small reliability degrees, which expose the network to potential severe outages. Therefore, we suggest network modifications that increase the reliability degree of the nodes which have a large electrical degree.

Acknowledgements

This work has been partially funded by the Foundation pour une Culture de Securite Industrielle of Toulouse, France, under the research contract AO2006-01.

References

[1] Albert, R., Albert, I., Nakarano, G.L. (2004). Structural vulnerability of the North American power grid, Phys.Rev.E, vol 69, pp 025103-4.

[2] Crucitti, P., Latora, V., Marchiori M. (2004). A Topological Analysis of the Italian Electric Power Grid, Physica A Vol. 338, pp. 92-97.
[3] Holmgren A. J. (2006). Using graph models to analyze the vulnerability of electric power networks, Risk Anal; 26:955-69.
[4] Jonsson, H., Johansson, J., Johansson, H. (2007). Analysing the vulnerability of electric distribution systems: a step towards incorporating the societal consequences of disruption. Int J Emerg Manage; 4:4-17.
[5] Zio, E., Petrescu, C.A., Sansavini, G. (2008) Vulnerability analysis of a power transmission network, Proceedings of PSAM9 - International Probabilistic Safety Assessment and Management Conference, Hong Kong , China.
[6] Yu, X., Singh, C. (2004). A practical approach for integrated power system vulnerability analysis with protection failures, IEEE Trans Power Syst; 19:1811-20.
[7] Doorman, G., Uhlen, K., Kjolle, G. H., Huse, E. S. (2006). Vulnerability analysis of the nordic power system, IEEE Trans Power Syst; 21:402-10.
[8] Nedic, D. P., Dobson, I., Kirschen, D. S., Carreras, B. A., Lynch, V. E. (2006). Criticality in a cascading failure blackout model, Electr Power Energy Syst; 28:627-33.
[9] Koonce, A. M., Apostolakis, G.E., Cook, B.K. (2007). Bulk power risk analysis: Ranking infrastructure elements according to their risk significance, Int J Electr Power Energ Syst, doi:10.1016/j.ijepes.2007.06.013.
[10] Schläpfer, M., Kessler, T., Kröger, W. (2008). Reliability Analysis of Electric Power Systems Using an Object-oriented Hybrid Modeling Approach, in Proceedings of the 16th Power Systems Computation Conference, Glasgow.
[11] Vaurio, J. K., Tammi, P. (1995). Modelling the loss and recovery of electric power, Nuclear Engineering and Design, Volume 157, Issues 1-2, Pages 281-293.
[12] Degtiarev, K. Y. (2000). System analysis: mathematical modelling and approach to structural complexity measure using polyhedral dynamics approach, Complexity International, http://www.complexity.org.au/.
[13] Salazar, D., Rocco, C. M., and Galván, B. J. (2006). Optimization of Constrained Multiple-Objective Reliability Problems Using Evolutionary Algorithms. Reliability Engineering and System Safety, Vol. 91(9):1057-1070.
[14] Cadini, F., Zio, E., Petrescu, C. A. (2009). Optimal expansion of an existing electrical power transmission network by multi-objective genetic algorithms, Reliability Engineering & System Safety, Article in press.
[15] Bompard, E., Napoli, R., Xue, F., Masera, M. (2008). Assesment of structural vulnerability for power grids by network performance based on complex networks, Third International Workshop on Critical Information Infrastructure Security, CRITIS 2008.
[16] Hines, H. and Blumsack, S. (2008). A Centrality Measure for Electrical Networks, Proceedings of the 41st Hawaii International Conference on System Science.
[17] Zio, E., Golea, L.R. (2009). Identification of betweenness-central groups of components in a complex network infrastructure by genetic algorithms, accepted, ESREL Safety and Reliability for Managing Risk, Prague, Czech Republic.
[18] Eusgeld, I., Kroger, W., Sansavini, G., Schlapfer, M., Zio, E. (2009). The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures, Reliability Engineering & System Safety, Vol. 94, Issue 5, pp 954-963.
[19] Bompard, E., Napoli, R., Xue, F. (2009). Analysis of structural vulnerabilities in power transmission grids, International Journal of Critical Infrastructures, Volume 2, Issues 1-2, Pages 5-12.
[20] Billinton, R., Li, W. (1994). Reliability Assessment of Electric Power Systems Using Monte Carlo Methods, Springer, pp.229-308.
[21] Nieminen, J. (1974). On the Centrality in a Graph, Scandinavian Journal of Psychology, n.15.

[22] Latora, V. and Marchiori, M. (2001) Efficient Behavior of Small-World Networks, Physical Review Letters, Vol. 87, N. 19.
[23] Volkanovski, A., Cepin, M. and Mavko, B. (2009). Application of the fault tree analysis for assessment of power system reliability, Reliability Engineering & System Safety, Vol. 94 (6), pp. 1116-1127.
[24] Zio, E. (2007). From Complexity Science to Reliability Efficiency: A New Way of Looking at Complex Network Systems and Critical Infrastructures, Int. J. Critical Infrastructures, Vol. 3, Nos. 3/4, pp. 488-508.
[25] Zio, E., Librizzi, M., Sansavini, G. (2008). A combined Monte Carlo and cellular automata approach to the unreliability analysis of binary network systems, Proceedings of the Institution of Mechanical Engineers Vol. 222(1) Part O: J. Risk and Reliability.
[26] Crucitti, P., Latora, V., Marchiori M. (2005). Locating critical lines in high-voltage electrical power grids, Fluct. Noise Lett., 5, L201-L208.
[27] Bier, V. M., Haphuriwat, N., Menoyo, J., Zimmerman, R. and Culpen, A.M. (2008). Optimal resource allocation for defense of targets based on differing measures of attractiveness, Risk Analysis 28, 3, pp. 763-770.
[28] Brown, G. G., Carlyle, W. M., Salmerón, J., Wood, K. (2006). Defending critical infrastructure. Interfaces 36, 6, 530-544.
[29] Cox, L. A. (2009). Making telecommunications networks resilient against terrorist attacks (Chapter 8). Game Theoretic Risk Analysis of Security Threats, eds. Bier, V.M., Azaiez, M.N., Springer: New York, pp. 175-198.
[30]. Solé, R. V., Casals, M. R., Corominas-Murtra, B. and Valverde, S. (2008). Robustness of the European power grids under intentional attacks, Physical Review E 77, 26102.
[31] Eusgeld, I., Henzi, D., Kroger, W. (2008). Comparative evaluation of modeling and simulation techniques for interdependent critical infrastructures, Scientific Report, Laboratory for Safety Analysis, ETH Zurich.
[32] Kroger, W., Zio, E. (2011). Vulnerable Systems, Springer London Dordrecht Heidelberg New York, DOI 10.1007/978-0-85729-655-9.
[33] Zio, E., Kroger, W. (2009). Vulnerability assessment of critical infrastructures, e IEEE Reliability Society 2009 Annual Technology Report.
[34] Watts, D.-J. and Strogatz, S.H. (1998). Collective dynamics of „small-world" networks, Nature, Vol. 393, pp. 440-442.
[35] Rocco, C., Ramirez-Marquez, J.E., Salazar, D. and Zio, E. (2010). A Flow Importance Measure with Application to an Italian Transmission Power System, International Journal of Performability Engineering, Vol. 6, No. 1, pp. 53-61.
[36] Casals, M. R. and Solé, R. V. (2011). Analysis of major failures in Europe's power grid, International Journal of Electrical Power & Energy Systems.
[37] Dekker A. H. (2005) Simulating Network Robustness for Critical Infrastructure Networks, Conferences in Research and Practice in Information Technology, Proceedings of the 28th Australasian Computer Science Conference, The University of Newcastle, Newcastle, Australia, Vol. 38, V. Estivill-Castro, Ed.
[38] Debon, A., Carrion, A., Cabrera, E., and Solano, H. (2010). Comparing risk of failure models in water supply networks using ROC curves, Reliability Engineering and System Safety, vol. 95, pp. 43–48.
[39] Patterson, S. Apostolakis, G. 2007, Identification of critical locations across multiple infrastructures for terrorist actions, Reliability Engineering & System Safety, 92(9), pp. 1183-1203.
[40] D'Inverno, M. and Luck, M. (2004). Understanding Agent Systems, Springer, Berlin.
[41] Moore, A.D. (2006). Application of the API/NPRA SVA methodology to transportation security issues, Journal of Hazardous Materials, vol. 130, pp. 107–121.

[42] Garrick, B. J., Hall, J. E, Kilger, M., McDonald, J. C., McGroddy, J. C., O'Toole, T., Probst, P. S., Rindskopf, Parker, E., Rosenthal, R., Trivelpiece, A. W., Van Arsdale, L., Zebroski, E. (2004). Confronting the risks of terrorism: making the right decisions, Reliab. Eng. Syst. Safe., 86:129–176.

Tables and figures

Table 1. Degree indicators of the 24 network nodes

Topological Degree		Reliability Degree		Electrical degree		Electrical-reliability degree	
node	degree	node	degree	node	degree	node	degree
9	5	9	19.0939	18	0.2469	7	0.4215
10	5	10	19.0928	17	0.2467	22	0.4149
11	4	11	19.0926	21	0.2467	18	0.3781
12	4	12	19.0912	15	0.2465	17	0.3622
16	4	13	18.1300	16	0.2462	21	0.3592
1	3	3	18.0415	22	0.2452	19	0.3515
2	3	24	17.9313	19	0.2449	20	0.3440
3	3	1	17.6274	24	0.2447	14	0.3317
8	3	16	17.5905	20	0.2433	15	0.3304
13	3	23	17.4177	23	0.2423	16	0.3238
15	3	2	17.3933	14	0.2419	23	0.3198
17	3	15	17.2740	13	0.2388	4	0.3176
21	3	5	17.0725	11	0.2386	8	0.3149
23	3	8	16.9606	12	0.2370	24	0.3133
4	2	14	16.7865	3	0.2368	5	0.3030
5	2	4	16.7335	9	0.2340	13	0.3029
6	2	6	16.6817	8	0.2316	3	0.3021
14	2	20	16.3159	7	0.2315	2	0.2985
18	2	19	16.0972	4	0.2303	1	0.2951
19	2	21	16.0233	1	0.2250	6	0.2914
20	2	17	15.8838	2	0.2245	11	0.2872
22	2	18	15.2564	5	0.2242	12	0.2858
24	2	22	13.8271	10	0.2219	9	0.2820
7	1	7	12.7517	6	0.2107	10	0.2678

Table 2. Ranking of network connections with respect to the reliability, electrical and reliability-electrical distances

From node	To node	Reliability	Rank	Electrical distance	Rank	Electrical-reliability distance	Rank	From node	To node	Reliability	Rank	Electrical distance	Rank	Electrical-reliability distance	Rank
1	2	0.8991	6	0.1505	15	-	-	10	24	0.8822	16	-	-	-	-
1	9	0.8869	13	-	-	-	-	11	12	0.9996	2	-	-	-	-
1	10	0.8870	12	-	-	-	-	11	13	0.9389	5	-	-	-	-
1	11	0.8869	13	-	-	-	-	11	23	0.8730	22	-	-	-	-
1	12	0.8868	14	-	-	-	-	11	24	0.8822	16	-	-	-	-
2	9	0.8786	19	-	-	-	-	12	13	0.9391	4	-	-	-	-
2	10	0.8787	18	-	-	-	-	12	24	0.8821	17	-	-	-	-
2	11	0.8786	19	-	-	-	-	15	16	0.8900	10	0.1506	16	-	-
2	12	0.8785	20	-	-	-	-	15	17	-	-	0.1484	11	-	-
3	9	0.8919	7	-	-	-	-	15	18	-	-	0.1470	9	-	-
3	10	0.8917	9	-	-	-	-	15	19	-	-	0.1584	28	-	-
3	11	0.8918	8	-	-	-	-	15	21	-	-	0.1455	8	-	-
3	12	0.8918	8	-	-	-	-	15	22	-	-	0.1477	10	0.1061	25
3	22	-	-	-	-	0.1085	32	15	24	-	-	0.1535	20	-	-
3	24	0.9862	3	0.1580	25	-	-	16	17	-	-	0.1493	12	-	-
4	7	-	-	-	-	0.1027	19	16	18	-	-	0.1501	14	-	-
4	22	-	-	-	-	0.1024	17	16	19	-	-	0.1551	21	-	-
5	7	-	-	-	-	0.1076	30	16	20	-	-	0.1620	34	-	-
5	22	-	-	-	-	0.1090	34	16	21	-	-	0.1506	17	-	-
7	8	-	-	0.1030	1	0.0763	1	16	22	-	-	0.1512	18	0.1070	28
7	14	-	-	-	-	0.1004	13	16	24	-	-	0.1606	33	-	-
7	15	-	-	-	-	0.0999	12	17	18	-	-	0.1375	4	-	-
7	16	-	-	-	-	0.1020	16	17	19	-	-	0.1575	24	0.1085	33
7	17	-	-	-	-	0.0891	4	17	20	-	-	-	-	0.1062	26
7	18	-	-	-	-	0.0850	3	17	21	-	-	0.1413	7	-	-
7	19	-	-	-	-	0.0944	8	17	22	-	-	0.1392	6	-	-
7	20	-	-	-	-	0.0980	11	17	24	-	-	0.1593	31	-	-
7	21	-	-	-	-	0.0899	5	18	19	-	-	0.1582	26	0.1024	18
7	22	-	-	-	-	0.0772	2	18	20	-	-	-	-	0.1006	15
7	23	-	-	-	-	0.1083	31	18	21	0.8898	11	0.1366	2	-	-
8	9	0.8731	21	-	-	-	-	18	22	-	-	0.1380	5	0.1037	21
8	10	0.8731	21	-	-	-	-	18	23	-	-	-	-	0.1047	23
8	11	0.8730	22	-	-	-	-	18	24	-	-	0.1583	27	0.1065	27
8	22	-	-	-	-	0.1042	22	19	20	-	-	0.1522	19	-	-
13	22	-	-	-	-	0.1031	20	19	21	-	-	0.1586	29	0.1075	29
14	22	-	-	-	-	0.1004	14	19	22	-	-	0.1594	32	0.0930	7
9	10	0.9997	1	-	-	-	-	19	23	-	-	0.1570	22	-	-
9	11	0.9997	1	-	-	-	-	20	21	-	-	-	-	0.1060	24
9	12	0.9997	1	-	-	-	-	20	22	-	-	-	-	0.0915	6
9	13	0.9389	5	-	-	-	-	20	23	-	-	0.1493	13	-	-
9	24	0.8826	15	-	-	-	-	21	22	-	-	0.1367	3	-	-
10	11	0.9997	1	-	-	-	-	21	24	-	-	0.1572	23	-	-
10	12	0.9997	1	-	-	-	-	22	23	-	-	-	-	0.0951	9
10	13	0.9389	5	-	-	-	-	22	24	-	-	0.1592	30	0.0965	10

Table 3. Evaluation of the four perspectives based on literature review and developed criteria

	Accounting for system structure	Accounting for physical properties	Accounting for dynamics	Identification of importance indicators	Identification of vulnerability indicators	Data needs	Maturity	Complexity	Requested time
Graph-theoretical analysis	YES	NO	NO	YES	NO	LOW	HIGH	LOW	LOW
Reliability analysis	YES	YES	NO	YES	NO	LOW	MIDDLE	MEDIUM	LOW
Electrical analysis	YES	YES	YES	YES	YES	HIGH	HIGH	MEDIUM	MEDIUM
Reliability-electrical analysis	YES	YES	YES	YES	YES	HIGH	POOR	MEDIUM	MEDIUM
Statistical analysis	NO	NO	NO	YES	YES	HIGH	HIGH	LOW	LOW
Risk analysis	YES	YES	YES	YES	YES	HIGH	HIGH	HIGH	HIGH
Agent-based modeling	YES	YES	YES	YES	YES	LOW	HIGH	HIGH	HIGH
Object-oriented modeling and simulation	YES	YES	YES	YES	YES	HIGH	HIGH	HIGH	HIGH

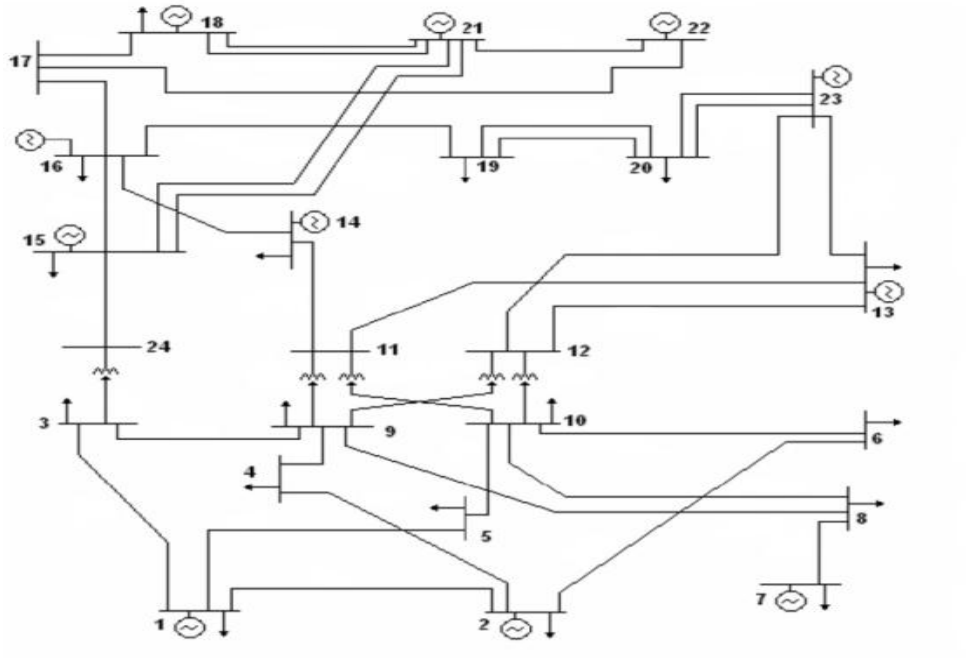

Figure 1. The IEEE RTS 96

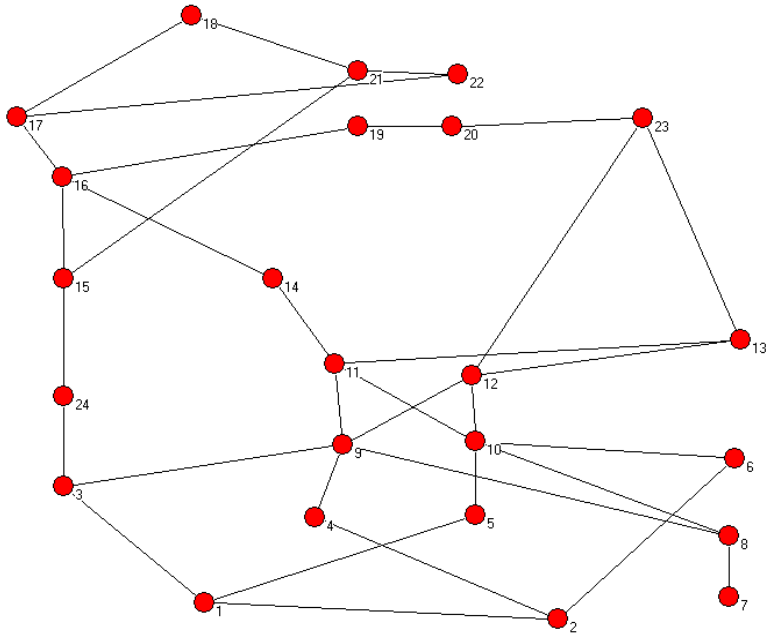

Figure 2. The topological graph of the IEEE RTS 96

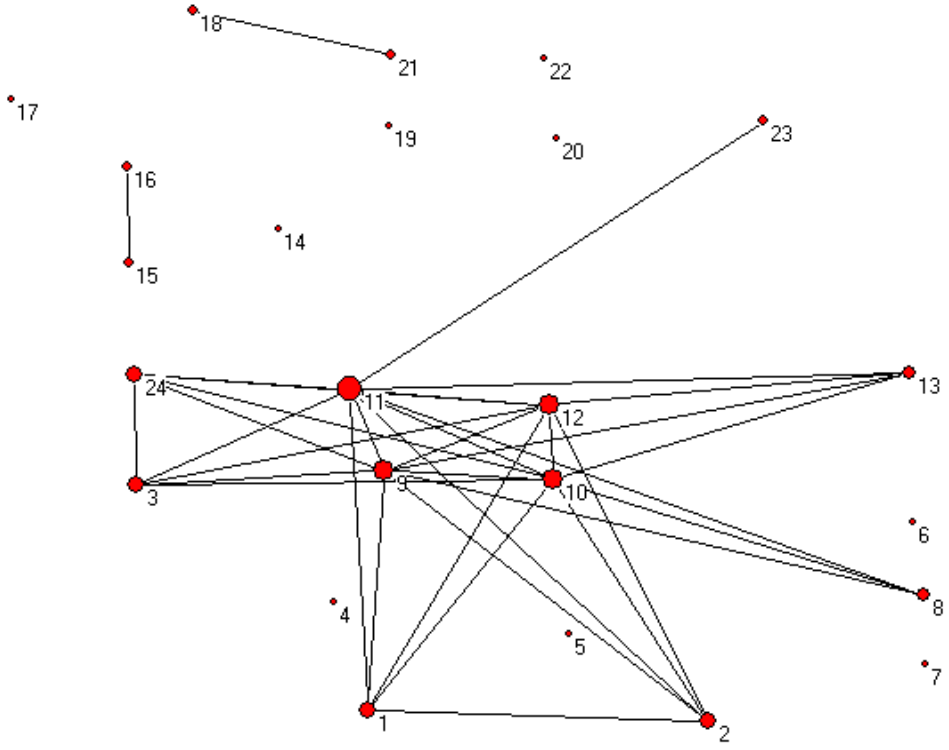

Figure 3. The IEEE RTS 96 redrawn to highlight the structure of the 34 most reliable connections

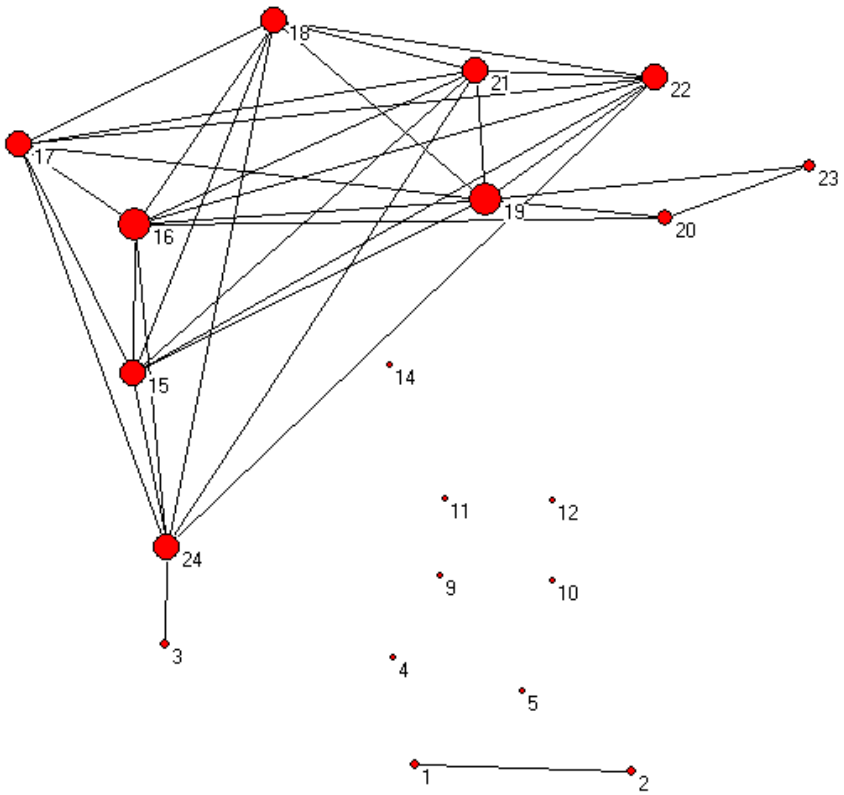

Figure 4. The IEEE RTS 96 redrawn to highlight the structure of the shorter electrical connections

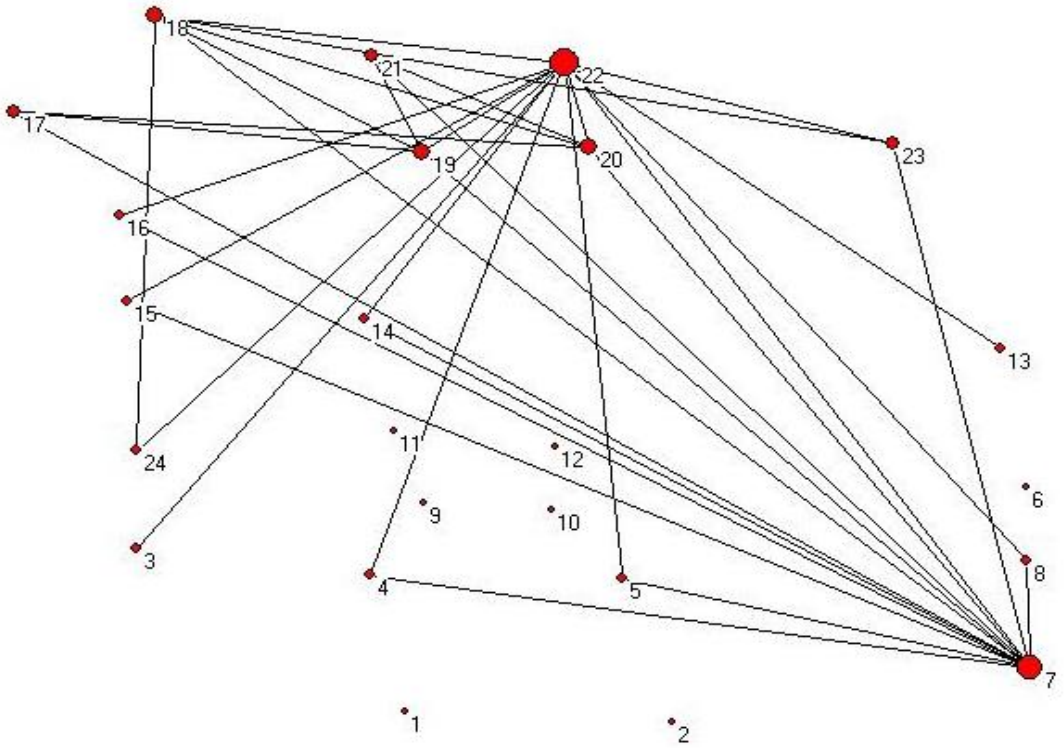

Figure 5. The IEEE RTS 96 redrawn to highlight the structure of the most reliable electrical connections