ÉVALUATION DU RISQUE POUR LA SÉCURITÉ DES RÉSEAUX ÉLECTRIQUE FACE AUX ÉVÉNEMENTS INTENTIONNELS

Carolina Tranchita

INSTITUT POLYTECHNIQUE DE GRENOBLE

N° attribué par la bibliothèque
|__|__|__|__|__|__|__|__|__|__|

THESE EN COTUTELLE INTERNATIONALE

pour obtenir le grade de

DOCTEUR DE L'Institut Polytechnique de Grenoble
et
de l'Université de LOS ANDES

Spécialité « Génie Electrique »

préparée au laboratoire de Génie Electrique de Grenoble

dans le cadre de **l'Ecole Doctorale**

« Electronique, Electrotechnique, Automatique et Traitement du Signal »

présentée et soutenue publiquement

par

Leidy Carolina TRANCHITA RATIVA
Ing. MSc. en Génie Electrique

le 30 Avril 2008

RISK ASSESSMENT FOR POWER SYSTEM SECURITY WITH REGARD TO INTENTIONAL EVENTS

Directeurs de Thèse : M. Nouredine HADJSAID
M. Alvaro TORRES MACIAS

JURY

M. Jean-Claude SABONNADIERE	, Président
M. Rune GUSTAVSSON	, Rapporteur
M. Xavier GUILLAUD	, Rapporteur
M. Nouredine HADJSAID	, Directeur de thèse
M. Alvaro TORRES MACIAS	, Directeur de thèse
M. Mario RIOS MESIAS	, Examinateur

INSTITUT POLYTECHNIQUE DE GRENOBLE

N° attribué par la bibliothèque
|__|__|__|__|__|__|__|__|__|__|

THESE EN COTUTELLE INTERNATIONALE

pour obtenir le grade de

DOCTEUR DE L'Institut Polytechnique de Grenoble
et
de l'Université de LOS ANDES

Spécialité « Génie Electrique »

préparée au laboratoire de Génie Electrique de Grenoble

dans le cadre de **l'Ecole Doctorale**

« Electronique, Electrotechnique, Automatique et Traitement du Signal »

présentée et soutenue publiquement

par

Leidy Carolina TRANCHITA RATIVA
Ing. MSc. en Génie Electrique

le 30 Avril 2008

ÉVALUATION DU RISQUE POUR LA SÉCURITÉ DES RÉSEAUX ÉLECTRIQUE FACE AUX ÉVÉNEMENTS INTENTIONNELS

Directeurs de Thèse : M. Nouredine HADJSAID
M. Alvaro TORRES MACIAS

JURY

M. Jean-Claude SABONNADIERE , Président
M. Rune GUSTAVSSON , Rapporteur
M. Xavier GUILLAUD , Rapporteur
M. Nouredine HADJSAID , Directeur de thèse
M. Alvaro TORRES MACIAS , Directeur de thèse
M. Mario RIOS MESIAS , Examinateur

REMERCIEMENTS

Je tiens tout d'abord à remercier mes directeurs de thèse, Messieurs Nouredine HadjSaid professeur à l'INP Grenoble et Alvaro Torres professeur à l'Université des Andes pour m'avoir guidée, encouragée et conseillée, tout en me laissant une grande liberté dont j'espère avoir été à la hauteur.

Alvaro je vous remercie pour toutes ces années de formation et pour m'avoir donné la possibilité de travailler avec vous à l'Université des Andes en Colombie. Depuis l'année 2000 j'ai fait tous me projets de recherche avec Maria Teresa et vous. J'ai été toujours impressionnée par votre intelligence et votre savoir faire.

Nouredine je vous remercie de m'avoir reçu dans l'équipe Systèmes et Réseaux Electriques (SYREL), et avoir accepté cette cotutelle. Merci de m'avoir donné beaucoup de confiance et de liberté pendant ces trois ans. J'ai beaucoup d'admiration pour vos qualités scientifiques, votre goût pour le travail et ainsi que pour votre gestion. J'ai apprécié énormément vos qualités humaines et également votre soutien quand j'ai eu mes problèmes de santé. Je vous exprime mon profond respect, ma gratitude et toute mon amitié.

Je remercie aussi Maria Teresa de Torres pour son soutien depuis l'année 1999. *Maria Teresa* vos conseils ont été toujours pertinents et adéquats, j'ai démarré cette thèse grâce à vous.

Je tiens à remercier les membres du jury:

Jean Claude Sabonnadiere, professeur émérite à l'Institut National Polytechnique de Grenoble et conseiller du président de l'INP Grenoble, merci de m'avoir fait l'honneur de présider le jury. *Jean Claude*, je vous remercie pour vos conseils, vos corrections et votre intérêt sur mes travaux de thèse.

Xavier GUILLAUD, professeur des universités à l'École Centrale de Lille (ECL), rattaché au Laboratoire d'Électrotechnique et d'Électronique de Puissance (L2EP), merci d'avoir accepté d'être rapporteur et avoir porté de l'intérêt à mes travaux.

Rune Gustavsson, professeur des universités à Blekinge Institute of Technology en Suède, merci d'avoir accepté d'être rapporteur et avoir porté de l'intérêt à mes travaux.

Mario Alberto Rios Mesias, professeur à l'université des Andes en Colombie, merci d'avoir accepté d'être membre du jury. *Mario*, vous avez apporté tout au long de ma thèse un intérêt certain pour le sujet et les résultats et vous avez toujours cherché à les mettre en valeur. Merci pour les corrections de ma mémoire, vous avez été très rigoureux et merci aussi d'avoir fait le déplacement à la soutenance.

Je remercie également Messieurs Seddik Bacha et Daniel Roye, responsables de l'équipe pour m'avoir accueillie au sein de l'équipe SYREL.

Je remercie l'ancienne direction du G2ELab (M. Yves Brunet et Jean Paul Ferrieux) et la nouvelle (M. James Roudet, Yves Marechal et Olivier Lesaint) pour m'avoir accueilli dans le laboratoire et permis de faire cette thèse.

Je remercie Benoit Rozel pour les discussions sur ma thèse, leurs corrections de français et bien sûr pour son amitié. Merci également à Maria Viziteu pour son aide dans le dernier chapitre du document.

Pendant ces années de thèse, j'ai rencontré des gens magnifiques de cultures très diverses qui m'ont appris beaucoup de choses. Cette richesse culturelle fait de ce laboratoire un endroit magnifique.

Je remercie tous mes amis du labo pour les inoubliables moments passés ensemble. Je commence avec ceux de ma génération : Bogdan E., Octavian E., Silvye C., Diana M., Erwan P. et Gustavo R., aussi les anciens du laboratoire : Stefan S., Cristophe G., Miguel F. et Olivier R. Merci mes amis SYREL : Lina R., Maria A., Dan O., Bianca O., Didier B., Marie-Cecile A., Yann R., Asma M., Maxime L., Philip T., Alexandre T., Damien P., Szymon, Khaled A., Diem, les non SYREL : Jérémie A., Marcel E., Benjamin V. et les Colombiens Andrea H., Natalia R., Alejandro L., Monica O., Aline C. et Jorge A. (los mex's).

La liste est trop longue, alors merci à vous tous mes collègues, permanents et le personnel du laboratoire G2Elab pour les bons moments passés ensemble (pots de thèses, pot de noël, journées scientifiques, repas d'équipe, tournoi de foot, concours de pâtisserie…)

Je remercie mon mari Fabian Leistikow pour sa patiente, son soutien et ses encouragements continus pendant ces années de thèse. Merci *Mi Fabileine* pour tes réflexions et ta vision très critique des choses. Je te remercie pour les discussions sur les problématiques sociales qui touchent cette thèse. Merci pour ton amour et j'espère compter sur toi toute ma vie !

Cela va de soi, je remercie évidemment ma famille pour son irremplaçable et inconditionnel soutien, même si j'étais de l'autre côté de l'atlantique. Gracias Mami, Papi, Abuelita, Wilson, Juli, Tia Ligia, Andres F., Juan C., Camila, Fabian, la familia Gonzales y Esperanza y flia. Muchas gracias a todos los amigos y familiares en Colombia que vinieron a la espectacular fiesta que me organizaron los de mi casa!

Merci Dieu pour me permettre de faire et finir ce doctorat.

TABLE OF CONTENTS

INTRODUCTION

THE ELECTRICAL NETWORK AS A MAIN CRITICAL INFRASTRUCTURE

Electricity is a vital service. The electrical power system is a set of networks and assets offering a service of public nature essential for the society and its economy. It is recognized as a critical infrastructure because a partial or total loss of one or more of its components may have negative economical, environmental, political, or social incidence and affect the welfare of societies in general [CE, 2004].

Due to the interdependence of other systems with the electrical power network, and due to the current dependency of human economical activities on power systems, a single fault in the electrical system can cause cascading effects, the interruption of a considerable number of basic services and catastrophic damages. Since electricity cannot be easily stored or rerouted, the generation must instantly match the demand. Interruption of the service can have severe economic consequences and threaten human life. The existing synergy between different infrastructures is a key point in this process.

Historically, interruptions in electrical energy have played a central role in the disruption of many other infrastructures. The California crisis of 2001, the electricity blackout of August 2003 in the United States and Canada and the blackout in Italy, illustrated the strong dependency between electricity and other sectors of the energy market that were affected, e.g. oil refining, oil and gas pipelines and potable water distribution [FLE, 2001], [TF, 2004]. In the same way, in crisis situations caused by disastrous events, the electrical network plays and will play a more and more significant role. On many occasions the network itself is the origin of this type of crisis.

The power system is also dependent on other infrastructures. Some power plants need energy sources as gas and oil. Pipelines disturbances can affect electricity generation. Operation, control, protection and management of power systems are highly dependent on communication systems. Telephone, satellite and computer networks are used at different levels. Data acquisition from devices and equipments, communication among control centres, substations and other utilities, frequency and voltage control, automatic protection are possible thanks to communications networks [SHA, 2003]. As a consequence, damages in these infrastructures can cause damages in the power system.

Because of this relevance, the electrical sector has been and will continue to be a target of outlaw groups, ill-disposed people, and terrorist groups that intend to interrupt the system.

Especially the constant threat of terrorism throughout the world makes it reasonable to assume that the electrical network is permanently in danger of attacks. Considering the interdependency with other systems, a direct or indirect attack on electrical assets can entail severe economical consequences, threaten human life and finally induce terror in civil populations [AMI, 2002], [ZER, 2005].

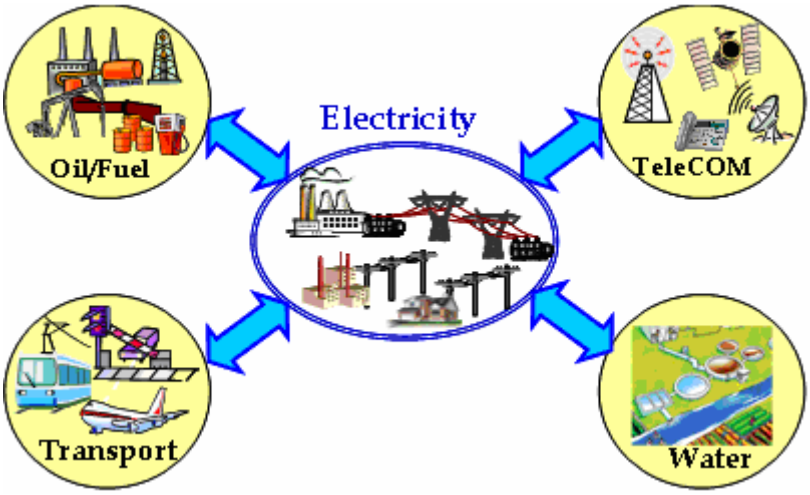


Figure 1. The electrical system in the core of the critical infrastructures.

Countries with internal conflicts like Peru, Colombia and Iraq have demonstrated and continue to demonstrate that the attack of electrical infrastructures is a common tactic and electric power systems are the most important targets.

Different types of attack scenarios can be distinguished. The electric infrastructure may either be a target, a weapon or be affected indirectly:

1. The electrical infrastructure is a target if the main purpose is to damage, to a higher or lower degree, an individual or several components of the system. The component may be critical for the system operation or be significant for the population. Typical examples are the attacks with conventional weapons on key power plants. But the infrastructure can be used as a means of harassment. In this case the objective is not to affect the system but to demonstrate power in public. EPRI defines this type of action as "attack upon the power system" [AMI, 2002]. It is also possible to use another infrastructure as a weapon to harm the power system. A particular case is the use of computer technology either as a weapon or as a target of an attack to harm the power system. This type of attack may be qualified as so-called cyberterrorism.

2. The electrical infrastructure is a weapon if the infrastructure is used to damage another infrastructure or to harm individuals. Terrorists could e.g. use nuclear plants in order to disperse nuclear material which is used in these installations. EPRI distinguishes two types of targets when the power system is a weapon. If the target is the population, this constitutes an "attack by the power system"; if the target is the civil infrastructure, it is qualified as an "attack through the power system" [AMI, 2002]. As in these scenarios the power system is not the target, operation or integrity of the electrical system might not necessarily be affected.

3. The electrical infrastructure may be indirectly affected if other infrastructures are subject to attacks. Although not directly targeting the electrical sector attacks can interrupt the operations of an electrical system due to interdependencies of the power systems and due to the geographical location of its components.

The continuity of organized and systematic global terrorism has demonstrated that an attack against an electricity system is an issue concerning all countries and not just those currently undergoing an internal conflict. Many countries are currently subject to threats and generally to the possibility of attacks that jeopardize the security of power systems. While in most of the industrialized nations such damages to their systems have not been experienced in the post-World War II era, it is possible that deliberate attacks against such systems will occur in the future. Recent attacks on non-electrical infrastructures in New York and Washington on September 11, 2001, Russia and Madrid in 2004 and London in 2005 and 2007 have demonstrated that the threat is real.

The unavailability of structures such as power plants, lines, or towers, and services such as telecommunication, which support the electrical power network, reduces the capacity of energy transmission between electricity generation centres and big consumption centres. In case of an attack assets may fail to continue their operation leading subsequently to unavailability in supply, which can affect in different degrees the security and reliability of an electrical system as a whole.

Taking into consideration the terrorist threat for security assessment

Security has been defined as the ability of a system to withstand sudden disturbances and losses or failures of system components [KUN, 2004]. Security assessment is one of the most important activities of planning and operation of an electric power system. Dealing with the security of a power system only before natural events is not enough to satisfactorily overcome the economic and technical challenges imposed on this type of system. A suggestion is made to analyse the security of power systems in the present world and to consider the occurrence of terrorists' acts.

Therefore, in the power system security assessment process, the materialization of terrorist threats must be considered. In this way, proper decisions in planning and operating the power system can be taken and an appropriate balance between operative cost and robustness can be reached.

The use of ICTs as weapon to attack the power grid

The information and communication technologies (ICTs) that support the operation of the power system can also be attacked and be used as a weapon to finally affect the power system and interrupt the electric power supply. Given the characteristics of the cyberspace and the vulnerabilities of the ICTs, it is reasonable to consider that this might occur. The literature dealing with the security of electrical infrastructure widely recognizes the importance of considering the threats on ICTs and suggests evaluating the risk but a detailed approach on how to handle this challenge has not been yet presented.

One of the principal problems of evaluating the impact of attacks on ICTs and in the behaviour of power systems is the modelling of the interdependency between ICTs and the power grid. Open models and tools of simulation that allow a modelling of this interdependency are currently not available.

The uncertainty present in the problem

The main problem of considering terrorism in security studies is the kind of uncertainty present in this type of event: vagueness and ambiguity. It is difficult to create "possible" and "probable" scenarios. It is not actually possible to use traditional statistical tools because there is no wide database available which concerns the changing nature of motivation and other variables influencing terrorist acts.

At the same time in a security study it is advisable to consider the uncertainties present in load and generation. Therefore, a deterministic approach may not be the best solution since all uncertainties are neglected and a "frequentist" approach of the probability may lead to erroneous models of the uncertainties present in the study.

This work

Being able to deal with these terrorism situations, will depend to a great extent on the anticipation capacity, the reflection in no-crisis times (off-line) and the operational management on the side of the owners of critical infrastructures.

In the last few years and especially after September 11th, numerous governmental organizations, private groups, utilities and universities around the world are studying the terrorist threat against critical infrastructures. Choice of targets, weapons, behaviour of terrorists, counterterrorism and impact of the service offered by the infrastructure are the main topics of investigations.

The main objective of this thesis is the security analysis of a power system and the definition of indicators that allow the risk level of a power system to be assessed. The objective mainly includes the consideration of the threat situations and the operation conditions resulting from terrorist activities against the security of system components as well as of the system. This security assessment takes into account the uncertainty of the variables involved from the probabilistic and possibilistic or vagueness perspectives.

In this thesis, attacks upon a power system are particularly examined. We divide the analysis into two parts: the physical attacks on the power grid and the cyberattacks on the information and communication system. Analysis and models of the motivation of attacking the electrical infrastructure, terrorist groups involved, targets and weapons used, were accomplished in order to know how these factors influence the terrorist attacks on the power system. A study of postcontingency operation conditions is made in order to evaluate the impact of terrorist attacks on the electrical infrastructure and the consequences for the security of the power system.

Route map of the following chapters

This thesis is structured in the following 6 chapters:

The First Chapter offers a general overview on what is understood by "terrorism" and a world-wide overview on terrorist attacks on electrical infrastructure. Thus the motivations of terrorism, the goals, the targets and the used weapons are analysed. This study allowed us to establish the most important variables and the relations of causality that influence the decision to attack, the selection of the targets and the possible consequences on the

threatened infrastructure. Likewise, in this chapter we approach the topic and offer a definition of cyberterrorism. An analysis of the Colombian case and of the world situation of terrorist assaults against electrical infrastructure is done in Chapter 1 and elaborated in Appendix A.

In the Second Chapter the reader will find a review of the state of the art of power system security assessment. We recall some important definitions and suggest some modifications in the literature on power systems with the intention of incorporating terrorist acts in the security analyses.

In the Third Chapter we analyze the different types of uncertainties present in the security studies on power systems. This study allows us to understand and to choose the most adapted approach to model every type of uncertainty. Likewise, the principal approaches to model uncertainties used along this thesis are detailed; especially the probabilistic inference and more exactly the Bayesians networks and the theory of fuzzy sets and the theory of possibilities.

Physical attacks on the power grid that can affect the power system operation are analyzed in Chapters 4 and 5, and the cyberattacks on the communication and information system of the power systems are dealt with in Chapter 6.

In the Forth Chapter we describe the proposed method for ranking contingency resulting from physical attacks against electrical power grids. Based on the study done in the first three chapters and the experts' elicitation we use the Bayesian networks to model the most important variables of the problem of security assessment bearing in mind the terrorist threat. The Bayesian networks enable us also to model the causality relationships among these variables. Apart from the contingency ranking we obtain via the Bayesian network the probabilities of the attack for every component modelled of the power system.

In the Fifth Chapter a suggestion for calculating an index based on risk is made in order to assess the security of a power system after the occurrence of terrorist attacks. For this purpose we use the theory of probability to model the occurrence of an attack. In addition, the theory of possibility is used to model the uncertainty of power injections. By using the fuzzy load flow and possible types of arithmetic of fuzzy numbers we can establish a measure of possibility that a security problem of the power system occurs. We use the results of the Fourth Chapter to choose the group of contingencies which will be analyzed. However, the method presented in the Fifth chapter for the security assessment can be applied for the analysis of contingencies no matter their causes.

In the Sixth Chapter we analyze the problem of cybersecurity of the information and communication system affecting the security of the power grid. Based on a study on how the cyberattacks happen, on the terrorist motivations to use the ICTs as weapons, on possible security measures, and the vulnerabilities of ICTs, we use Bayesian networks again with the intention of assessing the risk for the security of power systems.

Finally we present in this document the conclusions and the perspectives of this research.

CHAPTER I

1 THE PHENOMENON OF TERRORISM

The events on September 11, 2001 will forever stay in our memories. With the murder of thousands of innocent people, terrorism has escalated to an unprecedented level. At the same time the attacks reminded us that the environment we live in may be under more threat than we used to believe.

Many people were surprised by the danger that seemed to come out of the blue. However, terrorism is a dynamic process, and not a chain of incidents without a history. Terrorists have learnt to integrate previous ideas into their attacks. The concept of using civilian aircrafts as bombs in suicide attacks was not new. There were indications before 2001 that this kind of event could happen. For example, in 1986 in Pakistan a TWA airliner was seized. The hijackers reportedly intended to fly the aircraft to Israel with the aim of crashing it into the centre of Tel Aviv [HOF, 2002]. Algerian terrorists hijacked an Air France flight in 1994 with the intention of crashing the aircraft in Paris. French commandos recaptured the aircraft while it was on the ground in Marseille [SHP, 2003]. We do not know how much information terrorist groups such as al Qaeda had about these operations.

Today we know from experience that the electrical infrastructure of numerous countries is a key target for terrorist groups. In countries such as Peru, Colombia, El Salvador, Pakistan and Iraq attacks on the electrical system were and continue to be a common tactic, the aim being the collapse of the entire power system. The accidental blackouts that occurred in the Northeast of the USA and in Italy in 2003 demonstrated how a successful terrorist attack on the electrical system of a highly industrialised country could potentially have disastrous effects.

As much as modern technology contributes to the wealth of high-tech societies, its progress makes them more vulnerable to attacks from small groups, which have the potential to cause widespread effects. The increase in the destructive capacity of small groups is mainly owed to two reasons.

The first reason is that the key characteristics of weapons i.e. accuracy, destructive power, range, portability, ease-of-use, and affordability, have significantly improved. Significant attention is given to the so-called NBC-terrorism which involves the use of weapons of mass destruction. Both the number of people that could be affected by such an assault and its psychological effect could potentially be enormous. But unlike conventional arms NBC-weapons are still relatively difficult for insurgent groups to acquire and to handle.

The second reason is the vulnerability of modern societies, which stems from their dependence on a multitude of economic and technological systems. These so-called critical infrastructures consist of networks that affect all areas of daily life, including electrical power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking and finance, emergency and governmental services, agriculture, and other fundamental systems and services. These systems are often comprised

of components that are packed with energy, combustibles, and poisons, giving terrorists ample opportunity to divert such technologies to destructive ends. Critical infrastructures are highly interconnected and interdependent in complex ways. Disruptions in one infrastructure can directly or indirectly affect other infrastructures and hence affect large geographic regions, having devastating effects on national security, the economy, and every citizen's life. Terrorists can magnify the effects of their assaults by exploiting the features of complex and interdependent networks.

This thesis particularly focuses on the challenge of maintaining the security of electrical infrastructure. The dependence of major infrastructural systems on a continued supply of electrical energy is well recognized. Information technology (e.g. internet), telecommunications, transportation, food and water supply, homes, and worksites are all dependent on electricity. Electrical infrastructures have widely dispersed assets that can never be absolutely defended against a determined attack. Terrorists might exploit this vulnerability of the electrical infrastructure. In order to cause as much destruction as possible to high-tech societies, terrorists will probably launch attacks in a form as unexpected as on September 11, 2001. Thomas Homer-Dixon [HOM, 2004] showed what a future attack could look like. He described an attack on the USA, a highly industrialised country which depends a lot on technology. In the US the electricity grids are already under strain due to the massive population. The attack that Homer-Dixon describes involves many simultaneous attacks on the power system across America, with terrorists releasing things such as aluminium chaff and balloons over power lines in order to cause massive short cuts and consequently a cascade of power failures across the country. The effects of such an attack would be disastrous, all traffic lights, water, sewage and communication systems would all be disabled, and the financial system and national economy would come to a complete halt.

The goal of this thesis is to develop methodologies and tools for determining/quantifying the risk of terrorist attacks against the electrical infrastructure, in order to reduce the potential consequences on power system security. The protection of this infrastructure implies a notion of the terrorists' strategy. In order to understand and combat terrorism we need to have a grasp of the way it works. Thus, most importantly we have to know: What are the mechanisms of terrorism?

1.1 No Single Accepted Definition of Terrorism

Terrorism is a subject strongly linked to emotions. It may create fear, desperation, and uneasiness, a feeling of defence, hunger for sensation, malicious joy, or even fascination. This variety of emotions corresponds to a certain ambiguity in the term itself. Despite the frequent condemnation of terrorism by governments, international organisations, and intellectuals, they are incapable to agree on a single definition of terrorism.

One of the reasons why consent on an international definition could not be reached is that numerous countries as diverse as Israel, Kenya, Cyprus and Algeria owe their independence at least in part to nationalist political movements that employed terrorism against colonial powers. Many countries argue until now that anyone or any movement that fought against "colonial" oppression and/or Western domination should not be described as "terrorist", but were properly deemed to be "freedom fighters". What distinguishes a terrorist organisation from a liberation movement? In November 1974 the chairman of the Palestine Liberation Organization (PLO) Yassir Arafat explained in the United Nations General Assembly: "The difference between the revolutionary and the terrorist lies in the reason for

which each fights. For whoever stands by a just cause and fights for the freedom and liberation of his land from the invaders, the settlers and the colonialists, cannot possibly be called terrorist …". After the assaults in London and Sharm el-Shaik in 2005 the Organisation of Islamic Conference (OIC) and the League of Arab States insisted that a UN treaty should exempt all those engaged in conflicts against "foreign occupation" and not deem them to be terrorists. [DEE, 2005].

Terrorism usually has connotations of evil intent, indiscriminate violence, or brutality. It is generally applied to one's enemies and opponents. As the use of the term implies a moral judgement, any party who successfully attaches the label terrorist to its opponent indirectly persuades others to adopt its moral viewpoint. Cynics have often commented that one man's freedom fighter is another man's terrorist. Some intellectuals maintain that it is neither possible nor worthwhile to find an explanation of the word terrorism. However, having a definition of terrorism is essential when considering its occurrence in the world. How do you distinguish a terrorist group from a non-terrorist group? What types of terrorism exists? What are the motivations of terrorists? What measures of protection against terrorism can be taken?

1.2 Definition of Terrorism

Rather than providing a discussion of the different definitions that already exist, the approach of Bruce Hoffmann [HOF, 1998] will be adopted throughout this thesis. In order to escape from definitional paralysis, Bruce Hoffmann suggests distinguishing terrorism from other types of violence, and identifying the characteristics that make terrorism the distinct phenomenon of political violence that it is.

Hoffman defines terrorism "*as the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change*." His definition comprises five key elements that allow distinguishing terrorism from other forms of crime. "Terrorism is ineluctably political in aims and motives, violent – or, equally important, threatens violence, designed to have far-reaching psychological repercussions beyond the immediate victim or target, conducted by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia), and perpetrated by a sub-national group or other non-state entity.

The first key element of this definition is that the violence is undertaken primarily for political reasons. It is about the pursuit of power, the acquisition of power, and the use of power to achieve a political change. While political objectives are a key aspect for defining terrorism, the goals that are sought by the terrorists can fall into a number of categories. The terrorists may be seeking to have a government change its policies. The political objectives may involve an effort to change leaders or the political elite. Goals may go further, seeking to bring about a complete change in the framework of the government – changing from a monarchy to a republic or from a strongly centralized system to a more decentralized one or from a military dictatorship to a theocratic state run by religious leaders. Finally, the terrorists may be seeking to change national boundaries – to detach a region to create a new state, to attach some territory to another state, or to amalgamate existing states into a new country.

The second element is violence, or as equally important is the threat of violence. Actual violence is fairly obvious to detect and recognise. The threat of violence is only likely to be

effective as a technique with a group that has already demonstrated that it is able and willing to be violent. Once violence has been used, the threat of additional violence may generate the necessary fear that the dissident group desires and lead the government to give in to the demands of the group, whatever those demands might be.

The third key element of the definition is an act designed to have far-reaching psychological repercussions beyond the immediate victim or target. For violence to qualify as terrorism, it must affect a target audience beyond the immediate victims. Influencing such audiences is part of the attempt to achieve the political objectives of the organisation. The key to reaching their target group is the media. In modern society, media allows millions of people worldwide to be informed of important news in a very short space of time. Victims such as children, women, or innocent bystanders also communicate the message, e.g. that anybody may share the victims' destiny if they obstruct the terrorists' objectives. Terrorism is a strategy of communication. Terrorists need to reach their target audience by using violence as a symbol. The atrocities committed by terrorists are a means by which they attract media attention and therefore the attention of a wider public. In 1972 members of the Palestinian organisation "Black September" kidnapped athletes from Israel during the Olympic Games in Munich. The operation itself failed. All of the hostages and the majority of the terrorists were killed. However, the attention of people around the world was drawn to the cause of the Palestinians. When PLO chairman Yassir Arafat talked later in the General Assembly of the United Nation the problem was being discussed in all countries across the world. In this respect the operation was a full success. After the US invasion of Iraq in 2003 Muslim extremists, and particularly al Qaeda, attempted to erode the US's political influence in this country. Although Iraq's electrical infrastructure was already damaged by former allied bombings it was again subjected to numerous assaults[1] after the war. Reportedly, the shortage of electrical energy in 2005 was a huge source of Iraq's public anger. The Iraqis voted "inadequate electricity" as a higher political priority than "crime", "the presence of coalition forces", and "terrorists" [MUR, 2005]. The inability of the US to re-establish electrical power supply punctured the Iraqis' belief in the Americans' technical superiority and power. In countries that are constantly subjected to terrorist attacks, e.g. Colombia, the inability to protect their population against assaults may undermine the credibility of the government's power.

The forth key element of terrorism is that terrorist groups have an organisation with an identifiable chain of command or conspiratorial cell structure. An individual acting on his or her own initiative cannot be called a terrorist. Even if the tactics and targets of a single person and a group are identical, an individual will hardly be able to carry out the actions or reach the target audience which would be required to change a political system. An effective campaign to create change requires repeated efforts over time. This cannot be achieved by a single person since they would most likely be caught very easily, as it would be difficult to hide their activity if working alone. As stated before, terrorists pursue political goals. The motivation of an individual is likely to be personal rather than political, unless the objectives are shared by others. Just as an individual cannot claim to be a political party he or she cannot be considered to constitute a terrorist organisation.

The fifth key element that allows us to define terrorism is the distinction of state-directed terror and violence by non-state entities. The differentiation between state and non-state violence is a point of debate [STO, 2002, 2005]. Including or excluding state acts in the term

[1] Statistics 2003-2005.

of terrorism serves different political agendas. Equality between governments and dissident groups is established if state actions are included. This may promote the objectives of dissidents. Eliminating state-directed acts serves the agenda of states that use terror as a means of politics. Terrorism and state-directed violence share some characteristics, which imply that they could be put in the same category, e.g. the intention to gain power by spreading fear. The use of "death squads", the unconcealed intimidation of political opponents, human rights workers, student groups, trade union representatives, and journalist are effective means by which total power can be seized within a state. But there are profound differences which strongly suggest that the not putting the two phenomena into the same category. Governmental "terror" is far more deadly than violence committed by non-state entities. Practices of mass repression employed by totalitarian states such as Nazi Germany, Stalinist Russia, Mao's China during the Culture Revolution, Central American right-wing regimes of the 1960s and 1970s or African and Asian states in the post-independence era, resulted in the death, exile, imprisonment and suppression of millions of people.

In comparison with terrorist groups, repressive political regimes have much less to risk and therefore act unscrupulously. This difference may explain the higher bloodshed of state-directed violence. Terrorists live a risky life. They are likely to be killed or imprisoned for life. The "security personnel" of authoritarian regimes do not have to fear anything. They can pursue their activity without being punished. As terrorist groups are weak they have to watch out for allies. This restrains their strategy of violence. Totalitarian states may employ violence pretty much without taking notice of the reaction of the population.

1.3 Terrorist Strategy

Terrorism is the strategy of relatively small and weak groups. It is the extreme form of what can be called an asymmetric conflict constellation. Terrorist groups lack sufficient combat strength and backing in a population to occupy territory and to openly attack the government. They only survive by hiding and by running small, precise operations. If they do not comply with these rules of behaviour they run the risk of becoming a target themselves and being either arrested or killed. These groups have to be very careful of who they allow to be members. If they become too numerous spies might intrude and destroy the group. This fact restricts their possible field of activities. They cannot prepare a wide front of resistance that requires a high number of people. Instead they have to rely on well prepared attacks, which are supposed to attract attention to them and their goals.

The typical terrorist line of thought is threefold. First, a terrorist act is committed or publicly announced. Secondly, terrorists intend to evoke a strong emotional reaction, feelings of fear and panic among their enemies, support and agreement from sympathetic people. Thirdly, terrorist assaults intend to provoke panic-driven reaction such as acts of retaliation or protection and active support and cooperation in their combat. Three different groups are involved in terrorist acts. The terrorists themselves, the victims, and the audience group which is supposed to be influenced. Within the audience group two subgroups have to be distinguished. The enemies and potential future victims of the terrorists are on one side and the sympathisers, who are supposed to be animated to support the terrorists in their combat, are on the other side.

In very general terms terrorism can be described as a form of provocation. The stronger enemy shall be unmasked as the true attacker once he overreacts and appears to be brutal,

unfair, or excessive. In order to make the mechanism work two conditions have to be met. The violent message has to be understood and the audience groups have to be able to react as wished by the terrorists.

1.4 Categories of Terrorist Groups

Although various terrorists groups may apply similar strategies there are elements that allow a distinction between different dissident movements. Their ideology plays a key role as it is the basis on which the group was founded and by which their endurance over a long period of time can be explained. Four different main motives exist. However, it is often difficult to draw a sharp line between motives as some groups are driven by more than one thing. Terrorism may be justified by religion; it may be based on ethnic and national motivations, or it may be based on extreme left- or rightwing ideologies.

It has to be considered that terrorist groups reflect a social-historical background specific to the region or country where they are founded. Examples will be given in order to illustrate each category that terrorist groups can fall into. The intention, however, is not to give a comprehensive overview of existing terrorist group as this would go beyond the limits of this thesis.

1.4.1 Terrorism justified by religion

The recent growing importance of terrorist activities by Islamist extremist groups and particularly al-Qaeda can be explained by two key events. In 1979 for the first time a revolution succeeded, which was not based on the political concepts of socialism or democracy. From the perspective of extremist groups Ayatollah Ruhollah Khomeini showed with the Islamic revolution that a movement based on religion can be successful against the Western world and its ideas. Furthermore, it offered a way to identify values that originated from their own culture.

The second key event was the reaction of the Muslim world to the occupation of Afghanistan by the troops of the Red Army in 1979. The invasion was considered to be an attack on Islam, which justification for the launch of a jihad in counterattack. Muslim fighters were recruited in many different states in order to fight side by side with the Afghans. In order to improve recruitment and the training of the fighters the Saudi militant Islamist Osama bin Laden founded al-Qaeda (the basis), an international network of fighters. When the Red Army left Afghanistan in 1989 many mujahedeen went back to their countries and formed or adhered to extremist groups. Until now the grade of internationalisation of these groups has been quite high. Although these groups use religion as a justification for their terrorist activities it can be stated that their objectives are mostly political, complimented by objectives that are derived from the political interpretations of Islam religion.

1.4.2 Ethnic and national bases of terrorism

Since the end of the 1960s ethnic-nationalist terrorism developed. Examples are the Palestine Liberation Organisation (PLO), the IRA in Northern Ireland, the PKK in Turkey, and the ETA in Spain. This type of terrorism is the most common one. The objectives of these groups are political independence, autonomy, or particular rights of co-determination. Ethnic-nationalist terrorism often coincides with leftwing extremist rhetoric. These groups usually

try to establish and maintain relations with legally accepted groups or parties in order to further their objectives.

1.4.3 Terrorism and ideologies of the left

Leftwing terrorists usually refer to the writings of Marx and Engels, and writings of later communists such as Lenin and Mao Tsetung. Their objective is the establishment of greater equality and the reduction or destruction of privileges and rank. Typical representatives of this category are the Baader-Meinhof Gang in West Germany, the Italian Red Brigades and the 17 November Organisation in Greece.

1.4.4 Terrorism and ideologies of the right

Rightwing terrorists usually stress the need for order and hierarchy, and the presence of ordering of groups in political systems. Their goal is to support existing institutions in society and the ruling elites, or to return these elites to power and re-establish institutions. Representatives of this category are storm troopers in Weimar Germany, neo-fascists in post-war Italy, the American militia, and neo-Nazis and skinheads in Europe.

1.5 Technology As a Target and Weapon

As indicated earlier, terrorism is an extreme form of an asymmetric conflict constellation. In order to reach their goal the dissidents need to take advantage of the vulnerable aspects of their opponents. The aspects of modern societies that are vulnerable to terrorist attacks are in the first place a consequence of integrated, highly efficient so-called "critical infrastructures" on which our daily lives depend. Other vulnerabilities result from the production of nuclear, biological, and chemical weapons of mass destruction. Consequently, modern technology is important for terrorists in two ways. It may be the object of an attack or a way by which the damages of an assault can be multiplied.

1.5.1 Technology as a target

Technology plays a key role in modern societies. Highly efficient and interconnected systems affect all areas of daily life, including among other things, electric power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking and finance, emergency and governmental services, and agriculture. These systems are critical to the security, economic prosperity, and social well-being of a country and can be referred to as "critical infrastructures". "Critical infrastructures" can be defined as the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defence and economic security, the smooth functioning of governments at all levels, and society as a whole [GER, 2006]. Disruptions within and across these systems could lead to widespread or catastrophic failures.

Where traffic intersections, production and distribution streams meet, where competences concentrate, and where information processes focus, in places such as airports, train stations, telephone exchanges, banks, insurance companies, seats of government, sport venues, or diplomatic conferences an attack would hit the centre of industrialized societies and provoke wide publicity irrespective of its success. The same goes for attacks on facilities of

production, storage, transmission and distribution of energy such as, barrages, power plants including nuclear plants, substations, electric towers, gasworks, water containers, and information networks.

Besides attacking individuals that represent their "enemies" terrorists seek to exploit the vulnerable aspects of the systems on which society depends. Attacking critical infrastructures can reduce the available resources of a country, and undermine confidence in its supporting systems. The continuity of the underlying structure of a society is one of its key success factors. Once people become dependent on the availability of services such as electricity, water, telecommunication, transportation of goods, or financial governance a relevant number of economic activities will not be engaged because of increased risks. If the enemy attacks a superior economic power, attacks against critical infrastructures are a logical step in an asymmetric conflict constellation.

In 1983 and in 1985 the Shining Path (sendero luminoso) sabotaged electrical transmission towers causing blackouts in Lima. In Colombia and Iraq the electrical infrastructure remains until today one of the main targets of insurgents' attacks. In February 2007 a Saudi Arabian terrorist group with ties to al Qaeda called for Muslims around the world to attack oil installations in order to stop the flow of oil to the US [REG, 2007].

The interconnection of the electrical infrastructure within and across other vital systems in highly industrialised countries can lead to widespread and catastrophic results in the case of their disruption. The outage of the electrical power system might cause cascading failures of oil and gas supply, water purification systems, or public transport. Recent blackouts in the US and Europe give us an idea of what the consequences of massive outages in industrialised countries could be.

On August 14, 2003 a massive power outage occurred throughout parts of the North-eastern and Midwestern US and Ontario, Canada. Electricity was fully restored by August, 16, 2006. About 10 million people in Canada and 40 million people in the US were affected [CBC, 2003]. Telecommunication systems remained operational in most areas although the increased demand left many networks overloaded. Mobile phones experienced significant service disruptions as transmission towers were overloaded with the sudden increase in volume of calls. Television and radio stations continued to provide services with the help of backup generators. Most interstate rail transport was shut down. The impact on international air transport was widespread. Passenger screening at affected airports became impossible. Electronic-ticket information was unavailable. Oil refineries on the East Coast of the US were shut down. Petrol production slowed down and many petrol stations were unable to pump fuel due to the lack of electricity. Canadian authorities considered patrol rationing. Some areas lost water pressure since pumps did not have power. The loss of water pressure entailed a boil water advisory as water was potentially contaminated. Large numbers of factories in the affected area were closed and others outside the area had to slow down production because of insufficient supply and the need to conserve energy. In urban centres like New York a gridlock occurred when people fled their offices. For hours the streets, highways, bridges and tunnels were jammed with traffic and pedestrians. Many commuters could not find sleeping arrangement and had to sleep in parks or on the steps of public buildings. Fire calls were reported, many from using candles or open fire to create light. Looting was reported from the cities of Ottawa, Ontario, and Brooklyn, New York. The losses related to the blackout were estimated at 6 billion US$ [TFO, 2004].

In the same year a number of European countries experienced widespread outages affecting more than 60 million people. The worst blackouts were the interruption of supply in South London on August 28, 2003, the power outage in Southern Sweden and Eastern Denmark on September 23, 2003, and the Italian blackout of September 28, 2003. In Italy it turned out to be the most serious blackout in 20 years. 56 millions people in the whole country except Sardinia have been affected. Restoring power to the whole country took up to 18 hours. Luckily people did not panic as the lights were turned off in the streets of Rome because half a million people were celebrating the "Notte Bianca". As the blackout happened on a Sunday morning the financial damages were limited to about 120 million € due to spoiled food and belated opening hours of shops and restaurants. As in the Northeast blackout in the US and Canada people were stuck in trains and subways. Flights were cancelled or delayed and the outage of traffic lights led to chaotic situations in major urban areas. In Southern Italy the water supply was interrupted for 12 hours. Although internet data transfer went down to 5% of its normal value telephone and mobile phone networks underwent a critical state but remained operable. Due to diesel-driven generators in hospitals health services could be maintained [GER, 2006].

The experiences with blackouts in North America and Europe show that terrorist attacks against critical infrastructure, namely electrical infrastructure can draw attention to a specific agenda because if committed at the right moment and at the right place there is a high probability that essential social functions will be disrupted and widespread panic, fear and devastating economic losses will be created.

1.5.2 Technology and weapons

Weapons are of particular importance for terrorists. In the past terrorist groups avoided the risk of failure by using weapons that they could control easily and which they had already proved to be efficient. Their operations could be qualified as "conservative" because they operate according to a specific pattern. Their weapons of choice were the bomb and the gun. The techniques evolved as the dynamite bomb was replaced by the plastic bomb, heavy machine guns were replaced by lighter automatic guns. Furthermore, terrorists learnt how to use electronics and photo mechanics in order to place bombs precisely and to have them explode at a precise moment. Even the use of manually controlled missiles did not constitute a change in traditions as they simply were based on conventional technology. Some bombs proved to be particularly deadly. They were going off in passenger aircrafts causing the death of hundreds of people. Security agencies for airliners or airports developed detection systems that made it harder to place bombs in planes. The improvement of weapons and detection systems is an ongoing battle between terrorists and security. For every weapon rendered ineffective, a new weapon will be developed. As technology provides higher capacity to cause damages, it will also provide mechanism to protect against assaults. In the course of time terrorists took advantage of developments in the technical field as much as in the strategic-tactical field.

Terrorists depend on high attention of the media and a wide public, i.e. the physical effect of an assault might be less important than the psychological effect. In the latter case weapons of mass destruction, i.e. nuclear, biological, or chemical weapons (NBC terrorism), and cyberterrorism bear clear advantages for terrorists. By using these weapons higher attention of the media and the public can be raised as during the years people have become used to reports on conventional assaults except for spectacular attacks. The mere threat of a NBC attack can raise a high level of fear and panic in a population. People react sensitively on

incidents in the domains of health, leisure time, and in their immediate living environment. Therefore, threats in these areas are particularly suitable to put governments under pressure. This does not only go for terrorists that are capable to run NBC attacks but also for those who simply pretend to have such capabilities.

Economic losses and a high level of fear can be created by egotistic individuals, imitators and other ill-minded people. Terrorist include this kind of behaviour in their calculations as it amplifies the effect of the threat. The terrorists' objective in using NBC weapons is not to cause mass casualties. Their goal is to attract public attention and not warfare. They only need small amounts of the deadly agents to cause a considerable effect. Access to the agents is not a major obstacle. An intrusion, manipulation, sabotage, disruption or even destruction of a computer system that controls a nuclear power plant, an electrical power control centre, substations, electronic banking, global stock markets, international traffic systems, water supply purification and distribution systems, may have similar public effects as the usage of NBC weapons because of the large number of people that could be affected by such an incident, as well as the possible proportions that it could reach.

1.5.3 Nuclear weapons

Two categories of nuclear devices have to be distinguished. Nuclear bombs require fissile material that can be split in a self-sustaining chain reaction. The fission energy is used to produce a violent explosion. A radiological weapon (or radiological dispersion device) is any weapon that is designed to spread radiological material. It is known as a "dirty bomb" because it is not a true nuclear weapon and does not yield the same destructive power.

Different scenarios can be imagined:

- Terrorist could illegally acquire nuclear weapons or steal them. As long as the respective arm deposits are properly guarded this scenario seems to be less likely.
- Another way of preparing a nuclear assault would be the acquisition of weapons grade uranium or plutonium and of know-how regarding the construction of nuclear weapons.
- In a third scenario terrorists could construct a radiological weapon. In this case explosives are combined with radiological material. A nuclear chain reaction would not take place. Instead the radiological material would contaminate a relatively limited area. The dispersion of the material could damage the health, property of people, etc.
- A last scenario could be the attack of electrical power nuclear plants in order to disperse the nuclear material which is used in these places. This kind of attack is difficult to realise because of the heavy encasement and reinforcement of reactor buildings. Nevertheless, such scenarios play an important role in terrorist plans. It has repeatedly been reported that the only Australian nuclear reactor located in Sydney was the alleged target of terrorists groups. Early in 2007 newspapers reported that the research reactor was supposedly the target of a planned attack with stolen rocket-launchers.

1.5.4 Biological and chemical weapons

Biological and chemical agents are easily accessible since they are traded for medical use and can be bought legally. The access to bacteria can hardly be limited as they exist in the biosphere and may be isolated and cultivated. The know-how regarding the manipulation of these agents is publicly accessible, e.g. on the internet.

Besides the advantages of high media and public attention such weapons bear numerous disadvantages for the terrorists. The production and dispersion of these agents is difficult. The substances are too fugitive and unstable to be spread by air, for example in an aerosol. Biological agents are sensitive with regard to different environmental influences. Neither biological nor chemical weapons distinguish between enemy and friend. The terrorist might become victims of their own weapons.

1.6 Cyberterrorism

Another way in which terrorists could attack modern societies is the abuse of computer systems or networks, which once again demonstrates how the technological sophistication of society makes it vulnerable to attack. As computer systems become increasingly important for modern societies any intrusion, sabotage, disruption, or destruction might lead to effects that go far beyond the simple effect on the system itself. As stated earlier, the goal of terrorists is drawing public attention to their agenda. By attacking a form of technology used everyday by millions of people, terrorists would have hold of an effective tool by which they would spread fear in a large audience.

1.6.1 Definition of cyberterrorism as opposed to cybercrime

Cyberterrorism is a specific form of terrorism. Its main characteristic is the way in which it turns computer technology into either a weapon or a target of an attack. However, the abuse of new technologies is not limited to terrorists. As for "terrorism" it is necessary to define "cyberterrorism" in order to identify the attackers and the way in which computer systems and networks can be protected against cyberterrorism.

The term of cyberterrorism has continued to change in definition since the 1980s when Barry Collin first described it as the "convergence of cyberspace and terrorism". As no written or agreed definition exists, the definition is as ambiguous as the term terrorism. Some authors expanded the scope of the term labelling aggressive non-violent acts or acts of major computer disruption as cyberterrorism [COL, 2006]. Such wide definitions of cyberterrorism, however, have the tendency to stigmatise individuals who use the internet for criminal or non-criminal goals that are not related to terrorism. In the scope of this thesis terrorism is defined as the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change [HOF, 1998]. Acts that cannot be qualified as fear-inducing or violent or acts that are conducted by people without any political motivations are not qualified as terrorist acts outside of cyberspace. Definitions of cyberterrorism that turn hackers, individual crackers, and financially minded cybercriminals and organisations into cyberterrorists are likely to attain fundamental rights of citizens in liberal societies. Once governments start to take action against what is understood as cyberterrorism. Measures taken against law infringements shall commensurate with the gravity of the infringement. The protection of society against terrorist attacks deserves a priority that differs from the protection of society against simple crimes. The goal of a suitable definition of cyberterrorism should therefore be the identification of the true target of action.

A crime is an act that infringes criminal law and that entails punishment if the person committing it is found guilty. Cybercrime is an infringement of criminal law in cyberspace, e.g. the selling or transport of contraband, the theft of property including people's identity or the host of other offences deemed inappropriate by societies. Crime legislatures ultimately determine the labelling of criminals and the application of law on a given individual's

actions. In the last few years highly sophisticated criminal gangs have committed fraud or collected propriety information by exploiting vulnerabilities in business networks. Their activities remain the source of most serious losses. As cyberspace encompasses jurisdictions of different countries, cybercriminals still often circumvent prosecution by operating in countries that have either weak or nonexistent cybercrime laws, or lack the resources of law enforcement. As crime legislation itself differs from country to country it is hard or even impossible to draw a straight line between cybercrime and cyberterrorism. The difficulty is not to bring severe terrorist acts under the rules of criminal law as these acts usually inflict enough violence or threat of violence against people or property to constitute a crime. As a result cyberterrorism can always be qualified as cybercrime. It is much harder to define when a criminal act committed in cyberspace shall not to be qualified as cyberterrorism.

The particularity of cyberterrorism compared to terrorism in general is that the action takes place electronically. However, if the intention is to spread fear in a target population for political purposes it cannot make any difference whether the objective is reached by means of physical violence or threat of violence or by electronic means.

Therefore, in the scope of this thesis the following definition of cyberterrorism is suggested: *Cyberterrorism is the deliberate creation and exploitation of fear through violence or the threat of violence resulting from acts against information, computer systems, computer programs, and data, in the pursuit of political change conducted by an organization with an identifiable chain of command or conspiratorial cell structure, and perpetrated by a sub-national group or other non-state entity.*

Considering this definition, legal hacking, the use of computing resources in a legal manner to solicit societal change (hacktivism), and even entering into computer systems by breaking protective mechanisms (cracking) do not constitute cyberterrorism.

1.6.2 Scenarios of cyberattacks

Cyberattacks are a form to attack that is cheaper and less risky in comparison with a physical attack. Neither explosives are needed, nor arms or vehicles. They are less risky, because they are anonymous. The identity can be hidden in the internet and physical barriers such as customs or the borders between countries do not exist. Also, a cyberattack is physically less risky, since there is no corporal exhibition during the attack i.e., mortality risk for the attacker is practically zero.

The fact that modern societies are increasingly dependent on systems that are interconnected with the internet gives way to a great variety of possible attacks. There are numerous targets and due to the systems' complexity numerous vulnerabilities and weaknesses that may be exploited by terrorists.

According to an internet security threat report of July 2002 [BEL, 2002] "Power and Energy, Financial Services, and High Tech sectors suffered relatively high rates of attack activity, while industries, such as E-Commerce and Manufacturing suffered relatively moderate to low rates of attack activity". As hackers, crackers, and cyber criminals depend on the services of the reportedly more intensively attacked sectors for their activities, there is some likelihood that the attacks originate from terrorists.

Power generation and transmission utilities are quite an attractive target for terrorists. The physical distribution and control structures that are used to administer the grid are vast and

cover great distances. This involves a significant amount of work in maintenance, control, and transportation. The administration of these various tasks has been improved by the implementation of electronic information and communication systems (ICS) that better govern daily operations, and provide critical data for load balancing. Attacks concentrate on system vulnerabilities of the ICS.

Individuals with insider information may electronically access protective equipment and change settings such that the equipment either fails to operate when it should, causing bus, line, or transformer damage, or operates when it should not, causing service interruption.
Another possible scenario is the access of a cyberterrorist to the system after having discovered the phone number of a modem connected to the substation computer. Login information could be acquired through social engineering or password attack. Once having accessed the system the cyberterrorist could alter or destroy data, reset devices, and block or re-route communications. This would potentially affect electronic devices, intelligent electronical devices (IED), controllers and the supervisory control and data acquisition (SCADA) systems.

1.7 Terrorism Against Electrical Infrastructure - World-Wide Situation

Numerous countries around the world have experienced attacks on electrical infrastructure. The number of terrorist attacks has been documented around the world in the last decades. The data on these attacks are available in the terrorism data base, which is maintained by the National Memorial Institute for the Prevention of Terrorism in the US (www.MIPT.org).
The MIPT Terrorism Knowledge Base has classified terrorist acts depending on targets. In this data base the electrical sector infrastructures are classified as "utilities". Further details on voltage and power ratings and the technology used to make an exhaustive classification between generation, transmission, distribution and business infrastructures are not always available. The categories shown in Figure 1-3 are deducted from the description of the events found in the MIPT data base. It has to be taken into consideration that such categories may well be country specific because of the voltages levels or the electrical market structure.

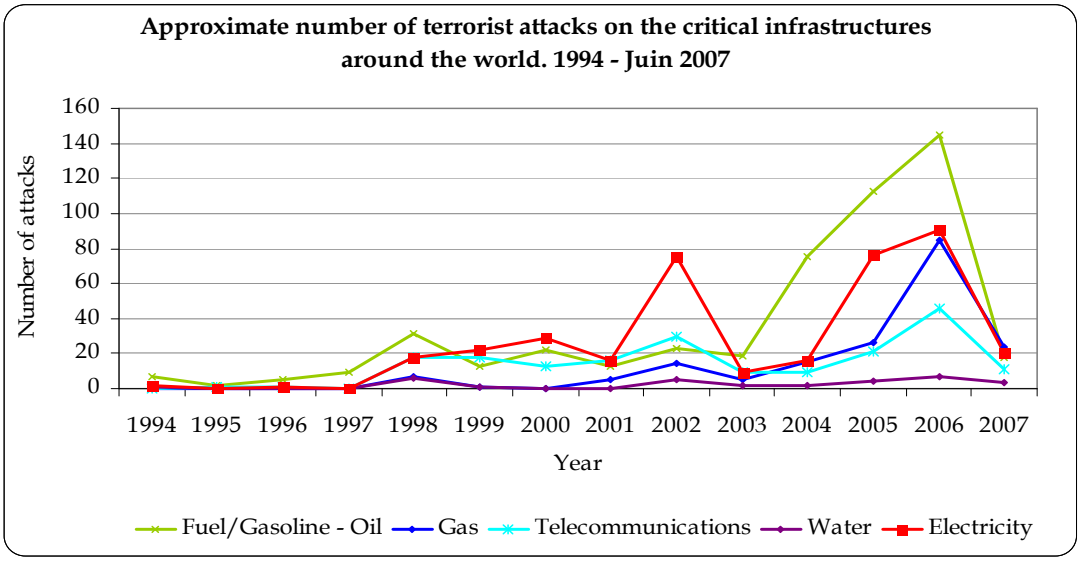


Figure 1-1. Number of terrorist attacks against the critical infrastructures worldwide: 1994 to June 2007. Source: Figure created by handling the information of the "National Memorial Institute for the Prevention of Terrorism (MIPT)" database.

The data base only includes events that were published through any local or international mass media, which limits the veracity of numbers. In some countries there have been policies against broadcasting terrorist attacks in order to avoid fear in their population. Figure 1-1 illustrates the trend of terrorist attacks against the critical infrastructures.

We can see that the electricity sector has been attacked continually in the period from 1994 to June 2007. Interdependency between electrical infrastructure and other critical infrastructure may entail cascading effects so that, e.g. attacks on telecommunications and oil infrastructures can produce damages in electrical networks.

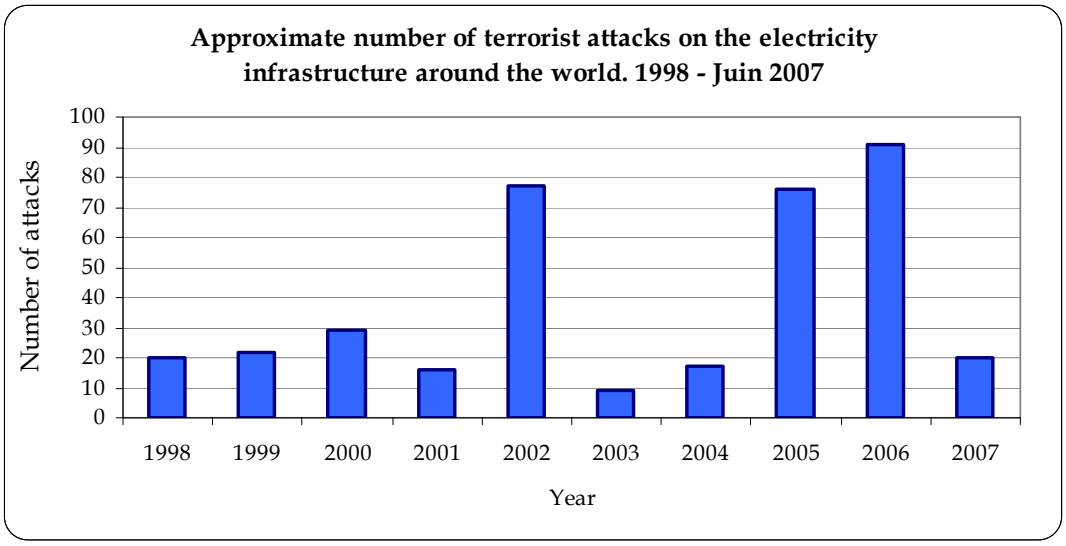


Figure 1-2. Number of terrorist attacks against the electricity infrastructure: from 1998 to June 2007. Source: Figure created by handling of information database of the "National Memorial Institute for the Prevention of Terrorism (MIPT)".

Figure 1-2 shows the number of terrorist attacks against the electricity sector for the same period. The countries concerned are: Colombia, Iraq, Pakistan, Spain, India, Russia, Sri Lanka, Afghanistan, France, Albania, Nepal, Thailand, Algeria, Israel, Turkey, Burma, Kashmir, Brazil, Indonesia, Peru, Chechnya, Georgia, Italy, Angola, Chile, Kosovo, Latvia, Paraguay, Philippines, Sudan, and Tajikistan. It can be observed that in 2005 and 2006 terrorism increased. The most active groups were in Iraq opposing the US's occupation of this country, the Islamic terrorism of the Al-Qaeda groups and Taliban in Pakistan and the FARC and ELN guerrillas in Colombia.

Figure 1-3 shows the results of an analysis of the information regarding attacked electricity infrastructures which can be found in the MIPT database. The different business functions of generation, distribution, transmission and others were identified. Yet this categorisation is approximate as the data available in the MIPT database does not allow identifying the exact characteristics of the business functions that were under attack.

The most attacked function is obviously transmission. Given the length of transmission systems, it is impossible to protect all of the assets whether by physical barriers or human resources. Most electrical towers are located in totally uninhabited zones which facilitates attacks. It just takes two or three people to down an electrical tower, an operation which is difficult to prevent using armed forces. Yet the impact of power outages on public opinion

can be enormous. Different cases are generation assets which are constantly protected either by civilian forces or in some countries by public forces.

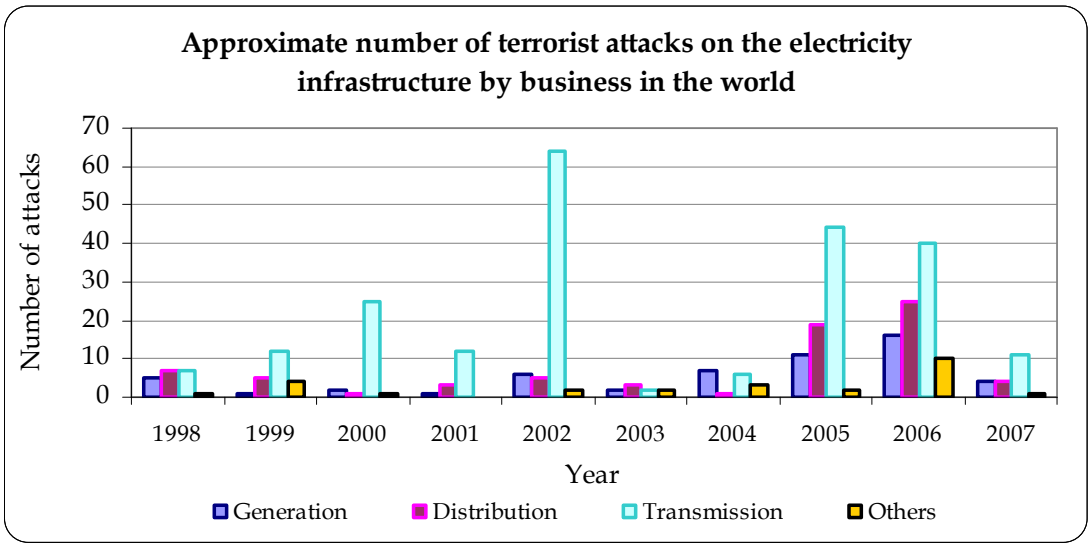


Figure 1-3. Approximate number of terrorist attacks against the electricity infrastructure: from 1998 to June 2007 discriminated by business function. Source: Figure created by analysis of database of the "National Memorial Institute for the Prevention of Terrorism (MIPT)".

The classification made in [ZIM, 2005] illustrated in greater detail what kind of terrorist attacks take place on electric infrastructure. Four different groups can be distinguished:

1. Attacks on generation infrastructure, which includes attacks on power generation stations and dams.
2. Attacks on substations (transmission and distribution), which includes attacks on equipment as well as on the transformers of substations.
3. Attacks on transmission lines and their components, such as the pylons.
4. Attacks on other network components of the distribution network and the electrical commercialization infrastructure. This includes for example attacks on invoicing offices, utility poles and human resources.

Figure 1-4 shows the distribution of these events, depending on the target of attack and the previous classification based on [ZIM, 2005].

In Table 1-1 we can see percentages of the total number of attacks that occurred throughout the world in the period between 1994 and June 2007 classified by countries derived from the MIPT database. Nearly half of the attacks occurred in Colombia. Other highly affected countries are Iraq being the second most affected country; Pakistan and Spain occupy the third and fourth position respectively. In each of the remaining countries less than 3% of the attacks have happened, which corresponds to 10 or less attacks during the last 13 years.

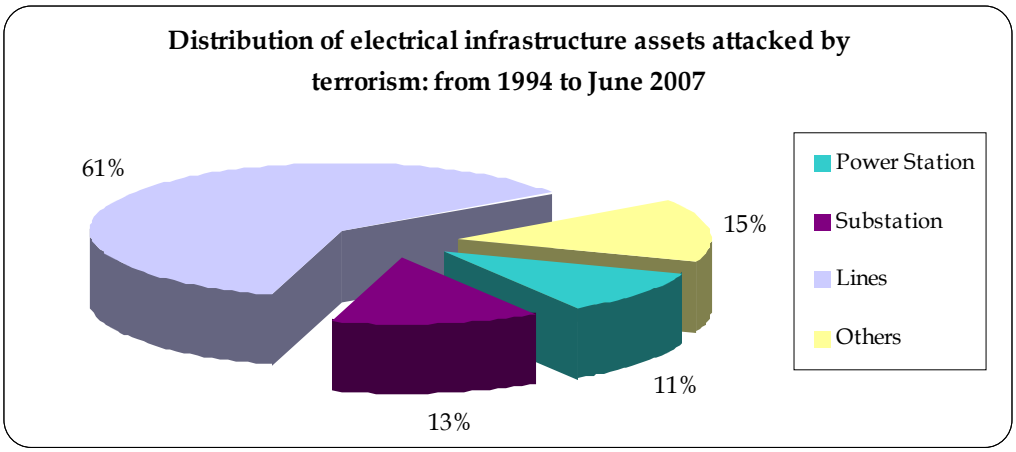


Figure 1-4. Distribution of electrical infrastructure assets attacked by terrorism: from 1994 to June 2007. Source: Figure created by analysis of data from the "National Memorial Institute for the Prevention of Terrorism (MIPT)" database.

TABLE 1-1. DISTRIBUTION OF TERRORIST ATTACKS ON THE ELECTRIC INFRASTRUCTURE BY COUNTRY: 1994 TO JUNE 2007

Country	Percentage
Colombia	42,40%
Iraq	17,33%
Pakistan	12,80%
Spain	4,00%
India	3,47%
Russia	2,67%
Sri Lanka	1,87%
Afghanistan	1,60%
France	1,60%

Source: Table and figure created by analysis of data from the "National Memorial Institute for the Prevention of Terrorism (MIPT)" database.

In Appendix A a more detailed overview of the causes and impacts of terrorism in different regions and countries in the world will be presented.

References

[BEL, 2002] Belcher T., Yoran E., Riptech Internet Security Threat Report, Vol. II, July 2002, p.p 23.

[CBC, 2003] CBC News, "Blackout by the numbers", CBC News online, November 14 2003. Available in http://www.cbc.ca/news/background/poweroutage

[COL, 2006] Colarik A. M., "Cyber Terrorism: Political And Economic Implications", Idea Group Publishing, January 31, 2006.

[DEE, 2005] Deen T.,"U.N. Member States Struggle to Define Terrorism" United Nations Inter Press Service News Agency, North America, 27 July 2005. Available in http://www.ipsnews.net/

[GER, 2006] Gheorghe A.V., Masera M., Weijnen M., De Vries L., "Critical Infrastructures at Risk: Securing the European Electric Power System", Ed Springer, Netherlands, 2006.

[HOF, 1998] Hoffmann B., "Inside Terrorism", Columbia University Press, 1998.

[HOF, 2002] Hoffmann B., "Rethinking Terrorism and Counter-Terrorism since 9/11", Studies in Conflict and Terrorism, Vol. 25, Issue 5, September 2002, USA, pp. 303-316 (306).

[HOM, 2004] Homer-Dixon T., "The Rise of Complex Terrorism", in: Gus Martin (editor), The New Era of Terrorism, Selected Reading, Sage Publications 2004, pp. 134-143.

[MUR, 2005] Murphy C., Sebti B., "Power Grid in Iraq Far From Fixed, New Government Inherits Huge Task. Washington Post Foreign Service, USA, May 1, 2005.

[REG, 2007] Regan T., "Al Qaeda calls for attacks on oil facilities", The Christian Science Monitor, posted February 15, 2007.

[SHP, 2003] Shapiro, J., Suzan, B., "The French Experience of Counter-Terrorism", Survival, Vol. 45, Issue 1, 2003, Routledge Ed., pp. 67-98 (81).

[STO, 2002] Stohl M., "The Mystery of the New Global Terrorism: Old Myths, New Realities?", New Global Terrorism, The:Characteristics, Causes, Controls, Prentice Hall, Upper Saddle River NJ, USA, October 2002.

[STO, 2005] Stohl M., "Expected utility and state terrorism", Root Causes of Terrorism, 2005, London, Routledge Ed., pp. 198-214.

[TFO, 2004] USA - Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations", April 2004. Available in https://reports.energy.gov/

[ZIM, 2005] Zimmerman R., Restrepo C., Dooskin N., Hartwell R., Miller J., Remington W., "Electricity Case: Risk, Consequences, and Economic Accounting", May 31, 2005. New York University-Wagner Graduate Sc.

CHAPTER II

2 POWER SYSTEM SECURITY ASSESSMENT

This chapter summarizes the most important aspects of the power system security and the relation with other important concepts such as reliability and adequacy. Also, a short description of operating states, the common technical problems and different security assessment approaches are given. Since in traditional security literature only natural events have been covered, new considerations in security analyses are proposed when dealing with intentional attacks and in particular terrorist events.

2.1 A Global Overview of Power System Security

Power systems are nonlinear dynamic, complex and large systems, which are developed in diverse time scales and geographical areas. A power system can be divided into two important structures: the power grid and the communication/information system [SHA, 2003].

The power grid consists of power plants that use different primary sources, control systems, control centres and substations, transformers, lines and protections, which constitute distribution and transmission networks [AMI, 2001]. All of this equipment must be operated correctly. The balance between electrical energy generation and consumption must be assured at all times due to the fact that it is impossible to store electricity on a large scale. The electrical network must be controlled continuously to deliver the required power levels in the place of demand, while maintaining frequency and voltages within secure and reliable areas of operation. The power system components have different temporal and also spatial requirements since they are distributed over immense geographic zones. This is why the control of system components is organised in different hierarchical levels.

Electrical utilities carry out their operation, planning and maintenance tasks by using communication and computers networks. These networks have been extended because of the interconnection between utilities. The interconnections require sharing and coordinating basic tasks, such as maintenance programming, control, protections and coordination of emergencies; among producers, operators and clients (who act on the power network in physically isolated places) [SHA, 2003]. Due to the electrical market deregulation, convergence of the participants' information is necessary to reach a global optimization of the system.

The use of standardized mass media such as the internet has become an important characteristic of electricity management. The flow of information at different levels of the power system is possible thanks to the communications system. This last one is generally composed of three networks: a) fixed networks including public switched telephone and data networks; b) wireless networks with cellular phones and wireless ATM (Asynchronous Transfer Mode); c) computing networks including different dedicated LANs, WANs and the internet [SHA, 2003].

In addition to this complexity, systems are aging and the electrical energy demand continues to grow. However, investments to expand the power system are increasingly difficult to realise. Environmental restrictions, high investment costs and low return on investment, the market deregulation and the electrical utilities' need for technical and economic optimisation are some common causes. Consequently, the transmission system loadability is lower than in the past and the systems are operated close to their limits, diminishing conservative security margins and the system's robustness in general. A key factor of this difficulty is the disparity between growth of demand and investment.

The power system is exposed to a series of events that can adversely affect (from a lower to a higher degree) the security of the system's operation and as a consequence stress the system (i.e. reduce the loadability margin of the system). Traditionally, these disturbances have been considered in the system planning, so that the system can withstand them and continue providing electrical energy within its operational limits. In addition to this concept, security appears as the ability of a power system to withstand sudden disturbances.

Operators are responsible for the continual power provision while at the same time complying to comply with the system's capabilities and considering economical aspects. They must find the optimal point between reliable technical operation and economic efficiency [KIR, 2002]. The operator verifies the system's security and the distance from security limits. If the system is highly loaded or under disturbance, the operator can take preventive measures to ensure that the system does not carry more power than it can actually support. In an insecure situation of the system, the operator will take corrective actions so that the system returns to normal condition and recuperates it, as soon as possible. Therefore, the operator needs to know the real degree of the system security, the nearby horizon in relation to security, load and possible contingencies and, if insecurity occurs, solutions for reestablishment of an acceptable security degree.

Operator actions are possible thanks to the supervision and control devices, protections and mathematical tools that allow the analysis of the power system security under given conditions and probable future conditions with eventual disturbances. Thus, security supervision and "security analysis" are two important functions.

Security analysis are executed so that the decisions taken during planning and operation of the power system are appropriate, and a suitable balance is reached between operative cost (and investment) and the robustness with respect to possible disturbances [KUN, 2003]. Firstly, the planning of power systems takes into account security as a fundamental aspect. Secondly, during the operation, powers systems are monitored and controlled assuring a permanent security margin. Traditionally, these analyses have been made by using the definition of power system operating states and the possibility of changing the operating state given the occurrence of a contingency. The contingency list (each contingency generally defined as the loss of a single power grid component) is previously established by using historical data or based on experience. This analysis is well known as the "N-1 criterion".

Nowadays security assessment of a power system is mostly carried out with deterministic methods. With this approach, simulated scenarios may lead to a pessimistic appreciation of the security level. It is widely recognized that the analysis and the management of

uncertainties, including probabilistic and possibilistic[1] models, may offer strategic guidelines on how to use more advantageous security improvement resources. Efforts to assess security by using the probability theory have been made during the last years.

The security assessment of a power system is a complex process due to the power system dimension and other aspects such as the system model, the uncertainty handling, the specific security problem which has to be considered, the computational efficiency and the interpretability of the results. This area has been developed during the last two decades thanks to the computational advances both in software and in hardware.

2.1.1 The repercussion of intentional attacks and terrorism on the power system security assessment

Besides the progressive complexity of power systems and the changes due to electricity market regulation, the threat to the national electrical infrastructure's security is present today more than ever. As mentioned in the first chapter, terrorism is a constant threat to societies throughout the world and the electrical network is potentially a key target for terrorist attacks.

At the moment, many countries are subject to the possibility of attacks that jeopardize the security of their electric system. The dispersed nature of system equipment and facilities makes it difficult to physically protect electrical power systems against intentional attacks. Therefore, physical vulnerabilities of a power system (power grid and system of communications) and cybersecurity of the communications system that supports the power grid operation must be considered in security analyses [AMI, 2003]. The current methods of the power system security assessment only consider "natural"[2] events; however it is not enough to overcome the imposed challenges effectively. Rigorous power security assessments and different considerations are necessary to continue fulfilling quality and continuity standards.

In contrast to other disturbances, intentional attacks and terrorism are not random events. Targets are perfectly chosen and normally a reason for selection exists. In terrorist attacks that took place in the past, it was established that terrorists planned and coordinated the attacks for a long time before executing them. Taking into account these attacks in the contingency list for security studies is not feasible by using traditional statistics tools, because of the inexistence of randomness. This subject will be looked at in more detail in the following chapter.

Another major difference with respect to the contingencies by "natural" causes is that intentional attacks depend on human will. An attack can be a single attack or a coordination of simultaneous attacks on tactically important points that can quickly lead the power system from a normal operating state to a critical one. Moreover, it is very important to recognize that the attacker can have a high degree of knowledge about the power system behaviour; even worse, if the attacker is an employee or an ex-employee, he could have access to privileged information, to physical places of protected devices, and to the power system control.

---

[1] The term "possibilistic" is used when the uncertainty is dealt with by the possibilities theory. Membership values of the possibility distributions represent degrees of possibility of the variables.

2 Natural events are those that occur without human intervention.

All of these factors increase the probability of occurrence of contingencies to a degree which was not foreseen when power grids and communications systems were put into place. Operators have never been faced with these types of events due to their "improbable" characteristics. Nevertheless, in the future, operators will have to take timely decisions with more uncertainty than in previously predicted situations.

Being able to deal with these intended situations will depend to a great extent on the anticipation capacity, the reflection in no-crisis times (off-line) and the operational management of the owners of critical infrastructures. Therefore, in the power system security assessment process, analyses taking into account the possibility of natural events and also intentional and terrorist attacks are indispensable. These last acts should no longer be categorised as "impossible" events but as one of the main threats to the security and adequacy of a system. In this way, proper decisions in power system planning and operation can be taken as counterterrorism measures, reducing or eliminating negative consequences of intentional attacks on the system. The deficiencies exposed above show the necessity to use new mathematical tools and technologies when dealing with power system security.

2.2 Concepts of Security, Adequacy and Reliability

The power system reliability denotes the ability to supply an adequate electricity service to end users on a continual basis, with few interruptions over an extended period of time [KUN, 2003]. Thus, a system must be secure and adequate in order to be reliable. The security is defined as follows:

System security of a power system refers to the degree of risk in the ability of a system to withstand sudden disturbances (contingencies) and losses or failures of system components without interruption of customer service. It is related to system robustness to imminent disturbances, and hence, depends on the operating system condition as well as the probability of occurrence of contingencies [IEE, 1978] [WGC, 1987] [IEC, 1999].

Due to interaction of the security and adequacy concepts, it is important to define the area of action of adequacy. Two definitions of adequacy are widely accepted in literature:

- *System adequacy* is the ability of the power system to supply aggregated electrical power and customers' energy requirements within the nominal component ratings and voltage limits, taking into account planned and unplanned component outages [IEE, 1978] [WGC, 1987] [IEC, 1999].
- *System adequacy* relates to the ability of the installed generation and transmission facilities to serve the total system-load requirements [BIL, 1984].

This division into security and adequacy guarantees that reliability can be calculated in a simply structured and logical approach. Adequacy and security are not numerical quantities and they are traditionally measured through indices.

The concept of system adequacy is completely static and is more related to the planning studies. Habitually, it is associated with the existence of sufficient resources both generation and transmission, to provide electrical power where it is required and taking into account also the losses. In addition, operational restrictions must be adhered to, i.e. equipment cannot be overloaded and the loads must be served within the limits of acceptable voltage. In adequacy studies, extreme conditions of the load, programmed outages of the components

and contingencies are taken into consideration. Adequacy is generally measured by indices that are computed for a period (commonly one year) employing parameters of frequency, duration and magnitude of power outages. The main indices are: Expected Energy Not Served (EENS) and Loss of Load Expectation (LOLE).

The system security is related to the ability of the system to continue operating satisfactorily when one or more contingencies occur. This concept refers to the operating conditions before the disturbance and the new operating conditions after the contingency. Security also concerns the ability to prevent cascades and to avoid the non-controlled loss of load when the system is disturbed.

Nevertheless, it is difficult to draw a straight line between security and adequacy analyses. Some authors in these areas proclaim the absence of a boundary between the two terms and prefer to employ the word reliability [LEV, 2001] to cover both aspects security and adequacy. Other works employ security for both aspects [CHE, 2000].

Different authors [WGC, 1987, 1993, 1997] [LAW, 1993] [END, 2000] distinguish adequacy from security analyses arguing that adequacy studies are those reliability studies that only take into account steady state conditions. Dynamic studies of reliability that include stability analysis refer to the security concept. Some authors following this classification strictly consider the terms "static security studies" and "adequacy studies" as equal [LAW, 2000] [DIM, 2005].

For [BRO, 2001], adequacy is assessed considering the possible states of generators (probability of being available, being available with a reduced capacity and being unavailable) and the load behaviour. For each combination of generation and load, a power flow is performed. If the available generation cannot supply the loads or if any constraints are violated, the system becomes inadequate and certain loads must be shed. In this approach, we assume that transmission components are available. Consequently, to address such events, a system security assessment is made.

In the power industry, operators have a tendency to use the term security to evaluate the limits of acceptable operating conditions when the system is perturbed in the present and a probable future load situation. The term security is used indifferently including both static and dynamic failure conditions. We adopt this terminology throughout this thesis and security is divided into two separate areas. The first one is the *steady-state security assessment*, which examines after to the occurrence of a disturbance, the capability of a power system to supply the load without violating the system's and equipment's operating limits. The second area is the *dynamic security assessment*, which tests the capability of a system to be operated in such a way that it remains stable when disturbances occur. Using this approximation, adequacy is only employed in relation to the ability of the installed generation and transmission facilities to serve the total system-load requirements. Adequacy is solely focused on power system planning and, planned outages are taking into account contrary to other security studies.

2.3 Hazards, Threats to the Power System Security

Diverse hazards[3] and threats[4] can affect the security of a power system. The appropriate knowledge as to the causes of the threats and hazards is useful in order to find the probability or possibility of these events occurring and also to have an idea of the consequence for the system. Threats or the hazards occurring do not necessarily mean the loss of one or several components of the power system. The contingency term is amply utilized in power system industry to relate to sudden disturbances leading to the loss of any component of the system, such as a transmission line, a transformer or a generator.

The word "event" is used in this document to include both hazards and threats. An event is a fact or phenomenon of uncertain occurrence that adversely affects the system performance. The occurrence of an event can lead the power system to have a single or multiple contingency. We suggest a classification of the possible events in Table 2-1 [TRA, 2004].

2.3.1 Events classification by the nature of the cause

Events in a power system can be classified according to whether there are people involved in the cause of the event or not. Thus, *Natural events* are events which occur without human intervention. They arise from phenomena to which system components are subjected because of operation, exhibition, aging and production failures, among others. Natural phenomena such as atmospheric discharges (lightning), animals in transmission lines, winds, and others are also considered.

By contrast, an *intentional event* is a non natural event where the liable person or group has the objective of damaging the power system. The following three types of events can be taken into account:

- Attacks upon the power system. In this case, the electricity infrastructure itself is the primary target. The attack point could be a single component, a critical substation or a transmission tower. Or it could be simultaneous [AMI, 2002].
- Attacks by the power system. Here, the target is the population, using parts of the electricity infrastructure as a weapon [AMI, 2002].
- Attack through the power system. The target in this case is civil infrastructure [AMI, 2002].

A *non intentional event* is a non natural event where the person responsible damages the power system by means of a human error, i.e., it is not the objective of the person liable to cause damage. Examples of this are: operators or maintenance staff taking wrong decisions or accidentals mistakes in the task's execution. It can also be produced as a consequence of other actions performed near the power system in which human beings are involved. For example tree-pruning that does not necessarily correspond to maintenance work.

[3] Hazard: is a source of danger to a system, a possibility of incurring loss.
[4] Threats: a specific hazard.

TABLE 2-1. DESCRIPTION AND CLASIFICATION OF POSSIBLES EVENTS THAT CAN AFFECT THE OPERATION OF A POWER SYSTEM

CAUSES CLASSIFICATION			DESCRIPTION OF CAUSES	CLASSIFICATION CONSEQUENCE	SOME CASES
NATURAL Events which occur without human intervention. They include the phenomena to which the components of a system are subjected for operation, for ageing, failures in the manufacturing, exposure and location of the system, among others. They also include natural phenomena.	**INTERNAL** Events associated with abnormal conditions which are purely related to system operation. In general they involve the failure of elements of the power grid and of the communication system.		Originated from failure of the constituent equipments of the power system. For example failure of transformers, lines, protections, etc.	**ADMISSIBLE**	• Technical failure of system equipments • Errors in the equipment production
				NON ADMISSIBLE	• Technical failures of critical system equipment • Technical failure of primary equipment and protection • Failure of the SPS • Errors in production of critical equipment and protections
	EXTERNAL Events associated whit abnormal conditions which are NOT due to system operation. These are events to which the power system is exposed either due to its geographical location or its environment.		These are events to which the power system is exposed due to its geographical location and exposure to the environment. They occur because of natural phenomena such as atmospheric discharges, winds etc.	**ADMISSIBLE**	• Atmospheric discharges • Animals on the transmission lines • Winds and telluric movements under design specifications • Pollution
				NON ADMISSIBLE	• Atmospheric discharges overcoming the design specifications • Winds and atypical telluric movements overcoming the design specifications • Avalanches and floods; high pollution
NON NATURAL Events which occur due to human intervention. These events can either be intentional or unintentional.	**INTERNAL** Events associated with abnormal conditions which are purely related to system operation. In general they involve the failure or the incorrect operation of elements of the power system due to operators' actions on the system.	**INTENTIONAL** Events where the person responsible has as objective to damage the power system.	These occur due to intentional human acts in the system operation and maintenance, which have the purpose of harming the integrity and operation of the system. They can cause hidden failures.	**ADMISSIBLE**	• Internal sabotage (strikes, syndicates)
				NON ADMISSIBLE	• Internal sabotage or terrorism: coordinated cyberattacks to network computers from a worker with high level access to system communications.
		NON INTENTIONAL Events where the person responsible has NOT as objective to damage the power system.	These occur due to errors and human accidents (unintentional) during the planning, operation and maintenance of the system	**ADMISSIBLE**	• Errors in the system design • Wrong decisions in operation, errors in execution • Accidents in maintenance
				NON ADMISSIBLE	• Decision mistakes made by the operators, errors in execution in an alert or emergency state of system operation • Catastrophic accidents in maintenance
	EXTERNAL Events associated whit abnormal conditions which are NOT due to system operation. These are events to which the power system is exposed either due to its geographical location or its environment, the economic impact in society and the interdependence of the electric power system with other systems.	**INTENTIONAL** Events where the person responsible has as objective to damage the power system.	These are events to which the power system is exposed for its impact in economy and due to its interdependence with other systems. The objective is to cause damage to the power system.	**ADMISSIBLE**	• Terrorist attacks affecting individual and non critical components. War Acts • Attacks to other systems having dependence on the power system. • Cyberattacks on control equipment
				NON ADMISSIBLE	• Coordinated terrorist attacks on diverse critical points of the power systems. War acts • Coordinated cyberattacks on SCADAs
		NON INTENTIONAL Events where the person responsible has NOT as objective to damage the power system.	These are unnatural events to which the power system is exposed due to its geographical location and exposure to the environment. Can occur as a consequence of other actions occurring near the power system.	**ADMISSIBLE**	• Human Errors: tree-pruning, lines, neighbouring constructions.
				NON ADMISSIBLE	• Human Errors: tree-pruning, light planes and helicopters falling on critical transmission lines, neighbouring constructions

Events affecting power system security can also be classified by internal and external causes. An *internal event* is one that has an associated abnormal condition such as an over-current, over or under voltage or frequency due purely to normal system operation. In general they involve failures of the power system elements, protections and inclusive system failures produced by actions from operators.

An *external event* is one that comes from an abnormal condition not due to normal system operation. These are events to which the power system is exposed either by its geographical location, environmental exhibition, economic impact on society and interdependence of the electric power system with other systems.

In the security assessment not only the nature of contingency is analyzed, but also the effect on the power system and its ability to respond properly to the disturbance. In this way, a simple classification of the disturbance consequence is suggested.

2.3.2 Classification of events by the consequence

Events are admissible if they have consequences that have been modelled and accounted for during system design. Although the cause of an event may not always be probable, the consequence of such an event may be very probable. Therefore the consequences of an admissible event should neither finish in cascade, nor in an extreme emergency state. For example, transmission lines are normally designed against lightning with a parameter of a certain number of outages per year for every 100 km. Damages are not expected in the facilities thanks to the correct operation of protection and control systems and to the appropriate selection of equipment. Another example could be a terrorist attack leading to a line outage. In this case, the consequence has been accounted for in the design and it is considered as an admissible event.

In general an admissible event does not entail stability problems. The system can operate near its security limits and may have a loss of load.

Most of the non admissible events are unpredictable events which lead the system to operate outside of its operating limits entailing instability. Usually, it is a combination of forced outages of several elements or only a few elements but critical for the system operation. In many cases the security limits of these events depend on the SPS (special protection system).

In the following sections we will show that an admissible event can lead the system to move between the normal and alerts operating states. A non admissible event always generates transitions from any operating state to extreme emergency. When the system collapse is reached it consequently leads to the restorative state. The previous transitions to extreme emergency states are not controlled.

Since the events' consequence and the effects of the power system security assessment are closely related to the system operating states, it is necessary to review these concepts.

2.4 Operating States of Power Systems

A power system is a structure that works continuously but it is not identical all the time. A generator can be working for one hour and generate a certain quantity of electricity, but in the following hour it can generate a different quantity, or simply cease to work. Also,

transmission lines may be available or not, for reasons of technical and/or economic viability, maintenance or for contingencies. The demand of electrical energy varies constantly and depends on many random factors such as temperature and others that have a higher degree of uncertainty e.g., human behaviour. The condition of operation of the system changes also continuously. The operation can be described by a series of states. An operating state indicates the degree to which constraints of security and adequacy are satisfied.

The first and most frequently used classification scheme of states in reliability/security analysis was the one proposed by Fink and Karlsen [FIN, 1978] showed in Figure 2-1. Later EPRI [EPR, 1987] modified this scheme by dividing the emergency state into temporary emergency and controlled emergency. The resulting scheme is shown in Figure 2-2.

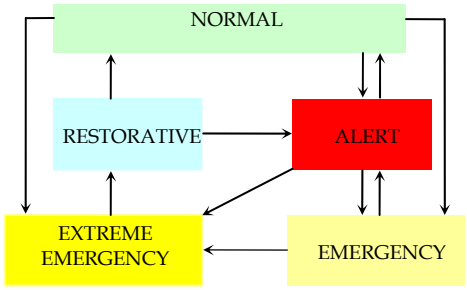


Figure 2-1. System operating states by Fink and Karlsen in 1978. Source: [FIN, 1978].

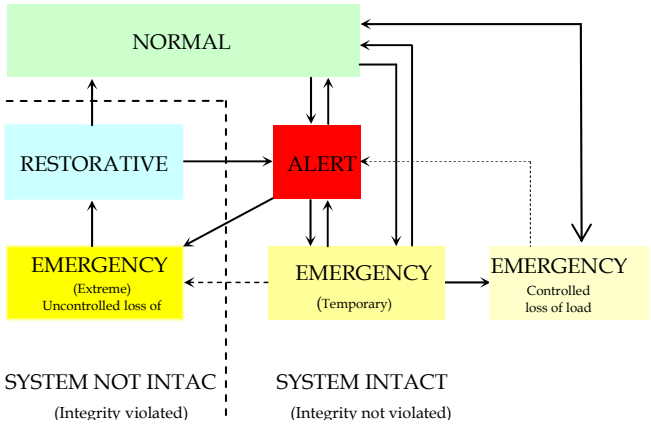


Figure 2-2. System operating states by EPRI in 1981. Source: [EPR, 1987].

Before continuing with the definition of each operating state, the classification scheme of states proposed by CIGRE [WGC, 1997] is shown in Figure 2-3, where alert states, the concepts of adequate states (different from adequacy concept) and stability are included. In the present chapter this scheme is analyzed and forms the basis of a more detailed scheme that has been proposed.

The CIGRE's diagram is valuable in the sense that it shows that there is a new definition of states in terms of adequacy and stability. The only transitions among states that are considered are those due to the consequences of natural events. Transitions caused by non-natural events are not considered, neither are transitions which are caused by control actions. Consequently, the controlled emergency condition which is almost always reached from the inadequate domain using the operator's intervention is ignored.

<table>
<tr><td></td><td colspan="2">ADEQUATE</td><td>INADEQUATE</td></tr>
<tr><td rowspan="3">STABLE</td><td rowspan="2">NORMAL</td><td>ALERT: potentially inadequate</td><td>EMERGENCY (temporary)</td></tr>
<tr><td>ALERT: potentially inadequate and unstable</td><td rowspan="2">Inadequate: Potentially unstable</td></tr>
<tr><td>ALERT: Potentially unstable</td><td></td></tr>
<tr><td>EXTREME EMERGENCY</td><td colspan="3">CASCADING</td></tr>
<tr><td></td><td colspan="2">UNSTABLE (system collapse)</td><td>STABLE (Inadequate)</td></tr>
</table>

Figure 2-3. Classification of operation states of the system. Source [WGC, 1997].

A new classification of the operating states of the power system, as well as new transitions between operating states is being proposed in Figure 2-4 [TRA, 2004]. In this graph, horizontal and vertical transitions are allowed.

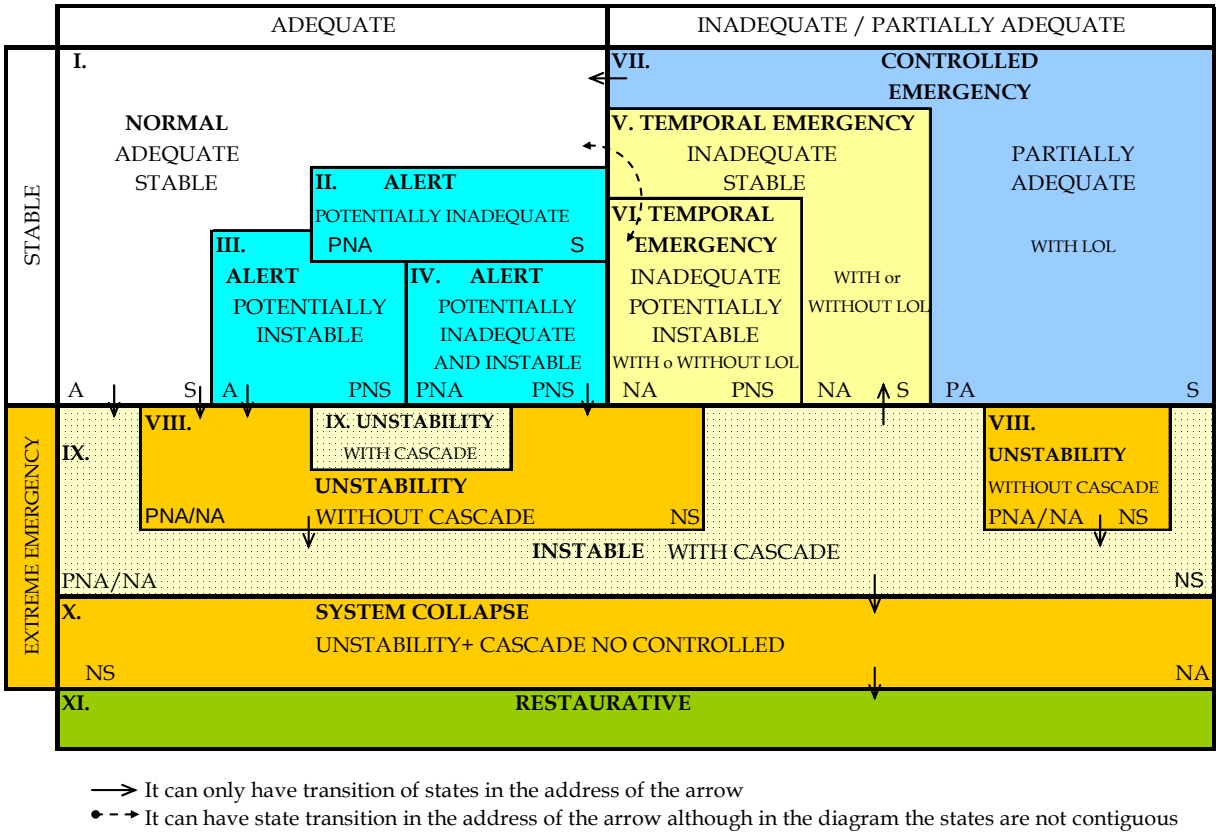


Figure 2-4. Classification of operation states of the system using as a reference [FIN, 1978] and [WGC, 1997]. A: Adequate, S: Stable, NA: Inadequate, NS: Instable, P: Potentially, LOL: Loss of load.

Keeping in mind that the best state is normal and the worst state is system collapse, any transition to a "better" state is due to an appropriate control action which is executed correctly or due to a damping effect inherent to the disturbance.

Any transition to a worse state is due to a disturbance that had a negative effect which then evolved, inadequate control actions, incorrectly executed control actions and, in general, uncontrolled disturbances. The arrows in the scheme indicate that transitions between those states are not allowed in the opposite direction. For example, the direct transition from the unstable state without cascade to the alert and normal states is not possible. This is because a later control action leads the system to a controlled emergency state since there was inevitably a load loss. Another example is that once the system collapse is reached, only one later state is possible: the restorative.
An adequate state is reached when all loads are supplied, system components are not loaded beyond their nominal ratings and the system frequency and voltages stay within their limits.

The adequacy system and an adequate state are two different concepts. The operating states of the system are defined by means of the definitions made by [WGC, 1997].

Normal state
State I: The system is in a normal state if it can withstand any natural or non-natural event, sufficiently possible to occur in that state. The occurrence of possible events in a normal state does not lead the system to inadequacy or instability. The normal state is adequate and secure. Because all the event types are being taken into account, there are new transitions in this diagram. In general, an event that leads the system directly from a normal condition to an extreme emergency state will be an event corresponding to the situation where the consequence magnitude is not admissible. An emergency state is caused by a catastrophic event that provokes a cascade or instability. However, most of these transitions are made possible by external natural events of large magnitude and by non natural events with massive destructive goals. Furthermore, there can also be simultaneous and coordinated events [WGC, 1997].

If there are transitions among states that lead the system to an extreme emergency state, it could be due to the natural evolution of an uncontrolled failure, caused by the mismanagement of controls or incorrect actions taken by the operator. It should be noted that there is no transition from the normal state to the controlled emergency state, because this last one is reached from the inadequate states. Making use of this definition, security *concerns the ability of the system to stay in the NORMAL state* even if a disturbance affects the system.

Alert states
The system is in an alert state if there are one or more very probable natural or non-natural events that can lead the system to inadequacy and/or to instability. The alert state is defined by means of events that can occur while being in that state and that can cause instability and/or inadequacy. In the alert state the security margins have been decreased and it is necessary to take manual or automatic preventive control action so that the system returns to the normal state [WGC, 1997].

Three types of alert states are recognized:
- State II. An *alert state* is *potentially inadequate*, if in this state events can occur that lead the system to inadequacy but not to instability [WGC, 1997].
- State III. An *alert state* is *potentially unstable*, if events can occur that lead the system to instability. In this state, the occurrence of the event can lead directly to instability, or may involve a sequence of events that lead to instability [WGC, 1997].

- State IV. An *alert state* is *potentially inadequate and potentially unstable*, if events can occur that lead to inadequacy and unstable conditions. Consequently, this state is a combination of the last two [WGC, 1997].

Temporary emergency states

Temporary emergency states are stable but inadequate. In these states the integrity of the power system is assured thanks to manual or automatic emergency control measures. These actions lead the system at least to an alert state or to a controlled emergency state. If effective measures were taken quickly the system would return to the normal state.

- State V. Temporary Emergency: inadequate and stable. This state is an inadequate state and there are no possible events that can lead to the instability state.
- State VI. Temporary Emergency: inadequate and potentially unstable. This is an inadequate state and there are possible events that can lead to the instability state.
- State VII. Controlled emergency is a partially adequate state, because the previous state was inadequate. There was load loss in this inadequate state and the transition to the controlled emergency is thanks to manual control actions. There are also transitions from this state to the extreme emergency states, which can occur due to non-natural events, such as incorrect operator actions.

Extreme emergency states

An unstable state is considered a state of extreme emergency. It is extreme because the instability can lead to system collapses. It depends if remedial action is carried out in a sufficiently short time to avoid the beginning of a cascade, or whether the cascade is controlled (or not) once it is initiated [FIN, 1978].

In extreme emergency state, it is not possible to maintain stability. Therefore, a major disturbance of the power system has occurred which causes the readjustment of the voltage angles of synchronous machines and creates an unbalance between the system generation and the load. Synchronous machines can not maintain synchronism at the end of the transient period. In extreme emergency there must be a loss of generation, load shedding or system isolation in order to be able to balance load and generation.

- State VII. Extreme emergency: unstable without cascade. It is a state where instability has been reached but a cascade has not begun in the system; this condition will improve only if very quick control actions are taken.
- State IX. Extreme emergency: unstable with cascade. Once the instability is reached and a cascade has begun the stability can be recovered, either thanks to an inherent damping in the process, or a quick protective action of the system. However, the later state is generally inadequate. If it is not controlled it leads to system collapse.
- State X. Extreme emergency: system collapse. It is necessary that the system is unstable and that the cascade has not been controlled for the system to reach the collapse.

Restorative state

State XI**:** Once the collapse has been stopped, the system enters into the restorative state when there is remaining operative equipment with nominal capacity or if some equipment has been restarted. The control actions taken should minimize the quantity of energy not delivered by the resynchronization of generation, recapture the whole lost load and reconnect the system. From this state the system can transfer to the normal state or to any alert state depending on the circumstances [FIN, 1978].

2.5 Security Problems

Different security problems vary according to time scales, characteristic symptoms such as low/high voltage, and the application domains. Under normal conditions the fault of a component will not have serious consequences for the system. Nevertheless, if the affected component is critical for the operation, and appropriate corrective actions are not taken, this can trigger a sequence of events causing the partial or total collapse of the system. Although the cascade is not an event that occurs continuously, consequences are usually catastrophic.

Figure 2-5 shows a classification of typical security criteria taking into account both static and dynamic aspects [MCC, 2000].

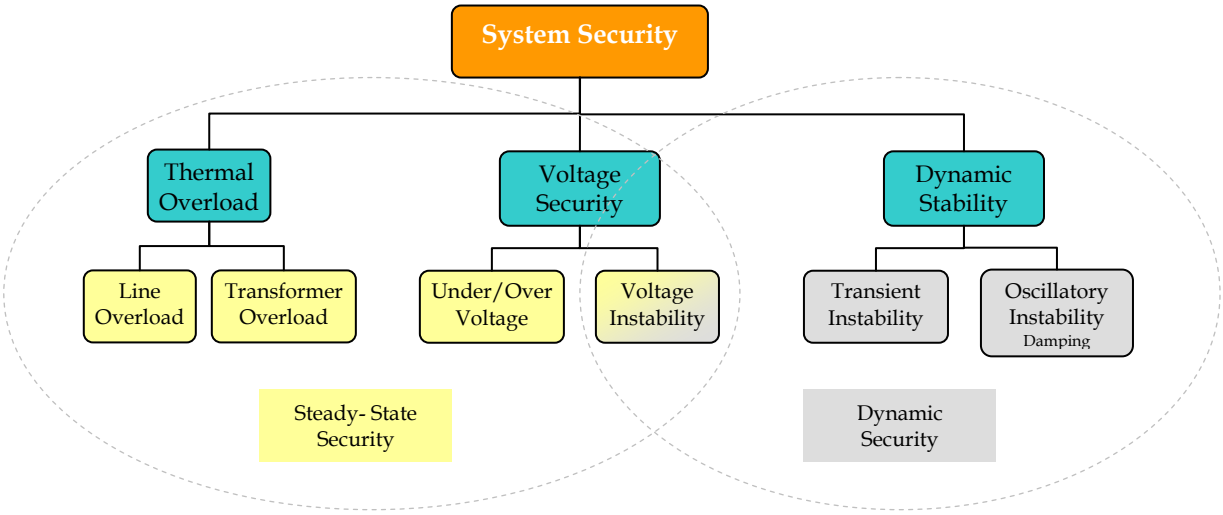


Figure 2-5. System power security criteria.

The most common problem of static security essentially involves the thermal overload of generation and transmission system components, where the phenomena normally occur over long periods of time. The studies of line overload are of great interest because of its potential to cause a cascade. When a line is overloaded, protections put the line out of service. If the system is highly loaded and there is no load shedding, given the contingency, the power must be distributed to other lines (which will transmit more power than planned). Therefore, the probability that these lines will be overloaded is higher. If this occurs, protections act again and the lack of remediable automatic actions of the system or of operator's actions can trigger the successive outage of components.

Voltage security is defined as the ability of a power system to maintain acceptable voltages in all the system buses when the system is under normal operation or in post-contingency conditions. The voltage security study is made in order to analyze two main problems: over/under and instable voltage. If bus voltages fall below a minimum limit, there will be a risk of voltage collapse in addition to high losses. On the other hand, if bus voltages are too high in relation to the maximum limit, there will be equipment degradation or damage. Line overload may be followed by unpredictable line tripping that accelerates the degradation of the voltage profile [HAD, 2001]. In static analyses, voltages are checked and compared with the operational limits. In the case of voltages being outside the limits, the planner/operator takes decisions and actions in order to avoid severe consequences (i.e. the voltage collapse).

A system enters into the voltage instability state when an increase of load or a change of system conditions cause a progressive and uncontrollable voltage fall. The main source of voltage instability is a lack of balance between the reactive power generation (provided by generators and devices of reactive compensation) and the reactive demand causing the fall of voltages in the system buses [KUN, 1994]. The relevant time frame for voltage stability problems may vary from a few seconds to ten minutes. Consequently, voltage stability is analyzed in two frames: static and dynamic stability.

The steady state insecurity includes the following problems:

1. Bus voltage is outside of tolerance limits
2. Overload of transmission lines
3. Overload of transformers and other equipment
4. Static voltage instability

Dynamic insecurity comprises all of the instability forms. The transient stability refers to the ability of the generators of a power system to recover the synchronous operation that follows the electromechanical oscillations caused by a great disturbance (sudden load changes, the loss of generating units and loss of important transmission lines). Oscillatory stability depends on the initial operating state of the system and is usually associated with insufficient damping of oscillations. These dynamical aspects are mentioned to give a general vision of the security analyses but they will not be covered in this thesis.

2.6 What Is the Security Assessment For?

The decisions made in respect to the network are taken in different time frames. Security studies are elaborated for different application domains: system planning, operation planning, and on-line operation.

Power System Planning
Security studies in planning allow planners to determine the security level of the system for different scenarios (network topology, injected powers and contingencies). The planner will discard configurations which do not respect the security and reliability levels, and will take actions to reinforce the transmission system based on security criteria. For example, a voltage security study for the planning makes it possible to specify the amount and response of necessary reactive sources on each bus of the transmission system. If the planning is correct, the system will only reach an insecurity voltage condition after a catastrophic event of large proportion. In general, a security study for the planning identifies the structural weaknesses of the system and provides guidelines to improve the system security [WEH, 1997].

A major difficulty of the security analyses in the long and medium-term is that many assumptions have to be taken, or are based on forecasts of the other variables, and the amount of uncertainties present in the analyses can be enormous.

In *operation planning*, the security analyses will enable us to establish an efficient maintenance schedule, a definition of operation strategies for usual and abnormal situations and the protections coordination. It is guaranteed that the system is in normal conditions when:

- Frequency is within the established limits (generally between 59,8Hz and 60,2Hz or 49,95Hz and 50,05Hz), searching a balance between demand and generation variables, and

- Substations voltages limits are within the operative ranks (generally +/- 5% of nominal voltage), and
- There is security or reserve generation

Operation of Power Systems
Since the system operation can be different in normal or contingency conditions in comparison to the conditions for which it was planned, operating security studies make it possible to monitor the operation and to assure a security margin [MOR, 2004]. In system operations, with the help of Energy Management Systems (EMS), contingency analysis can be performed to determine how far the system is from its operational limits. In addition, it is also possible to establish the operating risk of the system. EMSs allow us to identify possible actions which can help to reduce the system risk and to justify decisions which will make the system more efficient in technical and economical terms.

Off-line analyses are applicable to and constitute an important part in all domains of security analysis, including online studies. Off-line analyses are based on probable future conditions and the operating rules and limits are also identified. In the operation, based on the current condition, the security level is evaluated and compared with off-line studies in order to find the correct decisions.

2.7 The Complexity of the Security Assessment

Three main steps can be roughly distinguished in the security assessment as follows:

- Selection of the power system model
- Selection and ranking of the contingencies
- Impact assessment of each contingency on the system behaviour

The model
The amount of components that make up a system, the possibility of whether each component will operate properly or not, the pre-contingency operation conditions, the contingency list and the criteria of security to be considered, all entail the evaluation of numerous cases. The exhaustive study of each possible combination is not practical since a very high computational cost would be required.

The system topology to be studied is traditionally chosen on the basis of the system's historical database or of the circuits in operation. However, other topologies can be selected since the security study can be made with the purpose of evaluating the robustness of a given topology.

Operation ranges and parameters of components and load magnitude are quantities that must be defined, taking into account their coherence and credibility. The selection of the system model depends mainly on the application area (planning and operation) and on the security problem to be analyzed (static or dynamic state).

Load flow has been the model used in steady state security studies. Voltage magnitude of any point of the network and active and reactive powers flowing on all of the lines will be the outcomes of the power flow studies. Thus, it will be achievable to determine possible

conditions of under/over-voltage and overload. Also other types of security problems can be analyzed by using these results, e.g. the risk of cascading outages.

Uncertainty management is generally valuable at the time of modelling the reality more satisfactorily. It is clear that the degree of uncertainty in load demand or generation would not be equal if the purpose was to plan a secure system over a five year time scope or just over the following day. In the planning domain, inclusion of injected power uncertainty into the system will be very constructive since power is better modelled as a range, a probability variable, or a fuzzy value than as a crisp value. Through this type of modelling, computational efforts can be reduced and a big number of the possible cases can be included more easily.

In the context of on-line assessment, ranges of power load and generation are narrow and more precise than in other domains and the status of operation of each component is fully known. Here, more information is available, uncertainty is reduced and diverse aspects such as calculation time become a high-priority compared to, e.g. the insertion of the load uncertainty. Complexity, computational cost and results accuracy are factors that need to be considered at the time of selecting the model, as well as considering the balance between these factors. Simplifications of areas of the power system have also been made in an effort to reduce the complexity of the model (number of components) and consequently of the simulations. Simpler equivalent models of interconnected areas replace detailed models, yet they conserve the vital information of the area. In this way, the complexity present in the security calculation is reduced.

Contingency selection and ranking
Once a model is chosen, another way to reduce calculation complexity is to select probable and/or critical contingencies between all of the possible contingency sets. A contingency group is listed and afterwards the influence of each contingency on the security of the system is analyzed.

Contingency ranking is the process of indexing the possible contingencies of a system on the basis of their negative impact on the system operation. The contingencies of a higher rank are further analyzed. The objective of using a contingency selection and ranking process is to establish those critical contingencies through a general, easy, and efficient method.

The first common practice was to select a contingency list based on operators' experience. The contingencies set consisted of a group of events that operators had identified and that could cause unacceptable behaviour. However, the disadvantage of this method is the lack of a clear physical meaning. Another practise consists of analysing the contingencies through a very simple method of severity assessment. For example, performing one iteration of the fast decoupled load flow [ALB, 1982]. Then, contingencies are ranked according to a performance index (PI), which is a scalar that reflects the degree of severity of a contingency [ALU, 2003].

Other approaches are based on the probability of event occurrence. In this case, contingencies are ranked using the probability value. Statistic tools are frequently used to estimate probabilities. Nevertheless, in principle very probable contingencies can have no influence on the behaviour of the system and therefore detailed analyses to evaluate the security are not required. Conversely, severe contingencies for the system which have a low probability of occurrence can be ignored in the security study. Improved versions, that

include both probability of contingency occurrence and the impact on the system, have been developed. The risk concept has been used for this aim [TRA, 2000a].

In the framework of an on-line security analysis, the speed of the selection of contingencies must be made in a minimum time and fast algorithms are used to select the most restraining contingencies. Depending on the analysis perspective, one method of selection of contingencies can be more appropriate than another one.

Impact assessment
Regardless of the contingency cause or of the selection technique of the contingencies list, the impact assessment corresponds to how and in what proportion the system is affected by the occurrence of a disturbance. Here, analyses must indicate to the operator, what happens to the system if the unplanned outage of a component occurs. Steady-state security as well as the system stability are aspects of interest to the operator. Transient stability, voltage security and overload are evaluated to determine the security degree of the system.

The result must be easy to interpret for the operator. Using deterministic approaches, the outcomes of the security assessment can be among others, the post-contingency operating state due to a disturbance, the time of fault clearance or the reactive power margin before the voltage collapse. Making use of probability theory, some examples of the outcomes are: the probability that the next disturbance moves the system from a secure operating state to a non acceptable state, the probability of voltage collapse, the probability of cascading outages or the risk of the system of not being secure.

2.7.1 Security assessment: probabilistic vs. deterministic procedures

The general practice in the industry for the security assessment has been the use of a deterministic approach. This practise has served reasonably well to the industry in the past since it gave rise to high security levels. The method has a very simple rule for making decisions: "to optimize the economy within the operational restrictions of the security region" [CHE, 2000]. In practice this means that the planning engineers propose robust systems and the operators operate with high safety margins, which also results in a high reliability degree by using redundant configurations and/or elements in most of the power systems [NI, 2003]. This way is usually economically expensive and undesirable for the companies, because of present pressures due to competition.

Information available for system operators and planners contains different levels of uncertainty: randomness, ambiguity and vagueness, just like future load patterns, possible contingencies and the probability of their occurrence, and states of neighbouring power systems, among others. It is expected that with the use of the probabilistic and inclusive possibilistic approaches, probability or possibility functions can be used to model the contingency occurrence and the intrinsic variables of the security problem.

For example, considerations, concerning how probable or improbable each one of the different contingencies is, help to choose the contingencies for the security assessment. By incorporating a suitable representation of uncertainty into the models, this allows the generation of appropriate scenarios which fit in more with the reality of the power system, from a technical point of view as well as from an economical point view [SCH, 1999].

As mentioned before, the uncertainty present in the security problem is of diverse types. Appropriate uncertainty modelling and handling, can offer advantageous strategic guides on how to use security improvement resources and on how to make systematic use of the information available in any decision making context. Probabilistic models, Bayesians decisions analysis and fuzzy arithmetic are some techniques used in this thesis to deal with uncertainty.

2.7.2 Security assessment based on risk

A different approach of probabilistic analysis has been the use of a risk index [WGC, 1997] [CHE, 2000] [DAI, 2001] [NI, 2003] [TRA, 2006b]. The most important aspect of this approach is to measure the system security by using the traditional definition of risk that captures two attributes: the consequence of an unwanted event, and the probability of this actually occurring. Different approaches can be found in documents, but in general the security assessment based on risk includes these two attributes as following:

1. Power system security can be affected by the occurrence of events classified in table 1. Probability of occurrence of events is calculated to model this uncertainty and depends on factors such as meteorological conditions, manufacturing problems, etc.
2. The probability of operating conditions is calculated in order to model, for example the uncertain conditions of the load and the economic dispatch.
3. Severity of the event is measured in terms of economic and/or technical repercussions on the system. Severity functions including technical aspects which indicate how far or close the system is to its operational limit, given the occurrence of the event.

Roughly, the risk has been calculated as the sum or integral of the product of the probability of occurrence of an uncertain event, the probability of an uncertain operating condition in the case of this event occurring, and its corresponding impact on the system.

The security assessment based on risk is the basis of the proposed method in this thesis for this purpose. Advantages of this approach are made clear in [MCC, 1999], [WGC, 1997] and [JAY, 2003]. One of the main advantages is that the security assessment can be performed using the expected cost due to possible insecurity problems. The operator or planner can easily relate to both technical aspects of operation and the business economy. This is important at the time of making preventive and corrective decisions in order to preserve or to improve the security of the system. On the other hand, risky components or operating conditions can be identified without difficulty since risk evaluation is done for each component and each contingency. Moreover, several steady-state problems can be taken into consideration when calculating severity, rather than just considering only one aspect, as this can give a more comprehensive idea of the security level of a region.

References

[ALB, 1982] Albuyeh E., Bose A., and Heath B., "Reactive power considerations in automatic contingency selection," IEEE Transactions on Power Apparatus and System, Vol.PAS-101, No. 1, 1982, pp. l07-ll2.

[ALU, 2003] Albuquerque M., Castro C., "A Contingency Ranking Method for Voltage Stability in Real Time Operation of Power Systems", Proceedings of IEEE Bologna PowerTech Conference, June 23-.26, Bologna, Italy, 2003.

[AMI, 2001] Amin M., "Toward Self-healing Energy Infrastructure Systems", IEEE Computer Application in Power, Vol. 14, No.1, January 2001, pp. 20-28.

[AMI, 2002] Amin M., "Security Challenges for the Electricity Infrastructure", IEEE Computer, Suplement 2002, pp. 8-10.

[AMI, 2003] Amin M., "North America's Electricity Infrastructure: Are we ready for more perfect storms?", IEEE Computer Society, October 2003, pp. 19-25.

[BIL, 1984] Billinton R., Allan R. N., "Power system Reliability in Perspective", IEE Journal Electron Power, Vol. 30, March 1984, pp.231-236.

[BRO, 2001] Brown R. E. "Power System Reliability", The Electric Power Engineering Handbook Chapter 13-5. Ed. L.L. Grigsby Boca Raton, CRC Press LLC, 2001, USA.

[CHE, 2000] Chen J., McCalley J., "Comparison between Deterministic and Probabilistic Study Methods in Security Assessment for Operations,"Proceedings of the VI International Conference on Probabilistic Methods Applied to Power Systems, September 2000, Madeira Island, Portugal.

[DAI, 2001] Dai, Y.; McCalley, J.D.; Abi-Samra, N.; Vittal, V., "Annual risk assessment for overload security", IEEE Transactions on Power Systems, Vol. 16, Issue 4, November 2001, pp. 616 - 623.

[DIM, 2005] Dimitrovski A. , Tomsovic K., "Uncertainty in Load Flow Modeling: Application of the Boundary Load Flow", Automation of Electric Power Systems: Special Issue on Developments in Load Flow and Optimal Power Flow Techniques, Vol. 29, No. 16, August 2005, pp. 6-15.

[END, 2001] Endrenyi, J.; Wellssow, W.H., "Power system reliability in terms of the system's operating states, Power Tech Proceedings, 2001 IEEE Porto, Vol. 2, 2001, pp. 6.

[EPR, 1987] EPRI, "Composite System Reliability Evaluation: Phase I – Scoping study". Report EL-5290, December 1987.

[FIN, 1978] Fink L., Carlsen K., "Operating under stress and strain", IEEE Spectrum, March 1978. pp. 48-53.

[HAD, 2001] Hadjsaid N., "Security Analysis", Electrical Engineering Handbook, Chapter 12, CRC Press LLC, Boca Raton, USA, 2001.

[IEC, 1999] IEC: International Electrotechnical Vocabulary (International Standard 60050-191), Chapter 191: "Dependability and quality of service", Geneva Switzerland, 1999.

[IEE, 1978] IEEE Working Group, "Reliability Indices for Use in Bulk Power System Supply Adequacy Evaluation", IEEE Transactions on Power Apparatus and Systems, Vol. 97, No. 4, July-August 1978, pp. 1097-1103.

[JAY, 2003] Jayaweera D., Kirschen D.,"Value of Security Assessment - Extensions and Applications", These of Department of Electrical Engineering and Electronics, UMIST, Manchester, Great Britain, 2003.

[KIR, 2002] Kirschen D., "Power system security", Power Engineering Journal, October 2002, pp. 241-248.

[KUN, 1994] Kundur P., Voltage Inestability in Power Systems Stability and Control, Chapter 14, McGraw-Hill Professional, January 1994.

[KUN, 2003] Kundur P., Parseba J., Vite S., "Overview on Definition and Classification of Power System Stability". On Behavior IEEE/ClGRE Joint Task Force on Stability Terms and Definition. Quality and Security of Electric Power Delivery Systems, 2003. CIGRE/IEEE PES International Symposium, October 2003, pp. 1 – 4.

[LEI, 1993] Leite da Silva A.M., Endrenyi J., Wang L., "Integrated Treatment of Adequacy and Security in Bulk Power System Reliability Evaluations", IEEE Transactions on Applied Superconductivity, Vol. 3, No.1, March 1993.

[LEI, 2000] Leite da Silva A., Rei A., Jardim J., de Oliveira J., "Static and Dynamic Aspects in Bulk Power System Reliability Evaluations", IEEE Transactions on Power Systems, Vol. 15, No. 1, February 2000, pp 189 – 195.

[LEV, 2001] Levi V.A., Nahman J., Nedic P., "Security Modeling for Power System Reliability Evaluation", IEEE Transactions on Power Systems, Vol. 16, No. 1, February 2001.

[MCC, 1999] McCalley J., Vittal V., Abi-Samra N., "An Overview of Risk Based Security Assessment", Proceedings of the IEEE Power Engineering Society Summer Power Meeting, 1999, pp. 173-178.

[MCC, 2000] McCalley J., "Security Assessment: Decision Support Tools for Power System Operators", Presentation slides, September 5 2000, Iowa State University.

[MOR, 2004] Morison, K., Wang L. Kundur, P., "Power system security assessment", IEEE Power and Energy Magazine, Vol. 2, No. 5, September 2004.

[NI, 2003] Ni M., McCalley J., Vittal V., Tayyib T., "Online risk-based security assessment", IEEE Transactions on Power Systems, Vol. 18, No. 1, February 2003, pp. 258-265.

[SCH, 1999] Schlumberger Y., Lebrevelec C., De Pasquale M., "Power system security analysis: New approaches used at EDF", Proceedings of IEEE SM'99, Alberta Canada, July 18–22, 1999, pp. 147–151.

[SHA, 2003] Shahidehpour M. , Y. Wang, Communication and Control in Electric Power Systems, IEEE Pres Power Engineering Series, 2003, Chapter 1.

[TRA, 2004] Tranchita C., Torres A. "Events classification and operation states considering terrorism in security analysis". Proceedings IEEE Power Systems Conference and Exposition, October 2004, Vol. 3, pp. 1265 – 1271, ISBN : 0-7803-8718-X

[TRA, 2006a] Tranchita C., Hadjsaid N., Torres A., "Ranking Contingency Resulting from Terrorism by Utilization of Bayesian Networks". Proceedings IEEE Mediterranean Electrotechnical Conference MELECON 2006, pp. 964–967, ISBN : 1-4244-0087-2.

[TRA, 2006b] Tranchita C., Hadjsaid N., Torres A., "Security Assessment of Electrical Infrastructure under Terrorism", Proceedings IEEE Third International Conference on Critical Infrastructures, Town Alexandria VA, USA, September 2006.

[WEH, 1997] Wehenkel L., "Machine-Learning Approaches to Power System Security Assessment. IEEE Expert: Intelligent Systems and Their Applications archive. Vol. 12, Issue 5 September 1997, pp: 60 – 72. ISSN: 0885-9000

[WGC, 1987] CIGRE WG 38-03, D. McGillis Chairman, Power System Reliability Analysis Application Guide. CIGRE, Paris, 1987.

[WGC, 1993] Working Group 37.08 CIGRE, "Adequacy and Security of Power System at Planning Stage", CIGRE Electra, No. 149, August 1993, pp. 111-121.

[WGC, 1997] CIGRE WG 38-03, "Power Systems Security Assessment: A position Paper". CIGRE Electra, No. 175, December 1997, pp 53-77.

CHAPTER III

3. UNCERTAINTY MODELLING

Uncertainty is a term that involves diverse concepts and can be used differently in multiple domains. It is defined as: "the quality or state of being ambiguous"[1], "doubtfulness", "vagueness", "an expression of the magnitude of a possible deviation of a measured value from the true value"[2], "incompleteness of knowledge". Uncertainty occurs in a situation in which it is not possible to assign a definitive value to objects or events or when it is impossible to predict a situation accurately. At this point, uncertainty is a consequence of non-sharp boundaries between notions or objects and is not necessarily caused by lack of information.

Traditionally, uncertainty has been modelled using the probability theory. Nevertheless, given that uncertainty is not equal in every case, other forms have been formulated to handle a variable's uncertainty, e.g. the possibilities theory (Zadeh, 1978; Dubois and Prade, 1985), the Dempster-Shafer theory (Dempster, 1967; Shafer, 1976), and the Hints models (Kohlas and Monney, 1995).

Uncertainty and imprecision analyses associated with the modelling of real physical power system phenomena and events that affect the operation of the power grid are useful for security assessment. When uncertainty is incorporated into models it is often used in providing information which can be used to take correct actions and make appropriate decisions. Some sources of uncertainty are the data acquisition, the perception, the interpretation and the simplifications and solutions of the model formulation.

We have identified two principal categories of uncertainty in the security assessment of power systems, with regard to the possibility of intentional attacks. The first uncertainty is related to the occurrence of attacks upon the power system and the magnitude of the attack. The second uncertainty is linked to the impact on the power system behaviour given the occurrence of an attack.

The decision of whether to attack a power system or not, depends on factors of a diverse nature which constantly change over time. The motivation, the weapons and the targets all influence the decision. These factors and the magnitude of the attack are uncertain and difficult to model since various types of uncertainty are involved. To model an attack means having to model human will, social, psychological, economical, political and technical variables but also the cause-effect relationships; and herein lays another difficulty, as almost all inferences are uncertain, too.

The theory of probability and more specifically the Bayesian Networks, is employed in our methodology to model the intentional attacks against the power system and to rank contingencies linked to terrorism (the specific case of intentional attacks covered in this

[1] Thesaurus Dictionary
[2] European Committee for Electro technical Standardization

work). Moreover, an extension of the model is made in this work to assess the risk of cyber attacks on the power system network.

The chosen method in this thesis for evaluating the impact of the attacks on steady-state operation is the load flow. The sources of uncertainty in this model come from mathematical approximations, parameter values and the inability of the model to appropriately represent the components' behaviour. In addition, the power injections have different uncertainty levels that come from data collection, measurement and load forecasting. We use fuzzy set theory, in particular fuzzy number arithmetic, to model uncertainties present in the load flow problem.

This current chapter is an attempt to familiarize the reader with the type of uncertainties present in the power engineering problems and (depending on the case) when one representation is more appropriate than another. We will analyze in detail the uncertainty representations used in this thesis and the mathematical foundation supporting our work.

3.1 Taxonomy and Representation of Uncertainty

The uncertainty taxonomy is usually classified in accordance with different research areas and the purview. In power systems engineering, uncertainty influences models, designs and decisions as much in the technical as in the economic scope. In the last three decades much of the research done on the area has tried to include uncertainty in the power systems planning and operation analyses.

The purpose of defining and differentiating the type of uncertainty present in the problems, is to determine which uncertainty modelling is the most advisable one to use. This is necessary in order to mitigate the impact of uncertainty on the models, designs and decisions. Nevertheless, a proper taxonomy in this field does not exist and classifications are frequently made in a practical rather than in a theoretical sense [TUN, 2003]. The classification given by Torres in [TOR, 2002, 2004] is adopted. Different types of uncertainty can be found: determinism, randomness, ambiguity or non-specificity, vagueness and confusion.

Determinism, as the lowest degree of uncertainty, corresponds to the perfect knowledge of the results and of the occurrence of the events. Therefore, it is the non-existence or non-consideration of uncertainty. Determinism is the belief that all phenomena can be explained by the cause-effect relationship. The effect is explained by the cause, any incidence from the environment is excluded and the fact that many causes take part in any phenomena is ignored (the effect is not just the product of a single one of them).

Randomness, as a higher degree of uncertainty, is present when the possible results of an experiment are known, for example in the throwing of a dice or a coin. It also appears in conflicting situations, such as in the case of a statement that can be true or false. This type of uncertainty has been represented with the theory of probability.

Ambiguity results from the existence of different meanings for a word or an expression. In this case, events are not clearly specified or defined. It corresponds to a lack of information and it occurs when a relation of one-to-many exists. Ambiguity can be stated when there is a discrete set of possible meanings, which produces uncertainty about which is the appropriate one in a certain instance (polysemy) [LAV, 1994]. Ambiguity is also related to non-specificity,

which is the failure to give in sufficient detail, which would otherwise permit identification. But non-specificity may not always be undesirable, non-specific designation may preserve a degree of generality and this is welcomed in an otherwise over-specialized world [SHE, 2003].

Vagueness makes it impossible to establish the truth or falseness of a statement and is related to Fuzziness. In general, vagueness differs from ambiguity as vagueness comprehends different incompatible meanings but can be solved with more information [TOR, 2002, 2004]. Vagueness comes from a continuous spectrum of interpretations, the absence of precise limits (combined with a multiplicity of use of criteria), and leads to a set of meanings that overlap. Fuzziness is associated with the absence of sharp boundaries and occurs when the law of non-contradiction (and equivalently the law of excluded middle) is violated [KOS, 1990]. Fuzzy measures indicate the degree to which an event occurs, not whether it occurs or not.

Confusion is a conflict uncertainty type, which combines ambiguous and vague characteristics. This type of uncertainty is not solved with more information.

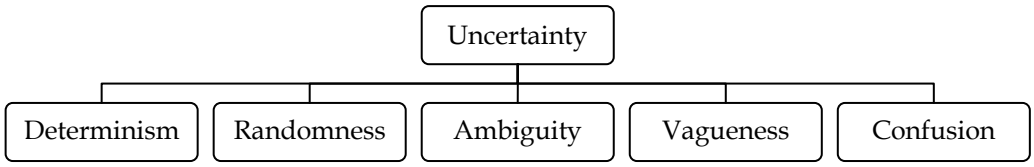


Figure 3-1. Uncertainty taxonomy.

Finally, risk in engineering can be considered as a measurement of uncertainty because it involves the uncertainty linked to the occurrence of an unwanted event and its consequence. Normally, risk is quantified as a measurement of fulfilment regarding a technical requirement, a technical or economic objective or of accomplishment of a planning in the occurrence of undesired events that affect the respective requirement, objective, or planning.

In order to assess the risk, the threats due to the occurrence of events or phenomena have to be represented by means of uncertainty models. Assuming that an event has taken place, the consequence and the uncertainty associated with it are modelled. Therefore, the risk is the multiplication of these factors using coherent arithmetic alongside the modelling. Technical risk in power systems has traditionally been a measurement of the proportion in which the system fulfils reliability and security standards in disturbance conditions or in a normal state.

3.1.1 Approaches for representing uncertainty

Some approaches for modelling uncertainties are: the classical set theory, the probability theory, the evidence theory, the possibility theory, and the interval analysis among others. These theories are used more and more in power engineering, and mathematical models are constantly being developed in order to deal with uncertainties.

Probability is the most developed model for representing an uncertainty. The quantification of uncertainties allows us to deal with inherent uncertainties in real problems. In addition, the set of principles that define the probability provides a basis for rational inference [TOR,

2002, 2004]. A single definition of probability does not exist. Two approaches are mentioned: objectivist probability and subjectivist probability.
From the objectivist or frequencist viewpoint of probability, the information about an uncertain event has to be registered in an exact form (historical or experimental) with the aim of defining a probability degree. In this case, probability is identified as an infinite sequence of identical and independent tests, which are actually "very large", replacing the word "infinite". As a general principle, probability varies with the availability of information. Estimations of any event are more reliable when the data of more events exists. Based on this approach, the uncertainty problems can be modelled assigning probabilities to the different events by means of a relative frequency and statistical analysis. These outcomes are clearly defined and a very concrete measurement of the probability of events is obtained. The objectivist probability models especially the randomness uncertainty.

However, if this is not possible from the subjectivist viewpoint of probability or Bayesianism, probability can be considered as a personal measurement of uncertainty or belief in an event. The probability then does not exist as something concretely defined. This consideration enables us to model some problems in which the data of the occurrence of an event is not available (e.g. when it is impossible to repeat an experiment in several occasions). In this case, the probability may be assigned based on the belief of people about the occurrence of the event. Some authors affirm that any type of uncertainty can be dealt with using the subjectivist theory of probability, thereby reducing the non-precise characteristics of the event. Thus, it is possible to assign probabilities in a highly practical degree, without the need of absolute precision of the probability. The appreciation can also be non-numerical, i.e. it is possible to give a grade of probability, such as "the probability is high". This means that Bayesianism can represent ambiguity and vagueness and can even be extended to fuzzy set theory.

Fuzzy theory and *possibility theory* are methods that facilitate the analysis of uncertainty for systems where uncertainty arises due to ambiguity, vagueness or fuzziness rather than randomness [ZAD, 1978]. In fuzzy sets, the membership is not a matter of affirmation or denial, but rather a matter of degree.

Zadeh presented his possibility theory and the development of fuzzy sets at the same time. This theory was presented as a "complementary, but non-equivalent" alternative to the theory of probability [ZAD, 1978]. The non-random uncertainty can arise from imprecision and lack of specificity related to vagueness or ambiguity. According to Zadeh, ambiguous or vague predicates lead to fuzzy sets. Vague predicates, quantifiers and qualifiers are intrinsic in natural languages and they produce uncertainties in sentences. For instance, in the sentence "there is a high possibility that the load exceptionally exceeds 10MW", the source of uncertainty does not appear to be probabilistic. Possibilistic concepts depend mainly on sources such as planning, selection, preparation, difficulty and opportunity among others. In this scope, possibility is measured in the interval [0,1], instead of only the two values {0,1}.

The use of intermediate degrees of possibility fits better with the meaning of the frequent expressions that produce the so-called nonrandom uncertainty. This is the foundation of the possibility theory, which is an extension of the fuzzy set theory. The possibility distribution can be represented by a fuzzy number, where the possibility has the same numerical value as the grades of membership of the fuzzy number. This theory measures plausibility and belief. It is also possible to have a correspondence to the classical probability measures.

3.2 Sources of Uncertainty for Power Systems

It can be stated that a problem of power engineering does not exist with all the information about all of the variables and where information does not have a degree of uncertainty or imprecision. A problem of power engineering completely deterministic and with all of the data is not a "real" problem. Uncertainty arises from ignorance, from chance, from imprecision, from complexity, etc.
Table 3-1 shows the main sources of uncertainty in the planning and operation of a power system.

3.3 Modelling Uncertainties by Using Probabilistic Inference

The development of the current theory of probability is based on the following postulates (axiomatic definition of probability):

Definition 1. The probability of an event A is a number $P(A)$ that obeys:

1. $P(A)$ is positive:

$$P(A) \geq 0 \qquad [3\text{-}1]$$

2. If S represents a certain event the probability of S equals 1:

$$P(S) = 1 \qquad [3\text{-}2]$$

3. If A and B are mutually exclusive:

$$P(A + B) = P(A) + P(B) \qquad [3\text{-}3]$$

An uncertainty is described by the probability distribution and the probability density functions. A probability distribution is a function that according to the situation, assigns numbers between 0 and 1 (probabilities) to events. For any set of events there are many ways to give probabilities, so the choice of one distribution or another is equivalent to making different assumptions about the events or propositions in question.

3.3.1 Probabilistic inference

When real life problems occur, immediate information (data, experience, a priori reasoning) is used to make inferences that lead us to have more extensive information, which is not directly observed. Therefore through inference, observations of circumstances are used to reveal other facts not immediately visible or to establish causal-effect relationships.

The term inference is used as a synonym for connectedness. In a broader sense, inference goes from the implication, to the operative mental process by means of which (starting from given information) a conclusion is reached by implication or by induction [KIN, 2000].

In the probabilistic inference, the probability models the uncertainty. The joint probability distribution function of a system of variables is used to describe the dependency relationship between variables and, even to obtain conclusions about cause-effect relationships. The introduction of probabilistic network models has allowed us to bypass some probabilistic inference obstacles (caused by lack of clearness to understand relationships into models). The Markov and the Bayesian networks are the most used graphic models representing probabilistic inference.

TABLE 3-1. SOURCES OF UNCERTAINTY IN THE PLANNING AND OPERATION OF POWER SYSTEMS

Criteria	Description
Power System Model	Uncertainty associated with the modelling of the phenomenon under study and the representation of actual variables in the power system behaviour. In this case, a source of uncertainty is the use of mathematical approaches and of simplifications. This usually takes place when equilibrium between the complexity of the model, the precision and the computational cost (measured in time) is desired. Another source of uncertainty is the lack of knowledge of an appropriate modelling of the phenomenon and the lack of numerical solution methods of the mathematical formulations. Also, numerical and programming errors of the models arise because of the use of computers and software.
Model Parameters	The parameter values of the models are also a source of uncertainty since the modelled value can differ from the real value. The components' parameters can change, for example, because of external variables, the exposure of the components to the environment or by the natural wearing down of the materials. Parameters on some occasions are uncertain or erroneous because of wrong calculations or inaccurate measurements of components, such as lines, transformers and generators.
Measurements	Uncertainty due to the inability to perform adequate measurements of real values of the power system's physical magnitudes. The uncertainty associated with measurements can occur because of the inaccuracy of measuring instruments or due to the approach and errors in the data acquisition. For example, for security analysis purposes, physical measurements are analyzed to establish an instantaneous "image" of the power system, in order to operate the system appropriately. Algorithms are used to diminish the uncertainty contained in the data.
Predictions and forecasting	Uncertainty associated with the prediction of some future state of affairs. The prediction of hydro-meteorological phenomena is an important task since these phenomena affect power generation, transmission and distribution, and behaviour of the electricity demand. The occurrence of these phenomena is predominantly of a random nature. A good example of this is the situation of countries that depend on hydraulic generation. Rain prediction is one of most important and influential tasks at the time of planning the generation unit commitment and market prices. In addition, many of the faults of the transmission and distribution systems are due to the occurrence of meteorological phenomena. A correct design must take the occurrence of theses events into consideration. Electrical load forecasting is necessary to plan and to correctly operate the power system. The load is mainly influenced by meteorological conditions, seasonal effects, gross state product, price index, electricity tariff, etc. Uncertainty in the load forecasting, depends predominantly on human will and meteorological conditions, which means dealing with the uncertainty becomes very complex.
Human intervention	This uncertainty is associated with man's intervention in different processes, from design, instruction, operation, maintenance due to the use of the power network, etc. Humans can make mistakes at any level. Humans can also intentionally act with the objective to affect the "good" operation of the power system. These acts can be significant and change the behaviour of the power system.

3.3.2 Bayesian networks

A Bayesian network or a belief network is a graphical network that allows us to model problems related to uncertain situations. This is based on conditional probabilities and also on the Bayesian probability. A Bayesian network enables us to include experts' concepts. In addition to this, new information (about the occurrence of the events or dependency relationships between variables) can be incorporated in a consistent manner with the aim of analyzing their propagation throughout the network. Probability values of uncertain events or variables can be found and by consequence this fact helps the decision making and the diagnostic process.

The Bayesian network is built on the well known Bayes' theorem, which is itself derived from the fundamental rule for probability calculus:

$$P(A|B) = \frac{P(A,B)}{P(B)} = \frac{P(A) \times P(B|A)}{P(B)} \qquad [3\text{-}4]$$

Where, $P(A)$ is the current probability of the hypothesis. It is the belief measure about the event A and the event B is observed. Then $P(A)$ is the prior probability. $P(B|A)$ is the conditional probability of event A occurring given that event B occurred. This probability shows that the evidence is present, given that the hypothesis is true. For a fixed B, $P(B|A)$ is called the likelihood of B. We can read Bayes' Theorem as:

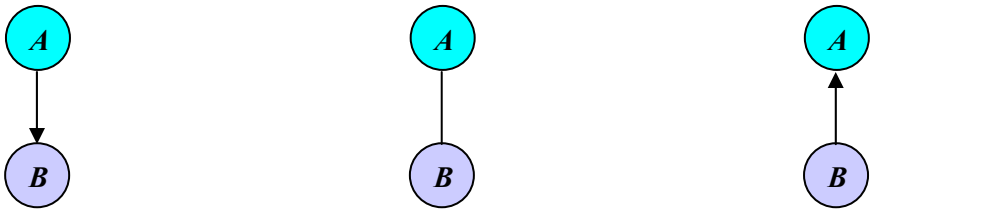
$$\text{Posterior} = \frac{\text{Prior} \times \text{Likelihood}}{\text{Probability of evidence}}$$

The structure of a Bayesian network is a graphical and qualitative illustration of the interactions between the set of variables that it models. In a Bayesian network each node is a variable X that can be discrete or continuous (normally it is a discrete variable because continuous variables are very limited by the type of distribution). A node can represent propositions taking Boolean values (i.e. yes or no), a set of ordered values (i.e. low, medium, high) or integral values (i.e. all possible values between $[x_1, x_2]$).

The directed graph structure can mimic the causality present in the modelled domain through arrows. However, in a broader sense arrows can represent inference, and not only causality. If the structure is causal, it gives a useful, modular insight into the interactions between the variables and allows predictions about the effects of external manipulation. In a Bayesian Network, the quantitative relationship between variables is the joint probability distribution among them.

When data are observed, an inference procedure is required and this involves calculating marginal conditional probabilities by means of the Bayes' theorem. Graphically it involves inversing the arrows in the graphs [COW, 1998]. We will discuss this concept in more detail further in the chapter.

Figure 3-2 shows in the simplest way the process of inference. The links or arrows between the events or nodes represent causal relationships between those nodes.



$P(A)\times P(B|A)$
Prior belief
A is a possible cause of the effect B

$P(A,B)$
Joint probability of both events A and B occurring

$P(B)\times P(A|B)$
Posterior belief
A can be inferred from B

Figure 3-2. Prior-to-posterior inference process [COW, 1998].

In order to find the joint probability of a group of n variables, the general factorization formula is showed in the equation [3-5] (in accordance with the Bayes' Theorem of the equation [3-4]):

$$\begin{aligned} P(X_1, X_2, \ldots, X_n) &= P(X_1|X_2, \ldots, X_n)\times P(X_2, \ldots, X_n) \\ &= P(X_1|X_2, \ldots, X_n)\times P(X_2|X_3, \ldots, X_n)\times P(X_3, \ldots, X_n) \\ &= \vdots \\ &= P(X_1|X_2, \ldots, X_n)\times\cdots\times P(X_{n-1}|X_n)\times P(X_n) \end{aligned} \qquad [3\text{-}5]$$

If n is a large value, this procedure is complex. Conditional independence properties are used to simplify the general factorization for the joint probability distribution.

The modelling of a Bayesian network requires applying the Markov property. This states that a variable is conditionally independent of its non-descendants given its parents. Graphically it means that there are no direct dependencies between the model's variables if not already explicitly shown via edges.

Using the Markov property and the general factorization formula, we can determine the probability distribution of a node by considering the distributions of its parents $P(X|parents(X))$. If x_i denotes some value of the variable X_i and $parents_i$ denotes some set of values for X_i's parents, the full joint probability distribution for the network can be specified by the use of the recursive factorization:

$$p(x_1, x_2, \ldots, x_n) = \prod_{i=1} p(x_i \mid parents_i) \qquad [3\text{-}6]$$

Prior probability distributions describe the nodes with no predecessors.

Consider a Bayesian network of three events X, Y and Z. The joint probability distribution of the whole system is formulated without difficulty in Figure 3-3.

It is to be noticed that a Bayesian network is a directed acyclic graph whose structure describes a set of conditional independence properties [PEA, 1988]. The network offers for a set of variables $\{X_1, X_2, \ldots, X_n\}$ a compact representation of the joint probability distribution.

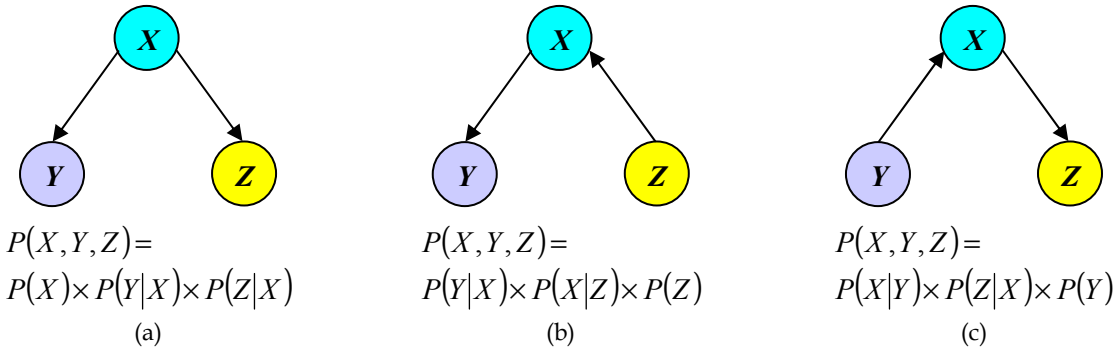


Figure 3-3. Joint probability distributions using the conditional independence properties and the Bayes' theorem.

3.3.2.1 How to construct a Bayesian network?

Both the structure and the numerical parameters of a Bayesian network can be elicited from the experts. We can distinguish between three situations: i) Experts construct the network based on determinist knowledge. The modelling is typically unproblematic because laws and variables are known, e.g., if the transmission line flow exceeds its capacity, the line is overloaded; ii) Experts' knowledge is modelled because the inferences are uncertain. In this case, the modelling can take into account information of a diverse nature and is often laborious, although the experts know this subject matter very well. A good example is the modelling of terrorists' motivation to attack. Experts resort to intuitive reasoning in order to establish variables and cause-effect relationships; iii) Experts assign subjective probability values to network parameters. This practice is used when there is no data available, or frequency probability or statistic methods are not advisable, because of the type of uncertainty.

It is also possible to construct a Bayesian network based on data. Variables and links between variables can be established from statistical (analysis of correlation, covariance, etc.) and optimisation techniques. Nevertheless, it is more common to exploit data with the purpose of finding or completing network probabilities values than to build the topology. The Bayesian network in most cases is then constructed by a mixture of experts' knowledge and the data exploitation (obviously when the data is available). Experts' elicitation is often employed to build the structure due to the reasoning necessary to make inferences.

Although the reader may think that network construction is a simple sequential task of establishing variables, links and parameters, this construction is often complex. Evaluations of probabilities, judgements of conditional independency and cause-effect relationships can lead to changes in the whole topology. Some references on how to construct a Bayesian network are given in [JEN, 1996] and [HEC, 1996].

3.3.2.2 Inference and learning

Once the Bayesian network is constructed, via the *probabilistic inference* we can determinate the posterior probability distribution of variables of interest from the model. The problem is to find the probability of a set of query variables given a set of evidence, which is possible with sequential applications of Bayes' theorem.
Let us observe the Bayesian network of the Figure 3-4. We can use this network with the intention of making different types of inferences; it is illustrated in the Figure 3-5.

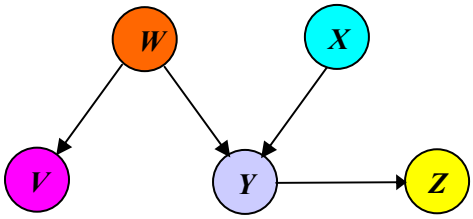


Figure 3-4. An example of a Bayesian network.

If the inference goes from effects to causes it is called diagnostic, or "bottom up". This practice is usual when the network is employed as an expert system or for pattern recognition. The network can also be used for causal or "top down" reasoning; in this case the inference goes from causes to effects. Bayesian networks are often called "generative" models, because they specify how causes generate effects; this is shown in Figure 3-5(a) and (c). Besides, it is possible to make a combination of "bottom up" and "top down" inferences (Figure 3-5(d)).

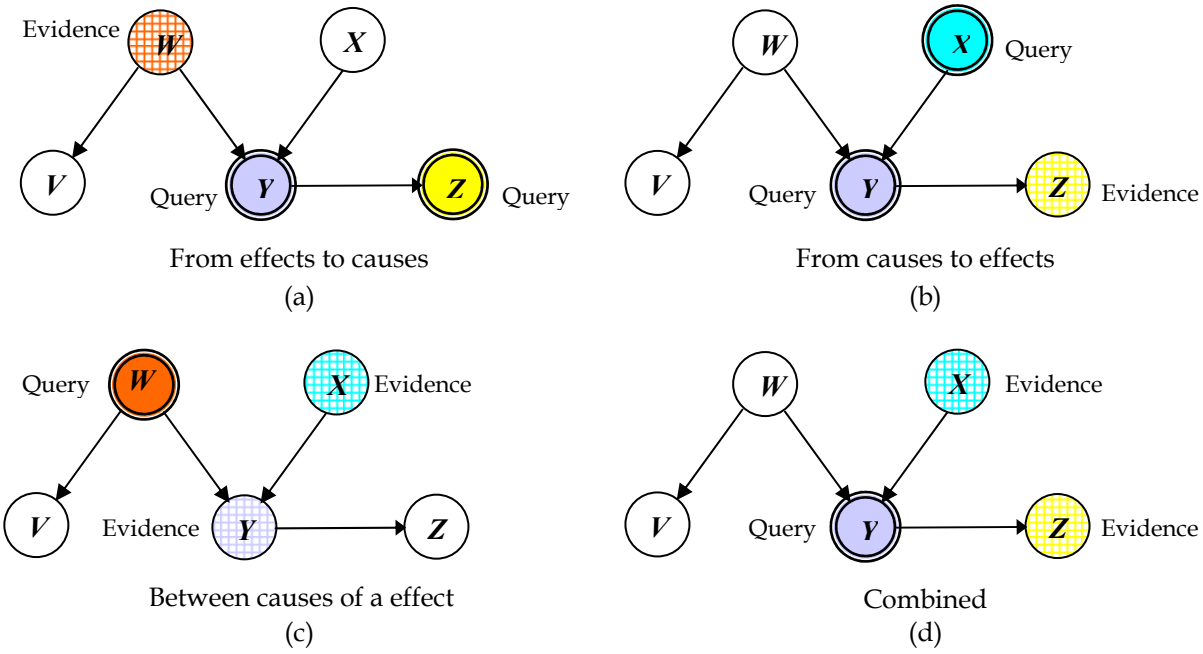


Figure 3-5. Types of inferences.

Now, we illustrate the inference procedure. For the network of the Figure 3-4 we would like to infer W when there is evidence in V, X, Y and Z.
The probability of w given observations of the other variables is equal to:

$$P(w|v,x,y,z)=\frac{P(w,v,x,y,z)}{P(v,x,y,z)} \qquad [3\text{-}7]$$

The calculus of this probability is extensive; however the use of the conditional independencies of the network simplifies it:

$$\begin{aligned} P(w|x) &= P(w) \\ P(x|w) &= P(x) \\ P(v|w,x,z) &= P(v|w) \end{aligned} \qquad \begin{aligned} P(z|y,w,x) &= P(z) \\ P(y|v,w,x,z) &= P(y|w,x) \end{aligned} \qquad [3\text{-}8]$$

The simplified resultant equation is [HEC, 1996]:

$$P(w|v,x,y,z)=\frac{P(w)\times P(x)\times P(v|w)\times P(y|w,x)\times P(z|y)}{\sum_{w'} P(w')\times P(x)\times P(v|w')\times P(y|w',x)\times P(z|y)} \qquad [3\text{-}9]$$

This approach is not always the best, because it entails significant calculation efforts, even if the network has five variables and four edges.

When networks are large, i.e. they are characterised by many variables and links, efficient algorithms are necessary in order to minimise calculations. Numerous probabilistic inference algorithms for Bayesian networks exist. We mention some of them which are detailed in the references. Some exact algorithms are: the junction tree [HUA, 1996], the variable elimination [McE, 2000], the brute force enumeration (for discrete nets) and the Pearl's algorithm (for polytrees) [PEA, 1986]. The algorithms for approximate inference are: likelihood weighting, Gibbs sampling and loopy belief propagation [MUR, 1998].

One major property of the Bayesian networks is the learning. They allow updating the parameter values when new information is available. Once evidence is entered for a node in the network, the evidence is propagated through the network, updating the conditional probabilities $P(X|parents(X))$. The update is possible from observation data using gradient-based or EM (Expectation-Maximization) methods that only utilize local information derived from inference [PEA, 2000]. Evidence can be propagated from parents to children as well as from children to parents, making this method very effective for both prediction and diagnosis [HEC, 1996]. It is also possible to learn the graph topology based on the evidence but this work can be difficult and computationally expensive.

3.3.2.3 When is a formulation of a Bayesian network appropriate?

Bayesian networks are very useful when nondeterministic relationships have to be modelled. It is also possible to integrate both deterministic (linear and nonlinear) and nondeterministic relationships into a single model. This type of graph constitutes a powerful tool to represent prior knowledge and, in a general way, to appropriately model various types of relationships, problems, phenomena, etc.

An advantage of these networks is the ability to mix (in an exceptional theoretical framework -the theory of probability) objective probabilities resulting from a statistical processing and subjective probabilities derived from experts' knowledge. The possibility of incorporating subjective probability values allows us to model different types of uncertainty. This means that, with only one structure, we can represent real problems related to randomness, ambiguity and vagueness uncertainty.

According to Pearls [PEA, 2000], "Bayesian networks are direct representations of the world, not of reasoning process", which it is correct. Unlike neural networks and rule-based systems the links in the graph represent real causal connections and not the flow of information during reasoning. Therefore, inferences can be obtained from Bayesian networks by propagating information in any direction.

All the advantages mentioned above and the capacity learning of the Bayesian networks make using them useful in many fields. Bayesian networks can be employed for the purpose of simulation, prediction, diagnosis, propagation of restrictions as well as for understanding

a specific phenomenon, among others applications. Given the Bayesian network structure, it is intuitive and uncomplicated for a person to understand the direct dependencies and variables' distributions. As a result, sometimes, these graphs are also built with the purpose of improving the communication between experts.

3.4 Modelling Uncertainty by Using Fuzzy Set Theory and Possibility Theory

In this section, we will explain in detail the theory of fuzzy sets and fuzzy numbers that will enable us to formalize the possibility theory.

A set is a well-defined collection of elements and where it is possible to determine if an element belongs to the mentioned set or not. One must answer if the element "belongs" or "does not belong" to the set. As opposed to this, in a fuzzy set, each element of the universe has an associated membership degree to this set, corresponds to a number between 0 and 1. We can say then, that a fuzzy set is a correspondence or function in which each element of the universe has a membership degree associated to it. A fuzzy set can be viewed as a generalization of the concept of a classic set, in which the membership function takes only two values [0,1].

A fuzzy set is a function whose domain is the universe and whose range is the interval [0,1]. The closer the membership degree is to one, the bigger the certitude is for it to be in the set; inversely, the closer the membership degree is to zero, the bigger the certitude is of not being in the set.

Definition 2. A fuzzy set $\tilde{a}$ is a set of ordered pairs, as follows:

$$\tilde{a} = \{(x, \mu_{\tilde{a}}(x)) | x \in X\} \qquad [3\text{-}10]$$

Where, $\mu_{\tilde{a}} : X \to [0,1]$ is called the *membership function*, and x is the *universe of discourse*, $x \in X$.
The membership degree $\mu_{\tilde{a}}$ to a fuzzy set $\tilde{a}$ of an element can be interpreted in different ways, depending on the context. Following are only some possible interpretations:

- Proportion in which an element owns an attribute: If we consider an attribute $\tilde{a}$, then for each element x, the percentage of which x has $\tilde{a}$ is given by the expression $100 \cdot \mu_{\tilde{a}}(x)$.
- Possibility: If we consider an event $\tilde{a}$, then for each element x, $\mu_{\tilde{a}}(x)$ is the possibility of the occurrence of x in the event $\tilde{a}$, i.e. $\mu_{\tilde{a}}(x) = \text{Poss}(x \in \tilde{a})$.
- Measure of belief: If we consider an attribute $\tilde{a}$, then for each element x, $\mu_{\tilde{a}}(x)$ is the degree to which we believe that x has the attribute $\tilde{a}$.

Notice that contrary to the crisp set, one element can be (partially) in a fuzzy set and at the same time in its complement. This condition is not possible in crisp sets because it would violate the exclusion principle. In addition to this, while the borders of a concrete set are exact, those of a fuzzy set are not. An element in the border of a fuzzy set can be in the set and at the same time, out of the set.

3.4.1 Definitions and terminology

Definition 3. The *height* $h(\tilde{a})$ of a fuzzy set $\tilde{a}$ is the largest membership value reached by any point:

$$h(\tilde{a}) = \sup_{x \in X} \mu_{\tilde{a}}(x) \qquad [3\text{-}11]$$

If the height of a fuzzy set $\tilde{a}$ is equal to one, $h(\tilde{a}) = 1$, $\tilde{a}$ is a *normal* fuzzy set.
Definition 4. The *support* of a fuzzy set $\tilde{a}$ is a crisp set which contains all of the elements of X that have a membership value greater than zero:

$$\text{supp}(\tilde{a}) = \{x \in X | \mu_{\tilde{a}}(x) > 0\} \qquad [3\text{-}12]$$

Definition 5. An $\alpha - cut$ of a fuzzy set $\tilde{a}$ is a crisp set ${}^{\alpha}\tilde{a}$ which contains all of the elements in X that have membership value in $\tilde{a}$ greater than or equal to α:

$${}^{\alpha}\tilde{a} = \{x \in X | \mu_{\tilde{a}}(x) \geq \alpha\} \qquad [3\text{-}13]$$

A fuzzy set can be decomposed into a family of fuzzy set by using the concept of $\alpha - cut$ and the resolution principle as follows.

If equation [3-13] is fulfilled for $0 < \alpha \leq 1$, the membership function of the fuzzy $\tilde{a}$ in the universe of discourse X can also be expressed in terms of the characteristic function of the crisp set ${}^{\alpha}\tilde{a}$:

$$\mu_{\tilde{a}}(x) = \sup_{0<\alpha\leq 1} \left[\min\left(\alpha, \mu_{{}^{\alpha}\tilde{a}}(x)\right)\right], \ \forall x \in X \qquad [3\text{-}14]$$

Where $\mu_{{}^{\alpha}\tilde{a}}(x)$ is the characteristic function of ${}^{\alpha}\tilde{a}$ and is given by:

$$\mu_{{}^{\alpha}\tilde{a}}(x) = \begin{cases} 1 & if\ x \in {}^{\alpha}\tilde{a} \\ 0 & \text{otherwise} \end{cases} \qquad [3\text{-}15]$$

Let $\alpha^{\alpha}\tilde{a}$ denote a fuzzy set with de membership function:

$$\mu_{\alpha^{\alpha}\tilde{a}}(x) = \min\left(\alpha, \mu_{{}^{\alpha}\tilde{a}}(x)\right), \ \forall x \in X \qquad [3\text{-}16]$$

The *resolution principle* declares that a fuzzy set $\tilde{a}$ can be expressed by equation [3-17] or the equation [3-18]:

$$\tilde{a} = \bigcup_{\alpha \in \Pi_{\tilde{a}}} \alpha^{\alpha}\tilde{a} \qquad [3\text{-}17]$$

$$\tilde{a} = \int_0^1 \alpha^{\alpha}\tilde{a} \qquad [3\text{-}18]$$

This decomposition of the fuzzy set in term of its $\alpha - cuts$ allows us to use non fuzzy techniques for the operations. After, by means of the representation theorem, the fuzzy is reconstructed as a union of its $\alpha^{\alpha}\tilde{a}$.

Definition 6. A fuzzy set $\tilde{a}$ defined on X is *convex* if the equation [3-19] is fulfilled for all $\lambda \in [0,1]$, $x_1, x_2 \in X$:

$$\tilde{a}(\lambda x_1 + (1-\lambda)x_2) \geq \min(\tilde{a}(x_1), \tilde{a}(x_2)) \qquad [3\text{-}19]$$

$\tilde{a}$ is *convex* if and only if all its $\alpha - cut$ ${}^{\alpha}\tilde{a}$ are convex sets, for any α in the interval $\alpha \in [0,1]$.

Definition 7. A fuzzy set $\tilde{a}$ defined on X is *concave* if the equation [3-20] is fulfilled for all $\lambda \in [0,1]$, $x_1, x_2 \in X$:

$$\tilde{a}(\lambda x_1 + (1-\lambda)x_2) \leq \max(\tilde{a}(x_1), \tilde{a}(x_2)) \qquad [3\text{-}20]$$

3.4.2 Fuzzy numbers

Fuzzy numbers can be considered as a special class of fuzzy sets with specific properties [DUB, 1980]. These numbers express approximate amounts and are a correspondence between the real numbers R and the unit interval: $R \to [0,1]$.

Definition 8. A fuzzy number is a fuzzy set $\tilde{a}$, $R \to [0,1] = I$,which is uppersemicontinuous, normal and convex, i.e.,

- $[\tilde{a}]^{\alpha} = \{x | \tilde{a}(x) \geq \alpha\}$ is a closed interval
- $\exists x$ such that $\tilde{a}(x) = 1$
- The equation [3-19] is fulfilled for $\lambda \in I$

The fuzzy number can have a variety of forms always keeping a correspondence with the reality. For example, the uncertain value of an electrical load can be represented by a fuzzy number. This number will be a membership function on the real line. A linguistic declaration as "the maximum values of the electrical load will possibly not occur below 20MW and over 30 MW, and the best estimation is, for example, between 24 MW and 26 MW", will be interpreted as in the Figure 3-6.

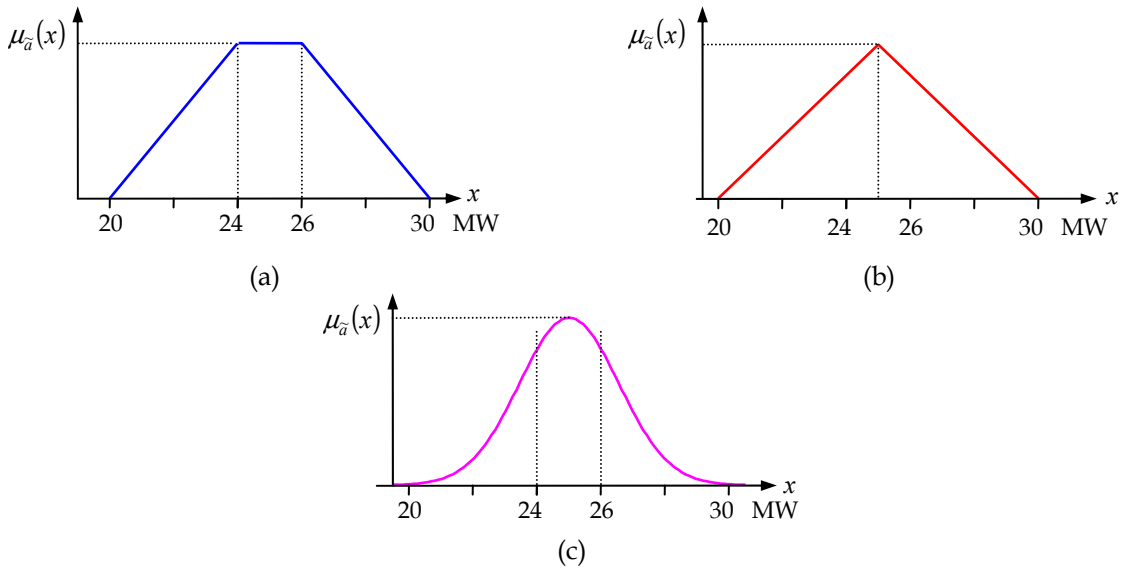


Figure 3-6. Representation of the electrical load by means of different types of fuzzy numbers.

We can employ the *extension principle* in order to define algebraic operations for the fuzzy set and accordingly for fuzzy numbers [MIZ, 1976].

Suppose a function $y = 2x + 1$; the value of y for the crisp value $x = 2$ is $y = 5$. The extension principle gives a method to calculate the value of y when x is a fuzzy number. If, for example x is the fuzzy number "about three", Figure 3-7 shows the process and the result "about 7".

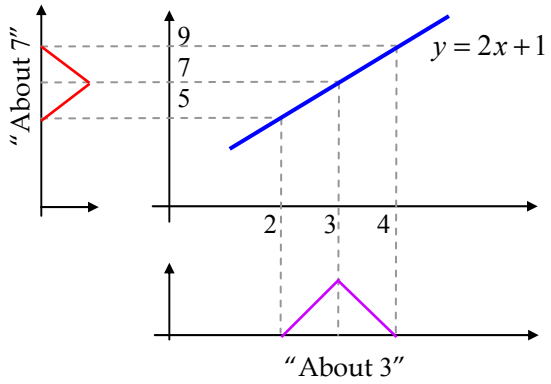


Figure 3-7. An example of the extension principle.

Given a transformation function $f : X \to Y$, $y = f(x)$. Let X be the Cartesian product of universes of discourse $X = X_1 \times X_2 \times \ldots \times X_n$. The principle transforms n fuzzy sets $\tilde{a}_1, \ldots, \tilde{a}_n$ in $X_1, \ldots, X_n$ universes respectively, in a fuzzy set $\tilde{b} = f(\tilde{a}_1, \tilde{a}_2, \ldots, \tilde{a}_n)$ in Y, defined as:

$$\tilde{b} = \left\{ \left(y, \mu_{\tilde{b}}(y) \right) \middle| y = f(x_1, x_2, \ldots, x_n), (x_1, x_2, \ldots, x_n) \in X \right\} \qquad [3\text{-}21]$$

With its membership function as follows:

$$\mu_{\tilde{b}}(y) = \sup_{\substack{(x_1, x_2, \ldots, x_n) \in X \\ y = f(x_1, x_2, \ldots, x_n)}} \min\left[\mu_{\tilde{a}_1}(x_1), \mu_{\tilde{a}_2}(x_2), \ldots, \mu_{\tilde{a}_n}(x_n) \right] \qquad [3\text{-}22]$$

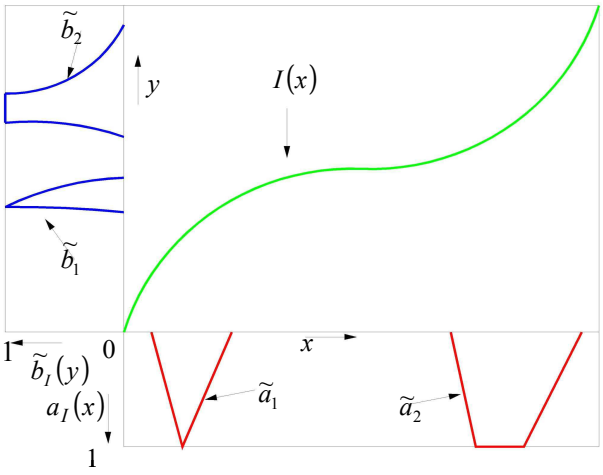


Figure 3-8. Transformation of two fuzzy sets in the universe X, in two fuzzy sets in the universe Y, by the use of the extension principle.

It permits the generalization of conventional operators. Now, we define the extension principle for fuzzy numbers. Let R be the real line, if f is a continuous and increasing operation on two fuzzy numbers $\tilde{a}$ and $\tilde{b}$, the fuzzy number $\tilde{c}$ is obtained with $\tilde{c} = F(\tilde{a}, \tilde{b})$. F is the induced function of f, such as: $F(\{x\},\{y\}) = f(x,y)$. Then its membership function is continuous and is given by [3-23]:

$$\mu_{\tilde{c}}(z) = \sup_{x,y \in R: z = f(x,y)} \min\left[\mu_{\tilde{a}}(x), \mu_{\tilde{b}}(y)\right] \qquad [3\text{-}23]$$

As a consequence, the number $\tilde{c}$ is normal because $\tilde{a}$ and $\tilde{b}$ are normal.

There are different ways to implement the extension principle that entail various fuzzy types of arithmetic. These concepts differ in how the numbers have been implemented [HAN, 2000].

3.4.3 *Implementation of fuzzy numbers*

Figure 3-9 shows schematically the different implementations of fuzzy numbers.

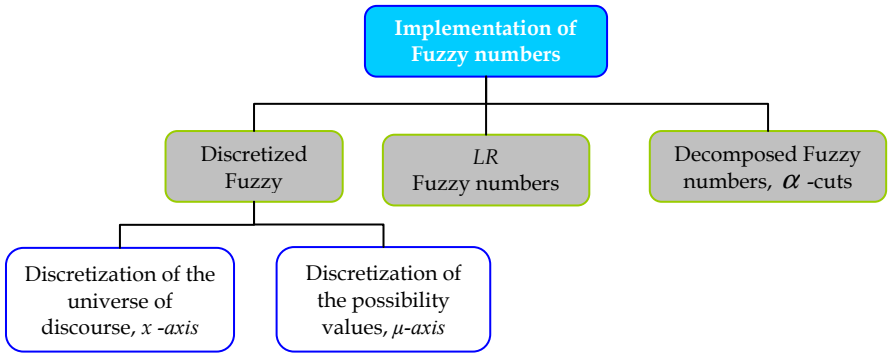


Figure 3-9. Implementation of fuzzy numbers

3.4.3.1 Discretized fuzzy numbers

Two different ways of obtaining the discretization are: discretizing the membership functions by subdividing either the abscissa or the ordinate into intervals of definite length [HAN, 2000].

Let us suppose that $m+1$ intervals are given as a result of the discretization of the x-axis. Each interval is increased in a $\Delta x = (x_{\max} - x_{\min})/m$ value. Then depending on the universe of discourse x of the fuzzy number m will be a more or less suitable number for discretization. This entails unintended effects when arithmetical operations are performed. Very fine intervals of x involve a high computational cost. Reducing the x subdivision, the operations result may show non-convexity and therefore the result cannot continue to be operated [HAN, 1999]. It is also possible to discretize $\mu(x)$, however given the similarity with the α-cuts sets decomposition; we will only discuss this last method.

3.4.3.2 *L-R* numbers

LR numbers are a special class of fuzzy numbers. The membership function is characterized by a left ascending function (L) and a right descending function (R). The reference functions L and R are functions fulfilling the symmetry, convexity and normality properties [DUB, 1980].

We define a LR fuzzy number as equation [3-24]. There are two reference functions and three scalar values: m is the modal value, α is the left spread, and β is the right spread.

$$(m,\alpha,\beta)_{LR} = \tilde{a}(x) = \begin{cases} L\left(\dfrac{m-x}{\alpha}\right) & \text{si } x \le m, \quad \alpha > 0 \\ R\left(\dfrac{x-m}{\beta}\right) & \text{si } x > m, \quad \beta > 0 \end{cases} \qquad [3\text{-}24]$$

Given two fuzzy LR numbers, by means of the extension principle, operations such as sum, negation and multiplication can be used in a very simple way.

$$\tilde{a}_1 = (m_1,\alpha_1,\beta_1)_{LR} \quad \tilde{a}_2 = (m_2,\alpha_2,\beta_2)_{LR}$$

$$\tilde{a}_1 + \tilde{a}_2 = (m_1+m_2,\alpha_1+\alpha_2,\beta_1+\beta_2)_{LR} \qquad [3\text{-}25]$$

$$-\tilde{a}_1 = (-m_1,\beta_1,\alpha_1)_{LR} \qquad [3\text{-}26]$$

The exact product of two fuzzy LR numbers is not a LR fuzzy number. There are approximate formulas to make the product a LR number. For $\tilde{a}_1 \cdot \tilde{a}_2 > 0$, the tangent approximation is shown in [3-27] and secant approximation in [3-28]:

$$\tilde{a}_1 \cdot \tilde{a}_2 \approx (m_1 m_2, m_1\alpha_2 + m_2\alpha_1,\ m_1\beta_2 + m_2\beta_1)_{LR} \qquad [3\text{-}27]$$

$$\tilde{a}_1 \cdot \tilde{a}_2 \approx (m_1 m_2, m_1\alpha_2 + m_2\alpha_1 - \alpha_1\alpha_2,\ m_1\beta_2 + m_2\beta_1 + \beta_1\beta_2)_{LR} \qquad [3\text{-}28]$$

For $\tilde{a}_1 \cdot \tilde{a}_2 > 0$, the secant approximation for the division operation is:

$$\frac{\tilde{a}_1}{\tilde{a}_2} \approx \left(\frac{m_1}{m_2}, \frac{m_1\beta_2 + m_2\alpha_1}{m_2(m_2+\beta_2)}, \frac{m_1\alpha_2 + m_2\beta_1}{m_2(m_2-\alpha_2)}\right)_{LR} \qquad [3\text{-}29]$$

Although these sorts of approaches in the operations calculation facilitate the use of LR numbers, the disadvantages can be even greater. For example, the fact that basic nonlinear operations such as multiplication and division must be linealizared, causes a loss in the uncertainty information. Additionally, since these numbers are a combination of $L-R$ functions, the representation of uncertainty with the base functions can not always be successfully guaranteed [HAN, 2000].

3.4.3.3 Decomposed fuzzy numbers

Another way to implement fuzzy numbers is to decompose the membership axis $\mu(x)$ in $(m+1)$ levels [KAU, 1980]. This approach will allow us to simplify the fuzzy calculation. The fuzzy number $(\tilde{p})$ is decomposed into α-cuts, leading to a set:

$$P = \left\{ X^{(0)}, X^{(1)}, \ldots, X^{(m)} \right\} \qquad [3\text{-}30]$$

of $(m+1)$ intervals:

$$X^{(j)} = \left[a^{(j)}, b^{(j)}\right] \quad , a^{(j)} \le b^{(j)}, \quad j = 0,1,\ldots,m \tag{3-31}$$

For the purpose of decomposing into α-cuts, the μ-axes are equally subdivided, spaced by $\Delta\mu = 1/m$ and $(m+1)$ levels of membership μ_j are then given by $\mu_j = j/m$, $j = 0,\ldots,m.$ Given the decomposition characteristics and since operations among fuzzy numbers are based on the extension principle, the intervals arithmetic can be generalized for fuzzy numbers [KAU, 1980]. Then, considering two fuzzy numbers $\tilde{a}$ and $\tilde{b}$ decomposed into the sets of intervals A and B with [KAU, 1980]:

$$A = \left\{\left[a_1^{(0)}, b_1^{(0)}\right], \left[a_1^{(1)}, b_1^{(1)}\right], \ldots, \left[a_1^{(m)}, b_1^{(m)}\right]\right\} \tag{3-32}$$

$$B = \left\{\left[a_2^{(0)}, b_2^{(0)}\right], \left[a_2^{(1)}, b_2^{(1)}\right], \ldots, \left[a_2^{(m)}, b_2^{(m)}\right]\right\} \tag{3-33}$$

Operations of standard arithmetic can be defined by applying interval arithmetic separately to each membership level μ_j, $j = 0,1,\ldots,m$ [KAU, 1980]:

$$\left[a_1^{(j)}, b_1^{(j)}\right] \circ \left[a_2^{(j)}, b_2^{(j)}\right] = \left[\min\left(O^{(j)}\right), \max\left(O^{(j)}\right)\right] \tag{3-34}$$

$$O^{(j)} = \left\{a_1^{(j)} \circ a_2^{(j)}, a_1^{(j)} \circ b_2^{(j)}, b_1^{(j)} \circ a_2^{(j)}, b_1^{(j)} \circ b_2^{(j)}\right\} \tag{3-35}$$

With theses last equations, the elementary operations are given by:

$$\tilde{a} + \tilde{b} = \left[a_1^{(j)}, b_1^{(j)}\right] + \left[a_2^{(j)}, b_2^{(j)}\right] = \left[\left(a_1^{(j)} + a_2^{(j)}\right), \left(b_1^{(j)} + b_2^{(j)}\right)\right] \tag{3-36}$$

$$\tilde{a} - \tilde{b} = \left[a_1^{(j)}, b_1^{(j)}\right] - \left[a_2^{(j)}, b_2^{(j)}\right] = \left[\left(a_1^{(j)} - b_2^{(j)}\right), \left(b_1^{(j)} - a_2^{(j)}\right)\right] \tag{3-37}$$

$$\tilde{a} \cdot \tilde{b} = \left[a_1^{(j)}, b_1^{(j)}\right] \cdot \left[a_2^{(j)}, b_2^{(j)}\right] = \left[\min\left(M^{(j)}\right), \max\left(M^{(j)}\right)\right] \tag{3-38}$$

$$M^{(j)} = \left\{a_1^{(j)} a_2^{(j)}, a_1^{(j)} b_2^{(j)}, b_1^{(j)} a_2^{(j)}, b_1^{(j)} b_2^{(j)}\right\} \tag{3-39}$$

$$\frac{\tilde{a}}{\tilde{b}} = \left[a_1^{(j)}, b_1^{(j)}\right] / \left[a_2^{(j)}, b_2^{(j)}\right] = \left[\min\left(Q^{(j)}\right), \max\left(Q^{(j)}\right)\right] \tag{3-40}$$

$$Q^{(j)} = \left\{\frac{a_1^{(j)}}{a_2^{(j)}}, \frac{a_1^{(j)}}{b_2^{(j)}}, \frac{b_1^{(j)}}{a_2^{(j)}}, \frac{b_1^{(j)}}{b_2^{(j)}}\right\} \text{ if } \quad 0 \notin \left[a_2^{(j)}, b_2^{(j)}\right] \tag{3-41}$$

Finally, the fuzzy-valued results of the operations can be obtained by recomposing the corresponding intervals into fuzzy numbers. A precise analysis of this arithmetic is presented [KAU, 1980].

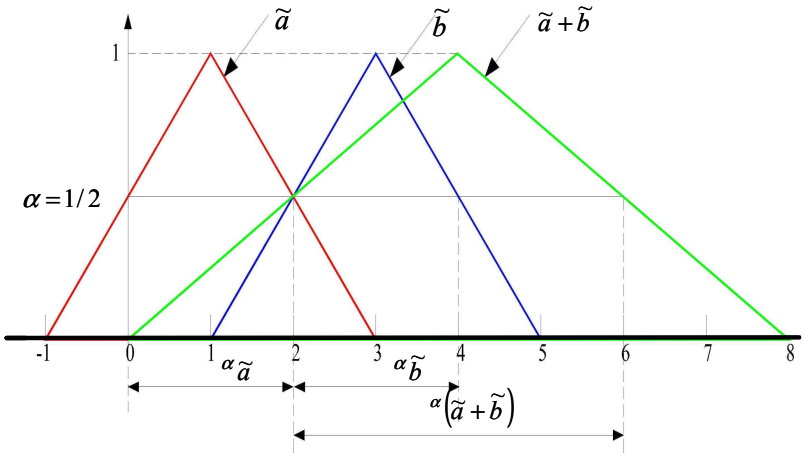


Figure 3-10. Sum of two fuzzy numbers using the standard fuzzy arithmetic.

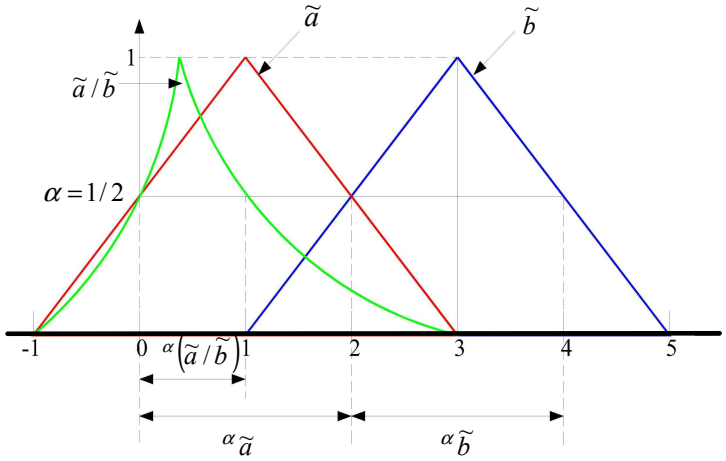


Figure 3-11. Division of two fuzzy numbers using the standard fuzzy arithmetic.

3.4.4 Standard vs. constrained fuzzy arithmetic

In this thesis we have called standard fuzzy arithmetic the *LR* fuzzy numbers arithmetic and the intervals arithmetic. Although these tools have been used in many engineering applications, their main limitation is the overestimation or "pessimism" problem [HAN, 2000], [KLI, 1997]. In parameterized fuzzy models, each variable is independently considered in each occurrence, although the same variable occurs several times in the model [KLI, 2003]. In the case of the intervals arithmetic "the overestimation effect arises from evaluating the arithmetical expression by mistake for combinations of elements of the support part of the fuzzy numbers which in reality can never occur" [HAN, 2000].

In order to counteract the short-comings of standard arithmetic, some algorithms that take into account the dependency from variables have arisen and most of them use optimization routines. These methods have been called "constrained fuzzy arithmetic". Details of the most used methods are in [KAU, 1980], [DON, 1987] and [HAN, 1999, 2000].

3.4.5 Transformation method [HAN, 1999, 2000]

The transformation method can be considered as an advanced and extended version of the so-called vertex method [DON, 1987]. By using this technique for the simulation of fuzzy parameterized models, the complete information about the uncertainties in the model and

how the uncertainties are propagated can be included through the calculation procedure [HAN, 1999, 2000].

The implementation of fuzzy arithmetic using the transformation method reduced as a main topic of [HAN, 1999] and [HAN, 2000] is presented as follows:

We assume that the fuzzy-parameterized model is given by arithmetical expression F:

$$\tilde{q} = F(\tilde{p}_1, \tilde{p}_2, \ldots, \tilde{p}_n) \qquad [3\text{-}42]$$

There are n independent fuzzy-valued model parameters $\tilde{p}_i$ with memberships: $\mu_{\tilde{p}_i}(x_i),\ i = 1, \ldots, n$. Each input fuzzy parameter $\tilde{p}_i$ is decomposed into α-cuts, as shown before:

$$P_i = \left\{ X_i^{(0)}, X_i^{(1)}, \ldots, X_i^{(m)} \right\}, \quad i = 0,1,\ldots,n \qquad [3\text{-}43]$$

$$x_i^{(j)} = \left[a_i^{(j)}, b_i^{(j)} \right] \quad , a_i^{(j)} \le b_i^{(j)} \quad j = 0,1,\ldots,m \qquad [3\text{-}44]$$

The intervals $X_i^{(j)}, i = 1,2,\ldots,n,$ of each membership level $\mu_j, j = 0,1,\ldots,m,$ can now be transformed into arrays $\tilde{X}_i^{(j)}$ of the following form:

$$\tilde{X}_i^{(j)} = \overbrace{\left(\left(\alpha_i^{(j)}, \beta_i^{(j)}\right), \left(\alpha_i^{(j)}, \beta_i^{(j)}\right), \ldots, \left(\alpha_i^{(j)}, \beta_i^{(j)}\right) \right)}^{2^{i-1}\ pairs} \qquad [3\text{-}45]$$

$$\alpha_i^{(j)} = \underbrace{\left(a_i^{(j)}, \ldots, a_i^{(j)} \right)}_{2^{n-i}\ elements}, \quad \beta_i^{(j)} = \underbrace{\left(b_i^{(j)}, \ldots, b_i^{(j)} \right)}_{2^{n-i}\ elements} \qquad [3\text{-}46]$$

Supposing that the model has N functions $f_r, r = 1,2,\ldots,N$, and N fuzzy-valued output parameters $\tilde{q}_r$ with $\mu_{\tilde{q}_r}(z_r),\ r = 1,2,\ldots,N$. The estimation of [3-42] is carried out by evaluating the expression separately at each of the columns of the arrays, using the conventional arithmetic for crisp number. Thus, if the output $\tilde{q}$ can be expressed in its decomposed and transformed form by the arrays $\tilde{Z}^{(j)}, j = 0,1,\ldots,m,$ the k th element ${}^k\tilde{z}^{(j)}$ of the array $\tilde{Z}^{(j)}$ is then given by:

$${}^k\tilde{z}^{(j)} = F\left({}^k\tilde{x}_1^{(j)}, {}^k\tilde{x}_2^{(j)}, \ldots, {}^k\tilde{x}_n^{(j)} \right) \qquad [3\text{-}47]$$

Finally, the fuzzy-valued result of the problem $\tilde{q}$ expressed by the set in [3-48]:

$$Q = \left\{ Z^{(0)}, Z^{(1)}, \ldots, Z^{(m)} \right\} \qquad [3\text{-}48]$$

can be obtained in its decomposed form:

$$\tilde{Z}^{(j)} = \left[a^{(j)}, b^{(j)} \right], \quad j = 0,1,\ldots m, \qquad [3\text{-}49]$$

by retransforming the arrays $\tilde{Z}^{(j)}$ according to the recursive formulae:

$$a^{(j)} = \min_k \left(a^{(j+1)}, {}^k\widetilde{z}^{(j)} \right)$$
$$b^{(j)} = \max_k \left(b^{(j+1)}, {}^k\widetilde{z}^{(j)} \right) \qquad [3\text{-}50]$$
$$j = 0,1,\ldots m-1,$$
$$a^{(m)} = \min_k \left({}^k\widetilde{z}^{(m)} \right) = \max_k \left({}^k\widetilde{z}^{(m)} \right) = b^{(m)} \qquad [3\text{-}51]$$

3.4.6 The possibility theory

The basis of fuzzy numbers and fuzzy arithmetic is called the possibility theory [DUB, 1985, 2001]. The possibility theory is a simple and versatile tool of uncertainty, preference and similarity modelling. It is mainly employed to handle incomplete information. This theory is similar to the probability theory because it is based on set-functions [DUB, 2003].

3.4.6.1 Possibility distribution

Let S be a frame of discernment or a set of "states of the world". Let x be an ill-known description of the current state of affairs taking its value on S. If L is the plausibility scale, a possibility distribution π_x is a mapping from S to the L; i.e. to each realization s of a variable x in a domain S is associated a $\pi_x(s)$ value, which is the degree of possibility of the proposition $x = s$. The minimum value of the possibility distribution is 0 and the maximum value is 1, such as the unit interval [DUB, 2001].

The function π_x corresponds to the status of knowledge of an agent about the actual state of affairs, differentiating what is possible from what is less possible [DUB, 2001]. The possibility value can mean, but is not limited, to the occurrence of something, the feasibility to do something, the permission to do something and the compatibility with what is known.

We adopt the following conventions:

$\pi_x(s) = 0 \quad x = s$, means that the event is impossible, totally excluded

$\pi_x(s) = 1 \quad x = s$, means that the event is completely possible, fully plausible

Possibility distributions are recognized as special cases of fuzzy sets with specific normalization. Subsequently, given the fuzzy number's characteristics, a possibility distribution can be appropriately represented by a fuzzy number. The relationships between the membership function of a fuzzy number $\widetilde{a}$ and the possibility distribution is shown as follows:

$$\mu_{\widetilde{a}}(s) = \pi_x(s), \ \forall s \in S \qquad [3\text{-}52]$$

The degree of possibility of the proposition A, being A a subset of S is given by:

$$\Pi(A) = \sup_{s \in A} \pi_x(s) \ \ \forall s \in A \qquad [3\text{-}53]$$

Possibility theory is related to the theory of probability, but is different. In the theory of probability an event A has a probability value of $p(A)$, then the probability of the opposite event of $\overline{A}$ is $p(\overline{A}) = 1 - p(A)$. This is not true in the theory of possibilities. If the possibility of A is defined as $\pi(A)$, then the possibility of the opposite event $\overline{A}$ is denoted $\pi(\overline{A}) + \pi(A) \geq 1$,

since the relationship $\sup[\pi(\overline{A})+\pi(A)]\geq 1$ is always true. In general, everything that is probable is also possible, but the affirmation is not valid in the opposite sense. Notice that the probability and possibility value do not necessarily have to be the same. Therefore, the possibility always will be greater or equal to the probability [DUB, 1985, 2001].

3.4.6.2 When is the use of the possibility theory suitable?

The possibility distributions are noted for their ability to model linguistic categories. They are related to the representation of incomplete or vague states of information, for instance in natural language ("low") [ZAD, 1978]. They can model imprecise knowledge, e.g. an approximation of a numerical value. In a broader sense, possibility distributions are advisable to represent uncertainties, to express preferences and to capture similarities.
The possibility theory is then a unifying framework to model and to combine knowledge (symbolically expressed by a human) and historical data. Note that this theory can be used as a bridge between human knowledge and the objective probability.

The possibility theory also offers the option of a qualitative solution to deal with non-probabilistic uncertainties on events. Consequently vagueness and ambiguity are represented through this theory.
Since the uncertainty is modelled by the possibility function, which at the same time is a fuzzy number, fuzzy arithmetic can be used to make calculations of distribution functions. The possibility to decompose a fuzzy number into a α-cuts allow us to calculate in a simple way possibility distributions. Therefore, possibility theory is satisfactory to represent uncertainties, with the aim of knowing its propagation in computations.

References

[COW, 1998] Cowell R., "Introduction to inference for Bayesian Networks", in Learning in Graphical Models edited by Jordan M., MIT Press, November 1998, pp. 9-25.

[DON, 1987] Dong W.M., Wong F.S.,"Fuzzy weighted averages and implementation of the extension principle", Fuzzy Sets and Systems, Vol. 21, 1987, pp. 183-189.

[DUB, 1980] Dubois D., Prade H., "Fuzzy sets and systems: theory and applications", Mathematics in Science and Engineering, Vol. 144, Academic Press, New York, 1980.

[DUB, 1985] Dubois D., Prade H., Théorie des possibilités: Application à la représentation des connaissances en informatique , Editeur Masson, Paris, 1985.

[DUB, 2001] Dubois D., Prade H., "Possibility theory, probability theory and multiple-valued logics: A clarification, Annals of Mathematics and Artificial Intelligence, Vol. 32, 2001, pp. 35-66.

[DUB, 2003] Dubois D., Prade H., "Possibility Theory and its Applications: A Retrospective and Prospective View", The IEEE International Conference on Fuzzy Systems, 2003, pp. 1-11.

[HAN, 1999] Hanss M., "On using fuzzy arithmetic to solve problems with uncertain model parameters", Proceedings Euromech 405 Colloquium, Valenciennes France, November 17-19 1999, pp. 85-92.

[HAN, 2000] Hanss M., "A nearly strict fuzzy arithmetic for solving problems with uncertainties", Proceedings 19th International Conference of the North American Fuzzy Information Processing Society, Atlanta, USA, 2000, pp. 439-443.

[HEC, 1996] Heckerman D., "A tutorial on learning Bayesian networks", Microsoft Technical Report 95-06, 1996.

[HUA, 1996] Huang C., Darwiche A., "Inference in Belief Networks: A procedural guide", Intl. Journal Approximate Reasoning, 15(3), 1996, pp.225-263.

[JEN, 1996] Jensen, F., An Introduction to Bayesian Networks, Ed. Springer-Verlag, 1st Edition, New York, USA, 1996.

[KAU, 1980] Kaufmann A., Gupta M., Introduction to fuzzy arithmetic, Van Nostrand Reinhold, New York-London, 1980.

[KIN, 2000] King, G..; Keohane R.O.., Verba S., "La ciencia en las ciencias sociales", El diseño de la investigación social, Ed Alianza, Cap. 1, Madrid, 2000, pp. 13-43.

[KLI, 1997] Klir G., "Fuzzy arithmetic with requisite constraints", Fuzzy Sets and Systems, Vol. 91, 1997, pp. 165-175.

[KLI, 2003] Klimke A., "An efficient implementation of transformation method of fuzzy arithmetic", Proceedings of 22nd International Conference of the North American of Fuzzy Information Processing Society, 24-26 July 2003, pp. 468 – 473.

[KOS, 1990] Kosko B., "Fuzziness vs. probability", International Journal of General Systems, Vol. 17, No. 1, 1990, pp. 211-240.

[LAV, 1994] Laviolette M., Seaman J.W., "The efficacy of fuzzy representations of uncertainty", IEEE Transactions on Fuzzy Systems, Vol. 2, Issue 1, February 1994, pp. 4 –15.

[McE, 2000] McEliece R., Aji S. M., 2000. The Generalized Distributive Law, IEEE Transacction on Informatic Theory, Vol. 46, No. 2, March 2000, pp. 325-343.

[MEL, 1999] Melchers, R., "Uncertainties in Reliability Assessment," Structural Reliability Analysis and Prediction, 2nd edition, John Wiley & Sons, Chichester, United Kingdom, 1999, pp. 34-45.

[MIZ, 1976] Mizumoto M., Tanaka K., "The Four Operations of Arithmetic on Fuzzy Numbers". Systems, Computers, Controls 7, No.5, 1976, pp. 73-81.

[MUR, 1998] Murphy K., "Bayes Net Toolbox for Matlab", available in: http://bnt.sourceforge.net/

[OBE, 1999] Oberkampf W.L., Helton J.C., Sentz K.,"Mathematical Representation of Uncertainty", in proceedings of AIAA Non-Deterministic Approaches Forum, Seattle, WA, paper No. 2001-1645, April 2001.

[PEA, 1986] Pearl J., "Fusion, propagation, and structuring in belief networks", Artificial Intelligence, No. 29, pp. 241-288.

[PEA, 1988] Pearl J., Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference, Morgan Kaufmann, September 1988.

[PEA, 2000] Pearl J., Bayesian Networks, in Handbook of Brain Theory and Neuronal Networks, MIT Press, November, 2000.

[SHE, 2003] Sheridan W., "Coping with ignorance in the information age, In Sensible Signage", 3rd Edition, 2003, The Thinking Person's Portal.

[TOR, 2002] Torres A., Teoría básica de la probabilidad, Procesos estocásticos - Notas de Clase, Universidad de los Andes, Colombia, Chapter 1, Colombia, 2002, pp. 2-4.

[TOR, 2004] Torres, A., Tranchita C., "Inferencia y razonamiento probabilístico o difuso", Revista de Ingenieria de la Universidad de los Andes, Vol. XIX, Bogota Colombia, ISSN : 0121 – 4993, pp. 174 – 184.

[TUN, 2003] Thunnissen D., "Uncertainty Classification for the Design and Development of Complex System", California Institute of Technology, USA, 2003.

[VEL, 1996] Velarde J., "Pensamiento Difuso, Pero No Confuso: de Aristóteles a Zadeh (y Vuelta)", Psicothema, Vol. 8, No. 2, Universidad de Oviedo, Spain, 1996, pp. 435-446.

[ZAD, 1978] Zadeh L., "Fuzzy sets as the basis for a theory of possibility", Fuzzy Sets and Systems, Vol. 1, 1978, pp. 3-28, (Reprinted in Fuzzy Sets and Systems 100, 1999, pp. 9-34).

CHAPTER IV

4. RANKING CONTINGENCIES RESULTING FROM PHYSICAL TERRORIST ATTACKS FOR SECURITY ASSESSMENT

The importance of electricity lies in the fact that is one of the main energy forms used in contemporary societies. The electrical energy delivery is a technical activity focussed on satisfying a collective necessity. This public service must be permanent because it constitutes a strategic pillar for the production and development of a country. An interruption or insufficiency of the electrical service may paralyze productive activities of a large number of organizations. This causes serious damages to the economy, the society and, depending on the concerned sectors, may affect the physical integrity of the people and even inflicts disturbances to the public order.

As we discussed in Chapter 1, the electrical infrastructure is considered a *critical infrastructure* that offers an essential service to multiple organizations (delivery of fuel, telecommunications, transport, sanitary and security services, etc.). Nevertheless, this critical infrastructure simultaneously depends on other critical infrastructures that are indispensable for their management and delivery of services. This causes a dangerous circle, as the fault propagation works in both directions, i.e., a disturbance in an infrastructure (e.g. in the electrical system) can produce disturbances in the others infrastructures (e.g. the system of communications) and vice versa. Due to the globalized nature of the world, these types of incidents can negatively affect a single country or even have serious effects on the international community.

The significance and vulnerability of the power system and its interdependency to other infrastructures has also been recognized by outlaw groups, ill-disposed people, and terrorist groups. We cannot deny that power systems (as other critical infrastructures) are exposed to serious threats. Considering that terrorism is a constant threat to societies throughout the world, the electrical network is potentially a dominant target for terrorist attacks. A frontal or indirect attack to assets can adversely affect the electrical infrastructure; by creating severe economical consequences, by raising threat to human life and finally by inducing terror to civil population [AMI, 2002].

According to Chapter 2, intentional attacks against the electrical infrastructure can entail sudden losses or inadequate operation of its components. These threats, in addition to the natural load growth and the liberalization of the electric energy market, force the systems' operators to face different and more problematic scenarios than in the past.

In order for the infrastructures' owners to be able to overcome situations related to terrorism (and other types of intentional attacks), they must improve their abilities to anticipate future events. It is therefore necessary to create possible terrorist scenarios with the aim of analyzing potential consequences to the power system. In this way, planners and operators will be able to create and to plan appropriate measures to diminish or to thwart the possible negative effects to the system, thus guaranteeing the system's secure operation. The power systems security is one of the most important design criterion and a primary objective in the

operation. Security is defined as the ability of a power system to withstand sudden disturbances [IEE, 1978].

The purpose of assessing the power system security is to establish a security margin value when disturbances occur. Once this value is known, operators make correct decisions to avoid the system's collapse. Therefore, in the power system security assessment, the occurrence of intentional attacks (that may affect the system) especially those caused by terrorism must be considered. Thus, when a terrorist act affects the power system, proper decisions can be made in order to reach an appropriate balance between operative cost and robustness.

Traditionally in security assessment studies, different system scenarios are developed. This includes several levels of load and generation, loss of components and different network topologies, among others. As we mentioned in Chapter 2, it is necessary to create a list of the possible contingencies in order to diminish the number of scenarios. Later, the impact of each contingency on the power system security is analyzed in detail. One approach is the consideration of the probability of occurrence of contingencies as a method of ranking the contingencies. The result of theses probabilities can also be used in combination with the consequence in order to obtain a risk value.

Modelling the uncertainty of the intentional acts and the contingencies resulting from these attacks is not an easy task. Because of their intentional nature, the occurrence of attacks is not random. It is therefore difficult to answer the following type of questions: What is the probability of the materialization of the terrorist threats? What is the probability that the attack is catastrophic? Answering to these questions requires thinking about the attackers' motivation, the possible utilized weapons, the infrastructures location and its physical protection, in addition to other variables that contain different uncertainty levels. According to Chapter 3, we cannot employ only the objective probability theory or purely frequencists' approaches to answer this type of questions. These approaches do not correctly model all the present types of uncertainty and the non-random causality relationships in the problem.

This chapter introduces a probabilistic technique for ranking contingency resulting from terrorist acts that could cause major risks to a power system. With the use of probabilistic inference, through a Bayesian network, the probability of attacks against the power system is obtained. In addition, we obtain the probability of severity of attacks. The network is constructed based on experts' judgment and the base load flow for the power system. This type of probabilistic graph was explained in the preceding chapter. In this Bayesian network, the nodes may represent events, proposals about events and/or uncertain variables. The connections or arcs represent causality relationships between these variables.

With the Bayesian network's results, we calculate the risk for each contingency and we rank the contingencies using this value. Therefore, a set of contingencies is found and it will be used in security analyses which will allow the diminution of the number of scenarios to be studied. Likewise, obtaining the probability of contingencies occurring will allow us to make non deterministic security analysis of the power system.

Before explaining the proposed method, we give a formal definition of term "risk" and why we use the risk index to rank contingencies. This thesis focuses on topic of terrorism as a particular study case of the intentional attacks. Next, we describe the proposed method to rank contingencies based on the real case of intentional attacks against the Colombian

electrical infrastructure. We construct a Bayesian network by taking into account the Colombian experts' judgement, author's analysis, historical database and available information of the conflict. Two numerical cases are developed to validate our method. Although we only work with this specific case, the method can be extended to other types of intentional attacks as well as to other nations.

4.1 The Risk Analysis

Because of the power systems' size and its geographical extension and the changing dynamic of the terrorist groups, it is useless and practically impossible to generate all the possible scenarios and to evaluate in detail the severity of each one. A possible solution to this problem is to use risk analysis techniques in order to find the most probable and severe cases for the power systems. Nevertheless, to assess the impact to the power systems operation means having to evaluate the security of each case. This is not a simple task because different security problems (mentioned in Chapter 2) can be analyzed and both the modelling and the solution are complex processes.

In order to find a risk value and to rank contingencies caused by attacks we suggest the use of a non-exhaustive measurement. This approach is justified because the resulting value does not necessarily represent a measure of the power systems' security.

The objective then of performing risk analyses is to create an index, which will allow us to select a certain number of contingencies among of all the possible ones. Later, each selected contingency will be analyzed in more detail in order to deeply assess the security and to establish a better measurement of its risk. We will describe this process in the following chapter.

Traditionally, risk assessment has been used to support decision making processes. This is relevant to our work, as we use risk assessment to obtain a list of contingencies, avoiding a simplistic and subjective selection by operators.

The term "risk" has diverse meanings, depending on its context. In addition, the perception of the risk can be different for each person even within the same organization. For example, the notion of risk to a power system when facing terrorist threat can be dissimilar for the system operators, maintenance engineers, planers, and also to the police or to public safety analysts. It is imperative that risk has the same meaning to experts who will participate for obtaining the risk value as well as to the decisions makers who will then use these results.

In Chapter 3, we defined risk as a measure of uncertainty. Now, we will go into the risk definition in depth (including the uncertainty modelling employed), which we use throughout the following sections and chapters.

4.1.1 Definition of risk

Risk is related to unwanted but possible occurring events. In some fields, the risk is defined by using a purely qualitative measure. Therefore, the risk is: i) *an unwanted event* which may

or may not occur[1] or; ii) *the cause of an unwanted event* which may or may not occur[2] [HAN, 2002].

However, in other fields, especially in economics and engineering, risk is used in a quantitative sense, but there are many possible definitions. The risk can be: iii) *the probability of an unwanted event* which may or may not occur. This usage is very common, and is exemplified by the following statement (not necessarily true): "The risk that the system's operation will be affected by heavy storms is about 1%".

Next, the most common definition of risk used by experts is: iv) *a numerical representation of probability of an unwanted event and some measure of its severity*. This concept of risk can also be interpreted as an *expectation value* of an unwanted event which may or may not occur. This measure is often used by risk experts, whereas non-experts use the risk to indicate the disaster potential [PER, 1999]. The use of the term "risk" in this last sense was introduced into risk analysis in the major Reactor Safety Study [RAS, 1975]. Today this usage is standard in many technical disciplines. Furthermore, some experts considered it to be the only correct handling of the term [STA, 2007].

We employ the latter risk definition in this thesis. When considering intentional attacks, the risk to a power system is a function of the probability of materialization of the existing threats (attack probability and the probability of loosing or erroneously performing components) and the severity level to the system.

In order to assess the risk, the occurrence of unwanted events is represented by means of an uncertainty model, i.e., by the subjective or objective theory of probability. Once an event has taken place, we must model its severity. However, the severity can also be a non-deterministic value and we can integrate a type of uncertainty modelling. For example, the economic consequence of an attack is better represented by an interval (between x and y euros) than by a crisp value (x euros). The risk is then determined by the multiplication of these two quantities[3]:

$$\text{Risk} = \text{Probability of ocurrence} \times \text{Severity}$$

Within this single definition, there are also many different types of risk. These risks are determined by the way in which the probability has been modelled (subjective or objective) and by severity measure employed; however the latter is the most important aspect. When assessing severity, it is common to utilize the repair cost value of the damage to the infrastructure. In this case, we are concerned about the economical risk, while the other measures of severity give rise to other types of risk. Technical risk in power systems is traditionally a measure of the proportion in which the system fulfils reliability and security standards under perturbed conditions or in a normal state.

1 An example of this usage is: "The instability voltage is one of the major risks that affect the power system's operation".
2 For example: "Heavy storms are by far the most common operating risk to a power system within a specific country".
3 If the severity is not a crisp value, the arithmetic used in the multiplication must be in agreement with the uncertainty theory that is employed.

4.1.2 Severity evaluation

We suggest and describe variables that can be employed in order to evaluate the severity of possible intentional attacks that may affect the power system. In our work, however, we only refer to the technical and to the economical risks.

1. Technical severity: As mentioned above, the technical consequence is mostly evaluated in terms of the power system's operating parameters, in addition to its adequacy and security (reliability) margins. A disturbance is considered severe if it causes the system to change from a normal to an emergency operating state or if it causes the system to collapse. A possible measure of severity is the ratio between the value of the parameter of study that has been reached (voltage, frequency, power flow, etc.) and the possible maximum value. This measure is exemplified by the transmission lines' power flow and its overload limit. Severity is high if the flow value exceeds or is very close to the limit value; conversely, it is low or non-existent if it is far away from the security limit.
   Also technical severity can be measured by the number of affected components and the relevance of these components in the system.

2. Physical security (public safety): The possibility that the occurrence of events can injure or kill a person or a group of people must be evaluated. This type of impact is usually difficult to assess and its importance depends completely on the utility's policies. Generally, this impact measure is subjective. At this point, risk analyzers determine if the attack on certain components would affect the utility staff, the people near to the infrastructure or the network end users.

3. Impact on the image: Here we consider the negative impact that a terrorist attack could have on the image of the electrical sector. The risk analyzer is concerned with the impact of this image on society. Because a close relationship between the electrical sector and the government exists, if the electrical infrastructure is attacked the government's existing image can be affected. This element must be taken into consideration when analyzing this particular impact.
   In addition, the social impact of a terrorist attack on a power system is dependent upon whether or not society (including the clients) is aware of the attack and of its possible consequences. Furthermore, the risk analyzer must consider if contracts have not been fulfilled when assessing the impact on the image.

4. Environmental severity: At this point, the environmental (flora and fauna) consequences of attacks are considered. Many cases of public health are also affected. For example, in the case of an attack against a power generating nuclear station, we must take into account the consequences of radiation or nuclear proliferation.
   Violations of environmental laws and regulations can be also included.
   Attacks which have environmental impacts are of particular interest because they normally put the health and the physical well-being of people in danger and entail long-term economic effects. An extreme case of this kind was the Chernobyl tragedy in 1986.

Most of the abovementioned aspects can also be evaluated in economic terms. A technical problem can be measured by the subsequent loss of the utility's income. Another example is

the measurement of public safety in term of possible compensations for death or injury (e.g. permanent or temporary disability).

5. Economic severity is related to the amount of money that an electrical utility loses or has to pay due to power system faults resulting from an attack.
   We suggest taking the following categories into account:
   - Economic costs due to physical damages of the system: We evaluate the cost of replacing or repairing equipment or a system (labour + physical components). It is necessary to include damages to other infrastructures' equipment including the interconnected power systems.
   - Economic costs due to non availability of service: Here, several aspects can be included: i) penalties linked to regulations regarding the quality of service indices; ii) the loss of income caused by power outages and; iii) the loss of end users' income due to the lack of electricity. The following factors have to be considered: the duration of the interruption, the number of affected users, the non served load and the geographical extension of the fault.

4.2 A Method of Contingency Ranking [TRA, 2006a , 2006b]

Our objective is to obtain a group of probable contingencies, which will be analyzed later in order to find a measure of the power system's security. Contingencies are caused by terrorist activity in a specific place.

In the following sections we will explain the three main parts of our method: the selection of the system model, the construction of a Bayesian network to obtain the probabilities that will allow us to evaluate the risk and finally the contingency ranking obtained via the indices of risk.

4.2.1 System modelling, configuration selection and operating conditions

As in any other security study of a power system, before beginning the analysis process, operators or planners must define which grid, or which part of the grid will be considered. In our case this power grid must correspond to the assets installed in the geographical area where evidence or suspicions suggest an exposition to the risk of terrorist activity.

Credible network topologies and the system's operating conditions must be chosen on the basis of experience and the purpose of the study. This includes the transmission lines and the generators in service as well as the level of the load, i.e. whether the study is carried out based on the peak load, the average load, the partial peak load, etc. All these factors also depend on the season of the year in which the analysis will be completed.

Operators could eventually base their selection of the system topology on historical data. They may notice if there is a certain correlation between the times (hours) or dates of the attacks and the occurrence of the attacks. We reiterate that given the dynamic nature of the terrorist groups' activity, these approaches are usually very difficult to establish.

We have to choose the power transmission system model with the details that are required. A balance between the exactitude of the modelled system and the complexity of the model has to be guaranteed. Although very detailed models may represent the real system behaviour more accurately, they are not necessarily the best option due to the time required

and the complexity of the solution (which in some cases cannot be produced using the mathematical tools available). In this thesis we will perform only steady-state security studies. Therefore we have chosen the load flow model.

4.2.2 Implementation of the Bayesian network

In the previous Chapter we described the Bayesian Network and its mathematical basis. In this section we will describe details of the use of Bayesian networks as a tool to evaluate risks.

4.2.2.1 How can we use a Bayesian network to assess risk resulting from terrorist attacks?

The major problem in dealing with intentional assaults is that they are not random events which occur by chance. Attacks are normally planned some time in advance and the time and place of attack are chosen in order to have the desired impact. The inherent uncertainty of a terrorist attack is high and dynamic. The terrorist group can adapt its behaviour and strategies according to its financial resources and knowledge of the vulnerabilities of potential targets.

The uncertainty of terrorism is comprised of the elements of randomness, ambiguity and vagueness and is mainly due to a lack of knowledge. It is not possible to briefly define the truth or falsity of a statement. Therefore, a deterministic approach may not be the best solution since all uncertainties are neglected and a "frequentist" approach of the probability may lead to erroneous models of the uncertainties present in the study. Moreover, even if we would like to use traditional statistical tools, it is not actually possible to do, because no robust wide database is available. In fact, grouping all terrorist acts into the same category is inadequate, given the changing nature of the motivation and the variables influencing terrorist acts.

Terror is used as a strategic resource (in most cases explosive devices are used) in order to achieve political (or sometimes religious) goals by putting security to the test and at the same time to spread a constant feeling of threat throughout many communities. There are social, economical, political, religious and geographical factors which will lead to a prediction based on the probability of attacks taking place. The economic strength of a terrorist group, the policies of counter-terrorism of a zone or a country, the measures adopted by public and civil forces, the foreign policies and the dependency of a zone on a critical infrastructure are only a few of the examples of variables which can influence a terrorist's decision regarding the significance of any potential attack as well as the time at which it will take place. Techniques such as the probabilistic inference have turned out to be useful in representing the causality between variables and in calculating the probability of events when different types of uncertainties are exhibited.

By taking into consideration social, economical, technical, political, religious, and geographical variables, relating to the case of terrorism in a country, we use a Bayesian network in order to *infer* both the probability that an attack against a power system component occurs and the probability of the severity of this attack.

Bayesian networks are a framework for uncertainty and risk analysis. The observable quantities or variables express states of the world and quantities of physical reality or nature.

These variables are unknown when utility' operators carry out a security analysis, but in an actual situation, they can take a value, thus becoming known.
We can interpret Bayesian networks as reflections of the real world which include a representation of relationships between variables. Our aim is to predict the value of a set of observable variables $\mathbf{Y}=(Y_1,Y_2,\ldots,Y_n)$ by expressing the knowledge of $\mathbf{Y}$ in terms of a specific group of variables $\mathbf{X}=(X_1,X_2,\ldots,X_m)$ and the causal relationships between $\mathbf{Y}$ and $\mathbf{X}$ [4].

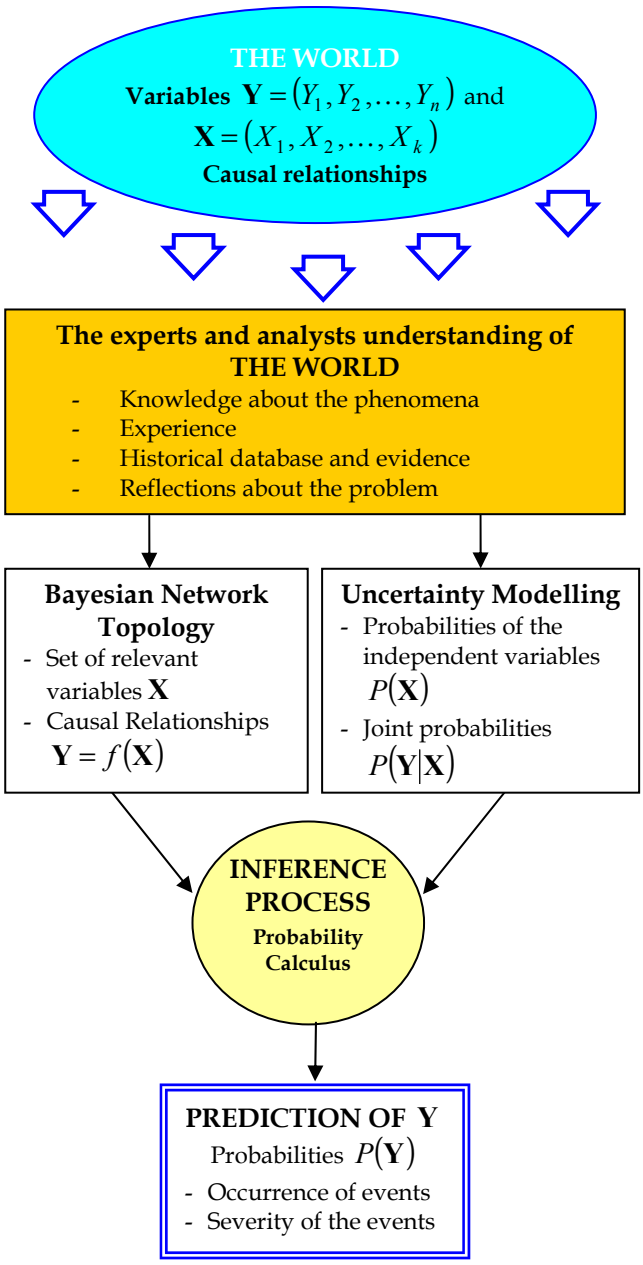


Figure 4-1. Uncertainty modelling by using Bayesian Networks in order to assess the risk.

4 Notice that in the classical models of risk assessment, the relationships between the variables (without representation of uncertainty) $\mathbf{Y}$ and $\mathbf{X}$ are always represented by means of deterministic relationships. i.e., $\mathbf{Y}$ is a mathematical function of the independent variables $\mathbf{X}$. If the variables' uncertainty $\mathbf{X}$ is modelled by the use of probability, the results, i.e. the functions of probability of $\mathbf{Y}$ could be found by using the analytical approximation or by Monte Carlo simulations.

Figure 4-1 shows in a simple way how we can use a Bayesian network in order to obtain the probability which is necessary to evaluate the risk.

4.2.2.2 Identification of goals of modelling

We apply Bayesian networks because it is necessary to define which elements of the power system are at risk from terrorist attacks, as well as the degree of intensity of these attacks, in order to determine the corresponding impact on the power system.

We must then infer the probabilities of:
- The occurrence of an attack against a super-component of the power system
- The severity of an attack on the power system

With the aim of inferring the probabilities defined above, we are going to build a Bayesian network, starting from the definitions and the hypothesis about events and variables.

4.2.2.3 Definitions

Some definitions of terms that will be used from here on:

- Event: An Ei event is a fact or phenomenon of uncertain occurrence that adversely affects a system's super-component and therefore the power system performance [TRA, 2004].

- NonNatural-Intentional Event: An ENN-Ii event is an event that occurs due to human intervention. The attackers' objective is to damage the power system. Examples of these events are terrorist attacks, military acts and, cyberattacks. However, in this chapter only physical terrorist attacks are addressed [TRA, 2004].

- Super-component: principal power system components that completely define the system. These super-components (SC) are also composed of components. They are defined in Table 4-I [TRA, 2004].

TABLE 4-I. DEFINITION OF SUPER-COMPONENTS

GENERATING PLANTS		Generator type
		Hydro-electrical
		Thermal
		Nuclear
SUBSTATIONS	**Substation Type**	**Configuration type**
	Encapsulated	Encapsulated double bus
	Conventional	Single bus
		Main bus and Transfer
		Double bus
		Ring bus
		Breaker-and-a-half
TRANSMISSION LINES		

- Attack probability: In our Bayesian network, the probability of an attack refers to the probability that a particular super-component is subjected to a nonnatural-intentional event, (e.g. the *x* generating plant of a power system has a 40% probability of being attacked and not a 60% probability); this means that, it is not intended to determine or to

project rate of attacks over a specific period of time for each of them (e.g. average number of attacks on a given super-component by unit of time).

4.2.2.4 Hypothesis

The following hypotheses are used in this thesis to construct the Bayesian network.

1. Each variable or node takes values from a collection of *mutually exclusive* states at every instant of time. The events A_1, A_2, ..., A_n are said to be mutually exclusive if the occurrence of any one of them automatically implies the non-occurrence of the remaining n−1 events. This property is illustrated by Figure 4-2 (a).

   One of the most important variables that we need to predict is the occurrence of an attack (which is necessary to measure the risk). This property means that an attack against one super-component excludes the possibility of an attack against another super-component at the same moment. Just one super-component of the power system can be attacked at one moment in time. We consider that terrorist attacks always occur at different moments in time. Even if attacks occur simultaneously, our approach is to model them with infinitesimally short lapses between each other.

2. Each variable or node takes values from a group of collectively exhaustive state, i.e. with the property that at least one must happen. This property is illustrated by Figure 4-2 (b).

If a set of events is collectively exhaustive and mutually exclusive, the sum of the probabilities of all events is equal to 1. The hypotheses are shown in Figure 4-3.

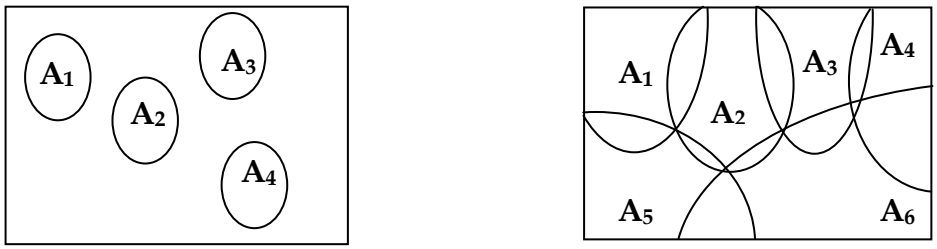


Figure 4-2. (a) Mutually exclusive events; (b) Collectively exhaustive events.

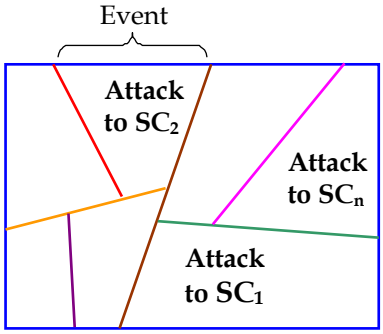


Figure 4-3. Sample space used to identify which super-component of the power system is attacked. Events are both mutually exclusive and collectively exhaustive.

3. The occurrence of a terrorist attack (non-natural events) is independent of the number of terrorist attacks that occur over a specific period of time.

4.2.2.5 Information sources

In compliance with the aforementioned characteristics of terrorism, we will be able to implement our Bayesian network using real life social and political factors in Colombia. We insist that this methodology is also relevant to other places, but depending on the case, conditional probabilities can change or new variables can be included.

Armed conflict in Colombia has affected the main industrial activities of the country. The transmission of electrical energy has been attacked numerous times by narco-guerrilla groups and the assets of the electrical sector have frequently become a prime target. During the last seven years (1999 - 2006) 2,362 attacks on electrical power towers have occurred. Acts against substations and generator stations have been fewer in relation to those on electrical towers, as the security mechanisms implemented by public forces and the companies involved have succeeded in limiting the number of attacks on theses places. In Appendix A, there is further information concerning the Colombian case mentioned above.

There are many variables involved in the decision of whether to attack or not to attack an electrical infrastructure. Furthermore, the information about these variables is also plentiful, as the experts' judgments, historical data, models and simulations results must all be considered.

An expert's judgement is defined as a recognized and authorized opinion, and is based on information and evidence as much as it is on the experience of the expert in a given subject.

In this study, for the construction of the Bayesian network we used the judgements of terrorism experts, and/or the experiences of power system operators always in combination with the evidence. The case of terrorism was revised in detail. We include the most important aspects in Chapter 1 and in Appendix A, allowing the reader to understand the results of our reflections and findings.

The sources of information are as follows:

- Evidence of the terrorist attacks occurred in Colombia between 1999 and 2006 against the electrical infrastructure (described in Chapter 1 and Appendix A)
- Evidence of the terrorist attacks occurred throughout the world between 1994 and 2006 (described in Chapter 1 and Appendix A)
- Information about the problem of terrorism published in books (Chapter 1 references)
- Authors' reflections about terrorism (Illustrated in Chapter 1).
- Authors' experience about the power system operation.
- Power flow simulations
- Interviews of terrorism sociologists
- Interviews of Colombian system operators
- Previous works [TOR, 2005].

4.2.2.6 What are the relevant variables and the relationship between them?

The idea in this section is to determine which variables are relevant to the goals that we want to achieve, and to establish causal relationships between variables (represented in the Bayesian network by arrows).

In order to achieve the goals of modelling (section 4.2.2.2), we considered the experts' knowledge on terrorism in Colombia, the experiences of Colombian power system operators and the information resulting from technical studies of power systems. We also analyzed the evidence of the attack, i.e. the information about terrorist attacks on Colombian electrical infrastructure (without necessarily establishing statistical indices). After analyzing this information, we determined the most important variables of the model are:

- The motivation to attack
- The vulnerability (accessibility and visibility) of the super-component
- Intensity of the attack on the super-component
- The consequence or severity for the power system because of the unavailability of the super-component (resulting from the attack)

A. Motivation to attack

The first element analyzed is the motivation of the terrorist attack. The most critical variables that influence this motivation, which have been identified by experts and by authors are explained as follows.

- *Political situation:*

  Terrorism is an intrinsically political phenomenon. Every terrorist organization has its own reasons and particular circumstances which lead it to the decision to use violence in order to accomplish its political objectives. Religious and ethnic differences, and left-wing and right-wing ideologies, or a mixture of these factors, have been sources of previous terrorist acts [LUT, 2004]. By attacking the electrical infrastructure, terrorist groups have the possibility to change the socioeconomic dynamics of a country, to obtain legitimacy by generating political discussions and interests, and to press the government with their demands.

  The motivation behind a terrorist group's attack can vary considerably. Examples of this variation may result from the behaviour of a government, the discourse of a main religious or political representative, or from economic globalization policies that can be disadvantageous for certain groups or countries.
  Within the Bayesian network, this variable reflects the influence of the current political facts that affect civil order and the level of governability in a country or in a certain region.

  The possible states which can be used to define this variable are: critical, moderately critical, and non-critical situation. The subjective probabilities are obtained by a group that consists of politicians and sociology experts, so that the historical correlation of terrorist attacks against critical infrastructure in periods of political strain is considered.

Political Situation		
critical	moderately critical	non-critical

- *Position of the terrorist group*

The position of the terrorist group in a given country is qualified and understood by the degree of social and territorial control possessed by these groups. This variable also represents the vitality and financial power of the group. The resources of a terrorist organization, principally money and manpower, are very important to determine what weapons are used by the group, and what their targets are. The financial situation of a group enables them to have the logistic, materials, and other elements which are necessary to commit terrorist acts; therefore, a powerful group can plan sophisticated and effective attacks.

Thus, the activity of a terrorist group shows the capacity and financial structure of a group. Some terrorist groups are solely financed by foreign countries, others by foreign countries supplemented by other revenues such as crimes (e.g. drug trafficking, kidnappings, and extortions), while others are solely financed by preceding crimes. The above crimes also play a secondary role in intimidating society. Moreover, terrorist groups may dedicate themselves to large scale contraband, several types of fraud (through institutions of charity or credit cards), robberies and thefts.

The variable states of the position of a terrorist group are:

Position/Activity of Terrorist Group		
High presence/activity	average presence/activity	low presence/activity

- *Criticality for the power system*

This variable refers to how critical the forced unavailability of a given super-component is for the functionality of the power system. In this thesis, our approach is to create an order of importance founded on the base power flow in order to obtain the probability values. However, system operators of the local or regional control centres can assign these values based on their knowledge of the power system performance as well as on the evidence of incidents that occurred in their power grid and in others electricity utilities. For this estimation, the cause of the event is not important. In most of utilities there is already this categorization (used in reliability studies).

The criticality for a power system given the forced unavailability of the super-component can be:

Criticality for Power System		
highly critical	averagely critical	lowly critical

The relationships between the motivation of an attack and the variables discussed above that influence this motivation are illustrated in Figure 4-4.
The possible states used to define the motivation of attack are:

Motivation of the attack		
high	medium	low

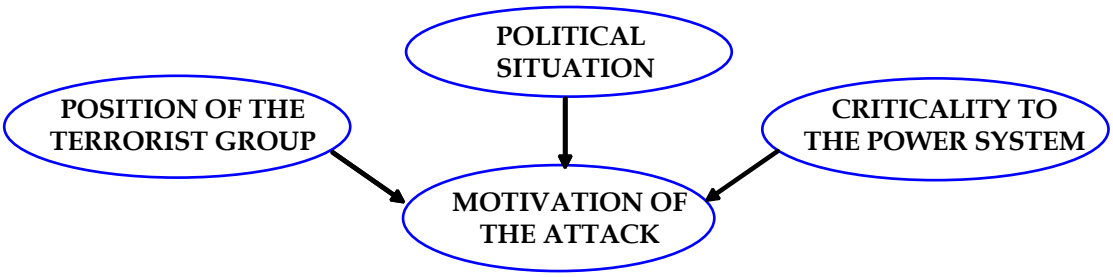


Figure 4-4. Relevant variables influencing the attack motivation.

B. Vulnerability of the target: accessibility and visibility

The second element analyzed is the accessibility and the visibility of the target. We consider this variable to be important, as although a terrorist group may have a great motivation to attack, the execution of the assault largely depends on how accessible the target is. The most critical variables that experts have identified are explained as follows.

- *Geographical location*

  This variable refers to the vulnerability of the assets due to their geographic location. One of the reasons as to why certain assets of the power systems are vulnerable is because their locations are aloof.

  In the Colombian case, this factor has enabled the terrorists to place explosive devices in the electrical towers and to make attacks on generator plants and substations[5]. The geography of Colombia includes many areas with a high vegetation density and which have little road access making locations become prime targets for attack. The inaccessibility facilitates the outlaw groups' activity and further obstructs the speedy defence of these targets by the national armed forces[6].

  Probabilities of this variable are determined by government and national security experts. The possible states are:

Geographical situation		
high exposure	average exposure	low exposure

- *Physical protection of assets*

  Because the power system's assets are located in large areas, it is impossible to protect all of the assets. Nevertheless, some assets are more protected than others, depending on their importance to the power system's behaviour as well as on the possible consequences (economic, environmental, etc.) resulting from external or internal events

[5] Terrorist groups not only plant explosive devices in electrical towers but they also plant landmine explosives, causing further harm and even death to the maintenance staff who repair these towers after the attack. It is therefore necessary for the Colombian army to accompany staff when they make these repairs.

[6] In Colombia this situation is also a result of the guerrillas' ability to take advantage of the lack of state presence in rural zones.

(which affect the component). For example, nuclear generating plants have high security and safety systems because of the serious consequences of nuclear radiation.

In this variable we can also consider that assets located in inhabitable zones are more vulnerable than those in populated areas, as their visibility is in itself a mechanism of protection.

Therefore, this variable refers to the means of protection possessed by a super-component, most often in the case of generating plants and substations. Probabilities of this variable can be calculated taking into consideration whether or not generating plants and substations have the following protections:

- Lights
- Special locks
- Fences
- Solid walls
- Motion detection systems
- Video camera surveillance equipment, building security systems.
- Alarm systems
- Electronic protections
- Security guards

It is not common practice to protect transmission lines, but we must not forget that in the case of insurgent attacks against the Iraqi electrical infrastructure, the government of this Country made two unsuccessful attempts to protect the lines through the employment of security guards. In the first attempt, security guards were trained and equipped with weapons; in the second attempt, tribes living close to the transmission lines were hired to protect the nearby towers. These plans failed principally because of the inability of the protectors to guard all of the towers, the corruption of the protectors and also because of the potential of the terrorist groups to extend their terror to include the guards and their families. In Appendix A further this case is further explained.

The protection of a super-component can be:

Physical Protection of Assets		
high protection	average protection	low protection

Based on the IEEE and CIGRE survey concerning the effectiveness of each type of security system used to protect substations, we propose a physical protection index for each security measure in order to assign these probabilities.

Table 4-II shows the possible types of protection that can be implemented for rural substations, the index suggested in this thesis for each measure and the categorization of the probabilities given the value obtained. In the same manner Table 4-III and Table 4-IV show the values for suburban and urban substations.

Another option to obtain an approximate value of the marginal probability is by calculating the ratio between the sum of indices of all the physical forms of protection that the utility has and the possible maximum value of protection (i.e. when all measures are implemented).

TABLE 4-II. POSSIBLE PROTECTIONS FOR RURAL SUBSTATIONS

Physical security system RURAL Substations	Responses	Not effective (%)	Somewhat effective to effective (%)	Very effective to completely effective (%)	Physical security index
Security guard	4	25	50	25	1
Lights	31	13	74	13	1
Signs	22	11	77	12	1
Optical alarms	5	0	100	0	2
Manned station	3	0	100	0	2
Special equipment	3	0	100	0	2
Solid wall	1	0	100	0	2
Special locks	17	6	65	29	2
Video camera	3	0	66	34	3
Fence	5	0	60	40	3
Passive and microwave systems	4	0	0	100	3
Alarm system	2	0	0	100	3
Door alarm to SCADA	1	0	0	100	3
Motion detectors	1	0	0	100	3
Electronic protection	1	0	0	100	3
			Possible Maximum Value		**34**

Level of protection	High	Average	Low
	1 - 11	**12-22**	**23-34**

TABLE 4-III. POSSIBLE PROTECTIONS FOR SUBURBAN SUBSTATIONS

Physical security system SUBURBAN Substations	Responses	Not effective (%)	Somewhat effective to effective (%)	Very effective to completely effective (%)	Physical security index
Security guard	6	0	100	0	1
Lights	31	6	78	16	1
Signs	27	11	81	8	1
Optical alarms	4	0	100	0	1
Manned station	4	0	100	0	1
Special equipment	3	0	67	33	2
Solid wall	4	0	75	50	2
Special locks	19	5	69	26	1
Video camera	3	0	100	0	1
Fence	5	0	60	40	2
Alarm system	2	0	0	100	3
Door alarm to SCADA	2	0	0	100	3
Motion detectors	1	0	0	100	3
Electronic protection	2	0	0	100	3
			Possible Maximum Value		**25**

Level of protection	High	Average	Low
	1 - 8	**9 - 16**	**17-25**

TABLE 4-IV. POSSIBLE PROTECTIONS FOR URBAN SUBSTATIONS

Physical security system URBAN Substations	Responses	Not effective (%)	Somewhat effective to effective (%)	Very effective to completely effective (%)	Physical security index
Security guard	5	0	60	40	2
Lights	31	7	77	16	1
Signs	27	7	78	15	1
Optical alarms	4	0	75	25	2
Manned station	4	0	100	0	1
Special equipment	3	0	67	33	2
Solid wall	7	0	57	43	1
Special locks	18	1	66	33	2
Video camera	3	0	100	0	1
Fence	4	0	75	25	2
Alarm system	2	0	0	100	3
Door alarm to SCADA	2	0	0	50	2
Motion detectors	1	0	0	100	3
Electronic protection	1	0	0	100	3
			Possible Maximum Value		**26**

Level of protection	**High**	**Average**	**Low**
	1 - 8	**9 - 17**	**18-26**

The relationships between the vulnerability of the assets and the variables explained above are shown in Figure 4-5.

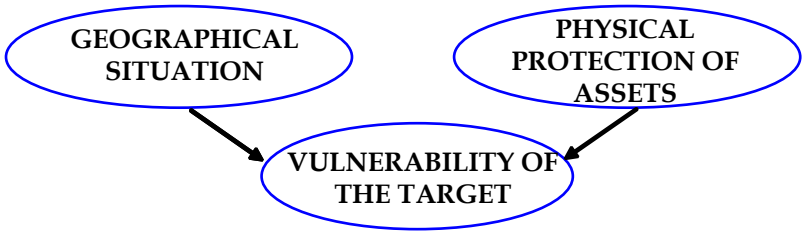


Figure 4-5. Relevant variables which influence the vulnerability of the targets.

And the possible states defined for the vulnerability of the target are:

Accessibility / visibility		
high	medium	low

C. Intensity of the attack on the super-component

The third element analyzed is the intensity of the attack on the super-component, which is understood as the quantitative estimation of the degree of activity, the power and/or force that can be employed in the attack's execution on the super-component. In the Bayesian network, this variable shows the probability that a terrorist group uses a certain quantity of resources, i.e. the quantity and the type of explosives and the number of people employed for the attack against the super-component.
This variable depends on the motivation of the attack and the vulnerability of the target. Here, we also include a new variable that represents the type of super-component. However, these last three variables are not the only variables that may influence the intensity of the

attack. For example, a new node can be included in the Bayesian network in order to represent the probability that a terrorist group uses a certain type of weapon. This probability can be specified by a Country's security information service. However, we limit the representation of the intensity by the three aforementioned variables because of our limited knowledge of the topic and the difficulty of establishing conditional probabilities.

- *Type of super-component*

  Here we differentiate the assets of Table 4-I in our Bayesian network. Because there is no uncertainty in this variable, as there is always either a generator, substation or transmission line, the probabilities take a value of 0 or of 1. We suggest especially in the case of having different types of generators, i.e. nuclear plants, thermal plants, etc., to divide this variable into more states so that each type of generator can be distinguished from one another.

Type of super-component		
generator	substation	transmission line

Therefore, the relationships between the causes and the intensity of the attack on the super-component are illustrated in Figure 4-6:

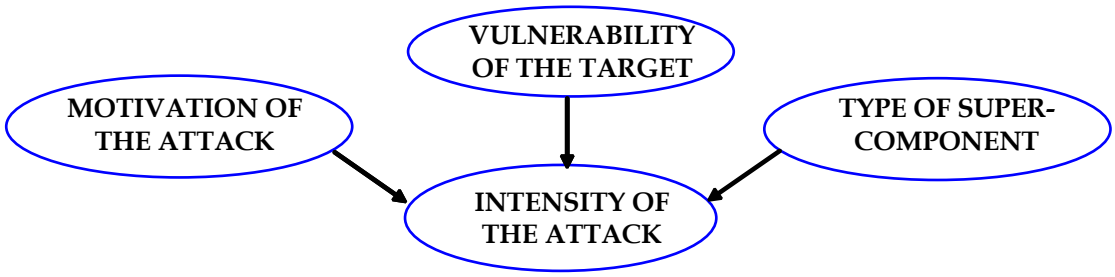


Figure 4-6. Relevant variables which influence the intensity of the attack on the super-component.

For each super-component the probability will be calculated in terms of high, average or low intensity of the attack or non-occurrence of the attack.

Intensity of the attack			
high intensity	average intensity	low intensity	no attack

In the Colombian case, an attack with a low intensity is an attack without a lot of force in relation to the man deployment and where the type of explosives used were, for example, gas cylinders. This kind of scenario suggests that the objective of terrorists is more to harass than to destroy the infrastructure.

Note that because we define the variable's states in this way, the probability that the attack has a high, medium or low intensity implies that the attack took place. Consequently, in this node, the marginal probability that the attack will occur is found by adding the probabilities as follows:

$$\Pr(Attack) = \Pr(high\ intensity) + \Pr(average\ intensity) + \Pr(low\ intensity) \qquad [4\text{-}1]$$

Or by using the equation [4-2]:

$$\Pr(Attack) = 1 - \Pr(No - Attack) \qquad [4\text{-}2]$$

The probabilities inferred in this node are important because they can be used by utilities as a measurement of risk (as was mentioned earlier in this chapter). This is not our approach, but the electrical utilities or other governmental entities can use these results in future planning or operation studies.

D. Consequence of the attack

Based on the purpose of the risk study, it is necessary to establish the variables needed to measure the severity. If the study is technical, a variable to measuring the severity can be the number of affected components. If the study is economic, for example it must be considered not only the loss of the components but also the loss of the supply of electricity. This point was explained in section 4.1.2., and authors suggested some possible variables.

In our network, the consequence or severity of the attack on a super-component is directly inferred from the intensity of the attack and from the type of super-component. Though the consequence and the intensity of the attack are directly related in most cases; these quantities can have no proportional relation. An attack of low intensity against a super-component can only affect a simple component but if it is critical for the super-component, the consequence can be significant. Moreover, this relation depends also on the design specifications of the components and whether the probability of the attack overcomes these parameters or not.

For example, a nuclear plant is composed of several buildings that do not have the same vulnerability. The core of a nuclear plant has over 100 tones of radioactive material at extra-high temperature and the safety systems include mainly cooling systems [CHO, 2001]. The fence of the reactor building is made up of one or two walls in pre-stressed concrete which are almost one meter thick (these walls act as barriers and radiological shields). The probability that an external physical attack against the reactor building has a catastrophic consequence (for us, an ionising radiation) is extremely low thanks to the inherent strength of containment and radioactivity removal capabilities of containment and systems design. Specifically, walls can resist very strong impacts and explosives, and also operator action plans and safety systems are prepared in order to mitigate accident propagation. In the specific case of aircraft crashes the consequence depends on the size, the speed and the angle of the aircraft. However it is known that most of reactors constructed before twenty years can support the impact of the small aircrafts [POS, 2004]. Supposing that a core damage occurs because of a terrorist attack occurring, the consequences to the plant's structure can be serious. The effects on public's health or the environment are not likely to be severe. This last is due to the fact that a core damage tends to occur over a longer period, which allows emergency response measures to be taken. However, the probability of the destruction of certain indispensable elements for the functioning of the plant can also lead to important economic consequences (without being the worst case). Therefore, the severity assessment in this case can be measured by the radiological consequence or by the economic damage.

A possible quantification of the severity suggested in this thesis is the use of the number of components or the percentage of the components affected by the attack. A second possibility is to rank the components depending on their importance and to quantify the severity based on the type of the component affected. Which type of components enters in this rule and

which ones are exceptions should be defined. In order to show these approaches a very simple suggestion for generating plants is presented in Table 4-V.

TABLE 4-V . SEVERITY OF THE ATTACKS ON GENERATING PLANTS

TYPE OF SUPER-COMPONENT		ATTACK SEVERITY			
		LOW	MEDIUM	HIGH	CATASTROP.
Generating plants	Hydro electrical	N-1 Components	N-2 Components	N-3 Components	N-n Components n>3
	Thermal	<=20% Components	>20% and <=50% Components	>50% and <=80% Components	>80% Components
	Nuclear	Damage to the external physical protection of the plant's place.	Damage to the redundancy systems, such as secondary power supplies. Damage to the control's building.	Partial loss of the cooling circuit Damage to turbines. Damage to the control system. Damage to the critical safety components.	Damage to the entire reactor's building. Damage to the reactor's core Total loss of the principal cooling circuit.

For the substations, the relationship between the intensity of the attack and its consequence depends mainly on the substation's configuration, the reliability and the area extension. This last parameter is very important because of the concentration of assets. If the concentration is high, the probability that a single attack entails to have more unavailable components is higher than when the concentration of assets is low. Again, here we can include more nodes into the Bayesian network in order to take these aspects into account. Table 4-VI is given as a guide to calculate the conditional probabilities. In this table, the area and reliability indices are suggested.

TABLE 4-VI. PARAMETERS TO CALCULATE THE SEVERITY OF THE ATTACKS ON SUBSTATIONS [MCD, 2003]

Substation	Single failure	Reliability Index	Area	Area Index	Price (p.u)
Single bus	Can cause complete outage	1	Very Low	1	1
Main bus and Transfer	Can cause complete outage	2	Low	2	1.76
Ring bus	Isolates single component	3	Moderate	3	1.56
Double bus	Isolates single component	4	Large	4	1.8
Breaker-and-a-half	Bus: no affectation of circuits Circuit: isolates single circuit	5	Large	4	1.57

Once more, we can use the percentage of the components affected in order to establish the severity of the attack as follows.

ATTACK SEVERITY			
LOW	MEDIUM	HIGH	CATASTROP.
<=20% Components	>20% and <=50% Components	>50% and <=80% Components	>80% Components

Note that, in order to determine the severity of the attack, other variables (suggested by the authors in section 4.1.2.) can be considered and added to the Bayesian network.

4.2.2.7 Obtaining the Bayesian network

The total implemented network is shown in Figure 4-7.

Once the network is built, the priori conditional probabilities must be evaluated by experts. We will show these evaluations in the next section. Various information can be obtained from the network; however, the most relevant information is used in order to achieve our goal: to find the set of most the important contingencies that will be used in the security study (one contingency is a successful attack against one system super-component). Thus, the probability of the severity of the attack is obtained by using the Bayesian network of the Figure 4-7.

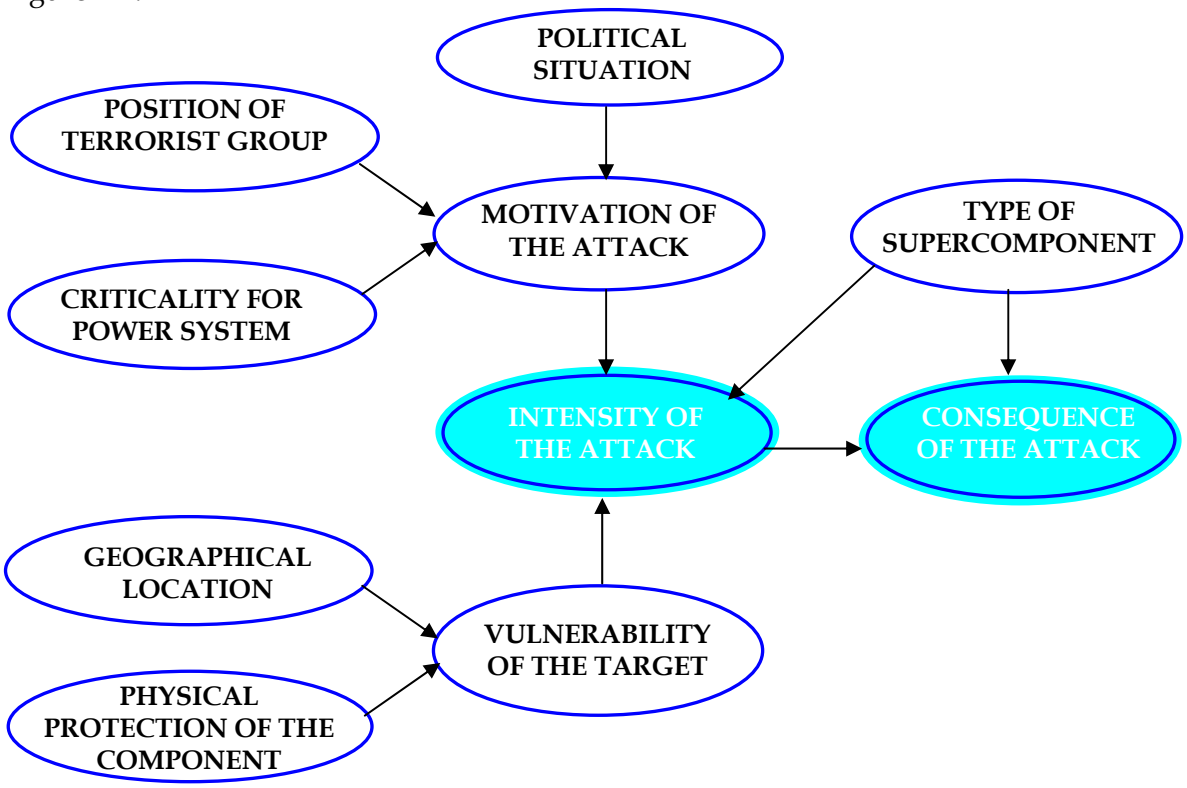


Figure 4-7. Bayesian Network constructed to determine the intensity of an attack and its consequence to the electrical infrastructure.

4.2.3 Contingency ranking

Through the use of the Bayesian network we obtain the necessary elements to calculate measurements of risk. The values obtained are all probabilities. For example we can use the single value of probability of attack or the probability of severity as a measurement. However, the definition of risk adopted in this thesis is the probability of occurrence multiplied by the impact or the severity of the event. Because we only have the probabilities, a method of calculating the risk is suggested as follows.

4.2.3.1 Calculating the risk

The definition of risk has two elements: the probability and the consequence. The results of the Bayesian network show the probability of an attack against the *i*-th super-component of the power system and the probability that the severity is catastrophic, high, average or low.

The probabilities of severity obtained for Bayesian networks include the fact that the attack was produced (without importance of the intensity of the attack). If there is no attack, there is no severity. Internally, the conditional probabilities of severity given the occurrence of an attack were taken into consideration. For that reason, we only use the probabilities of severity in order to obtain the risk value.

With the aim of calculating the second element of the formula of risk, one weight is assigned to every single probability of severity and to every single super-component. This weight can be understood as the cost produced by the attack. These values must be coherent with the risk measurement chosen (section 4.2.2.6), e.g. if the definition of a catastrophic severity for a specific substation is the destruction of the control building, the weight assigned to the probability that the severity is catastrophic, is the replacement value for this building.

In our approach, the weights are the repair cost (in some cases this may be the replacement cost) to each super-component depending on the definition of the severity. In this thesis, the weights are chosen according to the number or the percentage of components affected. The risk value is then, the sum of the products of the probability by the weight.

$$Riskc_i = W_{1,i}\ \Pr(Sev_i catas) + W_{2,i}\left(\Pr Sev_i high\right) + W_{3,i}\ \Pr(Sev_i medium) + W_{4,i}\ \Pr(Sev_i low)$$
$$i = 1,2,3,\ldots,q \qquad [4\text{-}3]$$

This risk is calculated for q super-components. W_i are the weights (or costs) aforementioned and $\Pr(Sev_i catast)$ is the probability that the severity of the attack against the i-th super-component is catastrophic. For other probabilities of severity, the formula applies in the same way.

In addition, we divided the value of risk by the maximum repair cost of a super-component in the power system (depending on the approach, the replacement cost). In this way, all probabilities are considered and severity standardized values between 0 and 1 are obtained. The normalized risk for an i-th attack is calculated by the equations [4-4] and [4-5]:

$$Risk_i = \frac{W_{1,i}\ \Pr(Sev_i catas) + W_{2,i}\left(\Pr Sev_i high\right) + W_{3,i}\ \Pr(Sev_i medium) + W_{4,i}\ \Pr(Sev_i low)}{W_{\max}}$$
$$i = 1,2,3,\ldots,q \qquad [4\text{-}4]$$
$$W_{\max} = \max\left(W_{i,j}\right)$$
$$\forall\ i = 1,2,3,\ldots,q\ ;\ \forall\ j = 1,\ldots,4 \qquad [4\text{-}5]$$

Where, $W_{\max}$ is the maximum repair cost for a single super-component (normally the most important) of a power system.

It should be made clear that this method is not the only way to calculate risk. The probabilities are obtained by the use of the Bayesian network but the measurement of severity can be a function, a fuzzy set, an interval, among others models. For that reason, there is other ways to find this measure that go from the concept of an expert to sophisticated calculations with theories such as fuzzy logic and expert systems.

4.2.3.2 Contingency arrangement

There is a number for every super-component of the system, which is understood as the risk associated with the occurrence of a contingency resulting from an attack. Because the value obtained is a scalar, the contingency ranking results in a problem of arrangement.

Contingencies are sorted from a lowest to a highest risk value. On the one hand, operators can establish a threshold value α from their judgement and, subsequently create the list by taking the contingencies that possess a value higher than this threshold.
A simple way to establish α is by calculating a relative measure between the maximum and minimum values:

$$\alpha = Risk_{\min} + \left(\frac{Risk_{\max} - Risk_{\min}}{2} \right) \quad [4\text{-}6]$$

$$Risk_{\min} = \min\left(Risk_1, Risk_2, \ldots, Risk_q\right) \quad [4\text{-}7]$$

$$Risk_{\max} = \max\left(Risk_1, Risk_2, \ldots, Risk_q\right) \quad [4\text{-}8]$$

or α can simply be the average of the risk values:

$$\alpha = \frac{\sum_{i=1}^{q} Risk_i}{q} \quad [4\text{-}9]$$

On the other hand, it is possible to establish an arbitrary number x of contingencies to be analysed. Therefore, the first x contingencies will be selected. It is very important that each contingency has an index which shows the difference between the more and less important ones. Figure 4-8 shows the process of the contingency ranking explained in the present Chapter.

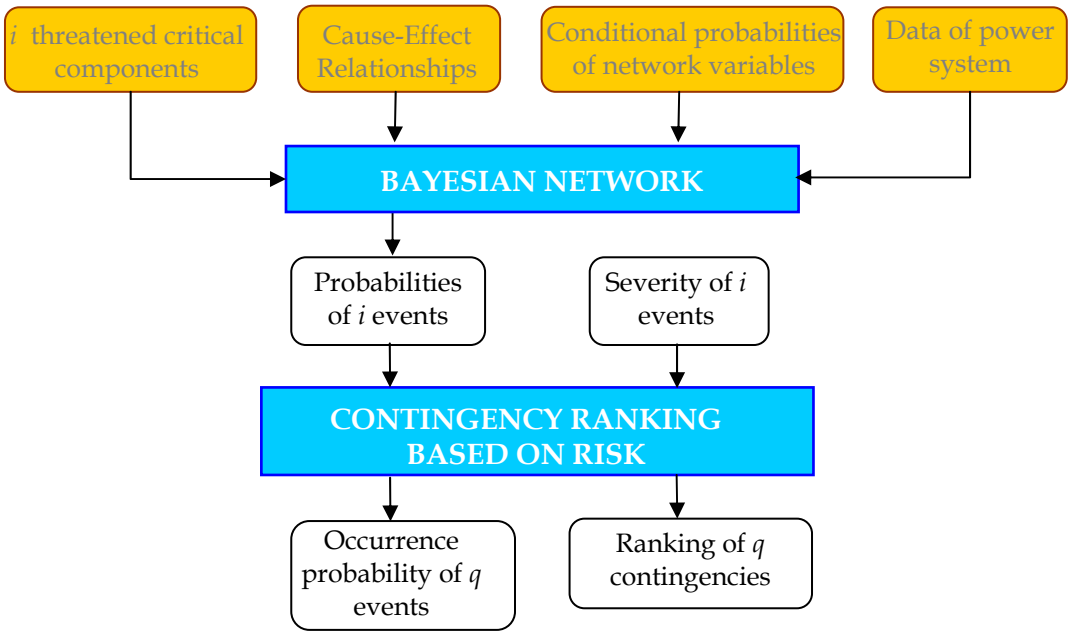


Figure 4-8. Contingency ranking resulting from physical terrorist attacks under security assessment.

Before going on to the numerical cases, we finally want to emphasize that the contingency ranking can be made only by taking into account the probability value of the actual occurrence of the attacks. This depends on the objective of the study, as well as on the criteria of evaluation of every utility.

4.3 Study Cases

The Bayesian network was constructed in the previous section and the conditional probability values were obtained from elicitation to experts, the operators of the Colombian system, terrorism experts, and the analysis of the authors. We have also used the database of the attacks on the Colombian electrical infrastructure in order to analyse the behaviour of the terrorist groups in this Country.

The next tables show the established values for the dependent variables of the Bayesian Network. These values are very high but they are acceptable in countries where there is a lot of terrorist activity. These tables are used in the test-cases shown in this section.

TABLE 4-VII. CONDITIONAL PROBABILITIES FOR THE "MOTIVATION OF THE ATTACK" VARIABLE

POSITION OF THE TERRORIST GROUP	POLITICAL SITUATION	CRITICALITY FOR POWER SYSTEM	MOTIVATION OF THE ATTACK		
			High	Medium	Low
High Presence	Critical	High	0.800	0.100	0.100
		Medium	0.550	0.150	0.300
		Low	0.300	0.250	0.450
	Moderately critical	High	0.500	0.250	0.250
		Medium	0.400	0.250	0.350
		Low	0.100	0.400	0.500
	Non critical	High	0.200	0.300	0.500
		Medium	0.100	0.400	0.500
		Low	0.050	0.450	0.500
Average Presence	Critical	High	0.350	0.500	0.150
		Medium	0.250	0.350	0.400
		Low	0.050	0.650	0.300
	Moderately critical	High	0.050	0.450	0.500
		Medium	0.050	0.350	0.600
		Low	0.050	0.250	0.700
	Non critical	High	0.000	0.400	0.600
		Medium	0.000	0.300	0.700
		Low	0.100	0.100	0.800
Low Presence	Critical	High	0.200	0.550	0.250
		Medium	0.200	0.450	0.350
		Low	0.000	0.100	0.900
	Moderately critical	High	0.000	0.350	0.650
		Medium	0.000	0.150	0.850
		Low	0.000	0.050	0.950
	Non critical	High	0.000	0.200	0.800
		Medium	0.000	0.150	0.850
		Low	0.000	0.025	0.975

TABLE 4-VIII. CONDITIONAL PROBABILITIES FOR THE "VULNERABILITY OF THE TARGET" VARIABLE

GEOGRAPHICAL LOCALIZATION	PHYSICAL PROTECTION OF THE SCOMP	VULNERABILITY OF THE TARGET		
		High	Medium	Low
High Exposure	High	0.200	0.400	0.400
	Medium	0.500	0.200	0.300
	Low	0.700	0.000	0.300
Average Exposure	High	0.100	0.300	0.600
	Medium	0.300	0.300	0.400
	Low	0.500	0.200	0.300
Low Exposure	High	0.050	0.500	0.450
	Medium	0.100	0.400	0.500
	Low	0.300	0.300	0.400

TABLE 4-IX. CONDITIONAL PROBABILITIES FOR THE "INTENSITY OF THE ATTACK" VARIABLE

TYPE OF SCOMP	MOTIVATION OF THE ATTACK	VULNERABILITY OF THE TARGET	INTENSITY OF THE ATTACK			
			High	Medium	Low	No attack
GENERATOR	High	High	0.200	0.150	0.100	0.550
		Medium	0.150	0.150	0.100	0.600
		Low	0.100	0.150	0.050	0.700
	Medium	High	0.150	0.100	0.100	0.650
		Medium	0.100	0.100	0.100	0.700
		Low	0.075	0.075	0.050	0.800
	Low	High	0.075	0.150	0.100	0.675
		Medium	0.050	0.075	0.100	0.775
		Low	0.025	0.050	0.075	0.850
SUBSTATION	High	High	0.300	0.100	0.100	0.500
		Medium	0.200	0.150	0.075	0.575
		Low	0.150	0.100	0.050	0.700
	Medium	High	0.250	0.150	0.200	0.400
		Medium	0.150	0.200	0.150	0.500
		Low	0.100	0.200	0.100	0.600
	Low	High	0.150	0.100	0.200	0.550
		Medium	0.100	0.100	0.150	0.650
		Low	0.050	0.050	0.100	0.800
LINE	High	High	0.800	0.100	0.050	0.050
		Medium	0.600	0.200	0.100	0.100
		Low	0.200	0.100	0.100	0.600
	Medium	High	0.600	0.100	0.100	0.200
		Medium	0.400	0.200	0.050	0.350
		Low	0.300	0.050	0.025	0.625
	Low	High	0.300	0.100	0.050	0.550
		Medium	0.100	0.100	0.100	0.700
		Low	0.050	0.050	0.025	0.875

TABLE 4-X. CONDITIONAL PROBABILITIES FOR THE "CONSEQUENCE OF THE ATTACK" VARIABLE

TYPE OF SCOMP	INTENSITY OF THE ATTACK	CONSEQUENCE OF THE ATTACK				
		Catastrop.	High	Medium	Low	No attack
GENERATOR	High	0.200	0.500	0.250	0.050	0.000
	Medium	0.050	0.100	0.600	0.250	0.000
	Low	0.000	0.000	0.250	0.700	0.050
	No attack	0.000	0.000	0.000	0.000	1.000
SUBSTATION	High	0.200	0.500	0.250	0.050	0.000
	Medium	0.050	0.150	0.500	0.300	0.000
	Low	0.000	0.000	0.200	0.750	0.050
	No attack	0.000	0.000	0.000	0.000	1.000
LINES	High	0.000	0.000	1.000	0.000	0.000
	Medium	0.000	0.000	0.400	0.600	0.000
	Low	0.000	0.000	0.100	0.800	0.100
	No attack	0.000	0.000	0.000	0.000	1.000

In order to illustrate our method we have used two test power systems.

4.3.1 Case 1: five-bus test system.

The first power system used is shown in Figure 4-9. Geographically the system is divided into five zones with different socio-political characteristics. The system has 14 super-components: 2 generators, 5 substations and 7 transmission lines. Based on the experience gained from the Colombian case, some assumptions were made about the five zones, which concerned the territorial control of the terrorist group, the political situation in the zone and the exposure of components regarding their geographic location. The situation in each zone is the following:

Zone	The political situation in the zone is:	The level of control by the terrorist group is:	The exposure of components is:
1	Non Critical	Low	Between medium and high. Some SCOs high.
2	Non Critical	Reasonably high	Different levels of exposure
3	Critical	Medium	Different levels of exposure
4	Moderately Critical	Relatively high	Different levels of exposure
5	Moderately Critical	Low	Low exposure

In order to completely characterize the Bayesian network, the load flow data was developed and the most important data are shown in Figure 4-9. The information of the power system and the load flow results are detailed in the Appendix B. We have used the voltage values, the power flows on transmission lines and the technical characteristics of super-components to establish the criticality and the severity of the attacks on the super-components of the power system. Based on the abovementioned hypothesis and the power flows, Table 4-XI shows the grade of severity for each super-component.

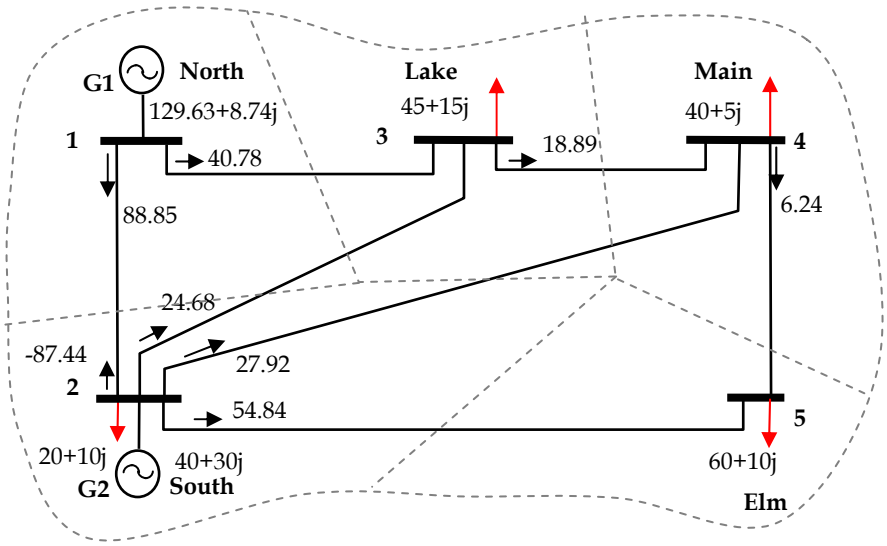


Figure 4-9. Five-bus test system.

TABLE 4-XI. SEVERITY ALLOCATION FOR THE TEST SYSTEM

TYPE OF SCOMP	NAME	SEVERITY			
		Catastrop	High	Medium	Low
GEN, x units	G1North	All units	2<N unit<x	2 Units	1 Unit
GEN, y units	G2South	All units	2<N unit<y	2 Units	1 Unit
SUB	SUB1North	Subst	Transformator	Line 1-2	Line 1-3
SUB	SUB2South	Subst	Transformator	Line 1-2	Line 2-4
				Line 2-5	Line 2-3
SUB	SUB3Lake	Subst	Transformator	Line 1-3	Line 3-4
				Line 2-3	
SUB	SUB4Main	Subst	Transformator	Line 2-4	Line 4-5
				Line 3-4	
SUB	SUB5Elm	Subst	Transformator	Line 2-5	Line 4-5
LINE	LIN1-2			Line 1-2	
LINE	LIN1-3			Line 1-3	
LINE	LIN2-3				Line 2-3
LINE	LIN2-4			Line 2-4	
LINE	LIN2-5				Line 2-5
LINE	LIN3-4				Line 3-4
LINE	LIN4-5				Line 4-5

4.3.1.1 Simulation

In order to simulate the Bayesian Network, the freeware Bayes Net Toolbox for Matlab 7.0 was used. The code implemented for the network is shown in Appendix C.

The probabilities of the independent variables, according to the socio-political conditions of the place where each super-component is located, are exposed in Table XII. We have simulated the 14 cases, i.e., one simulation for every super-component of the power system. The results of the simulation, specifically the probabilities of the dependent variables, are given in Table 4-XIII and in Figures 4-10.

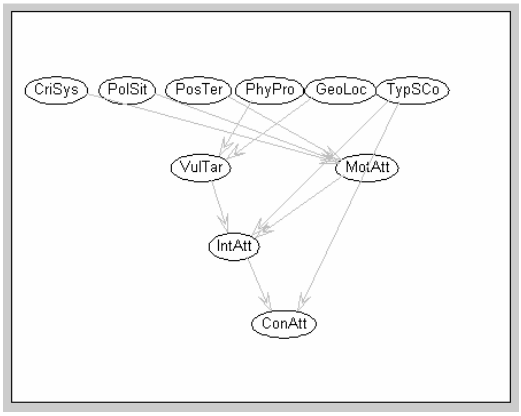
Table 4-XIV illustrates the probabilities of intensity of the attack and the probability of attack against each component is obtained through [4-2].

TABLE 4-XII. PROBABILITY VALUES OF THE BAYESIAN NETWORK INDEPENDENT VARIABLES: FIVE-BUS POWER SYSTEM

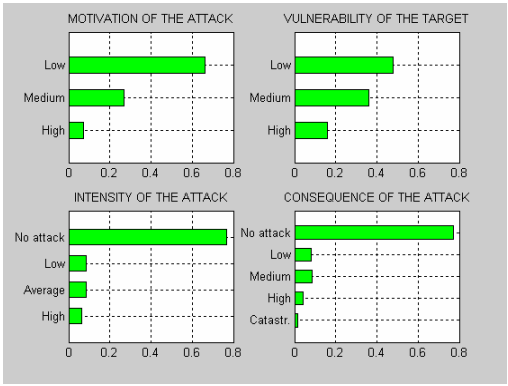
SCOMP	ZONE	CriSys High	CriSys Medium	CriSys Low	PolSit Critical	PolSit Moderately	PolSit Noncritical	PosTer High	PosTer Medium	PosTer Low	GeoSit High	GeoSit Medium	GeoSit Low	PhyPro High	PhyPro Medium	PhyPro Low	TypSCo Gen	TypSCoSub	TypSCo Lin
G1North	1	0.900	0.100	0.000	0.045	0.212	0.743	0.221	0.108	0.671	0.491	0.400	0.109	0.940	0.041	0.019	1	0	0
SUB1North	1	0.850	0.100	0.050	0.045	0.212	0.743	0.221	0.108	0.671	0.491	0.400	0.109	0.940	0.041	0.019	0	1	0
LIN1-2	1	0.850	0.100	0.050	0.045	0.212	0.743	0.221	0.108	0.671	0.840	0.139	0.021	0.006	0.139	0.855	0	0	1
LIN1-3	1	0.750	0.100	0.150	0.045	0.212	0.743	0.221	0.108	0.671	0.840	0.139	0.021	0.006	0.139	0.855	0	0	1
G2South	2	0.600	0.300	0.100	0.281	0.152	0.567	0.498	0.375	0.128	0.022	0.170	0.808	0.081	0.125	0.794	1	0	0
SUB2South	2	0.700	0.200	0.100	0.281	0.152	0.567	0.498	0.375	0.128	0.022	0.170	0.808	0.081	0.125	0.794	0	1	0
LIN2-3	2	0.150	0.500	0.350	0.281	0.152	0.567	0.498	0.375	0.128	0.457	0.308	0.235	0.783	0.121	0.097	0	0	1
LIN2-4	2	0.150	0.500	0.350	0.281	0.152	0.567	0.498	0.375	0.128	0.457	0.308	0.235	0.735	0.254	0.011	0	0	1
LIN2-5	2	0.650	0.300	0.050	0.281	0.152	0.567	0.498	0.375	0.128	0.574	0.380	0.045	0.454	0.274	0.273	0	0	1
SUB3Lake	3	0.750	0.200	0.050	0.731	0.201	0.068	0.100	0.685	0.215	0.301	0.177	0.521	0.943	0.050	0.007	0	1	0
LIN3-4	3	0.100	0.500	0.400	0.731	0.201	0.068	0.100	0.685	0.215	0.795	0.197	0.008	0.113	0.333	0.554	0	0	1
SUB4Main	4	0.800	0.150	0.050	0.595	0.326	0.079	0.492	0.317	0.191	0.557	0.273	0.170	0.901	0.081	0.018	0	1	0
LIN4-5	4	0.330	0.330	0.340	0.595	0.326	0.079	0.492	0.317	0.191	0.110	0.268	0.622	0.638	0.223	0.139	0	0	1
SUB5Elm	5	0.850	0.100	0.050	0.075	0.573	0.351	0.101	0.223	0.676	0.018	0.201	0.781	0.808	0.151	0.041	0	1	0

TABLE 4-XIII. PROBABILITY VALUES OF THE BAYESIAN NETWORK DEPENDENT VARIABLES: FIVE-BUS POWER SYSTEM

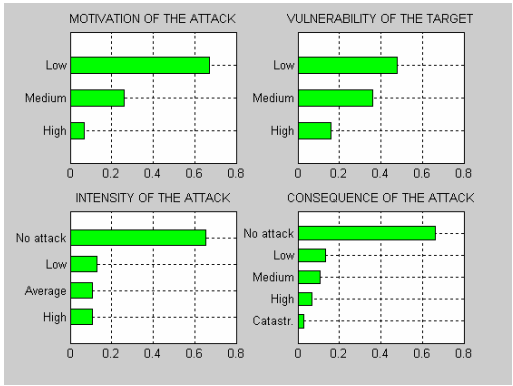
SCOMP	ZONE	MotivAtt High	MotivAtt Medium	MotivAtt Low	VulneTar High	VulneTar Medium	VulneTar Low	IntensAtt High	IntensAtt Medium	IntensAtt Low	IntensAtt None	SevAtt Catastrop	SevAtt High	SevAtt Medium	SevAtt Low	SevAtt No impact
G1North	1	0.0708	0.2678	0.6614	0.1614	0.3615	0.4771	0.0631	0.0839	0.0840	0.7689	0.0168	0.0399	0.0871	0.0830	0.7731
SUB1North	1	0.0684	0.2609	0.6707	0.1614	0.3615	0.4771	0.1068	0.1092	0.1296	0.6544	0.0268	0.0698	0.1072	0.1353	0.6609
LIN1-2	1	0.0684	0.2609	0.6707	0.6331	0.0619	0.3051	0.3125	0.0878	0.0545	0.5451	0.0000	0.0000	0.3531	0.0963	0.5506
LIN1-3	1	0.0636	0.2471	0.6893	0.6331	0.0619	0.3051	0.3067	0.0876	0.0540	0.5517	0.0000	0.0000	0.3472	0.0958	0.5571
G2South	2	0.2127	0.3143	0.4731	0.2950	0.3044	0.4006	0.0861	0.1014	0.0847	0.7278	0.0223	0.0532	0.1035	0.0889	0.7320
SUB2South	2	0.2208	0.3161	0.4631	0.2950	0.3044	0.4006	0.1405	0.1210	0.1287	0.6097	0.0342	0.0884	0.1214	0.1399	0.6161
LIN2-3	2	0.1564	0.3057	0.5379	0.1990	0.3537	0.4474	0.2560	0.0975	0.0594	0.5871	0.0000	0.0000	0.3009	0.1060	0.5931
LIN2-4	2	0.1564	0.3057	0.5379	0.1917	0.3608	0.4475	0.2545	0.0978	0.0595	0.5881	0.0000	0.0000	0.2996	0.1063	0.5941
LIN2-5	2	0.2207	0.3152	0.4641	0.3466	0.2584	0.3951	0.3177	0.0985	0.0610	0.5229	0.0000	0.0000	0.3632	0.1078	0.5289
SUB3Lake	3	0.2581	0.4250	0.3169	0.1142	0.4270	0.4588	0.1337	0.1383	0.1156	0.6123	0.0337	0.0876	0.1257	0.1349	0.6181
LIN3-4	3	0.1589	0.3776	0.4635	0.5367	0.1400	0.3234	0.3598	0.0939	0.0603	0.4860	0.0000	0.0000	0.4034	0.1046	0.4921
SUB4Main	4	0.3847	0.3122	0.3031	0.1734	0.3743	0.4522	0.1462	0.1289	0.1099	0.6151	0.0357	0.0924	0.1230	0.1284	0.6206
LIN4-5	4	0.2795	0.3042	0.4163	0.1503	0.3895	0.4602	0.2860	0.1062	0.0640	0.5438	0.0000	0.0000	0.3349	0.1149	0.5502
SUB5Elm	5	0.0613	0.3123	0.6264	0.0872	0.4381	0.4747	0.1040	0.1163	0.1266	0.6530	0.0266	0.0695	0.1095	0.1351	0.6594



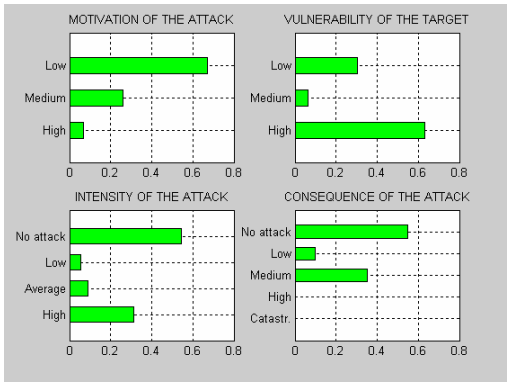
(a) The Bayesian Network implemented in Matlab



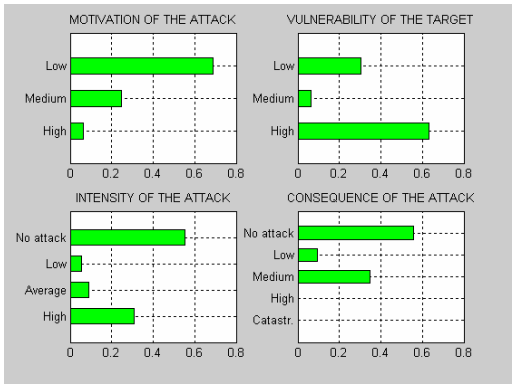
(a) Results G1North



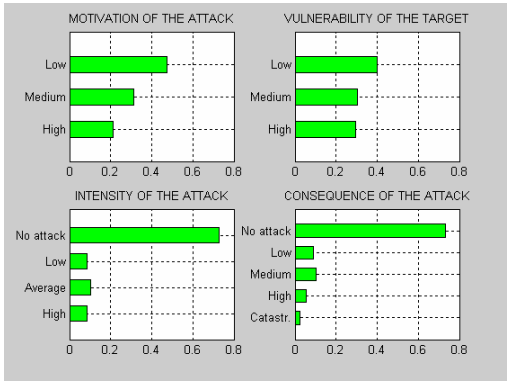
(b) Results SUB1North



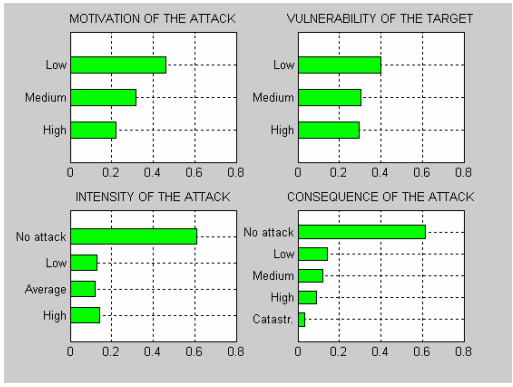
(c) Results LIN1-2



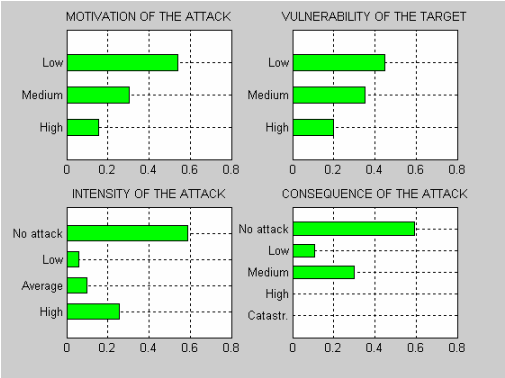
(d) Results LIN1-3



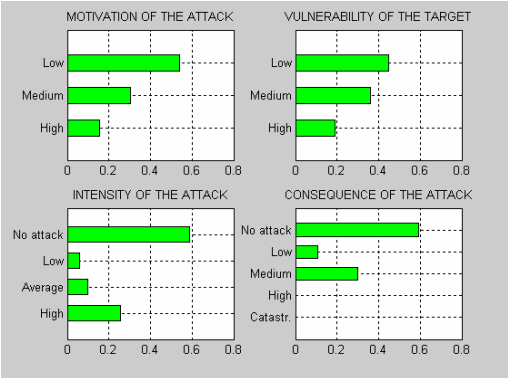
(e) Results G2South



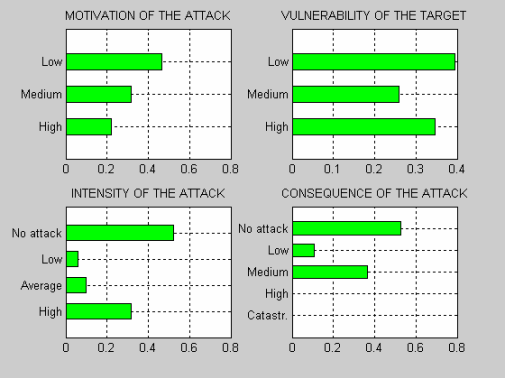
(f) Results SUB2South



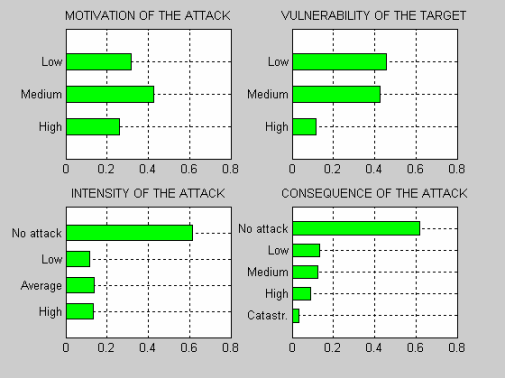
(g) Results LIN2-3



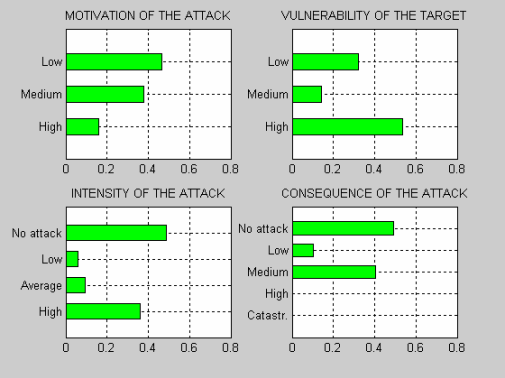
(h) Results LIN2-4



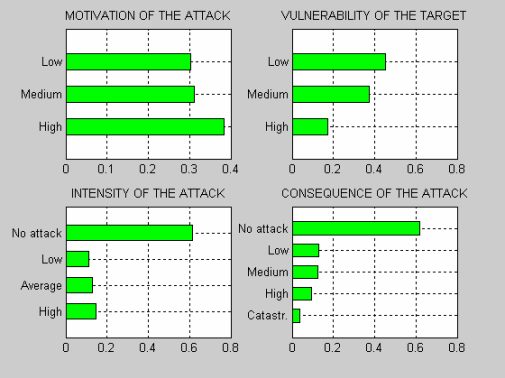
(i) Results LIN2-5



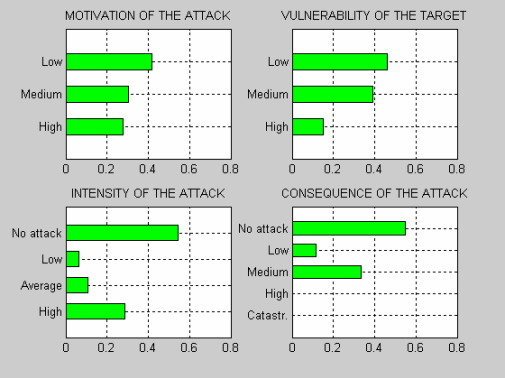
(j) Results SUB3Lake



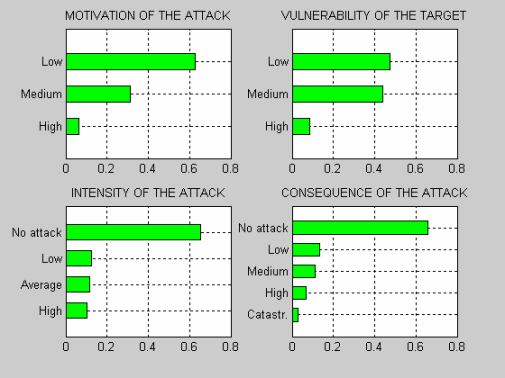
(k) Results LIN3-4



(l) Results SUB4Main



(m) Results LIN4-5



(n) Results SUB5Elm

Figure 4-10. Graphical results of the Bayesian Network: five-bus test power system.

TABLE 4-XIV. PROBABILITY OF THE ATTACK FOR THE SYSTEM SUPER-COMPONENTS: FIVE-BUS SYSTEM

ZONE	NAME	INTENSITY OF THE ATTACK				PROB ATTACK
		High	Medium	Low	None	
Zone 1	G1North	0.0631	0.0839	0.0840	0.7689	0.2310
	SUB1North	0.1068	0.1092	0.1296	0.6544	0.3456
	LIN1-2	0.3125	0.0878	0.0545	0.5451	0.4548
	LIN1-3	0.3067	0.0876	0.0540	0.5517	0.4483
Zone 2	G2South	0.0861	0.1014	0.0847	0.7278	0.2722
	SUB2South	0.1405	0.1210	0.1287	0.6097	0.3902
	LIN2-3	0.2560	0.0975	0.0594	0.5871	0.4129
	LIN2-4	0.2545	0.0978	0.0595	0.5881	0.4118
	LIN2-5	0.3177	0.0985	0.0610	0.5229	0.4772
Zone 3	SUB3Lake	0.1337	0.1383	0.1156	0.6123	0.3876
	LIN3-4	0.3598	0.0939	0.0603	0.4860	0.5140
Zone 4	SUB4Main	0.1462	0.1289	0.1099	0.6151	0.3850
	LIN4-5	0.2860	0.1062	0.0640	0.5438	0.4562
Zone 5	SUB5Elm	0.1040	0.1163	0.1266	0.6530	0.3469

The next step is the calculation of the risk. For this purpose, we use the equation [4-4] and the results are presented in Table 4-XV. In general, the weights or costs (produced by the occurrence of the attack) in this formula must be given by the utilities according to the reparation cost of the percentage of the components affected. However for this test system, we assign these weight values in a coherent way (in Table 4-XVI) but they are not real costs. These weights depend on various factors, such as the technology of the components and their age and location, among others.

TABLE 4-XV. NORMALIZED RISK FOR EACH SUPER-COMPONENT: FIVE-BUS SYSTEM

ZONE	NAME	SEVERITY OF THE ATTACK					Risk	Risk / max(Risk)
		Catastrop	High	Medium	Low	No impact		
Zone 1	G1North	0.0168	0.0399	0.0871	0.0830	0.7731	0.1033	0.7803
	SUB1North	0.0268	0.0698	0.1072	0.1353	0.6609	0.1111	0.8387
	LIN1-2	0.0000	0.0000	0.3531	0.0963	0.5506	0.1070	0.8082
	LIN1-3	0.0000	0.0000	0.3472	0.0958	0.5571	0.1054	0.7958
Zone 2	G2South	0.0223	0.0532	0.1035	0.0889	0.7320	0.1274	0.9622
	SUB2South	0.0342	0.0884	0.1214	0.1399	0.6161	0.1308	0.9878
	LIN2-3	0.0000	0.0000	0.3009	0.1060	0.5931	0.0944	0.7128
	LIN2-4	0.0000	0.0000	0.2996	0.1063	0.5941	0.0941	0.7105
	LIN2-5	0.0000	0.0000	0.3632	0.1078	0.5289	0.1112	0.8401
Zone 3	SUB3Lake	0.0337	0.0876	0.1257	0.1349	0.6181	0.1307	0.9868
	LIN3-4	0.0000	0.0000	0.4034	0.1046	0.4921	0.1215	0.9178
Zone 4	SUB4Main	0.0357	0.0924	0.1230	0.1284	0.6206	0.1324	1.0000
	LIN4-5	0.0000	0.0000	0.3349	0.1149	0.5502	0.1046	0.7902
Zone 5	SUB5Elm	0.0266	0.0695	0.1095	0.1351	0.6594	0.1115	0.8421

TABLE 4-XVI. WEIGHTS (COSTS) ASSIGNED FOR EACH TYPE OF SUPER-COMPONENT ACCORDING TO THE SEVERITY OF THE ATTACK

	Catastrophic	High	Medium	Low
Generators	15	11	7	3
Substations	10	7.5	5	2.5
Lines			4	2
			Maximum Value	15

By using [4-6] and [4-9] the possible threshold values are: relative: 0.1132; median: 0.1111 and average: 0.1132.

Taking the median value into consideration, the result of the contingency ranking is the loss of assets with a risk that is greater than the threshold value: 0.111. In our case the most important contingencies are:

1. SUB4Main
2. SUB2South
3. SUB3Lake
4. G2South
5. LIN3-4
6. SUB5Elm and,
7. LIN2-5.

4.3.1.2 Results analysis

The loss of substation 4 (SUB4Main) is the most important contingency. Having analyzed the probabilities for this super-component we realize that, in comparison with the other components, there is a higher probability that the intensity of an attack on the substation would be high or catastrophic. This asset is located in a zone where the terrorist group is well positioned and the political situation is critical. Compared to the other substations it is not the one with the highest level of protection and its operation is important for the power system.

The next most important super-component is substation SUB2South, which is very vulnerable and is placed in a zone where the level of control of the terrorist group is also high. We notice that with the third super-component of the list, there is a large motive to attack it (SUB3Lake).

At first glance, it is a little surprising to find that the loss of the generator of the slack node (G1North) is not within the most important contingencies. Nevertheless, it can be stated that although its operation for the system is highly critical, the zone where the asset is placed does not have important characteristics at a socio-political level and the physical protection of the assets is high (in some cases including military presence at the facilities). This results in a low probability of access as well as little motivation for an attack.

In the case of the transmission lines, two of them were found to be at high risk of attack, and even more than assets such as generators and substations. This can be explained by the level of exposure of these lines, their low protection and the severity that the loss of these lines would have in comparison with the others. For example, by looking at the results we can notice that LIN 3-4 is very vulnerable and the political situation is critical in this zone.

4.3.2 *Case 2: nine-bus test system*

In this section, we illustrate the application of the method for the Western System Coordinating Council WSCC nine-bus system shown in Figure 4-11. This second power system has 15 main components: 3 generators, 5 substations and 6 transmission lines, and it is geographically divided into three zones. The socio-political situation of the zone where the power system is located is presented as follows:

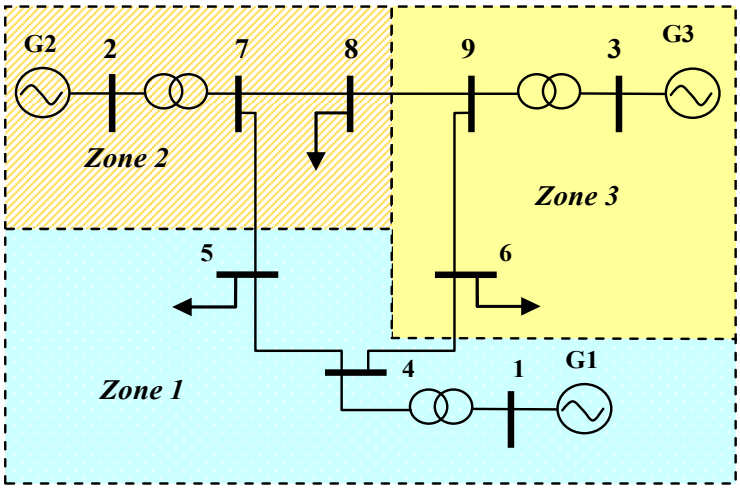


Figure 4-11. Western System Coordinating Council WSCC nine-bus test system.

Zone	The political situation in the zone is:	The level of control by the terrorist group is:	The exposure of components is:
1	Between moderately and noncritical	Medium	Between high and medium
2	Noncritical	Low	Relatively high
3	Moderately	High	Between medium and low

For each component the probabilities of the independent variables of the Bayesian network are shown in Table 4-XVII.

4.3.2.1 Simulation

The 15 cases (attacks against each of the systems' components) were simulated. The results of the simulation can be found in Table 4-XVIII and Figures 4-12.

In theses scenarios, we realize that through using only the value of the probability of attack in order to rank contingencies, the results show that the transmission lines are the first super-components in the list, followed by substations and generators respectively. These outcomes are consistent with the statistics of the super-components which were attacked in the Colombian power system (See Appendix A).

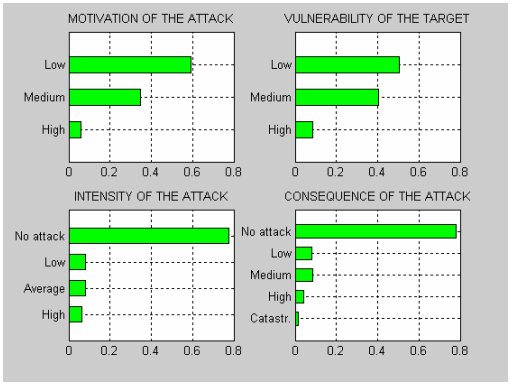
With the aim of assessing the risk, taking into consideration the cost of the attacks, we slightly modified the weights assigned in Table 4-XVI for each super-component. We diminished the costs of severity for generators. The values taken were: 14 for the catastrophic case, 10, 6 and 2 for the high, medium and low severities.

Table 4-XVII. PROBABILITY VALUES OF THE BAYESIAN NETWORK INDEPENDENT VARIABLES: WSCC NINE-BUS TEST SYSTEM

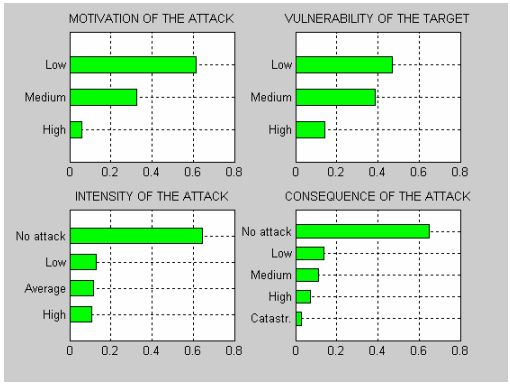
SCOMP	ZONE	CriSys High	CriSys Medium	CriSys Low	PolSit Critical	PolSit Moderately	PolSit Noncritical	PosTer High	PosTer Medium	PosTer Low	GeoSit High	GeoSit Medium	GeoSit Low	PhyPro High	PhyPro Medium	PhyPro Low	TypSCo Gen	TypSCoSub	TypSCo Lin
G1	1	0.900	0.100	0.000	0.032	0.509	0.459	0.110	0.505	0.385	0.105	0.415	0.480	1.000	0.000	0.000	1	0	0
SUB 14	1	0.800	0.100	0.100	0.032	0.509	0.459	0.110	0.505	0.385	0.407	0.305	0.288	0.940	0.041	0.019	0	1	0
SUB 5	1	0.650	0.250	0.100	0.045	0.652	0.303	0.110	0.685	0.205	0.630	0.100	0.270	0.750	0.240	0.010	0	1	0
LIN 45	1	0.700	0.150	0.150	0.045	0.652	0.303	0.110	0.685	0.205	0.745	0.127	0.128	0.000	0.200	0.800	0	0	1
LIN 46	1	0.600	0.150	0.250	0.045	0.652	0.303	0.110	0.720	0.170	0.507	0.305	0.188	0.000	0.300	0.700	0	0	1
G2	2	0.750	0.200	0.050	0.104	0.112	0.784	0.108	0.153	0.739	0.387	0.307	0.306	1.000	0.000	0.000	1	0	0
SUB 27	2	0.850	0.100	0.050	0.104	0.112	0.784	0.108	0.153	0.739	0.387	0.307	0.306	0.850	0.125	0.025	0	1	0
SUB 8	2	0.750	0.150	0.100	0.104	0.152	0.744	0.100	0.125	0.775	0.454	0.320	0.226	0.900	0.081	0.019	0	1	0
LIN 75	2	0.250	0.500	0.250	0.050	0.430	0.520	0.050	0.350	0.600	0.800	0.117	0.083	0.150	0.150	0.700	0	0	1
LIN 78	2	0.500	0.350	0.150	0.104	0.152	0.744	0.100	0.125	0.775	0.557	0.293	0.150	0.150	0.150	0.700	0	0	1
G3	3	0.850	0.100	0.050	0.100	0.723	0.177	0.790	0.195	0.015	0.145	0.301	0.554	0.950	0.050	0.000	1	0	0
SUB 39	3	0.850	0.100	0.050	0.100	0.723	0.177	0.790	0.195	0.015	0.177	0.301	0.522	0.113	0.333	0.554	0	1	0
SUB 6	3	0.750	0.100	0.150	0.100	0.723	0.177	0.790	0.195	0.015	0.170	0.170	0.660	0.750	0.150	0.100	0	1	0
LIN 96	3	0.500	0.350	0.150	0.100	0.723	0.177	0.790	0.195	0.015	0.018	0.781	0.201	0.050	0.150	0.800	0	0	1
LIN 98	3	0.330	0.330	0.340	0.100	0.723	0.177	0.452	0.395	0.153	0.110	0.622	0.268	0.150	0.250	0.600	0	0	1

Table 4-XVIII. PROBABILITY VALUES OF THE BAYESIAN NETWORK DEPENDENT VARIABLES: WSCC NINE-BUS TEST SYSTEM

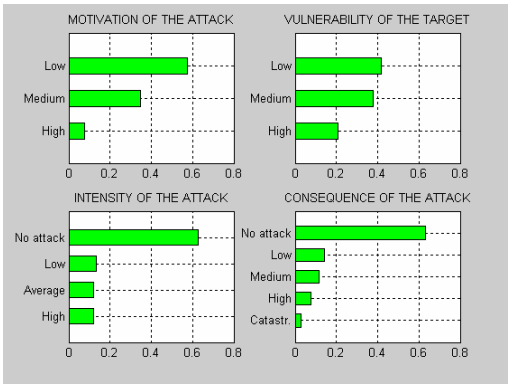
SCOMP	ZONE	MotivAtt High	MotivAtt Medium	MotivAtt Low	VulneTar High	VulneTar Medium	VulneTar Low	IntensAtt High	IntensAtt Medium	IntensAtt Low	IntensAtt None	SevAtt Catastrop	SevAtt High	SevAtt Medium	SevAtt Low	SevAtt No impact
G1	1	0.0606	0.3471	0.5923	0.0865	0.4065	0.5070	0.0630	0.0802	0.0822	0.7747	0.0166	0.0395	0.0844	0.0807	0.7788
SUB 14	1	0.0590	0.3274	0.6136	0.1420	0.3890	0.4690	0.1087	0.1172	0.1297	0.6445	0.0276	0.0719	0.1117	0.1379	0.6510
SUB 5	1	0.0751	0.3493	0.5757	0.2071	0.3771	0.4158	0.1189	0.1208	0.1343	0.6260	0.0298	0.0776	0.1170	0.1429	0.6327
LIN 45	1	0.0753	0.3497	0.5751	0.5834	0.0987	0.3179	0.3294	0.0895	0.0573	0.5239	0.0000	0.0000	0.3709	0.0995	0.5296
LIN 46	1	0.0742	0.3362	0.5896	0.5038	0.1626	0.3336	0.3078	0.0912	0.0574	0.5436	0.0000	0.0000	0.3500	0.1006	0.5494
G2	2	0.0494	0.2592	0.6914	0.1234	0.3999	0.4767	0.0594	0.0803	0.0844	0.7759	0.0159	0.0377	0.0841	0.0821	0.7801
SUB 27	2	0.0508	0.2652	0.6840	0.1573	0.3802	0.4624	0.1056	0.1096	0.1313	0.6535	0.0266	0.0692	0.1074	0.1366	0.6601
SUB 8	2	0.0472	0.2517	0.7011	0.1590	0.3765	0.4645	0.1044	0.1078	0.1316	0.6563	0.0263	0.0684	0.1063	0.1362	0.6628
LIN 75	2	0.0323	0.2252	0.7425	0.5433	0.1275	0.3292	0.2685	0.0874	0.0536	0.5905	0.0000	0.0000	0.3088	0.0953	0.5959
LIN 78	2	0.0429	0.2292	0.7278	0.4864	0.1693	0.3443	0.2612	0.0881	0.0546	0.5961	0.0000	0.0000	0.3019	0.0966	0.6015
G3	3	0.3671	0.2882	0.3447	0.0934	0.4211	0.4855	0.0884	0.1045	0.0799	0.7272	0.0229	0.0546	0.1048	0.0865	0.7312
SUB 39	3	0.3671	0.2882	0.3447	0.3260	0.2792	0.3948	0.1584	0.1224	0.1197	0.5995	0.0378	0.0975	0.1247	0.1344	0.6055
SUB 6	3	0.3379	0.2961	0.3660	0.1335	0.4123	0.4542	0.1368	0.1263	0.1113	0.6256	0.0337	0.0873	0.1196	0.1282	0.6312
LIN 96	3	0.3147	0.2948	0.3905	0.4148	0.2380	0.3471	0.3680	0.1026	0.0640	0.4653	0.0000	0.0000	0.4155	0.1128	0.4717
LIN 98	3	0.1694	0.3037	0.5269	0.3628	0.2565	0.3807	0.3010	0.0963	0.0598	0.5429	0.0000	0.0000	0.3455	0.1056	0.5489



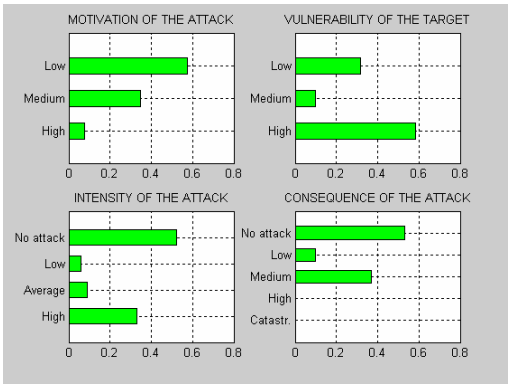
(a) Results G1



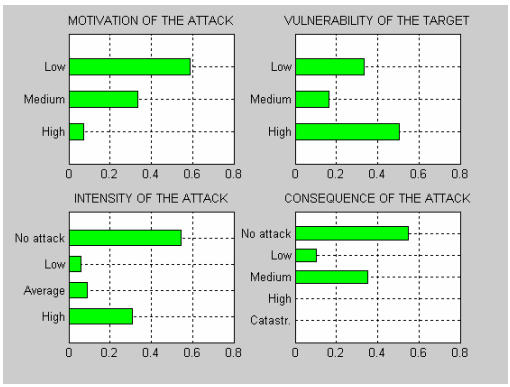
(b) Results SUB14



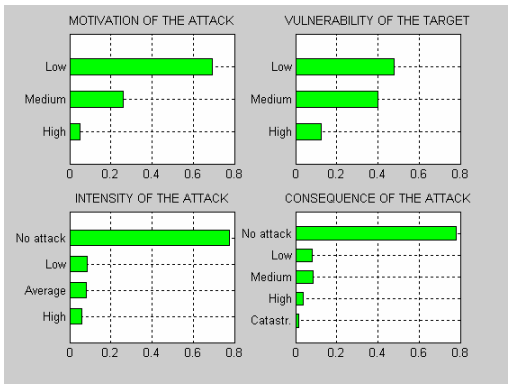
(c) Results SUB5



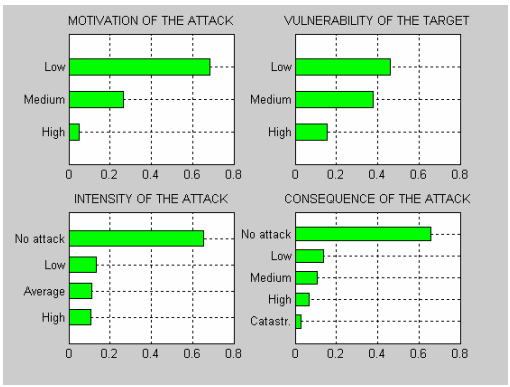
(d) Results LIN45



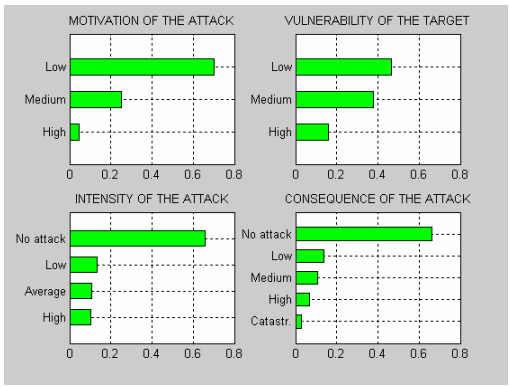
(e) Results LIN46



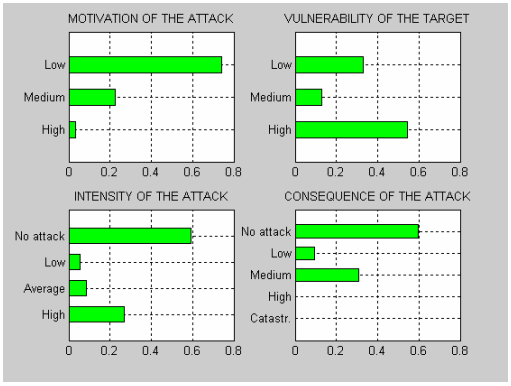
(f) Results G2



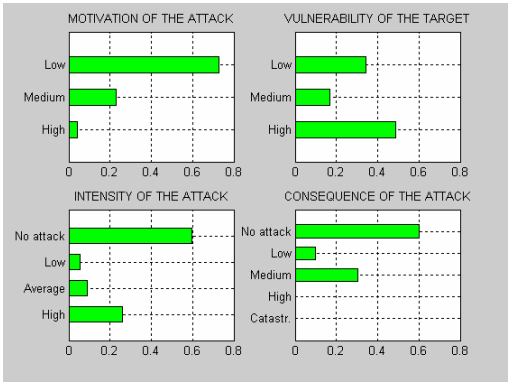
(g) Results SUB27



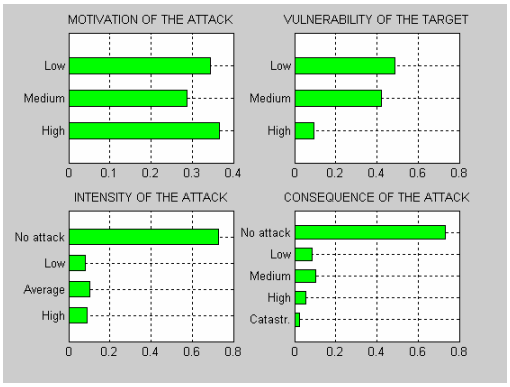
(h) Results SUB8



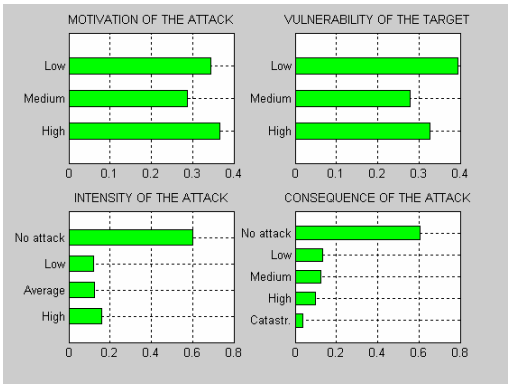
(i) Results LIN75



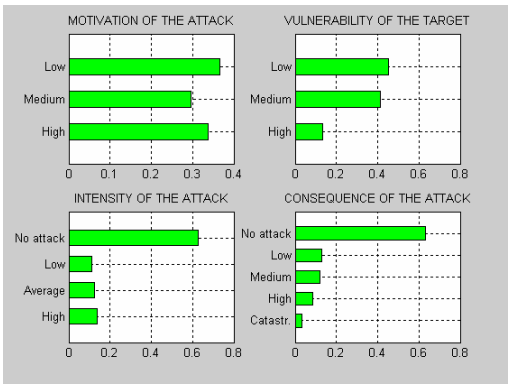
(j) Results LIN78



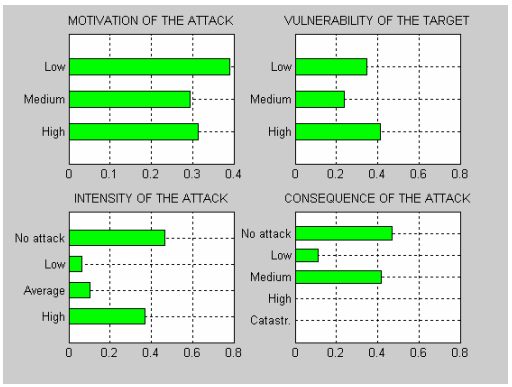
(k) Results G3



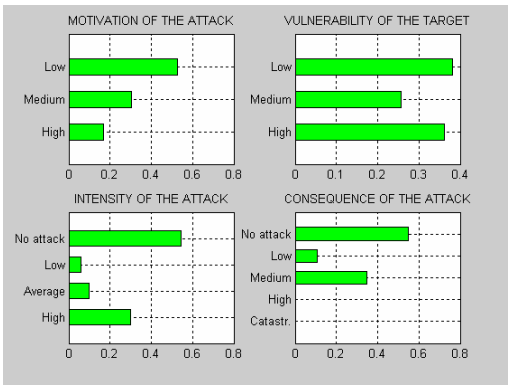
(l) Results SUB39



(m) Results SUB6



(n) Results LIN96



(o) Results LIN98

Figures 4-12. Graphical results of the Bayesian Network: WSCC nine-bus test system.

Later, with the use of equation [4-4] the contingency ranking is made. The risk values are shown in Table 4-XIX.

TABLE 4-XIX. NORMALIZED RISK FOR EACH SUPER-COMPONENT: NINE-BUS SYSTEM

NAME	PROB ATTACK	SEVERITY OF THE ATTACK					Risk	Risk/max (Riski)
		Catastrop	High	Medium	Low	No impact		
G1	0.2253	0.0166	0.0395	0.0844	0.0807	0.7788	0.0925	0.6261
SUB 14	0.3555	0.0276	0.0719	0.1117	0.1379	0.6510	0.1228	0.8307
SUB 5	0.3740	0.0298	0.0776	0.1170	0.1429	0.6327	0.1302	0.8808
LIN 45	0.4761	0.0000	0.0000	0.3709	0.0995	0.5296	0.1202	0.8133
LIN 46	0.4564	0.0000	0.0000	0.3500	0.1006	0.5494	0.1144	0.7740
G2	0.2241	0.0159	0.0377	0.0841	0.0821	0.7801	0.0906	0.6131
SUB 27	0.3465	0.0266	0.0692	0.1074	0.1366	0.6601	0.1188	0.8041
SUB 8	0.3437	0.0263	0.0684	0.1063	0.1362	0.6628	0.1177	0.7966
LIN 75	0.4095	0.0000	0.0000	0.3088	0.0953	0.5959	0.1018	0.6892
LIN 78	0.4039	0.0000	0.0000	0.3019	0.0966	0.6015	0.1001	0.6771
G3	0.2728	0.0229	0.0546	0.1048	0.0865	0.7312	0.1192	0.8065
SUB 39	0.4005	0.0378	0.0975	0.1247	0.1344	0.6055	0.1478	1.0000
SUB 6	0.3744	0.0337	0.0873	0.1196	0.1282	0.6312	0.1364	0.9234
LIN 96	0.5347	0.0000	0.0000	0.4155	0.1128	0.4717	0.1348	0.9124
LIN 98	0.4571	0.0000	0.0000	0.3455	0.1056	0.5489	0.1138	0.7701

The result of the contingency ranking displays the loss of assets with a risk greater than the threshold value. For this second case, we take the relative value. (e.g. Relative: 0.1192; Median:0.1190; Average:0.1177). The contingency ranking is then:

1. SUB 39
2. SUB 6
3. LIN 96
4. SUB 5
5. SUB 14
6. LIN 45
7. G3

4.3.2.2 Results analysis

In this case the most important contingencies are attacks on substation 39 and substation 6. Analyzing the ranking, these substations are located in a zone that has critical socio-political characteristics. The motive for attacking the SUB39 is high even though the component is well protected and more vulnerable than SUB6.

We can see that LIN 96 is not the most critical line for the operation of the power system but it is the super-component that has the highest probability of attack. The other line present in the list is LIN 45, which is critical for the system. The motivation to attack this asset is lower but it is still very vulnerable.

In this ranking, G3 is the only generator in the list. Unlike other generators, there is a significant motive to attack this asset and its vulnerability is higher than in the other cases.

4.4 Conclusions

We have presented a method for ranking contingencies in power systems resulting from terrorist attacks on the electrical infrastructure. Although we do not pretend that the risk measures obtained constitute a security measurement of the power systems, the results do allow us to decide on which asset is the most exposed to risk and on which the security study must be concentrated in terrorist scenarios. Thereby the reduction of attacks can be achieved as well as the number of study cases, which constitute one of the main problems in the security assessment of the critical infrastructures.

We believe that risk is a satisfactory measure in our problem. This is due to the fact that the risk not only takes into account the probability of whether a component is attacked but also the consequences of such an attack. Therefore, as we could see in both simulated cases, when we only used the probability value in order to rank contingencies, the result shows the transmission lines to be at the top of the list. Nevertheless, an attack of low intensity on a substation can affect the power system more than an attack of major intensity on a transmission line. In order to include these facts, the measure of severity in the evaluation of the risk is an excellent alternative solution.

The method presented in this chapter can be perfectly applied to the contingency ranking of other critical infrastructures which are threatened by terrorist actions. It is possible that the Bayesian networks' variables are mostly the same variables as for the electrical case, since some of these are typical of the socio-political conflict of a zone more than of the infrastructure. Likewise, the values of these variables are provided by the security services of a government. Nevertheless, as it was indicated in the description of the construction of the Bayesian network, other particular variables peculiar to every case can be included.

We considered that the results are satisfactory under the test scenarios. Although the learning was not yet included during the simulation, since it is not a real system, the incorporation of the evidence will improve the network precision.

It is possible that the reader thinks that the results analyzed for our test-systems were predictable in some cases. But it is necessary to emphasize that our test-systems are small and the analysis of all the zones and all the super-components is not excessively challenging. Nevertheless, our method is powerful because not only all the variables are taken into account, but it can be applied to large power systems (the usual case) and in zones which have similar characteristics. In these cases the analyses are more complicated and the Bayesian networks become a very useful tool in dealing with all the components, all the present variables in the problem and to differentiate different super-components of the power system.

Terrorism depends on the changing conditions of the surroundings, and involves uncertainties of ambiguity and vagueness. The probabilistic inference, the probability subjective theory and, especially in the Bayesian networks, there are important and appropriate tools, which allow this changing characteristic of terrorism to be involved.

References

[AMI, 2002] Amin M., "Security Challenges for the Electricity Infrastructure", IEEE Computer, Suplement 2002, pp. 8-10.

[CEC, 2004] Commission of the European Communities, "Critical Infrastructure Protection in the fight against terrorism". Communication from the commission to the council and the European parliament. Brussels, 20.10.2004, COM(2004) 702 final. Available in http://ec.europa.eu/dgs/justice_home/index_en.htm

[CHO, 2001] Choudens H, Le risque nucléaire, Ed. Tec&Doc Lavoisier, Chapter 10, Paris, France, 2001.

[HAN, 2002] Hansson S.O., "Philosophical Perspectives on Risk Royal Institute of Technology – Stockholm", Proceedings of the conference Research in Ethics and Engineering, Delft University of Technology, April 25 2002, pp. 1-32. Available in http://www.infra.kth.se/phil/riskpage/index.htm

[IEE, 1978] IEEE Working Group, "Reliability Indices for Use in Bulk Power System Supply Adequacy Evaluation", IEEE Transactions on Power Apparatus and Systems, Vol.97, No 4, July-August 1978, pp. 1097-1103.

[LUT, 2004] Lutz J., Lutz B., "Terrorism in the world today and yesterday", in Global Terrorism, London, 2004, Routledge Ed., pp. 16-21.

[MCD, 2003] McDonald J.D., Electric Power Substations Engineering, Ed. CRC Press, 1st edition, USA, 2003.

[NIL, 2003] Nilsen T., Aven T., "Models and Model Uncertainty in the context of risk analysis", pp. 1-11.

[PER, 1999] Perrow C., Normal Accidents: Living with High-Risk Technologies, Chapter 1, Princeton University Press, Updated, 27 September 1999.

[POS, 2004] Parliamentary office of science and technology, "Assessing the risk of terrorist attacks on nuclear facilities", Report 222, United Kingdom, July 2004. Available in www.parliament.uk/post

[RAS, 1975] Rasmussen, N. C., Reactor Safety Study, WASH-1400, U.S. Nuclear Regulator Commission, Washington DC, USA, October 1975.

[STA, 2007] Stanford Encyclopaedia of Philosophy, "Risk", Mars 2007. Available in http://plato.stanford.edu/entries/risk/#Oth

[TRA, 2004] Tranchita C., Torres A. "Events classification and operation states considering terrorism in security analysis". Proceedings IEEE of the Power Systems Conference and Exposition, October 2004, Vol. 3, pp. 1265 – 1271, ISBN : 0-7803-8718-X

[TRA, 2006a] Tranchita C., Hadjsaid N., Torres A., "Ranking Contingency Resulting from Terrorism by Utilization of Bayesian Networks". Proceedings IEEE of the Mediterranean Electrotechnical Conference MELECON 2006, pp. 964–967, ISBN : 1-4244-0087-2.

[TRA, 2006b] Tranchita C., Hadjsaid N., Torres A., "Security Assessment of Electrical Infrastructure under Terrorism", Proceedings IEEE of the Third International Conference on Critical Infrastructures, Town Alexandria VA, USA, September 2006.

CHAPTER V

5. RISK INDEX FOR SECURITY ASSESSMENT BASED ON PROBABILISTIC AND POSSIBILISTIC APPROACHES

The goal of this thesis is to evaluate the security of the power system when it is exposed to a terrorist threat. As indicated in Chapter 2, in the security assessment we can distinguish three main steps: i) the selection of the power system model; ii) the selection of the contingencies to be analysed; and iii) the impact assessment of each contingency on the system behaviour.

Considering the size of power systems, and the non-random and dynamic characteristic of terrorist attacks, a contingency ranking was suggested in order to minimize the sample space of all the possible physical attacks on super-components of the system. In the previous chapter, with this purpose in mind, a method of classification and arrangement of the most important contingencies resulting from potential terrorist attacks on the power system was proposed.

Our approach was based on Bayesian networks with the aim of obtaining the probability of the occurrence and severity of attacks on the power system. Subsequently, a numerical calculation of an "a priori" risk measure for the system was made, which allowed us to rank the contingencies. It is to be noted that the contingency ranking process includes necessarily the selection of the power system model. The first two steps of the security assessment were approached in Chapter 4.

Nevertheless, this established value of risk is not exhaustive. It is due to the fact that the criticality of the super-component in the operation of the power system is modelled by a Bayesian variable. This means that the criticality of the component is evaluated by a value of probability, which was obtained by taking into consideration the experience and analyses of operators originating from the base case power flow. Therefore, we believe that this value serves us to classify the contingencies. Indeed, it does not accurately represent the security of the power system.

The Bayesian network constructed in the previous chapter provides us with different values, among which the most important are the probability of occurrence of attacks and the probability that attacks produce critical, less critical or non-critical contingencies to the operation of the system. These last probabilities were combined with the economic severity and were used to obtain the risk value. In this chapter, we will use not only the ranking but also some outcome probabilities of the network.

The model we use to assess security complies with the most important abovementioned "traditional" steps used in security assessment, but we propose a probabilistic and possibilistic approach.

For the probabilistic line, the Bayesian network of the previous chapter is used to find the probability of occurrence of the attacks and also to rank the contingencies [TRA, 2006a]

[TRA, 2006c]. Therefore, we can take into consideration and model the uncertainty coming from the causes of contingencies.

In the security study it is advisable to consider the uncertainties present in load and generation. Hereby, the ambiguity and the imprecision of the models and of the dynamic behaviour of the load are kept in mind.

A deterministic approach is not the best solution because obviously all the uncertainties are neglected and a probabilistic approach may lead to erroneous models taking into account the types of uncertainties analyzed in Chapter 3. Therefore, for the possibilistic line, the fuzzy load flow [TRA, 2006b] and the fuzzy performance parameters are used to calculate the risk of power system security [TRA, 2006c]. The reader will find these modelling steps explained in detail in this chapter.

In short, the method works as follows. Once the ranking is done, we analyse in more detail the (technical) severity resulting from the unavailability of the attacked asset. This has the aim of obtaining more useful information about the operating conditions of the system, and of finding answers to questions such as: How is the system affected by the occurrence of an attack? Are there performance criteria that are violated? If yes, in what proportion?. With this information it will be possible to establish an accurate measurement of the power system security.

In this work the security study is limited to steady-state operating conditions. Therefore, we use the load flow, and in particular the Fuzzy Load Flow (FLF) for modelling the uncertainty of the load and to diminish the possible number of simulations. By integrating the probabilistic contingency ranking, which was done in the previous chapter, we suggest a procedure to find a security index based on probabilistic-possibilistic risk assessment process. Depending on the domain of application of the power system security study some variants of the method are suggested.

In the first part of the document, the fuzzy load flow problem is reviewed. A detailed analysis of the possible fuzzy load flow implementations is made in order to demonstrate their respective advantages. These implementations differ in the way in which the load is modelled and in the type of fuzzy arithmetic used (as seen in Chapter 3). We propose to use a new type of fuzzy arithmetic which can, in some cases, improve the accuracy of the results.

Next, some performance parameters of the power system are calculated by employing the results of the post-contingency fuzzy load flow. Specifically two security parameters are used: the overload and the security of voltage, but the methodology can be extended to other criteria. These parameters are compared with the security limits, which are also fuzzy numbers, and the risk indices of the system are calculated.

Finally the method is validated with the WSCC 9-bus test system by using the results of the contingency ranking of Chapter 4.

5.1 Fuzzy Load Flow [TRA, 2006b]

Our approach consists in using load flow techniques, specifically the fuzzy load flow one, with the purpose of analyzing operating conditions of the system following a contingency entailed by a terrorist attack. For each of the most important contingencies found by using

the Bayesian network of the previous chapter, there will be a post-contingency analysis of the system operation. The post-contingency fuzzy load flow is performed for that reason. So, the FLF allows us to compare the post-contingency performance of the power system with the operating criteria. These criteria must be respected in order to the power system stays in the normal operating state.

In contrast, dealing with the uncertainty present in the load and generation is one of the most important problems in load flow studies. Correct modelling of uncertainties enables us to evaluate the effect of load and different generation sources in the operation and expansion plans of power systems [SAR, 2004].

Up to now, different theories have been used in order to model the uncertainty of load and generation in the load flow problem. These theories are: the probability theory and statistics, the theory of possibilities and the fuzzy numbers, the interval mathematics and also models of hybrid theories which combine the others. The different forms of uncertainty modelling, along with the various approaches in the solutions to the nonlinear equations of the power flow model, have given rise to numerous types of load flows. The probabilistic load flow was the first approximation developed [BOR, 1974] [ALL, 1977, 1981] [MEL, 1984]. It uses random variables with probability distributions or statistical moments to model load and generation. The results are also probability distributions or statistical moments of voltages and power flows. These methods can be classified as simulation methods, analytical methods, or as a combination of both [MIR, 1989].

Later at the end of the eighties, fuzzy load flow was introduced. This method uses fuzzy numbers with appropriate possibility functions to model load and generation. Different methods such as FLFs based on DC load flow [MIR, 1989, 1990, 1991, 1992] have been developed. In the literature, approaches based on AC load flow models can be found: i) linearized methods [SAR, 2004] [MIR, 1990, 1991, 1992], ii) nonlinear methods [HAO, 2004] [SUN, 2000] [DIM, 2003] and iii) multi-linearized methods [HAO, 2004] [SUN, 2000].

Based on Chapter 3, there are also multiple types of fuzzy numbers arithmetic, which differ according to how the fuzzy numbers are implemented. As a result, FLFs cannot only be differentiated by the model on which they are based but also by the type of arithmetic used. This can significantly change the results. Although we believe that the model is the most important factor in the success of the FLF results, an inadequate implementation of fuzzy numbers or the use of an inappropriate type of fuzzy arithmetic can lead to overestimated or underestimated results. On the contrary, a good implementation can contribute to the accuracy of the solution and as a result improve the outcome.

5.1.1 Formulation of the load flow problem

The fuzzy load problem is formulated as the solution of a nonlinear set of equations.

$$\begin{aligned} 0 &= f(\mathbf{X}, \mathbf{Y}, \mathbf{U}) \\ \mathbf{Z} &= g(\mathbf{X}, \mathbf{Y}, \mathbf{U}) \end{aligned} \qquad [5\text{-}1]$$

Where,
$\mathbf{Y}$ is the input variables vector (i.e. real and reactive nodal power injections),
$\mathbf{U}$ is the control vector (i.e. real power generation and generation voltage magnitude at PV buses, transformer tap settings, shunt compensation),

$\mathbf{X}$ is the state variables vector (i.e. voltage amplitudes V and phases θ at the PQ buses, and generation voltage phases at PV buses),
$\mathbf{Z}$ denotes the vector of desired output variables (usually real and reactive power flows), f and g are the functions vectors. Then, n being the number of buses in the network, the problem is of dimension 2n, since there are 2 equations per bus [HAT, 1999]

The values of nodal voltages and phases at any point of the network as well as the values of the active and reactive powers flowing on all the lines are the outcomes of power flow studies. Thus, it is easy to determine the possible conditions of overload and the voltage violations and to choose the actions that need to be taken in order to solve these situations.

In the load flow problem, real and reactive nodal power injections are modelled as deterministic values. However, it is well known that power injections have different uncertainty levels and that they result from data collection, measurement and load forecasting [SUN, 2000]. The uncertainty in these variables can have a nature of vagueness, imprecision, and ambiguity.

The difficulty to forecast accurately the load exists because the electric load is directly or indirectly affected by various factors which have different types of uncertainty. Short-term load forecasting is mostly influenced by meteorological conditions, as well as calendar holidays, daily and weekly cycles and also by special events. Meanwhile in long-term forecasting, variables influencing the electrical demand, and consequently the prediction, are among others: population of the country, number of consumers, gross state product, price index, electricity tariff, etc. We can see that most of these variables depend on human will and on conditions that change quickly (i.e. the environmental factors). Therefore, high levels of uncertainty are due to vague and incomplete human knowledge [MIR, 1991], and to qualitative information that does not exhibit randomness [ALV, 1992], but characteristics of vagueness, fuzziness and non-specification.

In addition, in probabilistic analyses, a main problem observed is the lack of accuracy in calculating the relationship between the power values and the probability of occurrence for all the buses concerned. This situation leads to an inherent problem concerning the accuracy of the load flow inputs and outcomes.

We consider that to begin transforming the uncertainty present in the load and the generation of crisp information can introduce a bias, which would inevitably be reflected in the quality of results. It is preferable to maintain the fuzziness throughout the process and to slice up only at the end, for example when operators make decisions.

In accordance with Chapter 3, the fuzzy theory is a formal framework that allows the modelling of this type of uncertainty. Particularly, arithmetic fuzzy enables us to model and to deal with vague numerical quantities. This fact makes it possible to carry out complex models closer to reality and to conserve the uncertainty until when the results are produced. By using this technique, we can try to obtain crisp results from vague data.

Based on the propriety that fuzzy numbers can be understood as the assignation of different true values to statements, power injections in the load flow formulation can be modelled as fuzzy numbers. Linguistic declarations such as "load is around x value", or "load peak will be between x and y value" can be modelled by different forms of fuzzy numbers and can be interpreted as possibility functions. This property was illustrated in Figure 3-6.

The possibility measures can replace probability when the decision maker has to evaluate event occurrence, on which little historical data or data of bad quality exist. Another advantage of this approach is that the knowledge of system experts can be easily incorporated [DIM, 2003].

5.1.2 The formulation of the fuzzy load flow

In the fuzzy load flow the input variables, i.e. the vector **Y** (Pload, Qload, Pgen, Qgen) in [5-1] are fuzzy numbers, which model the uncertainty present in these variables. The fuzzy numbers are interpreted as possibility functions and they can model a full input variable, or a portion or a deviation from a central value. Various forms of fuzzy numbers can be employed, such as triangular and Gaussian. The form most used, at least found in the references of this chapter, is the trapezoidal form.

Based on the available knowledge and information of the power flows, the values of the fuzzy numbers parameters can be defined. For example, the forecasted value of power injections or the medium point in an operating possible interval is the point that has a possibility value equal to 1. This point could be in the case of triangular function the parameter b_t in [5-2]; the average value between b_{tr} and c_{tr} in equation [5-3] of the trapezoidal function; and the parameter c_g in equation [5-4] of Gaussians. The values a_t and c_t in [5-2], a_{tr} and d_{tr} in [5-3] are the minimum and maximum values of the universe of discourse, i.e. of the powers.

$$\mu_t(x, a_t, b_t, c_t) = \max\left(\min\left(\frac{x-a_t}{c-a_t}, \frac{b_t-x}{b_t-c_t}\right), 0\right) \quad [5\text{-}2]$$

$$\mu_{tr}(x, a_{tr}, b_{tr}, c_{tr}, d_{tr}) = \max\left(\min\left(\frac{x-a_{tr}}{b_{tr}-a_{tr}}, \frac{d_{tr}-x}{d_{tr}-c_{tr}}, 1\right), 0\right) \quad [5\text{-}3]$$

$$\mu_g(x, c_g, \sigma) = e^{-\left(\frac{x-c_g}{\sqrt{2}\cdot\sigma}\right)^2} \quad [5\text{-}4]$$

In [5-4] the minimum value can be approximated to $c_g - 3\sigma$ and the maximum value $c_g + 3\sigma$, where σ is the standard deviation of a normal random variable in the probability theory. Nevertheless, the concept of standard deviation cannot be widely extended in fuzzy numbers since this concept is based on the fact that the area under the curve is 1. Although this condition is not true for these numbers, we can use these values for normalized fuzzy numbers just as a reference.

The load flow result is a fuzzy numbers' vector for the voltage angle and magnitude. These numbers express the possibility of occurrence for the universe of discourse.

Figure 5-1 shows the solution approaches to the fuzzy load flow problem that have been used up to present. In all applications, the fuzzy numbers have been decomposed into α-cuts. As a result, standard arithmetic has also been applied.

A detail of the implementation of the DC fuzzy load flow and of the implementation of the non-linear and multi-linearized[1] FLF is made in [TRA, 2006c]. We only deal with the AC model since it is the one that we use to ultimately analyse the security of the power grid.

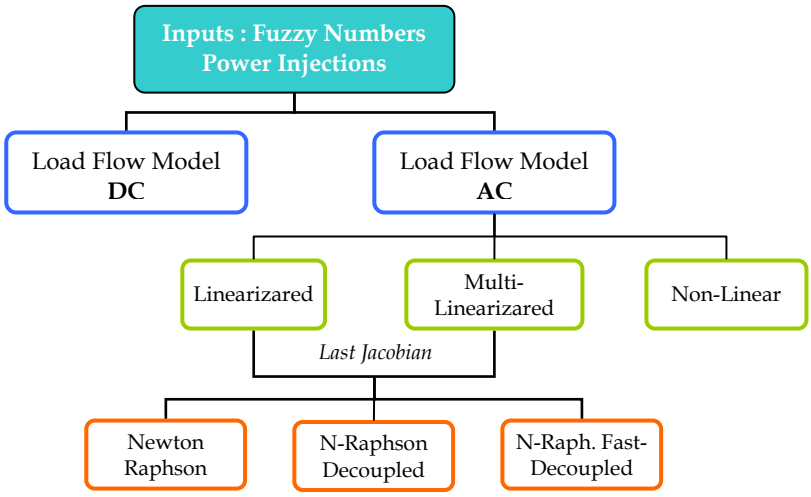


Figure 5-1: Solution approaches to fuzzy load flow problem.

5.1.3 Linearized fuzzy AC load flow

One way to solve the load flow problem is not to make simplifications in the system of equations [5-1]. Since **X** and **Z** in [5-1] cannot be explicitly expressed in terms of **Y**, the system is solved by iterative methods.

This method is based on [SAR, 2004] and [MIR, 1990, 1991, 1992]. The Newton Raphson method (total, decoupled or fast decoupled) is applied. Using the linearization of [5-1], for a fixed control vector $\mathbf{U}'$, around the operating point defined $\mathbf{Y}'$, the deterministic load flow is solved in order to obtain the linearization points $\mathbf{X}'$ and $\mathbf{Z}'$ (where the possibility of input fuzzy numbers is 1).

If we denote the input vector of fuzzy numbers as $\hat{\mathbf{Y}}$ the output vectors of fuzzy numbers $\hat{\mathbf{X}}$ and $\hat{\mathbf{Z}}$ are found by using the linearized equations system resulting from Taylor expansions in [5-7]. **S** and **W** are called sensitivity matrices.

$$\begin{aligned} \mathbf{X_0} &= \mathbf{X}' - \mathbf{S}\cdot\mathbf{Y}' \\ \mathbf{Z_0} &= \mathbf{Z}' - \mathbf{W}\cdot\mathbf{Y}' \end{aligned} \qquad [5\text{-}5]$$

$$\mathbf{S} = -\left[\frac{\partial f}{\partial x}\bigg|_{x=x'}\right]^{-1}\frac{\partial f}{\partial y} \qquad \mathbf{W} = -\left[\frac{\partial g}{\partial x}\bigg|_{x=x'}\right]^{-1}\frac{\partial g}{\partial y} \qquad [5\text{-}6]$$

$$\begin{aligned} \hat{\mathbf{X}} &= \mathbf{X_0} + \mathbf{S}\cdot\hat{\mathbf{Y}} = \mathbf{X}' + \mathbf{S}\cdot\left(\hat{\mathbf{Y}} - \mathbf{Y}'\right) \\ \hat{\mathbf{Z}} &= \mathbf{Z_0} + \mathbf{W}\cdot\hat{\mathbf{Y}} = \mathbf{Z}' + \mathbf{W}\cdot\left(\hat{\mathbf{Y}} - \mathbf{Y}'\right) \end{aligned} \qquad [5\text{-}7]$$

[1] In the multi-linearizared FLF, fuzzy numbers are split up to different regions. In each region the linear FLF is run around an operating point.

If the admittance of the branch *ij* is given by the expression $Y_{ij} = G_{ij} + jB_{ij}$, output variables such as the active and reactive power flows in the lines are nonlinear expressions of the nodes' voltages and angles, as shown in [5-8] and [5-9].

$$P_{ij} = G_{ij}V_i^2 - V_iV_j\left[G_{ij}Cos(\delta_{ij}) - B_{ij}Sen(\delta_{ij})\right] \quad [5\text{-}8]$$

$$Q_{ij} = B_{ij}V_i^2 - V_iV_j\left[B_{ij}Cos(\delta_{ij}) + G_{ij}Sen(\delta_{ij})\right] \quad [5\text{-}9]$$

Where, and V_i and δ_i are the voltage and the voltage phase of the node *i*. We denote $\delta_{ij} = \delta_i - \delta_j$.

Power flow deviations of the line *ij* from the operating point are found with [5-10] and [5-11].

$$\Delta P_{ij} \approx \left.\frac{\partial P_{ij}}{\partial V_i}\right|_{V_i=V_i'} \cdot \Delta V_i + \left.\frac{\partial P_{ij}}{\partial V_j}\right|_{V_j=V_j'} \cdot \Delta V_j + \left.\frac{\partial P_{ij}}{\partial \delta_i}\right|_{\delta_i=\delta_i'} \cdot \Delta\delta_i + \left.\frac{\partial P_{ij}}{\partial \delta_j}\right|_{\delta_j=\delta_j'} \cdot \Delta\delta_j \quad [5\text{-}10]$$

$$\Delta Q_{ij} \approx \left.\frac{\partial Q_{ij}}{\partial V_i}\right|_{V_i=V_i'} \cdot \Delta V_i + \left.\frac{\partial Q_{ij}}{\partial V_j}\right|_{V_j=V_j'} \cdot \Delta V_j + \left.\frac{\partial Q_{ij}}{\partial \delta_i}\right|_{\delta_i=\delta_i'} \cdot \Delta\delta_i + \left.\frac{\partial Q_{ij}}{\partial \delta_j}\right|_{\delta_j=\delta_j'} \cdot \Delta\delta_j \quad [5\text{-}11]$$

Therefore, voltages and angles deviations are expressed in terms of active and reactive power deviations by using the sensitivity matrix directly.

$$\hat{P}_{ij} = P_{ij}' + f(\Delta\hat{\mathbf{P}}, \Delta\hat{\mathbf{Q}}) = P_{ij}' + \Delta\hat{P}_{ij} \quad [5\text{-}12]$$

$$\hat{Q}_{ij} = Q_{ij}' + f(\Delta\hat{\mathbf{P}}, \Delta\hat{\mathbf{Q}}) = Q_{ij}' + \Delta\hat{Q}_{ij} \quad [5\text{-}13]$$

Similarly, other variables with nonlinear relations of the voltage and the angles are present in the power system such as active power generation in the slack bus and the reactive power in generation nodes. By obtaining these functions and by later making the Taylor expansions around an operation point (traditionally the deterministic values obtained by the load flow), the fuzzy numbers of these variables can be found.

5.1.4 Approach proposed: Using fuzzy arithmetic and LR numbers for FLF solutions

In Chapter 3 we presented possible implementations of fuzzy numbers. Therefore, there are different ways of solving the load flow problem. We chose the linearized fuzzy AC load flow model. At this stage it is necessary to decide what type of arithmetic needs to be used for solving the operations described in the previous section.

The interval arithmetic has been the arithmetic traditionally employed, which is one of the so-called arithmetical standards. Mathematical operations are realized by means of the equations in the section 3.4.3.3.

We introduce the use of the LR fuzzy number arithmetic and the "transformation method" in the FLF problem. This last method is part of the "constrained fuzzy arithmetic" method in order to counteract the short-comings of standard fuzzy arithmetic. Fuzzy numbers are decomposed in intervals and the transformation method is used as Hans presented in references [HAN, 1999, 2000].

5.1.4.1 Using LR fuzzy numbers

In this case, LR fuzzy numbers model the input variables. This option is attractive considering that these numbers are operated by using LR fuzzy arithmetic (all operations are described in section 3.4.3.2.). Consequently, the discretization is not necessary and as a result, it does not have to evaluate multiple intervals. The computational cost is minimal but it is possible to sacrifice some accuracy. The main problem is that the support of LR fuzzy numbers grows quickly when the numbers are operated.

On the one hand, we suggest the use of this type of arithmetic only for linear models, i.e. for DC fuzzy load flow and the linearized AC load flow model, because most of the nonlinear operations in this arithmetic are only approximations. Moreover, this type of number also has some restrictions even in basic operations. For example, for adding LR numbers must have an identical shape, and for subtractions LR numbers must be semi- symmetric.

On the other hand, we want to emphasize that most of the operations used to solve the load flow problem are exact in LR fuzzy arithmetic: multiplication by a scalar and addition of fuzzy numbers. Consequently, the results can be satisfactory principally when computation speed is required.

5.1.4.2 Using transformation method

In this approach, input variables are modelled with fuzzy numbers and decomposed in $(m+1)$ cuts. Operations of the equations system are solved by making use of the transformation method as explained in Chapter 3. The method is used to overcome the short-comings that appear by using the standard intervals arithmetic.

Better results are expected because more points in each interval are evaluated; again, the problem is a balance of speed and accuracy. Since the implementation of the transformation method for such large systems as power systems can be computationally costly, we have used as our basis the work of Klimke in [KLI, 2003]. It used multi-dimensional arrays for the fast processing of discretized fuzzy numbers, elimination of recurring permutations, automatic decomposition of models, treatment of single occurrences of variables through interval arithmetic, and a monotonicity test. In [KLI, 2003] the triangular and Gaussian-shaped fuzzy numbers are implemented. We have extended the application for trapezoidal numbers. Notice that this implementation and type of arithmetic can be applied to solve the linear and nonlinear fuzzy load flow model. In spite of the efforts to reduce the time of calculation we realize that in some cases the computational cost may be very high.

5.2 Calculation of Performance Parameters

In the previous section, we used the fuzzy load flow in order to obtain the fuzzy numbers of the post-contingency bus voltages and line power flows. This means that for each of the contingencies chosen in the ranking, we simulate the fuzzy load flow. By using these results, we calculate the following performance parameters:

1) the possibility function of low post-contingency bus voltages and severity
2) the possibility function of lines overload and severity.

Other parameters can be calculated using the same methodology.

5.2.1 Low voltage situation

The possibility function of post-contingency voltage in a bus is defined as the fuzzy number obtained through the post-contingency fuzzy load flow:

$$\pi_V(x) = \mu_{\tilde{V}}(x),\ \forall x \in X \qquad [5\text{-}14]$$

Here X is the all possible values of a voltage in a bus and $\mu_{\tilde{V}}(x)$ is the membership degree of $x \in X$ to the fuzzy number $\tilde{V}$.

We can also find the possibility value of low voltage at bus *j* as follows:

$$\Pi_j^{LV}(x) = \max\left(\pi_{Vj}(x \le 0.95)\right) \quad \forall x \in X \qquad [5\text{-}15]$$

Through [5-15] the maximum possibility value for all the voltage values lower than 0.95p.u. can be obtained. This limit value of 0.95 can be changed for the limit value established by the planners and operators of the utility.

Equation [5-15] is interpreted graphically by Figure 5-2. In figure (a) the bus voltage resulting from the fuzzy load flow is always lower than the limit. As a consequence the possibility of low voltage is 1. Conversely, figure (b) shows the voltage of a bus where the voltage is always higher than 0.95. Here the possibility of low voltage is 0. In the third case, the possibility of low voltage in this bus is the maximum value of possibility of all values of voltage lower or equal to 0.95; the possibility of low voltage is $\pi_V(0.95) = 0.33$.

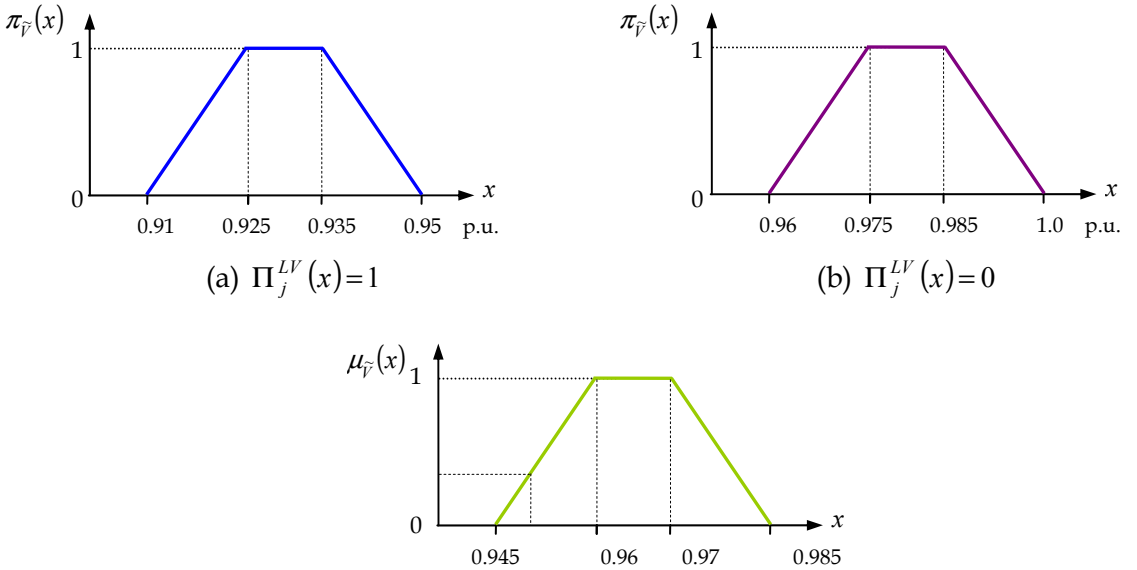


Figure 5-2. Calculation of the possibility value of low bus voltage.

We can use this value in order to calculate the risk. In our approach we do not use directly this value, because we use a function of severity that model the problem of low voltage. However the analysis of the possibility value allows us to understand the necessary operations and the logic in the calculation of the risk.

Now, we model the severity entailed by the problem of low voltage. We employ a fuzzy number for this purpose and we suggest the use of a trapezoidal fuzzy number $\langle 0.73,0.75,0.90,0.95\rangle_{tr}$, which is illustrated in Figure 5-3. This is only a suggestion and obviously other types of numbers can be used. Then, for the universe of discourse of post-contingency voltages X, the low voltage severity function in bus j is given by [5-16]. For simplicity of notation, we are going to use indistinctly $Sev_j^{LV}(x) = \mu Sev_j^{LV}(x)$.

$$Sev_j^{LV}(x) = \left\{ \max\left(\min\left(\frac{x-0.73}{0.02}, \frac{0.95-x}{0.05}, 1 \right), 0 \right) \quad \forall x \in X \right. \qquad [5\text{-}16]$$

Equation [5-16] assigns a severity value of zero to all voltage values higher or equal to 0.95 p.u., a severity value of 1 to voltage values lower or equal to 0.90 p.u., and between 0.90 and 0.95 p.u. a severity value given by the linear equation $\left(\frac{0.95-x}{0.05} \right)$. The fuzzy number is illustrated in Figure 5-3. It should be noticed that for values lower than 0.75 the equation does not make any sense but we consider that these very low voltage values are practically out of range of the operation.

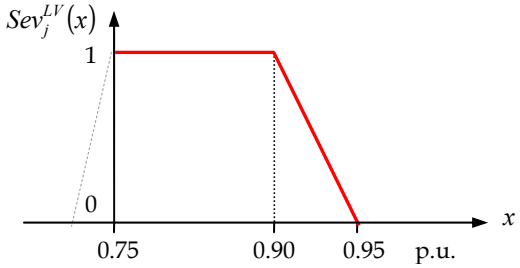


Figure 5-3. Fuzzy number of the severity of low voltage.

5.2.2 Line overload situation

A line k is considered to have overload problems when the flow exceeds the allowed value Pmax (or Imax: maximum allowed flowing current), which is the value established by planners for each line, in order to keep the thermal limits and the stability of the power system.

The possibility function of power flowing through a line obtained by the post-contingency fuzzy load flow is:

$$\pi_P(x) = \mu_P(x), \ \forall x \in X \qquad [5\text{-}17]$$

Where, X is all the possible power flow values in a line.

Similarly to equation [5-15], the overload possibility value by a transmission line k is:

$$\Pi_k^{OL}(x) = \max(\pi_{Pk}(x \le P\max)) \ \ \forall x \in X \qquad [5\text{-}18]$$

By using equation [5-18], the maximum possibility value for all power values superior to Pmax can be obtained.

The loadability fuzzy number is defined as a trapezoidal number. The parameters are percentages of Pmax: $\langle 0.90P\max, P\max, 1.5\cdot P\max, 1.55\cdot P\max\rangle_{tr}$. Then, for the universe of discourse of post-contingency powers for a line, X, the loadability severity function is given by [5-19]. The fuzzy number is shown in Figure 5-4. For simplicity of notation, the formulation $Sev_j^{LV}(x) = \mu Sev_j^{LV}(x)$ will be used indistinctly.

$$Sev_k^{OL} = \begin{cases} \mu_{tr}(x, 0.9P\max, P\max, 1.5\cdot P\max, 1.55\cdot P\max) \\ x \in X \end{cases} \qquad [5\text{-}19]$$

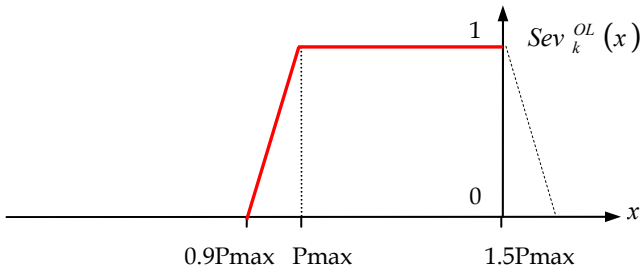


Figure 5-4. Fuzzy number of the severity of overload.

It can be observed that severity definitions are given by trapezoidal numbers formed by two straight lines, but in all of the cases, the possibility value of the right-side straight line (for positive power flows) makes no sense for the purposes of analysis. The severity for the power values higher than Pmax is always 1, but we assume that the lines power flow will not exceed 1.5 times Pmax.

5.3 Fuzzy Risk Index

In the previous section we defined the parameters of performance. Our last step is to find the risk index, which will allow us to obtain a security value.

Assume that the contingency set found after ranking contains p contingencies. A study scenario corresponds to a time period (season, year), a loading condition (i.e. peak, partial peak, off peak) and the occurrence of a contingency. The system consists of j buses and k lines. By using the risk definition, we can find the low voltage security risk index at j bus for n-th contingency with [5-20].

$$R_{j,n}^{LV}(x) = p(E_n)\cdot\left(\pi_{V\,j,n}(x) \otimes Sev_{j,n}^{LV}(x)\right) \qquad \forall x \in X \qquad [5\text{-}20]$$

Where:

$p(E_n)$ is the probability of occurrence of an attack against the super-component, which was found by using the Bayesian network

$\pi_{V\,j,n}(x)$ is the possibility function of the post-contingency voltage, taking the occurrence of the attack into account

$Sev_{j,n}^{LV}(x)$ is the low voltage severity function

$\otimes$ is the multiplication by using the theory of fuzzy sets

In this way, it is possible to take the following uncertainties into account: i) the probability of a physical attack against a certain super-component; ii) the possibility of a low voltage

problem given the unavailability of the super-component; and finally iii) the quantification of how severe the problem is. Notice that the result of the risk calculation is a fuzzy set. We can present entirely this function to the operator, but the most significant value is the maximum value of the risk. Therefore, the defuzzification of the fuzzy set, which results from the procedure, can be obtained by calculating the height of the set.

In analogy, the loadability security risk index for the system lines is [5-21].

$$R_{k,n}^{OL}(x) = p(E_n) \cdot \left(\pi_{P_{k,n}}(x) \otimes Sev_{k,n}^{OL}(x)\right) \qquad \forall x \in X \qquad \text{[5-21]}$$

Where,

$p(E_n)$ is the probability of occurrence of an attack against the super-component found by using the Bayesian network

$\pi_{P_{k,n}}(x)$ is the possibility function of loadability

$Sev_{k,n}^{OL}(x)$is the loadability severity function

Graphically the calculation of the risk is illustrated as follows:

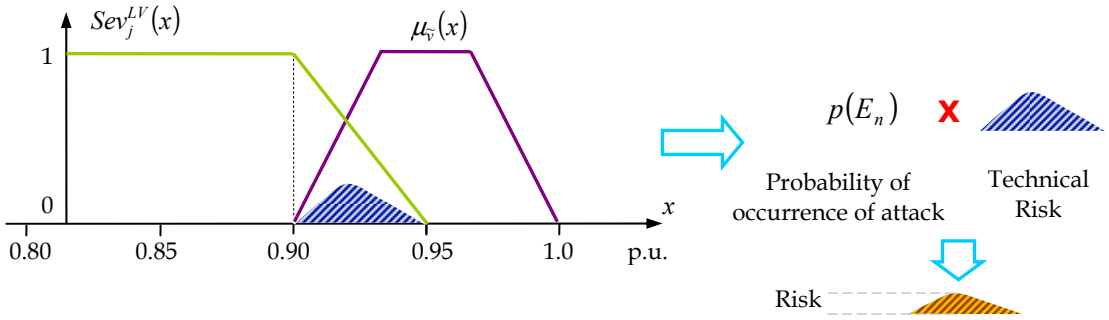


Figure 5-5. Calculation of the risk index of the power system security.

Before illustrating the method, we would like to highlight some advantages of the approach which is presented here. Independent of how the contingency analysis is made, this method can always be used when the uncertainty of the load is included. The fuzzy logic presents a unique framework, in which we can integrate historical information of the behaviour of the power system as well as the experts' experience and knowledge. In addition, by using fuzzy numbers to model the load and the generation, we apply the theory of possibility, which allows us to interpret values of membership as degrees of possibility that a certain power flow could occur.

It is possible that the reader wonders why we multiply probabilities and possibilities. As mentioned in Chapter 3, the theory of possibilities and the theory of probability are based on the theory of sets. An event with possibility 1, is interpreted as a totally possible event and an event with possibility 0 is interpreted as an impossible event. Bearing in mind that i) everything that is probable is also possible, and ii) that probability is always smaller than possibility; we interpret the value of probability in equations [5-20] and [5-21] as a penalizing factor in the risk formula. In addition, we multiply by a probability value and not by a distribution probability function.

Similarly, one of the advantages of fuzzy degrees is that we can then use different t-norms, and choose the t-norm which is the most adequate. Depending on the goals of the use of

fuzzy sets, we should use more or less conservative approaches, which allow us to get better results. We believe the same is true here: the fact of using a value of probability allows us to obtain more conservative results. This can be positive because it can compensate for less moderate values of the possibility in the formulae of risk. Therefore, we believe that this combination of possibility and probability is not only possible in our definition of risk, but is also appropriate.

Figure 5-6 shows the scheme of the security assessment model based on probabilistic and possibilistic approaches - fuzzy load flow, performance parameters calculation and fuzzy risk indices - , subsequent to the contingency ranking.

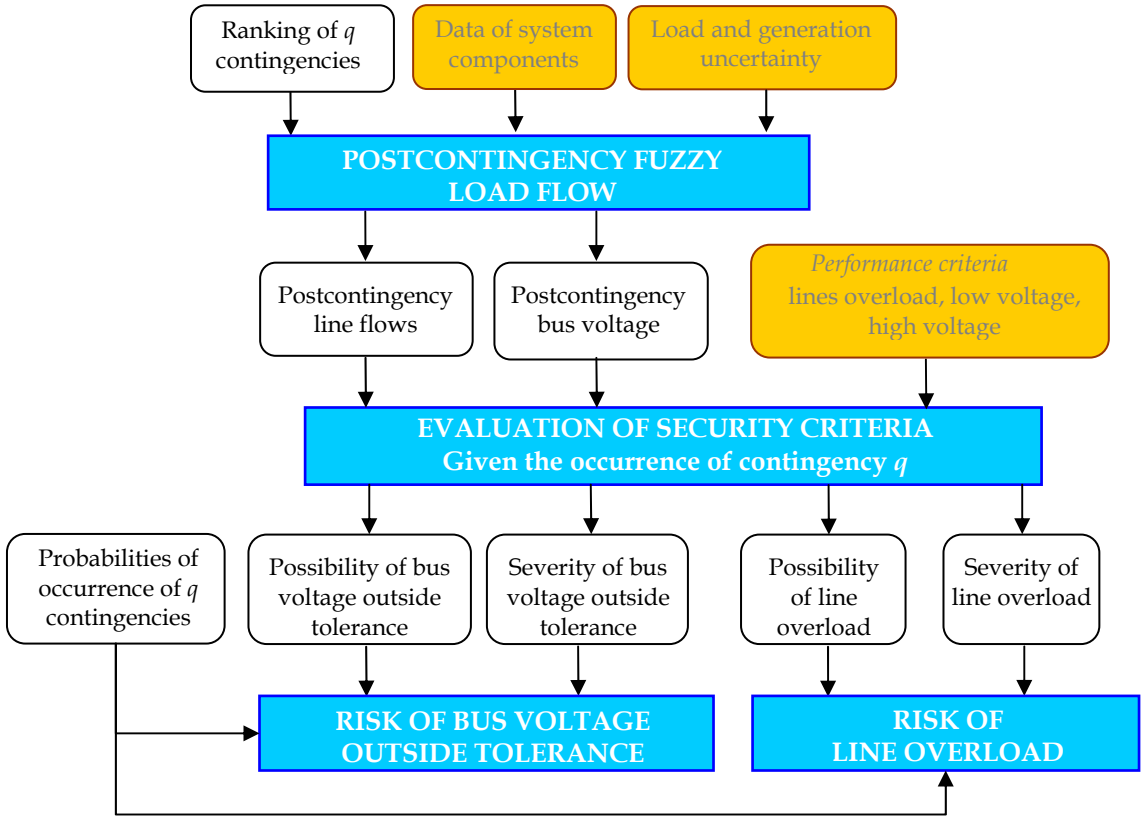


Figure 5-6. Model of security assessment based on probabilistic and possibilistic approaches.

5.4 Study Case

In this section, we illustrate the application of the method for the Western System Coordinating Council WSCC 9 bus system, which is illustrated in Appendix B.

Contingency ranking

In Chapter 4, we employed this test-system in order to illustrate the ranking contingency method. We created different situations in the zones with regard to the terrorist group position, the political situation in the zone and the exposure of super-components regarding their geographic location. For each super-component the probabilities of the independent variables of the Bayesian network were defined: variables of the zone, the type of component, the criticality for the power system and the physical protection. The 15 cases (attacks against each of the system's super-components) were simulated. The most important

contingencies were the loss of the super-components: SUB 39, SUB 6, LIN 96, SUB 5, SUB 14, LIN 45 and G3.

Probabilistic and possibilistic security assessment

The stable state study for the power system is made in order to evaluate the post-contingency operation conditions and to be able to calculate the index of risk.

5.4.1 Fuzzy load flow simulations

The first step is to model the uncertainty present in the power injections and to run the fuzzy load flow simulations. As we propose to employ different types of fuzzy arithmetic, in this section we show the use of the LR fuzzy arithmetic and the transformation method used to solve the linearized fuzzy AC load flow for the WSCC 9 bus system. Data of the system are specified in appendix B.

We make a comparison between the solutions proposed and the interval arithmetic. This comparison is interesting in order to validate our solutions but also to evaluate the impact of the types of arithmetic in the solution of a single problem.

We have modelled the injection of powers at all buses as triangular and trapezoidal numbers. These types of fuzzy numbers have been implemented in numerous engineering problems because the elementary fuzzy arithmetical operations are very simple and the implementation of numbers is easy. For simplicity, we model the fuzzy numbers as the deviation of the power values from the forecasted deterministic value.

5.4.1.1 Base case

All of the simulations of the base case are detailed in Appendix D. Here, we analyse only some results in order to illustrate the main differences between the methods.

Triangular fuzzy numbers
Same percentages of variation are assumed for each input variable as follows:
Active powers: $\langle 0.90 \cdot P_i, P_i, 1.1 \cdot P_i \rangle_T$ illustrated in Figure 5-7(a).
Reactive powers $\langle 0.90 \cdot Q_i, Q_i, 1.1 \cdot Q_i \rangle_T$ illustrated in Figure 5-7 (b).

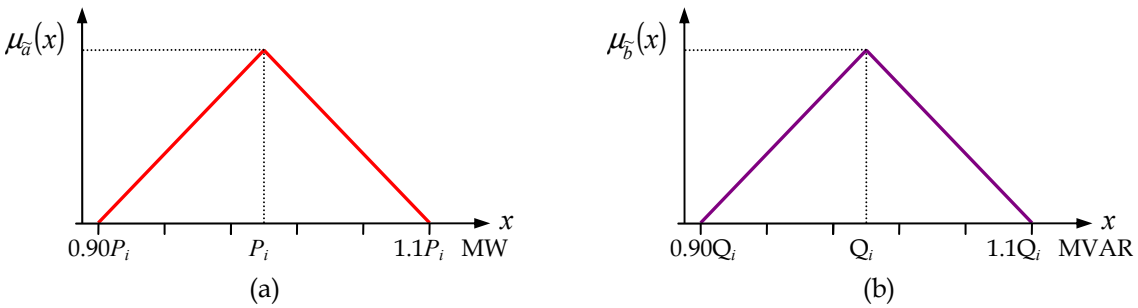


Figure 5-7. Injection powers in the fuzzy load flow by using triangular fuzzy numbers.
(a) Trapezoidal fuzzy numbers of the active powers.
(b) Trapezoidal fuzzy numbers of the reactive powers.

P_i is the forecasted value of the active power injections and Q_i of the reactive power injections. These fuzzy number parameters are chosen because at the moment, the errors of short-term load forecasting are around ± 2% or ± 2.5%. Thus, the possibility that load could be in this interval is high and we put as limit interval of the load a variation between ±10% of the forecasted value. It has to be taken into account that the input fuzzy numbers in a solution algorithm of linearized FLF are the deviations of powers P_i and Q_i. As a result, fuzzy numbers must be transformed, e.g. in the case of triangular active powers, the deviation is modelled as: $\langle 0.1 \cdot P_i\ ,\ 0\ ,\ 0.1 \cdot P_i \rangle_T$.

The FLF was run using the 3 approaches. Each number has been decomposed in 5 arithmetic intervals (m=4), in order to use the interval arithmetic and transformation method. In Figure 5-8, the differences between the fuzzy numbers of the output voltage at bus 5 which were obtained using the approaches, can be observed.

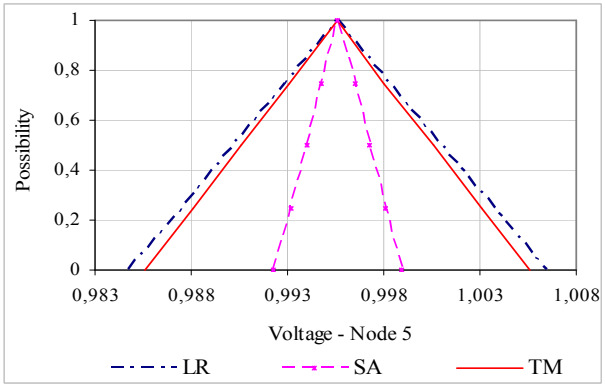


Figure 5-8. Triangular fuzzy numbers of the output voltage at bus 5 obtained by using LR arithmetic, Standard Arithmetic and the Transformation Method.

Trapezoidal fuzzy numbers

The power injections are modelled by fuzzy numbers as follows:

Active powers: $\langle 0.90 \cdot P_i, 0.975 \cdot P_i, 1.025 \cdot P_i, 1.1 \cdot P_i \rangle_{tr}$ illustrated in Figure 5-9 (a).

Reactive powers $\langle 0.90 \cdot Q_i, 0.975 \cdot Q_i, 1.025 \cdot Q_i, 1.1 \cdot Q_i \rangle_{tr}$ illustrated in Figure 5-9 (b).

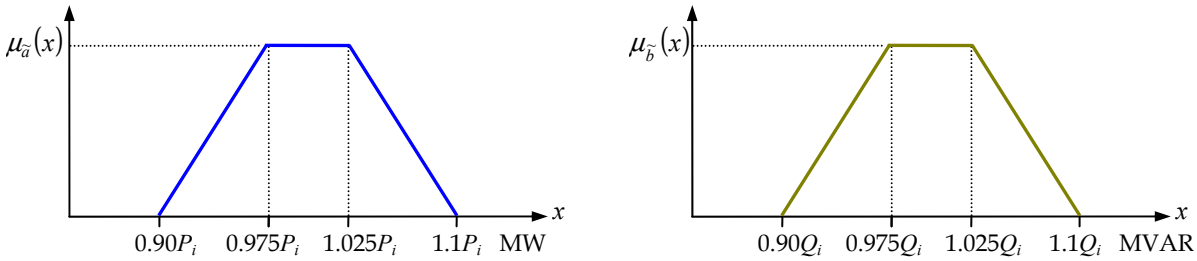


Figure 5-9. Injection powers in the fuzzy load flow by using trapezoidal fuzzy numbers.
(c) Triangular fuzzy numbers of the active powers.
(d) Triangular fuzzy numbers of the reactive powers.

Each fuzzy number was decomposed again into 5 cuts. Figure 5-10 (a) shows the different results for the voltage at bus 8. The calculation of the line power flows is made using the linear approach in [5-10] and [5-11]. Figure 5-10 (b) shows graphically the different fuzzy numbers of the output power flow at line 9-6.

The results in both cases with triangular and trapezoidal numbers, show that the type of arithmetic employed can change the results. However, in the three cases the results tend to be satisfactory compared with the range of values of the traditional fuzzy load flow. Despite the overestimation in the support of fuzzy numbers, the results do not significantly differ in comparison with the results of the transformation method and the standard arithmetic. Notice that the alpha-cut $[a^{(1)},b^{(1)}]$ is practically identical in all cases; this is not surprising because the main difference between the types of arithmetic is the form to operate the support.

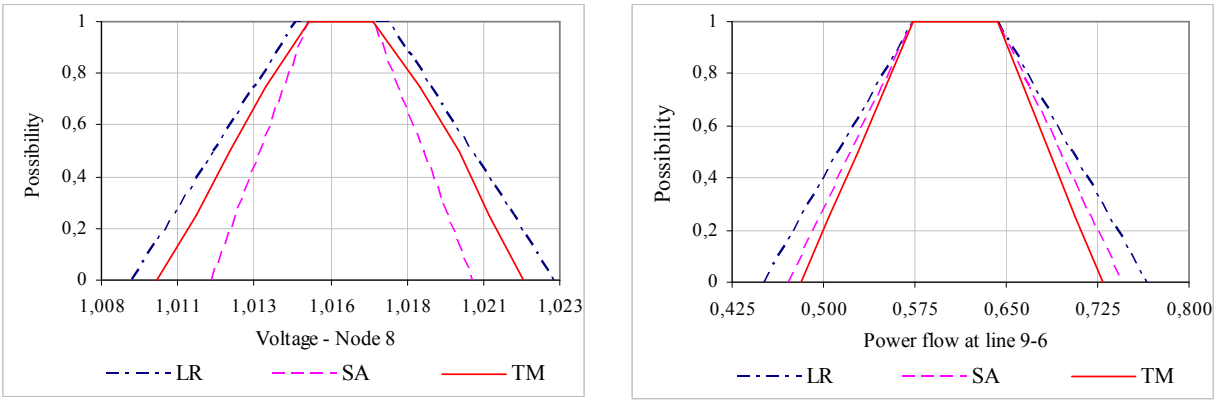


Figure 5-10. Trapezoidal fuzzy numbers of the (a) output voltage at bus 8; and (b) of the line power flows at line 9-6 obtained by using LR arithmetic, standard arithmetic and the transformation method.

In the case of LR numbers, the approach is valid because its simplicity of the implementation and the adequacy of the results; then its use can be justified when very fast solutions are necessary. We verify that the use of the standard arithmetic tends to present some important problems of overestimation or of "pessimism", above all in the support. In Appendix B it is possible to see these problems for the base case in more detail.

5.4.1.2 Post-contingency load flow - Analysis of the ranking list

In this section we will analyze the group of contingencies selected from the contingency ranking of Chapter 4.

For the simulation we have modelled the power injections in the following way:
Active powers: $\langle 0.90 \cdot P_i, 0.98 \cdot P_i, 1.02 \cdot P_i, 1.1 \cdot P_i \rangle_{tr}$.
Reactive powers $\langle 0.90 \cdot Q_i, 0.98 \cdot Q_i, 1.02 \cdot Q_i, 1.1 \cdot Q_i \rangle_{tr}$.

A. Loss of SUB 93

We assume that a physical attack against substation 93 has catastrophic consequences when the transformer is destroyed and nodes 9 and 3 are unavailable. Therefore, the zone 3 becomes completely dependent on the sources of other zones and the whole power transmission to the load of node 6 is just done by line 4-6. The resulting system after the physical attack is shown in Figure 5-11.

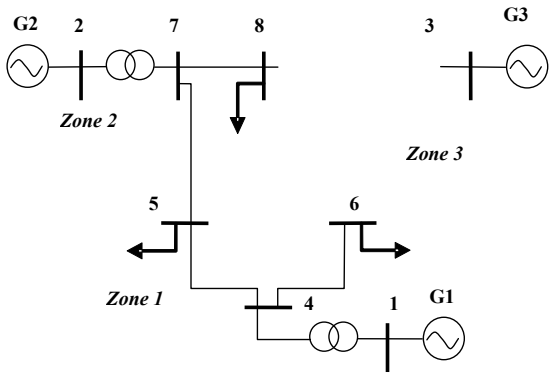
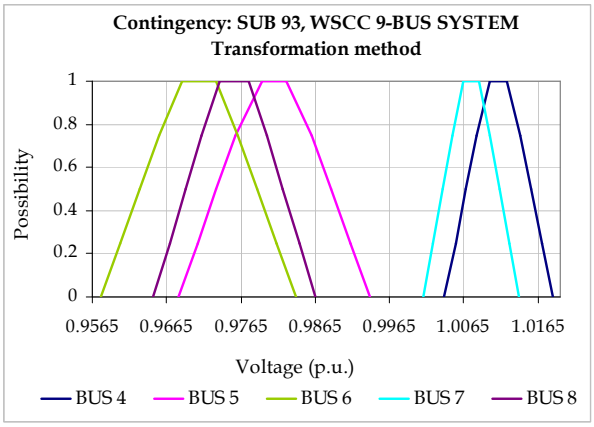
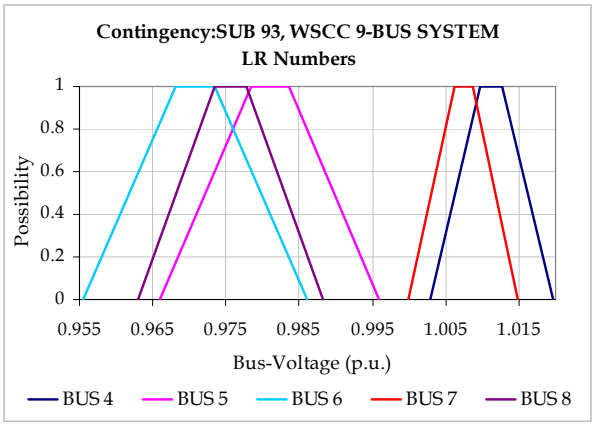


Figure 5-11. Power system WSCC 9-bus after a catastrophic attack against the substation 93.

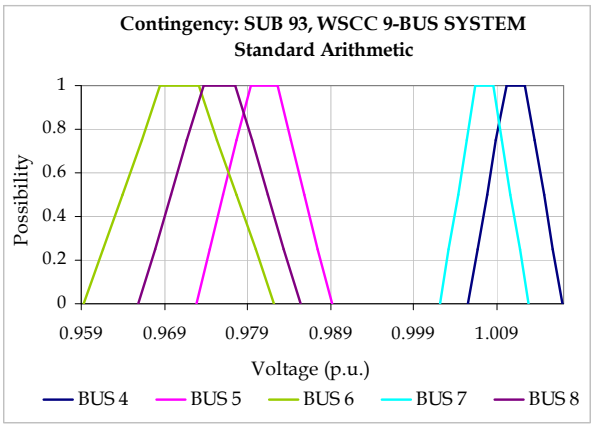
The results of the possibility function of voltage profiles after the attack, calculated by using the three types of arithmetic, are shown in Figure 5-12.



(a) Transformation method



(b) LR numbers



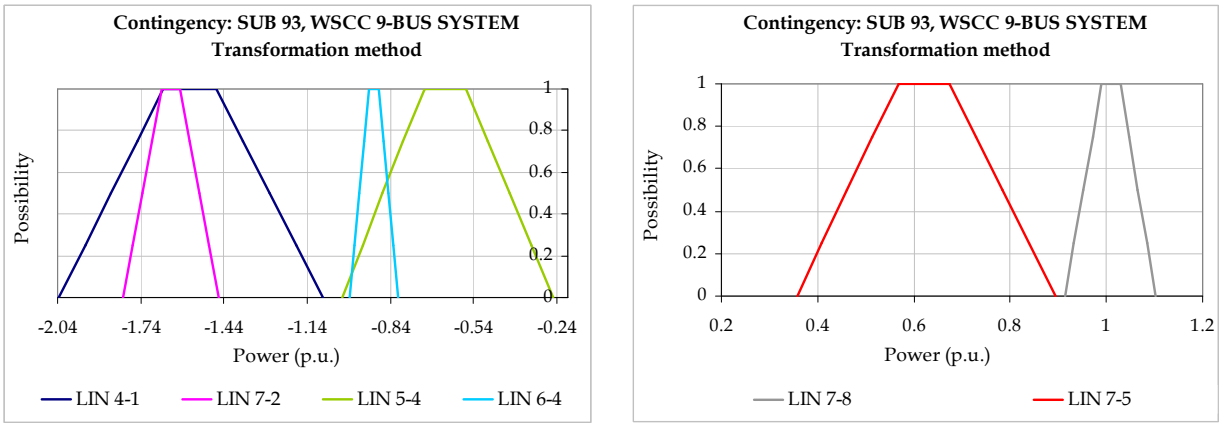
(c) Standard arithmetic

Figure 5-12. Possibility functions of post-contingency bus-voltage resulting of the unavailability of substation 93.

The possibility functions show that no bus-voltage is lower than 0.95. Therefore, the severity function of low voltage is always 0. According to the risk definition of equation [5-20], the value of risk for this case is zero. The unavailability of the component does not leave any security problem of low voltage.

In analyzing the results for every type of arithmetic (as Figure 5-12 shown), we see that the possibility functions support of the LR numbers for the voltage profiles are larger than the other possibility functions.

Figure 5-13(a) and Figure 5-13(b) show the results of the post-contingency power flows using the arithmetic of the transformation method. We have separated into two graphs because of the sense of power flows. As expected, line 4-1 carries the highest power flow since it is the only line that connects the load of node 6. Likewise, line 7-2 is heavily loaded due to the considerable power contribution of generator 2 .



(a) (b)

Figure 5-13. Possibility functions of post-contingency power flows given the unavailability of substation 93.

The limit of overload for the transmission lines of this system is 300MVA, i.e. 3 p.u. With this limit value no line is showing overload conditions. Since this contingency is one of the cases where overload is the most possible, the limit will be diminished to 200MVA only in order to illustrate how the risk index of overload is calculated.

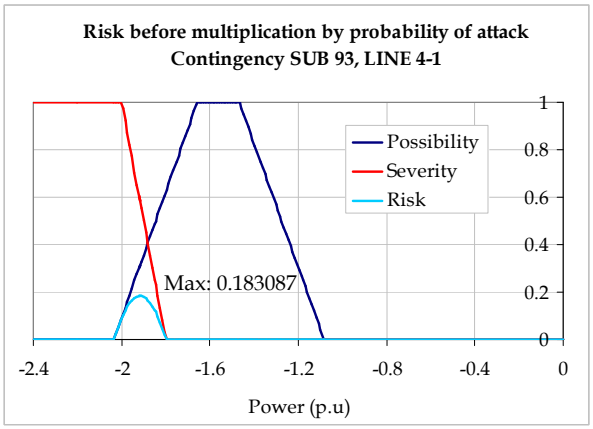


Figure 5-14. Calculation of the risk of overload for the line 4-1 given the unavailability of substation 93.

In Figure 5-14 we can see that when power flows exceed 200MVA (2 p.u.) the severity of the overload is at maximum, i.e. 1. For the powers between 180 and 200 MVA there are different values of severity of overload. Therefore, the maximum value of the risk of overload for the line 4-1 before the multiplication by the probability of an attack against the substation 93 is 0.1831. In accordance with the previous chapter the probability of an attack for this

contingency is 0.4005, thus the value of risk of overload is 0.0733. The power flow for the other lines is significantly below the limits, and then the severity of overload for these lines is zero.

As a result of the security analysis for this contingency:

Node	**BUS 4**	**BUS 5**	**BUS 6**	**BUS 7**	**BUS 8**	
Risk index of low voltage	0	0	0	0	0	
Line	**LIN 4-1**	**LIN 7-2**	**LIN 7-8**	**LIN 7-5**	**LIN 5-4**	**LIN 6-4**
Risk index of overload	0.0733	0	0	0	0	0

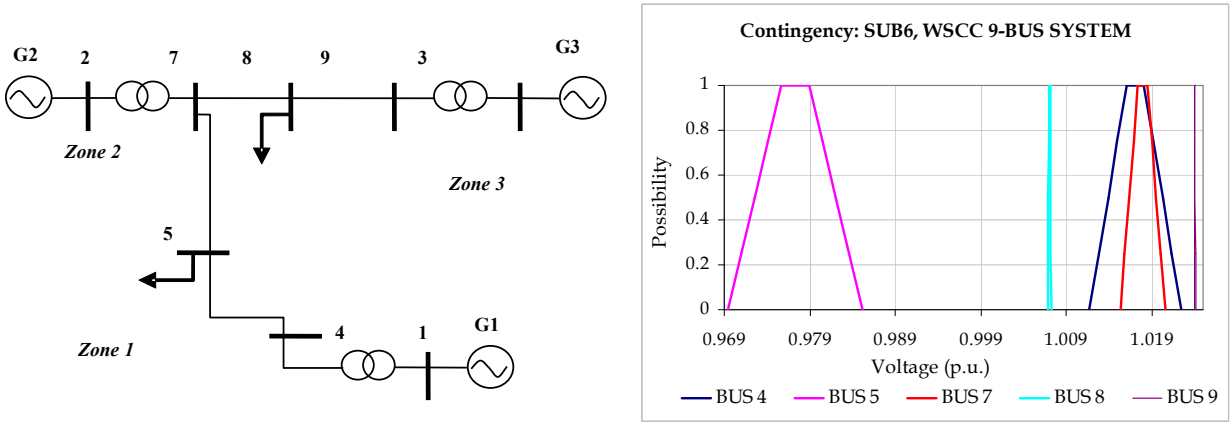
However, assume a physical attack of high intensity against substation 93 without being catastrophic, that leads to the unavailability of the transformer. As a consequence, generator 3 will be isolated from the power grid but node 9 continues to work. The load in node 6 will not be exclusively dependent on the transmission line 4-6, because line 9-6 will also transmit power to the load. So, this case corresponds to the same case of the unavailability of generator 3, the voltage profiles and the analysis of the case will be made later on when we deal with contingency G3.

B. Loss of SUB 6

Assume a catastrophic physical attack against the substation 6 that leaves zone 3 without load supply as it can be seen in Figure 5-15 (a). In this case neither low voltage nor line overload problems exist, because the loss of load at node 6. The possibilities functions of bus-voltage profiles are shown in the Figure 5-15 (b). No universe of discourse of voltages includes values lower than 0.95. The risk values of low voltage and overload for this case are all zero.

Node	**BUS 4**	**BUS 5**	**BUS 6**	**BUS 7**	**BUS 8**	
Risk index of low voltage	0	0	0	0	0	
Line	**LIN 4-1**	**LIN 7-2**	**LIN 7-8**	**LIN 7-5**	**LIN 5-4**	**LIN 6-4**
Risk index of overload	0	0	0	0	0	0

Nevertheless, it is necessary to emphasize that the load 6 is one of the important loads of the system and it may be suitable to add a risk index which takes the loss of load into account. This issue, however, is out of the scope of this thesis.



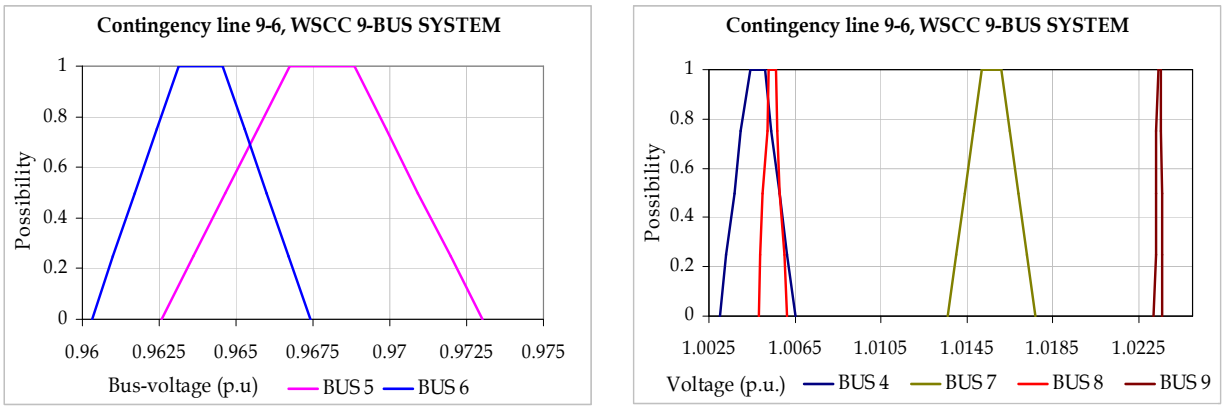
(a) (b)

Figure 5-15. (a) Resultant power system after the unavailability of SUB6; (b) Possibility functions of post-contingency bus-voltages given the attack on SUB6.

C. Loss of line 9-6

As aforementioned, load 6 is important for the power system. The unavailability of line 9-6 implies that power is only transmitted to this load by line 4-1.

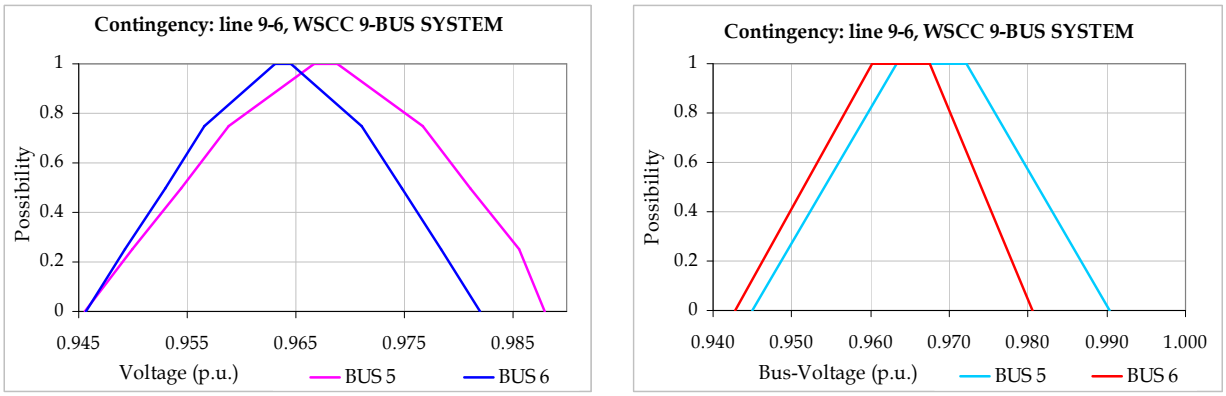
Figure 5-16 shows the different fuzzy numbers which are the result of the fuzzy load flow simulation by using the standard arithmetic. We separated the resulting possibility functions of voltages into two groups. Figure 5-16(a) shows the voltages at buses 5 and 6; although they do not present any voltage problem they tend to be relatively low. Figure 5-16(b) shows that the ranges of the most possible values are ranges of completely normal voltages and the loss of the line does not represent any type of danger for the security.



(a) (b)

Figure 5-16. Post-contingency bus-voltages by using the fuzzy load flow and the standard arithmetic. Unavailability of line 9-6.

By simulating the "normal" load flow for the load at 1.1Pi and 1.1Qi, we found that the voltage at bus 5 is 0.9600 p.u. and at bus 6 is 0.9540 p.u. This fact suggests that the simulation using the standard arithmetic leads to slightly conservative values.



(a) Transformation method (b) LR Numbers

Figure 5-17. Post-contingency bus-voltages by using the transformation method and LR Numbers. Unavailability of line 9-6.

Now, we analyze the results of the simulations using two other types of arithmetic. We see in Figure 5-17 that the results for these two nodes when using the arithmetic of LR numbers and the transformation method are more conservative. By employing these types of arithmetic we have a risk value of low voltage. Depending on utility policies, the use of

different types of arithmetic can be more or less suitable according to the risks that planners and operators are ready to take. An alternative is to make a sensitivity analysis for a case which is considered to be critical, to select the arithmetic which is to be used and then to generalize it for other cases.

Let us look at the risk value that we would have if we exploited the results of Figure 5-17(a) and Figure 5-17(b). When we use the transformation method, the risk calculation is shown in Figure 5-19 and Figure 5-20. The maximum value of the risk (without taking the probability of an attack into account) in node 5 is 0.0056. According to the previous chapter the probability of an assault against the line 9-6 is 0.5347. Consistently the risk of low voltage for node 5 is 0.0030 and analogously for node 6 it is 0.0034.

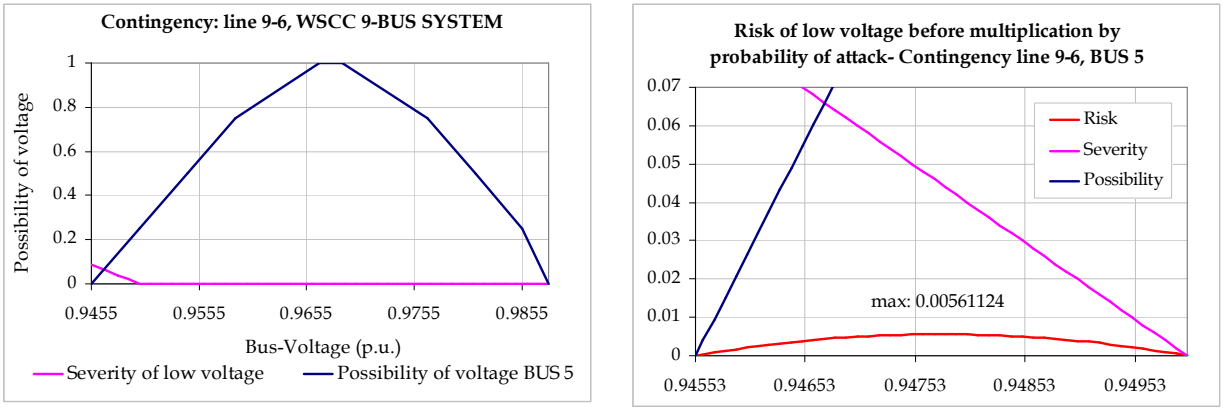


Figure 5-18. Calculation of the risk of low voltage at bus 5, by using the transformation method. Contingency line 9-6.

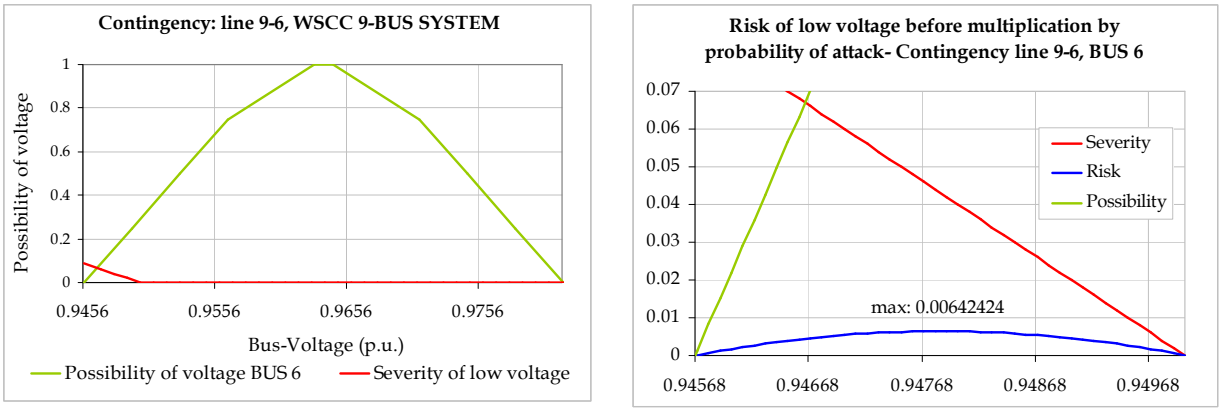
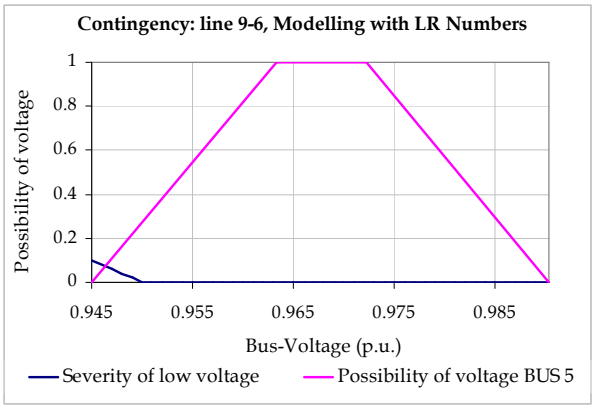


Figure 5-19. Calculation of the risk of low voltage at bus 6, by using the transformation method. Contingency line 9-6.

Thus the risk values for the buses and for the lines are:

Node	**BUS 4**	**BUS 5**	**BUS 6**	**BUS 7**	**BUS 8**	
Risk indices of low voltage	0	0.0030	0.0034	0	0	
Line	**LIN 4-1**	**LIN 7-2**	**LIN 7-8**	**LIN 7-5**	**LIN 5-4**	**LIN 6-4**
Risk indices of overload	0	0	0	0	0	0

If we model the power injections as LR numbers, the risk values of low voltage are respectively 0.00037 and 0.0080. In this case we have higher risk values but they are not significantly different compared to those obtained using the transformation method.



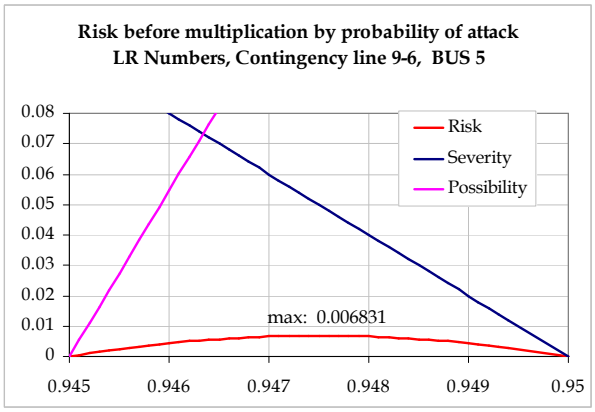
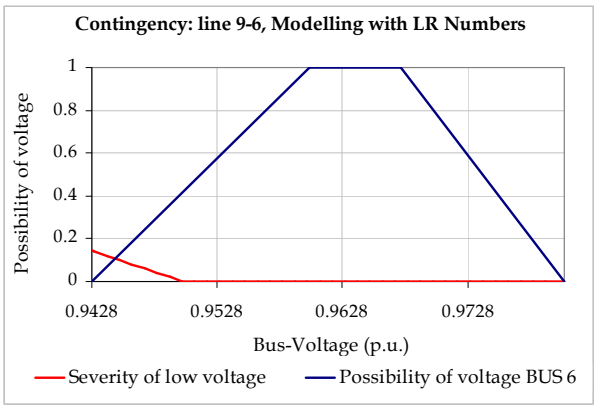


Figure 5-20. Calculation of the risk of low voltage at bus 6, by using LR numbers. Contingency line 9-6.



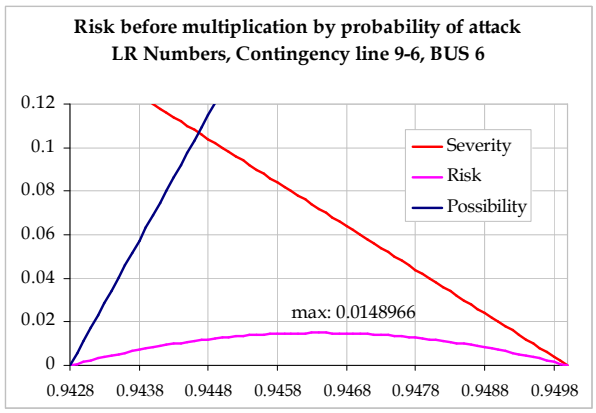


Figure 5-21. Calculation of the risk of low voltage at bus 6, by using LR numbers. Contingency line 9-6.

D. Loss of SUB 5

The loss of this substation is analogous to the loss of substation 6. Thus, there is a loss of load in zone 1, which is the most important load of the system.

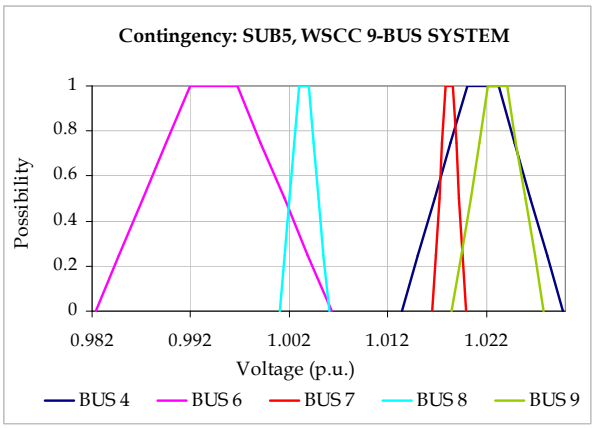


Figure 5-22. Possibility functions of voltage, contingency substation 5.

We can see in Figure 5-22 that the universes of discourse values of the possibility functions of voltage are higher than 0.95, hence severity is 0 in all cases. The power flow universes for the lines are lower than 0.90 times the limit, thus problems of overload do not exist either.

E. Loss of SUB 14

Assume that a catastrophic assault against substation 14 would leave zone 1 without generation and the loads of the zone 1 and 2 would be entirely supplied by other generators. The resulting system is shown in Figure 5-23.

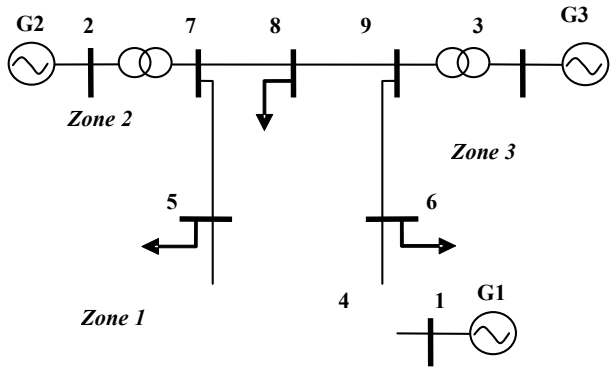
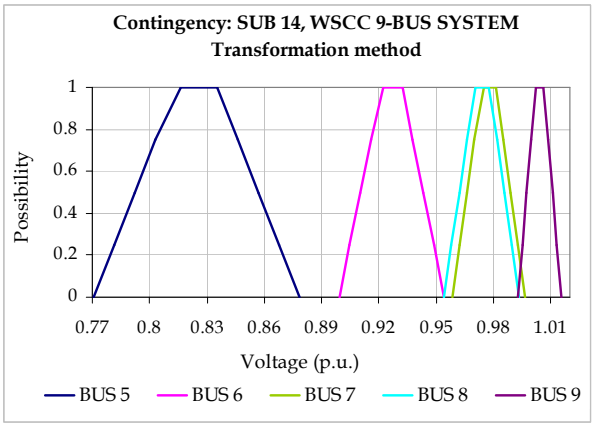
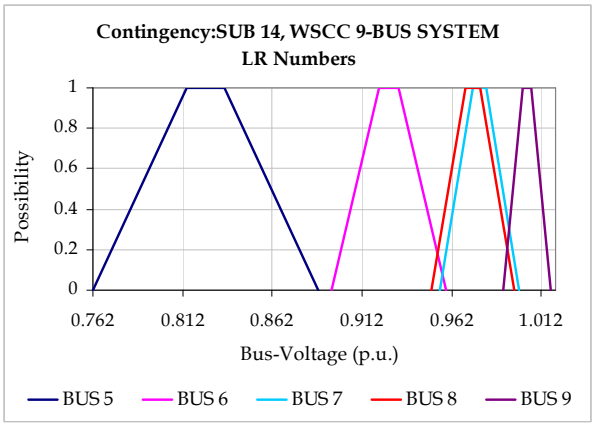


Figure 5-23. Power system WSCC 9-bus after a catastrophic attack against the substation 14.

Figure 5-24 shows the possibility functions of bus-voltages. Calculating the risk indices via the transformation method, we realize that the universes of discourse of the possibility functions of buses 5 and 6 are entirely lower than 0.95p.u. Therefore the severity value for any voltage value of these nodes is 1. In theses cases the risk value is the probability of an attack against substation 14. Inversely, the possible voltage values for buses 7, 8 and 9 are higher than 0.95p.u., thus the severity in these cases is 1 and the risk value is 1.



(a)

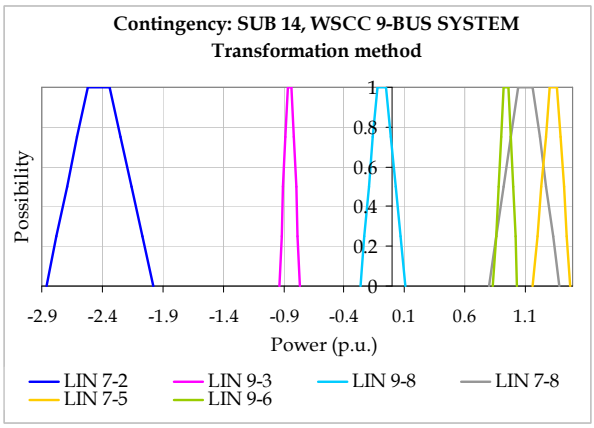


(b)

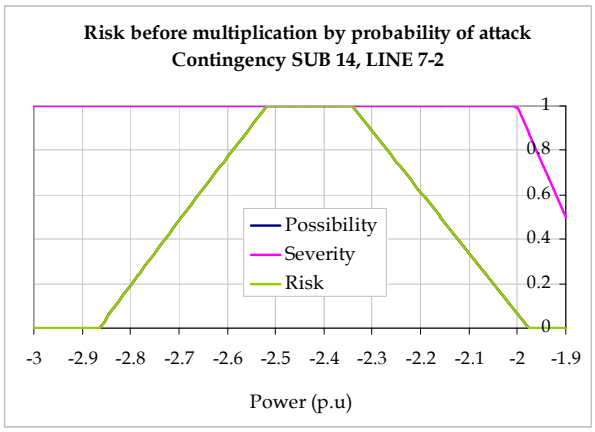
Figure 5-24. Possibility functions of voltage (a) using the transformation method; (b) using LR numbers. Contingency substation 14.

Since in this case the power is mostly supplied by the generator 2, we have an overload problem for line 7-2, as shown in Figure 5-25(a). If we preserve the originally established limit of power i.e. at 300 MVA, the risk value before the multiplication by the probability of an attack against the substation is 0.0155. Multiplied by the probability of an attack, the risk of overload for line 7-2 is 0.0550.

In order to be coherent with the security analysis of the power system, we calculate now the risk value of overload with the power limit value as 200 MVA (we used this limit for the first contingency). In accordance with the risk definition for this type of contingency, the risk of a low bus-voltage for any voltage value is numerically the probability of an attack. This is due to the fact that the possibility of failure in the case of an attack is 1 and the severity of the attack is maximal.



(a)



(b)

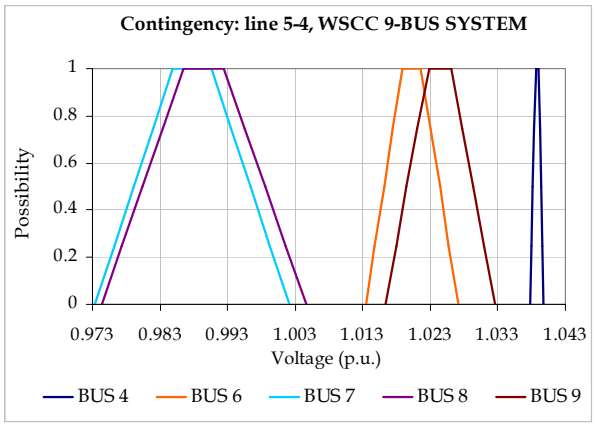
Figure 5-25. (a) Possibility functions of power flows; (b) Calculation of the risk of overload at line 7-2. Contingency substation 14.

Thus, the risk values, given the unavailability of the substation 14, are (using the limit of power at 200 MVA):

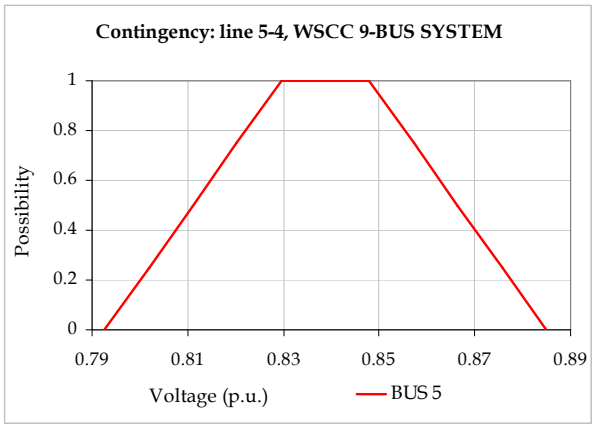
Node	**BUS 4**	**BUS 5**	**BUS 6**	**BUS 7**	**BUS 8**	
Risk index of low voltage	0	0.3555	0.3555	0	0	
Line	**LIN 4-1**	**LIN 7-2**	**LIN 7-8**	**LIN 7-5**	**LIN 5-4**	**LIN 6-4**
Risk index of overload	0	0	0	0	0	0

F. Loss of line 4-5

Figure 5-26, Figure 5-27 and Figure 5-28 show the voltages fuzzy numbers obtained by post-contingency fuzzy load flow calculations via the use of different types of arithmetic.

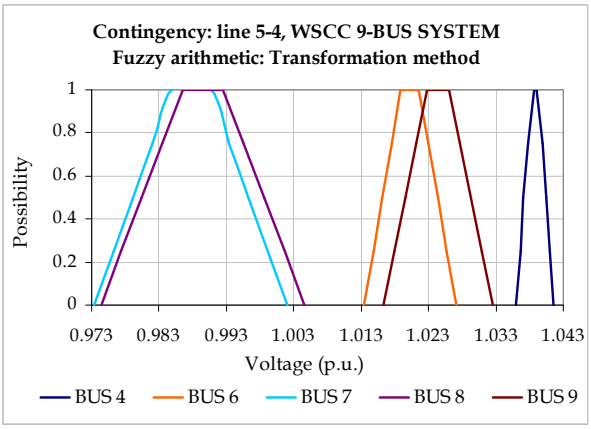


(a)

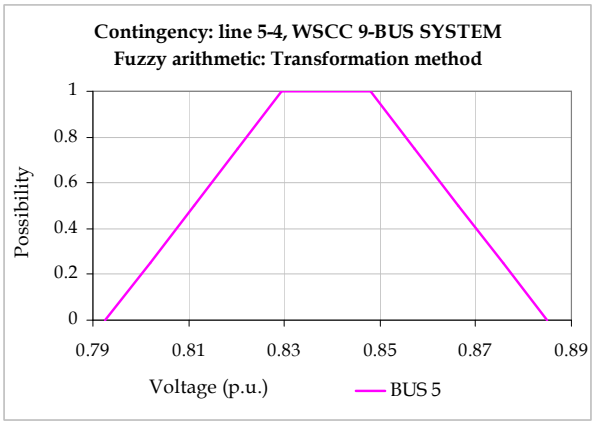


(b)

Figure 5-26. Possibility functions of post-contingency bus-voltage by using the standard arithmetic. Contingency line 5-4.

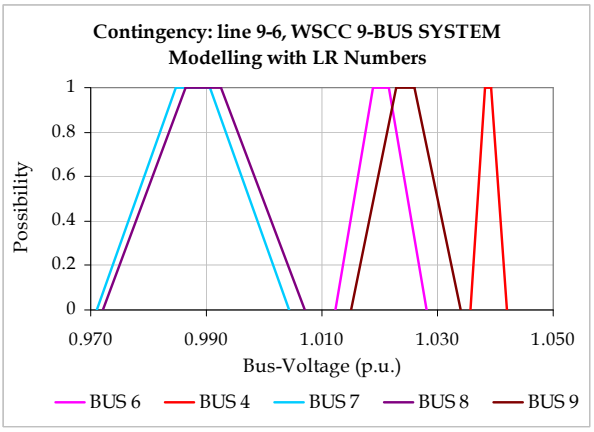


(a)

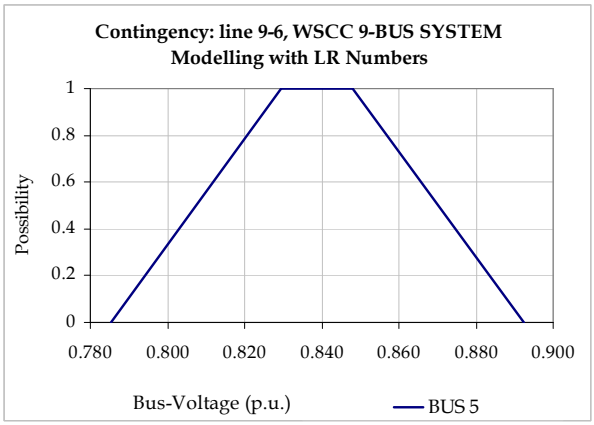


(b)

Figure 5-27. Possibility functions of post-contingency bus-voltage by using the transformation method. Contingency line 5-4.



(a)



(b)

Figure 5-28. Possibility functions of post-contingency bus-voltage by using LR numbers. Contingency line 5-4.

In all cases, the voltage at bus 5 is smaller than the permitted minimum voltage. In the other bus there is no voltage violation. We found that the severity of low voltage is always 1 for the universe of discourse of bus 5 and zero for the others. In this case, the risk is the probability of an attack on line 5-4, i.e. 0.4761. The risk is shown in Figure 5-29. The loss of line 5-4 represents a very high risk for the bus as well as for the system.

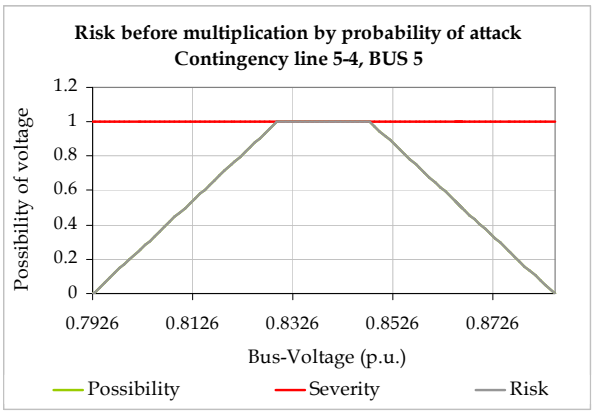


Figure 5-29. Calculation of the risk of low voltage at bus 5. Contingency line 9-6.

This contingency does not cause problems of lines overload. Consequently the risk values for the nodes and for the lines are:

Node	**BUS 4**	**BUS 5**	**BUS 6**	**BUS 7**	**BUS 8**	
Risk index of low voltage	0	0.4761	0	0	0	
Line	**LIN 4-1**	**LIN 7-2**	**LIN 7-8**	**LIN 7-5**	**LIN 5-4**	**LIN 6-4**
Risk index of overload	0	0	0	0	0	0

G. Loss of generator G3

Finally, we analyze the unavailability of generator 3. In steady-state, by analyzing the possibility functions of voltage we can conclude that the loss of this generator does not represent any problem of low voltages. As a consequence, the risk of low voltages for all the nodes is zero. Likewise they do not present problems of overload. These facts are illustrated in Figure 5-30.

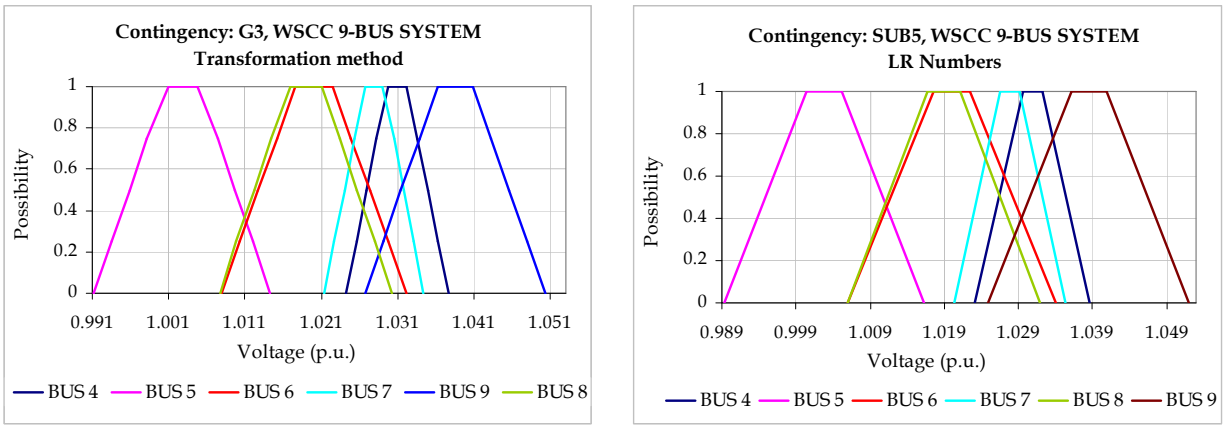


Figure 5-30. Possibility functions of voltage (a) using the transformation method; (b) using LR numbers. Contingency generator 3.

Thus, the risk values given the unavailability of the generator 3 are:

Node	**BUS 4**	**BUS 5**	**BUS 6**	**BUS 7**	**BUS 8**	
Risk index of low voltage	0	0	0	0	0	
Line	**LIN 4-1**	**LIN 7-2**	**LIN 7-8**	**LIN 7-5**	**LIN 5-4**	**LIN 6-4**
Risk index of overload	0	0	0	0	0	0

5.5 Conclusions

This chapter illustrates a method for security assessment taking into consideration the most important uncertainties resulting from the issue. With the use of possibility functions for modelling load and generation we can run fuzzy load flow calculations in order to obtain risk indices. This allows us to interpret them as "probabilistic-possibilistic" indices.

The indices show the risk evolution of the values different variables of the system (voltage and power flows) taking into account the possibility of these variables and also the severity for the security of the power system. Although the indices show the risk as such for nodes and lines and not for the whole system, operators and planners of the system can directly use

these values. Nevertheless, with the use of fuzzy techniques and the method presented here we think that a global risk index of a system can be found.

We draw attention to two important aspects of our method. The first one is the conservation of the uncertainty until the end of the method. This means that we analyze the effect of the uncertainty of the power injections in the solution of the load flow and combine it with the uncertainty of possible reasons of contingencies. Hereby we avoid certain mistakes that may occur when ignoring the uncertainty from the beginning. The second aspect is that by having used the fuzzy load flow we can considerably diminish the number of simulations to be realized and in addition we are able to associate a possibility value (analogous to the probability) for every obtained voltage value.

Finally, in this chapter, different types of fuzzy arithmetic are used with the purpose of solving the load flow problem considering the existing uncertainties in the power injections. The use of different types of arithmetic is possible since fuzzy numbers can be implemented in several ways. Thus, for a single model of fuzzy load flow multiple solutions exist for input variables.

The fuzzy load flow problem has been treated generally by decomposing fuzzy numbers in alpha-cuts and by using the interval arithmetic. The use of the arithmetic of LR fuzzy numbers and the transformation method are proposed. Similarly to the use of the T and S norms in the theory of fuzzy sets, the use of different types of arithmetic can lead to overestimated or more pessimistic results. Consequently, the risk estimations and the security measures based on these results can be more or less conservative.

With the use of the transformation method, the fuzzy load flow can be more accurate, surpassing some of the presented problems of overestimation or "pessimism" in the use of the traditional fuzzy arithmetic. However, since we use a linearized model, major differences between these two types of arithmetic do not exist. The arithmetic of LR numbers applied in the fuzzy load flow presents problems of "overestimation", but the results are not significantly distant from the values obtained with the other types of arithmetic. The use of this arithmetic can be justified by the simplicity and rapidity of implementation. The two suggested approaches are verified with the given examples. The supports of the obtained fuzzy numbers are satisfactory compared with the values' range of the traditional fuzzy load solution. Each way of implementing fuzzy numbers - including the standard arithmetic - has its advantages and drawbacks and the selection of an approach must be justified according to the time and the accuracy required.

References

[ALL, 1977] Allan R. N., Al-Shakarchi M. R. G., "Probabilistic techniques in AC load flow analysis", IEE Proceedings, Vol. 124, February 1977, pp. 154-160.

[ALL, 1981] Allan R. N., Leite da Silva A. M., "Probabilistic load flow using multilinearizations", IEE Proceedings, Vol. 128, No. 5, September 1981, pp. 280–287.

[ALV, 1992] Alvarado F., Yi H., Adapa R., "Uncertainty in power system modeling and computation", Proc. IEEE International Conference on Systems, Man and Cybernetics, October 1992, Vol. 1, pp. 18-21.

[BOR, 1974] Borkowska B., "Probabilistic load flow", IEEE Transactions Power Apparatus System, Vol. PAS-93, May 1974, pp. 752–759

[DIM, 2003] Dimitrovski A., Tomsovic K., "Boundary load flow solutions", IEEE Transactions on Power Systems, Vol. 19, No. 1, February 2003, pp. 348-455.

[HAN, 1999] Hanss M., "On using fuzzy arithmetic to solve problems with uncertain model parameters", Proc. Euromech 405 Colloquium, Valenciennes France, November 17-19, 1999, pp. 85-92.

[HAN, 2000] Hanss M., "A nearly strict fuzzy arithmetic for solving problems with uncertainties", Proc. 19th International Conference of the North American Fuzzy Information Processing Society, Atlanta, USA 2000, pp. 439-443.

[HAO, 2004] Hao, L. Shi, G. Xu, Y. Xie, "Study on the fuzzy AC power flow model", Proc. 5th World Congress on Intelligent Control and Automation. Hangzhou, P.R. China, June 15-19, 2004, pp. 5092-5096.

[HAT, 1999] Hatziargyriou N.D., Karakatsanis T.S., "Probabilistic load flow for assessment of voltage instability". IEE Proceedings ofGeneration, Transmission and Distribution. Vol. 145, Issue 2, March 1999, pp. 196 – 202.

[KAR, 1994] Karatsanis T. S., Hatziargyriou N. D., "Probabilistic constrained load flow based on sensitivity analysis", IEEE Transactions on Power Systems, Vol. 9, No. 4, November 1994, pp. 1853-1860.

[KLI, 2003] Klimke A., "An efficient implementation of transformation method of fuzzy arithmetic", Proc. 22nd International Conference of the North American of Fuzzy Information Processing Society, 24-26 July 2003, pp. 468 – 473.

[MEL, 1984] Meliopoulos A. P., Bakirtzis A. G., Kovacs R., "Power system reliability evaluation using stochastic load flows", IEEE Transactions on Power Apparatus & Systems, Vol. 103, No. 5, May 1984, pp. 1084-1091.

[MIR, 1989] Miranda V., Matos M.A., "Distribution system planning with fuzzy models and techniques", Proc. CIRED 89, Brighton 1989.

[MIR, 1990] Miranda V., Matos M.A., Saraiva J.T., "Fuzzy load flow – new algorithm incorporating uncertain generation and load representation", Proc. 10th Power Systems Computing Conference, Graz, Austria, 1990, pp. 621-627.

[MIR, 1991] Miranda V., Saraiva J.T., Matos M.A., "Generation and load uncertainties incorporated in load flow studies", Proc. MELECON 91, Ljubljana, May 1991.

[MIR, 1992] Miranda V., Saraiva J.T., "Fuzzy modeling of power system optimal load flow", IEEE Transactions on Power Systems, Vol. 7, No. 2, May 1992.

[SAR, 2004] Saraiva J.T., Fonseca N., Matos M.A., "Fuzzy power flow – an AC model addressing correlated data". Proc. 8th International Conference on Probabilistic Methods Applied to Power Systems, 12-16 September 2004, pp. 519-524.

[SUN, 2000] Sun H., Yu D.C., Xie Y., "Application of fuzzy set theory to power flow analysis with uncertain power injections", Proc. IEEE Power Engineering Society Winter Meeting 2000, Vol. 2, 23-27 January 2000, pp. 1191 – 1196.

[TRA, 2004] Tranchita C., Torres A. "Events classification and operation states considering terrorism in security analysis". Proceedings IEEE of the Power Systems Conference and Exposition, October 2004, Vol. 3, pp. 1265 – 1271, ISBN : 0-7803-8718-X

[TRA, 2006a] Tranchita C., Hadjsaid N., Torres A., "Ranking Contingency Resulting from Terrorism by Utilization of Bayesian Networks". Proceedings IEEE of the Mediterranean Electrotechnical Conference MELECON 2006, pp. 964–967, ISBN : 1-4244-0087-2.

[TRA, 2006b] Tranchita C., Hadjsaid N., Torres, A.; "Using Fuzzy Arithmetic for Power Flow Analysis with Uncertainty", International Review of Electrical Engineering (I.R.E.E.), Praise Worthy Prize, August 2006. ISSN : 1827- 6660.

[TRA, 2006c] Tranchita C., Hadjsaid N., Torres A., "Security Assessment of Electrical Infrastructure under Terrorism", Proceedings IEEE of the Third International Conference on Critical Infrastructures, Town Alexandria VA, USA, September 2006.

CHAPTER VI

6. POWER SYSTEM RISK ASSESSMENT RESULTING FROM CYBERTERRORISM ON INFORMATION AND COMMUNICATION TECHNOLOGIES

The components of an electrical power system make up multiple hierarchical layers and operate on several levels, including energy control centres, power generation plants, transmission and distribution networks and corporate information systems. As mentioned in Chapter 2, the power grid must be controlled at all times, so that the level of power needed by loads can be adjusted, and the frequency and the voltages maintained within secure and reliable operational areas.

In order to achieve and facilitate the planning and the operation of power systems, the use of information and communication technology (ICT) has become necessary. ICT was defined as the technology involved in acquiring, storing, processing and distributing information via electronic means (including radio, television, telephone, and computers) [BJO, 2004]. We can distinguish three separate processes in this definition: the acquisition of information, the communication of information between different entities and computerization of information. ICTs in power systems are mostly used to control the system, to operate the electrical energy market and to the utilities' management and business.

The increased use of ICTs, and the dependency of the power grid on such technology, has created a new form of vulnerability - ICTs are exposed to denominated "cyberattacks". The use of ICT means that elements of power systems, such as control centres, substations, protection schemes, are increasingly becoming the targets of such acts, whereas before they were a lot more difficult to attack. The more technologically developed a power system is, the more vulnerable the infrastructure is to cyberattacks.

Recent arrests in Europe and events around the world indicate that terrorism continues to be a real threat and that terrorists are still resolved to attack different nations. Terrorism is not a new phenomenon, but its organization, aims, weapons and targets change and evolve constantly over time. Nowadays, the different governments of the world face a terrorism which has not only a national, but an international, character and which is continually finding new ways of achieving its aims. At current, terrorist have found that the use of ICTs can be an effective and advantageous mean to bring about fear by disrupting the society.

In Chapter 1, we suggested a definition of Cyberterrorism which was as follows: "*Cyberterrorism is the deliberate creation and exploitation of fear through violence or the threat of violence by using electronic means, in the pursuit of political change conducted by an organization with a conspiratorial cell structure, and perpetrated by a sub-national group or non-state entity*".

Cyberterrorism on power systems can be defined as using electronic means to attack an electrical infrastructure. These attacks involve the damage of information and communication technologies upon which the performance of the power system depends (such as SCADA - Supervisory Control and Data Acquisition, protections and applications of

EMS – Energy Management System or DMS – Distribution Management System). The objective of these acts is to damage equipment, prevent the execution of the systems' control processes, and to corrupt data; but their ultimate aim is to interrupt the supply of electrical energy. ICT is a weapon which can achieve the attackers' objectives.

A large number of computers are used in the power system at different levels, e.g. from basic operations such as the protection schemes for relaying to client invoicing operations. Consequently, the risk of attack on power systems through ICTs exists. Also, there exists the risk of more simple attacks on platforms, operating systems or computer codes, on which the operation of power systems depends. In this way, attacks that do not directly target the power grid can still affect and interrupt the operation of an electrical power system.

Given the interaction of power grids with, and their dependency on, ICTs, as well as the importance of the electrical infrastructure, it is necessary to assess the risk of how the power system would be affected if it was subjected to cyberattacks resulting from terrorist actions. Unlike physical attacks, the risk of cyberterrorism is present in all countries across the world, and not only in those that are currently experiencing intense political conflict.

The security assessment of a power system must take cyberattacks into consideration in order to satisfactorily deal with the economic and technical challenges faced by this type of system. Therefore, new factors must be considered, and innovative approaches are needed, so that the security of a system can be properly evaluated, in order to respond to the new threats to which it is exposed.

Regarding the facts of the last years, physical attacks continue to be the greatest threat to power systems because of terrorist activity, but cyberattacks are considered to be an emerging threat, which need to be studied more closely. The electrical sector cannot ignore the fact that cyberattacks on the electrical network are a reality. Forbes, in January 2008, published that Tom Donahue, a CIA official, revealed at the SANS security trade conference in New Orleans that hackers have penetrated power systems in several regions outside the U.S., and "in at least one case, caused a power outage affecting multiple cities". All intrusions were made through the Internet. Finally, according to well-known cybersecurity companies, such as Symantec, vulnerabilities which expose also power systems to cyberattacks are constantly being discovered.

This chapter introduces the risk assessment of power systems with regards to the possible consequences of cyberterrorism. We offer some important definitions (which are not always obvious) with the aim of understanding what a cybernetic attack actually is, who the initiators of such an attack are, and what the possible consequences are. Later, using a Bayesian network, we will attempt to model the possible causes of cyberterrorism against power systems and the consequences of such an act of terrorism. We suggest using this Bayesian network in order to estimate the probability of attack on the communication system and the probability of the severity of the attack on the performance and operation of the power grid, which will be used as a measurement of the risk of the attack. Despite the limitations of the software for modelling the interdependency between the IC system and the power grid as well as the confidentiality of the utilities in this field we will present an "academic" example to show the use of our approach.

6.1 What are the motives behind cyberterrorism?

A terrorist act, whatever weapon is used, is characterized as inducing terror in the civilian population, with the intention of influencing a certain sector of the public, or in order to communicate a political message.

Why have terrorist groups moved on to cyberspace in order to execute their acts of terrorism? The motives which lie behind of cyberattacks are numerous. Attacking via electronic means is just one more way to commit terrorism, but in most cases it is cheaper and easier to execute than a physical attack and can be done without being in the country (remotely). Neither explosives, nor arms or vehicles etc. are needed. This type of attack is less risky, because it is relatively anonymous. The attackers' identity can be hidden in cyberspace, and physical barriers, such as customs or the borders between countries, do not exist. Also, the attacker takes less of a personal risk, since they do not reveal themselves during the attack and the mortality risk is practically zero [STA, 1997].

It is known that countries such as China, Iran, Iraq, the USA, Libya, Syria, India, Russia and North Korea have recognized the facilities and advantages of these acts and have manifested openly that their offensive and defensive computer science capacity is totally desirable and is being explored [THE, 2005].

The fact that present society is more and more dependent on computers means that an endless number of attacks are possible. Firstly, because there are so many targets, and secondly because, given the systems' complexity, it contains a lot of vulnerabilities and weaknesses. Cyberattacks can affect a great number of computers and in this way their coverage, "publicity" and impact can be on a much larger scale than those of traditional attacks.

The electrical power industry is vulnerable because ICTs are necessary for the supply of electrical energy. Furthermore, cyberattacks are a potentially effective strategy because of the dependence of various critical infrastructures on power systems, and so the impact of an attack could be wide-ranging.

6.2 Definitions

Cyberterrorism is in short, the convergence of cyberspace and terrorism [WEM, 2004]. In order to understand better the type of cyberattacks that exist and the vulnerabilities of power systems, we will subsequently define the term cyberspace and who possible are the initiators of cyberattacks.

6.2.1 The cyberspace and cyberactors

According to UNESCO's definition, "Cyberspace is a new human and technological environment of expression, information and economic transactions. It consists of a) persons supplying and demanding information; and b) a world network of computers interconnected by means of telecommunication infrastructures enabling the information supplied and demanded, to be processed and transmitted digitally" [UNE, 2005] . At the moment, the Internet is one of the most important components of cyberspace.

There are many ways to make the classification of the inhabitants of cyberspace, but one of the most current is by considering the knowledge of available means on cyberspace. Thus, there are users who have a minimum knowledge of the operation of cyberspace, average users, advanced users, technical users, and then programmers of all the levels and hackers.

The term hacker was first coined by programmers at the Massachusetts Institute of Technology in USA, who wanted to distinguish between those that could make computer programs better and more effective and those that could make things that nobody had made before. In reference [RAY, 1996] eight different definitions of the term hacker are shown. We mention the two definitions used most often: *"Hacker: [originally, someone who makes furniture with an axe: a person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary; 2) one who enjoys the intellectual challenge of creatively overcoming or circumventing limitations"*.

Hackers look for defects, back doors and holes in security in order to improve software, and to prevent possible errors in the future. This happens neither with the permission, nor with the previous notice of owners. The results of their actions are usually published. A hacker acts to amuse himself or to learn. Within the hacker culture, the idea of freeware, shareware and open source software exists. When the action of a hacker is more than intrusion and is in fact destructive, this individual is called "cracker" or "dark hat hacker". Crackers are hackers who use their knowledge in computer science and communication technologies in order to fulfil malicious, immoral, and warlike aims. Their actions usually include: illegal entrance into systems, creation of a virus, theft of secret information, distribution of illegal material, elements of terrorism, piracy, tools to crack programs (programs that eliminate the restrictions of commercial software) and all types of similar actions. A cracker also distinguishes himself from the hacker by their moral, social and political values, which are generally contrary to capitalist values. A cracker "activist" is a cracker whose actions are motivated by political activism and analysis. Consequently the distinction between cyberterrorists, crackers and professional cybercriminals can be blurred and difficult to identify, and so it can be difficult to identify who is responsible for what.

These definitions are necessary so that one can define the degree of threat posed by different types of hackers. As we will see further on, we model the intensity of the attack depending on the resources that the cyberterrorist has at hand, but also on the abilities and knowledge of the perpetrator. The fact that the results of an attack depend on the abilities of the attacker is fortunately an obstacle for terrorists at the time of attack.

Nevertheless, we can imagine different scenarios regarding the possible relationships between terrorist groups and hackers. Terrorists could be trained by hackers, recruit crackers, ask cyber criminals for specific services, or in more violent cases intimidate hackers and force them to do something against their wishes.

6.2.2 What is a cyberattack?

A cyberattack is generally a computer attack aiming to disturb and/or stop the functions and services of systems that depend on computers and that can therefore affect individuals. Generally, a cyberattack implies a series of actions that exploit the vulnerabilities of a system and which then entails a negative consequence. The attack is an action or a series of actions that are not permitted by the systems' owner.

The effect that a damaged computer can have on people is not, in most cases, direct, and in this sense cyberattacks must be seen as acts that affect the physical world indirectly. This type of attack is generally performed by infecting a computer using malevolent codes, exploiting program faults, disturbing the operation of programs, and accessing, using and even stealing confidential information that it is stored in a computer network.

Not all attacks made through the communication network have terrorist objectives, and these are considered as cybercrimes. Nevertheless, due to the collaboration of hackers, cybercriminals and terrorists and also due to economic interests, the risk of cyberterrorism increases.

For example, the website "InfoWorld", in 2005, provided the information that vulnerabilities and codes for unknown defects are sold on the black market between $1000 and $5000 and that the main buyers are foreign governments, spam companies and terrorists. IP lists of computers which are infected with spy-ware and ready to be attacked already exist, and these can be sold to anyone who is willing to pay. A terrorist group with motivation to attack, and with the sufficient money and organization, could buy codes for destructive uses.

In the literature, we find that cyberattacks can be classified and put into different categories. We are particularly interested in this classification because it means we can distinguish between different cyberattacks and see whether one is more intense than another, depending on the tools used to attack, which weaknesses are exploited, and the consequences that an attack has on the information and communication system.

Taking as reference [HOW, 98], Figure 6-1 roughly illustrates how a cyberattack happens. The attack is realized by using tools such as a program packet sniffer, a toolkit, keyloggers, among others. With these tools, the attacker exploits a weak point or vulnerability in the system, which can be there due to the design, to the software or hardware implementation or to the computer system configuration. Thanks to these vulnerabilities, the attacker can take action in order to affect a component or process and thereby achieve his aim.

Figure 6-1. Taxonomy of attacks on computers and networks.

A successful attack that has taken place involves one or more unauthorised results. The loss of integrity, the loss of availability, and the loss of confidentiality are unauthorised because theses consequences are not approved by the owner or administrator of the IC network [HOW, 98].

The categories shown in Figure 6-1 are not mutually exclusive. A complex and coordinated cyberattack can simultaneously need the use of several tools, and need several actions to be taken, in order to affect more than one component or process and so cause a range of consequences.

6.2.2.1 Consequences of a cyberattack

The consequences of a cyberattack regarding only the IT and communication system can be classified into five main groups as follows:

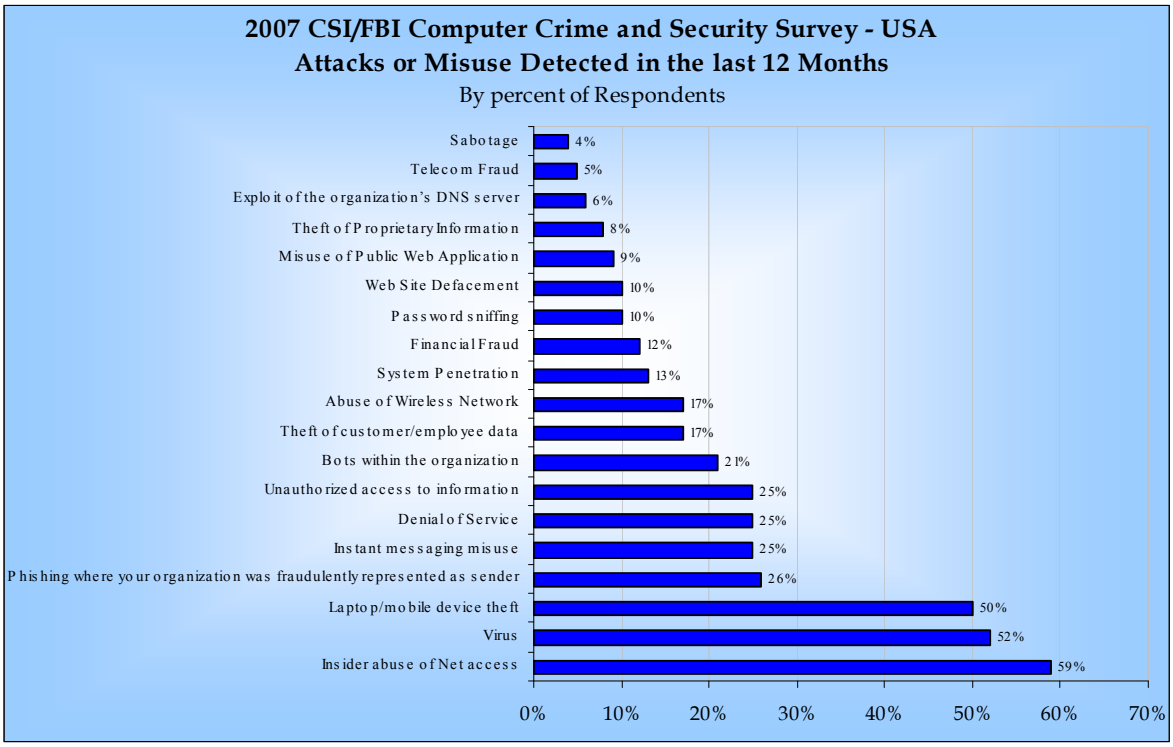
1. *Corruption of information - Loss of Integrity:* This happens when data on a computer or network suffers improper modification. Integrity is lost if unauthorized changes are made to the information by unauthorized persons or systems. Violation of integrity may be the first step in a successful attack against system availability or confidentiality. Some examples are: virus, modified password files, e-mail spoofing, etc.
2. *Denial-of-service (DoS) - Loss of Availability:* Loss of availability occurs if unauthorized persons or systems can deny access to authorized users. In this case, the attacker's goal is to put an end to the operation or minimize the operational efficiency of a service or of a network. For example, an attacker can overload the data processing of a PC; or can generate big network traffic, consuming all available bandwidth and therefore rendering certain components unavailable; or disabling the access of authorized users to certain basic services.
3. *Disclosure of information - Loss of Confidentiality:* When critical information is disclosed to unauthorized persons or systems. We can consider this type of attack as a passive assault. Some examples are: sniffers, spying, the use of backdoors, etc.
4. *Theft of resources - Loss of Availability:* When computers or the resources of a network are used by unauthorized entities. This is a technique used to create "denial of service" but we have created this category because the theft of resources can be possible without going until the DoS.
5. *Physical Destruction:* It refers to the ability to create actual physical harm or destruction through the use of IC systems. Command systems can be attacked and used to cause malfunctions in others IC components until the system is destroyed. These types of scenarios have not occurred, but are potential.

As we can appreciate, the cyberattacks entail the loss of any security pillar of the IC systems, that is to say, the loss of integrity, availability and/or confidentiality. *Availability* means to ensure the operation of assets, applications, networks and data, whenever they are required. *Confidentiality* means to ensure that stored and transmitted information is unavailable to unauthorised people and applications. *Integrity* means to ensure that information is accurate, up-to-date, comes from correct sources, and is sent to correct destinations [SHA, 2006].

The impact of cyberattacks does not merely have an impact on the communications system, but also on the productivity, efficiency and economy of the process for which the ICT is being used. In the case of power systems, one of the major risks is that an attack would entail the absence or the erroneous execution of protections or the functions of control devices. We will examine this topic in more detail in this document.

Finally, we want to show the results of Annual Computer Crime and Security Survey – 2007 [CSI, 2007]. Figure 6-2 illustrates different classes of attacks and misuses that respondents to the survey experienced during the last 12 months before the survey date. Observing this graph, we want to highlight two aspects. The first one is the fact that with 52%, abuses of insiders was the second most prevalent security problem, showing that one of the major threats comes from within companies. Second, we can see even if Denial of service is not in

the top list, it continues to be in the group of the most common problems, which represents a real threat for the correct performance of IC systems.



Source: The CSI/FBI 12th Annual Computer Crime and Security Survey – September 2007 [CSI, 2007]
Figure 6-2. Variety of attacks or misuse detected in the last 12 months.

6.2.3 Cybersecurity of IC Systems

The cybersecurity of an IC system refers to the establishment and maintenance policies and methods that ensure integrity, availability and confidentiality of the organization's IC resources. This requires taking the actual and potential threats into consideration and to oversee and put a defence strategy into action.

The major techniques and tools used in order to keep and guarantee the security of IC systems are: firewalls, antivirus software, intrusion detection systems, strong authentication (such as voiceprint, fingerprint, retinal scanning, and smart cards) and encryption. Other ways include the concepts of redundancy and back-up components.

The security problems of IC systems must be dealt with as a whole and not as isolated points. An analogy is the physical security of a house. Even if the doors are reinforced with the most sophisticated locks available, it makes no difference if the windows are left without such protection. In a similar way, the use of the best security technologies, such as cryptography, intrusion detection methods and others, are useless if, for example, the confidentiality of the working stations is not protected. Finally, we want to remember that "Social Engineering" [1] must be an important aspect to keep in mind regarding the security measures that need to be taken. The education of the users is fundamental in order to ensure that security technology can work correctly.

[1] The social engineering simply consists of ensuring - by means of deception or manipulation - that the legitimate and authorized users cannot reveal confidential information.

6.3 Cybersecurity of a Power System

An IC system of a power system is the group of technologies and services that guarantee the acquisition, the processing, the transport, the routing, the delivery and the availability of the information (whether it is data, sound or image) supporting the activities of generation, transmission, distribution and commercialization of the electric energy. It can make a variety of important possible functions, some of which are summarised below:

- Power system control: SCADA system, EMS, DMS, RTU (Remote Terminal Unit) and IED (Intelligent Electronic Device) communications
- Communication of protections
- Metering
- Maintenance of equipment
- BMS (Business Management System) or market operations system: communications with other market participants, contracts, day ahead schedules, hour ahead adjustments, real-time dispatches, billing [WU, 2005].
- ERP Systems (Enterprise Resource Planning): production planning, material purchasing, maintaining inventories, interacting with suppliers, tracking transactions, and providing customer service [WU, 2005].
- Communications between different sites as control centres and substations of a single utility
- Coordination of emergencies, control and protections between other utilities

Before approaching the topic of cybersecurity of IC systems (ICS), let us see the principal differences between a traditional IC network and the ICS of the power systems. For convenience, we are going to divide the communication system into two subsystems: the system of communications necessary for the control system and the corporate information system [GER, 2006].

The control system monitors, supervises and controls real physical processes related to the generation, transmission and distribution of electric power. This system comprises of a large number of applications (in extensive geographical areas) of data acquisition and the provision of information to the control centres, substations and market operation system. SCADA allows operators to "view" and control the equipment. It collects measurements and information (real and reactive power, voltage, current, transformer taps) from distant facilities known as RTU and IEDs, and sends control instructions to these facilities. The data are also used by other applications needed for system operation (such as load forecasting, state estimation, and security analysis). Most of these applications belong to EMS.

Nowadays, the communications systems in substations and control centres tend to be identical to other IC networks, but facilities such as SCADA handle very specialized programs. This restricts the identical use of many traditional security technologies in control systems, but particularly the main objectives of the cybersecurity.
Due to the importance of the functions of control systems, communication between facilities must be available 100 % of the time [SHA, 2006] and the integrity of the information must be guaranteed. Large delays or downs in response times create difficulties. For example, the response times in the control-loops are deterministic. Likewise, the loss or interruption of information are less tolerated than in the traditional IC networks because it can result in serious damage to power equipment and also put human life at risk.

Let us consider incidents that could affect cybersecurity and the paradigm integrity – availability – confidentiality, regarding the power control system and potential impacts on the security of power systems:

1. *Corruption of information - Loss of Integrity:* In an electrical power control system the loss of integrity is important because acquisition devices, such as RTUs and IEDs, can send incorrect data, SCADA can send erroneous commands, display wrong images, set off incorrect alarms, etc. This also includes the possibility of changing the settings of devices. Consecutive decisions or events caused by incorrect information can lead to a very bad impact on the power grid. Information must be accurate at all levels of the control, i.e., from the collection of information, processing, transporting, to the units of decision, control devices, interfaces, and storage devices, etc.
2. *Denial-of-service (DoS) - Loss of Availability:* All the IC elements of an electrical power control system, like operator workstations, SCADA, as well as the communication channels between these elements and to the outside world need to be available at all times. Because control systems emphasize reliability and time-response, the loss of availability is very significant especially in emergency situations. For example, if a power system is near its instability limit and an important control device does not work, its unavailability can destroy main components and affect the system stability.
3. *Disclosure of information - Loss of Confidentiality:* In general, for electric power control systems, it is most important to keep the IC availability and integrity confidential because these systems monitor and control in real-time the actual operation of a power system [WES, 2006]. Confidentiality in the control of power systems is much less important because the impact is usually not immediate, even if the information concerns security mechanisms, such as passwords and encryption keys. Conversely, there could be any impact in the long term.
4. *Theft of resources - Loss of Availability:* This aspect is important if the theft of resources affects the readiness of a service or information when it is urgently needed, and the impact can be catastrophic in emergency situations. Not all components have restriction of time and only in this case can the delay of data be accepted.
5. *Physical Destruction:* The loss of a component of the ICS is important because it causes the unavailability of services or information; however some systems such as SCADA are usually fault-tolerant and have back-ups allowing in most cases the loss of a component. This situation becomes difficult if there is a security problem with the ICS, if a component of the power system is destroyed.

The second subsystem is the corporate information system, which includes some tasks of business and management, such as finance, billing, personal management, etc. In this case, the paradigm of cybersecurity tends to be the same as that of normal IT. Here, even if the unavailability is important, it is not critical for the operation of the power system. In addition to this, the loss of confidentiality becomes important because of potential future problems of fraud, theft of information and competition with other utilities, etc [GER, 2006].

6.3.1 Definition

Cybersecurity in a power system concerns the safety of all IC services and computer-based applications employed for the planning, the security coordination of the power grid, the market operation, and the utilities' business management. Most of the related applications are executed in power stations, substations and control centres. Cybersecurity principally guarantees the availability and integrity of information, such as measurements, data and

commands sent and/or received by components and transmitted by communication channels. The cybersecurity of a power system must focus on the preservation of the reliability and security (including concepts of adequacy) of a power system.

Cybersecurity in a power system is different from the power system security with regard to contingencies resulting from cyber intrusions and therefore we distinguish these terms in this thesis. Cybersecurity concerns, in a strict sense, the safety of the components and of the process of the information and communication systems. It guarantees the integrity of a group of functions that support the power system operation. However, the correct performance of these functions does not necessarily guarantee the security of a power system. Inversely, if these functions do not work correctly, such situation can put the security of the power system in danger, because the communication system is a vital part of it. In short, cybersecurity is necessary for the security of a power system, but the cybersecurity of the communication system does not ensure the security of the entire power system.

6.3.2 Cyber vulnerabilities of power systems

It is widely accepted that IC technologies, such as Ethernet, Internet, others protocols and operating systems have a large number of known cyber vulnerabilities, and new vulnerabilities are reported on a daily basis. Exploitation tools, worms, viruses, as well as papers often become available shortly after the discovery of a new vulnerability.

Until now incidents which affected the ICTs of power systems and which led to large blackouts have not been reported. This is due to, among other factors, the lack of hackers' knowledge on control system technologies, the use of property technologies for utilities, the increasing emphasis of utilities in ICSs security and also because these systems are considerably robust. For example, the SCADA systems placed in control centres and important substations have complete redundancy; masters have back-up and also have duplicates, and sometimes even triplicates. Usually, these last security measures were implemented in order to oversee failures, fires, earthquakes, or physical attacks against facilities.

Old Equipment was not designed with cyber security as a priority
Due to high investments, control equipment (including ICTs) is designed to work for a long period of time. In the past, much of the equipment that was installed, which is still in use at the moment, was not designed with cybersecurity as a main requirement. Most real-time systems have no, or very poor, methods of authentication, no encryption, and no capacity to detect intrusions. Existing hardware devices using early microprocessor technology might not have the memory or processor capabilities to support encryption, and existing communications infrastructures may not have the bandwidth to support link level encryption.
Nevertheless, certain trends of power have increased the cyber vulnerabilities as we will see in the following.

6.3.2.1 Trends of the ICTs in power systems vs. cybersecurity

Restructuring and technological advances in the electricity sector favoured the innovation of electrical utilities in IT and CS. Currently, utilities work is based in a more market-oriented model in which any kind of investment has to be justified. At the same time the computer systems and communication networks that support the power operations became

increasingly pervasive. This led to the convergence of both systems, which in the past were totally separate - IC applications in the fields of power systems are now supposed to be implemented on a single platform.

The operation of transmission and distribution networks has become more complex. The network itself becomes more complex as new generators are set up and new transmission and distribution lines are added. Maintaining the reliability of a system requires more robust data acquisition, better analysis and faster coordinated controls.

Remote access
The vulnerability of power systems to cyberattack has grown as power companies have increased the use of remotely operated systems to control their equipment. Increasingly, power systems are being hooked up to open networks, including corporate intranets and the Internet, in an attempt to improve efficiency and lower costs. Nevertheless, this remote access also creates a new vulnerability because it exposes the system to remote attacks. Remote access includes a variety of direct or indirect links to RTUs, substations, power plants and control centres.

Corporate networks
Substations are being linked to corporate networks to provide business units with real-time operational data or to automate other processes, such as maintenance, billing, operation planning, etc. Corporate networks remain highly vulnerable to intrusions and the compromise of the system at the application or network levels. Administrators and operators are often not aware of these links, and there is sometimes little or no security to protect them.

Standardization vs. propriety programs
Nowadays, companies are renewing their control systems equipment in substations and control centres, or are investing in new ICS. This is due to the deregulation and new tendencies of business management. As a common rule, applications, devices and software, which can communicate with the technologies of other vendors, are required as well as ICTs which facilitate upgradeability and expandability. Therefore, the current trend is the use of standardized protocols[2] and open systems (non-proprietary and standard software and hardware). Unfortunately this situation means that ICTs become more vulnerable. Firstly, because one of the barriers for hackers has been the lack of knowledge on protocols, operating systems, network configuration, etc., that electrical companies use. The standardization and the availability of information offer the possibility of acquiring the necessary information and knowledge to attack. The operating systems for the newer ICSs are either Windows or Unix-based [GOE, 2002], which have, as is widely known, many vulnerabilities, and so the system is even more exposed to attacks. Presently, the IC61850 standard is an attempt to establish a single worldwide standard for substation automation communications. This norm has been amply discussed and documented.

Interconnections
Electrical energy deregulation rendered the development of ICTs imperative to supply the market. In a competitive environment, economic decisions are made individually by market participants and system-wide reliability is achieved through coordination of parties belonging to different companies, therefore the paradigm has shifted from centralized to

[2] Most of the first control systems for electrical networks possessed proper ICT, with specializing proper protocols or for a specific vendor. Equipment upgrade needed complete replacement.

decentralized decision making. This requires information and application software in control centres to be decentralized and distributed. Consequently, control systems are being linked to corporate networks in order to provide business units with real-time operational data or to speed up or automate other processes, such as customer service, power and outage management and supply procurement. Corporate networks remain highly vulnerable to intrusions and the compromise of the system at the application or network levels [GOE, 2002].

Some Incidents

In the following we mention some cyber-incidents that have interfered power systems' communications security during the last few years.

- Tom Donahue, a CIA analyst, in January 2008 warned the electric power sector that cyberattackers had hacked into the computer systems of utility companies outside the United States and made demands, in at least one case causing a power outage that affected multiple cities. He said "We do not know who executed these attacks or why, but all involved intrusions through the Internet".

- January 2003, an incident occurred when the worm "Slammer" of the Internet infected the monitoring network of the nuclear plant Davis-Besse of First Energy Corporation in Ohio, the reactor happened to be offline. The worm entered the plant network via a contractor's infected computer connected through a T1 line (telephone dial-up) directly to the plant network, thus bypassing the firewall [NRC, 2003]. The electric utility company lost control of their EMS/SCADA for system nearly five hours. A later report made by North American Electric Reliability Council (NERC) reached the conclusion that while nothing serious happened as a result, the EMS/SCADA system was not able to communicate with substations and plants, forcing the company operations staff to resort to manual operation of their transmission and generation assets until control could be restored. By the company's own admission, this incident would not have happened if the requirements of the proposed Urgent Action standard had been implemented.

- In September 2001, the Nimda worm was circulated widely throughout the world. The NERC know of an electric utility whose EMS/SCADA network was compromised by the Nimda worm. The worm then propagated itself and spread to the internal project network of a major EMS/SCADA vendor via the vendors' support communications circuit, devastating the EMS vendors' internal network and launching further attacks against the EMS/SCADA networks of all other customers of the vendor with support communications circuits [NER, 2003].

- In August 2001, the Code Red II worm successfully compromised the internal network of a company that provides services to NERC and numerous electric utility companies. This worm then attacked customers connected to this company, successfully compromising an exposed web server at one of the utility control centres. It is important to note that the compromised server was presumed to be protected, as it was not exposed to the Internet. This attack was propagated via the private frame relay network connecting the service company, the impacted utility, and the other connected utility companies [NER, 2003].

- For 17 days, between April 25 and May 11 of 2001, hackers managed to remain undetected after they breached the network of the Folsom, based California Independent System Operator. However, the attacks were limited to a "practice network" and so they posed no threat to the real power grid or the primary power distribution network that handles the Western U.S. Although no damage was reported, officials traced the intrusion back to a system in China [WEI, 2001].

- In December 2000 the National Infrastructure Protection Centre (NIPC), said that "A regional entity in the electric power industry has recently experienced computer intrusions through anonymous FTP (File Transfer Protocol) login exploitation and the intruders used the hacked FTP site to store and play interactive games that consumed 95 per cent of the organization's Internet bandwidth". NIPC added that "the compromised bandwidth threatened the regional entity's ability to conduct bulk power transactions" [GRE, 2000].

A document prepared for the CIGRE Joint Working Group -Security for Information Systems and Intranets in Electrical Power Systems- entitled "Cyber security considerations in power system Operations" [CIG, 2005] said that a significant number of cyber incidents have taken place but only some have been admitted to or described. A sample of incidents described in this document is given below:

- "Large Generating Plant Output Reduced to Zero: The control system of a large generating plant operating at a number of 100 MW was infected by a virus and its output was reduced to virtually zero in a few seconds. The infection came from a connected corporate IT network. The solution was to rigorously separate the real-time and corporate networks" [CIG, 2005].

- "Distribution SCADA System Partly Disabled: A virus infected a lap-top which was used by a maintenance technician to modify a telecoms router. The virus affected all telecom nodes, including some used by a SCADA system. The SCADA system was rendered partially inoperable for a number of days. A partial solution required better management of virus protection on lap-tops" [CIG, 2005].

- "Unauthorised Access to EMS Applications: A utility gave remote access rights to an EMS supplier. It was observed that application patches had been applied without agreement. No problems arose, but the situation revealed that continuous, non-verified access had remained open to an external" [CIG, 2005].

Other important facts

- Idaho National Laboratory in USA performed an experiment for the Department of Homeland Security (DHS) in March 2007 in order to evaluate the potential damage resulting from cyberattacks. The laboratory successfully destroyed a generator while conducting an experimental cyberattack. The attack involved the controlled hack of a replicated control system commonly found throughout the American power systems. Members of the House Committee on Homeland Security are concerned that malicious actors could use the same attack vector against large generators and other critical rotating equipment that could cause widespread and long-term damage to the electric infrastructure of the United States.

- In 2001 and 2002, several documents found in Afghanistan, and after investigations into the Al Qaeda networks, it was shown that cyberterrorism was actively studied by Osama Bin Laden, passionate about this type of modern war. He has invested a lot of money in the recruitment in the Arab world of the best data processing specialists and Internet specialists. A plan in this direction had been given to him in June 2001 by a fundamentalist Saudi from London. Moreover, in the British capital, fundamentalist Internet networks are increasingly active.

- Data collected by Riptech, Inc. — a Virginia-based company specializing in the security of online information and financial systems — on cyberattacks during the six months following the 9/11 attacks showed that companies in the energy industry suffered intrusions at twice the rate of other industries, with the number of severe or critical attacks requiring immediate intervention averaging 12.5 per company.

The identification of cyber vulnerabilities is an important challenge for electric utilities. This task allows owners to correct the holes in the system in order to protect the power system against attacks on the information and control systems. In addition, finding out the possible threats on the system is necessary, as it will allow utilities to not only improve cybersecurity but also to establish whether insecurities of the communication system also represent insecurity for the power system operation.

The first known study showing power grid vulnerabilities to cyberattacks was published in 1997. A vulnerability assessment carried out over six months by the White House's National Security Telecommunications Advisory Committee in USA and Canada found basic security flaws in the computerized systems that control generators, switching stations and electrical substations [STA, 1997]. Among other things, the committee reported that operational networks controlling critical portions of the grid were accessible through electric companies' corporate LANs; some digital circuit breakers could be remotely tripped by anyone with the right phone number; and fixed passwords for remote vendor access went unchanged for years.

6.4 Bayesian Inference to Cyberterrorism Risk Assessment

Risk quantification in the Cyberterrorism case is very complex: cyberspace does not have physical limits like a country, it is not always easy to grasp the capabilities and behaviour of attackers and a lot of vulnerabilities exist in the ICS, more of which are being discovered everyday. In addition, ICS gives support to most forms of infrastructure, which creates very complex interdependencies that have to be understood and modelled.

Relations between the power grid and the communication system are not obvious. At the moment, only a few tools exist which can be used to obtain measures of the risk of interdependencies. We take advantage of the fact that modelling on Bayesian networks can make use of subjective probability. We can model interdependencies risk using the operators' experience, their belief in criticality and the knowledge of experts. Based on these results we calculate the "a priori risk". We have called the risk in this way because the calculation depends on the subjective judgment of experts and the criticality calculation is not exhaustive. Modifications in the criticality calculation can be introduced and we also present some other options here.

6.4.1 Implementation of the Bayesian network

In the majority of references found on cybersecurity of ICSs, and especially on SCADA systems, authors recommend the management of risk. The risk assessment is generally defined as a series of "common" steps:

- Identification of network above, to which the analysis of risk is going to be applied.
- Gathering of necessary information on network assets.
- Identification of possible threats: who is interested in attacking and who would have the knowledge to make it possible.
- Identification of network vulnerabilities and the components that can facilitate the success of an attack (hardware, software, information, etc.)
- Determination of probability that vulnerability in the ICS might be exploited by a threat.

- Evaluation of whether the occurrence of an attack would lead to the loss of any equipment or function, and whether any performance or security criteria are being violated.
- Quantify the impact depending on the type of risk that will be evaluated. (See section 4.1.2)
- Calculation of the risk of the multiplication of the probability that the attack has a "successful" impact.

We propose to evaluate the risk by means of a Bayesian network, as graphically presented in Figure 6-3. In our Bayesian network we implemented a methodology making it possible to integrate and identify the motivations and resources that a cyber terrorist may have, as well as the means that assets have to protect themselves in case of attack. With these elements, we determine the probability of whether or not an attack will take place, as well as the intensity of such an attack on ICS. Later, by using the subjective probability, we quantify the probability of whether the attack on the ICS would affect the operation of the power system to a major or minor degree.

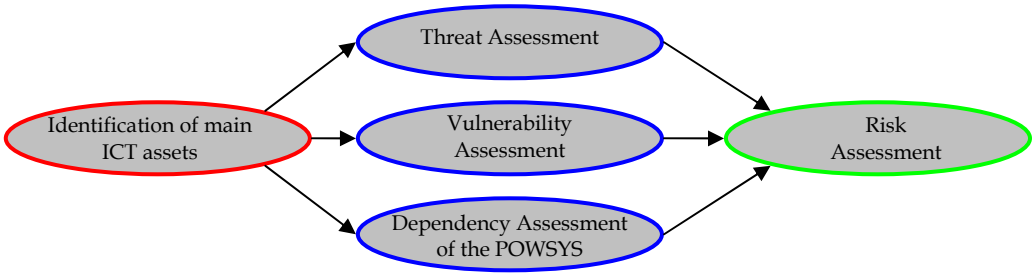


Figure 6-3. Risk assessment with regard to cyberattacks.

The Bayesian network must not be understood as an attack graph. That is to say, we do not simulate the different steps and actions that must be realized to actually attack assets. Nevertheless, an attack graph based on Bayesian networks or Petri nets could be integrated into our network. In this case, the relation between the input variables and the attack probability is determined by a more detailed vulnerability analysis, including some parameters, such as the privilege violations and the probability of detection, among others.

6.4.1.1 Identification of goals of modelling

- To model by using the theory of probability the interdependencies between the power grid and the communications system.
- To obtain the probability of whether an asset of the ICS may be cyberattacked for terrorist reasons.
- To obtain the probability of whether a cyberattack would affect the operation of the power system.

6.4.1.2 Definitions

Following are the definitions of some terms that will be used from now on, which we need in order to develop our Bayesian Network. Some of the terms have already been used in chapter 4, when we used Bayesian networks for the risk assessment of the operation of power systems in case of physical attacks. Here, we extend these definitions to the case of cyber terrorism against the ICTs of the power systems.

- Components: Principal assets of the information and communications system of the power system. In our case, we only model the principal assets which guarantee the execution of principal tasks of the communication system. Table 6-I shows the main components to be modelled. We can model, for example, only the principal components of the control system and associate with each one the components of the communication network without having to model the latter in detail. Another alternative is to model as many components of the control system as of the information and communication network. Nevertheless, this can be impractical because of the quantity of components involved.

TABLE 6-I. COMPONENTS OF THE IC SYSTEMS

Hardware	Mainframes/SCADA servers
	Storage systems/ Data Historian
	Remote terminal Units (RTU)
	Intelligent Electronic Devices (IED)
	Human-Machine Interface
	Laptops / Desktops
Network appliances	Routers (WAN)
	Switches (LAN)
	Remote Access points
Support	Technical operation applications
	Corporate applications
	Business applications
Communication services	Phone
	Mobile phones

- Internal Event: The event occurs because of the system operation. In the case of intentional events[3], these events are caused by insiders.
- Insider: People that have rightful access to the ICS and who use it for illegal purpose [RIG, 2006]. Employers, long-term and temporary-term service providers, outsourcing vendors, consultants can manipulate ICS for terrorist causes, revenge or personal gain.
- Cyberattack: unnatural and intentional events caused by using ICT as a weapon. In this document, all cyberattacks have terrorist purposes. The definition of the attacker depends on whether the event is internal or external.

6.4.1.3 Information sources

The following sources of information were used in order to build the Bayesian network:
- Interviews with experts in computer security
- Interview with the operators of the substation Champagnier 400KV - RTE France. In this substation there is a PEXI (Pupitre d'Exploitation Informatisé - SCADA)
- Interview with the Rhone Alpes Region PGC's coordinator , Antenne Dauphine (based in Grenoble)
- Interviews with a trainer of dispatchers in the power control centre of Lyon - RTE
- Analysis of the survey GRID results
- Books specializing in security of SCADA systems
- IEC 61850 standard
- Analysis of the authors

[3] Events that occur because of the intervention of humans. In such events the liable person or group has as their objective the damage of the power system, including the IC system and the power grid.

6.4.1.4 What are the relevant variables?

Due to the characteristics of cyberterrorism, which have already been described, our network will be implemented based on social, religious and political factors, which are characteristic of both internal and global terrorism. On the other hand, we also model attributes of the ICT system reliability and the interdependency between the communication and information network and the power grid.

A. Motivation to attack - Threat assessment

As for the Bayesian network of Chapter 4, we analyze the motive for an attack. Though the assessment of the motivation for attack is essentially made by using the same variables of the Bayesian network for physical attacks (political situation and position/terrorist activity) we also include here proper factors of the global terrorism.

i. Political - or "religious"- situation

Within the network, as in chapter 4, this variable is used to reflect the incidence of political and/or religious factors affecting the civil order of a region or a country. Cyberterrorism exists because terrorism exists, and terrorism is, in general terms, a political phenomenon. We know that religion is used as a justification for terrorist activities but objectives are mostly political, as well as objectives that are derived from the political interpretation of religion[4]. In the last few years, we have seen above all the emergency of extremist religious groups proclaiming openly their will to hurt citizens and to economically affect different western countries; principally those which represent social ideas fundamentally dissimilar to theirs [END, 2006].

We define this variable using the following states: critical, moderately critical, and non-critical situation. The subjective probabilities are obtained from politic and/or sociologic experts and the correlation of terrorist attacks against the critical infrastructure in periods of political and religious strain.

Political and/or Religious Situation		
critical	moderately critical	non-critical

ii. Position/activity of terrorist group

This variable represents the vitality and power of the group. The financial resources and the quantity of men belonging to the terrorist group allow us to identify the power of the group. Likewise, it is important to include in this variable; the current activity of the terrorist group such as, means of recruitment and the acceptance or "sympathy" for the terrorist group in the civil population. One must give particular attention to the sympathy of young people for the terrorist group. A large number of hackers are teenagers or young adults who have the knowledge to attack efficiently and who can be easily manipulated. An important tool to define the activity of the terrorists is information from the internet. Terrorists increasingly exploit the Internet as a communication, intelligence, and propaganda tool by which they can safely

[4] Notice that the network we are constructing is not specific for the Colombian case and for this reason also we include the religious motivations of the cyberterrorism.

communicate with their affiliates, coordinate action plans, raise funds, and introduce new supporters into their networks.

The variable states are:

Position/Activity of Terrorist Group		
high presence/activity	average presence/activity	low presence/activity

iii. Expected public reaction

In this variable we model the desired public reaction supposing that the cyberattack was successful and reached its objective, i.e. the public reaction caused by the consequences of the cyberattack. For example, the motivation of attacking the control system of a nuclear plant may be higher -although this component is not as important for the production or stability of the power system- than the one of a substation which is relatively more critical for the electrical network.

In this variable we also include, modernization and globalization factors of a region or country. The massive use of ICTs in a country could motivate terrorists to attack because there are represent many targets as well as weapons. In addition, modernization and globalization may contribute to terrorism because these factors affect the structure of values and norms. The integration of marginalized or weakly developed countries into the global economy entails modest growth, the loss of competitiveness and decrease of profits. Some possible consequences are the increase of unemployment, political conflicts and religious fundamentalism. Reality shows that some symbols of modernisation have already become a target of attack [KLA, 2002].

The states of the variable "expected public reaction" are:

Expected public reaction		
high	medium	low

Motivation of the attack is then inferred from the variables discussed above and the illustrated relationships.

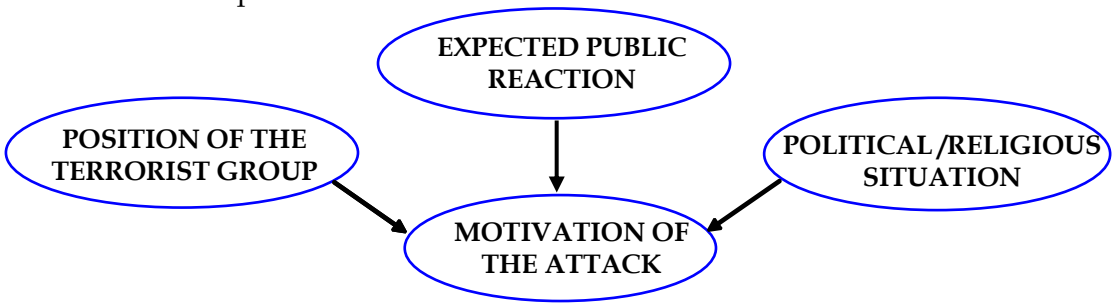


Figure 6-4. Relevant variables influencing the attack motivation.

Depending on the level of detail of the model of the ICT system, it is possible that the motivation for an attack a group of components has the same value. For example, when the IC system is analysed in detail for a single substation or control system is probable that the motivation of the attack is the same for the entire modelled targets. If different ICS are modelled, and one of them controls a symbol of technology such as the biggest hydroelectric plant of a country, for example, then we may find large differences in the motivation value.

The possible states used to define the motivation of an attack are:

Motivation of the attack		
high	medium	low

B. Available resources to attack the target - Threat assessment

The following variable to be analyzed involves the quantity of resources that the terrorist group has at its disposal of and that are generally openly known.

iv. Type of Perpetrator

In our network we include the probability whether the attack is made by an insider or an outsider and we try to predict approximately the level of sophistication of the attacker. The attacker may belong to a terrorist group, work in exchange of remuneration or work under menace. This variable is very important due to the privileged access and the specialized knowledge of the attacker. Figure 6-5 shows the taxonomy of the possible attackers against the ICS.

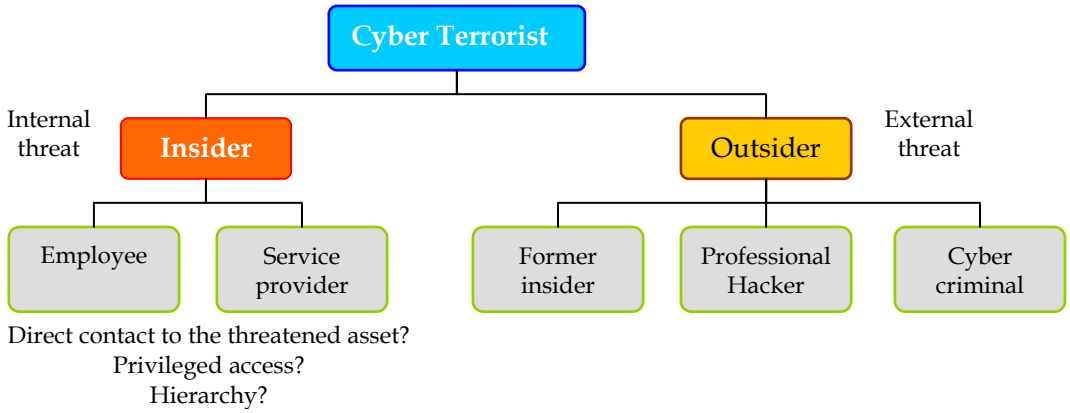


Figure 6-5. Taxonomy of the possible cyberattackers against the ICS, motivated by terrorist causes.

An *insider* is a current employee or contractor and therefore he/she has a significant advantage compared to other possible attackers. The privilege of information and access of an insider and even one ex-insider entail a major probability of success of the attack and the impact could be more significant. The danger increases when a person has a high level of authority.

The second category consists of potential external attackers or outsiders. Theoretically, these are those persons who do not have authorized access to the assets, i.e. that they do not have passwords, do not dispose of confidential information, do not have physical access to the equipments, etc. Nevertheless, there is a difference between former-insiders and the others. The former-insider may have knowledge on the assets, the security policies, the persons in charge of the assets, because he/she was employed at the utility. We believe that ex-employees as much as ex-contractors represent a threat for the equipments. We give the example of the current maintenance of the digital control systems, which is realized for the most part by vendors. This contractor (vendor) is someone who disposes of passwords and knows the security means of the command equipments. These mechanisms protect the modification of settings and the integrity of the component. The contractor has additionally the knowledge of how to modify or to

affect the asset. An ex-contractor can perfectly sell all this information to terrorist groups, only days before or after leaving his work, in exchange for money.

Another category of outsiders are those who have special knowledge, such as hackers or cyber criminals. The difference is that these attackers never had direct contact with the assets or with confidential information of the utility. Nevertheless, they have skills that make them dangerous. Here, we do not include naive novices or apprentice hackers.

The possible states of this variable correspond to the probability that the attacker is:

Type of perpetrator				
Insider employee	Insider Service provider	Outsider Former-Insider	Outsider Professional cracker	Outsider Cyber criminal

These probabilities can be obtained by security analysts inside the utilities and companies who provide services. It is also necessary to exchange information with the security services of a country or international services that track and dispose of information about the activities of terrorist groups.

v. Information availability of the target and the network

In this variable we include all the information on the targets, i.e., assets or subsystems and their functioning in the IC system, which the attacker may have or acquire, such as:

- Technology of the equipments that belong to the ICS, i.e. the workstations, software, hardware and security technologies.
- Specific information about default configurations of operating systems and software used in power systems control, procedures for restoring ICS configuration, etc.
- Typical security technologies which this type of assets have.

In the risk assessment methodology it is very important to determine the technologies generation and whether open software and protocols are used or not. This is equally important if the equipments use hardware or software that was discussed in conferences and this is documented in papers or technical reviews [STO, 2006].

Finally, it is possible to analyze the quantity of resources such as open training, consultants, or any type of expertise that allows terrorists to understand the functioning of the assets in the network and the functioning of the network itself (software, hardware, networks topologies).

The possible states of the variable are:

Information availability of the target		
enough	regular	low

The probabilities of these variables are determined by evaluating the quantity of available information about the topic, i.e. information of the equipment operation and its performance in the network on the Internet, in bookshops and in libraries. Likewise the variables can be determined by the evaluation of the offer of open trainings and the easiness of attending them, the advising of consultancies and possible programs of simulation.

vi. Public knowledge of the vulnerabilities of the target and attack tools

In this variable we include all the information that the attacker may have on the vulnerabilities that are discovered, and of the new tools that are available to attack targets. Basically, we separate this variable from the previous one in order to rapidly include the recent information about vulnerabilities of the operating systems, the software, the protocols, the safety means, etc., and the creation of viruses, Trojans, etc., which can affect the asset and the network. In this variable we also include the possibility that the attacker has information on:

- Vulnerabilities of the specific equipment, subsystems, the network, the operating system and of the protocols belonging to the ICS of the power system.
- Software typically used for power system control which is really vulnerable to buffer flows or Denial-of-Service attacks.
- Open information on tools, types of assaults and the necessary intelligence to attack the specific target.
- Experience of other companies that possess ICSs similar to the ones used for the power system or other attackers' experiences from assaults against these systems. Examples are the SCADAs used for the water - wastewater or pipeline industries.
- Consultants or any type of expertise that allows the terrorists to develop the assaults (software, hardware, networks topologies) exploiting the known vulnerabilities.

The states of the variable "public knowledge of the vulnerabilities" are defined as follows:

Public knowledge of the vulnerabilities		
enough	regular	low

Thus, the resources that the terrorist group intend to use for the attack are then inferred with the variables discussed above and the relationships are illustrated in Figure 6-6.

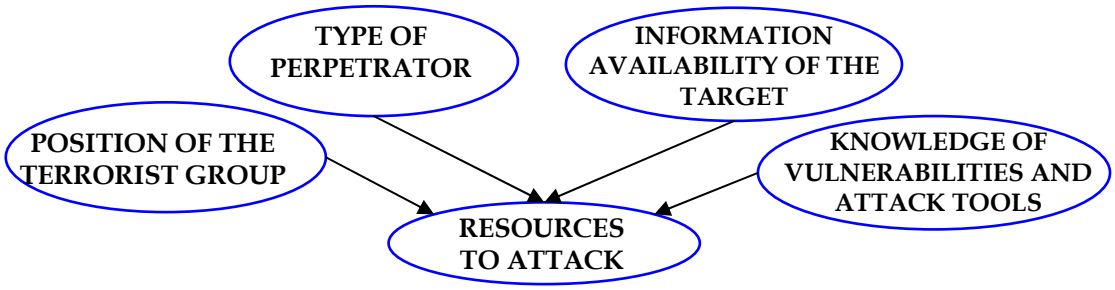


Figure 6-6. Relevant variables influencing the resources that terrorist group has to attack.

The possible states of the variable "resources used for the attack" are:

Resources to attack the asset		
enough	regular	low

C. Vulnerability of the target – Vulnerability assessment

In this variable we infer the vulnerability of the target, by analyzing the specific vulnerabilities of the asset and the vulnerabilities of the network. Theoretically, a target without vulnerabilities, and which has all the possible measures of security that a network can provide, should be able to resist and survive to external attacks.

vii. Security vulnerabilities of the asset

The first factor which ensures the failure of an attack against a target is the non-existence of vulnerabilities, or seen from another perspective the success of security measures that were implemented in order to repel attacks. In order to find the vulnerabilities in a system it is necessary to analyze the holes in security as well as all tools, actions, best practices, and technologies that are implemented to resist the attacks, and which affect the availability, integrity, real-time responsiveness and confidentiality of the component. A variety of equipment does not allow the inclusion of these security measures due to their generation and specifications, which give place to vulnerabilities. The mismanagement of passwords, clear text, and the lack of updates are only some examples of vulnerabilities.

Since not all types of vulnerabilities can give the same results, we are going to classify the vulnerabilities of the equipment in accordance with the possible severity of the impact. This means that experts carry out a subjective evaluation of the proportion of the results that affect the network, if this vulnerability is exploited. We suggest that the severity evaluation should be done bearing the following criteria [FIN, 2006] in mind:

Severity	Criteria
Low severity expected	Terrorists can obtain information that is not directly exploitable, such as usernames without passwords, application version numbers
Medium severity expected	Terrorists can degrade the performance of the IC System
High severity expected	Terrorists can act as legitimate user of the ICS Terrorists can gain "root" privileges , i.e., with a lot of rights Terrorists can be undetected and consequently can make sophisticated attacks

The possible states of this variable are high, average, low, and no vulnerability. Based on [SOU, 2006] we suggest that the probabilities should be obtained as a percentage of the security vulnerabilities displayed by the equipment that exists in the component as illustrated in Table 6-II. If for example a component does not have physical ports, the vulnerability related to the lack of protection of physical ports does not apply. Cybersecurity experts classify the vulnerabilities depending on their knowledge about possible impacts for a specific vulnerability. We suggest a classification of severity in Table 6-II as an example, but it is not necessarily the unique categorization. These values can be changed regarding the policies of the utility and perception of the risk of each expert.

Supposing that k vulnerabilities can be analyzed and that the binary variable $Applicable_i(0,1)$ takes the value of 1, if the vulnerability i concerns the analyzed assets, and 0 if it does not apply; that the binary variable $Sevhigh(0,1)$ takes the value of 1 if the exploitation of the vulnerability i has a high impact, and takes the value of 0 otherwise; the vulnerability of an equipment with high impact is found as [6-1].

$$Vulnhigh = \frac{\sum_{i=1\ldots k} Applicable_i \cdot Sevhigh_i}{\sum_{i=1\ldots k} Applicable_i}$$

TABLE 6-II. VULNERABILITIES OF THE IC ASSETS BELONGING TO THE POWER SYSTEM, BASED ON [SOU, 2006]

Type	Description of the vulnerability	Applicable?	Severity		
			High	Medium	Low
CONFIGURATION	Once a new vulnerability is discovered, patches cannot be quickly developed because of the complexity of the operating system and software			X	
	Security applications and operating system patches are not updated		X		
	Use of default configurations which frequently have open ports, open exploitable services, application running in hosts		X		
	Data unprotected on portable devices which can be likely stolen			X	
	Lack of password policy or deficient policy		X		
	No password for system login or system power-on and system screen saver				X
	Password disclosure			X	
	Password guessing			X	
	Incorrect access controls: unnecessary user privileges, lack of privileges for a legitimate user		X		
HARDWARE	Lack of security test			X	
	Deficient physical protection of main assets			X	
	Insecure remote access on assets		X		
	Physical access to the asset for unauthorized person			X	
	Inappropriate representation of the configuration of the hardware in the documentation				X
	Unsecured physical ports			X	
SOFTWARE	Use of clear text			X	
	Unneeded services running		X		
	Incorrect access controls that allow changing of the software configuration		X		
	Inadequate authentication		X		
	Logs not maintained				X
	Lack of malware protection software		X		
	Malware no updated		X		
	Incorrect configuration of malware or inappropriate malware affecting the operation of power system control tasks		X		
	Possibility to disable security capabilities of the software		X		

In the same way we can find the probability of whether the vulnerability has a medium (*Vulnmedium*) or low (*Vulnlow*) impact. Since this categorization of the security vulnerabilities is mutually exclusive, i.e. if we associate the exploiting of a vulnerability with a degree of severity high, we cannot associate this vulnerability with any other degree of severity; then the sum of the levels of vulnerabilities (*Vulnhigh*, *Vulnmedium*, *Vulnlow*) equals 1. Therefore, we can assign the probabilities of the variable as follows:

Security vulnerabilities of the asset		
Highly vulnerable	*Averagely vulnerable*	*Lowly vulnerable*
Vulnhigh	*Vulnmedium*	*Vulnlow*

Notice that the idea of risk assessment is about eliminating vulnerabilities which can potentially produce high severities. Nevertheless, various vulnerabilities will remain in place some time before being eliminated and others, as mentioned before, will not be eliminated unless the assets are replaced.

viii. Security vulnerabilities of the IC network

In the same way that the security vulnerabilities of the IC asset were evaluated by using Table 6-II, now we assess the security vulnerabilities concerning the communication and information network. This variable is considered here because depending on the protection strategy of the network, a vulnerability of the network could also in itself be a vulnerability of the assets. In table 6-II, we do not categorize the severity for each vulnerability of the IC network because this depends mainly on its design, the parameters and the protection strategy adopted.

The states of the variable and the evaluation process of the probabilities are identical to the ones of the vulnerabilities of the assets. In this case we use Table 6-III for the vulnerabilities assessment of the IC network.

Security vulnerabilities of the network		
High vulnerability	*Average vulnerability*	*Low vulnerability*
Vulnhigh	*Vulnmedium*	*Vulnlow*

TABLE 6-III. VULNERABILITIES OF THE IC NETWORK OF THE POWER SYSTEM, BASED ON [SOU, 2006]

Type	Description of the vulnerability	Applicable?	Severity		
			High	Medium	Low
CONFIGURATION	Inadequate configuration of routers and firewalls, or default configurations: open ports, open exploitable services running in hosts				
	Passwords transmitted without encryption				
	Lack of password policy or deficient policy				
	Incorrect access controls: unnecessary user privileges, lack of privileges for a legitimate user				
HARDWARE	Deficient physical protection of the asset				
	Unsecured physical ports as USB and PS/2				
	Physical access to the asset for unauthorized person				
	Inappropriate representation of the configuration of the hardware in the ICS				
	Control network services not within the network control				
NET WORK PERI METER	No security network perimeter defined				
	Firewalls nonexistent or improperly configured				
COMMUNI CATIONS	Lack of integrity checking for communications				
	Authentication is nonexistent or not strong				
	Inadequate authentication in access points				
	Inadequate data protections between users and access points				

Since it often turns out to be difficult to analyze whether the asset or the network displays certain vulnerabilities or not, Table 6-IV offers a short summary of possible mitigations that can be recommended.

TABLE 6-IV. MOST USED MITIGATIONS OF VULNERABILITIES, BASED MAINLY ON [SHA, 2006]

Asset	Vulnerability	Security Mitigation
IP-based communication links	Multiple vulnerabilities	1. Firewalls 2. Encryption functions of routers 3. Protection of communication path
Devices with remote phone access	Unsecured dial-in telephone line	1. Modem dial-back mechanism, or encrypting modems 2. Strong authentication: a. Digital certificates or b. ID/password mechanism or c. Token-based password 3. Limitations on remote login attempts 4. Nondisclosure and confidentiality agreements for insiders 5. Policy of revocation system user IDs, electronic access rights and passwords for ex-insiders
Devices with removal media (CD, flash drive, memory card)	Malware can be introduced into a system or network	1. Virus-scanning in every PC 2. Network intrusion detection packages (Identification of malware sending messages) 3. Strong authentication 4. Disable CD/DVD and USB/PCMCIA ports on all computers having very secure information 5. Encrypt all sensitive information and limit number of personnel with decryption keys
Bluetooth-enabled devices	Transmission of virus in other devices	1. Virus-scanning in all laptops 2. Network intrusion detection packages 3. Policy that all Bluetooth-enables devices are turn-off in dangerous areas
WiFi-enabled devices with Ethernet connection	WiFi connection is used to bridge the LAN of SCADA	1. Policy of disallowing WiFi connection while a LAN connection is in use 2. Implement WPA encryption 3. Implement device registration
Connexions between the main SCADA assets and other LAN/WANs	Access for external attacker	1. Appropriated firewall technology 2. Current update of firewalls 3. Application proxy server (if the number of applications is fixed)
Connexions between consoles PCs and servers	Multiple vulnerabilities	1. VPN among the console PCs and servers using Internet protocol security (authentication and encryption function embedded)

The vulnerability of the target is inferred by using the two last variables as shown in figure 6-7.

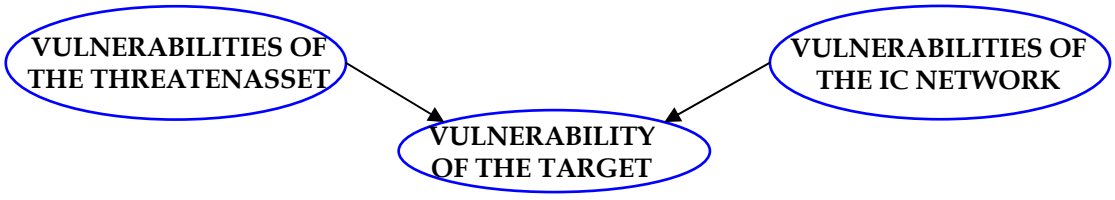


Figure 6-7. Relevant variables which influence the vulnerability of the target.

The states of the variable "vulnerability of the target" are:

Vulnerability of the target		
Highly vulnerable	*Averagely vulnerable*	*Lowly vulnerable*
Vulnhigh	*Vulnmedium*	*Vulnlow*

Conditional probabilities must be assigned which take into consideration the defence strategy adopted to protect the ICS. The two most popular practices for the defence of an ICT are "defence-in-depth" and "hard perimeter" [NAE, 2002]. The idea of the latter approach is to construct a strong wall around the ICS and to ignore all the measures of security inside. Thus, if this practice is assumed by the utility, the conditional probabilities must reflect the strong dependency of the target on the security of the IC network.

D. Sophistication of the attack against the target

The next variable to infer is the level of sophistication of the cyberattack against the target. This variable shows the probability that a terrorist can carry out successful attacks against the target, and affect the performance of the asset at different levels depending on the sophistication of the attack.

The sophistication of the attack is inferred from the motivation of the attack, resources available to use in the assault and the vulnerability of the target. We do not detail the actions done by the terrorist, i.e., we do not model specifically if the assailant accomplished actions such as bypass, spoof, steal, etc. We make a direct relationship between the assault and its consequences. Thus, a successful cyberattack depends on the use of sophisticated tools and techniques will always be classified in the following categories: loss of availability, loss of integrity and loss of confidentiality. Although the attack can have various unauthorized results, it will be classified in terms of the most severe result that it can cause. An attack that results in the loss of integrity and availability is considered to be the most catastrophic type of attack. Inversely, an attack which results in the loss of confidentiality is considered to be less serious, though it is possible that in the future this attack will lead onto more severe attacks. We assume that a successful attack will always leave unauthorized results; for example an assailant that penetrates the network without affecting the behaviour of the network, has violated confidentiality simply by entering the system.

The states of this variable are:

Sophistication of the attack against the target				
Loss of availability and integrity	Loss of availability	Loss of integrity	Loss of confidentiality	No attack

Conditional probabilities are assigned for experts of IC security, the analyses of databases of cyberattacks against the ICS.

The probability of the different types of unauthorized results implies the occurrence of the cyberattack itself. Therefore, in this node of the Bayesian network the marginal probability that the attack occurs is found as follows:

$$\Pr(Attack) = 1 - \Pr(No - Attack) \qquad [6\text{-}1]$$

The probabilities inferred for this variable are important because they can be used by risk analysers as a measurement of risk.

E. Continuity of the function performed by the target

In view of the volume and the constant progress of the attackers, it is impossible to thwart completely the attacks against the IC systems, even if they have very sophisticated security

strategies. Moreover there are no systems totally immune to attacks. At the present time, for example, one of the security key points is the use of firewalls, which are designed to keep the intruders outside of the network. The difficulty is that once the firewall is compromised, it is neither possible to guarantee the integrity of the information nor of the IC network.

The unavailability of certain component because of a cyberattack is not really important for the operation of a power system, as long as the function that offers the component is guaranteed for the network in a correct way. In this thesis, the word continuity involves both the availability and the integrity of the function. Therefore, once the attack is made, we infer the continuity of the function by assessing the asset and IC network survivability.

ix. Survivability of the ICS to cyberattack of the target – Vulnerability assessment

In the computers and communications fields, the survivability refers to the capability of an asset, system, subsystem, process, to fulfil its mission, in a timely manner, even if a part of their functions or their sub-components are compromised by the occurrence an unwanted event [ELL, 1999] [MEA, 2000]. The survivability assessment of a network concerns the quantification of the satisfactory continuity of its requirements (for example, reliability, real-time responsiveness) in the face of adverse conditions [NEU, 1993], such as a cyberattack against IC assets.

We will calculate the survivability estimating whether the assets or the network dispose intrusion detection systems and if there are redundant components, data replication, system backup and restoration. Another attribute in order to determine the survivability is the existence of contingency planning.

The states of this variable are:

Survivability of the network		
high survivability	average survivability	low survivability

The continuity of the function is then inferred as shown in the Figure 6-8:

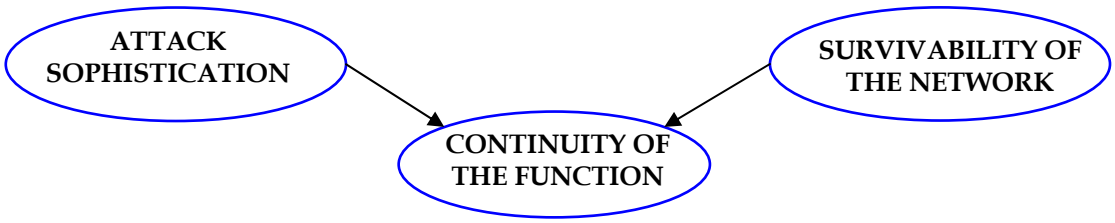


Figure 6-8. Relevant variables influencing the continuity of the function assured by the asset of the ICS.

The states of the variable "continuity of the function" are:

Continuity of the function			
Continuity of the function	Continuity with loss of confidentiality	Non Integrity of the function	Unavailability of the function

This variable can be evaluated also using network simulators so that more accurate indicators on operation of the ICS can be found, e.g., the time of unavailability.

F. Consequence for the power system operation - Dependency assessment

This variable captures a priori knowledge of the criticality of an IC system component in the power system operation. The variable refers to how critical the forced unavailability or non integrity of a given IC component is for the power system. At this point, the interdependency of both the ICS and the power system is shown.

Basically, the impact of a cyberattack on the power system is dependent on several factors. The first one refers to the unauthorized effect of the cyberattack on the component of the communications system; the second factor relates to the type of functions that the IC asset carries out inside the power system and the criticality of each function; the third factor is related to the criticality of the component of the power system which is controlled by the IC asset; the final factor concerns the operating state of the power system at the moment when the cyberattacks occurs.

x. Criticality and Type of functions realised by the target

For the operation of the power system it is not really important if any of the functions of the power system stop working for a certain time, but this is dependent on how critical the function that the asset is carrying out actually is. For this reason, the type of functions carried out by the component of the ICS must be specified for procuring an indicator. For example, a server which executes certain functions of human resources management and which is connected to the IC system is important for the utility but without importance for the operation of the power system. As opposed to this, the fault of a controller can be serious since it can stop the sending of data which is absolutely necessary for the command of a component in the power grid and the avoidance of a major failure.

Therefore, for every target the type of function that it carries out should be specified according to the following categories: protection, switching control, voltage/power control, enhanced control, monitoring, measurement, management, and other functions. The functions of the network appliances should be associated with the functions of the control equipments that communicate. We limit the classification to the following categories:

Type of functions executed for the target				
protection	control	monitoring	measurements	management

Currently IED's provide high integration of functions. However, at the moment we relate one function per component.

xi. Criticality of the power systems components controlled/communicated by the target

Similar to the Bayesian network built in Chapter 4, this variable refers to the criticality of the forced unavailability of the components that are controlled by, or that communicate with, the IC asset for the power system performance. We create an order of criticality founded on the base power flow with the aim of obtaining the probability values. However, system operators of the local or regional control centres can assign these values based on their own knowledge of the power system performance, but also on the evidence of incidents that occurred in their power grid and in other electricity utilities. For this estimation, the cause of the event is not important. In most of the utilities the categorisation normally used in reliability studies is already there.

The criticality of a power system given the forced unavailability of the super-component can be:

Criticality of the Power System components		
High criticality	Average criticality	Low criticality

xii. Operating state of the power systems

In this variable, the operating condition of the power system, which is under the configuration of the studied system, is shown. For example, it is possible that the power system works closely to its operational limits and that for this reason there is a high probability that the system is between the normal state and the state of alert. This variable is included since the functions of the control system are extremely critical when the system is in the condition of emergency or alert. Faults in the system of communications can be tolerated when the system is in normal state.

The states of this variable are defined as follows:

Operating state of the Power System		
normal	alert	emergency

The consequence for the power system is then inferred as shown in the Figure 6-9.

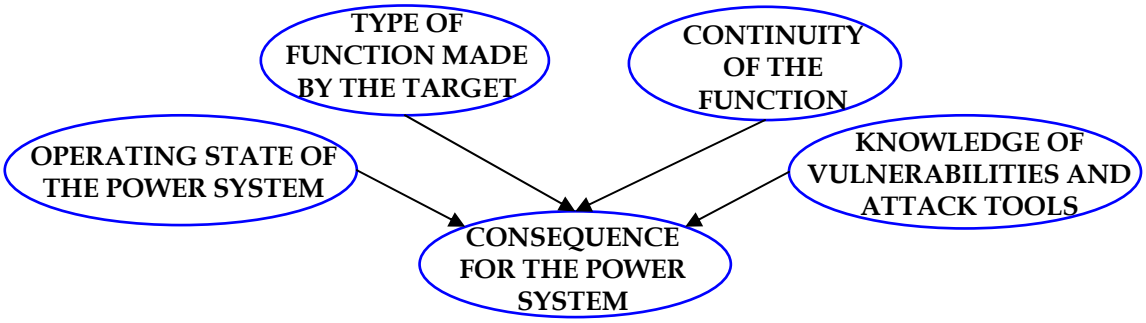


Figure 6-9. Relevant variables to infer the consequence for the system given the cyberattack against the IC asset.

The states of the variable "consequence for the system" are:

Consequence for the power system				
Catastrophic	High	Medium	Low	No attack

The conditional probabilities between these variables are supplied by the operators of the power system with the help of simulation tools. It can be noticed that this variable of the Bayesian network concerns part of the power grid.

Based on some interviews with control centre dispatchers and substation operators as well as on the survey [GAR, 2006], Table 6-V gives a suggestion of how to identify the criticality of functions for the power system operation. Suggestions are oriented to substation functions.

TABLE 6-V: GUIDELINES TO ESTIMATE HOW CRITICAL THE FUNCTIONS EXECUTED BY AN IC COMPONENT IN A SUBSTATION[5] FOR THE OPERATION OF THE POWER SYSTEM ARE

Importance	Function of the power system operation affected	Description
Highly Critical	***PROTECTION*** All protection functions required (Line, Transformer, Generator, Busbar) • Distance protection • Overcurrent protection • Differential protection • Thermal overload protection • Busbar protection • Breaker failure protection	Here, we include the probability that a failure of the ICT system component affects to a higher or lower degree the power system protections. Protections have been designed to limit the damages in power systems. These are important for the detection and elimination of faults or of abnormal conditions on power systems and for the restoration of service. Protections are a vital part of the control system. The failure of protections can seriously affect the power system, initiating a cascade and causing blackout. Using functions described in standard IEC 68150 as reference, these devices are all of those that perform functions with common prefixes "P" (protection). Also, functions of protection related, RREC: Automatic reclosing; RBFR: Breaker failure; RCPW: Carrier wire protection; RPSB: Power swing blocking.
Highly Critical	***SWITCHING CONTROL*** • All control functions of any switchgear: - Circuit breakers - Disconnectors - Grounding switches - Load breakers • Interlocking function • Synchrocheck	This refers to the probability that the unavailability of the component affects to a higher or lower degree the control system of switching operations of the power system. Switching local control is in charge of sending signals to process level, which will open or close a switch. Interlocking conditions must be checked (isolator switched under load, isolator switched to ground, equipment isolated before being grounded, tag of the operational equipment). The main target of interlocking is to block the opening or closing of a switch and to avoid equipment damage or the endangerment human health. IEC 61850 functions concerned are: RSYN: Synchrocheck; CSWI: Switch controller; CPOW: Point on wave controller; CILO: Interlocking; ITCI: Remote control interface/Telemonitoring interface; IHMI: Operator interface.
Critical	***VOLTAGE/ POWER CONTROL*** • Control of transformer tap positions (Load tap changing transformers and voltage regulators). • Switching of shunt reactive devices as capacitors and change of static VAR compensators. • Change of reference points of flow controlling FACTS devices.	Here, we include the probability that a failure of the component affects in a higher or lower degree the voltage and power basic control. In normal or alert operation state, voltage control is usually completely automated (no human intervention). For example, Under-Load Tap Changer Control (ULTC) can operate in agreement with given set points or operator commands. In emergency state, control actions can also be carried out by the operator. Subsequently, when control actions are not executed at the time required, or bad actions are taken, major problems such as instability can appear. This includes all of the devices performing most of the IEC 61850 functions with common prefix A. ATCC: Automatic tap changer control; AVCO: Automatic voltage control; ARCO: Automatic reactive control.
Critical	***MONITORING*** • Switchgear status condition • Event list • Alarm list • Fault records • Disturbance records	This illustrates the effect of component unavailability, and how it affects, to a greater or lower degree, monitoring functions. Monitoring in a substation provides the state for power circuit breakers, circuit switchers, reclosers, and other operations. Monitoring protection is important to identify coordination problems, misoperations, and maintenance requirements. Due to the critical nature of operator's actions with respect to network equipment, as well as in relation to the security of the personnel who work in the facilities, the possibility of monitoring ambiguities or errors is unsuitable. Checking a continuity of control circuits of circuit breakers and disconnectors. When a problem occurs, monitoring becomes a critical area. Indicators on the monitor to inform the operator of any deviations from normal conditions allowing a decision to be taken in a timely manner. Thus, functions such as monitoring fault events are necessary to determine probable causes and locations and to identify fault-prone areas and system problems. IEC 61850 functions concerned are: RDRE (bay/process level) and RDRS (station level): Disturbance recording; IHMI: Operator interface; ITMI: Remote monitoring interface.

[5] Four major types of substation are considered: switchyard at a generation station, customer substation, switching substation and distribution substation.

Importance	Function of the power system operation affected	Description
Averagely critical	***ENHANCED CONTROL FUNCTIONS***	IEC 61850 functions concerned are referenced as GAPC: Automatic process control. • Switching sequences • Automatic changes of busbar • Intelligent autoreclose • Automatic load shedding • Intelligent power restoration
Averagely critical	***MEASUREMENT***	Measurement of analogue quantities in a power system, as values from current transformers and voltage transformers. IEC 61850 functions concerned are : MSQI: Sequences and imbalances; MHAI: Harmonics and interharmonics.
Lowly critical	***MANAGEMENT and COORDINATION***	IEC 61850 functions concerned are : IARC: Archiving of historical data MMTR: Metering for commercial purpose
Lowly critical	***OTHERS***	Other operating functions of the power system no before mentioned.

This classification can be of great help at the moment when the conditional probabilities between the function, which has been affected by a cyberattack, and the impact of the cyberattack on the operation of the power system have to be established.

6.4.1.5 Obtaining the Bayesian Network

The complete implemented Bayesian network is shown in Figure 6-10.

We have constructed the Bayesian network taking into account factors with high levels of uncertainty, such as the motivation of the assailant, as much as technical aspects like those of the information and communication network and the power grid. The *a priori* conditional probabilities must be evaluated by experts. We will show the process for a simple example in the following section.

It can be noticed that the principal variables inferred from the Bayesian network represent fundamental parts in any process of risk evaluation.

We would like to draw attention to the fact that in the Bayesian network, the probability of a cyberterrorist attack on a specific target is found in the node "sophistication of the attack". This probability depends on a group of variables that are unnecessary for the following evaluation of the effect on the IC network and on the power grid. The Bayesian network is then modular since we can integrate the results of this node into any other tool for interdependencies analysis in order to evaluate the impact of a cyberattack on a specific target.

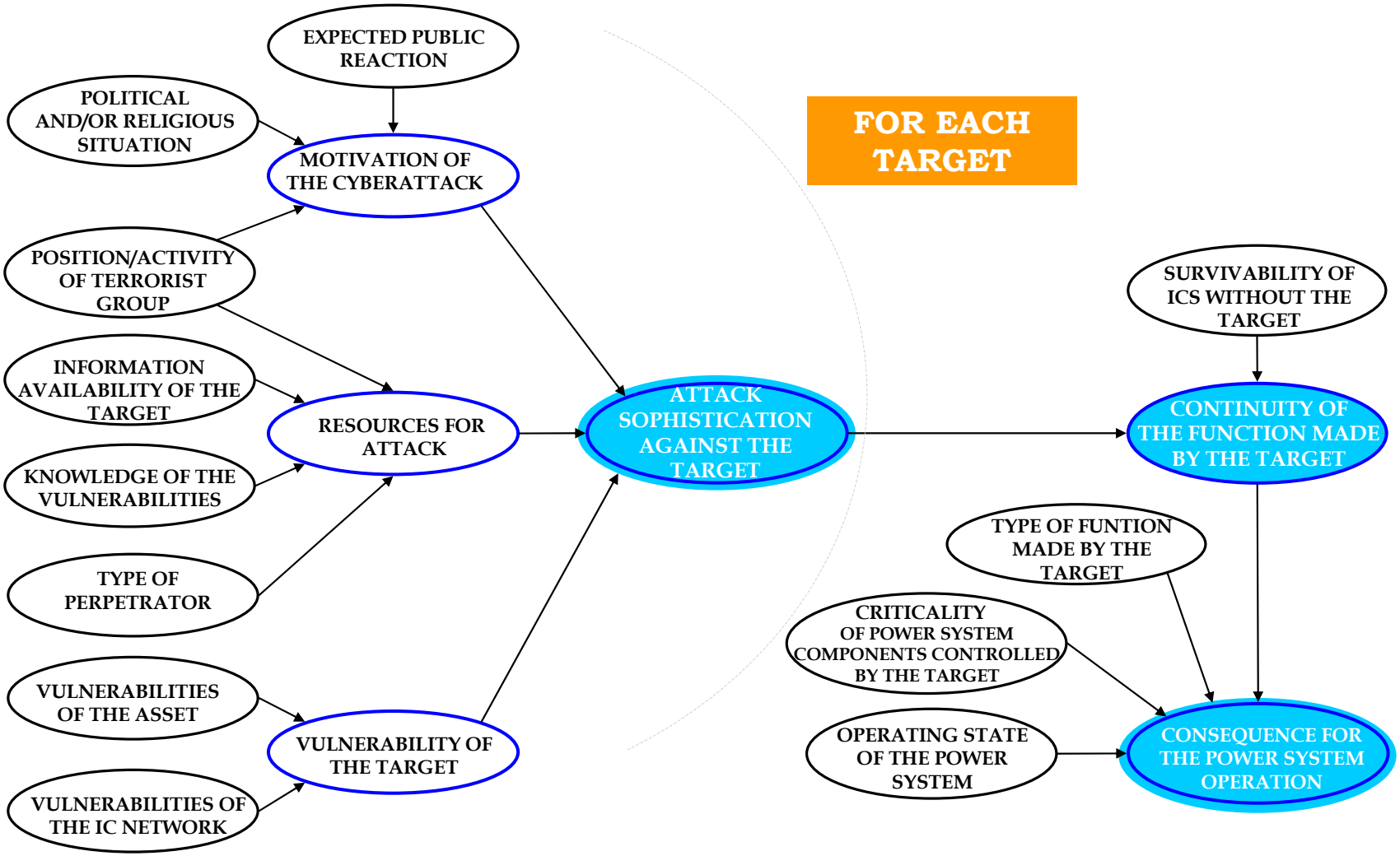


Figure 6-10. Risk assessment of power system security with regard to cyberattacks.

6.5 Study case

We will study the possibility of cyberattacks on certain substations of the power system WSCC 9-bus test system, which we have used along this thesis. However, this test system will be now used to analyse the security of the power system with regard to cyberattacks on the information and communications system.

As mentioned before, the consulted utilities did not give any specific information about their IC system in compliance with their security policy. Based on the few pieces of information available, we create some scenarios that will be useful to understand the performance of the Bayesian network. We simplify some state of variables of the Bayesian network due to the lack of knowledge from experts to obtain the conditional probabilities.

General assumptions

One of the major threats against to IC systems is an attack committed by an insider or a former-insider. Because terrorists have the intention to cause damage, we have simplified the possible states of the variable "type of perpetrator" assuming that we will always be able to categorise the attacker as an insider, an ex-insider and as a professional cracker. Moreover, this variable is of main importance when the resources for the attack are to be defined.

The conditional probabilities of the variable "sophistication of the cyberattack" are determined assuming that, in order to carry out an attack against the IC network with consequences for the integrity, requires more resources, high vulnerably of the target and a high motivation. Consequently, we categorize: loss of integrity, loss of availability and loss of confidentiality. We assume that any loss of integrity or availability implies a loss of confidentiality. In our study we also presuppose that for control functions attacks with loss of integrity are more severe than attacks with loss of availability. Thus, for the sake of simplicity in the evaluation of conditional probabilities, the case of loss of integrity and availability (simultaneously) will be classified as loss of integrity. However, the requirement of security: availability, integrity and confidentiality must be established for each asset taking into account its function and its interconnections.

We assume that the security policy of the utilities is to create a perimeter of defence but also to secure every asset individually. Therefore, the vulnerability of every asset is a combination, in the same proportion, of the vulnerability of the network and of the component.

Once the attack occurs, though the IC infrastructure can assure the continuity of the affected function (control and protection), there will always be a consequence, even if it is low, as we assume that the reliability is diminished due to the use of backup equipments.

6.5.1 Scenario of cyber – terrorism against the power system

We want to assess the risk for the security of the power test system assessment. In the grey square we describe the scenario, which will be analyzed. This scenario concerns substations 5, 6 and 8 in the WSCC 9 - bus test system which is illustrated in Appendix B. These substations are important for the power system because they are load nodes of the system.

A rich radical group stemming from an ethnic minority in one country strives for political independence. The major part of this ethnic minority does not share the radicals' ambition as their region (where is located substation 5) disposes of far-reaching autonomy and the economical exchanges with other parts of the country contributes to their high living standards. The electricity of the region is delivered by the national power company. It is a week before the regional elections and activity of the insurgents is expected.
The utility knows that an ex-employee who maintained the control equipment in the substation 5 belongs to this minority and that the group collaborates with crackers. The control systems of the substations 5, 4 and 8 were recently renewed almost in an identical way and the communications work under the norm 61850. In addition, it is known that the employee replaced another worker in substation 8.
This case presents a stable political situation with an insurgents group of weak political influence but sufficient economic resources. The terrorist have sympathisers in whole country. The group could take action as they expect some public attention because of the specifics of the installation they attack as well as the circumstance that elections take place. As former insiders their knowledge on the operation of the power system is high.

Performance of the test power system

After performing the power system load flow, we conclude that this system is not very secure, since it does not always stay in normal state under the condition N-1. Therefore, a component of the power system is designated: "very important" in the case that the loss of this component can lead to the transition of the power system from the normal state to a emergency state or when there is a very significant loss of load; "important" if the loss of the component leads the power system near to the operational limits; and "normal" if the loss of the component does not affect the behaviour of the system.

The limits of the line loadability are of 3 p.u. and unusually line overloads are produced. In real life, power system operators know this classification and in many utilities this categorization is already done.

As the power system has security problems, conditional probabilities between the operating state and other variables of the Bayesian network, which determine the consequence for the power system in view of the cyberattack, need to reflect the probability that the system moves quickly from the normal state to the emergency state.

Description of substations of the power system

We assume that the IC network of the substations only executes functions of switching control, protection and measurements for metering and maintenance. The measures for control are assumed as functions of control. Protection, metering and control applications reside in different devices. The setting and maintenance of a controller bay and IEDs is normally performed by technicians who access maintenance ports through remote dial-up connections. There is a bay unit for each entering line. Every bay has a bay controller and 2 IEDs (intelligent electronic devices) associated with the protection and metering functions. The bay equipment is not back upped.

Hierarchically, the substation system is divided into three levels: the process, the bay and the station levels. In general, the substation primary equipment is HV components and switchgear with associated sensor and actuators that are habitually located in the process level. Secondary equipment is the protection and control equipment on bay level and on station level.

The functions carried out in every substation are:

STATION LEVEL	Server of the substation Back-up	Switchgear control Synchrocheck relay setting read/write
	Human machine interface Monitor Back-up	Switchgear status graphical display Line/Bus display Alarms display
		Communication with the bay level
BAY LEVEL	Bay unit	Communication with the station level
		Synchrocheck function
		IED settings /read - write
		Line/Bus voltage estimation
		Local alarms
		Communication with the process level
PROCESS LEVEL	IED for each function	Depending on the function Switchgear operation – command Protection of lines and busbar
		HV Status acquisition - data
		Communication with the bay unit

Figure 6-11 shows the LAN network inside the control building.

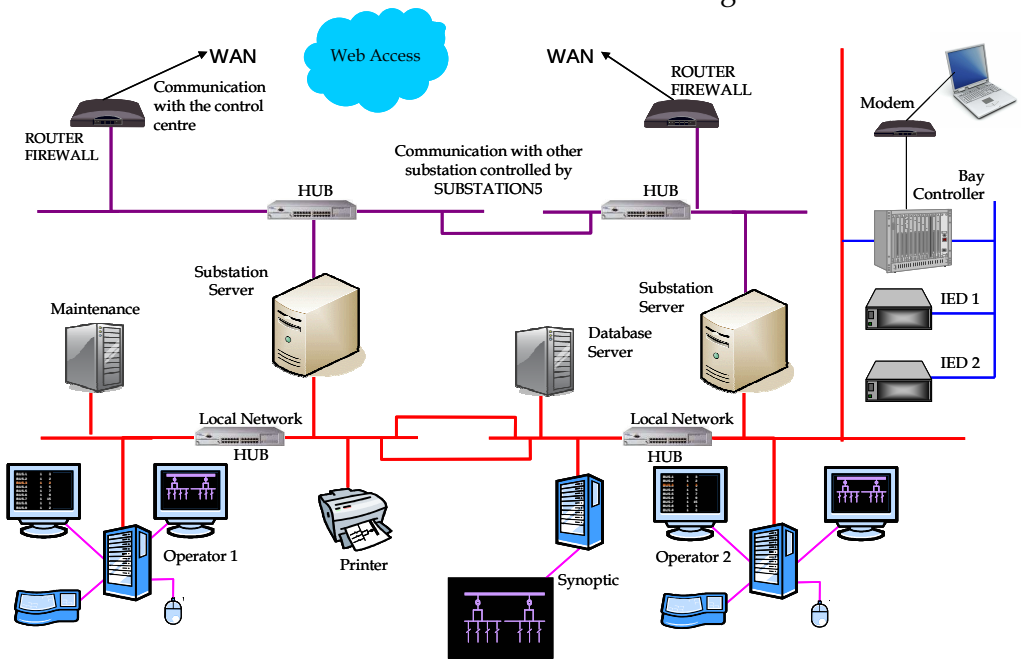


Figure 6-11. IC network of substations.

In Appendix E, tables of the conditional probabilities are illustrated. We remember that all of these conditional probabilities can be changed by experts and updated on the basis of evidence, i.e. when attacks against the communication and information system take place.

Evaluation of marginal probabilities for the specific scenario

From the described scenario we can deduce that the political situation can worsen within this period, that the group in spite of being a minority has sufficient financial resources and that the public reaction concerning an attack on a substation in zone 5 is more important than in

other zones. Although terrorist group has sufficient resources and sympathisers in the whole country, for obvious reasons we assume that it has major influence in the zone of substation 5.

The possible scenarios comprise a high probability that the attacker is a former-insider of substation 5. Due to the similarity of the substations, it is believed that there is also a probability that the "former insider" attacks the other two substations though with a lower probability.

The assets that we will take into account in our risk evaluation are shown in the following table, in which we include some vulnerability analysis for every asset and the importance of the power system components that controls/connects the IC asset.

IC ASSET	Information Asset	Vulnerab. Asset	New vulnerab. discovered?	Importance POWSYS components
Substation server SUB 5	Medium	Low	Non	Very important
Database server SUB 5	Medium	Low	Yes	Very important
Human-machine interface SUB 5	Medium	High	Non	Very important
IED 51 – Protections bay unit 1; L5-4 – busbar 1	High	Low	Non	Very important
IED 52 – Metering bay unit 1	High	Low	Non	Very important
IED 53 – Protection s bay unit 2; L7-5 – busbar 2	High	Low	Non	Very important
IED 54 – Metering bay unit 2	High	Low	Non	Very important
Substation server SUB 6	Medium	Low	Non	Very important
Database server SUB 6	Medium	Low	Yes	Very important
Human-machine interface SUB 6	Medium	Low	Non	Very important
IED 61 – Protections bay unit 1; L6-4 – busbar 1	High	Medium	Non	Normal
IED 62 – Metering bay unit 1	High	Medium	Non	Normal
IED 63 – Protection s bay unit 2; L6-9 – busbar 2	High	Medium	Non	Less important
IED 64 – Metering bay unit 2	High	Medium	Non	Normal
Substation server SUB 8	Medium	Low	Non	Very important
Database server SUB 8	Medium	Low	Yes	Very important
Human-machine interface SUB 8	Medium	Low	Non	Very important
IED 81 – Protections bay unit 1; L7-8 – busbar 1	High	Low	Non	Less important
IED 82 – Metering bay unit 1	High	Low	Non	Less important
IED 83 – Protection s bay unit 2; L9-8– busbar 2	High	Low	Non	Less important
IED 84 – Metering bay unit 2	High	Low	Non	Less important

We have changed arbitrarily some vulnerability values of every substation's components, since we believe that the fulfilment with certain security policies is handled differently in every substation.

According to the scenario and the conditions of security and reliability of the IC system, the probabilities of the independent variables are elicited from experts and are shown in Table 6-VI. Because the objective of this assessment is to find out a measurement of the risk for the power system due to an attack on the communications system, and the three substations were recently renewed, some probabilities values are similar. We realize that all the substations' IC networks have low vulnerable feature which diminishes the probability of the attack. Nevertheless, due to the standardization, some components as IEDs are widely documented and information is publicly available in books and specialised journals.

We have included this example to show the case of a security assessment of substations by using a risk measurement of every asset modelled. This allows us to see comparatively

where measures of mitigation should be focussed in order to avoid security problems in the power system. We have given an example in which a major threat is supposed to exist (the former-insider) and in a case where there is a similarity between the IC components.

TABLE 6-VI. PROBABILITY VALUES OF THE BAYESIAN NETWORK INDEPENDENT VARIABLES: WSCC 9-BUS TEST SYSTEM – CASE CYBERATTACKS

		ExpRea			PolSit			PosTer			VulAss			VulNet			TypPer		
	ASSET	High	Medi	Low	Crit	Mode	NoCr	High	Aver	Low	High	Medi	Low	High	Medi	Low	Insi	ExIn	Crim
Ser SUB 5	1	0.663	0.301	0.036	0.093	0.583	0.324	0.200	0.632	0.168	0.041	0.060	0.899	0.064	0.037	0.898	0.120	0.800	0.080
Datab SUB 5	2	0.663	0.301	0.036	0.093	0.583	0.324	0.200	0.632	0.168	0.041	0.106	0.853	0.064	0.037	0.898	0.120	0.800	0.080
HMI SUB 5	3	0.663	0.301	0.036	0.093	0.583	0.324	0.200	0.632	0.168	0.430	0.100	0.470	0.064	0.037	0.898	0.120	0.800	0.080
IED 51	4	0.663	0.301	0.036	0.093	0.583	0.324	0.200	0.632	0.168	0.063	0.261	0.676	0.064	0.037	0.898	0.120	0.800	0.080
IED 52	5	0.663	0.301	0.036	0.093	0.583	0.324	0.200	0.632	0.168	0.063	0.261	0.676	0.064	0.037	0.898	0.120	0.800	0.080
IED 53	6	0.663	0.301	0.036	0.093	0.583	0.324	0.200	0.632	0.168	0.063	0.261	0.676	0.064	0.037	0.898	0.120	0.800	0.080
IED 54	7	0.663	0.301	0.036	0.093	0.583	0.324	0.200	0.632	0.168	0.063	0.261	0.676	0.064	0.037	0.898	0.120	0.800	0.080
Ser SUB 6	8	0.426	0.395	0.179	0.115	0.452	0.433	0.134	0.354	0.512	0.000	0.106	0.894	0.204	0.036	0.760	0.050	0.600	0.350
Datab SUB 6	9	0.426	0.395	0.179	0.115	0.452	0.433	0.134	0.354	0.512	0.045	0.108	0.847	0.204	0.036	0.760	0.050	0.600	0.350
HMI SUB 6	10	0.426	0.395	0.179	0.115	0.452	0.433	0.134	0.354	0.512	0.091	0.108	0.801	0.260	0.035	0.705	0.050	0.600	0.350
IED 61	11	0.426	0.395	0.179	0.115	0.452	0.433	0.134	0.354	0.512	0.289	0.637	0.074	0.260	0.035	0.705	0.050	0.600	0.350
IED 62	12	0.426	0.395	0.179	0.115	0.452	0.433	0.134	0.354	0.512	0.289	0.637	0.074	0.260	0.035	0.705	0.050	0.600	0.350
IED 63	13	0.426	0.395	0.179	0.115	0.452	0.433	0.134	0.354	0.512	0.289	0.637	0.074	0.260	0.035	0.705	0.050	0.600	0.350
IED 64	14	0.426	0.395	0.179	0.115	0.452	0.433	0.134	0.354	0.512	0.289	0.637	0.074	0.260	0.035	0.705	0.050	0.600	0.350
Ser SUB 8	15	0.080	0.554	0.366	0.032	0.367	0.601	0.134	0.354	0.512	0.135	0.082	0.783	0.012	0.140	0.848	0.050	0.400	0.550
Datab SUB 8	16	0.080	0.554	0.366	0.032	0.367	0.601	0.134	0.354	0.512	0.050	0.026	0.924	0.012	0.140	0.848	0.050	0.400	0.550
HMI SUB 8	17	0.080	0.554	0.366	0.032	0.367	0.601	0.134	0.354	0.512	0.050	0.167	0.783	0.012	0.140	0.848	0.050	0.400	0.550
IED 81	18	0.080	0.554	0.366	0.032	0.367	0.601	0.134	0.354	0.512	0.023	0.112	0.865	0.012	0.140	0.848	0.050	0.400	0.550
IED 82	19	0.080	0.554	0.366	0.032	0.367	0.601	0.134	0.354	0.512	0.023	0.112	0.865	0.012	0.140	0.848	0.050	0.400	0.550
IED 83	20	0.080	0.554	0.366	0.032	0.367	0.601	0.134	0.354	0.512	0.023	0.112	0.865	0.012	0.140	0.848	0.050	0.400	0.550
IED 84	21	0.080	0.554	0.366	0.032	0.367	0.601	0.134	0.354	0.512	0.023	0.112	0.865	0.012	0.140	0.848	0.050	0.400	0.550

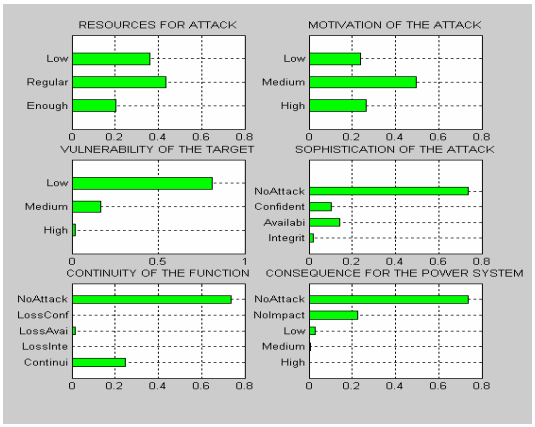
		KnoVul			InfTar			SurNet			CriFun			CriCom			OpeSta		
	ASSET	Enou	Regu	Low	Enou	Regu	Low	High	Medi	Low	PrCo	Prot	Meas	High	Aver	Low	Norm	Aler	Emer
Ser SUB 5	1	0.000	0.100	0.900	0.119	0.694	0.187	0.975	0.025	0.000	1.000	0.000	0.000	1.000	0.000	0.000	1.000	0.000	0.000
Datab SUB 5	2	0.000	0.700	0.300	0.119	0.694	0.187	0.975	0.025	0.000	0.000	0.000	1.000	1.000	0.000	0.000	1.000	0.000	0.000
HMI SUB 5	3	0.000	0.200	0.800	0.119	0.694	0.187	0.975	0.025	0.000	1.000	0.000	0.000	1.000	0.000	0.000	1.000	0.000	0.000
IED 51	4	0.000	0.200	0.800	0.785	0.131	0.084	0.000	0.100	0.900	0.000	1.000	0.000	0.800	0.200	0.000	1.000	0.000	0.000
IED 52	5	0.000	0.200	0.800	0.785	0.131	0.084	0.000	0.100	0.900	0.000	0.000	1.000	0.800	0.200	0.000	1.000	0.000	0.000
IED 53	6	0.000	0.200	0.800	0.785	0.131	0.084	0.000	0.100	0.900	0.000	1.000	0.000	0.750	0.250	0.000	1.000	0.000	0.000
IED 54	7	0.000	0.200	0.800	0.785	0.131	0.084	0.000	0.100	0.900	0.000	0.000	1.000	0.750	0.250	0.000	1.000	0.000	0.000
Ser SUB 6	8	0.000	0.100	0.900	0.119	0.694	0.187	0.975	0.025	0.000	1.000	0.000	0.000	0.850	0.150	0.000	1.000	0.000	0.000
Datab SUB 6	9	0.000	0.700	0.300	0.119	0.694	0.187	0.975	0.025	0.000	0.000	0.000	1.000	0.850	0.150	0.000	1.000	0.000	0.000
HMI SUB 6	10	0.000	0.200	0.800	0.119	0.694	0.187	0.975	0.025	0.000	1.000	0.000	0.000	0.850	0.150	0.000	1.000	0.000	0.000
IED 61	11	0.000	0.200	0.800	0.785	0.131	0.084	0.000	0.100	0.900	0.000	1.000	0.000	0.650	0.350	0.000	1.000	0.000	0.000
IED 62	12	0.000	0.200	0.800	0.785	0.131	0.084	0.000	0.100	0.900	0.000	0.000	1.000	0.450	0.500	0.050	1.000	0.000	0.000
IED 63	13	0.000	0.200	0.800	0.785	0.131	0.084	0.000	0.100	0.900	0.000	1.000	0.000	0.200	0.550	0.250	1.000	0.000	0.000
IED 64	14	0.000	0.200	0.800	0.785	0.131	0.084	0.000	0.100	0.900	0.000	0.000	1.000	0.200	0.550	0.250	1.000	0.000	0.000
Ser SUB 8	15	0.000	0.100	0.900	0.119	0.694	0.187	0.975	0.025	0.000	1.000	0.000	0.000	0.800	0.200	0.000	1.000	0.000	0.000
Datab SUB 8	16	0.000	0.700	0.300	0.119	0.694	0.187	0.975	0.025	0.000	0.000	0.000	1.000	0.800	0.200	0.000	1.000	0.000	0.000
HMI SUB 8	17	0.000	0.200	0.800	0.119	0.694	0.187	0.975	0.025	0.000	1.000	0.000	0.000	0.800	0.200	0.000	1.000	0.000	0.000
IED 81	18	0.000	0.200	0.800	0.785	0.131	0.084	0.000	0.100	0.900	0.000	1.000	0.000	0.000	0.500	0.500	1.000	0.000	0.000
IED 82	19	0.000	0.200	0.800	0.785	0.131	0.084	0.000	0.100	0.900	0.000	0.000	1.000	0.000	0.500	0.500	1.000	0.000	0.000
IED 83	20	0.000	0.200	0.800	0.785	0.131	0.084	0.000	0.100	0.900	0.000	1.000	0.000	0.000	0.480	0.520	1.000	0.000	0.000
IED 84	21	0.000	0.200	0.800	0.785	0.131	0.084	0.000	0.100	0.900	0.000	0.000	1.000	0.000	0.480	0.520	1.000	0.000	0.000

6.5.2 Simulation

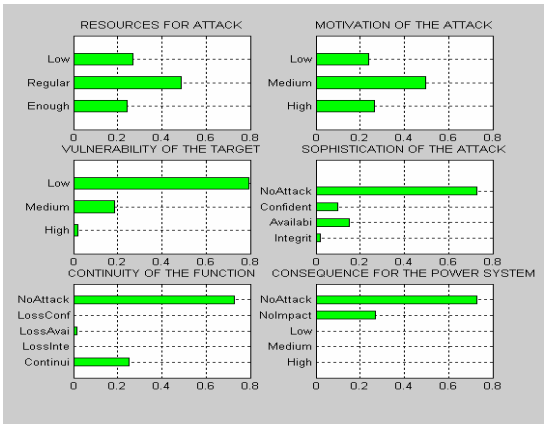
In order to simulate the Bayesian Network, the freeware Bayes Net Toolbox for Matlab 7.0 was used. We have simulated the 21 cases, i.e., one simulation for every modelled asset of the IC network of the power system (7 assets for every substation). The results of the simulation, specifically the probabilities of the dependent variables, are given in Table 6-VII and Figure 6-12.

TABLE 6-VII. PROBABILITY VALUES OF THE BAYESIAN NETWORK DEPENDENT VARIABLES: WSCC 9-BUS TEST SYSTEM – CASE CYBERATTACKS

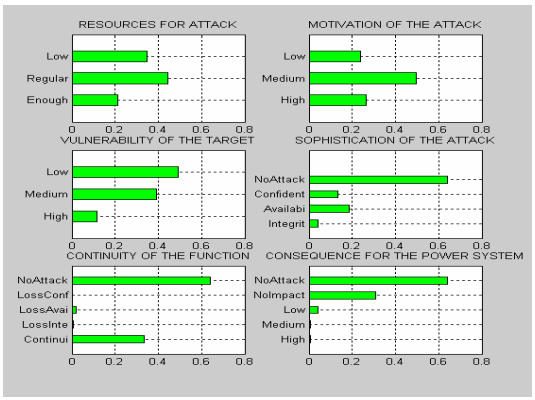
ASSET		Motivation			Resources			Vulnerability			Sophistication Attack				Continuity function					Consequence Power System				
		High	Medi	Low	Enou	Regu	Low	High	Medi	Low	Inte	Avai	Conf	NoAt	Cont	Inte	Avai	Conf	NoAt	High	Medi	Low	NoIm	NoAt
Ser SUB 5	1	0.204	0.497	0.237	0.018	0.434	0.362	0.266	0.169	0.813	0.018	0.143	0.104	0.735	0.246	0.002	0.016	0.001	0.735	0.017	0.001	0.123	0.124	0.735
Datab SUB 5	2	0.243	0.497	0.237	0.019	0.486	0.271	0.266	0.187	0.794	0.022	0.151	0.099	0.728	0.252	0.002	0.017	0.001	0.728	0.000	0.000	0.003	0.269	0.728
HMI SUB 5	3	0.210	0.497	0.237	0.116	0.443	0.347	0.266	0.391	0.493	0.043	0.185	0.133	0.639	0.334	0.005	0.020	0.002	0.639	0.024	0.001	0.167	0.168	0.639
IED 51	4	0.428	0.497	0.237	0.027	0.334	0.238	0.266	0.261	0.712	0.036	0.172	0.101	0.691	0.043	0.031	0.148	0.087	0.691	0.133	0.032	0.023	0.121	0.691
IED 52	5	0.428	0.497	0.237	0.027	0.334	0.238	0.266	0.261	0.712	0.036	0.172	0.101	0.691	0.043	0.031	0.148	0.087	0.691	0.000	0.000	0.073	0.236	0.691
IED 53	6	0.428	0.497	0.237	0.027	0.334	0.238	0.266	0.261	0.712	0.036	0.172	0.101	0.691	0.043	0.031	0.148	0.087	0.691	0.131	0.035	0.023	0.121	0.691
IED 54	7	0.428	0.497	0.237	0.027	0.334	0.238	0.266	0.261	0.712	0.036	0.172	0.101	0.691	0.043	0.031	0.148	0.087	0.691	0.000	0.000	0.073	0.237	0.691
Ser SUB 6	8	0.136	0.437	0.417	0.025	0.379	0.485	0.146	0.206	0.769	0.011	0.108	0.115	0.766	0.219	0.001	0.012	0.001	0.766	0.012	0.001	0.100	0.121	0.766
Datab SUB 6	9	0.151	0.437	0.417	0.040	0.450	0.400	0.146	0.225	0.735	0.015	0.117	0.114	0.755	0.229	0.002	0.013	0.001	0.755	0.000	0.000	0.002	0.243	0.755
HMI SUB 6	10	0.138	0.437	0.417	0.065	0.391	0.471	0.146	0.255	0.680	0.016	0.119	0.124	0.740	0.243	0.002	0.013	0.002	0.740	0.014	0.001	0.111	0.134	0.740
IED 61	11	0.289	0.437	0.417	0.167	0.387	0.324	0.146	0.527	0.306	0.046	0.180	0.153	0.621	0.053	0.039	0.155	0.132	0.621	0.136	0.045	0.028	0.169	0.621
IED 62	12	0.289	0.437	0.417	0.167	0.387	0.324	0.146	0.527	0.306	0.046	0.180	0.153	0.621	0.053	0.039	0.155	0.132	0.621	0.000	0.000	0.099	0.280	0.621
IED 63	13	0.289	0.437	0.417	0.167	0.387	0.324	0.146	0.527	0.306	0.046	0.180	0.153	0.621	0.053	0.039	0.155	0.132	0.621	0.102	0.083	0.027	0.167	0.621
IED 64	14	0.289	0.437	0.417	0.167	0.387	0.324	0.146	0.527	0.306	0.046	0.180	0.153	0.621	0.053	0.039	0.155	0.132	0.621	0.000	0.000	0.097	0.283	0.621
Ser SUB 8	15	0.121	0.351	0.590	0.036	0.350	0.529	0.059	0.226	0.737	0.008	0.081	0.118	0.793	0.196	0.001	0.009	0.001	0.793	0.009	0.001	0.087	0.111	0.793
Datab SUB 8	16	0.127	0.351	0.590	0.014	0.435	0.438	0.059	0.156	0.830	0.006	0.076	0.104	0.814	0.176	0.001	0.008	0.001	0.814	0.000	0.000	0.002	0.185	0.814
HMI SUB 8	17	0.122	0.351	0.590	0.016	0.364	0.514	0.059	0.216	0.767	0.007	0.078	0.114	0.801	0.188	0.001	0.009	0.001	0.801	0.009	0.001	0.083	0.106	0.801
IED 81	18	0.241	0.351	0.590	0.009	0.422	0.337	0.059	0.178	0.813	0.010	0.090	0.099	0.801	0.028	0.008	0.077	0.086	0.801	0.035	0.046	0.016	0.101	0.801
IED 82	19	0.241	0.351	0.590	0.009	0.422	0.337	0.059	0.178	0.813	0.010	0.090	0.099	0.801	0.028	0.008	0.077	0.086	0.801	0.000	0.000	0.057	0.142	0.801
IED 83	20	0.241	0.351	0.590	0.009	0.422	0.337	0.059	0.178	0.813	0.010	0.090	0.099	0.801	0.028	0.008	0.077	0.086	0.801	0.035	0.046	0.017	0.101	0.801
IED 84	21	0.241	0.351	0.590	0.009	0.422	0.337	0.059	0.178	0.813	0.010	0.090	0.099	0.801	0.028	0.008	0.077	0.086	0.801	0.000	0.000	0.057	0.142	0.801



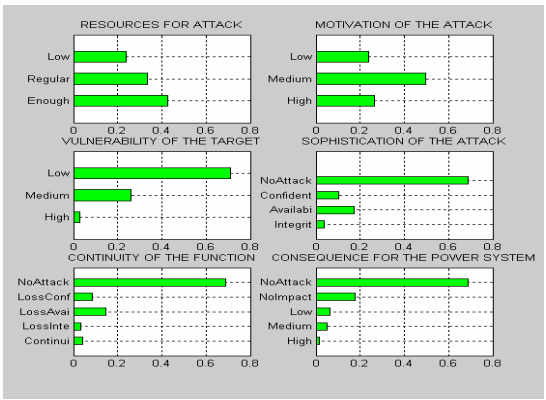
(a) Ser SUB 5



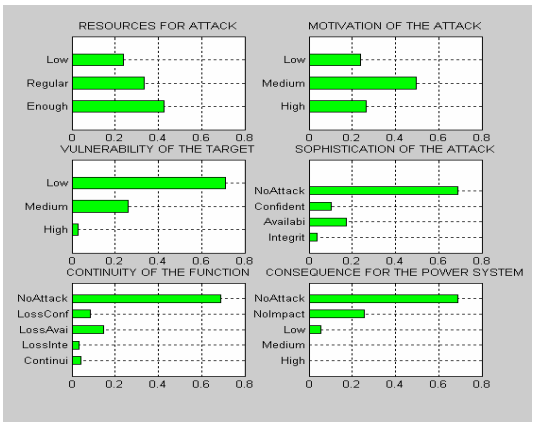
(b) Datab SUB 5



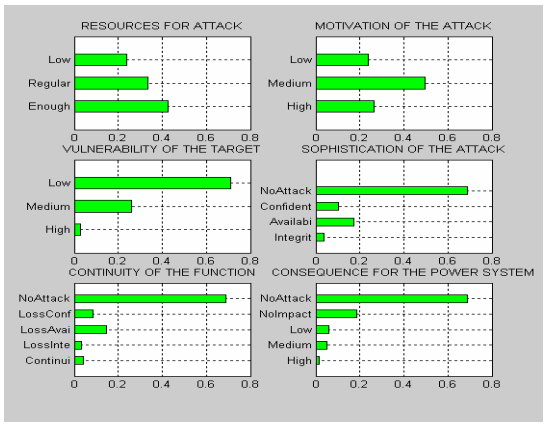
(c) HMI SUB 5



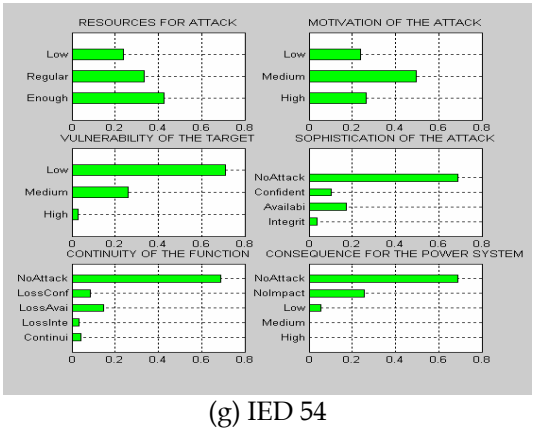
(d) IED 51



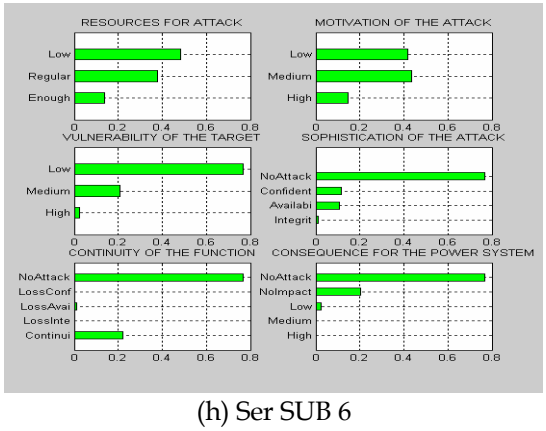
(e) IED 52



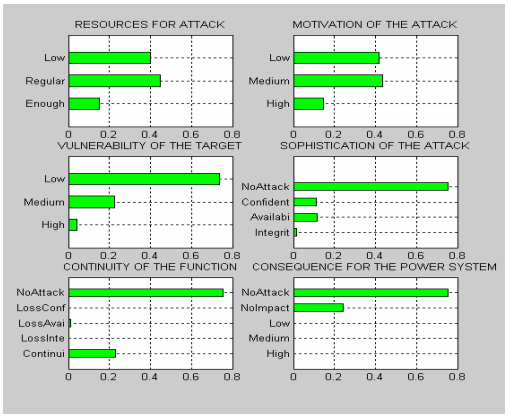
(f) IED 53



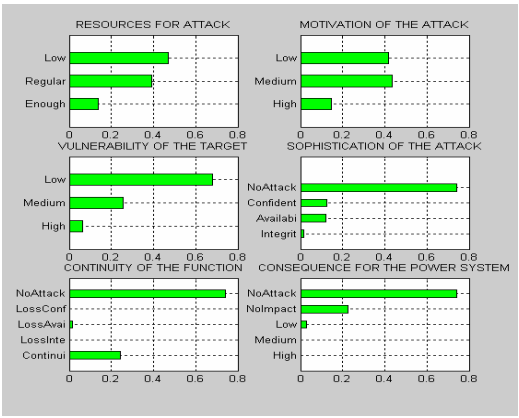
(g) IED 54



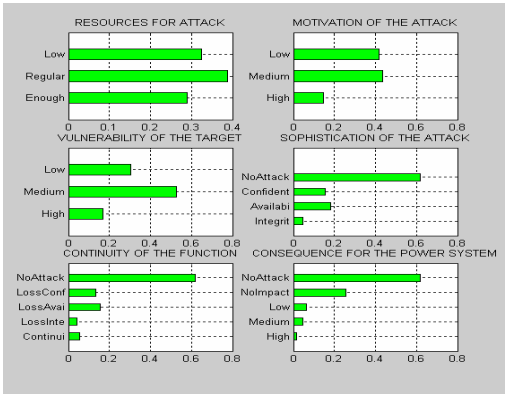
(h) Ser SUB 6



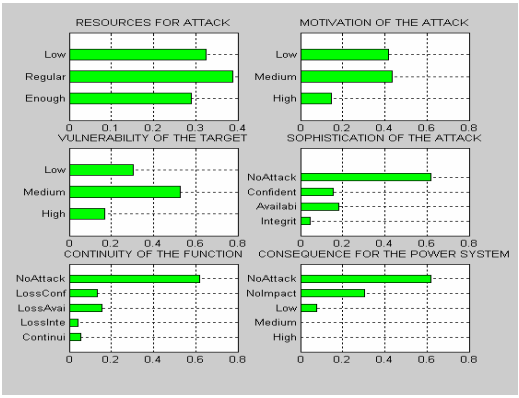
(i) Datab SUB 6



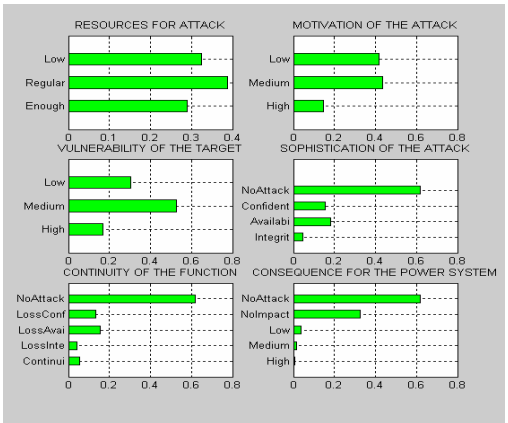
(j) HMI SUB 6



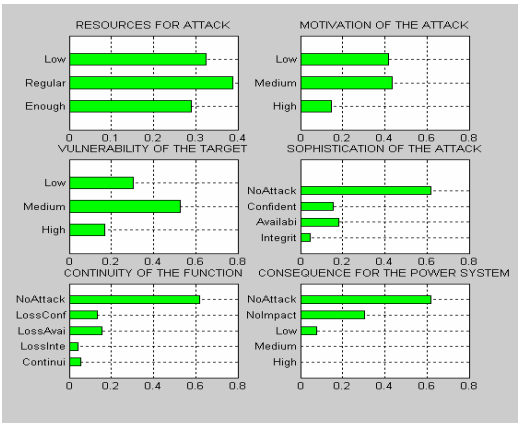
(k) IED 61



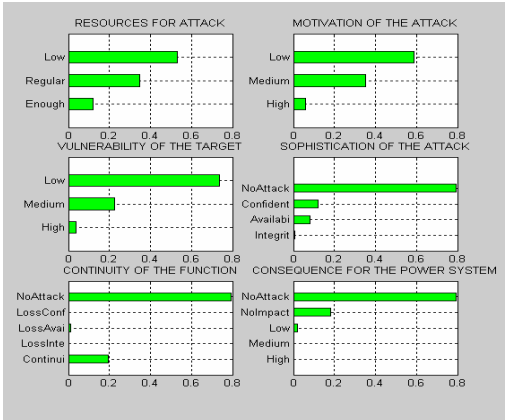
(l) IED 62

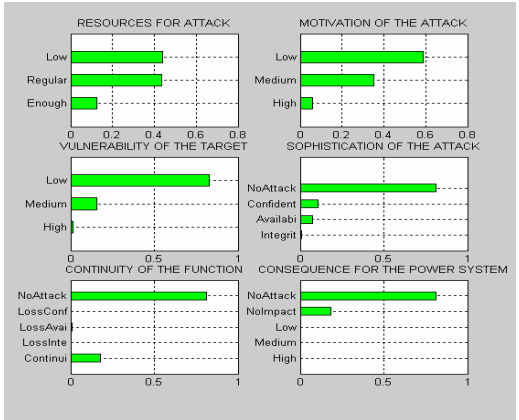


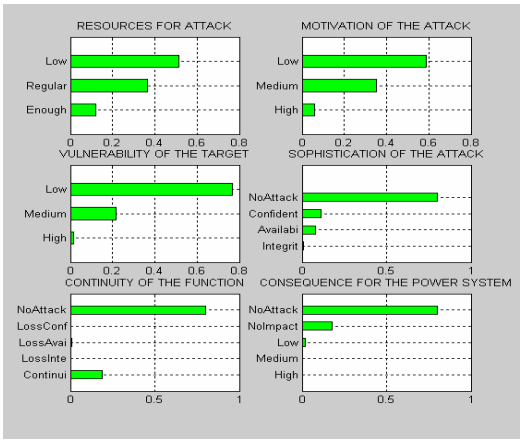
(m) IED 63



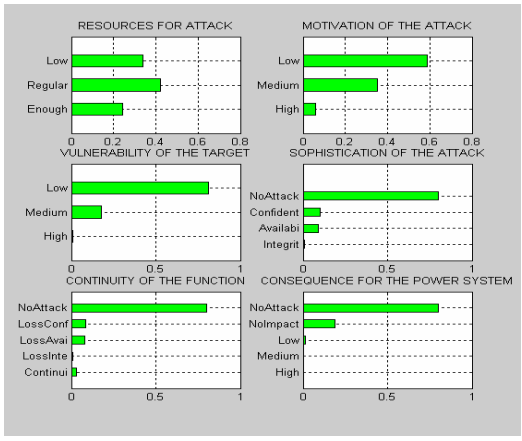
(n) IED 64



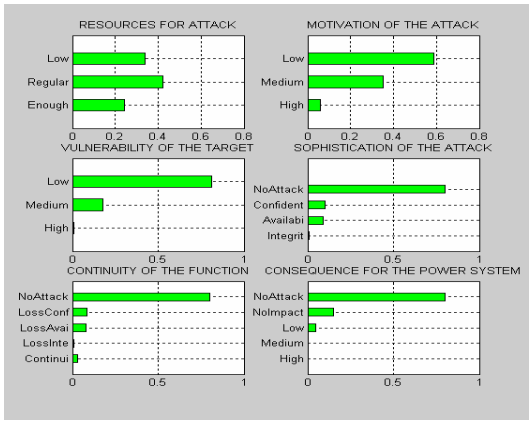




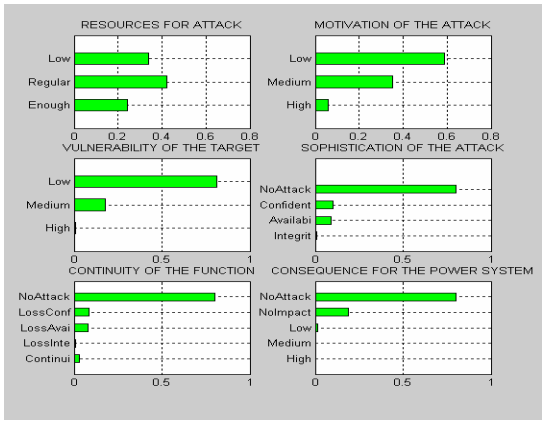
(q) HMI SUB 8



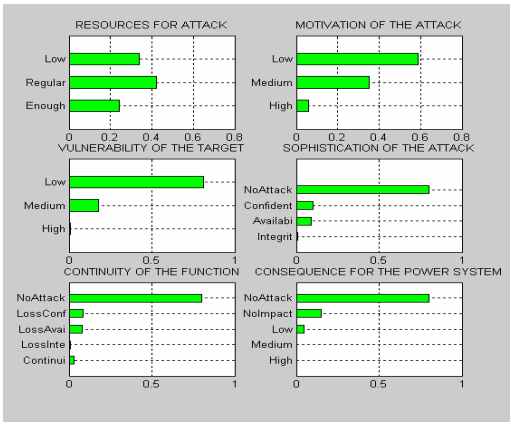
(r) IED 81



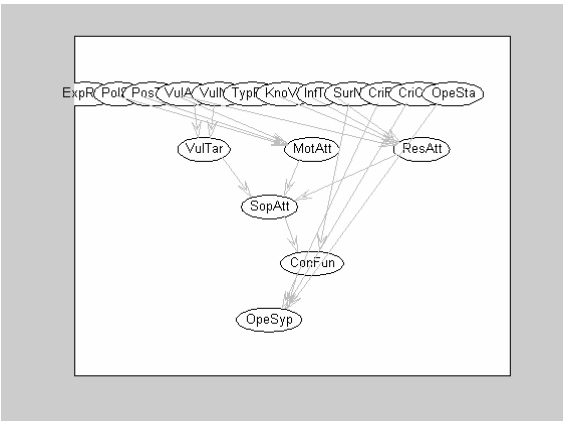
(s) IED 82



(t) IED 83



(u) IED 84



(v) Bayesian Network

Figure 6-12. Bayesian network results for each asset of the IC network

6.5.3 Results analysis

The probability of an attack is calculated in the node "sophistication of the attack" and is shown in Table 6-VIII.

On the basis of the results of the probability of a cyberattack against the substations, we realize considering the political factors, the available information on the components, the specific vulnerabilities of the different assets and of the network, that the IEDs of the substation 6 are the most threatened assets.

TABLE 6-VIII. PROBABILITY OF THE ATTACK AGAINST THE ASSETS OF THE IC NETWORK OF THE POWER SYSTEM

ASSET	SOPHISTICATION OF THE ATTACK				
	Pr (Integrity)	Pr(Availability)	Pr(Confidentiality)	No Attack	Pr Attack
SerSUB5	0.0179	0.1428	0.1044	0.7349	0.2651
DatabSUB5	0.0216	0.1515	0.0989	0.7281	0.2719
HMISUB5	0.0425	0.1852	0.1329	0.6394	0.3606
IED51	0.0363	0.172	0.1012	0.6906	0.3094
IED52	0.0363	0.172	0.1012	0.6906	0.3094
IED53	0.0363	0.172	0.1012	0.6906	0.3094
IED54	0.0363	0.172	0.1012	0.6906	0.3094
SerSUB6	0.0115	0.1078	0.1147	0.766	0.234
DatbaSUB6	0.0147	0.1168	0.1136	0.7549	0.2451
HMISUB6	0.0164	0.1193	0.124	0.7404	0.2596
IED61	0.0458	0.1801	0.1535	0.6206	0.3794
IED62	0.0458	0.1801	0.1535	0.6206	0.3794
IED63	0.0458	0.1801	0.1535	0.6206	0.3794
IED64	0.0458	0.1801	0.1535	0.6206	0.3794

After analysing the simulation's results, we remind that for this case there is a high probability that the attacker is a former-insider, who has specific knowledge on the substation and enough other information to attack. Likewise, the IEDs have been widely documented and we have to assume that a terrorist disposes of sufficient financial resources to attack. The IEDs of the substation are the assets of the highest vulnerability and the IC network of the substation is the one that has the highest vulnerability of the system under analysis.

In general, the probabilities of an attack are high which complies with the type of threat that represents a former-insider and the political situation. Nevertheless, note that in order to execute an attack that affects the integrity or the integrity and the availability of the assets requires much more effort and because of this fact the respective probabilities are lower. The HMI (Human Man Interface) and the group of IEDs at substation 5 also present a high probability of attack.

Also, bear in mind that the results regarding the probability of an attack can be combined with any other tool to evaluate the effect of an attack. For this reason, we mention the modularity of the Bayesian network.

Power System in normal operating state

We now analyze the consequences for the power system. The results are shown in Table 6-IX. Considering the "survivability" of the communication and information network and the effect on the power grid, we can observe that the probability of serious consequences is higher in the case of the IEDs which carry out protection functions of the most important lines.

Similarly to Chapter 4, probabilities of the consequence obtained by the Bayesian network include the fact that the attack occurred without considering the sophistication of the cyberattack. Without any attack there is no impact on the power system. Remember that these probabilities are marginal and not conditional probabilities. These conditional probabilities of the consequence for the power system, given the occurrence of a cyberattack were taken into account. The average weight method can be used and the equations of the section 4.3.2.1 are applied of the same way for the risk evaluation.

TABLE 6-IX. PROBABILITY OF THE CONSEQUENCE FOR THE TEST POWER SYSTEM – NORMAL STATE

ASSET	CONSEQUENCE FOR THE POWER SYSTEM				
	High	Medium	Low	No Impact	No attack
SerSUB5	0.0037	0.0057	0.0299	0.2259	0.7349
DatabSUB5	0.0000	0.0000	0.0017	0.2702	0.7281
HMISUB5	0.0070	0.0108	0.0418	0.3010	0.6394
IED51	0.0168	0.0523	0.0634	0.1769	0.6906
IED52	0.0000	0.0000	0.0540	0.2554	0.6906
IED53	0.0158	0.0490	0.0607	0.1839	0.6906
IED54	0.0000	0.0000	0.0540	0.2554	0.6906
SerSUB6	0.0023	0.0038	0.0241	0.2038	0.7660
DatbaSUB6	0.0000	0.0000	0.0015	0.2436	0.7549
HMISUB6	0.0034	0.0056	0.0275	0.2232	0.7404
IED61	0.0152	0.0454	0.0646	0.2542	0.6206
IED62	0.0000	0.0000	0.0777	0.3018	0.6206
IED63	0.0047	0.0140	0.0371	0.3237	0.6206
IED64	0.0000	0.0000	0.0777	0.3018	0.6206
SerSUB8	0.0016	0.0027	0.0204	0.1824	0.7929
DatbaSUB8	0.0000	0.0000	0.0011	0.1852	0.8137
HMISUB8	0.0020	0.0033	0.0200	0.1733	0.8014
IED81	0.0000	0.0000	0.0122	0.1866	0.8012
IED82	0.0000	0.0000	0.0474	0.1514	0.8012
IED83	0.0000	0.0000	0.0122	0.1866	0.8012
IED84	0.0000	0.0000	0.0474	0.1514	0.8012

Operators and planners can use the probabilities that the consequence for the power system is high, medium, etc., which are shown in Table 6-IX as a measure of risk, which is a valid approximation as demonstrated in chapter 4. Taking into consideration the social factors which motivate a terrorist to attack the IC network, the resources, the vulnerabilities of the asset, the countermeasures, and the interdependency, the assets with most important value of risk for the system are IEDs 51 (line protections 5-4), IED 7-5 (line protections 7-5) and IED 61 (line protections 6-4).

The servers display lower values of probability for the following reasons: the probability of a cyberattack is low and most notably because we define a level of very high survivability for these assets; so that if the cyberattack takes place, the communications and information system disposes of all the means to guarantee that the function continues being carried out. This corresponds to reality because the control servers in the large substations are duplicated and the security levels are high.

Power System in emergency operating state

In this case, the probability that the consequence for the power system is serious or average is expected to be much higher that when the power system is in the normal state.

The probability of an attack is equal in both case (normal and emergency) given that the only factor that has changed is the operating state of the system. This variable does not influence the decision whether to attack or not. It is possible that an insider or a former insider knows when the power system is nearer to its operating limits. This factor, however, have not been taken into account in the modelling process.

We make the scenario worse by slightly diminishing the level of survivability of the network in case of fault of the servers and the HMI's assets. Regarding the servers, the HMI and the

database we have diminished the survivability from "very high" to "between average and high". This means that we have reduced the probability that the communication and information system guarantees the function of each of these assets for the power system. The results of the consequence of the cyberattack are shown in Table 6-X.

TABLE 6-X. PROBABILITY OF THE CONSEQUENCE FOR THE TEST POWER SYSTEM – EMERGENCY STATE

ASSET	CONSEQUENCE FOR THE POWER SYSTEM				
	High	Medium	Low	No Impact	No attack
SerSUB5	0.0763	0.004	0.0715	0.1133	0.7349
DatabSUB5	0.0000	0.0000	0.0399	0.232	0.7281
HMISUB5	0.1081	0.0057	0.0968	0.1499	0.6394
IED51	0.1332	0.0316	0.0234	0.1212	0.6906
IED52	0.0000	0.0000	0.073	0.2364	0.6906
IED53	0.1306	0.0350	0.0228	0.1210	0.6906
IED54	0.0000	0.0000	0.0726	0.2369	0.6906
SerSUB6	0.0554	0.0034	0.0594	0.1158	0.766
DatbaSUB6	0.0000	0.0000	0.0413	0.2038	0.7549
HMISUB6	0.063	0.0038	0.0658	0.1270	0.7404
IED61	0.1364	0.0453	0.0284	0.1693	0.6206
IED62	0.0000	0.0000	0.0992	0.2802	0.6206
IED63	0.1023	0.0833	0.0272	0.1667	0.6206
IED64	0.0000	0.0000	0.0968	0.2827	0.6206
SerSUB8	0.0409	0.0026	0.0517	0.1119	0.7929
DatbaSUB8	0.0000	0.0000	0.0354	0.1509	0.8137
HMISUB8	0.039	0.0025	0.0496	0.1074	0.8014
IED81	0.035	0.0462	0.0163	0.1014	0.8012
IED82	0.0000	0.0000	0.0568	0.142	0.8012
IED83	0.0347	0.0464	0.0165	0.1013	0.8012
IED84	0.0000	0.0000	0.0568	0.142	0.8012

As being expected in the case of emergency, though the probability of the attack is equal, the probability of a serious impact for the power system is higher than with the system in the "normal" state. As we diminished the survivability, it is observable that servers have an important value of probability with regard to serious consequences.

6.6 Conclusions

We presented a tool which allows us to evaluate the risk to the power systems security as a result of cyberattacks against the information and communication system.

The use of the Bayesian networks enables us to quantify and to model some variables that are difficult to represent in traditional models. This model includes variables of different categories that range from sociological factors to totally technical variables. One of the particular advantages of this model is its capacity to encompass the interdependencies of the systems of IC, of control and of power.

By having created this modular Bayesian network, we can combine it with other assessment tools. In addition this modularity facilitates the evaluation of marginal probabilities of every variable and of conditional probabilities of the causality relationships.

For example, the survivability of the IC system, which we have modelled as an input variable, can be evaluated by a Bayesian sub-network or including other type of assessment systems such as those based on Petri networks. Survivability has not been included to

evaluate the probability of an attack because for this purpose we have only considered the vulnerabilities related to the IC system's security. Therefore, by including more accuracy in this variable we can fine-tune the results of the probability so that the function realized by the asset can be assured when it is attacked.

The most laborious work in this method is the establishment of conditional probabilities, which can and have to reflect specific aspects of the systems, since they model the knowledge of the experts. The interviews with the operators, though scanty, were a point of support in the assessment of these probabilities. We have put values of conditional probabilities that from our point of view and according to the literature (see references) are coherent.

This Bayesian network is an approximation of the interdependencies modelling (also called intra-dependencies) between critical infrastructures of the information and communication system and of the power grid. As future work, subsystems that model the reliability of both the IC system and of the power system can be included.

References

[AND, 1999] Anderson R., Feldman P., Gerwehr S., Houghton B., Mesic R., Pinder, J., Rothenberg J., Chiesa J., "Securing the U.S. Defense Information Infrastructure: A Proposed Approach" (RAND Report MR-993-OSD/NSA/DARPA), RAND Corporation, USA, 1999. Available in http://www.rand.org/pubs/monograph_reports/MR993/

[BJO, 2004] Bjorn T., Fontela M., Mellstrand P., Gustavsson, Andrieu C., Bacha S., N. Hadjsaid, Besanger Y., "Overview of ICT Components and its Application in Electric Power Systems", Proceedings of 2nd International Conference on Critical Infrastructures, October 25-27, 2004, Grenoble, France.

[CIG, 2005] Roche P., "Cyber Security Considerations in Power System Operations", CIGRE Joint Working Group Security for Information Systems and Intranets in Electrical Power Systems", JWG D2/B3/C2.01, 2005.

[CSI, 2007] Computer Security Institution (CSI), Federal Bureau of Investigation (FBI), "The Computer Crime and Security Survey 2007", USA, 2007. Available in http://www.gocsi.com/

[ELL, 1999] Ellison R., Fisher D., Linger R., Lipson H., Longstaff T., Mead N., "Survivability: Protecting Your Critical Systems", CERT Coordination Center Software Engineering Institute Carnegie Mellon University, Pittsburgh, USA, 1999.

[END, 2006] Enders W., Sandler T., The Political Economy of Terrorism, Cambridge University Press, NY, 2006.

[FIN, 2006] Lessons Learned from Cyber security Assessments of Scada and Energy Management Systems. Fink R. Spencer D. Wells R. September 2006

[GAR, 2006] Gardner M., "Questionnaire Consensus", The GRID Workshop on Vulnerabilities of power system controls: challenges and R&D needs, Belgium Leuven, November 14, 2006. Available http://grid.jrc.it/

[GER, 2006] Gheorghe A.V., Masera M., Weijnen M., De Vries L., "Critical Infrastructures at Risk: Securing the European Electric Power System", Ed Springer, Netherlands, 2006.

[GOE, 2002] Goetz E., "Cyber Security of the Electric Power Industry", Institute for Security Technology Studies at Dartmouth College, December, 2002, Hannover, Germany, Pp: 1-19.

[GRE, 2000] Greene T., "Civilization Hanging by a Thread", White papers, December, 2000, Washington, USA. Available in http://www.theregister.co.uk

[HOW, 1998] Howard J.D., Longstaff T. A., "A Common Language for Computer Security Incidents", Sandia National Laboratories, Report SAND98-8667, USA, 1998.

[KLA, 2002] Klare M., "The New Face of Combat: Terrorism and Irregular Warfare in the 21st Century," in Charles W. Kegley, Jr., ed., The New Global Terrorism: Characteristics, Causes, Controls, Upper Saddle River, NJ: Prentice Hall, 2002, pp. 27-35.

[MEA, 2000] Mead N., Ellison R., Linger R., Longstaff T., McHugh J., "Survivable Network Analysis Method", Internal rapport, Carnegie Mellon University and Software Engineering Institute September 2000.

[NAE, 2002] Naedele M., "IT-Security for Safety-Critical Automation Systems", Proceedings of 5th International Symposium on Programmable Electronic Systems in Safety Related Applications, Cologne, Germany, May 7-8, 2002 .

[NER, 2003] North American Electric Reliability Council NERC, "Permanent Cyber Security Standard", SAR Drafting Team, August 21, 2003. New Jersey, USA.

[NEU, 1993] Neumann P, Hollway A., Barnes A., "Survivable computer communication systems: The problem and working group recommendations", Technical report, U.S. Army Research Laboratory, AMSRL-SL-E, White Sands Missile Range, USA, May 1993.

[NRC, 2003] U.S. Nuclear Regulatory Commission NRC, Information Notice 2003-14. , USA, 2003. Available: in http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2003/in200 314.pdf

[PED, 2006] Pederson P., Dudenhoeffer D., Hartley S., Permann M., "Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research", August 2006.

[RAY, 1996] Raymond E.S., "The New Hacker's Dictionary", Ed. MIT Press, Third Edition, Octubre, 1996.

[RIG, 2006] Rigole T., Vanthournout K., Deconinck G., "Interdependencies between an Electric Power Infrastructure with Distributed Control, and the Underlying ICT Infrastructure", Proceedings of Int. Workshop on Complex Network and Infrastructure Protection CNIP-2006. Rome, Italy, 28-29 Mar. 2006, pp. 428-440.

[SCH, 2006] Schneider, K., Chen-Ching L., Paul, J.P., "Assessment of interactions between power and telecommunications infrastructures", IEEE Transactions on Power Systems, Vol. 21, Issue 3, August 2006, Pp: 1123 – 1130.

[SHA, 2006] Shaw W.T. Cybersecurity for Scada Systems, Ed. PennWell Books, 1st edition, USA, June 15, 2006

[STA, 1997] National Security Telecommunications Advisory Committee, "Electric Power Risk Assessment", 1997. Available in http://www.aci.net/Kalliste/electric.htm

[THE, 2005] Thévenet C., "Cyberterrorisme , Mythe ou réalité", Institut Francilien d'Ingénierie et des Services Centre d'Etudes Scientifiques de Défense – CESD, Université de Marne-La-Vallée, 2005, France.

[UNE, 2005] United Nations Educational Scientific and Cultural Organization, "Specificities of cyberspace". Available: http://www.unesco.org/cybersociety/cyberspace_spec.htm

[WEI, 2001] Weisman R., "California Power Grid Hack Underscores Threat to U.S.", June 13, 2001. Available in: http://www.newsfactor.com/perl/story/11220.html

[WEM, 2004] Weimann G., "Cyberterrorism: How Real Is the Threat?", United States Institute of Peace and University of Haifa, December, 2004, Israel. Available in: http://www.usip.org/pubs/specialreports/sr119.html

[WES, 2006] Weiss J., "The Current Status of Control System Cybersecurity", Utility Automation & Engineering T&D, Ed. PennWell Publishing Corp., USA, August, 2006. Available in http://uaelp.dev.pennnet.com/

[WU, 2005] Wu, F.F., Moslehi K., Bose A., "Power System Control Centers: Past, Present, and Future", Proceedings of the IEEE. Vol. 93, Issue 11, November, 2005, Pp.: 1890 – 1908.

CONCLUSIONS

In this thesis we were confronted with a major problematic which affects the security of power systems and in general the so-called critical infrastructures: intentional attacks. The research involved big challenges. The first one was how to take into account the intentional characteristic of attacks that affect electrical infrastructures. The second challenge was how to approach the problem concerning the quantity of possible cases to be studied. The third problem was how to take into consideration the uncertainties associated with every case. Finally we had to find out how to analyze the impact that these attacks had on the security of the power system.

Possible intentional events that could affect the power system were examined. We only addressed the issue of terrorism since it is an actual threat for the critical infrastructures of different countries in the world. Nevertheless, all the proposed methods in this thesis are extendable to other types of intentional attacks.

We presented a method that allows the ranking of possible contingencies that result from physical terrorist attacks against electrical infrastructure. This method is based on a study of the phenomenon of terrorism, the principal variables concerned, the dynamics of the problem, and the mathematical analysis of present uncertainty. Via this technique, which is based on Bayesian networks, we could model the inherent uncertainties of intentional attacks in a coherent and appropriate way. With the results of the probabilistic inference we established "a priori" risk value which qualifies the most important contingencies resulting from the attacks. However, this "a priori" measurement found in the contingency ranking is useful to rank contingencies but not adequate as a security index, because the criticality of the power system's components is established by using the load flow of the base case.

The proposed method of contingency ranking has the advantage that by associating a value of probability to every case we can carry out posterior probabilistic security analyses of the power system. This method is useful in addressing the problem of security assessment since it reduces the number of cases to be studied (which constitutes one of the problems of security analyses) and in addition it models the uncertainties linked to the causes of contingencies.

We presented a second method which enables us to assess the security of a power system more accurately by establishing an index based on risk. This method is based on theories of probability and possibility. One of the advantages of our method is that it takes into account the fact that power injections in models differ from predicted values because we modelled the load as a fuzzy number. This approximation is valid and has been widely used in the problem of fuzzy load flow, which we use for the analyses of steady state. This modelling allows us to obtain fuzzy numbers as well, as a result of the load flow.

In using these results, together with those of the contingency ranking, we find risk indicators that appropriately show the security problems in the nodes and in the lines. Our method is powerful in the sense that the uncertainty is preserved throughout the method and in a single simulation we can include different cases (corresponding to different power

injections). It should be emphasized that this method can be used in combination with any other contingency ranking and not exclusively with the one we use in this thesis.

In this work we evaluated the possible ways of implementing fuzzy numbers and its effect on the results of the fuzzy load flow. The traditional alpha-cuts method and standard arithmetic have been used. We implement the LR numbers and the transformation method. We conclude that though the transformation method improves precision, it requires more calculations, which make it computationally more expensive. Contrary to this, LR numbers do not need numerous calculations but precision is then sacrificed. Because of this, security analyses based on the results of the fuzzy load flow are more or less conservative. The operators and planners could choose the use of the arithmetic which best suits their risk policies.

Finally, we approached the problem of cybersecurity and more specifically the case of cyberterrorism against the information and communication systems, which affects the security of the power system. We extended the Bayesian network which was created for physical attacks, to cyberattacks, from the perspective of electrical engineering. By using the Bayesian network we can evaluate the risk, including the threat, the vulnerabilities, the impact and the modelling of the interdependences. This modelling allows the comprehension of interactions and variables involved in the problem. This proposal is new and a different way to assess the risk resulting from cyber attacks.

The work done on cybersecurity was not easy bearing in mind the different disciplines present in the problem, which include sociology, computers, communications and power engineering. Moreover, the different areas do not have a common language, and the objectives of the risk assessment can be different in all of disciplines. Concepts such as the resilience and survivability of ICS have been addressed to unify the security objectives of the ICS applied to control systems, such as the one of the power system.

Throughout this thesis, in the approach to the problem of terrorism, we analysed the main references and we suggested the review of some concepts as in the case of transitions of operating states of the power system. In addition, in some cases we suggested new definitions, as in the one of cyberterrorism. All this allowed us to obtain satisfactory results in the modelling.

We emphasize that in a problem which is difficult to approach, such as intentional attacks, physical or cybernetic; we managed to put up mathematical models which are solidly supported by the theory of probability, the Bayes theorem and the theory of fuzzy logic. These methods can be used in the analyses of the security risk of power systems.

In our case we used the example of terrorism against the electrical infrastructure of Colombia. We consider that the analyses realized concerning the physical attacks in this thesis can be used by operators of the Colombian system to complement their security analyses.

PERSPECTIVES

In spite of the realized work there is still a lot of space for improvement. As regards physical and cyber attacks and the modelling of the Bayesian network, it is necessary to establish efficient forms in order to extract the information from experts. We conducted interviews and collected the information based on our logic. Nevertheless, the implementation of efficient forms of expert elicitation could improve the performance of the Bayesian networks.

Due to the inscrutability of electrical utilities and governments we faced difficulties in validating our methodology. The information on the physical and cybernetic attacks available to the public is non-existent, or very vague, and does not contain details that are important for the validation of methodology. A lot of information was obtained from national newspapers, which obviously do not contain necessary technical details. It would be interesting to use a real, detailed database to analyze the scope of the proposition.

With regard to the security method it still remains to define global risk index for the system. We think that this task can also be realized by using fuzzy logic.

Though the problem of cybersecurity of power systems is widely recognized, the discussion and joint multidisciplinary collaboration between engineers in computer science, in communications and in electrical networks would allow an advance in the search for mathematical models which approach the problematic more adequately. This could be an effort to find different views and to come to a consensus regarding the objectives and the use of common vocabulary.

One of the limitations in the evaluation of the impact of intentional assaults was the lack of tools to model interdependences between infrastructures. Currently few simulation tools exist to realize this task. Although in our research team two theses are currently developing this area, a lot of work is to be done to explore this field.

A APPENDIX A

The following overview shows the situation in different countries in terms of terrorism.

A.1 Europe

Electrical infrastructure on the European continent has already been the target of terrorist attacks. Eight of the forty-six countries forming the continent have reported cases of terrorism. The most significant figures come from Spain, Russia and France. Interestingly, two of these countries are members of the European Union. In Table A-1 and Figure A-1, the distribution of terrorism in Europe in comparison to the world and the continent respectively is presented.

Country	Percentage
Spain	4,00%
Russia	2,67%
France	1,60%
Albania	1,33%
Turkey	0,80%
Others	0,53%
Chechnya	0,27%
Italy	0,27%
Total	11,47%

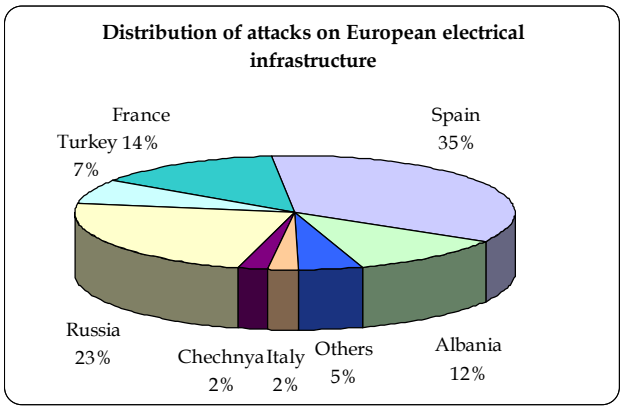


TABLE A-1: DISTRIBUTION OF TERRORIST ATTACKS ON ELECTRICAL INFRASTRUCTURE IN COUNTRIES ON THE EUROPEAN CONTINENT: 1994 TO JUNE 2007

Figure A-1 Distribution of attacks on European electrical infrastructure. Source: Table and figure created by analysis of data from the "National Memorial Institute for the Prevention of Terrorism (MIPT)" database.

A.1.1 Spain

Spain has suffered a series of attacks on its electrical infrastructure (documented from 1998), all of them are a result of the terrorist activity of the ETA Organization. ETA (Euskadi ta Askatasuna or Basque Country and Freedom) is a terrorist organization that aspires to create an independent Basque Marxist state by the unification of different territories pertaining to Spain and France. ETA is classified as a terrorist group by the main international organizations.

Between 1998 and 2003, 9 terrorist acts occurred, which caused damage to substations, transformers and towers of the Basque country. In September 2004 Spain suffered a series of attacks that started with the explosion of four low power bombs located in a high voltage tower of the Red Eléctrica de España located in Irún (Gipuzkoa) which caused damage in the base of this installation, forcing the company to cut off the electrical line of the sector in order to repair it. Ten days later, attacks took place against two energy towers that are owned by Red Eléctrica Española in Behobia (Gipuzkoa) and Bujaruelo (Huesca). Another two days

later ETA exploded a device next to an electrical power station in the Sierra del Moncayo. In January 2006 an explosive caused damage to a small electrical substation between located Aratores and Borau, in the province of Huesca.

Spain has its own strategies to counter ETA activity. However, the government has recognised the necessity of improving strategies against terrorism. The state has favoured pacific measures such as political dialogues that have regretfully failed. Police and military activities have been more effective and the ETA structure has successfully been undermined, mainly due to the cooperation between Spain and France.

A.1.2 France

France also has suffered from some terrorist acts against the electrical infrastructure, most of them caused by the FLNC group (National Liberation Front of Corsica). Unlike other countries, these acts mainly targeted invoicing and customer service offices which have a political purpose. In general these attacks have not been a significant danger to the well-being of people and in fact the local press has labelled them as symbolic and inoffensive. Another minor group is the ARB (Breton Revolutionary Army), who is part of the FLB (Liberation Front of Brittany), to which attacks against relays, an electrical substation and an electrical tower have been attributed in the last ten years.

For a long time France has been demonstrating its determination to counter manifestations by terrorist groups, whoever the people behind them might be. The threat of terrorist led France to progressively establish legislation, coherent operative organism and to reinforce international cooperation. France actively participates in the counter-terrorism committee tasks which are contributed to by the attendance and speeches of other states.

As member countries, France and Spain participate in the counterterrorist efforts of the European Union.

A.1.3 Action and preventive measures of the European Union

After the assaults on September 11, 2001 (New York), March 11, 2004 (Madrid) and July 7, 2005 (London) efforts against terrorism became a priority for all countries belonging to the European Union. These countries are making a united effort to counteract terrorism. Different strategies have been developed since 2004. The main topics are: the prevention, preparation for and response to terrorist attacks, victims of terrorism, the fight against financing of terrorism, police matters, data and information exchange, judicial and criminal matters, borders and security research [COE, 2006].

a) Prevention, preparation for and response to terrorist attacks
On 17th and 18th of June 2004 the European Council requested the Commission to come up with a global reinforcement strategy for the protection of critical infrastructures. On October 22, 2004 the Commission transmitted a communication named "Critical Infrastructures Protection in the Fight against Terrorism", in which measures are suggested for the reinforcement of prevention, preparation and response of the EU to terrorist attacks against critical infrastructures. Electrical infrastructure is treated as one of the critical infrastructures. This communication is important in the sense that it emphasizes the vulnerability of electrical systems and the problems experienced by these systems in the US and Europe [CEC, 2004]. The commission suggests the creation of a network that mainly serves to foment

the exchange of information regarding threats and common vulnerabilities and to develop suitable measures and strategies that limit the risk for critical infrastructures. The European Union is committed to guaranteeing the transmission of information to the respective governmental authorities including emergency services, which will be in turn in charge of informing the owners and operators of critical infrastructures, through a network established in the member states. The stakeholders of critical infrastructures are appealed, to ensure that their assets remain in a suitable condition through the regular improvement of technical and physical security. Inspections and permanent assessment are carried out in order to guarantee continued service supply.

The Commission published the "Green Paper on a European Program for Critical Infrastructure Protection (EPCIP)" in response to the Council's request in November 2005. The Paper was the synopsis of various discussions with the EU countries and the plan for the future of the EPCIP. Standardized definitions of the role of critical infrastructures' stakeholders as well as possible threat scenarios that the EPCIP should address were established. This communication specifies financial measures for the Council's programme called "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013 as part of the Framework Programme (FP) on Security and Safeguarding Liberties [CEC, 2005b]. On February 12, 2007, the Council of the European Union adopted the specific programme with a budget of € 137.4 million for projects presented by national, regional and local authorities. The principal objective is to support member countries' efforts to prevent, prepare for, and to protect people and critical infrastructure against terrorist attacks and other security related incidents.

b) Security research

The European Commission has launched new research initiatives to improve the security of EU citizens. In February 2004, before the attacks on London, the European Commission accorded a budget of € 65 million for a "Preparatory Action for Security Research" (PASR) between 2004 and 2006 preparing the way for a full European Security Research Programme (ESRP) starting in 2007. The purpose was to guarantee that all requirements of European security strategy and security and defence policy were taken into account in the development of the Security Research Programme. Most of the PASR projects were developed to support activities designed to tackle terrorism, improve the security of EU citizens and strengthen the European industrial base. The project VITA "Vital Infrastructure Threats and Assurance" proposed in 2004 was one of the first projects of PASR 2004. The aim was to devise exceptional emergency situations such as terrorist attacks or natural catastrophes, and to simulate them in order to assess the security of critical infrastructures. The project included the interdependences of the electrical infrastructure and terrorist attacks on power systems.

In April 2005, continuing the preparation of the European Security Research Programme (ESRP), the European Commission created the "European Security Research Advisory Board" (ESRAB). The Board was formed to prepare to the new financial period of 2007-2013 and to decide on the content and the implementation of European Security Research within the 7th Research and Technological Development Framework Programme (RTD FP). The Board was comprised of high level strategists, with a responsibility relating to security research and the participation of diverse groups including public and private users, industry, the European Defence Agency, and research institutes. The main research topics were: restoring security in case of crisis, protection against terrorism, and critical infrastructure

protection. The budget for related research activities is about € 408 millions per year [CEC, 2005a].

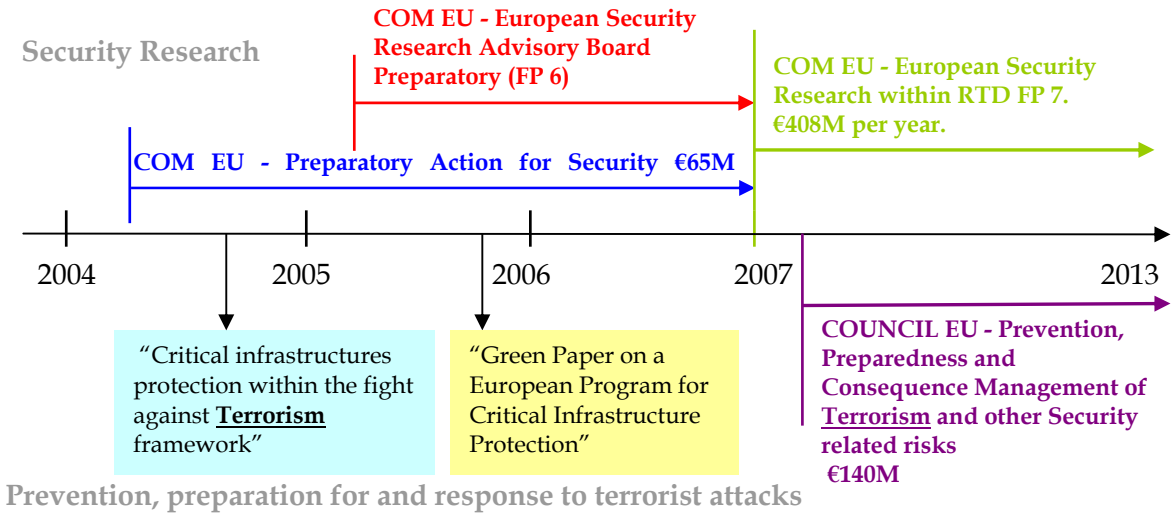


Figure A-2: Actions of "Security research" and "Prevention, preparedness and response to terrorist attacks" developed by European Union in the fight against terrorism.

A.2 United States of America

Since the attack on the Twin Towers on September 11, 2001 there is concern in the US to prevent this type of event from happening again. The assault inflicted losses of a number not caused before by one single terrorist attack. The US National Security Agency, together with numerous departments of the federal government has begun to put into practice protection measures under a national plan with the purpose of protecting the nation: the "Liberty Shield Operation". The Liberty Shield Operation theoretically improves the security of critical infrastructure, and assures that all the federal response actions can be quickly employed. Recent communications have shown that the level of threat has risen. Furthermore, the US keeps working on their information networks and motivates electrical networks owners and operators to improve their security levels.

Nevertheless, cases of cyberattacks have taken place. In March 2005, security consultants of the electrical industry disclosed that hackers targeted the US electrical power network and gained access to electronic control systems of some American companies in the electrical sector. The computer security specialists disclosed that in some cases, these intrusions "caused an impact". Despite these revelations civil employees of the companies indicated that hackers had not caused serious damage to the control systems used in the supply of electrical energy to the country. It is clear that the constant threat of intrusion has increased the concerns of electrical companies since they demonstrate that their defences would not be sufficient against a potential catastrophic blow [DHO, 2005].

In the US, 107 professors and graduate students from 26 different universities have established six groups to develop, advance knowledge, and create novel concepts in modelling, simulation, measurement, estimation, visualization, control operation, and management systems. Their purpose is to meet security challenges faced by interconnected power systems because of the threat of terrorism [IEE, 2002].

The US holds a quarter of the electrical energy generation capacity in the world, producing 950 MW, assets of infrastructure of worth 1 trillion dollars and 320,000 kilometres of lines in a highly integrated network. There are also 3,500 public services companies that depend on a network which serves 283 million people.

Outages of the system like the one that happened in August 2003 in the USA and Canada, have demonstrated the vulnerability of the American system. On this occasion, the blackout affected 50 million people with losses of 61.800 MW and economics losses of between 4 and 10 billion dollars. The disturbance lasted 16 hours and service in some zones could only be re-established four days later [TFO, 2004].

Given the complexity and vulnerability of the system, market features and socioeconomic and religious situation of the country, the USA is still concerned about terrorist attacks on electrical infrastructure and continues putting effort into preventative measures.

A.3 Latin America

Terrorism in Latin America has generally been a form of combat by leftwing guerrilla groups, rightwing opposition groups of paramilitaries and ordinary criminal organisations. In the tri-border region of Argentina, Brazil and Paraguay evidence of terrorism by extremist Islamic groups can be found as well.

Latin American guerrillas groups were initially a form of organised protest by farmers and native communities against a political, social and economic situation that was shaped by the abuse of power by political oligarchies. Historically, dictatorships dominated these political systems and suppressed public liberties. The majority of the guerrillas of Central and South America favoured democracy and demobilized themselves in compliance with agreements concluded with the respective governments.

Setting aside the Colombian case, the terrorist threat against electrical infrastructure has been low in South America in the last ten years in comparison to other regions of the world (see Table A-2).

TABLE A-2: DISTRIBUTION OF TERRORIST ATTACKS TO THE ELECTRICAL INFRASTRUCTURE OF COUNTRIES IN SOUTH AMERICA : 1994 TO JUNE 2007

Country	Percentage
Colombia	42,40%
Brazil	0,53%
Peru	0,53%
Chile	0,27%
Others	1,07%
Total	44,00%

Source: Table created by analysis of data from the "National Memorial Institute for the Prevention of Terrorism (MIPT)" database.

In 2001 members of the Communist Party of Peru, well known as the Sendero Luminoso group, destroyed two electrical energy towers near the town of Ayacucho. Later another attack was registered near to Lima and was also attributed to the guerrilla group. The

government recognized a new subversive outbreak in Peru, which caused a service shutdown in the Southeast Andean region.

During the 1980s and 1990s electrical energy towers were one of the preferred targets of Sendero Luminoso in Peru. Between 1980 and 1987, 3 blackouts took place, which left the capital Lima without service for several hours. Other regions and cities, such as Puno, Lampa, San Roman, Azángaro, Huancayo and Angaraes also experienced electrical power shutdowns. In 1987 the bombing of 30 high voltage towers of the Mantaro interconnected system caused significant blackout in different regions [CVR, 2003].

In El Salvador the Frente Farabundo Martí for the National Liberation (a revolutionary guerrilla that founded in 1980 and that is presently one of the most important political parties in the country) managed to interrupt up to ninety percent of the electrical production in El Salvador, and the organization produced a terrorists manual for such intention [ZER, 2005].

At the moment, the political will to fight terrorism is firm in Latin America although many countries still lack experience and operational capacity. However, the Latin American countries keep actively working on reinforcing the border and financial controls in order to prevent or to obstruct as much as possible degree activities related to terrorism in their respective territories [STA, 2003].

A.3.1 The Colombian Case

Since the 1990s attacks on the power infrastructure are a recurrent problem for the owners of electrical infrastructure, the users and for the mines and energy ministry of Colombia. From 1999 to 2006 2,362 towers of the almost 30,000 that support the energy transmission lines have been attacked. In these years a steady increase of attacks against the electrical infrastructure inflicted economic losses on energy companies, which count on the negotiated energy supply to the end user (who depends on the energy for survival).

Colombia experiences armed conflict between the guerrilla, paramilitary units, and armed forces of the national government. The guerrillas groups were created as a self-defence mechanism of the peasantry, their aim being to obtain better conditions of life. Over the years their occupation of the Eastern part of Colombia led them to create alliances with narcotics traffickers. At the moment guerrillas occupy different parts of the country. Their powerful infrastructure sometimes even allows them to be equipped with more war material and economic resources than the national army. The most important guerrillas group are the FARC and the ELN [GAR, 2003].

To confront the guerrilla groups, paramilitary forces were founded by narcotics traffickers and industrials who did not want to collaborate with the guerrilla groups or to pay ransoms. To a large extent the paramilitaries were formed by retired militaries and indoctrinated civilians. The paramilitary groups, which operated initially with the at least tacit support of the government, reduced the areas under control of the leftwing guerrillas. More recently the government has distanced itself from the paramilitaries given the increasing number of casualties that they have inflicted. Both the FARC and the ELN are permanently involved in confrontations with the paramilitaries.

Figure A-3 and Figure A-4 show the number of energy towers destroyed and downed from 1999 to May 2007. The year 2002 was a critical period, which coincided with the rupture of peace negotiations between the guerrilla and the government of President Andrés Pastrana and the change of government with the arrival of President Alvaro Uribe. After a reduction in the frequency of the attacks in 2004 the guerrilla groups increased their sabotage of the power system in 2005 and 2006. November and December 2005 were critical months as it was just after a sentence had been given by the Colombian Constitutional Court concerning the president's re-election. The attacks deprived whole sectors of the population of electrical energy, especially the poorest regions (departaments) of the Valle del Cauca, Antioquia, Putumayo, Nariño, and the Cauca.

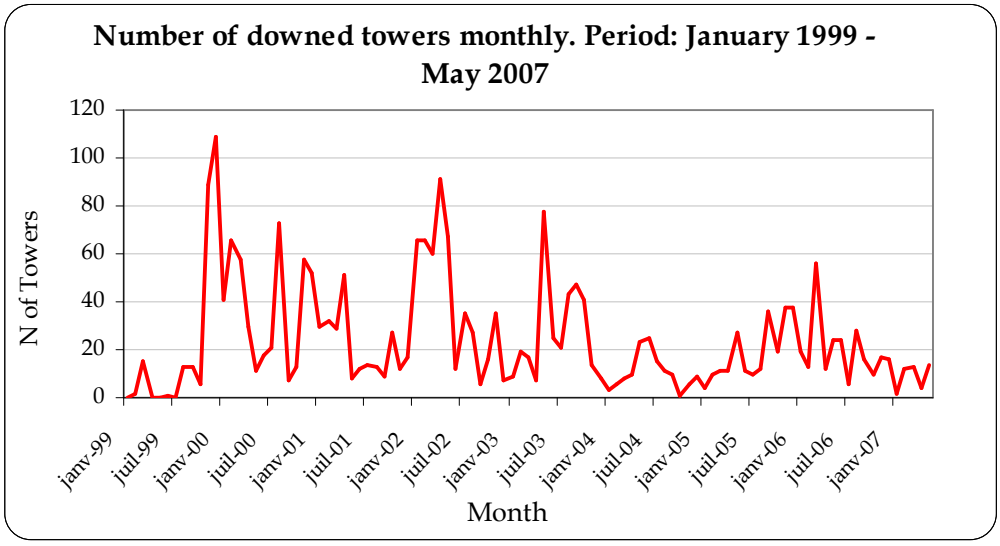


Figure A-3: Number of downed towers monthly. Period: January 1999 - May 2007. Source: ISA.

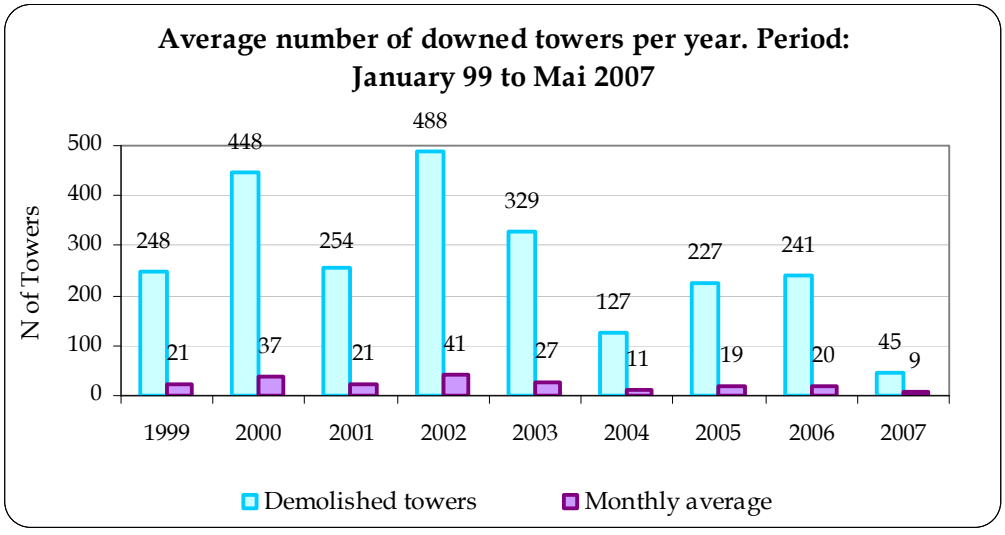


Figure A-4: Average number of downed towers per year. Period: January 99 to Mai 2007. Source: ISA.

Substations and Generating Stations

The attacks on substations and power generating stations were less frequent in comparison with those on towers. In the year 2000 the highest number of attacks was ten attacks against substations of the "Sistema de Transmisión Nacional" (STN) and two attacks against generation plants. In the year 2001 three attacks against substations of the STN and an attack against generating plants were committed and in 2003 three attacks against generating plants and two against substations took place. For security reasons statistics for the following years are not at hand.

For this type of asset the security mechanisms put in place by the government and the companies make it more difficult for potential attacks took place. This may explain why the number of attacks per year has not increased considerably in the case of the generating plants, and against substations of the STN.

A.3.2 The Middle East/ Asia

In Table A-3 and Figure A-5, the distribution of terrorist assaults in Asia in relation to worldwide attacks and relation to all the attacks on this continent respectively is presented.

Country	Percentage
Iraq	17,33%
Pakistan	12,80%
Others	4,27%
India	3,47%
Sri Lanka	1,87%
Afghanistan	1,60%
Nepal	1,33%
Thailand	1,33%
Total	42,93%

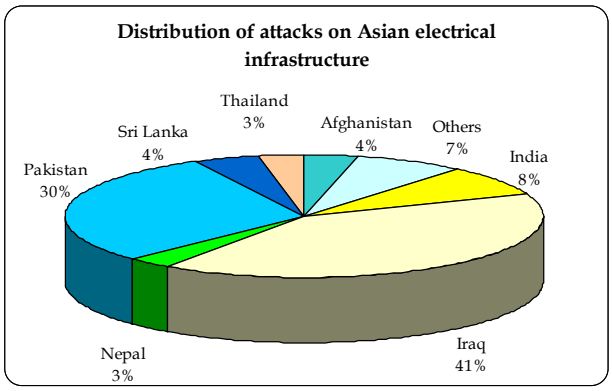


TABLE A-3: DISTRIBUTION OF TERRORIST ATTACKS ON ELECTRICAL INFRASTRUCTURE IN ASIAN COUNTRIES AS A PERCENTAGE OF WORLDWIDE ATTACKS FROM 1994 TO JUNE 2007

Figure A-5: Distribution of attacks on electrical infrastructure in Asian countries as a percentage of the Asian continent as a whole. Source: Table and figure created by analysis of data from the "National Memorial Institute for the Prevention of Terrorism (MIPT)" database.

The Middle East is strongly affected by terrorist acts. The root causes of these acts are complex and cause controversial debate among intellectuals.
To be considered are political factors such as the conflict between the West and East during the cold war era, the Israeli occupation of Arab lands, savage Middle Eastern security intelligence forces, policing methods of dictatorial regimes in the Middle East, the collaboration of the US with many dictatorial regimes in the region, and the supportive role of the US regarding Israel at the expense of Arab countries. In terms of socio-economic aspects it may be mentioned that many Middle-Eastern youths and well-educated citizens do not lead satisfactory lives. Linked to extremism and terrorism are difficult economic conditions, a high rate of illiteracy, the collapse of the family system, and religious fanaticism.

The terrorist acts have principally affected pipelines and oil fields in the Middle East. The electrical infrastructure in Iraq has been targeted in particular.

A.3.2.1 The case of Iraq

Before the Gulf war Iraq had one of the most reliable and efficient power systems in the Middle East. The total generating capacity was 9,295 MW with a peak demand of about 5,100 MW. Approximately 87% of the Iraqi population had access to electricity.

In the 1991 Gulf war the electricity system experienced severe damage. Several transmission lines were disrupted and substations were affected. However, the power generation equipment was the most seriously damaged. The capacity available was reduced to 2,325 MW and power shortages of up to fifteen hours or more were frequent. In some areas there was no supply at all. After the 1991 Gulf war, the annual per capita consumption of electricity dropped from about 1,700 kWh to about 900 kWh, mainly because of supply shortages [UNA, 2003].

Some of the damage of the 1991 war was repaired and about 4,500 MW of generating capacity was available in 2002. However, power supply remained unreliable throughout the 1990s and load shedding and unplanned power outages were frequent. From 1991 to the start of the Oil-for-Food Program, Iraqi engineers were able to repair some of the damaged units, either with available spare parts or by taking parts from other damaged units. Yet the state of the generation units remained unreliable due to the make shift nature of the repairs and general lack of major maintenance and spare parts [UNA, 1996].

After the most recent war, the situation deteriorated again. In 2003 capacity has been reduced to approximately 3,300 MW as a result of a combination of further breakdowns, lack of spare parts and interrupted maintenance cycles. Power outages have become more frequent [UNA, 2003].

The Iraqi government and people are faced with an immense challenge in establishing and maintaining a power network the can reliably provides the electricity necessary to sustain basic services and economic development.

Another critical aspect is the ability of the government to keep critical infrastructure operational. Power outages served to undermine the Coalition Provisional Authority's (CPA) popularity in Iraq and may also de-legitimize any following government. Power shortage creates a lot of public anger and dissatisfaction. A poll by the International Republican Institute, a US-funded non-profit organization that promotes democracy asked what the government's priorities should be. Iraqis put "inadequate electricity" first, ahead of "crime", which was fourth, "the presence of coalition forces", which ranked seventh, and "terrorists", which ranked eighth. Nevertheless, consumer demand for electricity will rise with supermarkets offering more refrigerators and air conditioners for Iraqi homes [MUR, 2005].

Terrorism is a serious challenge for Iraq's government. Since 2003, terrorists have destroyed key electricity infrastructure, threatened workers, compromised the transport of materials, and hindered project completion and repairs by preventing access to work sites [GAO, 2007]. More than 100 attacks against power lines and over 1,200 high voltage towers took place in 2004. Additionally, attacks on fuel supplies used by power plants shut down production [ROB, 2005]. In 2005 attacks on power lines permanently disrupted 2,800 MW of the

countries potential 7,100 MW (nearly 40%). Contractors and workers were attacked. In December 2005, 32 assaults against contractors were recorded including six deaths, five wounded casualties, and two kidnappings. Terrorism adds to the excessive cost of the reconstruction effort and, causes ongoing delays [SCI, 2005].

The increase in attacks on power systems urged the Iraqi government in September 2003 to establish the Task Force Shield to protect its oil and electrical infrastructure. The main objective was to allocate 6,000-person security force, the Electricity Power Security Services (EPSS) to infrastructure protection. An American security firm was contracted to train and equip the guards. The EPSS program barely got underway and only trained a limited number of guards [SIG, 2006]. In an interview in November 2006 the Iraqi Minister of Electricity said that it was virtually impossible to protect every tower in the most volatile corridors that were subject to continuous attack, let alone the 17,000 km of line and 66,000 towers across the country. He explained that terrorists were overwhelmingly difficult to counteract with the EPSS and they extended their terror further by threatening the families of the security guards" [SCI, 2005]. The EPSS program was cancelled in 2005, earlier than originally planned. Today, the Oil Ministry protects electricity infrastructure. The inspector general claimed however that "security forces are undermanned, poorly equipped and uncoordinated and acts of sabotage go un-investigated" [HAR, 2006].

Other initiatives to protect energy infrastructure have been put forward. The Iraqi Ministry of Electricity contracted tribal chiefs to protect the transmission lines running through their areas, paying them about $60 to $100 per protected kilometre [GAO, 2007]. In October 2006, Iraq Reconstruction Management Office (IRMO) officials reported that this scheme was inaccurate and did not improve infrastructure protection. Corruption related to the protection of key infrastructure was reported. Some tribes that were paid to protect transmission lines also sold materials from disrupted lines and charged for access to repair the lines [GAO, 2007].

As indicated above there is more at stake than the system security in Iraq itself: If the guerrilla strategy proves to be efficient this may well result in a destabilization of the Iraqi government. The insurgent forces may hone their skills and share them with other terrorist groups inside and outside of Iraq. Eventually, these strategies may be used in other countries, e.g. Saudi Arabia or even in Western countries.

References

[CEC, 2004] Commission of the European Communities, "Critical Infrastructure Protection in the fight against terrorism". Communication from the commission to the council and the European parliament. Brussels, 20.10.2004. COM(2004) 702 final. Available in http://ec.europa.eu/dgs/justice_home/index_en.htm

[CEC, 2005a] Commission of the European Communities, "Commission Decision of 22 April 2005 establishing the European Security Research Advisory Board", Official Journal of the European Union, 22 April 2005, Brussels.

[CEC, 2005b] Commission of the European Communities, "Green Paper on a European Programme for Critical Infrastructure Protection", Brussels, 17.11.2005 COM(2005) 576 final.

[COE, 2006] Council of Europe – Committee of Experts on Terrorism, "Developments in other for: European Union Commission Activities in the Fight against Terrorism", 11th meeting, Strasbourg, 4-6 December 2006.

[CVR, 2003] Comision de la Verdad y Reconciliación, "Informe Final". CVR, Lima Peru, Agosto 2003. Available in http://www.cverdad.org.pe/

[GAO, 2007] United States Government Accountability Office, "Rebuilding Iraq: Integrated Strategic Plan Needed to Help Restore Iraq's Oil and Electricity Sectors".

[GAR, 2003] García J., Verdú S. "El conflicto armado de Colombia: ¿Un callejón con salida?" La musa Digital. Universidad de Castilla La Mancha. 2003. ISSN 1579 2803.

[HAR, 2006] Harriman E., "The Least Accountable Regime in the Middle East". London Review Bookshop Vol. 28 No. 21, 2 November 2006, United Kingdom.

[DHO, 2005] Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities, "Critical Infrastructure Protection", May 2005, USA. Available in http://www.gao.gov/new.items/d05434.pdf

[IEE, 2002] IEEE Spectrum, "Taking on Terrorism", Sept. 2002, p.35-36. ISSN: 0018-9235

[ROB, 2005] Robb John, "New Post to Global Guerrillas: Iraq's Electricity Disruption", 29 Juin 2005. Available in http://globalguerrillas.typepad.com/globalguerrillas/

[SCI, 2005] Schimmoller B., "Rebuilding Iraq", Power Engineering Magazine, PennWell energy, USA, November 2005

[SIG, 2006] Office of the Special Inspector General for Iraq Reconstruction- Review of Task Force Shield Programs, April 28 2006. pp 16-21.

[STA, 2003] Departamento de Estado de Estados Unidos, "Tendencias del Terrorismo Mundial en 2003". Washington, USA, 29 April 2004. Available in http://usinfo.state.gov/esp/

[TFO, 2004] USA - Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations", April 2004. Available in https://reports.energy.gov/

[UNA, 1996] United Nations, "The United-Nations and the Iraq-Kuwait Conflict 1990-1996", UN Blue Book Series, vol. IX E.96.I.3, New York, UN Publications, ISBN 9211005965.

[UNA, 2003] United Nations, World Bank, "Iraq Needs Assessment", October 2003, pp. 28.

[ZER, 2005] Zerriffi H., Dowlatabadi H., Farrell A., "Incorporating stress in electric power systems reliability models". Energy Policy. Elsevier. November 2005.

B APPENDIX B

In this Appendix, we illustrate and describe the test power system used in this thesis.

B.1 Test System: 5 bus

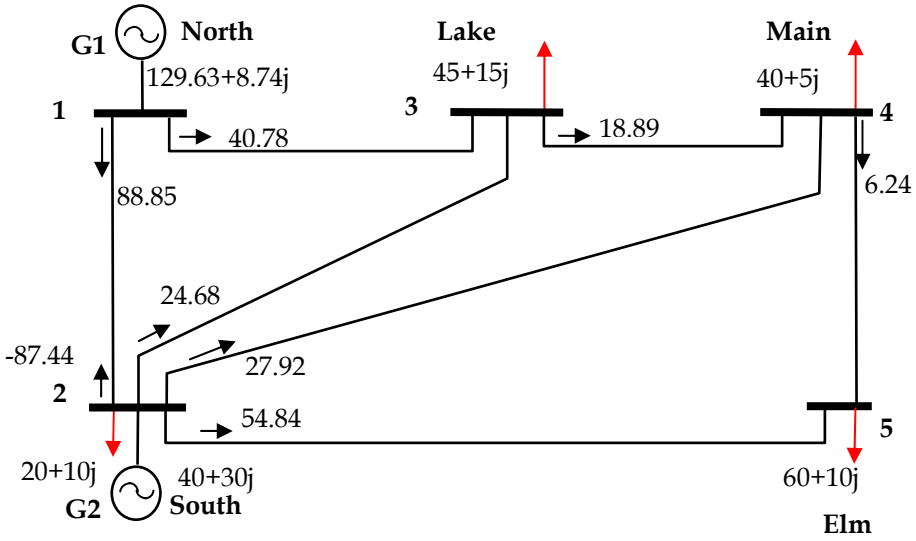


Figure C-1. Five-bus test power system.

B.1.1 Data of the power system

Bus p-q	Impedance	Admittance	Ypq/2
1-2	5.000-j15.000	0.020+j0.060	j0.030
1-3	1.250-j3.750	0.080+j0.240	j0.025
2-3	1.667-j5.000	0.060+j0.180	j0.020
2-4	1.667-j5.000	0.06+j0.18	j0.020
2-5	2.500-j7.500	0.040+j0.120	J0.015
3-4	10.000-j30.000	0.010+j0.030	j0.010
4-5	1.250-j3.750	0.080+j0.240	j0.025

Bus	Type	Pgen (MW)	Qgen (MVA)	Pload	Qload	Voltage (p.u)
1	Slack	0	0	0	0	1.06+j 0
2	Load	40	30	20	10	1+j 0
3	Load	0	0	45	15	1+j0
4	Load	0	0	40	5	1+j0
5	Load	0	0	60	10	1+j0

The matrix Ybus:

$$Y_{BUS} = \begin{bmatrix} 6.25000 - 18.69500 & -5.00000 + j15.0000 & -1.25000 + j3.75000 & 0 & 0 \\ -5.00000 + j15.000 & 10.833334 - j32.41500 & -1.66667 + j5.00000 & -1.66667 + j5.00000 & -2.50000 + j7.50000 \\ -1.25000 + j3.7500 & -1.66667 + j5.00000 & 12.91667 - j38.69500 & -10.0000 + j30.0000 & 0 \\ 0 & -1.66667 + j5.00000 & -10.0000 + j30.0000 & 12.91667 - j38.69500 & -1.25000 + j3.75000 \\ 0 & -2.50000 + j7.5000 & 0 & -1.25000 + j3.7500 & 3.75000 - j11.21000 \end{bmatrix}$$

B.1.2 Load Flow

Last Jacobian before the convergence:

$$\text{Jacobian} = \begin{bmatrix} 35.1237 & -5.3773 & -5.3804 & -8.0651 & 11.9855 & -1.5663 & -1.5339 & -2.1713 \\ -5.2416 & 40.3270 & -31.1666 & 0 & -1.9733 & 12.9579 & -10.1914 & 0 \\ -5.2247 & -31.0481 & 40.1572 & -3.8844 & -2.0011 & -10.5468 & 12.9794 & -1.2315 \\ -7.7548 & 0 & -3.8464 & 11.6013 & -3.1020 & 0 & -1.3455 & 3.2474 \\ -11.5855 & 1.5663 & 1.5339 & 2.1713 & 35.5237 & -5.3773 & -5.3804 & -8.0651 \\ 1.9733 & -13.8579 & 10.1914 & 0 & -5.2416 & 40.0270 & -31.1666 & 0 \\ 2.0011 & 10.5468 & -13.7794 & 1.2315 & -5.2247 & -31.0481 & 40.0572 & -3.8844 \\ 3.1020 & 0 & 1.3455 & -4.4474 & -7.7548 & 0 & -3.8464 & 11.4013 \end{bmatrix}$$

Bus voltages and powers:

Bus	Voltage (p.u.)	Angle (grades)	Active power (MW)	Reactive power (MVA)
1	1.0600	0.0000	8.7406	129.6289
2	1.0430	-2.7380	20.0000	20.0000
3	1.0188	-4.9329	-15.0000	-45.0000
4	1.0178	-5.2602	-5.0000	-40.0000
5	1.0129	-6.1047	-10.0000	-60.0000

Line power flows:

Line	Active power (MW)	Reactive power (MVA)
1-2	88,8506	0,8840
1-3	40,7784	3,4448
2-3	24,6829	1,7321
2-4	27,9207	4,0414
2-5	54,8407	3,7275
3-4	18,8921	7,7793
4-5	6,3287	-2,6184
2-1	-87,4443	-5,1452
3-1	-39,5666	-3,6033
3-2	-24,3256	-4,5557
4-2	-27,4715	2,6704
5-2	-18,8571	-2,5967
4-3	-53,7023	-5,9960
5-4	-6,2977	0,0999

B.2 Test System: Nine-bus

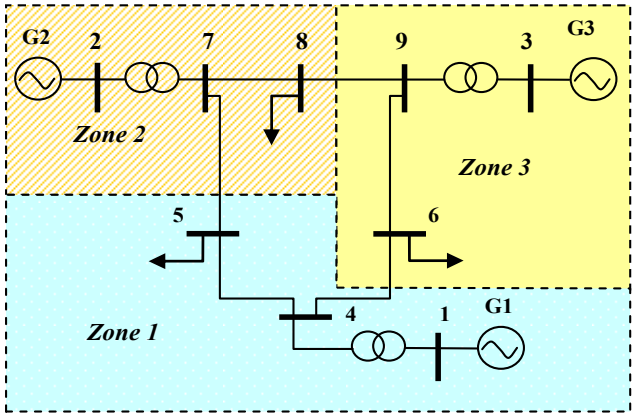


Figure C-2. Western System Coordinating Council WSCC nine-bus test system.

B.2.1 Data of the power system

From Bus	To Bus	Impedance	Admitance	Ypq/2
4	1	0,0000	0,0576	0,0000
7	2	0,0000	0,0625	0,0000
9	3	0,0000	0,0586	0,0000
7	8	0,0085	0,0720	0,1490
9	8	0,0119	0,1008	0,2090
7	5	0,0320	0,1610	0,3060
9	6	0,0390	0,1700	0,3580
5	4	0,0100	0,0850	0,1760
6	4	0,0170	0,0920	0,1580

B.2.2 Load Flow

Bus	Voltaje (p.u.)	Angle (grades)	P gen	Q gen	P load	Q load
1	1,0400	0,0000	0,7164	0,2705	0,0000	0,0000
2	1,0250	0,1620	1,6300	0,0665	0,0000	0,0000
3	1,0250	0,0814	0,8500	-0,1086	0,0000	0,0000
4	1,0258	-0,0387	0,0000	0,0000	0,0000	0,0000
5	0,9953	-0,0696	0,0000	0,0000	1,2500	0,5000
6	1,0127	-0,0644	0,0000	0,0000	0,9000	0,3000
7	1,0258	0,0649	0,0000	0,0000	0,0000	0,0000
8	1,0159	0,0127	0,0000	0,0000	1,0000	0,3500
9	1,0324	0,0343	0,0000	0,0000	0,0000	0,0000

From Bus	To Bus	Line	P Flow	Q Flow	P Loss	Q Loss
4	1	1	-0,7164	-0,2392	0,0000	0,0312
7	2	2	-1,6300	0,0918	0,0000	0,1583
9	3	3	-0,8500	0,1496	0,0000	0,0410
7	8	4	0,7638	-0,0080	0,0048	-0,1150
9	8	5	0,2418	0,0312	0,0009	-0,2118
7	5	6	0,8662	-0,0838	0,0230	-0,1969
9	6	7	0,6082	-0,1808	0,0135	-0,3153
5	4	8	-0,4068	-0,3869	0,0026	-0,1579
6	4	9	-0,3054	-0,1654	0,0017	-0,1551

C APPENDIX C

In order to simulate the Bayesian network, we used the freeware Bayes Net Toolbox for Matlab. The code developed for the Bayesian network created in Chapter 4 is shown as follows.

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%BAYESIAN NETWORK
%CONTINGENCY RANKING RESULTING FROM TERRORISM
%COLOMBIAN CASE
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

clear all
clc
%Specification the graph structure
%We create the adjacency matrix
N = 10;
dag = zeros(N,N);

%We have numbered the nodes as follows
CriSys = 1;
PolSit = 2;
PosTer = 3;
PhyPro = 4;
GeoLoc = 5;
VulTar = 6;
MotAtt = 7;
TypSCo = 8;
IntAtt = 9;
ConAtt = 10;

%Definition of the arrows
dag(PosTer,MotAtt) = 1;
dag(PolSit,MotAtt) = 1;
dag(CriSys,MotAtt) = 1;
dag(GeoLoc,VulTar) = 1;
dag(PhyPro,VulTar) = 1;
dag(TypSCo,IntAtt) = 1;
dag(MotAtt,IntAtt) = 1;
dag(VulTar,IntAtt) = 1;
dag(TypSCo,ConAtt) = 1;
dag(IntAtt,ConAtt) = 1;

%Specification of the size and type of each node
discrete_nodes = 1:N;
node_sizes = [3*ones(1,N-2) 4 5];

%If evidence, the nodes that will be observed
%onodes = [MotAtt VulTar IntAtt ConAtt];
```

```
%We create the Bayesian Network
%bnet = mk_bnet(dag, node_sizes, 'names', {'PolSit','PosTer','CriSys','GeoLoc', 'PhyPro', 'TypSCo', 'MotAtt', 'VulTar', 'IntAtt', 'ConAtt'}, 'discrete', discrete_nodes, 'observed', onodes);
bnet = mk_bnet(dag, node_sizes, 'names', {'CriSys','PolSit','PosTer','PhyPro','GeoLoc', 'VulTar', 'MotAtt','TypSCo','IntAtt', 'ConAtt'}, 'discrete', discrete_nodes);

%Parameters
%Load excel datafile of marginal probabilities
[Probpri, supcom] = XLSREAD('Probdata2.xls');
PrprCriSys=Probpri(:,2:4);
PrprPolSit=Probpri(:,5:7);
PrprPosTer=Probpri(:,8:10);
PrprGeoLoc=Probpri(:,11:13);
PrprPhyPro=Probpri(:,14:16);
PrprTypSCo=Probpri(:,17:19);

%Load excel datafile of conditional probabilities
[ConPr, label] = XLSREAD('CondProb.xls');
pMotAtt = [ConPr(1,:) ConPr(2,:) ConPr(3,:)];
pVulTar = [ConPr(4,1:9) ConPr(5,1:9) ConPr(6,1:9)];
pIntAtt = [ConPr(7,:) ConPr(8,:) ConPr(9,:) ConPr(10,:)];
pConAtt = [ConPr(11,1:12) ConPr(12,1:12) ConPr(13,1:12) ConPr(14,1:12) ConPr(15,1:12)];

[n,q]=size(Probpri);

for j=1:n
   pCriSys = PrprCriSys(j,:);
   pPolSit = PrprPolSit(j,:);
   pPosTer = PrprPosTer(j,:);
   pGeoLoc = PrprGeoLoc(j,:);
   pPhyPro = PrprPhyPro(j,:);
   pTypSCo = PrprTypSCo(j,:);

%Incorporating conditional probabilities
   bnet.CPD{CriSys} = tabular_CPD(bnet, CriSys, 'CPT', pCriSys);
   bnet.CPD{PolSit} = tabular_CPD(bnet, PolSit, 'CPT', pPolSit);
   bnet.CPD{PosTer} = tabular_CPD(bnet, PosTer, 'CPT', pPosTer);
   bnet.CPD{PhyPro} = tabular_CPD(bnet, PhyPro, 'CPT', pPhyPro);
   bnet.CPD{GeoLoc} = tabular_CPD(bnet, GeoLoc, 'CPT', pGeoLoc);
   bnet.CPD{VulTar} = tabular_CPD(bnet, VulTar, 'CPT', pVulTar);
   bnet.CPD{MotAtt} = tabular_CPD(bnet, MotAtt, 'CPT', pMotAtt);
   bnet.CPD{TypSCo} = tabular_CPD(bnet, TypSCo, 'CPT', pTypSCo);
   bnet.CPD{IntAtt} = tabular_CPD(bnet, IntAtt, 'CPT', pIntAtt);
   bnet.CPD{ConAtt} = tabular_CPD(bnet, ConAtt, 'CPT', pConAtt);
%inference
   engines = {};
   engines{end+1} = jtree_inf_engine(bnet);
   nengines = length(engines);

   % no evidence
   evidence = cell(1,N);

   ll = zeros(1, nengines);
   for e=1:nengines
```

```
    [engines{e}, ll(e)] = enter_evidence(engines{e}, evidence);
  end

  %Calculing marginal probabilities
  p=zeros(max(node_sizes),N);
  addev = 1;
  for e=1:nengines
    for i=1:N
      m = marginal_nodes(engines{e}, i, addev);
      p(1:node_sizes(i),i)=m.T;
    end
  end
  %if j==1
    %probabilities(j:10,1:max(node_sizes))=p';
    %else
    %probabilities(10*(j-1)+1:10*j,1:max(node_sizes))=p';
    %end
  probabilities(1:N,1:max(node_sizes),j)=p';

  figure('Name',supcom{j+1,1})
  subplot(2,2,1), barh(probabilities(7,1:3,j),'grouped',0.5,'g'),
  grid on
  set(gca,'yticklabel',{'High','Medium','Low'});
  title('MOTIVATION OF THE ATTACK')
  subplot(2,2,2), barh(probabilities(6,1:3,j),'grouped',0.5,'g'),
  grid on
  set(gca,'yticklabel',{'High','Medium','Low'});
  title('VULNERABILITY OF THE TARGET')
  subplot(2,2,3), barh(probabilities(9,1:4,j),'grouped',0.6,'g'),
  grid on
  set(gca,'yticklabel',{'High','Average','Low', 'No attack'});
  title('INTENSITY OF THE ATTACK')
  subplot(2,2,4), barh(probabilities(10,1:5,j),'grouped',0.6,'g'),
  grid on
  set(gca,'yticklabel',{'Catastr.','High','Medium', 'Low', 'No attack'});
  title('CONSEQUENCE OF THE ATTACK')
end

[n,q]=size(Probpri);
for i=1:n
  pratt(i,1:3)=probabilities(9,1:3,i);
  pratt(i,4)=1-probabilities(9,4,i);
  sevatt(i,1:5)=probabilities(10,1:5,i);
end
pratt
sevatt
```

D APPENDIX D

In this appendix, the lector can find a detail of fuzzy load flow simulations of the case base for the power system tested in Chapter 5. In this last chapter some figures were shown in order to illustrate de main differences of the types of arithmetic.

D.1 Base Case – Triangular Numbers

Injected powers at all buses have been modelled as triangular numbers as follows:

Active powers: $\langle 0.90 \cdot P_i, P_i, 1.1 \cdot P_i \rangle_T$
Reactive powers $\langle 0.90 \cdot Q_i, Q_i, 1.1 \cdot Q_i \rangle_T$

Where, P_i is the forecasted value of the active power injections and Q_i of the reactive power injections. Each number has been decomposed in 5 arithmetic intervals (m=4), in order to use the interval arithmetic and transformation method.

The FLF was run using the 3 approaches: interval and LR arithmetic and the transformation method. Table D-I shows the LR parameters.

TABLE D-I

PARAMETERS OF TRIANGULAR LR FUZZY NUMBERS OF THE VOLTAGE MAGNITUDE RESULTING FROM USE OF LR ARITHMETIC

	V4	V5	V6	V7	V8	V9
m-a	1,0201	0,9848	1,0041	1,0220	1,0105	1,0296
m	1,0258	0,9956	1,0127	1,0258	1,0159	1,0324
m+β	1,0315	1,0064	1,0212	1,0295	1,0213	1,0351

Table D-II and Table D-III show the intervals of the voltages' fuzzy numbers obtained.

TABLE D-II

INTERVALS OF TRIANGULAR FUZZY NUMBERS OF THE VOLTAGE MAGNITUDE RESULTING FROM USE OF STANDAR ARITHMETIC

	V4	V5	V6	V7	V8	V9
$a^{(0)}$	1,0250	0,9923	1,0095	1,0237	1,0116	1,0302
$a^{(0,25)}$	1,0252	0,9932	1,0103	1,0242	1,0127	1,0308
$a^{(0,5)}$	1,0254	0,9940	1,0111	1,0247	1,0138	1,0313
$a^{(0,75)}$	1,0256	0,9948	1,0119	1,0253	1,0148	1,0318
$a,b^{(1)}$	1,0258	0,9956	1,0127	1,0258	1,0159	1,0324
$b^{(0,75)}$	1,0260	0,9965	1,0134	1,0263	1,0169	1,0329
$b^{(0,5)}$	1,0262	0,9973	1,0142	1,0268	1,0180	1,0334
$b^{(0,25)}$	1,0263	0,9981	1,0150	1,0273	1,0191	1,0339
$b^{(0)}$	1,0265	0,9989	1,0158	1,0278	1,0201	1,0345

TABLE D-III

INTERVALS OF TRIANGULAR FUZZY NUMBERS OF THE VOLTAGE MAGNITUDE RESULTING FROM USE OF TRANSFORMATION METHOD

	V4	V5	V6	V7	V8	V9
$a^{(0)}$	1,0194	0,9856	1,0032	1,0216	1,0099	1,0293
$a^{(0,25)}$	1,0210	0,9881	1,0056	1,0226	1,0114	1,0300
$a^{(0,5)}$	1,0226	0,9906	1,0079	1,0237	1,0129	1,0308
$a^{(0,75)}$	1,0242	0,9931	1,0103	1,0247	1,0144	1,0316
a, $b^{(1)}$	1,0258	0,9956	1,0127	1,0258	1,0159	1,0324
$b^{(0,75)}$	1,0274	0,9980	1,0150	1,0268	1,0174	1,0331
$b^{(0,5)}$	1,0290	1,0006	1,0174	1,0279	1,0189	1,0339
$b^{(0,25)}$	1,0305	1,0031	1,0198	1,0289	1,0204	1,0347
$b^{(0)}$	1,0321	1,0056	1,0221	1,0300	1,0219	1,0354

Although it is not our idea to establish an error measure, Table D-IV illustrates the output voltage intervals for a variation of the power injections between 90% and 110% of the forecasted value.

TABLE D-IV

VOLTAGE LIMIT VALUES FOR A VARIATION OF THE POWER INJECTIONS BEETWEEN 90% AND 110%

	V4	V5	V6	V7	V8	V9
Min	1,0201	0,9848	1,0041	1,0220	1,0105	1,0296
Max	1,0258	0,9956	1,0127	1,0258	1,0159	1,0324

With the purpose of comparing and validating our approaches, next the results of the FLF are illustrated when the loads are modelled by another type of fuzzy numbers.

D.2 Base Case- Trapezoidal Numbers

Injected powers at all buses have been modelled as Trapezoidal fuzzy numbers, as follows:

Active powers: $\langle 0.90 \cdot P_i, 0.975 \cdot P_i, 1.025 \cdot P_i, 1.1 \cdot P_i \rangle_{tr}$

Reactive powers $\langle 0.90 \cdot Q_i, 0.975 \cdot Q_i, 1.025 \cdot Q_i, 1.1 \cdot Q_i \rangle_{tr}$

Now, power injections are modelled as trapezoidal fuzzy numbers. Each one is decomposed again in 5 cuts. Table D-V shows the LR parameters.

TABLE D-V

PARAMETERS OF TRAPEZOIDAL LR FUZZY NUMBERS OF THE VOLTAGE MAGNITUDE RESULTING FROM USE OF LR ARITHMETIC

	V4	V5	V6	V7	V8	V9
m_1-a	1,0185	0,9819	1,0018	1,0209	1,009	1,0288
m_1	1,0242	0,9926	1,0103	1,0247	1,0144	1,0316
m_2	1,0274	0,9986	1,015	1,0268	1,0174	1,0331
m_2+β	1,0331	1,0094	1,0235	1,0306	1,0228	1,0359

Table D-VI and Table D-VII illustrates the intervals of the voltages fuzzy numbers found.

TABLE D-VI

INTERVALS OF TRAPEZOIDAL FUZZY NUMBERS OF THE VOLTAGE MAGNITUDE RESULTING FROM USE OF STANDAR ARITHMETIC

	V4	V5	V6	V7	V8	V9
$a^{(0)}$	1,0250	0,9923	1,0095	1,0237	1,0116	1,0302
$a^{(0,5)}$	1,0253	0,9936	1,0107	1,0245	1,0132	1,0310
$a^{(1)}$	1,0256	0,9948	1,0119	1,0253	1,0148	1,0318
$b^{(1)}$	1,0260	0,9965	1,0134	1,0263	1,0169	1,0329
$b^{(0,5)}$	1,0263	0,9977	1,0146	1,0271	1,0185	1,0337
$b^{(0)}$	1,0265	0,9989	1,0158	1,0278	1,0201	1,0345

TABLE D-VII

INTERVALS OF TRAPEZOIDAL FUZZY NUMBERS OF THE VOLTAGE MAGNITUDE RESULTING FROM USE OF TRANSFORMATION METHOD

	V4	V5	V6	V7	V8	V9
$a^{(0)}$	1,0194	0,9836	1,0032	1,0216	1,0099	1,0293
$a^{(0,5)}$	1,0218	0,9881	1,0067	1,0231	1,0121	1,0304
$a^{(1)}$	1,0256	0,9948	1,0119	1,0253	1,0148	1,0318
$b^{(1)}$	1,0261	0,9965	1,0134	1,0263	1,0169	1,0329
$b^{(0,5)}$	1,0298	1,0031	1,0186	1,0284	1,0195	1,0343
$b^{(0)}$	1,0260	1,0076	1,0221	1,0300	1,0218	1,0354

The results in both cases with triangular and trapezoidal numbers show that the "arithmetic" can change the results. Taking as a reference the deterministic interval and the non consideration of the possibility value in the case of the standard arithmetic, some values of the interval of extreme voltage are not within the solution range.

The calculation of the line power flows is made using the linear approach in (36) and (37). Table D-VIII, Table D-IX, Table D-X show the results.

TABLE D-VIII

PARAMETERS OF TRAPEZOIDAL LR FUZZY NUMBERS OF LINE POWER FLOWS RESULTING FROM USE OF LR ARITHMETIC

	Lin 7-8	Lin 9-8	Lin 7-5	Lin 9-6	Lin 5-4
m_1-a	0,5595	0,0440	0,6990	0,4513	-0,5257
m_1	0,7194	0,1988	0,8298	0,5741	-0,4327
m_2	0,8082	0,2848	0,9026	0,6423	-0,3809
m_2+β	0,9681	0,4396	1,0334	0,7651	-0,2879

TABLE D-IX

INTERVALS OF TRAPEZOIDAL FUZZY NUMBERS OF LINE POWER FLOWS RESULTING FROM USE OF STANDAR ARITHMETIC

	Lin 7-8	Lin 9-8	Lin 7-5	Lin 9-6	Lin 5-4
$a^{(0)}$	0,5862	0,0698	0,7208	0,4717	-0,5844
$a^{(0,5)}$	0,6528	0,1343	0,7753	0,5229	-0,5178
$a^{(1)}$	0,7194	0,1988	0,8298	0,5741	-0,4512
$b^{(1)}$	0,8082	0,2848	0,9026	0,6423	-0,3624
$b^{(0,5)}$	0,8748	0,3493	0,9571	0,6934	-0,2958
$b^{(0)}$	0,9414	0,4138	1,0116	0,7446	-0,2292

TABLE D-X.

INTERVALS OF TRAPEZOIDAL FUZZY NUMBERS OF LINE POWER FLOWS RESULTING FROM USE OF TRANSFORMATION METHOD

	Lin 7-8	Lin 9-8	Lin 7-5	Lin 9-6	Lin 5-4
$a^{(0)}$	0,6006	0,0718	0,7391	0,4817	-0,5878
$a^{(0,5)}$	0,6600	0,1353	0,7845	0,5279	-0,5195
$a^{(1)}$	0,7194	0,1988	0,8298	0,5741	-0,4512
$b^{(1)}$	0,8082	0,2848	0,9026	0,6423	-0,3624
$b^{(0,5)}$	0,8635	0,3436	0,9444	0,6856	-0,2952
$b^{(0)}$	0,9188	0,4024	0,9863	0,7289	-0,2279

Table D-XI illustrates the extreme values of the power flows found by means of the deterministic load flow.

TABLE D-XI

EXTREME VALUES OF LINE POWER FLOWS FOR A VARIATION OF THE POWER INJECTIONS BEETWEEN 90% AND 110%

	Lin 7-8	Lin 9-8	Lin 7-5	Lin 9-6	Lin 5-4
Min	0,7135	0,1912	0,9165	0,6589	-0,2340
Max	0,8141	0,2926	0,8159	0,5574	-0,5798

In the three cases the results are satisfactory. Notice that the alpha-cut $[a^{(1)},b^{(1)}]$ is practically identical in all cases; this is not surprising because the main difference between the types of arithmetic is the form to operate the support.

Also, most of the intervals of extreme values are within the fuzzy numbers. This is a good indicator. Nevertheless, in the case of line 5-4, the result is not totally satisfactory. The negative flow is identified but some values that belong to the interval of power flow limit values are not within the solution, although the values obtained are not very distant. Algorithms of correction must be applied in this type of lines. A detail of the method is presented in [SAR, 1991] [1].

[1] [SAR, 1991] Saraiva J.T., Miranda V., Matos M.A., "Generation and load uncertainties incorporated in load flow studies", Proc. MELECON 91, Ljubljana, May 1991.

D. APPENDIX E

Tables of conditional probabilities of the Bayesian network created in chapter 6 in order to assess the security of the power system with regard to cyber attacks on the IC system.

POSITION OF THE TERRORIST GROUP	POLITICAL SITUATION	EXPECTED PUBLIC REACTION	MOTIVATION OF THE ATTACK		
			High	Medium	Low
High	Critical	High	0.900	0.100	0.000
		Medium	0.600	0.250	0.150
		Low	0.100	0.600	0.300
	Moderately critical	High	0.600	0.400	0.000
		Medium	0.400	0.600	0.000
		Low	0.100	0.600	0.300
	Non critical	High	0.200	0.600	0.200
		Medium	0.100	0.600	0.300
		Low	0.050	0.200	0.750
Average	Critical	High	0.700	0.300	0.000
		Medium	0.400	0.600	0.000
		Low	0.000	0.400	0.600
	Moderately critical	High	0.400	0.500	0.100
		Medium	0.100	0.700	0.200
		Low	0.050	0.500	0.450
	Non critical	High	0.100	0.500	0.400
		Medium	0.050	0.400	0.550
		Low	0.000	0.100	0.900
Low	Critical	High	0.300	0.700	0.000
		Medium	0.100	0.600	0.300
		Low	0.000	0.200	0.800
	Moderately critical	High	0.200	0.500	0.300
		Medium	0.050	0.600	0.350
		Low	0.000	0.200	0.800
	Non critical	High	0.050	0.400	0.550
		Medium	0.000	0.200	0.800
		Low	0.000	0.000	1.000

VULNERABILITIES OF THE NETWORK	VULNERABILITIES OF THE ASSET	VULNERABILITY OF THE TARGET		
		High	Medium	Low
High	High	0.900	0.100	0.000
	Medium	0.300	0.700	0.000
	Low	0.100	0.400	0.500
Medium	High	0.500	0.500	0.000
	Medium	0.100	0.800	0.100
	Low	0.000	0.200	0.800
Low	High	0.200	0.700	0.100
	Medium	0.000	0.500	0.500
	Low	0.000	0.100	0.900

RESOURCES FOR ATTACK	MOTIVATION OF THE ATTACK	VULNERABILITY OF THE TARGET	SOPHISTICATION OF THE ATTACK			
			Integrity	Availability	Confidentiality	No attack
Enough	High	High	0.700	0.300	0.000	0.000
		Medium	0.250	0.250	0.000	0.500
		Low	0.050	0.150	0.150	0.650
	Medium	High	0.300	0.400	0.100	0.200
		Medium	0.100	0.350	0.150	0.400
		Low	0.050	0.250	0.000	0.700
	Low	High	0.100	0.300	0.200	0.400
		Medium	0.000	0.150	0.250	0.600
		Low	0.000	0.100	0.050	0.850
Regular	High	High	0.300	0.300	0.100	0.300
		Medium	0.100	0.400	0.000	0.500
		Low	0.000	0.250	0.050	0.700
	Medium	High	0.100	0.400	0.200	0.300
		Medium	0.050	0.300	0.300	0.350
		Low	0.000	0.100	0.050	0.850
	Low	High	0.000	0.300	0.200	0.500
		Medium	0.000	0.100	0.100	0.800
		Low	0.000	0.000	0.100	0.900
Low	High	High	0.200	0.300	0.100	0.400
		Medium	0.050	0.300	0.150	0.500
		Low	0.000	0.150	0.250	0.600
	Medium	High	0.000	0.200	0.300	0.500
		Medium	0.000	0.150	0.250	0.600
		Low	0.000	0.100	0.100	0.800
	Low	High	0.000	0.000	0.300	0.700
		Medium	0.000	0.000	0.200	0.800
		Low	0.000	0.000	0.100	0.900

INFORMATION AVAILABILITY OF THE TARGET	KNOWLEDGE OF VULNERABILITIES	TYPE OF PERPETRATOR	POSITION OF THE TERRORIST GROUP	RESOURCES FOR ATTACK		
				Enough	Regular	Low
Enough	Enough	Insider	High	1.000	0.000	0.000
			Average	0.750	0.250	0.000
			Low	0.600	0.400	0.000
		Ex-Insider	High	0.800	0.200	0.000
			Average	0.700	0.150	0.150
			Low	0.500	0.250	0.250
		Professional cracker	High	0.500	0.500	0.000
			Average	0.300	0.700	0.000
			Low	0.200	0.600	0.200
	Regular	Insider	High	0.850	0.150	0.000
			Average	0.700	0.300	0.000
			Low	0.500	0.500	0.000
		Ex-Insider	High	0.700	0.200	0.100
			Average	0.600	0.200	0.200
			Low	0.400	0.400	0.200
		Professional cracker	High	0.300	0.600	0.100
			Average	0.150	0.650	0.200
			Low	0.100	0.500	0.400
	Low	Insider	High	0.750	0.175	0.075
			Average	0.600	0.280	0.120
			Low	0.450	0.385	0.165
		Ex-Insider	High	0.650	0.200	0.150
			Average	0.500	0.300	0.200
			Low	0.300	0.300	0.400
		Professional cracker	High	0.300	0.600	0.100
			Average	0.150	0.650	0.200
			Low	0.100	0.500	0.400
Regular	Enough	Insider	High	0.900	0.100	0.000
			Average	0.700	0.300	0.000
			Low	0.600	0.400	0.000
		Ex-Insider	High	0.700	0.300	0.000
			Average	0.500	0.500	0.000
			Low	0.400	0.400	0.200
		Professional cracker	High	0.300	0.600	0.100
			Average	0.200	0.700	0.100
			Low	0.100	0.500	0.400
	Regular	Insider	High	0.750	0.175	0.075
			Average	0.600	0.280	0.120
			Low	0.500	0.350	0.150
		Ex-Insider	High	0.300	0.700	0.000
			Average	0.200	0.600	0.200
			Low	0.100	0.500	0.400
		Professional cracker	High	0.100	0.600	0.300
			Average	0.050	0.600	0.350
			Low	0.000	0.350	0.650
	Low	Insider	High	0.600	0.200	0.200
			Average	0.500	0.250	0.250
			Low	0.450	0.275	0.275
		Ex-Insider	High	0.200	0.500	0.300
			Average	0.100	0.500	0.400
			Low	0.100	0.400	0.500
		Professional cracker	High	0.100	0.400	0.500
			Average	0.100	0.300	0.600
			Low	0.050	0.200	0.750
Low	Enough	Insider	High	0.750	0.175	0.075
			Average	0.650	0.245	0.105
			Low	0.550	0.315	0.135
		Ex-Insider	High	0.300	0.100	0.600
			Average	0.200	0.600	0.200
			Low	0.100	0.500	0.400
		Professional cracker	High	0.300	0.550	0.150
			Average	0.150	0.500	0.350
			Low	0.050	0.450	0.500
	Regular	Insider	High	0.600	0.200	0.200
			Average	0.450	0.275	0.275
			Low	0.400	0.300	0.300
		Ex-Insider	High	0.200	0.500	0.300
			Average	0.100	0.600	0.300
			Low	0.050	0.300	0.650
		Professional cracker	High	0.200	0.500	0.300
			Average	0.050	0.400	0.550
			Low	0.000	0.400	0.600
	Low	Insider	High	0.500	0.250	0.250
			Average	0.400	0.300	0.300
			Low	0.350	0.325	0.325
		Ex-Insider	High	0.200	0.600	0.200
			Average	0.100	0.500	0.400
			Low	0.000	0.400	0.600
		Professional cracker	High	0.050	0.200	0.750
			Average	0.050	0.100	0.850
			Low	0.000	0.100	0.900

VULNERABILITIES OF THE NETWORK	VULNERABILITIES OF THE ASSET	VULNERABILITY OF THE TARGET		
		High	Medium	Low
High	High	0.900	0.100	0.000
	Medium	0.300	0.700	0.000
	Low	0.100	0.400	0.500
Medium	High	0.500	0.500	0.000
	Medium	0.100	0.800	0.100
	Low	0.000	0.200	0.800
Low	High	0.200	0.700	0.100
	Medium	0.000	0.500	0.500
	Low	0.000	0.100	0.900

OPERATING STATE	CRITICALITY OF COMPONENTS POWER SYSTEM	CRITICALITY OF THE FUNCTION	CONTINUITY OF THE FUNCTION	CONSEQUENCE FOR THE POWER SYSTEM OPERATION				
				High	Medium	Low	No impact	No attack
NORMAL	High	Contr & Prot	Continuity	0.000	0.000	0.100	0.900	0.000
			Integrity	0.300	0.500	0.200	0.000	0.000
			Availability	0.200	0.300	0.300	0.200	0.000
			Confidentiality	0.000	0.000	0.100	0.900	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
		Protection	Continuity	0.000	0.000	0.200	0.800	0.000
			Integrity	0.200	0.200	0.400	0.200	0.000
			Availability	0.100	0.400	0.300	0.200	0.000
			Confidentiality	0.000	0.000	0.100	0.900	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
		Measurement	Continuity	0.000	0.000	0.000	1.000	0.000
			Integrity	0.000	0.000	0.100	0.900	0.000
			Availability	0.000	0.000	0.050	0.950	0.000
			Confidentiality	0.000	0.000	0.500	0.500	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
	Average	Contr & Prot	Continuity	0.000	0.000	0.050	0.950	0.000
			Integrity	0.000	0.200	0.200	0.600	0.000
			Availability	0.000	0.100	0.200	0.700	0.000
			Confidentiality	0.000	0.000	0.050	0.950	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
		Protection	Continuity	0.000	0.000	0.050	0.950	0.000
			Integrity	0.000	0.000	0.200	0.800	0.000
			Availability	0.000	0.000	0.050	0.950	0.000
			Confidentiality	0.000	0.000	0.050	0.950	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
		Measurement	Continuity	0.000	0.000	0.000	1.000	0.000
			Integrity	0.000	0.000	0.100	0.900	0.000
			Availability	0.000	0.000	0.050	0.950	0.000
			Confidentiality	0.000	0.000	0.500	0.500	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
	Low	Contr & Prot	Continuity	0.000	0.000	0.000	1.000	0.000
			Integrity	0.000	0.000	0.100	0.900	0.000
			Availability	0.000	0.000	0.050	0.950	0.000
			Confidentiality	0.000	0.000	0.100	0.900	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
		Protection	Continuity	0.000	0.000	0.000	1.000	0.000
			Integrity	0.000	0.000	0.100	0.900	0.000
			Availability	0.000	0.000	0.050	0.950	0.000
			Confidentiality	0.000	0.000	0.100	0.900	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
		Measurement	Continuity	0.000	0.000	0.000	1.000	0.000
			Integrity	0.000	0.000	0.100	0.900	0.000
			Availability	0.000	0.000	0.050	0.950	0.000
			Confidentiality	0.000	0.000	0.500	0.500	0.000
			No attack	0.000	0.000	0.000	0.000	1.000

ALERT	High	Contr & Prot	Continuity	0.000	0.000	0.100	0.900	0.000
			Integrity	0.500	0.500	0.000	0.000	0.000
			Availability	0.350	0.650	0.000	0.000	0.000
			Confidentiality	0.000	0.000	0.100	0.900	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
		Protection	Continuity	0.000	0.000	0.100	0.900	0.000
			Integrity	0.100	0.100	0.100	0.700	0.000
			Availability	0.100	0.100	0.100	0.700	0.000
			Confidentiality	0.000	0.000	0.100	0.900	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
		Measurement	Continuity	0.000	0.000	0.000	1.000	0.000
			Integrity	0.000	0.000	0.200	0.800	0.000
			Availability	0.000	0.000	0.050	0.950	0.000
			Confidentiality	0.000	0.000	0.600	0.400	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
	Average	Contr & Prot	Continuity	0.000	0.000	0.100	0.900	0.000
			Integrity	0.250	0.650	0.100	0.000	0.000
			Availability	0.200	0.550	0.250	0.000	0.000
			Confidentiality	0.000	0.000	0.050	0.950	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
		Protection	Continuity	0.000	0.000	0.100	0.900	0.000
			Integrity	0.100	0.100	0.100	0.700	0.000
			Availability	0.100	0.100	0.100	0.700	0.000
			Confidentiality	0.000	0.000	0.050	0.950	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
		Measurement	Continuity	0.000	0.000	0.000	1.000	0.000
			Integrity	0.000	0.000	0.200	0.800	0.000
			Availability	0.000	0.000	0.050	0.950	0.000
			Confidentiality	0.000	0.000	0.600	0.400	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
	Low	Contr & Prot	Continuity	0.000	0.000	0.100	0.900	0.000
			Integrity	0.100	0.500	0.400	0.000	0.000
			Availability	0.050	0.450	0.500	0.000	0.000
			Confidentiality	0.000	0.000	0.100	0.900	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
		Protection	Continuity	0.000	0.000	0.100	0.900	0.000
			Integrity	0.100	0.100	0.100	0.700	0.000
			Availability	0.100	0.100	0.100	0.700	0.000
			Confidentiality	0.000	0.000	0.100	0.900	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
		Measurement	Continuity	0.000	0.000	0.000	1.000	0.000
			Integrity	0.000	0.000	0.200	0.800	0.000
			Availability	0.000	0.000	0.050	0.950	0.000
			Confidentiality	0.000	0.000	0.600	0.400	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
EMERGENCY	High	Contr & Prot	Continuity	0.000	0.000	0.500	0.500	0.000
			Integrity	0.950	0.050	0.000	0.000	0.000
			Availability	0.950	0.050	0.000	0.000	0.000
			Confidentiality	0.000	0.000	0.100	0.900	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
		Protection	Continuity	0.000	0.000	0.400	0.600	0.000
			Integrity	0.800	0.100	0.000	0.100	0.000
			Availability	0.800	0.100	0.000	0.100	0.000
			Confidentiality	0.000	0.000	0.100	0.900	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
		Measurement	Continuity	0.000	0.000	0.000	1.000	0.000
			Integrity	0.000	0.000	0.250	0.750	0.000
			Availability	0.000	0.000	0.100	0.900	0.000
			Confidentiality	0.000	0.000	0.600	0.400	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
	Average	Contr & Prot	Continuity	0.000	0.000	0.200	0.800	0.000
			Integrity	0.900	0.050	0.050	0.000	0.000
			Availability	0.800	0.100	0.100	0.000	0.000
			Confidentiality	0.000	0.000	0.050	0.950	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
		Protection	Continuity	0.000	0.000	0.200	0.800	0.000
			Integrity	0.600	0.400	0.000	0.000	0.000
			Availability	0.500	0.500	0.000	0.000	0.000
			Confidentiality	0.000	0.000	0.050	0.950	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
		Measurement	Continuity	0.000	0.000	0.000	1.000	0.000
			Integrity	0.000	0.000	0.200	0.800	0.000
			Availability	0.000	0.000	0.050	0.950	0.000
			Confidentiality	0.000	0.000	0.600	0.400	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
	Low	Contr & Prot	Continuity	0.000	0.000	0.200	0.800	0.000
			Integrity	0.600	0.400	0.000	0.000	0.000
			Availability	0.450	0.400	0.015	0.135	0.000
			Confidentiality	0.000	0.000	0.200	0.800	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
		Protection	Continuity	0.000	0.000	0.200	0.800	0.000
			Integrity	0.400	0.500	0.100	0.000	0.000
			Availability	0.300	0.600	0.100	0.000	0.000
			Confidentiality	0.000	0.000	0.100	0.900	0.000
			No attack	0.000	0.000	0.000	0.000	1.000
		Measurement	Continuity	0.000	0.000	0.000	1.000	0.000
			Integrity	0.000	0.000	0.200	0.800	0.000
			Availability	0.000	0.000	0.050	0.950	0.000
			Confidentiality	0.000	0.000	0.600	0.400	0.000
			No attack	0.000	0.000	0.000	0.000	1.000

RISK ASSESSMENT FOR POWER SYSTEM SECURITY WITH REGARD TO INTENTIONAL EVENTS

Abstract

Power systems are critical infrastructures which are highly interconnected and highly interdependent on other basic infrastructures on which basic human activities depend. Due to this relevance, the electrical sector has been and will continue to be a target of terrorist groups. The ability to deal with these terrorist situations depends on the anticipation capacity, the reflection in times where there is no crisis and the operational management of the owners of the utilities. Therefore, contingencies resulting from terrorism must be taken into consideration when assessing security.

This thesis presents a method based on the evaluation of risk, which enables operators and planners to assess the power system security with regard to possible terrorist acts. By using probabilistic inference and theory of possibilities, we consider the uncertainty associated with the dynamic of terrorism as well as the uncertainty associated to load and generation forecasting. We attempt to take into account potential cyberattacks on the communication system of the power system, which can affect the security as a whole. The methods are validated with test systems, taking as example terrorist attacks on the Colombian electrical infrastructure.

Keywords: Power system security assessment, terrorism on electrical infrastructure, cybersecurity of power systems, risk assessment, Bayesian networks, theory of possibilities, fuzzy numbers.

ÉVALUATION DU RISQUE POUR LA SÉCURITÉ DES RÉSEAUX ÉLECTRIQUE FACE AUX ÉVÉNEMENTS INTENTIONNELS

Résumé

Les réseaux électriques sont des infrastructures critiques fortement interconnectées et dépendantes d'autres infrastructures essentielles pour assurer diverses activités humaines. Compte tenu ce rôle clef, le secteur électrique est, et continuera à l'être, une cible privilégiée pour les groupes terroristes. Pour palier à ces attaques terroristes, il est indispensable d'avoir une grande capacité d'anticipation, de moyens de réflexion lors des périodes d'accalmies, et une bonne gestion (de crise) de la part des exploitants. Ainsi, les aléas résultants des attaques terroristes doivent être pris en compte dans l'évaluation de la sécurité du réseau.

Cette thèse présente une méthode basée sur l'évaluation du risque, ce qui permet aux exploitants et aux planificateurs d'estimer la sécurité du réseau en considérant l'occurrence d'actes malveillants. L'utilisation de l'inférence probabiliste et de la théorie de la possibilité, permet de prendre en considération les incertitudes liées à la dynamique terroriste ainsi que les incertitudes dues aux prévisions de charge et de production. Nous avons aussi étendu notre méthodologie aux actes de malveillance liés aux cyberattaques sur les systèmes de communication du réseau électrique qui peuvent affecter la sécurité de ce dernier. Les méthodes sont testées avec des réseaux test standards, en prenant comme exemple l'expérience de l'infrastructure électrique Colombienne, fortement menacée par les attaques terroristes.

Mots clefs : Evaluation de la sécurité des réseaux électriques, terrorisme contre les infrastructures électriques, cybersécurité des réseaux électriques, évaluation du risque, réseaux Bayésiens, théorie de la possibilité, nombres flous.

Laboratoire

G2ELAB – Laboratoire de Génie Electrique de Grenoble – UMR 5529 Grenoble INP/UJF/CNRS
BP 46, Domaine Universitaire
38402 Saint Martin d'Hères Cedex - FRANCE

Universidad de los Andes
Departamento de Ingeniería Eléctrica y Electrónica
Bogotá D.C. COLOMBIA