Proceedings of the Seventh IASTED International Conference
POWER AND ENERGY SYSTEMS
August 29–31, 2007, Palma de Mallorca, Spain
ISBN Hardcopy: 978-0-88986-689-8 / CD: 978-0-88986-690-4

RELIABILITY AND SECURITY ANALYSIS OF ELECTRICAL INDUSTRIAL SYSTEMS USING PROBABILISTIC NETWORKS

Gustavo Ramos
Electrical Engineering Department
Universidad de Los Andes
Bogotá, Colombia
gramos@uniandes.edu.co

Alvaro Torres
Electrical Engineering Department
Universidad de Los Andes
Bogotá, Colombia
atorres@concol.com

Jean-Pierre Rognon
Laboratoire d'Electrotechnique de Grenoble-LEG
INPG, France
Jean-Pierre.Rognon@leg.ensieg.inpg.fr

Mario Rios
Electrical Engineering Department
Universidad de Los Andes
Bogotá, Colombia
mrios@uniandes.edu.co

ABSTRACT
Currently, there is a major interest into get electrical industrial systems (EIS) with high levels of security, quality, reliability and availability (SQRA) because of EIS are the most critical infrastructure of many industries that uses sensible electronic loads or major processes based on electricity supply. Current SQRA analysis in EIS uses methodologies to evaluate the performance of the system under steady state conditions; however, these methodologies do not consider effects caused by instantaneous and/or transient disturbances. This paper presents a methodology in order to evaluate the security of the EIS considering SQRA factors and the system response to sudden disturbances produced by internal, such as short circuits, or external factors, as energy supply interruption. It is proposed the security analysis of EIS based on Bayesian Networks and generalized stochastic Petri Networks and they are tested on the IEEE 493 system proposed by the IEEE Gold Book. The obtained results allow the development of analysis of power quality phenomena influence on the security and reliability of the EIS. Also, the methodology allows the identification of both hidden failures and erroneous coordination of protections.

KEY WORDS
Industrial power system, security, probabilistic networks.

1. Introduction

Nowadays; it is required high levels of security, quality, reliability and availability (SQRA) in the electrical industrial systems (EIS) because of EIS are the most critical infrastructure of many industries that uses sensible electronic loads or major processes based on electricity supply. For this reason, there is an increased interest into count with tools that allow the security evaluation of the EIS and, at the same time, include power quality and reliability criteria for this evaluation [1], [2].

The reliability evaluation of EIS must consider not only the adequacy evaluation of the system but also the security analysis in order to define the system response to several disturbances [3]. Current reliability techniques model disturbances in a probabilistic way; however, they do not model the stochastic response of the power system [4] and the system is analyzed under steady-state conditions after the disturbances occur; such techniques are: zone branch [5], cut set [6], go [7] and reliability block diagram [8]. So, using these techniques, it is not possible to define indicators that include the temporal response of the EIS when sudden disturbances occur.

This paper presents a methodology in order to evaluate the security of the EIS considering SQRA factors and the system response to sudden disturbances produced by internal, such as short circuits, or external factors, as energy supply interruption. It is proposed the security analysis of EIS based on Bayesian Networks and generalized stochastic Petri Networks.

Firstly, the application of Bayesian networks to evaluate the reliability of EIS is shown and compared to traditional techniques [5], [6] and [8] in order to show that the methodology is suitable. Then, power quality impact on reliability is modelled by the Bayesian networks. In addition, the reliability indicators computation is modified in order to consider the temporal response of the system to evaluate the security of the EIS.

Generalized stochastic Petri Nets are used to evaluate the security of EIS looking for the operation sequence of protection devices when short circuits or unplanned energy interruptions arise. The Petri Net model is based on the operational states of the system [9] and on the unreadiness probability of each protection device [10]. Hence, the Petri Net model allows the computation of probability of each operational state of the system as function of probability of the appropriate operation of protection devices.

Proposed methodologies are applied to the IEEE 493 system for testing purposes. The obtained EIS security indicators show the impact of both cause-effect phenomena and operational sequence of protection devices. In this way, the SQRA proposed methodology offers a solid conceptual fundament and a practical tool for the analysis and design of EIS.

2. The SQRA Methodology

Security of EIS is defined as the ability of the power system to respond to sudden disturbances without supply interruption. So, the EIS's security analysis must evaluate non-appropriate response of the system, unnecessary operation of any device (such as protection device) and/or bad operation of some subsystem when a sudden disturbance occurs that affects the power quality and/or the reliability of the electrical system and, in consequence, puts in risk the own electrical infrastructure and the associated productive industrial processes.

The proposed Bayesian models are solved with the Bayesnet Toolbox of Matlab [11] and the Petri Net models are solved using the PetriNet Toolbox of Matlab [12].

2.1 Reliability and Security Assessment by Bayesian Networks

A Bayesian Network represents a complete probabilistic model of a system because of the joint probability of any state of the system is computed from both conditional probability distributions and the net topology [13].

A Bayesian network us a direct acyclic graph G=(V, E), where V represents the set of nodes that could be modelled as random variables, and E are the set of arcs that represents the probabilistic influences between these variables.

The construction of a Bayesian Network is intuitive and based on the logical connection among system elements (graph) and the conditional probability tables (CPT) between them [14]. The most useful logical structures are: series connection, parallel connection and k-N net.

Fig. 1 shows the logical connection for the series connection of two elements and, since this graph; the CPT is established, as Table I shown. R will be in operational (up) state of the system if the two elements are in operation (up state).

By contrast, if two elements are in parallel logical connection, R will be in operational (up) state if one of the two elements is in operation (up state). So, Table II shows the CPT for this case.

Another useful structure for the construction of Bayesian Networks is the k-N case, where k elements are needed for the correct operation (up state) of the system (or subsystem) R. Table III shows the CPT for a 2 of 3 k-N case, where R is in an up state if two of three elements are in operation.

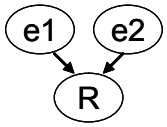

Fig. 1. Bayesian Network for modelling reliability performance of two elements connected in series

Table 1. CPT Series Connection of Two Elements

	Components	States			
	e1	up		down	
	e2	up	down	up	down
R	Up	1	0	0	0
	Down	0	1	1	1

Table 2. CPT Parallel Connection of Two Elements

	Components	States			
	e1	up		down	
	e2	up	down	up	down
R	Up	1	1	1	0
	Down	0	0	0	1

Table 3. CPT 2 of 3 Elements – Perfect Transference

	Comp	States							
	e1	up				down			
	e2	up		down		up		down	
	e3	up	dn	up	dn	up	dn	up	dn
R	up	1	1	1	0	1	0	0	0
	down	0	0	0	1	0	1	1	1

Once, the Bayesian Network is built using these structures; the system reliability is computed by computation of probability of the normal operational state.

Table I to Table III have assumed that the elements are perfect; this means that the operation of individual elements (as protection devices in the EIS) does not have uncertainty when a sudden disturbance occurs. That is the current assumption in traditional reliability techniques and it has been used for the evaluation of EIS reliability performance.

The EIS security assessment must include the uncertainty of individual elements (protection devices and others) as an extension of the EIS reliability evaluation. Therefore, the CPT is modified in order to incorporate the operational uncertainty of individual elements when a sudden disturbance is present.

As illustration of this uncertainty modelling, a CPT 2 of 3 k-N case is used. This case could represent an automatic transfer for an EIS where it is needed 2 of 3 generators for the appropriate supply of the system. Table III shows the CPT assuming perfect operation of the automatic transfer; however, real EIS have shown that the automatic transfer could fault when the transference is required [15] and, in consequence, the system could be arriving to an insecure state. The transference uncertainty is included in the CPT

by replacing the logical values (1 or 0) by the operational probability of the state success.

Table IV shows the CPT for the 2 of 3 k-N case assuming that the probability of a success transfer between generators is 95%. When 2 of the 3 generators are working and the transference is required, the probability of success is 95% (R in up state); while the failure probability is 5% (R in down state). On the other hand, there is not uncertainty if the three generators are in the same state (up or down); then, the system (R) maintains its state (1 or 0).

Table 4. CPT 2 of 3 Elements – Imperfect Transference

	Comp	States							
	e1	up				down			
	e2	up		down		up		down	
	e3	up	dn	up	dn	up	dn	up	dn
R	up	1	0.95	0.95	0	0.95	0	0	0
	down	0	0.05	0.05	1	0.05	1	1	1

Finally, the methodology for reliability and/or security assessment using Bayesian Networks follows these steps:

1- Define possible states for each system component (up and down, for example).
2- Compute the probability of each state for each system component based on historical data.
3- Build the Bayesian Network based on the logical connections of the system components. Definition of system states is made in this step.
4- Define the CPT for each connection in the Bayesian Network. If a security assessment is developed then uncertainty of operation of individual components must be modelled by probabilities.
5- Compute marginal probabilities of each state of the system.

2.2 Power Quality Effect on Security Assessment by Bayesian Networks

All EIS is exposed to internal and external factors that affect its normal operation. Power quality factors are among these factors, which could affect the electrical infrastructure, the industrial process' telecommunications network and the general production plant. A negative effect on these parts of the industrial system could provoke a total or partial shutdown of the productive processes.

As it is exposed, a cause-effect relationship could be established between external or internal disturbances that produce power quality perturbations (cause) on the industrial productive processes (effect) and these relationships must be modelled by Bayesian Networks.

The main power quality phenomena that can be modelled by relationship cause-effect are: sags and swells, harmonic distortion, electromagnetical transients and electromagnetical noise.

As, it was mentioned in section 2.1, the Bayesian Network construction is intuitive based on the logical connection of the elements of the system (in this case the EIS). As illustration, a Bayesian Network will be built for the study of the impact of electromagnetical transients on EIS security.

The main causes of transient phenomena in EIS are the atmospheric lightning, switching of capacitive banks and/or large loads switching. These transient phenomena are classified into impulsive or oscillatory (high, medium and low frequency) [16]. Damage or loss of configuration of telecommunications and control equipment and damage of power system equipment could be function of the type of transient phenomena and of the protection system (i.e. these are the effects on the system). Table V presents the steps included for the phenomena analysis and the characterization by nodes of each one with the possible states that each node can take.

Table 5. Definition of states and Variables for Bayesian Network Construction

Step	Nodes	States
Define phenomena, source and class	Lightning Flash Density	High, medium, low
	Point of strike	Direct, Near, Far flash
	Switching activity	Minor, multiple, Major
	Transient exposure	High, medium, low
	SPD exist?	Yes, no
Define first set of effect	Equipment damage	High, medium, low
	Operational upset	High, medium, low
Define final set of effect	Telecom process	No effect, upset, shutdown
	Production process	No effect, upset, shutdown
	Security	High, medium, low

Fig. 2 presents a graph that models the Bayesian Network for studying the impact of electromagnetical transients on the EIS security.

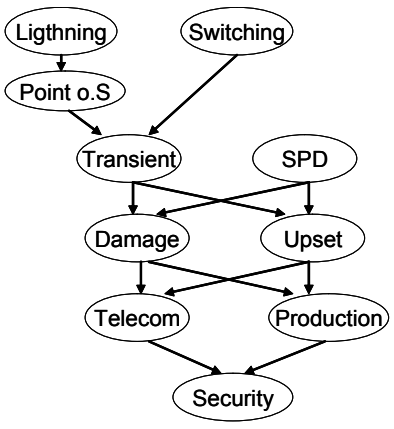

Fig. 2. Bayesian Network for Modelling Transient Phenomena in Security Evaluation

Finally, the methodology for EIS security assessment considering power quality impact using Bayesian Networks follows these steps:

1- Define power quality phenomena to be included. Define the sources of each particular phenomenon and classify phenomena on temporal or frequency domain.
2- Define the first set of effects on the EIS for each phenomenon that could be presented.
3- Define the final set of effects on the critical loads and on the productive processes and their relationship to the security of the system.
4- Build the Bayesian Network based on the logical connections of the system nodes. Definition of system states is made in this step.
5- Compute the CPT for each connection of the Bayesian Network.
6- Compute marginal probabilities of each state of the system.

2.3 Security Assessment using Petri Networks

Petri Networks (PN) allows the representation of the system behaviour by means of causal relationships between events and states in a sequential way. The stochastic Petri networks (SPN) are used when the transition time among several operational states follows a probabilistic modelling of exponential random variables and, in consequence, transition among system states can be represented by Markovian models. If logical transitions and exponential transitions are used simultaneously the Petri Nets are called generalized stochastic Petri Networks (GSPN). The Petri Nets are solved by simulation and has been used to evaluate the reliability of power systems [17].

A Petri Net is a particular kind of bipartite directed graphs comprises a set of places (P), a set of transitions (T) and a set of inputs (I) and outputs (O) and directed arcs (A). Arcs connect transitions to places and places to transitions. One particular state of a PN is defined by the number of tokens contained in each place denoted by vector marking M [18]. Then, a reachability graph is built from the possible sequence of transitions.

Fig. 3 shows a PN comprises by 3 places (p1, p2, p3), 4 transitions (t1, t2, t3, t4) and 4 arcs that connects transitions to places (t1 to p2, t2 to p3, t3 to p1, t4 to p1) and 4 arcs that connects places to transitions (p1 to t1, p1 to t2, p2 to t3, p3 to t4) and one token placed on p1. This token goes, by simulation, to places p2 or p3 by means of a sequence of transitions firings t1 or t2 and so on.

The initial marking M0 or state (1,0,0) specifies that the token is placed on p1 (see Fig. 3). As result of firing the transition 1, the PN reaches the marking M1 or state (0,1,0). Marking M2 or state (0,0,1) is reached by firing the transition t2. Since M1 or M2, the system returns to M0 by firing transitions t3 or t4, respectively. So, Fig. 4 shows the reachability graph for the PN of Fig. 3.

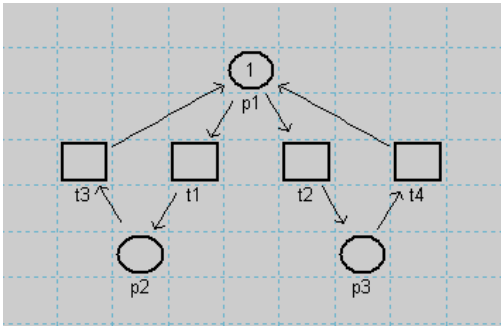

Fig. 3. A Basic Petri Network

As in any power system, such as the EIS, the relationship of all possible operational states of the system can be modelled by stochastic transitions. So, taking into account the system responses, it could be defined the following operational states: normal, alert, emergency, extreme emergency and restorative [9]. Fig. 5 shows the establishment of transitions between these operational states. In consequence, from these states, it could be stated that the EIS is secure if it is in normal, alert or restorative states. The EIS is non-secure if it is in emergency or extreme emergency.

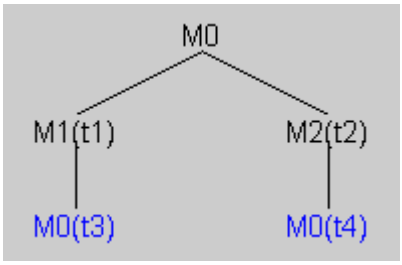

Fig. 4. Petri Net Reachability Graph

The main components, which are taken into account for the formulation of the PN with the purpose to define the operational states of the EIS according to Fig. 5, are de protective devices, such as: breakers, UPS, filters, among others. In the same way, the main events used in the PN formulation are: short circuits, interruption of energy supply and power quality problems.

Thus, taking into account the sequence operation of protective devices when a sudden disturbance occurs, the unreadiness probability, or the probability of non response of the protections when they are needed, is equivalent to the conditional probability of non-operation when the disturbance is present [10].

In the EIS, the non secure probability is computed from the probabilities that the system reaches an emergency or extreme emergency state when a sudden disturbance occurs (such as a short circuit) as function of the operation of main and backup protections.

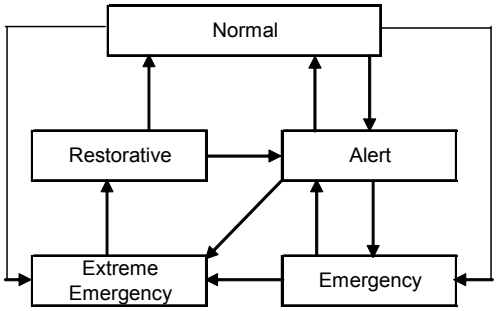

Fig. 5. Operational States in EIS [9].

Fig. 6 shows a PN for a basic protection system used in EIS, which is composed by a local primary protection (B2) and for a remote (backup) protection (B1). This PN can be used to evaluate the security of the EIS when a fault F1 take place downstream B2.

The normal state is represented by p1 and the system could reach the p2 state (faulted system) when the transition t1 occurs (short circuit at F). From p2, the system could reach p4 or p5 states by action of conflicting transitions t3 (action of the main protection B1 happens) and t4 (non-action of the main protection B1 happens), respectively. So, in p2 a logical decision is taken between action and non-action of the main protection modelled as a probability [10] of appropriate operation when it is required.

If the system has reached the p4 state, the transition t2 that represents the restoration of the system moves the system to the p1 state, i.e. to the normal operation state. By contrast, if the system reaches the p5 state (non-operation of the main protection), the same analysis is made for the operation of the backup protection device.

The model is easier to understand by means of the coverability graph, which is obtained when a validation of PN properties is run. The validated properties are boundedness, conservativeness, repetitiveness and consistency [19]. The PetriNet toolbox provides useful tools to obtain the coverability tree [12]. This graph shows all possible system states and their transitions in a consistent way to the PN diagram.

Thus Fig. 7 shows the coverability graph for the PN of Fig. 6, where M0 is the normal state that is moved to M1 (faulted system) when the short circuit at F happens (transition t1). As function of the main primary protection B1 response, the system reaches M2 or M3 states when transitions t3 or t4 happens. The system returns to the normal state M0 from the M2 state by the restoration transition t2.

If the main protection does not operate (state M3), it must be taken a decision between conflicting transitions (t6 operation and t5 non-operation of the backup protection device). If the backup protective device operates then the system will return to the normal state by the transition t7; however, if the backup protective device does not operate the system will be in an extreme emergency condition (state M4) and two restorative sequences could be taken place in order to bring the system to the normal state M0.

The direct association between the system states and the operation EIS system is made over the coverability tree by identification of alert, emergency and extreme emergency states, as Fig. 7 shows.

The security indicators are computed by simulations on the Petri Net. Thus, a 10000 probabilistic trials simulation has been made on the PN of Fig. 6 assuming a probability of 95% of appropriate operation of the main and backup protection devices. Thus, for each trial the token is moved through the system states by activation of transitions. The activation of transitions takes into account when a decision between conflicting transitions must take place.

As final result, Fig. 8 shows the conditional probabilities to reach the normal, emergency and extreme emergency states when a fault at F1 happens.

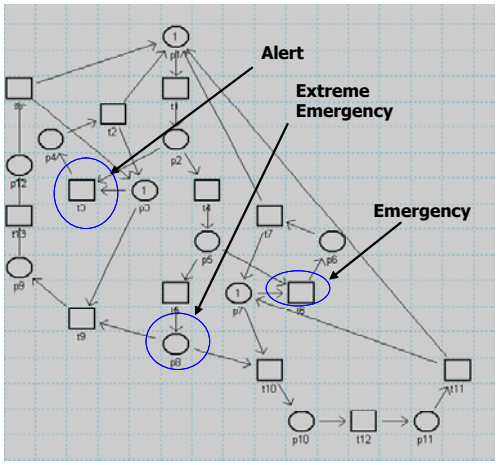

Fig. 6. Petri Network for the EIS basic protection system

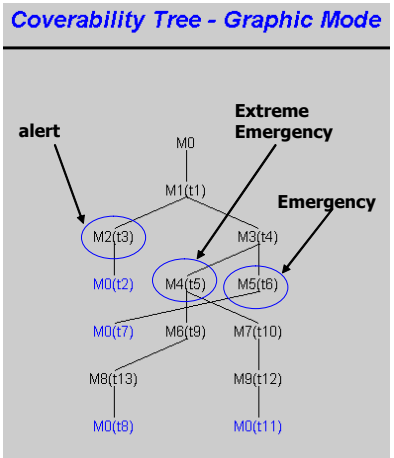

Fig. 7. Coverability Tree - EIS basic protection system

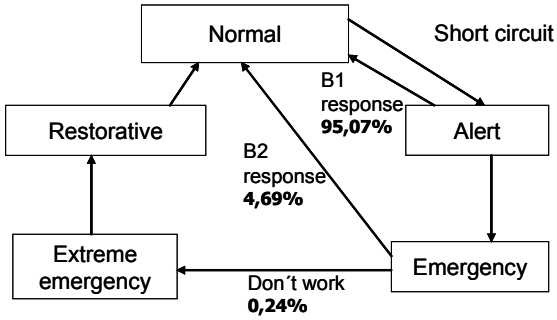

Fig. 8. Probabilities of Operational States Transitions

Hence, the methodology for security assessment using Petri Networks follows these steps:

1- Define the type of events to be analyzed.
2- Identify the protective devices.
3- Establish possible operation states for each device and the events that can cause its operation.
4- Define transitions among states.
5- Build, simulate and make the validation of the Petri Net.
6- Generate the reachability and coverability graph and identify the operational status of the EIS.
7- Compute security indicators.

3. Application of the SQRA Methodology

3.1 Test System

As test system was employed the IEEE 493 [4], developed to test methodologies of reliability evaluation in EIS. The Appendix presents an electric diagram of this system.

3.2 Reliability and Security Assessment by Bayesian Networks

The Bayesian Networks methodology was employed for computing the reliability of the following switchgears of the IEEE 493 system:

- Generator bus
- Main Bus A and Main Bus B
- Mechanical Bus A and Mechanical Bus B
- Lighting Bus
- Non-critical loads

In the first case, it is shown that for each generator there is a series logical connection of elements e3i (generator i), e6i (cable for generator i) and e8i (generator breaker i). The operation of minimum two generators is needed to supply the total demand (a 2 of 4 k-N structure) and the switchgear operation (E22) must be in operation. So, E22 is in a series connection to the k-N structure. Finally, the switchgear operation states are function of its protections devices (E8). So, the Bayesian Network for evaluation of the reliability of the Generator bus is built, as Fig. 9 shows.

Each element has two states: operation and non-operation. Their availability is computed from failure and repair rates [4].

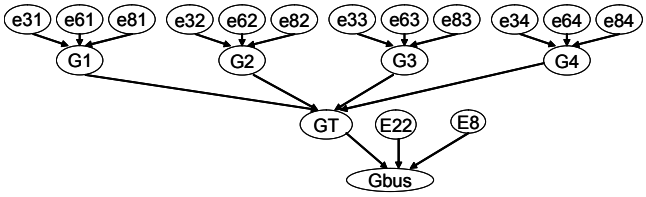

Fig. 9 Bayesian Network for Reliability Computation at Generator Bus - IEEE 493 System

Bayesian Networks for the other study cases are developed by the same procedure. Based on these Bayesian Networks (BN), the reliability for each bus is computed. Table VI presents the results using the Bayes modelling compared to traditional tools results (RBD, Zone and Branch, Cut Set) [4]. Table VII shows for the same cases, the estimated out of service time. These tables show that the BN is an valid methodology to compute the reliability indexes in EIS.

Table 6. Bus Reliability – Comparison of Availability Results – IEEE 493 System –

Bus	Bayes	RBD	Zone-Branch	Cut Set
Generator	0.9999963779	0.99999576	0.999649	0.99999638
Main bus A, B	0.9999906096	0.99999063	0.999443	0.99999061
Lighting	0.9999887889	0.99998878	0.999440	0.99998879
Noncritical	0.9999874643	0.99998880	0.999440	0.99998961
Mechanical	0.9999743359	0.99997454	0.999410	0.99997419

Table 7. Bus Reliability – Comparison of out of service Time (hours) – IEEE 493 System –

Bus	Bayes	RBD	Zone-Branch	Cut Set
Generator	0.03173057	0.0371424	3.074739	0.0371400
Main bus A, B	0.08225922	0.0820812	4.876143	0.0822296
Lighting	0.09820905	0.0982872	4.907155	0.0981796
Noncritical	0.10981292	0.0981120	4.907215	0.0909809
Mechanical	0.22481711	0.2230296	5.172254	0.2261322

Security assessment could be computed by assuming a non-perfect transference between generators at the generator bus. The computation has been made using a CPT for the 2 of 4 k-N case assuming that the probability of a success transfer between generators is 95%. As result, the unavailability changes from 2 minutes/year (result from reliability analysis with perfect transfer) to 29.4 minutes/year (using the imperfect transfer model).

3.3 Power Quality Effect on Security Assessment by Bayesian Networks

Fig. 2 has shown the Bayesian Network for studying electromagnetical transients in the EIS. It is assumed that the probabilities of high, medium and low atmospheric lightning activity are 75%, 20% and 5%, respectively. Also, it is assumed probabilities of 65%, 30% and 5% for a high, medium and low number of switching of the capacitive bank.

Table VII presents marginal probabilities for the security of the system for both cases: existence or not of a surge protection device (SPD). This table states that with a SPD the security of the system is high with a probability of 72%; while without the SPD the security is medium or low.

Table 8. Marginal Probability – Security Assessment - Electromagnetical Transients Case - IEEE 493 System

System	State	Probability (%)	
		with SPD	without SPD
Security	High	71.9	0.8
	Medium	16.9	40.7
	Low	11.2	58.5
Telecom	High	7.6	53.4
	Medium	9.8	25.8
	Low	82.6	20.8
Production	High	9.5	56.8
	Medium	11.0	25.9
	Low	79.5	17.3

3.4 Security Assessment using Petri Networks

The security indicators are computed by simulations on its Petri Net. Thus, a 10000 probabilistic trials simulation has been made on the PN assuming a probability of 95% of appropriate operation of the main and backup protection devices and for the automatic transference between generators. Thus, for each trial the token is moved through the system states by activation of transitions. The activation of transitions takes into account when a decision between conflicting transitions must take place.

Fig. 10 shows that the system could be in an extreme emergency state with a probability of 0.93%; while in an emergency state the probability is 12.56%. The system will be in secure states in a 87.43% when a fault (short circuit) occurs in the system.

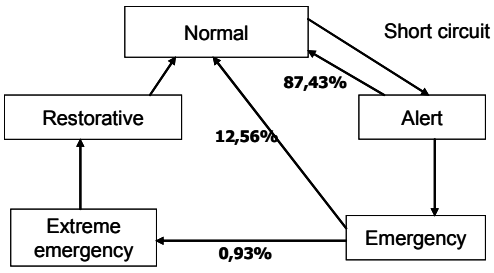

Fig 10. Operational States for the Main Bus A

4. Conclusion

This paper has shown that Bayesian Networks and Petri Networks are useful tools for computing security indices in EIS. As, it was shown, the Bayesian Networks can compute the reliability traditional indices and the same network could be used to compute security indices, with the appropriate changes in the characterization of perfect or imperfect components of EIS.

Also, the Bayesian Networks has shown that are useful for studying power quality phenomena that can affect the EIS. These studies allow the evaluation of effect to use some particular protective system or not by measurement of its impact on the EIS security.

On the other hand, this paper has shown that Petri Networks is useful tool to evaluate the security of the EIS based on the possible sequence of operation of protection devices.

References

[1] C. Gellings, M. Samotyj & B. Howe, The future's smart delivery system: Meeting the demands for high security, quality, reliability and availability, *IEEE Power and Energy Magazine*, 2(5), 2002, 40-48.

[2] M.F. McGranaghan, Quantifying reliability and service quality for distribution systems, *IEEE Transactions on Industry Applications*, 43(1), 2007, 188-195.

[3] M. Ali, Z.Y. Dong, X. Li & P. Zhang, RSA-grid: a grid computing based framework for power system reliability and security analysis, *IEEE Power Engineering Society General Meeting, 2006*, 1-7.

[4] D.O. Kobal, X. Zhang, J. Prost, T. Coyle, R.G. Arno, & R. Hale, Reliability methodologies applied to the IEEE Gold Book standard network, *IEEE Industry Applications Magazine*, 9(1), 2003, 32-41.

[5] D.O. Kobal, L. Jiao, R.G. Arno & P.S. Hale, Zone-branch reliability methodology applied to Gold Book standard network, *IEEE Transaction on Industry Applications*, 38(4), 2002, 990-995.

[6] T. Coyle, R.G. Arno, P.S. Hale, Application of the minimal cut set reliability analysis methodology to gold book standard network, *Proc. IEEE/IAS Industrial and Commercial Power System Conference*, Chicago, IL, 2002, 82-93.

[7] T. Coyle, R.G. Arno, P.S. Hale, Go reliability methodology applied to gold book standard network, *Proc. IEEE/IAS Industrial and Commercial Power System Conference*, Chicago, IL, 2002, 73-81.

[8] W. Wang, J.M. Loman, R.G. Arno, P. Vassiliou, E. Furlong, D. Ogden, Reliability block diagram simulation techniques applied to the IEEE std. 493 standard network, *IEEE Transactions on Industry Applications*, 40(3), 2004, 887-895.

[9] R. Billinton, M. Fotuhi-Firuzabad & S. Aboreshaid, Power system health analysis, *Reliability Engineering and System Safety*, 55, 1997, 188-195.
[10] P.M. Anderson, *Power system protection* (Wiley, 1998).
[11] K. Murphy, The bayes net toolbox for Matlab, *Computing Science and Statistics,* 33, 1-20, available: http://citeseer.ist.psu.edu/murphy01bayes.html.
[12]M.H. Matcovschi, C. Lefter, C. Mahulea, O. Pastravanu, Petri net toolbox for MATLAB in web analysis and design of discret-event systems, *Proc. 16th International Federation of Automatic Control World Congress*, Prague, 2005, pp 1-6.
[13] D. Yu, T.C. Nguyen & P. Haddawy, Bayesian network model for reliability assessment of power systems, *IEEE Trans. on Power Systems*, 14 (2), 1999, 426-432.
[14] P. Weber & L. Jouffeyen, Complex system reliability modelling with dynamic object oriented Bayesian network, *Reliability Engineering and System Safety*, 91, 2006, 149-162.
[15] R.J. Marceau & J. Endrenyi, Power system security assessment: A position paper, *Electra*, 175, 1997.
[16] *IEEE Recommended for Monitoring Electric Power Quality*, IEEE Standard 1159-1995
[17] W. Schneeweiss, Tutorial: Petri nets as a graphical description medium for many reliability scenarios, *IEEE Transactions on Reliability*, 50, 2001, 159-164.
[18] M.A. Marsan, G. conte & G. Balbo, A class of generalized stochastic Petri nets for the performance evaluation of multiprocessor systems, *ACM Transactions on Computing Systems*, 2(2), 1984, 93-122.
[19] J. Wang, *Timed Petri Nets, theory and applications* (Kluwer Academic Publisher, 1998).

Appendix

The following figure shows the IEEE 493 system.

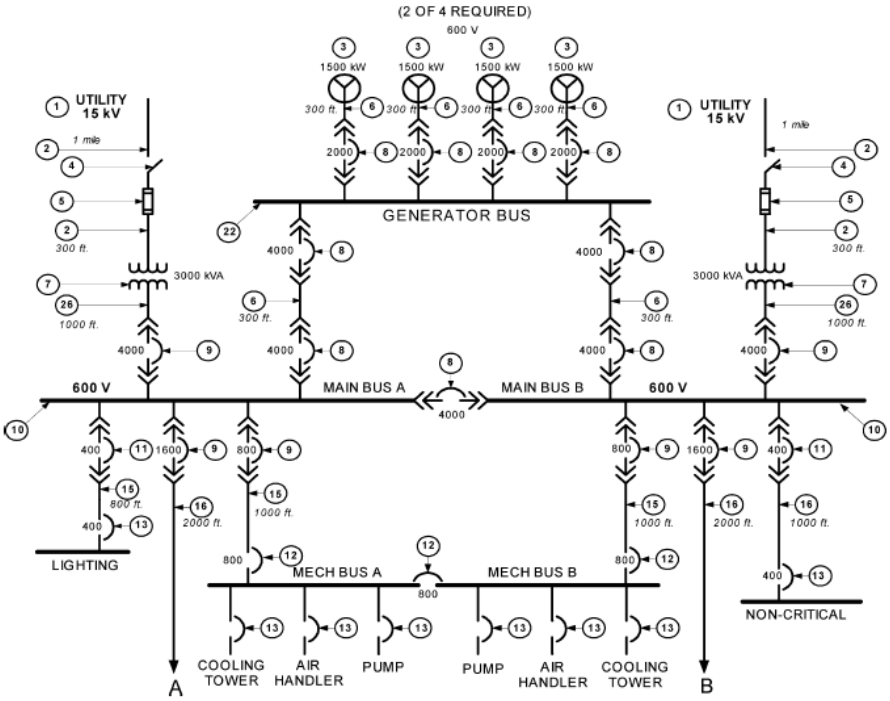

Fig. 11. IEEE 493 test system [4].