GIS-BASED TOOL FOR NETWORK CRITICAL INFRASTRUCTURE IDENTIFICATION IN EUROPE

C.Di Mauro[a,*], S. Contini[b], J-P. Nordvik[b]

[a] RGS S.r.l., Risk Governance Solutions, 21052 Busto Arsizio (VA), Italy cdmelo@tiscali.it
[b] European Commission – Joint Research Centre, via Fermi, 20125 Ispra (VA), Italy, sergio.contini@ jrc.ec.europa.eu, jean-pierre.nordvik@jrc.ec.europa.eu

KEY WORDS: Critical infrastructure, Fault Tree Analysis, Cut set, Network analysis, Network reliability

ABSTRACT:

The Council of the European Union Directive 114/EC published in December 2008, aims to ensure that there are adequate levels of protective security on critical infrastructure, minimal single points of failure and rapid recovery arrangements throughout the European Union. According to the Council of the European Union Directive, 'critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions. Therefore infrastructures are considered critical if they are used in the provision of services that are deemed to be vital for the functioning of society. However, such infrastructures can be destroyed or disrupted by deliberate acts of terrorism or natural disasters resulting in possible significant impacts on society. Infrastructural networks routed across the land. The exposure of network sections to natural events or malevolent actions depends on their spatial distribution and on the hazards type. The consequences of disruptions are typically considered in terms of human fatalities, but in the case of networks, such scenarios can be relevant only for a limited number of sections, i.e. for the branches located in the proximity of populated area. In case of localized damage the network can generally be reconfigured to reduce propagation of the effects to other branches; however, when this is not possible, the local damage may lead to economic loss or public impact to larger communities. It is therefore important to identify all network failures leading to large consequences in terms of affected population. According to the scope of the Directive, a Geographical Information System (GIS) based tool was developed to support the identification of European network infrastructures and critical network assets.

1. INTRODUCTION

Infrastructure networks are not on secure industrial sites, but are routed across the land. The exposure of network sections to natural events (but also to intentional ones) depends on the spatial distribution and the characteristics of such hazards. The consequences are typically considered in terms of human fatalities, but in the case of networks, such scenarios can be relevant only for a limited number of sections. Instead, it is also important to evaluate what may be the impact of a network failure for large communities in terms of economic loss or public impact. This work proposes a method based on Multi-State Fault Tree Analysis (FTA) (Lisnianski A. and G. Levitin, 2003) for identifying the most critical sections and minimal cut sets of a network.

2. CRITICAL INFRASTRUCTURES

Many definitions of Critical infrastructures may be found in the literature (e.g. S.Bouchon S. 2006). According to the Council of the European Union Directive, published in December 2008, 'critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions (Council Directive 2008/114/EC , 2008). The Council of the European Union Directive 114/EC published in December 2008, aims to ensure that there are adequate levels of protective security on critical infrastructure, minimal single points of failure and rapid recovery arrangements throughout the European Union.

Some infrastructures are considered critical because they are used in the provision of services that are deemed to be vital for the functioning of society. However, such infrastructure can be destroyed or disrupted by deliberate acts of terrorism or natural disasters resulting in possibly significant impacts on society. Many infrastructures are vulnerable to heat waves, ice storm, floods and hurricanes and to the inevitable equipment failure and employee mistakes that plague all complex, tightly coupled systems. Moreover, infrastructures such as pipelines, transportation, communication and power transmission systems, are networks which extend spatially over large geographical regions.

Those infrastructures that could possibly be identified as European Critical Infrastructures often form part of a larger network. Given this character, events at one location could, via the network linkages, propagate to other locations. An integrated process has therefore been developed by the Joint Research Centre (JRC) to evaluate the vulnerability of a network and the criticality of its assets against natural hazard impacts. The methodology is based on Fault Tree Analysis (FTA) (Lisnianski A. and G. Levitin, 2003). It identifies the most critical sections and minimal cut sets of a network to evaluate the expected consequences in term of economic loss. FTA can be considered as the most popular methodology for dependability studies of complex systems, allowing the systematic description of the system's failure logics and the assessment of the corresponding probabilities.

* Corresponding author.

3. MODEL DESCRIPTION

3.1 Background information

It is often assumed that the robustness of many complex systems is embedded in their redundancy, which for networks represents the existence of many alternative paths that can preserve communication between nodes even if some nodes are absent. The literature reports different ways of attacking networks and various method of evaluating the impacts. Such approaches are mainly based on topological evaluation of the networks and are not suitable for considering the rate of the availability of a service. These methods rely on the evaluation of the degree of connectivity of each node and the consequences are estimated considering a systematic removal of nodes. Networks vary in their level of resilience to such vertex removal. It has also been demonstrated that most networks (e.g. internet web) are robust against random vertex removal but considerably less robust to targeted removal of the highest degree vertices (e.g. Reka, A. et al, 2000; Reka A. and A.-L. Barabasi, , 2002).

It should also consider that many real world systems are composed of multi-state components, which have different performance levels and several failure modes with various effects on the system's performance. This is the typical characteristic of national infrastructures with different operational units and different operational characteristics and failure modes. Such systems are able to perform their task with partial performance. Failures of some system components lead only to the degradation of the system.

For this reason the developed model considers a multi-state fault approach which allows taking into account both the topological characteristics and the availability of the system. Fault Tree Analysis (FTA) can be considered as the most popular methodology for dependability studies of complex systems, allowing it to systematically describe the system's failure logics and to quantify the corresponding probabilities. It can be defined as a graphical representation of the various combinations of faults that will result in an undesired event (Vesely et al., 1981). FTA is used in many industrial fields, in particular at the design phase to improve the design through the systematic identification of weak components, but also for system diagnosis; and maintenance planning. Most of the FTA techniques are related to traditional binary reliability models that consider only two possible states for a system and its components: perfect functionality or complete failure.

Infrastructures are large and complex systems that can perform their tasks with various distinguished levels of efficiency usually referred to as performance rates. Therefore, we considered a multi-state fault tree approach. The reliability analysis of a multi-state system is more consistent with the operational behaviour of a large infrastructure system, but efficient analysis of large Fault Trees is still a complex problem. Also, the reliability analysis of a multi-state system is much more complex in comparison to a binary state system. (Lisnianski, A. and G. Levitin, 2003)

The model has been developed with a geographic information system, where the infrastructure network is represented and all data about the attributes and the characteristic of each component are stored. The Fault Tree is automatically generated by using a traceback algorithm routine.

Typically the definition and the construction of a Fault Tree is a very time consuming task. Moreover, the process relies on the experience and the need of the analyst therefore, sometime the same system represented as a fault tree in different ways (Carpignano A. and A. Poucet, 1994). In the contest of the Directive implementation, we considered that a common formalisation of the system allowed improving the common understanding and communication among the stakeholders. Therefore the automatic generation of the Fault Tree aims are:

- To give better guarantees for a detailed and complete analysis of the system,
- To obtain objective, repeatable and confrontable results, which do not depend on different system decomposition approaches,
- To improve the transparency of the analysis and to make the models and results more easier to review,
- To reduce the analyst's efforts especially in repetitive operations, like the generation and the comparison of several different scenario's;
- To allow the reuse of knowledge gained in previous analysis.

Starting from the Top Event, the routine considers the sequence of components in the reverse direction of the flow of the infrastructure service until the boundaries of the system are reached. For each component a logical gate is generated according to the characteristics of the connections and the series of status related to expected failures.

The following section illustrates the basic of the network model.

3.2 Mathematical formulation of the multi-state network model

In the contest of Directive implementation, a common formalisation of the system allows improving the common understanding and communication among the stakeholders. Hence, the aims of our decision support system for oil and gas networks are to:

- Simulate the consequences of the attack to one or more nodes (compression stations / pipelines);
- Identify the critical nodes;
- Determine the importance ranking of the nodes;
- Determine the causes that lead to a given consequence in one or more countries.

The infrastructure network considered in this paper can be modelled as a directed a-cyclic graph, defined as G={V, E}, where V is the set of nodes and E is te set of edges. Nodes represent the physical elements, e.g. compressing units; intercepting valves, whereas edges represent pipelines. Nodes with no up-stream nodes are the input nodes of the network, i.e. storages or the boundary limits of the system of concern, in any case the oil/gas inflow points; nodes with no down-stream nodes are delivery points or boundary limits of the system of concern, i.e. the oil/gas outflow points. All other nodes are referred to as "internal nodes" of the system.

The network flow and the node states are modelled as a multi-valued logic. Each node is associated with a vector of states representing the different failure modes. The generic node v_i is represented as $v_i=\{s_{i1}, s_{i2},\ldots, s_{im}\}$ with $s_{ij} \cap s_{ik} = 0$ for j, k = 1,..,m and $j \neq k$. States are ordered from s_0 (complete failure) to s_m (perfectly working). In a system there may be nodes described with different number of states; in our model we considered nodes with 2, 3 and 5 states.

Any network node can also be described by its outflow, referred to as "performance level" in this paper. Hence the generic j-th state of the i-th node, s_{ij}, is associated with a performance level ϕ_{ij}, which represents the service level provided.

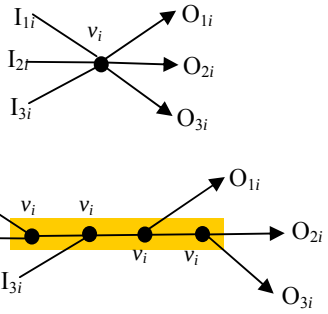
The number of states of the i-th component with different performance levels is indicated as y_i. Moreover let $L = \max_i (y_i)$ for i= 1,2,…,n where n is the total number of components.
A multi-valued logic can be defined when the system contains non-binary components. The order of the logic is obtained by subdividing the range of flow (0 – M) into a number of intervals equal to L. Since the state of a node determines its performance level φ, there is a close relationship between s_{ij} and ϕ_{ij}. The maximum performance level corresponds to the complete functioning of the node, i.e. $s_{im} \Leftrightarrow \phi_{iM}$.; the minimum corresponds to s_{i0}.
The dynamic variation of the flow in a pipeline can be described by means of a set of differential equations. However, in our simplified model we assume that there is a steady state condition in which the flow is constant in each node and that its variation is caused by an external event, i.e. an attack that changes the flow regime. Hence, each node is characterised by its maximum performance level ϕ_M before the attack and a different level $\phi < \phi_M$ after the attack.
Other assumptions

- The changing state of a node occurs only in case of an external intentional attack, i.e. random failures are not considered (however, the addition of the random causes of nodes' unavailability is quite simple);
- The behaviour of each node is independent with each other; however, one or more nodes can be attacked and damaged at the same time due to a concerted action among different groups of attackers;
- If pipelines are connected in parallel to the same couple of nodes, they are considered as a single pipeline with a total nominal flow given by the sum of the nominal flows of the pipelines;
- The attack of a node is described by the binary indicator variable: ai = 1 (0) means that the i-th node is attacked (not attacked).

We assume that the probability of a node of being attacked depends on the characteristics of the node itself:
$P(a_i = 1\} = g(c_{i1}, c_{i2}, ..,c_{il}) = g_i$, where c_{ij} is a variable that characterise a particular attractiveness aspect of the generic i-th node, g is function of the *l* properties characterising the i-th node, and g_i is the probability of the i-th node of being attached.
Examples of c_i factors are: location, visibility, inventory, ownership, impact of sabotage, security measures, etc.
As a consequence of an attack on the i-th node, v_i, the state node passes from s_{im} (working state) to one of its degraded states s_{ij} (indicated as $v_i = s_{ij}$) with probability $P\{v_i = s_{ij} \mid a_i = 1\} = p_{ij}$. Hence p_{ij} represents the probability that the i-th node fails in the j-th mode given the occurrence of an attack. The values p_{ij} can be determined through engineering judgement or expert elicitation. Conservatively, it can be assumed that in case of attack the i-th node takes the state s_{i0} (complete failure) with probability $p_{ij} = Pr\{s_{i0}=1\}$, corresponding to $\varphi_{ij} = 0$. Therefore, the probability that a node *i* is in the state $v_i = s_{ij}$ due to an attack is given by: $P\{v_i = s_{ij} \cap a_i = 1\} = P\{v_i = s_{ij} \mid a_i = 1\}\ P\{a_i = 1\} = p_{ij}\ g_i$.
If the network is working properly, i.e. there is no attack, then $p_{ij} = 0$ for all degraded states and $p_{i0} = 1$ for all nodes.
In case of attack to one or more nodes the performance levels of one or more output nodes is lower than ϕ_{iM}.
The random performance rate of the entire system ϕ depends on the nature of the node's interaction in the system and on the distribution of the related performances. It is determined by the system structure function: $\phi = f(\phi_1,\phi_2,..,\phi_n)$. The system survives if its performance rate is not less than the minimal required level k and the probability that the system survives is: $Q(k) = P\{\phi \geq k\}$.
In order to perform the automatic fault tree construction for a given Top-event it is necessary to characterise each node by means of its "Node Transfer Map, NTM", i.e. a map relating the output performance to the input performance and the internal (working and failed) states. The graph of the network can be built using a finite number of generic models. Pipelines are represented as binary models. Nodes can be of the following types:

- Type-1: one input and one output.
- Type-2: two inputs and one output.
- Type-3: one input and two outputs.

A node with multiple inputs and multiple outputs can always be described as a combination of the above types of nodes, as shown by the following simple example.



In this example v_i can be described by two nodes of type 2 and two nodes of type 1. The four nodes are replications of v_i, i.e. they assume the same name and characteristics. This solution has the disadvantage of increasing the number of nodes of the graph, but it presents the advantage of reducing the number of nodes transfer maps (NTM) to be defined, which otherwise, would be equal to the number of nodes with different number of inputs and outputs. The solution of NTM for nodes with multiple input and output edges have also be developed by the authors during the project as an alternative modelling.
The analysis of the network, modelled as a multi-state a-cyclic graph, implies the automatic construction of as many fault trees as the number of degraded states. The analysis of such fault trees is performed by means of ASTRA and results are displayed on the geographical map..

4. DECISION SUPPORT SYSTEM

Many definitions of a Decision Support System are available in literature. In general terms a Decision Support Systems is a specific class of computerized information system that assists people in making decisions based on data that is gathered from a wide range of sources. Decision Support System applications are not single information resources, such as a database, a model or a program that graphically represents results and figures, but the combination of integrated resources working together.
The structure and the design of a Decision Support System can vary according to the skill and aptitude of the decision maker and the needs of the decision-making process. In this chapter the structure of the system developed is illustrated.

Basically, the approach used in this project is based on the assumption following an informal expert judgement and iterative reviewing process of alternative scenario's. Actually, this approach is inline with many decision-making theorists involved in the social evaluation of complex systems (e.g. Aven T. and J. Kørte 2003, Ersdal G. and Terje Aven, 2008; Munda G., 2008; Renn O., 2008). The decision maker needs to take the results of the analysis and make his decision, following a review and a judgement process without having a predefined goal or criteria that need to be maximised.
In particular considering the aim of the Directive we would expect that many national experts will be involved and a collective decision would produce positive outcomes. In relationship to the Directive objectives where the starting point is a decision problem formulated as a task of choosing among a set of alternatives, i.e. assets that are considered critical.

4.1 Architecture of the tool

With a Geographical information System (GIS), the network is represented as a table, where each row represents an edge e and each column reports an attribute of the edge (e.g. flow, pressure, etc).
The first column, typically named "Shape", stores all the information related to the graphic representation and visualisation of the edge. As we assumed above, the model considers a direct network. The second column is a repository of identification codes of originating nodes (i.e. Node From) and the third one, of the destination nodes (i.e. Node To). Therefore, each row identifies a unique connection of two nodes and the related characteristics (binarisation).
A second table considers the full set of nodes and all the required information to characterize each node. In particular, a record reports:

- the node ID
- the label of the node;
- a node classifier;
- five attributes for the characterization of the node in order to calculate the proxy for the probability of a node to be attacked;
- five attributes that express the five different states of the node in case of an attack;
- five attributes that express the probability of the node of being in certain status in case of an attack.

All this information is stored in GIS Network Database. The routine for the automatic generation of the multi-state Fault Tree access the available information in the GIS Network Database and according to the specification of the user, defines a Fault Tree. The Fault Trees are stored in a repository where they can be accessed automatically or on demand by a Fault Tree analyser. The tool utilised is ASTRA-FTA (version 3.0) (Contini et al., 2008). ASTRA is an efficient fault tree solver developed at the Joint Research Centre. ASTRA is fully based on the state of the art approach: the Binary Decision Diagrams (BDD). The main advantage for this application is the much lower calculation times with respect to other approaches and to the exact probabilistic analysis. These capabilities are particularly relevant for the new emerging applications in the domain of security, where a high event probability is involved to prevent the use of techniques based on classical Fault Tree approximated methods. The results obtaining by running the ASTRA tool are stored in the GIS Database in order to be represented on the geographical map of concern.

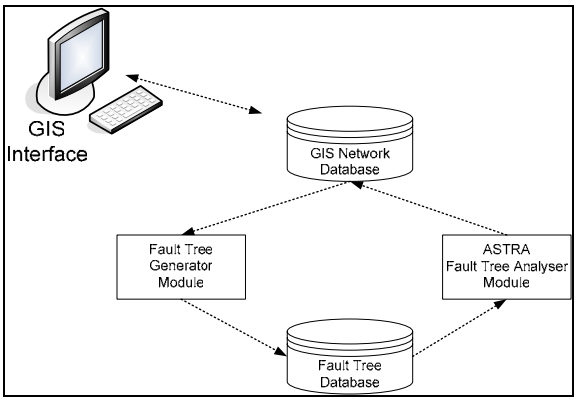


Figure 1. Scheme of the system architecture

5. CASE STUDY – HIGH PRESSURE GAS SUPPLY NETWORK

A case study has been undertaken in order to:

- check the applicability of the detailed approach and that data needs can be fulfilled,
- identify weaknesses and to further improve the modelling and the decision support system (DSS),
- validate the approach by checking against existing studies and experience.

The reference system selected to check the applicability of the proposed approach is a pressure transnational gas pipeline network. A reference scenario we used the results of the simulations performed by R. Pride (2008). The study considered the Czech Republic Slovakia and Hungary. For all three countries the components of the Trans-National transmission pipeline network and the National high pressure network have been introduced into the model. Figure 2 shows an overview of the pipelines modelled in the three countries. The flow directions determined during the analysis are indicated by arrows.
The assessment of the distribution of the gas over the transmission pipeline network was performed by using a commercial pipeline modelling software [SynerGee,]. All physical data, including information on maximum available storage and production flow rates, capacities, etc. has been taken from a number of open literature sources (Pride R., 2008). The software allows the underlying pipeline map to be built in a GIS environment. Pipeline asset data has been obtained from sources providing geographical locations (Platts, 2008). The model operates by solving multiple simultaneous flow equations for every element in the network based on a set of known pressures and flow rates, typically defined at the extremities of the system and at key points within the system such as at compressor station input/outputs and at supply sources. A detailed model was constructed comprising many of the pipeline and equipment properties, including simple control strategies and geographical locations (Pride R. et al, 2008). In particular, the compressor stations were modelled on the detailed level of multiple series parallel driver/compressor combinations and fuel consumption profiles. By considering the regulator stations as key outputs to a country's regions with gas demand requirements, or pressures, the system can be solved by quantifying the available supply rates under a range of operational conditions.

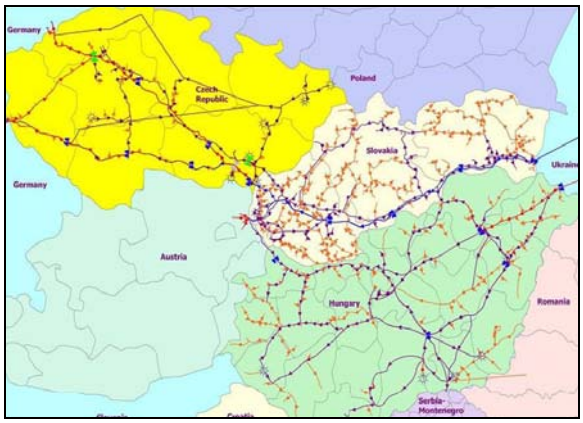


Figure 2. Gas network considered by the case study

The system is made up of N = 1095 nodes. Double lines are considered as single line with equivalent capacity. The main components are:

- No 1064 Pipelines
- No 13 Storage fields
- No 3 Valves & regulators
- No 15 Compressor stations

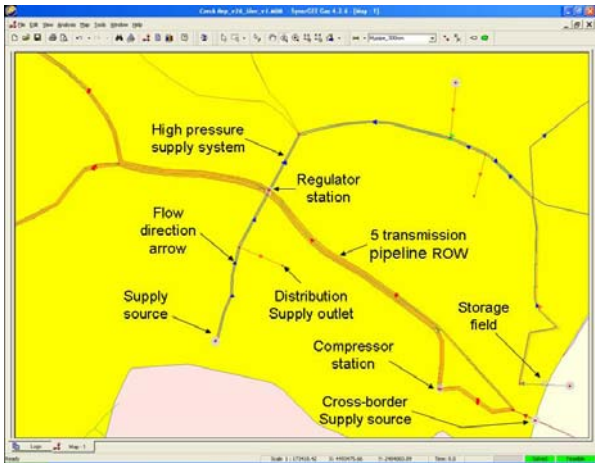


Figure 3. Example of the network element considered by the pipeline modelling software (Pride R.; 2008)

The network is modelled as stochastic, direct, connected graph in which each substation is transposed into a node. For the sake of simplicity, the probability of a node to be targeted by an intentional act, has been assumed proportional to the flow of node, i.e. the attacker considers that the magnitude of the impact is related to the unavailable quantitative of gas. The simplified scenario considers also that each node attacked has the same probability of consequences.

Percentage of the node flow	Probability	
0.00	0.01	*Full unavailable*
0.25	0.02	
0.50	0.10	
0.75	0.5	
1.00	0.37	*Full available*

Table 1. Assumptions of node availability as consequence of a successful attack expressed as percentage of the node flow

The Top Event has been defined as the unavailability of one of the three delivering nodes at the boundary between Czech Republic, Germany, Slovakia and Austria.
The number of events considered is 974 and the gates are 1060. The Minimal Cut set are considered with maximum rank (i.e. order) equal to 8. The minimal Cut sets of order one are related to the delivering nodes, i.e. the nodes that define the Top Event. The Cut set with a higher rank, there are three set with order two and three and four with order four. The following table reports the full set.

Cutset Order	No	Cutset Order	No
1	3	5	5
2	3	6	42
3	3	7	0
4	4	8	42

Table 2. Cutset results

It is interesting to evaluate that many of the higher degree cut set are related to all possible combination of serial module like for instance the case reported in the picture.

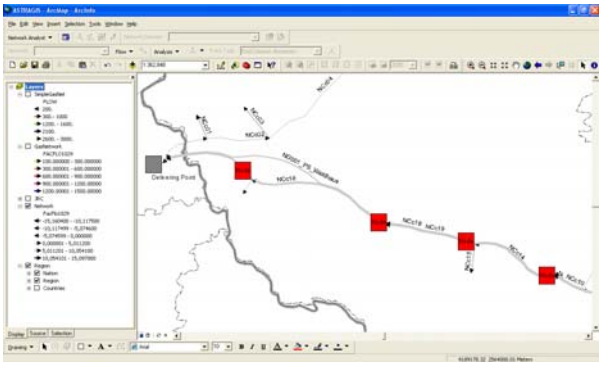


Figure 4. Example of identification of cutest nodes

The model provided the rank of the Critical index value for each node. The flowing plot reports the 20 most critical nodes. It is interesting to note for instance that the most critical node is related to redundant pipe line but directly connected with a delivery node.

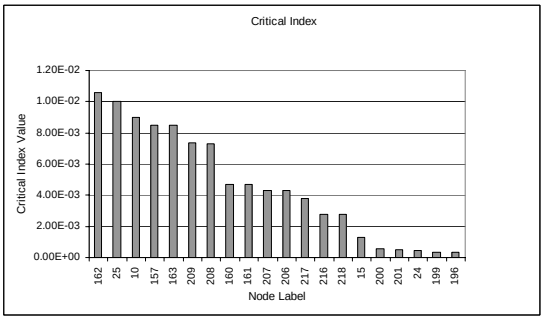


Table 3. Rank of the most critical nodes

6. CONCLUSIONS

The Council Directive 2008/114/EC establishes the procedure for the identification and designation of European Critical Infrastructures (ECI), the destruction or disruption of which would have significant crossborder impact. This may include transboundary effects resulting from interdependencies between interconnected infrastructures on at least two Member States. The current scope of the Directive is on the energy and transport sectors. Even though the general scope of the Directive and the implementation procedures are clear, the Directive permits the Member States to decide on the identification of important assets and the related vulnerability. Furthermore, it does not provide any indication about a common reference method to implement this Directive.

Therefore, we investigated the opportunity to develop a method that would help Member States to tackle this problem by using a common approach. The proposed technique is based on a Multi State Fault Tree Analysis. Fault Tree Analysis is a well consolidated method applied in many engineering fields. It is a deductive method whose input consists of knowledge of the system's functions as well as its failure modes and their effects. The result of the analysis is a set of combinations of component failures that can result in a specific malfunction.

This paper presents an algorithm based on Fault Tree Analysis. The algorithm considers the potential multi-state consequences of a failure related to an asset of a critical infrastructure. The algorithm was implemented within a Geographical Information System which was coupled with Fault Tree Analyser. This approach tool allowed the development of a method for the identification and characterisation of the critical assets of critical infrastructure network.

In our opinion this method constitutes a valid Decision Support System and has a number of advantages:

- The fault tree is automatically generated and it allows obtaining objective, repeatable and confrontable results;
- It reduce the effort of the generation of scenario's and the related comparisons,
- It merges the topological characterization with a Multi-State Fault Tree analysis
- It provides an indication about the criticality of each component of the system;
- It provides Cut-sets
- It supports the definition of a scenario and the related simulation results with geographical representation;
- The calculation is high speed, which helps users and decision makers to investigate and compare several alternative scenarios without much effort.

However, we are aware of some disadvantages:

- The Fault Tree model is an intrinsic static and discrete representation of a complex system, which is not able to evaluate the dynamic of the system and it does not consider some important operational constraints such as voltage limits or gas pumping rates;
- It relies on expert judgment in order to define the vulnerability and the importance of each component;
- For intentional acts the importance of each node is defined considering the attractiveness of each node in terms of the potential advantage for the attacker;
- The model overlooks the fact that is more difficult to organize an attack with multi targets.

Although we are aware that many real world systems have complex architectures and behaviours which can not be described in a simplified way, the model demonstrated a valid support for decision makers. So it is important to extend this work and to test it with the support of some potential real end user's.

7. REFERENCES

Aven T. and J. Kørte, 2003; On the use of risk and decision analysis to support decision-making, *Reliability Engineering & System Safety*, Volume 79, Issue 3, 1 March 2003, Pages 289-299

Bouchon, S. 2006 .*The Vulnerability of interdependent Critical Infrastructures Systems: Epistemological and Conceptual State of the Art*, EU report, EC JRC Ispra, 2006

Carpignano A. and A. Poucet, 1994, Computer assisted fault tree construction: a review of methods and concerns, Reliability Engineering & System Safety, Volume 44, Pages 265-278

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, Official Journal of the European Union, L 345/75, Published 23.12.2008.

Contini, S., Cojazzi, G.G.M., de Cola, G. 2006. On the exact analysis of non-coherent fault trees: the ASTRA package, *PSAM 8*, New Orleans, USA.

Ersdal G. and Terje Aven, 2008, Risk informed decision-making and its ethical basis, *Reliability Engineering & System Safety*, Volume 93, Issue 2, February 2008, Pages 197-205,

Lisnianski A. and G. Levitin, *Multi-State System Reliability. Assessment, Optimization, Applications*. World Scientific, New Jersey, ISBN 981-238-306-9, 2003.

Munda G. , 2008, *Social Multi-Criteria Evaluation for a Sustainable Economy*, XVIII, 210 p., Springer, ISBN: 978-3-540-73702-5

Platts, (2008), "Platts Natural Gas System of Europe", Commercially available data base. http://www.platts.com/

Pride R, Di Mauro C, Bouchon S, Logtmeijer C. 2008, *European Critical Infrastructure Directive Example Scenario - A Gas Transmission Network.* Ispra (Italy): European Commission - Joint Research Centre; 2008. JRC47726

Pride R., 2008 *A Gas Pipeline Model to Support Critical European Energy Infrastructure Assessment*. EUR 23434 EN. Luxembourg (Luxembourg): OPOCE; 2008. JRC43013

Reka A. and Barabasi, A.-L. (2002) 'Statistical mechanics of complex networks', *Reviews of Modern Physics* 74, 47, Obtained through the Internet: arXiv:condmat/0106096v1.

Reka, A., Jeong, H. and Barabasi, A.-L. (2000), 'Error and attack tolerance of complex networks', *Nature* 406, pp. 378-382, Obtained through the Internet: arXiv:cond mat/0008064v1

Renn O., 2008, *Risk Governance - Coping with Uncertainty in a Complex World,* The Earthscan Risk in Society Series, 368 pages, Earthscan, London, ISBN 9781844072927

Vesely W.E et al., Fault tree handbook. NUREG-0492, US Nuclear Regulatory Commission, Washington, DC (1981).[1]