

**REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE  
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE  
SCIENTIFIQUE**



**FACULTE DES HYDROCARBURES ET DE LA CHIMIE**

**LABORATOIRE DE RECHERCHE SUR L' ELECTRIFICATION DES ENTREPRISES  
INDUSTRIELLES  
(LREEI)**

**Mémoire de Magistère**

PRESENTE PAR :

**Mr. BOUREZG Abdrabbi**

EN VUE DE L'OBTENTION DU TITRE DE  
**MAGISTER EN AUTOMATISATION**

**OPTION : AUTOMATIQUE APPLIQUE ET TRAITEMENT DU SIGNAL**

**THEME**

**Design & Implementation of algorithms for dependability parameters  
evaluation and improvements of circuit breakers.**

Soutenu publiquement le : Date : **24/12/2006**    Heure : **9 :00**    Lieu : **Bibliothèque Centrale**

Devant le Jury composé de :

L. REFOUFI	Professeur	UMBB	Président
B. NADJI	Chargé de Cours	UMBB	Rapporteur
R. BENFDILA	Professeur	UMMTO	Examineur
D.OUAHDI	Maître de conférences	UMBB	Examineur
H. BENTARZI	Miâtre de conference	UMBB	Examineur

**Année Universitaire:200 6/200 7**

## **Acknowledgements :**

*For you & Thank you : Parents ;  
Sisters ;  
wife ;*

*To all of you students;*

## **Résumé**

Les systèmes de protection des disjoncteurs haute tension sont parfois très complexes contenant différents dispositifs, particulièrement pour les défaillances de contournement.

Le souci de l'ingénieur de protection des systèmes de puissance est leur sûreté de fonctionnement qui présente un problème analytique significatif.

Dans ce travail, nous présentons des méthodes et des outils de modélisation conçus au développement et à l'exécution d'un système sûr. Comme système à étudier, nous avons choisi le disjoncteur à haute tension.

La méthode de l'arbre de défaillance a été choisie pour sa simplicité. Une analyse qualitative et quantitative a été effectuée sur les différentes méthodes de protection des disjoncteurs et surtout les défaillances de contournement.

Nous avons appliqué une méthode de modélisation, en utilisant les fonctions de transfert au modèle pour les paramètres (disponibilité et de la fiabilité) au lieu de n'importe quelle autre méthode qui a comme contraintes la densité de probabilité de panne/réparation si elles sont constantes ou non distribuées.

Afin de modéliser les deux paramètres de la SdF à savoir disponibilité et fiabilité, nous avons appliqué une méthode basée sur l'utilisation des fonctions de transfert.

Ce travail présente une méthode novatrice permettant de calculer la disponibilité d'un système réparable quel que soit le taux de transition utilisé.

Afin de modéliser et d'améliorer les paramètres de sûreté comme la disponibilité et la fiabilité par rapport au coûts, la synthèse et l'implémentation sous SIMULINK et MAPLE a été réalisé pour la modélisation en utilisant des block de fonctions de transfert et l'implémentation des algorithmes d'allocation des paramètres au dessus est effectuée en Delphi.

Comme nous savons que la sûreté de fonctionnement (SdF) est une science définie par de nombreuses méthodes et concepts mathématiques. La plupart des études réalisées pour obtenir quantitativement les paramètres de sûreté de fonctionnement (Fiabilité, Disponibilité, Maintenabilité, Sécurité) sont des études asymptotiques à taux constants. L'hypothèse de taux constants facilite de telles études et permet de recourir à la

représentation markovienne, notamment pour des systèmes constitués de plusieurs entités. Cependant, lorsque le système étudié est systématiquement perturbé et atteint difficilement un état stationnaire, il est alors nécessaire d'intégrer des taux de transitions dépendant du temps : la représentation markovienne ne s'applique plus. Les lignes de production constituées de machines séparées par des stocks sont un exemple de tels systèmes. Il en est de même lorsque les systèmes ont une durée de vie très courte relativement au taux de défaillance.

A l'heure actuelle, les études de SdF sont encore trop souvent limitées au comportement stationnaire (étude asymptotique). Cette constatation nous a amené à développer une méthode novatrice d'évaluation de la SdF qui vise à faire une représentation dynamique de l'évolution du paramètre disponibilité dès la phase de conception. Cette méthode rejoint les méthodes de SdF dynamique actuellement en émergence pour l'étude des systèmes réparables à taux non constants (processus non markoviens).

L'allocation d'indicateurs de sûreté de fonctionnement (en particulier la fiabilité) est une phase importante du développement d'un équipement. Habituellement, elle a pour objet de faire atteindre à un produit objectif de performance intrinsèque spécifié, plus rarement de maximiser cette performance.

L'objet de la dernière partie de ce travail est de présenter un algorithme pseudo-optimal d'indicateurs de sûreté de fonctionnement pour un système à architecture fonctionnelle quelconque. L'algorithme élaboré présente une heuristique d'optimisation privilégiant la rapidité de résolution à la résolution exacte souvent très coûteuse en temps de calcul.

**Mots clés :**

Sûreté de fonctionnement, disjoncteurs à hautes tension, arbre de défaillances, algorithmes.

*“Well-structured and defined problems that have only one right and logical answer simply teach students about problem solving, not how to problem-solve. In the real world, workers rarely repeat exactly the same steps to solve problems; therefore the lockstep solution sequence taught in well-structured classroom problems is rarely transferable. To be successful students need to practice solving ill-defined problems that reflect life beyond the classroom.”* **A. Mohammed Hambaba**

## **Abstract**

Dependability of power systems is a concern of protection engineers and presents a significant analytical problem.

This work presents a dependability analysis framework that includes the construction flowchart of a system fault tree with any functional architecture.

Delphi- based software is first developed to convert a Boolean expression that represents top level event to a fault tree graphical model. In addition it allows calculating the probability of occurrence of this event.

The second part deals with the development of a modelling method that is based on the use of transfer functions to represent the failure/repair probability density function. Unlike other methods whose applicability is constrained by the requirements of constant failure/repair probability density function, this transfer function – based method is free of any analytical constraints ,i.e. it is applicable irrespective of whether the density functions is constants or not. The advantage of this method is to take into account the probability evolution of the system failure from initial state until the final value and will not be limited to an approximate evaluation.

The final part of our work is devoted to the allocation algorithms which are designed and implemented using the Delphi language and integrated with the previous ones developed to draw the fault tree from the Boolean expression. Hence, we proposed algorithms for allocation in the case of cost minimization under constraints of reliability, availability or maintainability (this is the dual problem that is also solvable using these algorithms). This iterative algorithm allows allocating the adequate redundancy level as well as the reliability level of subsystem components.

**Key words:**

Dependability, power system circuit breaker, fault tree, algorithms

**General Introduction:**

Issues in aeronautics, nuclear, electrical energy generation & distribution and spatial domains motivate dependability to impose itself progressively to most sectors of activity, petrochemical, transport and power systems. Dependability can be used in the identification, analysis, assessment, failures hierarchy in order to minimize their effects by taking into account the constraints of security and profitability.

The research for improving the power systems performances, requirements of functionalities, quality and cost, justifies needs to a dependability study.

The power systems dependability, aims a survey of the system during both, design and operating phases. Then, two major approaches can be used such as on-line and off-line.

The off-line approach corresponds to the survey of the system during its design phase. The developed research concerns the analysis of shop structure properties in terms of flexibility and tolerance, the models validation, the assessment of performance and dependability indicators, the survey of the different functioning modes. In brief, everything that permits to lead up to the design and design of a sure power system.

The on-line approach corresponds to the survey of the system during its operating phase. The work herein, deals with the development of compensation actions politics and restarting in case of failure. It is what corresponds to the survey, the monitoring, the risks management, functioning modes management, strategies of corrective maintenance, the operational security.... The final objective is the sure operating of a power system.

The study of any system dependability can be performed through the combined utilization of methods allowing, to measure determine different dependability parameters. No one has noted that dependability indicators as Reliability, Maintainability and Availability are the objectives measures of the quality and services. They must be valued since the design and must be tested permanently during the operating phase.

The aim of the present work is to study the whole methods and intended modelling tools to the development and the implementation of a dependable system.

**Chapter one** summarises techniques, tools and recent developments in the field of system dependability evaluation. System dependability measures are defined, and techniques to represent the system dependability behaviour are presented. Computational

methods for obtaining the system dependability measures from the models are also discussed. Several issues of importance in dependability evaluation are briefly discussed.

**The second chapter** deals with the design and application of electrical equipment namely the circuit breaker. The different design types of high voltage circuit breakers, moreover their typical ratings, and our case study, is the analysis and presentation of flashover failure and their different protection schemes. At the end of this chapter the breaker failure modes are mentioned.

**The third chapter** exposes one of the non-state space dependability models. We have been focused on fault trees analysis for their simplicity in understanding and manipulating. We described the fault trees flow-chart construction, by the fact, we explained the qualitative and quantitative analysis of the trees then we've ended this chapter by an application on the different circuit breaker-flashover schemes previously mentioned.

The kernel of this work is **the forth chapter** which consists of two parts:

The first part deals with a modelling method that is based on the use of transfer functions to model one of dependability parameters (availability & reliability) instead of any other method that has constraints such as the failure/repair probability density functions if they are constants or not (distributed). Dependability is a science that can be defined by numerous mathematical methods and concepts. Most studies achieved to get dependability parameters quantitatively (Reliability, Availability, Maintainability, Security) are asymptotic studies with constant rates. The constant rate hypothesis facilitates such studies and permits to resort toward Markovian representation, notably for systems consist of several entities. However, when the studied system is systematically disturbed and is reached a stationary state with difficulty, then, it is necessary to integrate time-dependent transition rates: Markovian representation doesn't apply anymore. Production lines constituted of machines separated by stocks are an example of such system. It's the same thing when systems have a very short life time with respect to the failure rate.

Till now, studies of RAMS are often limited to stationary behavior (approximate studies). This observation brought us to develop a new method for RAMS assessment and evaluation; it aims to make a dynamic representation of the probability evolution of the

availability parameter since the conception phase. This method rejoins methods of dynamic RAMS currently in parameter emergence for the repairable systems survey with non-constant rates (non-Markovian process).

The second part of this chapter concerns the design & implementation of algorithms for RAMS parameter's allocation.

The allocation of RAMS indicators (in particular of reliability) is an important phase of the development of a product. Usually, it commits in making a product reach a specified intrinsic performance objective, more rarely in maximizing this performance.

The purpose of this part is to present pseudo-optimal algorithms for allocation of RAMS indicators for a system having any functional architecture (we apply them in our case of protection breaker-flashover schemes).

The elaborated algorithm presents a heuristic of optimization giving the priority to speed of resolution rather than getting the exact solution, very expensive in time of calculation.

To be useful, allocations must be initialized very early in the life of the system and, so possible, at the time of the definition of its technical breakdown structure. It permits to optimize its definition, instead of depending of a fixed architecture. Besides, the presented algorithms enable on one hand, to allocate parameters of intrinsic reliability to the system components, but also to propose other design alternatives of conception while suggesting for example redundancies of certain equipments (namely power system equipments).

The algorithms of allocations propose a cost minimization under certain intrinsic performance constraints bound to the considered system (reliability, availability, but also objectives of mean time of unavailability or again of probability of the dreaded events,).

Let's note that in this part, mentioned allocation is of reliability, availability mainly, even though these works concern allocation done for other dependability indicators like maintainability, testability,...

Results in each part are presented and discussed, then finally we finished by a general conclusion.



## **TABLE OF CONTENTS.**

<b>CHAPTER I: Different Techniques of System Dependability .....</b>	<b>11</b>
<b>1.1. Introduction.....</b>	<b>11</b>
<b>I.2. Definitions and notations.....</b>	<b>12</b>
<b>I.2.1. Mathematical Element of the RAMS.....</b>	<b>12</b>
<b>I.2.2. Measures of Dependability.....</b>	<b>12</b>
I. 2.2.1. Reliability Measures.....	13
I. 2.2.2. Availability Measures.....	15
I. 2.2.3. Maintainability.....	16
I. 2.2.4. Security .....	16
<b>I.3. Dependability Model Types.....</b>	<b>17</b>
<b>I. 3.1. Non State Space Models.....</b>	<b>19</b>
I. 3.1.1. Reliability Block Diagrams (RBDs) .....	19
I. 3.1.2. Fault Trees (FTs).....	19
<b>I. 3.2. State Space Models .....</b>	<b>20</b>
I. 3.2.1. Continuous Time Markov Chains (CTMCs).....	20
I. 3.2.2. Markov Reward Models (MRMs).....	22
I. 3.2.3. Non-Markovian Models.....	23
I. 3.2.4. Supplementary Variables.....	24
I. 3.2.5. Phase Type Expansions .....	24
I. 3.2.6. Markov Renewal Theory.....	25
I. 3.2.7. Semi-Markov process.....	28
<b>I.4. Computational methods.....</b>	<b>30</b>
<b>I. 4.1. Non state space models.....</b>	<b>30</b>
I. 4.1.1. Reliability Block Diagrams.....	30
I. 4.1.2. Fault Trees.....	32
<b>I. 4.2. State space models.....</b>	<b>33</b>
I. 4.2.1. Continuous Time Markov Chains.....	33
I.4.2.2. Non-Markovian Models.....	34
<b>I.5. Conclusion.....</b>	<b>35</b>
<b>Chapter II: Circuit breakers theory, design and their flashover failures.....</b>	<b>36</b>
<b>II.1. Introduction.....</b>	<b>37</b>
<b>II.2. Role of circuit breakers in power systems.....</b>	<b>38</b>
II.2.1. Controlled switching.....	40
II.2.2. Controlled switching under steady state conditions.....	40
<b>II.3. Circuit breaker design .....</b>	<b>42</b>
II.3.1. Operating mechanisms.....	42
II.3.2. General.....	42
II.3.3. Working medium/stored energy.....	43
II.3.4. Latches.....	43
II.3.5. Release valves in pneumatic or hydraulic operators.....	43
II.3.6. Solenoids.....	44

II.3.7. Opening.....	44
II.3.8. Closing.....	44
II.3.9. Auxiliary switches.....	44
II.3.10. Mechanism auxiliaries.....	44
<b>II.4. SF6 circuit breakers.....</b>	<b>44</b>
<b>II.5. Bulk oil circuit breakers .....</b>	<b>50</b>
<b>II.6. Vacuum circuit breakers.....</b>	<b>51</b>
<b>II.7. Air magnetic circuit breakers.....</b>	<b>53</b>
<b>II.8. Air blast circuit breakers.....</b>	<b>54</b>
<b>II.9. Minimum oil circuit breakers.....</b>	<b>54</b>
<b>II.10. High voltage circuit breaker flashover failures.....</b>	<b>55</b>
II.10.1. Introduction.....	55
II.10.2. Example Real case analysis.....	57
II.10.3. Comparison between real & Simulation of different flashover conditions...	57
<b>II.11. Methods for flashover protection.....</b>	<b>60</b>
II.11.1. Method A. Residual Overcurrent and Breaker Auxiliary Contact.....	60
II.11.2. Method B. Current and Breaker Auxiliary Contact per Phase.....	63
II.11.3. Method C. Time Limits and Close-Signal Monitoring to Detect Flashover..	63
II.11.4. Method D. Live-Bus Voltage Supervision.....	64
II.11.5. Method E. Voltage at Both Sides of the Breaker.....	64
<b>II.12. Breaker states and failure modes.....</b>	<b>66</b>
<b>II.13. Conclusion.....</b>	<b>67</b>
<b>Chapter III: Dependability evaluation using static Fault Tree analysis.....</b>	<b>68</b>
<b>III.1. Introduction.....</b>	<b>69</b>
<b>III.2. The Fault Tree Approach.....</b>	<b>69</b>
<b>III.3. Qualitative and Quantitative Evaluations of a Fault Tree.....</b>	<b>70</b>
<b>III.4. Role of FTA in Decision Making.....</b>	<b>71</b>
<b>III.5. Fault tree construction.....</b>	<b>74</b>
III.5.1. Qualitative analysis: coherent structure functions and minimal cut sets.....	83
III.5.2. Quantitative analysis.....	86
<b>III.6. Dependability evaluation of methods for breaker- flashover protection.....</b>	<b>87</b>
III.6.1. Fault tree reliability analysis of flashover-protection methods.....	87
III.6.1.1. Fault Tree Methodology and Input Data.....	87
III.6.1.2. Fault Tree for Method A. Residual Current and 52b.....	92
III.6.1.3. Fault Tree for Method B, Phase Current and 52a Per Phase.....	94
III.6.1.4. Fault Tree for Method C, Close Monitoring and Coincidence Timers.....	94
III.6.1.5. Tree for Method D, Close Monitoring, Coincidence Timers, and Live-Voltage supervision.....	95
III.6.1.6. Fault Tree for Method E, Voltage at Both Sides of the Breaker.....	96
III.6.2. Monitoring and predictive maintenance of breakers.....	99
<b>III.7. Conclusion.....</b>	<b>100</b>
<b>Chapter IV: Dependability parameters modelling .....</b>	<b>101</b>
<b>IV.1. Introduction.....</b>	<b>102</b>
<b>IV.2. Methods for obtaining the availability.....</b>	<b>104</b>

IV.2.1. Markov method; $\mu$ and $\lambda$ are constants.....	104
IV.2.2. Analytical description of availability expression.....	104
IV.2.3. Monté-carlo Simulation .....	105
<b>IV.3. The renewal theory</b> .....	105
<b>IV.4. Calculation of availability from renewal theory</b> .....	107
<b>IV.5. Algorithms for allocation of rams indicators</b> .....	117
IV.5.1. Optimization heuristic for reliability allowance.....	117
IV.5.2. Taking into account the costs.....	117
IV.5.3. Optimization Heuristic.....	117
IV.5.4. Specifications on the input data.....	118
IV.5.5. Cost associated to failure rates .....	118
<b>IV.6. Principles of allowance algorithms</b> .....	118
IV.6.1. Algorithm of associated allowance for reliability and redundancy.....	118
IV.6.2. Availability allowance .....	123
IV.6.3. The heuristic Validation .....	123
IV.6.4. Calculation of all possible solutions on an example .....	124
IV.6.5. Interpretations.....	125
<b>IV.7. The disallowance procedure</b> .....	126
<b>V. General conclusion</b> .....	130
<b>Appendix</b>	
<b>References</b>	

**CHAPTER I:**

**DIFFERENT TECHNIQUES OF SYSTEM  
DEPENDABILITY.**

## I.1 INTRODUCTION

A major application area for the probability and numerical techniques in characterizing the behavior of complex systems. While system performance has received a lot of attention in the past, increasingly system dependability is gaining importance. The proliferation of computer and computer-based communication and control systems has contributed to this in no small measure. This chapter summarizes the techniques, tools and recent developments in the field of system dependability.

*Laprie [48]* defines system dependability as the ability of a system or a product to deliver its intended level of service to its users, especially in the light of failures or other incidents that affect its level of service. Dependability is a term that takes in consideration the system reliability, availability, safety and maintainability. Depending on the application environment, one or more of these characteristics are appropriate reflection of the system behavior. For example, in a power system, the electrical power that the system is able to deliver its intended level of service to the customers at any instant is important, and then system availability is an important measure. In an aircraft flight-control system, system failures may be catastrophic. Thus, in this application, the ability of the system to continue delivering its service without a catastrophic failure (system reliability) is of greater importance. *Heimann et al [35]* list three different reasons for using dependability in system evaluation:

1. Dependability allows comparisons between cost and performance. Along with cost and performance, dependability is the third critical criterion based system related decisions will be made.
2. Dependability study allows determining the adequate maintenance strategy.
3. Dependability can take into account safety and risk issues. Dependability evaluation enables us to identify unsafe situations and the inherent risks involved in the system being unable to deliver its intended level of service.

Traditionally, reliability block diagrams and fault trees were commonly used for system reliability and availability analysis [58]. These model types allow a concise description of

the system under study and can be evaluated efficiently, but they cannot easily represent dependencies occurring in real systems [42]. Markov models, on the other hand, are capable of capturing various kinds of dependencies that occur in reliability/availability models [52, 23, and 43].

In this chapter we give an overview of dependability evaluation techniques and tools. We start by defining the various measures of dependability in Section 2. Then we introduce the different modeling techniques commonly used in representing system dependability behavior. Thereafter, the computational methods used for evaluating the dependability measures from the dependability models have been reviewed in Section 3. Finally, some important issues encountered in dependability modeling have been mentioned in Section 4.

## **I.2. DEFINITIONS AND NOTATIONS**

### **I.2.1. Mathematical Element of the RAMS [14]**

The different notions that follow are primordial in dependability study of industrial complex systems:

#### **1. Random variables:**

A random variable, in probability lectures, are related to the distribution function, that can take all values for a particular interval (life-time for example).

#### **2. Distribution function:**

A Distribution function of a random variable  $X$  defines the probability that the random variable  $X$  is smaller or equal to a fixed value  $X$  is:

$$F(t) = P(X \leq t) \quad (1.1)$$

#### **3. The probability density**

The probability density ' $f$ ' represents the probability to find the random variable  $X$  exists between  $t$  and  $t + dt$  it is equal to the derivative of  $F$  is:

$$f(t) = dF(t)/dt \quad (1.2)$$

### **I.2.2 Measures of Dependability**

Dependability measures can take the system reliability; and availability as well as maintainability and safety. Depending on the specific situation under investigation, one

or more of these measures may be appropriate. System reliability measures are typically relevant in situations where the systems are highly sensitive to occurrences of system failures or interruptions. For example, in aircraft flight control and spacecraft mission control, the system is expected to provide uninterrupted service. System availability measures are more suitable for systems where short interruptions can be tolerated. Most of the commercial applications of computer systems, for example airline reservations systems, automated banking systems, power system stations fall into this category (electric power must be available for the customer whenever he wants). Other measures may be defined for specific systems, which better reflect the abilities of the systems under consideration. *Heimann and al.* [35] provide a good discussion on this topic.

### **I.2.2 .1Reliability Measures:**

System reliability is one of the most commonly used measures for evaluating critical systems missions.

**Definition 2.1:** The reliability  $R$  is the ability of a system  $S$  to accomplish a required function, under a given condition within the interval  $[0, t [$

$$R(t) = P\{S \text{ does not fail within } [0, t [ \};$$

So that:

The reliability  $R(t)$  of a system at time  $t$  is the probability that the system failure, has not occurred in the interval  $[0, t)$ . If  $X$  is a random variable, that represents the time to occurrence of system failure, then  $R(t) = P(X > t)$ .

We can compute the system unreliability as  $1-R(t)$ , a more appropriate measure for highly-reliable systems given the finite precision of numbers in digital computers. Another important and often used measure of interest is the *Mean Time To Failure* of the system.

**Definition 2.2** The **Mean Time To Failure** (*MTTF*) of a system is the expected time until the occurrence of the (first) system failure. If  $X$  is a random variable that represents the time to occurrence of system failure, then  $MTTF = E[X]$ .

For a given system reliability  $R(t)$ , *MTTF* can be computed as follows,

$$MTTF = \int_0^{\infty} R(t) dt \quad (1.3)$$

**Definition 2.3** The failure rate  $\lambda(t)$ :

The failure rate  $\lambda(t)$  is the failure probability between  $t$  and  $t+\Delta t$  of a component, knowing that it's survived until  $t$ . The function  $\lambda(t)$  is related to distribution functions and probability density by the relation ,

$$\lambda(t) = \frac{f(t)}{1 - F(t)} \quad (1.4)$$

The failure rate is an inverse rate of time (hour); the following mathematical expression may be used:

$$\lambda(t) = \lim_{\Delta t \rightarrow 0} \left( \frac{1}{\Delta t} \cdot \frac{R(t) - R(t + \Delta t)}{R(t)} \right)$$

(1.5)

Then,

$$\lambda(t) = \frac{-1}{R(t)} \cdot \frac{dR(t)}{dt}$$

(1.6)

**The combination of (1.3) and (1.6) gives:**

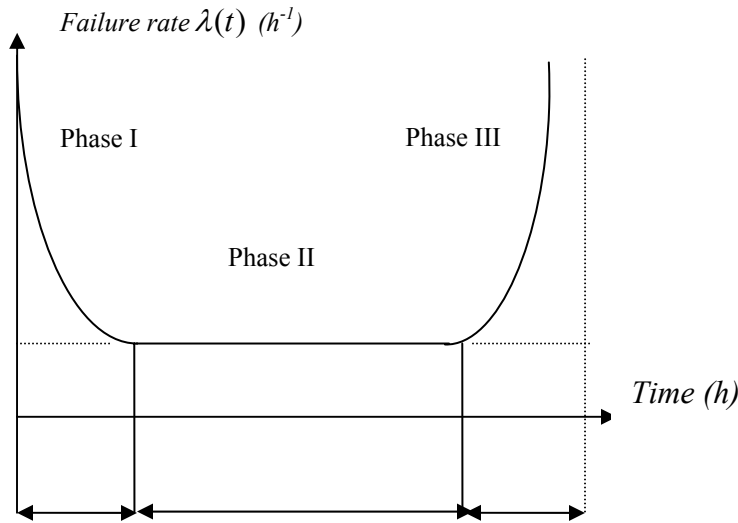
$$MTTF = \frac{1}{\lambda(t)}$$

(1.7)

The curve, so-called bathtub graph (figure 2-2) gives the evolution of the failure rate as function of time that can be divided into 3 phases of system behavior:

- Phase I: Youth period phase (Precocious failure).
- Phase II: Constant Failure Rate phase (useful life).
- Phase III: Ageing period.





**Figure I.1 Bathtub curve [9]**

### I.2.2 .2Availability Measures

System availability measures are especially relevant in repairable systems, where brief interruptions in service are tolerated, then:

The availability  $A(t)$  is the probability so that the system  $S$  does not fail at a given instant  $t$ :

$A(t) = P\{S \text{ does not fail at the instant } t\}$ ; Depending on the time interest, system availability measures can be expressed in three different forms.

**Definition 2.4** The **instantaneous availability**  $A(t)$  of a system at time  $t$  is the probability that the system is operating correctly at time  $t$ . Like the reliability measure, in some applications it is better to compute the system unavailability:

$$U(t) = 1 - A(t).$$

**Definition 2.5** The **interval availability**  $A(t)$  of a system during the interval  $[0, t]$  is the expected proportion of time within the interval where the system is operating correctly, it can be noted that,

$$\bar{A}(t) = \frac{1}{t} \int_0^t A(x) dx \quad (1.8)$$

**Definition 2.6 The steady-state availability**  $A_{ss}$  represents the long-term probability that the system is available.

$$A_{ss} = \lim_{t \rightarrow \infty} A(t) \quad (1.9)$$

The steady-state unavailability of the system is given by  $U_{ss} = 1 - A_{ss}$ .

**Definition 2.7 The limiting interval availability**  $\bar{A}$  is the expected fraction of time when the system is operating:

$$\bar{A} = \lim_{t \rightarrow \infty} \bar{A}(t) \quad (1.10)$$

If  $\lim_{t \rightarrow \infty} A(t)$  exists, then the steady-state availability and the limiting interval availability are equal [27', 29], i.e.,

$$\bar{A} = \lim_{t \rightarrow \infty} \frac{1}{t} \int_0^t A(x) dx = A_{ss} \quad (1.11)$$

Other possible measures of system availability are [34, 35]: (cumulative) availability distribution, tolerance availability, capacity-oriented availability, tolerance capacity-oriented availability, and degraded-capacity time.

### I.2.2.3 - Maintainability

The Maintainability  $M(t)$  is the ability of a system to be maintained or re-established to the state in which it can accomplish a requisite function,

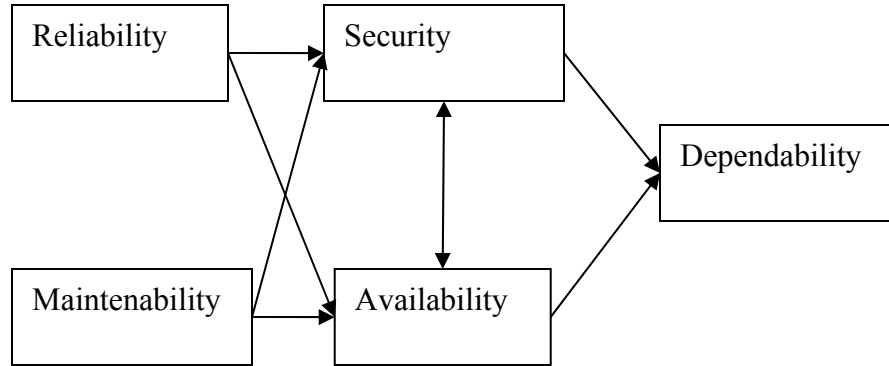
$$M(t) = P \{S \text{ is repaired within } [0, t]\};$$

### I.2.2.4. Security

The security  $S(t)$  is the ability of a system to avoid to make appear, under a given data conditions, a critical or catastrophic events;

$$S(t) = P\{S \text{ without catastrophic failure on } [0, t]\};$$

The four parameters, mentioned above, are interdependent [31] (**figure I.2**):



**Figure I.2 Interdependence among RAMS parameters**

This figure shows that:

- A bad reliability of a system can lead up to a bad availability in case of numerous breakdowns, but little also affect on the security since the occurrence of an accident is often associated with breakdown.
- An insufficient maintainability (in the case of repairable systems) can affect on the availability of a system (increase of the number of breakdowns) as well as on the security (increase of the accident risk)
- A system can be reliable and available without being secure.

### **I. 3. Dependability Model Types**

Several model types are used to represent the dependability behavior of complex systems and obtaining various measures of dependability. These methods can be broadly classified into two different types: (1) non-state space models, and (2) state space models, depending on the nature of their constitutive elements and solution techniques. Non-state space models do not require the values of systems states, while state space modeling techniques demand the collection of variables, which define the state of the system at a given point. Non-state space models allow a concise description of the system under study and can be evaluated efficiently, but they cannot represent system dependencies occurring in real systems [30] unlike state space based methods [62, 52, 58, 17, and 48].

State space models may be deterministic or stochastic in nature. Models are said to be deterministic if their elements are sufficiently specified so that the model behavior is exactly determined. Stochastic models, on the other hand, have probabilistic nature and do not determine numerical values for the variables as the deterministic models do. They

normally determine probabilities and/or moments associated with system state and output variables. The state probabilities are then calculated and, hence, the dependability measures of interest are determined.

Stochastic models are usually the method of choice when modeling dependability of computer systems since phenomena involving significant uncertainties and unpredictable variability (inherent in the system or in its inputs) frequently needs to be represented. Through the probabilistic approach, the uncertainties in the solution of such model can be clearly evidenced.

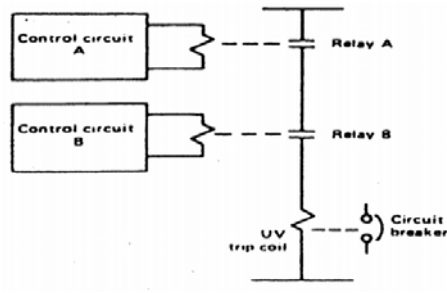
In the practice of reliability engineering, stochastic models are further classified as Markovian or non-Markovian. This distinction is based on the joint distribution of the underlying stochastic process. Reasons for the popularity of Markov models include the ability to capture various dependencies, the equal ease with which steady-state, transient, and cumulative transient measures can be computed, and the extension to Markov reward models useful in performability analysis [62]. A wide range of dependability modeling problems fall in the domain of Markov models (both homogeneous and non-homogeneous). However, some important, aspects of system behavior in stochastic models cannot be easily captured through a Markov model. The common characteristic of these problems share is that, the *Markov property* [62] is not valid (if valid at all) at all time instants. This category of problems is jointly referred as non-Markovian models.

Non-Markovian models can be analyzed introducing supplementary variables [62] or phase-type expansions [17, 61] in the state space of the model. In some circumstances, however, it is possible to analyze non-Markovian models by considering some appropriately chosen embedded epochs in the process evolution where the Markov property applies [14, 41]. Several well-known classes of stochastic processes such as regenerative, semi-Markov and Markov regenerative processes are based on this concept. Unlike the supplementary variable and phase-type expansion approaches, embedding techniques do not extend the cardinality of the state space of the model, and this is their utmost advantage over the other non-Markovian techniques mentioned.

Several model types that are commonly employed in dependability evaluation. Can be better illustrated through the following example:

**Example 1** Consider a circuit breaker system consisting of two control circuits connected together through two relays as shown in Figure I.3.

Each relay has its own local control circuit and supports the data needs of the circuit breaker on the system. The trip/close signal of each relay is received from its own control circuit so that the breaker can continue to operate even if one of the relays has failed.



**Figure I.3 The circuit breaker system**

The circuit breaker is a critical component in maintaining the system. Thus the system operates as long as one of the relays operates. The failure of one of the control circuits, which serve as the access points to the network, is ignored.

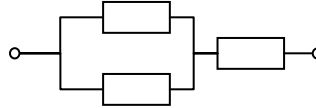
### *1. 3.1 Non State Space Models*

**I.3.1.1 Reliability Block Diagrams (RBDs):** In a reliability block diagram model, the components/subsystems are represented as blocks. The interconnections among the blocks reflect the operational dependency of the system on its constituent components/subsystems. Those components which are all required to be functioning for the (sub) system to be operational are connected in series. Component blocks are connected in parallel if the failure of all of them will result in the failure of the (sub) system. In this model-type the failures of the individual components are assumed to be independent, which means the failure of a component: will not, influence on the failure of any other component. RBDs are viewed *as* the probability of success approach to systems modeling [58].

In RBDs [43], can use a  $k/n$  structure where the block with  $n$  components is operational if at least  $k$  of its components are operational. Series and parallel block connections

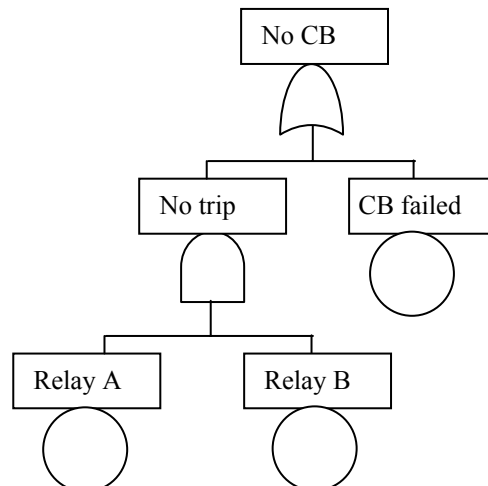
represent special cases of  $k/n$  blocks with  $k = n$  and  $k = 1$ , respectively. Other researchers have also considered RBDs with repeated blocks [12].

The RBD model for the circuit breaker system of Example 1 is shown in Figure I.4.



**Figure I.4 The RBD for circuit breaker system**

**I. 3.1.2 Fault Trees (FTs):** Fault trees, unlike RBDs, represent the probability of failure approach to systems modeling [18]. Fault trees use Boolean gates (e.g., AND and OR gates) to represent the operational dependency of the system on its components. Components are represented as nodes in the tree, which form inputs to the gates. When the component fails, the corresponding input to a gate becomes TRUE. If any input to an OR gate becomes TRUE, then its output also becomes TRUE. The inputs to an OR gate are those components which are all required to be functioning for the (sub) system to operate. The inputs to an AND gate, on the other hand, are those components all of which should fail for the (sub) system to fail. Whenever the output of the topmost gate becomes TRUE, then the system is considered failed. The fault-tree corresponding to the circuit breaker system of Example 1 is shown in Figure I.5.



### **Figure I.5 Fault tree for the breaker system**

Several extensions to FTs have been considered including the use of NOT, XOR, Priority AND, k/n gates [31]. Another extension considered is fault trees with repeated events (FTREs). In this case different gates are allowed to share inputs.

## **I. 3.2 State Space Models**

One major drawback of the non state space methods is that these methods assume stochastic independence between system components. Many intricate system dependencies that arise in modern complex systems cannot be adequately represented by these methods. We are then forced to use state space based methods like continuous time Markov chains, which can handle many of these dependencies. In a later subsection, we will investigate on various kinds of system dependencies that can be represented using state space models.

**Example 3** We introduce repairs in our circuit breaker system and suppose that the circuit breaker has repair priority over the relays. Furthermore, whenever the system is broken down, no further failures can take place. Hence, when the circuit breaker is broken down, the relays cannot fail. Similarly when both the relays are broken down, the circuit breaker does not fail.

Here we have introduced failure and repair dependencies among the components of the system. None of the non state space models can handle these interdependencies.

**I. 3.2.1 Continuous Time Markov Chains (CTMCs):** The continuous time Markov chains (CTMCs) can be used in the modeling of system dependability behavior. The state description of a CTMC can be used to explicitly keep track of the state of the components and subsystems comprising the system. Transitions among the states represent failure/repair events that occur in the system and result in a state change. In using the (homogeneous) CTMC, we are implicitly assuming that the times to occurrence of events (failures, repairs) in the system are all exponentially distributed. This assumption can be relaxed in situations where the distributions can be represented by phase-type

approximations [52], while still using the CTMCs. Alternatively, non-homogeneous CTMC can be used to allow globally time dependent failure rates [52].

Let  $\{Z(t), t \geq 0\}$  represent a homogeneous finite-state continuous time Markov chain (CTMC) with state space  $\Omega$ . Without loss of generality, we will assume that  $\Omega = \{1, 2, \dots, n\}$ : see below. The infinitesimal generator matrix is given by  $Q = [q_{ij}]$  where  $q_{ij}, (i \neq j)$  represents the transition rate from state  $i$  to state  $j$ , and the diagonal elements are  $q_{ii} = -q_i = -\sum_{j \neq i} q_{ij}$ . Further, let

$q = \max_i |q_{ij}|$  and let  $\eta$  be the number of non-zero entries in  $Q$ .

Let the failure & repair for the circuit breaker components are considered as shown in the table. I.1 .

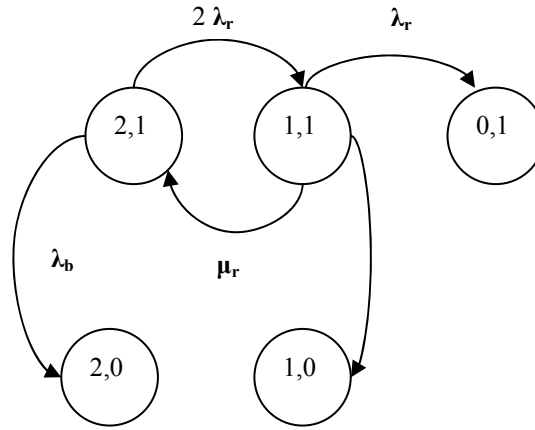
<i>Rates</i>		
<i>Failure</i>	<i>Repair</i>	<i>Meaning</i>
$\lambda_r$	$\mu_r$	Constant rates of relays
$\lambda_b$	$\mu_b$	Constant rates of the breaker

**Table. I.1 Data for circuit breaker system**

**Example 4** We can modify Example 1 further by assuming that the circuit breaker system does cover whenever both relays fail, or whenever the breaker fails. When this situation occurs, no further repairs are carried out on the system,

We obtain the CTMC corresponding to Example 4 by turning the states (0,1), (1,0). and (2,0) of the CTMC into absorbing states. The corresponding Markov chain is shown in Figure I.6.

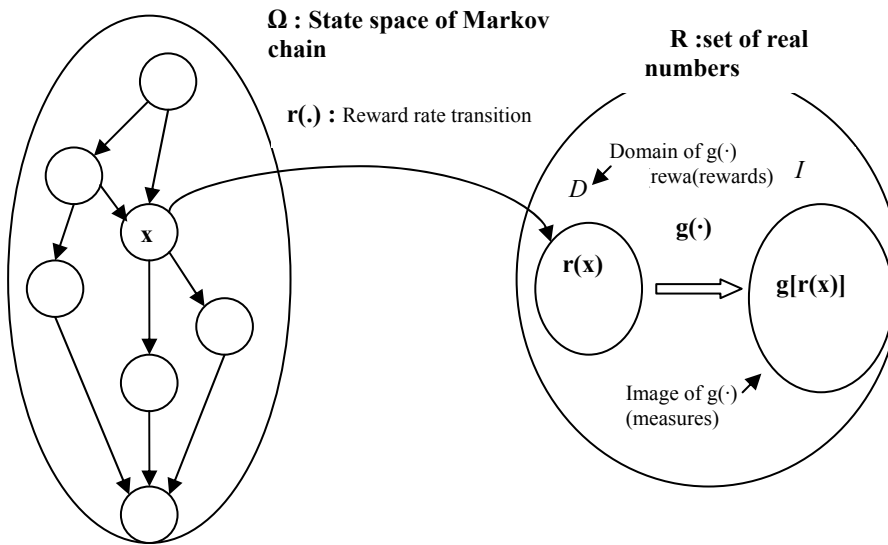




**Figure I.6 CTMC with absorbing state**

### I. 3.2 .2Markov Reward Models (MRMs)

Markov reward models are extensions to Markov chains obtained by assigning transformation functions  $r[X(\cdot)]$  (called reward rate functions) to map elements from the state space  $\Omega$  of a Markov chain into real numbers<sup>1</sup> (see Figure 1.7). If the MRM spends  $\tau_i$  time units in state  $i$  during the interval  $[0, t]$  then a reward  $\tau_i r_i$  is accumulated up to time  $t$ . Similar to the underlying Markov chains, MRMs form a special case of discrete-state stochastic processes in which the current state completely captures the past history pertaining to the system evolution.



**Figure I.7 Reward rate function concept.**

<sup>1</sup> It is also possible to associate reward rates with the transitions of a Markov chain [52]

The analysis of a generic MRM starts by finding the state probability vector functions of the underlying Markov chain and the associated reward rates. The analysis proceeds by combining the mapped reward rates, weighted by the corresponding state probabilities, according to a function  $g(\cdot)$  (That we call *measure function* in this chapter) defined based on a particular measure (as illustrated in Figure I.7). Possible measures of interest are [17]: the expected reward rate (instantaneous, accumulated and steady-state), the expected accumulated reward until absorption (for a Markov chain with absorbing states), and distribution of reward measures (instantaneous, accumulated, until absorption, and over a finite horizon).

With the combination of ingenious reward rate functions and measure functions, several interesting measures in performance, dependability, and performability can be determined as exemplified in [31, 38, 43]. For instance, availability analysis of a system can be carried out using MRMs by simply assigning reward rate 1 to all functional states of the system and reward rate 0 to all states in which the system is considered failed. Given this reward assignment, the steady-state availability  $A_{ss}$  is the expected reward rate in steady-state:

$$A_{ss} = \sum_{i \in \Omega} r_i \pi_i \quad (1.12)$$

With the same reward assignment, the instantaneous and interval availability can also be computed. The instantaneous availability  $A(t)$  is the expected instantaneous reward rate at time  $t$ :

$$A(t) = \sum_{i \in \Omega} r_i P_i(t) \quad (1.13)$$

The interval availability  $\bar{A}(t)$  is the expected time-averaged accumulated reward over the interval  $[0, t]$ :

$$\bar{A}(t) = \frac{1}{t} \sum_{i \in \Omega} r_i \int_0^t P_i(x) dx \quad (1.14)$$

Distinct reward rate functions associated with a given Markov chain produce distinct MRMs. Another property is that the definition of reward rates is orthogonal to the analysis type that is used. Thus, for instance, with the same reward definition we can compute the steady-state availability, as well as instantaneous availability, and interval availability in a dependability model.

### **I. 3.2.3 Non- Markovian Models**

The modeling framework presented so far allows the solution of stochastic problems enjoying the Markov property: the probability of any particular future behavior of the process, when its current state is known exactly, is not altered by additional knowledge concerning his past behavior [52]. If the past history of the process is completely summarized in the current state and is independent of the current time, then (THE process is said to be time homogeneous). Otherwise, the exact characterization of the present state needs the associated time information, and the process is said to be non homogenous. A wide range of real problems fall in the class of Markov models (both homogeneous and non-homogeneous). However, some important aspects of system behavior in a dependability model cannot be easily captured in a Markov model. The common characteristic these problems share is that the Markov property is not valid (if valid at all) at all time instants. This category of problems is jointly referred to as non-Markovian models and can be analyzed using several approaches. Among them we summarize three of the major options: (i) associating supplementary variables to non-exponential random variables: (ii) replacing non-exponential distributions by arrangements of exponential distributions, also called phase-type expansions: and (iii) searching for embedded epochs in the system evolution where the Markov property can be applied.

**I. 3.2.4 Supplementary Variables** This method, originally discussed in [62], allows for the solution of dependability models when the lifetime and or repair distributions of the CB system components are non-exponential. It is the most direct method of solving the modeling problem and is based on the inclusion of sufficient supplementary variables in the specification of the state of the system to make the whole process Markovian. In dependability models, the supplementary variables are the times expended in repairs and ages of network components. The purpose of the added supplementary variables is to

include all necessary information about the history of the stochastic process. The resulting Markov process is in continuous time and has a state space which is multidimensional of mixed type. Partly discrete and partly continuous.

Since, after the inclusion of the supplementary variables, the stochastic process describing the system behavior satisfies the Markov property, it is possible to derive the Chapman- Kolmogorov equations describing the dynamic behavior for such a process. The resultant set of ordinary or partial differential equations can be defined together with boundary conditions and analyzed. Several non-Markovian dependability models solved using the supplementary variables technique has been reported in recent literature [10, 12, 21, 22, 23, 32, 55].

**I. 3.2.5 Phase Type Expansions** The use of phase type distributions dates back to the pioneering work of Erlang on congestion in telephone systems at the beginning of this century [11] (named method of stages}. Although simple, was very effective in dealing with non-exponential distributions and has been considerably generalized since then. The age (repair time) of a component is assumed to consist of a combination of stages; each of which is exponentially distributed. The whole process becomes Markovian provided that the description of the state of the system contains the information as to which stage of the component state duration has been reached. The division into stages is an operational device and may not necessarily have any physical significance, and any distribution with a rational Laplace transform can, in principle, be represented exactly by a phase type expansion.

The major advantage of the phase type expansions is that once a proper stage combination has been found to represent or approximate a distribution, solutions can be obtained for the resulting Markov chain even with fairly complex models [52].

The basic phase type expansion techniques approximate a non-exponential distribution by connecting dummy stages with independent and exponential sojourn time distribution in series or parallel (or combination of both). A process with sequential phases gives rise to hypo exponential or an Erlang distribution, depending upon whether or not the phases have identical parameters. Instead, if a process consists of alternate phases (parallel connection) then the overall distribution is hypo exponential. The basic instrument when selecting one of these distributions to represent a non-exponential interval is given by the

coefficient of variation. The coefficient of variation,  $C_x$ , of a random variable is a measure of deviation from the exponential distribution and is given by

$$C_x = \frac{\sigma_x}{E[X]}$$

Where  $\sigma_x$  is the standard deviation of the random variable and  $E[X]$  is its expectation.

This coefficient varies as follows according to the selected distribution as shown in table:

$C_x$	Distribution
>1	Hyperexponential
1	Exponential
<1	Hypoexponential Erlang
0	Deterministic

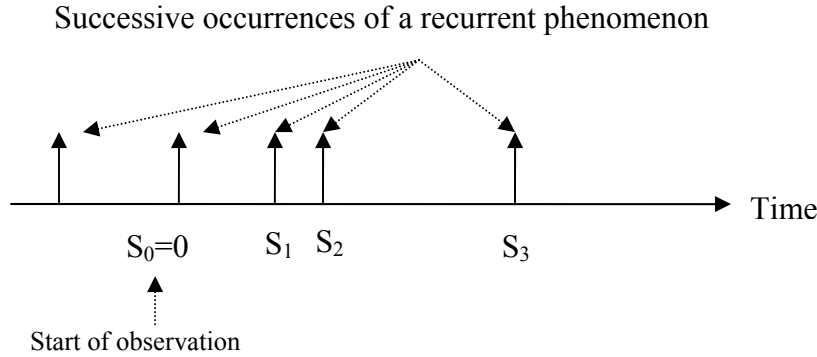
Important generalizations of the basic stage devices are the Coxian distributions [62], Phase Type [14], and Generalized Hyperexponential [6]. An alternative representation of the Coxian distribution with computational advantages is the exponential polynomial or exponential form [17].

**I. 3.2.6 Markov Renewal Theory** A set of techniques that proved very powerful for the solution of non-Markovian models of dependability is based on concepts grouped under the umbrella of Markov renewal theory [14, 16], a collective name that includes Markov renewal sequences (MRSs), and two other important classes of stochastic processes with embedded MRSs, named semi-Markov processes (SMPs) and Markov regenerative processes (MRGPs). Mathematical definitions for these stochastic processes are given now.

Assume the system we are modeling is described by a stochastic process  $\mathbf{Z} = \{Z_t; t \geq 0\}$  taking values in a countable set  $F$ . Suppose we are interested in a single event related with the system (e.g., when system components fail).

Additionally, assume the times between successive occurrences of this type of event are independent and identically distributed (*iid*) random variables. Let  $S_0 < S_1 < S_2 < \dots$  be

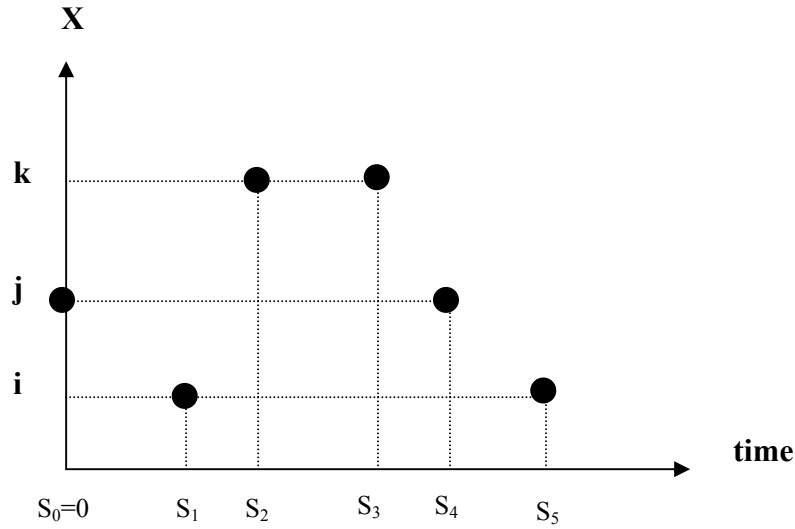
the time instants of successive events to occur (as shown in Figure 1.6). The sequence of non-negative *iid* random variables,  $\mathbf{S} = \{S_n - S_{n-1}; n \in N = [1, \dots, \infty)\}$  is a renewal process. Otherwise, if we do not start observing the system at the exact moment an event has occurred (i.e.  $S \neq 0$ ) the stochastic process  $\mathbf{S}$  is a delayed renewal process.



**Figure I.8 A sample realization of a renewal process.**

However, suppose instead of a single event, we observe that certain transitions between identifiable system states  $X_n$  of a subset  $\varepsilon$  of  $F$ ,  $\varepsilon \subseteq F$ , also resemble the behavior just described, when considered in isolation. Successive Times  $S_n$  at which a fixed state  $A_x$ , is entered form a (possibly delayed) renewal process. We are supposing  $X_n$  is the system state at time  $S_n$ . In the sample process realization depicted in Figure I.8 we see that the sequence of time instants  $\{S_0, S_1, \dots\}$  forms a renewal process, while  $\{S_1, S_2, \dots\}$  and  $\{S_2, S_3, \dots\}$  form delayed renewal processes.

Additionally, when studying the system evolution we observe that at these particular times the stochastic process  $\mathbf{Z}$  exhibits the Markov property, i.e., at any given moment  $S_n$ ,  $n \in N$  we can forget the past history of the process. The future evolution of the process depends only on the current state at these embedded time points.



**Figure I.9 A set of renewal process progressing concurrently.**

In this scenario we are dealing with a countable collection of renewal processes progressing simultaneously such that successive state visited form an embedded discrete-time Markov chain (DTMC)  $\{S_n ; n \in N\}$  with state space  $\varepsilon$ . The superposition of all the identified renewal processes gives the points  $\{S_n ; n \in N\}$ , known as *Markov regeneration epochs* (also called Markov renewal moments)), and together with the states of the embedded Markov chain (EMC) defines a Markov renewal sequence.

**Definition 2.7:** In mathematical terms, the bivariate stochastic process  $(\mathbf{X}, \mathbf{S}) = \{X_n, S_n ; n \in N\}$  is a **Markov renewal sequence** provided that :

$$\Pr\{X_{n+1} = j, S_{n+1} - S_n \leq t \mid X_0, \dots, X_n; S_0, \dots, S_n\} = \Pr\{X_{n+1} = j, S_{n+1} - S_n \leq t \mid X_n\}. \quad (1.16)$$

$\forall n \in N, j \in \varepsilon$ , and  $t \geq 0$ . The random variable  $X_n$  and  $S_n$  are the state being visited and the time, respectively, of the  $n^{\text{th}}$  transition.

Thus  $(\mathbf{X}, \mathbf{S})$  is a special case of bivariate Markov process in which the increments  $S_1 - S_0, S_2 - S_1, \dots$  are all non-negative and are conditionally independent given  $X_0, X_1, \dots$  these increments are called the sojourn times; if  $X_n = j$ , then  $S_{n+1} - S_n$  is called the sojourn time in state  $j$  or the  $n^{\text{th}}$  sojourn time.

We will always assume time-homogeneous MRSa; that is, the conditional transition probabilities  $K_{i,j}$ , where

$$K_{i,j}(t) = \Pr\{X_{n+1} = j, S_{n+1} - S_n \leq t | X_n = i\} \quad (1.17)$$

are independent of  $n$  for any  $i, j \in \mathcal{E}, t \geq 0$ . Therefore, we can always write

$$K_{i,j}(t) = \Pr\{X_1 = j, S_1 \leq t | X_n = i\} \forall i, j \in \mathcal{E}, t \geq 0. \quad (1.18)$$

The matrix of transition probabilities  $\mathbf{K}(t) = [K_{i,j}(t)]$  is called the kernel of the MRS. There are no restrictions regarding the structure of the EMC on a MRS, Form instance, there is no imposition that  $\{X_n, n \in N\}$  should be irreducible. Therefore, we can start at time  $S_0$  in a state of  $\mathcal{E}$  that will not be reached again at any other Markov regeneration epoch in the future evolution of the process.

**I. 3.2.7 Semi-Markov process:** It is a generalization of both types of Markov chains (i.e. continuous and discrete time) which permits arbitrary sojourn time distribution functions, possibly depending both on the current state and on the state to be visited next.

Given an **MRS**  $(\mathbf{X}, \mathbf{S})$  with state space  $\mathcal{E}$  and kernel  $\mathbf{K}(t)$ , we can introduce the counting process

$$N(t) = \sup\{n : S_n \leq t\}, t \geq 0. \quad (1.19)$$

To count the number of Markov regeneration epochs up to time (but not considering the one at zero. Using the counting process just defined, we introduce the definition of SMP.

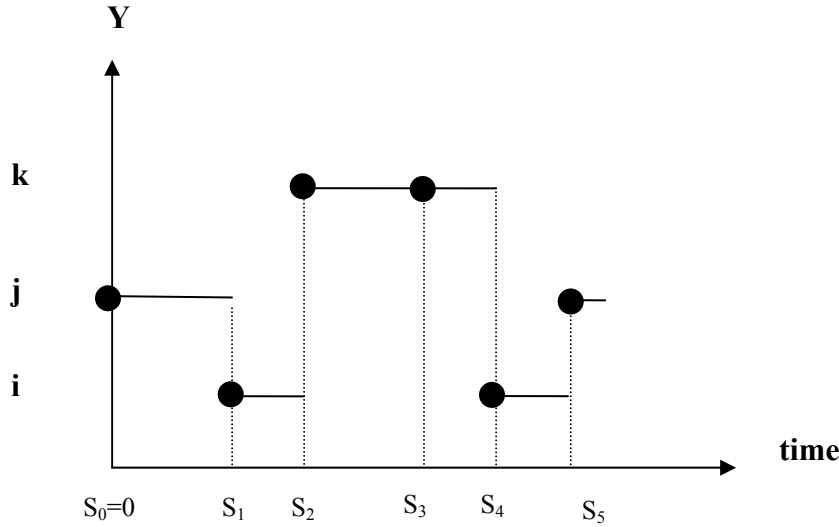
**Definition 2.8** A semi-Markov process is a process  $\mathbf{Y} = \{Y_t; t \geq 0\}$  defined By

$$Y_t = X_{N(t)} = X_n, \quad \text{if } S_n \leq t \leq S_{n+1} \quad \text{For all } t \geq 0. \quad (1.20)$$

An SMP (for a sample realization see Figure 1.8) is a stochastic process which moves from one state to another within a countable number of states with the successive states visited forming a discrete-time Markov chain, and that the time required for each



successive move is a random variable whose distribution function may depend on the two states between which the move is being made. From the SMP definition it should be observed that the process only changes state (possibly back to the same state as shown in Figure I.10) at the Markov regeneration epochs  $S_n$



**Figure I.10 A sample realization of a semi-Markov process**

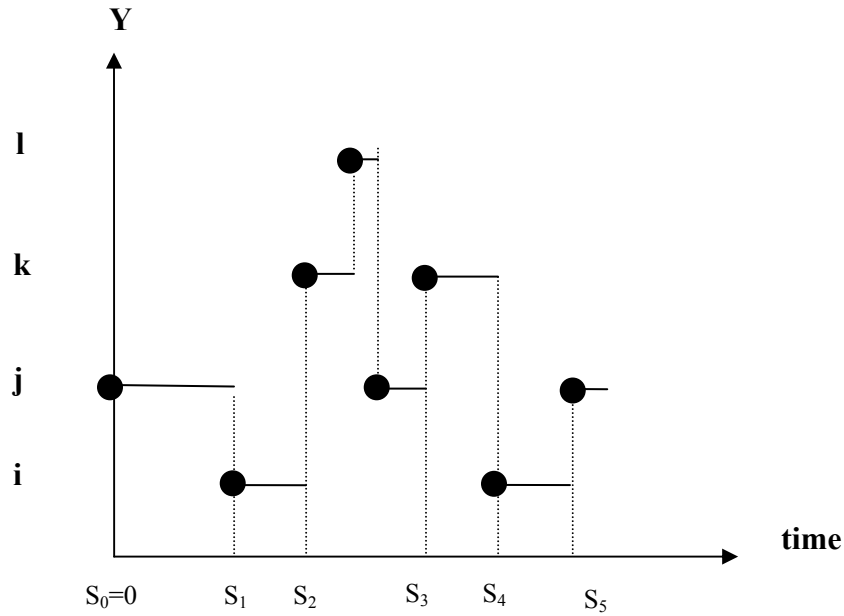
The name "semi-Markov" comes from the somewhat limited Markov property which  $Y$  has: the future of  $Y$  is independent of its past provided the present is a Markov regeneration epoch. Note that since we consider  $S_0 = 0$ , then the initial condition  $Y_0 = i$  always means that the SMP has just entered state  $i$  at the time origin.

A stochastic process  $Z = \{Z_t; t \geq 0\}$  with state space  $T$  is called regenerative if there exist time points at which the process probabilistically restarts itself. Such random times when the further of  $Z$  becomes a probabilistic replica of itself are named times of regeneration for  $Z$ . This concept may be weakened by letting the future after a time of regeneration depend also on the state of an MRS at that time. We then say that  $Z$  is an MRGP.

**Definition 2.9 Markov regenerative processes** are stochastic processes  $\{Z_t, t \geq 0\}$  that exhibit  $t$  embedded MRSs  $(X, S)$  with the additional property that all conditional finite distributions of  $\{Z_{S_n+t} > 0\}$  given  $\{Z_u: 0 < u < S_n, X_n = i, i \in \mathcal{E}\}$  are the same as those of  $\{Z_t, t > 0\}$  given  $X_0 = i$ . As a special case, the definition implies that.

$$\Pr \{Z_{S_n+t} = j \mid Z_u, 0 \leq u \leq S_n = i\} = \Pr \{Z_t = j \mid X_0 = i\}, \quad \forall i \in \mathcal{E} \quad (1.21)$$

This means that the MRGP  $\{Z_t; t \geq 0\}$  does not have the Markov property in general, but there is a sequence of embedded time points  $(S_0, S_1, \dots, S_n, \dots)$  such that the states  $(X_0, X_1, \dots, X_n, \dots)$  respectively of the process at these points satisfy the Markov property. It also implies that the future of the process  $Z$  from  $t = S_n$  onwards depends on the past  $\{Z_u, 0 \leq u \leq S_n\}$  only through  $X_n$ . Recall that in the regenerative process this future from  $S_n$  onwards was completely independent of the past.



**Figure I.11 A sample realization of a Markov regenerative process.**

In contrast to SMPs, state changes (possibly to states outside  $\varepsilon$ ) are allowed between two consecutive Markov regeneration epochs (see Figure I.11) in MRGPs, but this change does not imply regeneration. It is possible for the system to return to states in  $\varepsilon$  without these moments constituting Markov regeneration epochs. For example, suppose we start observing the system when it has just entered a state  $j$ , as shown in Figure I.11. At that particular instant the Markov property is applicable since there is no past history of the process, but because of system characteristics, we know this property will no longer be valid for that state after the first state transition (not necessarily to a state in  $\varepsilon$ ). This situation could be understood if we consider that although state  $j$  being part of the EMC  $X$ , it does not communicate with other states of  $X$  and, hence, the Markov chain  $X$  is

reducible. Although others states of  $X$  are (possibly) accessible from state  $i$ , this state cannot be accessed from any other state of  $X$ .

The stochastic process between the consecutive Markov regeneration epochs usually referred to as subordinated process, can be any continuous-time discrete state stochastic process over the same probability space. Recently published examples considered subordinated homogeneous CTMCs [13, 29], non-homogeneous CTMCs [5], SMPs [14,18]. MRGPs [6,1], or a more general stochastic reward process.

## 1.4 COMPUTATIONAL METHODS

### 1.4.1 Non state space models

#### 1.4.1.1 Reliability Block Diagrams

To compute the reliability of a system represented as a reliability block diagram, we normally break it down into its serial and parallel parts and compute the reliabilities of these parts and then compose the solution to obtain the reliability of the whole system. Given a system consisting of  $N$  components with  $F_i(t)$  representing the failure time distribution of component  $i$ , we know that  $F(t)$ , the distribution of the failure time of a subsystem with  $N$  components is given by [60]:

$$F(t) = \begin{cases} 1 - \prod_{i=1}^N (1 - F_i(t)) & \text{for a series structure,} \\ \prod_{i=1}^N F_i(t) & \text{for a parallel structure.} \end{cases}$$

(1.22)

In the RBD model of the circuit breaker of **example1** suppose  $R_r$ , and  $R_b(t)$  represent the individual reliabilities of the relays and the breaker respectively, then the overall system reliability  $R(t)$  is given by,

$$R(t) = [1 - (1 - R_r(t))^2] R_b(t)$$

(1.23)

Note that this expression is independent of the distribution associated with the time to failure of each component. In the present example, we assumed that the times to failure of each component are exponentially distributed. Hence, the reliability is given by,

$$R(t) = [1 - (1 - e^{-\lambda_r t})^2] e^{-\lambda_b t}$$

(1.24)

The system mean time to failure (MTTF) is given by:

$$MTTF = \int_0^{\infty} R(t)dt = \int_0^{\infty} (2e^{-(\lambda_r + \lambda_b)t} - e^{-(2\lambda_r + \lambda_b)t})dt = \frac{2}{\lambda_r + \lambda_b} - \frac{1}{2\lambda_r + \lambda_b} \quad (1.25)$$

We can also use the reliability block diagrams to compute the system unavailability if we assume that the failure and repair time distributions are all independent. This situation occurs when the system has enough repair resources to repair all the failed components simultaneously. Given the component instantaneous unavailability  $U_i(t)$ , the subsystem unavailability is computed as,

$$U(t) = \begin{cases} 1 - \prod_{i=1}^N (1 - U_i(t)) & \text{for a series structure,} \\ \prod_{i=1}^N U_i(t) & \text{for a parallel structure.} \end{cases}$$

(1.26)

The same formula can be extended to the steady-state unavailability.

For the circuit breaker system of Example 1 suppose we further assume that failed components can be repaired. The system unavailability  $U(t)$  is given by,

$$U(t) = 1 - (1 - U_b(t)) \cdot (1 - U_r^2(t)).$$

(1.27)

The instantaneous system availability  $A(t) = s$  then,

$$A(t) = [1 - (1 - A_r(t))^2] \cdot A_b(t).$$

(1.28)

Let the time to repair a relay and the time to repair the breaker be exponentially distributed with the parameters  $\mu_r$  and  $\mu_b$  respectively. Hence, the instantaneous availability is given by:

$$A(t) = \left\{ 1 - \left[ \frac{\lambda_r}{\lambda_r + \mu_r} \cdot (1 - e^{-(\lambda_r + \mu_r)t}) \right]^2 \right\} \cdot \left( \frac{\mu_b}{\lambda_b + \mu_b} + \frac{\lambda_b}{\lambda_b + \mu_b} e^{-(\lambda_b + \mu_b)t} \right)$$

(1.29)

### 1.4.1.2 Fault Trees

Analysis of a fault tree is similar to the reliability block diagram analysis. Given the failure time distributions of component  $i$ ,  $F_i(t)$ ; the failure time distribution  $F_G(t)$  for a gate with  $n$  inputs is computed as [17]:

$$F_G(t) = \begin{cases} \prod_{i=1}^n F_i(t) & \text{And gate} \\ 1 - \prod_{i=1}^n (1 - F_i(t)) & \text{Or gate} \end{cases} \quad (1.30)$$

For the circuit breaker system of Example 1, the reliability expression obtained from the fault-tree will also be the same as in Equation (1.23). Even in case of the fault-trees, the expression is independent of the distribution associated with the time to failure of the component-

If we consider a  $k/n$  gate, where the output, becomes 1 if  $k$  of the  $n$  components fail, then the corresponding distribution of failure time for the gate is given by:

$$F_G(t) = \begin{cases} \sum_{i=k}^n \binom{n}{i} F(t)^i (1 - F(t))^{n-i} \\ \sum_{|J| \geq k} \left( \prod_{j \in J} F_j(t) \right) \cdot \left( \prod_{j \notin J} (1 - F_j(t)) \right) \end{cases} \quad (1.31)$$

For the identically distributed and non-identically distributed inputs respectively. If we use fault trees with repeated components, then one of the approaches we can employ in solving the model is the factoring or decomposition method [17].

## 1.4.2 State space models

### 1.4.2.1 Continuous Time Markov Chains

**1.4.2.1.1 Instantaneous Transient Analysis** Let  $P_i(t) = \Pr\{Z(t) = i\}$  be the unconditional probability of the CTMC being in state  $i$  at time  $t$ . Then the row vector  $P(t) = [P_1(t), P_2(t), \dots, P_n(t)]$  represents the transient state probability vector of the CTMC. The behavior of the CTMC can be described by the following Kolmogorov differential equation:

$$\frac{d}{dt}P(t) = P(t)Q(t), \quad \text{Given } P(0), \quad (1.32)$$

Where  $P(0)$  represents the initial probability vector (at time  $t=0$ ) of the CTMC.

**1.3.2.1.2 Cumulative Transient Analysis:** Define  $L(t) = \int_0^t P(u)du$ . Then  $L_i(t)$  is The expected total time spent by the CTMC in state  $i$  during the interval  $[0,t]$ .  $L(t)$  satisfies the differential equation:

$$\frac{d}{dt}L(t) = L(t)Q(t) + P(0), \quad L(0)=0, \quad (1.33)$$

This is obtained by integrating equation (1.32).

**1.3.2.1.3 Steady-State Analysis** Let  $\Pi_i$  be the steady-state probability of state  $i$  of the CTMC, and let  $\Pi = \lim_{t \rightarrow \infty} P(t)$  be the steady-state probability vector. We know that in the steady state  $\frac{d}{dt}P(t) = 0$ . By substituting this into Equation (1.32) we can derive the following equation for the steady state probabilities:

$$\pi.Q=0, \quad \sum_{i \in \Omega} \pi_i = 1. \quad (1.34)$$

**1.3.2.1.4 Up-to-Absorption Analysis** Let A represent the set of absorbing states (a state is considered an absorbing state if there are no outgoing transitions from that state, i.e., an absorbing state  $i$  has

$q_{ij} = 0, \forall j, (j \neq i)$ . Let  $B = \Omega - A$  be the set of the transient states in the CTMC. From the matrix Q a new matrix can be constructed by restricting Q to states in B only.  $Q_B$  is of size  $|B| \times |B|$ , where  $|B|$  is the cardinality of the set B.

Let  $z_i = \int_0^\infty P_i(\tau) d\tau, i \in B$ , be the mean time spent by the CTMC in state  $i$  until absorption. The row vector satisfies the following equation;

$\mathbf{z} \cdot \mathbf{Q}_B = -\mathbf{P}_B(0)$ , where  $\mathbf{P}_B(0)$ , is the vector  $\mathbf{P}(0)$  restricted to the states in the set  $B$ . The above equation can be obtained by taking the limit as  $t \rightarrow \infty$  of equation (1.33), with  $\mathbf{z} = \mathbf{L}_B(\infty)$  and noting that  $\frac{d}{dt} L_B(\infty) = 0$ . The mean time to absorption, MTTA, of the

CTMC into an absorbing states is computed as

$$MTTA = \sum_{i \in B} z_i$$

(1.35)

#### 1.4.2.2 Non-Markovian Models

Let  $\mathbf{Z} = \{Z_t, t \in R_+\}$  be a stochastic process with discrete state space  $F$  and embedded MRS

$(\mathbf{X}, \mathbf{S}) = \{X_n, S_n; n \in N\}$  with kernel matrix  $K(t)$ . For such a process we can define a matrix of conditional transition probabilities as:

$$V_{i,j}(t) = \Pr\{Z_t = j | Z_0 = i\}, \forall i \in \mathcal{E}, \forall j \in F, t \geq 0.$$

(1.36)

In many problems involving Markov renewal processes, our primary concern is finding ways to effectively compute  $V_{i,j}(t)$  since several measures of interest (e.g., reliability and availability) are related to the conditional transition probabilities of the stochastic process.

At any instant  $t$ , the conditional transition probabilities  $V_{i,j}(t)$  of  $\mathbf{Z}$  can be written as [14,41]:

$$V_{i,j}(t) = \Pr\{Z_t = j, S_1 > t | Z_0 = i\} + \sum_{k \in \mathcal{E}} \int_0^t dK_{i,k}(u) V_{k,j}(t-u),$$

(1.37)

For all  $\forall i \in \mathcal{E}, \forall j \in F, t \geq 0$ . If we construct a matrix  $\mathbf{E}(t) = [E_{i,j}(t)]$  with

$$E_{i,j}(t) = \Pr\{Z_t = j, S_1 > t | Z_0 = i\}, \forall i \in \mathcal{E}, \forall j \in F, t \geq 0.$$

(1.38)

Then, the set of integral equations  $V_{ij}(t)$  defines a **Markov renewal equation**, and can be expressed in matrix form as

$$\mathbf{V}(t) = \mathbf{E}(t) + \int_0^t d\mathbf{K}(t) \mathbf{V}(t-u),$$

(1.39)

Where the Lebesgue- Stieltjes integral,

$$\int_0^t dK(u) V(t-u) = \int_0^t k(u) V(t-u) du,$$

(1.40)

When  $K(t)$  possesses a density function  $k(t) = \frac{dK(t)}{dt}$  is taken term by term. If the

stochastic process  $\mathbf{Z}$  is a SMP then  $\mathbf{E}(t)$  is a diagonal matrix with elements

$$E_{ij}(t) = I - K_i(t).$$

The Markov renewal equation represents a set of coupled Volterra integral equations of the second kind [60] and can be solved in Time-domain or in Laplace Stieltjes domain. For a discussion of approaches to solve these equations see [14, 53]. References for the application of Markov renewal theory in the solution of performance and reliability/availability models, [5, 29, 32, 34, 45, 47, 48].

To better distinguish the roles of matrices  $\mathbf{E}(t)$  and  $\mathbf{K}(t)$  in the description of the MROP we use the following terminology:

- We call matrix  $\mathbf{E}(t)$  the **local kernel** of the MRGP, since it describes the state probabilities of the process during the interval between successive Markov regeneration epochs. The matrix  $\mathbf{E}(t)$  describes the evolution of the MRGP between two Markov regeneration epochs.
- Since matrix  $\mathbf{K}(t)$  describes the evolution of the process from the Markov regeneration epoch perspective, without describing what happens in between these moments we call it the **global kernel** of the MRGP. The matrix is the joint conditional



probability of the time to the next Markov regeneration and the state right after the regeneration given the state at the current Markov regeneration.

**Conclusion:**

In this chapter, we have briefly reviewed the techniques and tools and recent developments in the field of system dependability evaluation, commonly used measures of system dependability were defined. Several modeling techniques, both non state-space and state-space based, have been then presented. Simple examples illustrating the use of the modeling techniques were also presented. Computational methods for obtaining the dependability measures from the system models have been then reviewed.

**Chapter II**

**Circuit breaker design and flashover failures.**

## **Chapter II                      Circuit breaker design and flashover failures.**

### **II.1 Introduction**

Electricity is directly associated with the quality of life in the modern world. In industrialized countries, access to highly reliable and high quality electrical energy is almost taken into account.

In developing nations, access to electrical power is an important pre-requisite to enhancing the standard of living, being crucial to such essentials as improved hygienic water supply, lighting, heating and enabling access to other critical infrastructure such as telecommunications and development of local industries. In short, within the last century society has become increasingly dependent on electrical energy to sustain and improve its standard of living. Critical aspects of society's dependence on electricity include the cost, the availability and the quality of the electricity supply. In respect of cost, the development of large scale generation coupled through similarly large scale transmission and distribution networks has generally resulted in a low cost of electricity to end users. While large scale power systems are very complex, the careful planning, development and operation of these systems, with security of supply as a main concern, has also resulted in high availability of electricity to most users, particularly within the industrialized nations. Effectively the majority of the population in such countries has access to electricity "on demand".

Quality of the electrical supply is more difficult to define and assess. Power quality may be considered as the measure of consistency with respect to nominal ratings i.e. voltage and frequency. It may also include reference to the level of disturbances to the supply including, but not limited to, harmonics, voltage dips, and voltages surges. A broader definition may well include measurement of the availability of electrical power on demand.

Within the context of electric power quality and availability, industry standard practices for the design and implementation of control and protection systems play an essential role. Power systems, large and small, operate under continual stress; ranging from voltage stresses on insulation, to overload of conductors, to stability within the network. The control and protection of the power system must cope with these various stress factors in order to maintain the desired level of power quality and availability.

Electrical power networks are dynamic systems, driven by the problem of balancing instantaneous demand and production of electricity. The supply and demand balance problem, coupled with management of faults within the system, requires that parts of any power network need to be switched on or off reliably and on-demand. All network switching events will result in some degree of transient response propagating within the system. Controlled, or synchronized, switching of circuit breakers within high voltage power systems has become an increasingly useful method to mitigate the severity of switching transients for a range of specific load cases.

This chapter introduces the high voltage circuit breakers theory and design. It focuses the study and analysis of different protection methods for circuit-breaker flashover failures. Dependability and their control systems to provide various benefits and improvements to the operation of AC power systems.. [49]

## **II.2 Role of circuit breakers in power systems**

An essential factor in achieving the desired level of power quality and availability in any power system is the performance of its circuit switching elements. Circuit breakers are the most critical switching elements in a power system. They are the only means of directly interrupting fault currents on a HV transmission power system. Fast and secure fault interruption is critical not only to protection of other power system components but also to the overall operational stability of a power system.

Circuit breakers are required not only to interrupt faults, but also to switch under system conditions ranging from “no-load” through to full rated asymmetrical fault currents. The stresses placed on a circuit breaker vary considerably in conjunction with the specific nature of the circuit being switched. Interrupting large fault currents at high voltages involves high thermal and dielectric withstand stresses being placed on a circuit breaker. However, even low level currents, especially highly inductive or capacitive currents can also place high (dielectric) stresses on a circuit breaker. [49]

The stresses experienced by HV circuit breakers are not only electrical. The magnitude of the electrical stresses and the demand for fast action response by HV circuit breakers require that they be correspondingly dimensioned to fulfil their rated performance. Consequently HV circuit breakers are large items of equipment, operated at high speeds

with associated high mechanical forces and energies being expended during their operation.

It is thus not a simple task to design and build a circuit breaker that can reliably operate for the range of possible switching cases that may arise on a HV power system. [49]

The major international standards pertaining to the design, testing and rating of HV circuit breakers (IEC 62271-100[36] and ANSI C37.06 [44]).

Despite the onerous demands placed on HV circuit breakers, the technologies applied in modern designs to achieve the desired level of interruption performance and reliability have reached a high level of maturity over the past half a century. HV circuit breakers have been found to generally exhibit a very high level of reliability in service.

Various industry driven surveys have been conducted to measure the level of reliability of HV circuit breakers. Up to the end of 2003, CIGRÉ had conducted two international surveys on HV circuit breaker reliability [28][50][45]. CIGRÉ working group WG A3.06 is presently undertaking a third international survey of a similar nature. Some of the results of these surveys are summarized in Table II.1 below. The results shown in Table II.1 clearly indicate a trend towards higher in-service circuit breaker reliability.

Survey Period	Breaker Interrupter Technologies Surveyed	No. of Surveyed Breakers	Accumulated Breaker Service Time CB-years	Reported Source of Failure	Reported Major Failure Rate per 100 CB-years
1974-1977	All (i.e. air, oil, SF <sub>6</sub> )	20 000	77 892	All sources	1.58
				High voltage components	0.76
				Control & auxiliary circuits	0.30
				Operating mechanism	0.52
				Other	n/a
1988-1991	SF <sub>6</sub> single pressure	18 000	70 708	All sources	0.67
				High voltage components	0.14
				Control & auxiliary circuits	0.19
				Operating mechanism	0.29
				Other	0.05

**Table****CIGRÉ International Surveys on High Voltage Circuit Breaker Reliability****II.1 Summary of Results for Major Failures [45],[46]**

It should be noted that the standards referred to above are not the only IEC or ANSI standards relevant to HV circuit breakers. A range of other related standards are also applicable in each case. The standards indicated here are simply the central and most commonly referred standards pertaining to HV circuit breakers. Further information can be obtained from IEC and ANSI.

While the second CIGRÉ survey was limited to HV circuit breakers with single pressure SF6 interrupters, it is noteworthy that the observed failure rate in the HV component part of the circuit breaker (which of course includes the interrupters) was found to be over five times lower compared to the results in the earlier survey.

A further important observation from the survey results is the relatively high proportion of circuit breaker failures attributed to either the control / auxiliary circuits and the operating mechanism; combining to between 52-72% of the overall failure rates. These potential sources of circuit breaker failure have an important bearing on assessment of any control scheme proposed to augment the behaviour of a circuit breaker and provide an important reminder that power system control and protection is a complex process dependent upon the correct performance of many interrelated subsystems for overall secure operation.

**II.2.1 Controlled switching**

“Controlled switching” is one of several terminologies applied to the principle of co-ordinating the instant of opening or closing of a circuit with a specific target point on an associated voltage or current waveform. Other common terminologies applied include “synchronized switching” and “point-on-wave switching”. [49]

**II.2.2 Controlled switching under steady state conditions**

The fundamental concept of controlled switching is straightforward and most easily explained by illustrating comparisons between “uncontrolled” or “non-synchronized” and a “controlled” or “synchronized” switching operation under stable, steady state conditions. Figures 1.1 and 1.2 below provide an example based on closing a circuit

breaker with respect to phase voltage. For simplicity only one phase is considered. In Figure 1.1 the following sequence of events is shown:

1. A request to close the circuit breaker is issued. In this case occurring at an instant near a negative peak of the phase voltage. Such an operation request could occur at any instant with respect to the phase voltage, indicated by the (A) arrow range (i.e. 0-360 electrical degrees).
2. The request is directly made as a closing command to the circuit breaker, which responds accordingly and within the time indicated by (B) completes its closing operation
3. The circuit breaker has now closed and resulted in the circuit being made at a point near to a positive phase voltage peak. Note that the closing instant will occur equally randomly with respect to voltage waveform as that of the original closing command request; as indicated by the (C) arrow range. [49]

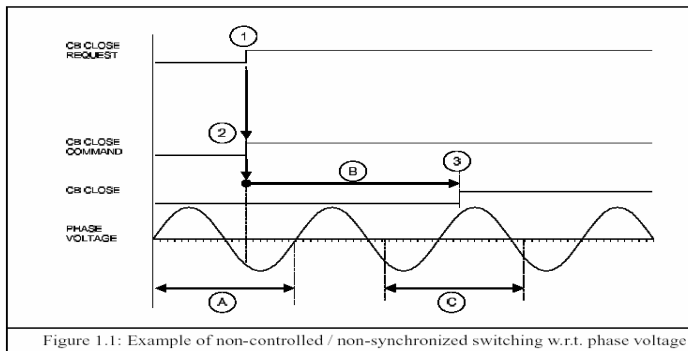


Figure 1.1: Example of non-controlled / non-synchronized switching w.r.t. phase voltage

Figure II.1

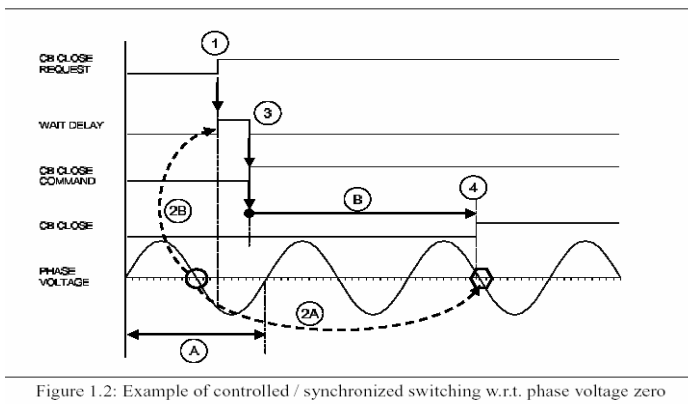


Figure 1.2: Example of controlled / synchronized switching w.r.t. phase voltage zero

Figure II.2

Now assume that it is desired to synchronize the control of the circuit breaker such that contact touch occurs at a phase voltage zero, as illustrated in Figure II.1.

Now the sequence of events proceeds as follows:

1. A request to close the circuit breaker is issued, at the same relative phase voltage angle as for the previous case in Figure II.1. Again such an operation request could occur at any instant with respect to the phase voltage (i.e. 0-360 electrical degrees); as indicated by the (A) arrow range.

2. In this example the goal is to synchronize the closing of the breaker contacts to be as close as possible to a phase voltage zero. A “future” phase voltage zero must therefore be identified as a “target” to which the closing command of the circuit breaker can then be synchronized.

2A. In order to establish the “target” the last previous phase voltage zero is identified.

Knowing the expected circuit breaker closing operation time and the power system frequency, the next viable future phase voltage zero to which the breaker shall be synchronized can be identified. Assuming symmetrical and periodic steady state behaviour of the phase voltage and stability in the circuit breaker operating time, this is a relatively simple task.

2B. With the “target” identified and the breaker closing operation time known, the close command to the circuit breaker can be suitably delayed until a synchronized closing operation can be achieved.

3. Once the required synchronizing delay time has expired the close command is issued to the circuit breaker, which in turn makes the closing operation with the same (or very similar) closing operation time (B) as per the previous case in Figure 1.1

4. The breaker now closes its contacts close to the targeted phase voltage zero and controlled, synchronized operation has been achieved.

## **II.3 Circuit breaker design**

### **II.3.1 operating mechanisms: [46]**

#### **II.3.2 General**

The purpose of the operating mechanism is to provide the driving energy to open and close the contacts of the circuit breaker at the required speeds. This function includes: acceleration, movement, in some cases overcoming the arc-generated back pressure, and deceleration at the end of the stroke. All circuit breaker operating mechanisms use some form of stored energy to accomplish opening. This is usually in the form of charged springs, but in some cases could be in the form of pressurized gas. Many circuit breaker



mechanisms use charged springs for opening energy and some other form of closing energy. Solenoid close circuit breakers receive their energy externally from station batteries or AC station service through a rectifier. Below is a list of some types of generic operating mechanisms:

- Spring open/spring close
- Spring open/solenoid close
- Spring open/hydraulic close

In the hydraulic system either a gas-charged hydraulic accumulator or spring accumulator may be used.

- Spring open/pneumatic close (compressed gas closing energy)
- Pneumatic open/spring close
- Pneumatic and spring open/pneumatic close
- Hydraulic open/hydraulic close

### **II.3.3 Working medium/stored energy.**

In the pneumatic cases, the energy is from compressed gas, and in the hydraulic cases, the energy is from either compressed gas accumulators or charged springs operating against a hydraulic piston.

In spring-operated mechanisms, the closing energy is stored in motor wound springs that are latched in the charged position until the circuit breaker is commanded to close. The opening energy is stored in two places—an opening spring or springs attached to the mechanism jack shaft, and the contact force springs that apply contact force on each interrupter. The mechanism is also latched in the closed position until the circuit breaker is commanded to open.

### **II.3.4 Latches:**

In the case of the spring open mechanisms, which are the large majority, there is a system of latches that holds a breaker in the closed position. Generally, this is like a mechanical amplifier with at least three stages of latching. There is a main latch that holds against the main opening spring. Second, there is the in-between latch, which holds the main latch. Then, finally, there is a trip latch, which holds the intermediate latch. The force restrained by the main latch is usually rather large, being several kilonewtons. The intermediate latch may only have to hold the force of one-tenth of the main. And finally, the trip latch

itself usually has to hold only a small force—tens of hundred Newton's. The purpose of this is to get the latch releasing energy down to a point that is easily managed by electromechanical devices of low energy. Obviously, with this type of setup, the further down the latching amplifier one gets, i.e., towards the low energy end, the more important the cleanliness, proper dimensions, lubrication, and freedom from corrosion become. For example, a very small amount of corrosion on the trip latch can restrain it from operating. On the other end, it takes a much larger amount of corrosion on the main latch.

### **II.3.5 Release valves in pneumatic or hydraulic operators:**

In the pneumatic or hydraulic systems, there generally is a pneumatic/hydraulic amplifier consisting of a main valve that is often hydraulically/pneumatically operated by a pilot valve, which is then operated by the closing or tripping coil. This is, again, to get the electromechanical energy requirement down.

### **II.3.6 Solenoids:**

Solenoid closed breakers are one case where the closing energy for a breaker is supplied by the station battery or ac station service operating through a rectifier. Although many of these circuit breakers are still in service, they are rarely produced any more due to extremely large electrical energy requirement.

### **II.3.7 Opening:**

Generally, the trip coil releases the small latch or pilot valve and from that point on, once the latch is released or pilot valve actuated, the motion is completed to full open. It is not necessary in most cases to maintain the tripping coil in an energized state through the entire opening operation. At the end of the opening stroke, dampers, usually of the hydraulic type, break the motion of the contact system so that it comes to a gentle stop and does not pound itself to death. In the closing stroke, usually a larger energy is required both to accelerate the contacts and also to overcome the opening springs. Of course, this does not apply in the pneumatic or hydraulic opened breakers where the opening is strictly by hydraulic or pneumatic means without springs.

### **II.3.8 Closing:**

The closing operation is mechanically similar to the tripping operation except the contacts are moving closed. The contact motion is slowed with dampers at the end of the stroke.

### **II.3.9 Auxiliary switches:**

In addition to the main contacts, there is a set of auxiliary contacts driven by the same means whether it be hydraulic, pneumatic or mechanical, which follow the motion of the main contacts. This is to provide control system intelligence on breaker position. Most breakers are designed to sit only in the fully open or fully closed state; therefore, intermediate position monitoring is not required.

### **II.3.10 Mechanism auxiliaries**

There are auxiliaries to the mechanism that include the means for replacing the stored energy which, in the case of springs, may be a spring winding motor. With hydraulic/pneumatics, a hydraulic pump/air compressor is used. Normally there is a system for monitoring adequacy of stored energy for operating circuit breakers.

## **II.4 SF6 circuit breakers: [46]**

### **II.4 .1 General Descriptions:**

This type of circuit breaker uses compressed sulphur hexafluoride gas (SF6) for both interruption and dielectric withstand. Bushings typically are insulated with SF6 at the same pressure as in the main tank. Interruption is accomplished by clean un-ionized SF6 gas blown across the separating contacts and through the nozzle structure.

For applications in extremely low ambient temperatures, the circuit breakers are usually provided with tank heaters to prevent gas liquefaction. Alternatively, they may employ an SF6-N2 gas mix.

In the pure form and room temperature and pressure, SF6 is a colourless, odourless, non-toxic gas that is heavier than air. When the gas has been exposed to electrical arcs, certain toxic by-products are generated. Care needs to be exercised by personnel who handle these arced gas by-products. In addition because the gas is heavier than air, it can displace the air and lead to asphyxiation if adequate ventilation is not present.

#### **2.4.2.2 High voltage SF6 circuit breaker design [46]**

There are many design variants that have been and are in use for HV SF6 circuit breakers but they

all contain certain common functional elements. The design aspects described here are intended to be as generic as possible and where relevant specific design variants will be mentioned.

Figure 2.8 below shows two (functional) block diagrams for HV SF<sub>6</sub> circuit breaker operational arrangements. The main functional elements are:

1. Interrupter
2. Operating mechanism
3. HV enclosure

One diagram illustrates a three pole operated (TPO) circuit breaker; the other a single pole operated (SPO) circuit breaker. A TPO breaker operates the interrupters for all three phases together via one operating mechanism; such designs are predominant in the 72-170kV voltage range. Single pole operated circuit breakers use a separate operating mechanism to control its own respective phase's interrupter; such designs are predominant in the 245-800kV voltage range, mainly due to the constraints of the physical size of such breakers (dictated by insulation coordination requirements) and the associated operating energies and forces of such large breaker.

The prevalence towards ganged three pole operation at lower transmission voltages is primarily cost driven, as it requires only one operating mechanism for all three poles, compared to a single operating mechanism per pole for single pole operation. The cost differences between single and three pole operation extend beyond the circuit breaker itself, as it also requires per phase control and in many cases protection, relays and cabling. [49]

The HV enclosure is intended to represent the means by which the interrupter is housed and the potential of that housing. Two (2) main forms of enclosure exist; "live tank" and "dead tank". A live tank circuit breaker is one in which the interrupter is housed within an insulator that is mounted at the high voltage level. The interrupter "tank" is supported by another fixed insulator to earth / ground. A dead tank circuit breaker has its interrupters enclosed within earthed metal tanks and the conductor connections to the interrupter come via some form of HV bushing. In terms of the functional descriptions contained here, there is no major difference between live or dead tank circuit breakers.

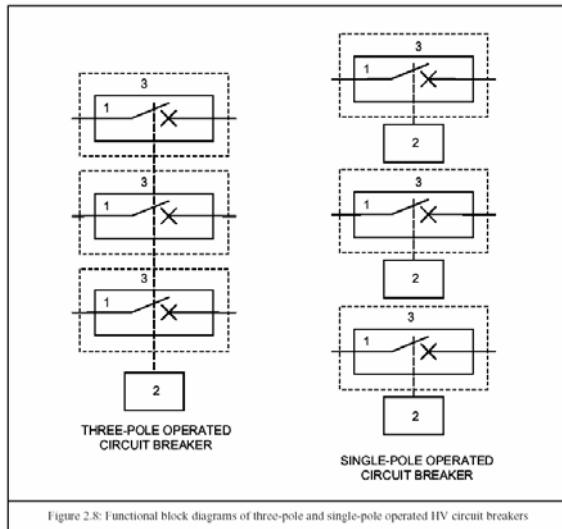


Figure II.3

Operating mechanisms for HV circuit breakers can vary widely in design. Historically the major types were pneumatic, hydraulic and spring based. Recent trends have led to predominance in spring-based operating mechanisms, driven largely by their perceived higher reliability compared to the pneumatic and hydraulic designs (Knobloch et al [3], Kuhn et al [30], Bosma et al [5]).

The interrupters in each phase can be comprised of one or more series connected interrupter units, depending on the rated voltage of the circuit breaker. The largest single unit HV interrupters developed to date are in the range of 300-420kV. Typically most 420-550kV circuit breakers have double-unit interrupters, while at 800kV four series connected interrupters are used.

The puffer interrupter operating principles have been explained earlier in section 2.2.1. Self-blast interrupters come in a variety of designs, but their central difference from puffers is that for large currents (typically above rated load current) they utilize energy radiated from the arc to generate the pressure build-up in the SF<sub>6</sub> volume contained within the moving contact cylinder. This use of the arc energy for gas pressure build up reduces the mechanical operating energy required by the interrupter and thus permits the use of a low energy operating mechanism. At lower currents the “self-heating” effect is normally too small to build up the required gas pressure to ensure interruption and so most self-blast interrupters also use a small “auxiliary puffer” action to manage interruption for such cases (Garzon pp175-177 , van der Sluis p65-66 , Knobloch et al [3], Duforenet et al [6]).

### **II.4 .2 Operating mechanism principles**

Various means of providing the mechanical energy and means to move the circuit breaker contacts. The required distance at the required speed has been used over time.

Transmission level HV circuit breakers are characterized by their relatively high operating energy demands, being anywhere in the range of 1 kJ to 20 kJ per opening operation (depending on the size of breaker, type of interrupter design, ratings etc). As the operating times of the circuit breakers are quite short ( $\delta$  100 ms) the associated peak operating forces expended by the circuit breaker can be very high (i.e. 10-100's kN) [16].

Various mechanical technologies have been employed in operating mechanisms to date.

Pneumatic mechanisms arose with air-blast circuit breakers but have also been employed on oil and SF6 circuit breakers. Hydraulic mechanisms have been used on oil and SF6 breakers. Spring operated mechanisms for HV oil and SF6 circuit breakers have been in use for many decades, however since the early 1990's they have progressively replaced the other mechanical technologies to become the dominant design type for modern HV SF6 circuit breakers. Various arguments have been proposed to explain the increased preference for spring operating mechanisms including their reported higher reliability and importantly for controlled switching applications, their reported higher operating time consistency under a wide range of operating conditions.

One of the most recent developments in HV circuit breaker operating mechanism technology has been the use of a digitally controlled servomotor drive.

### **II.4 .3 The interruption process:**

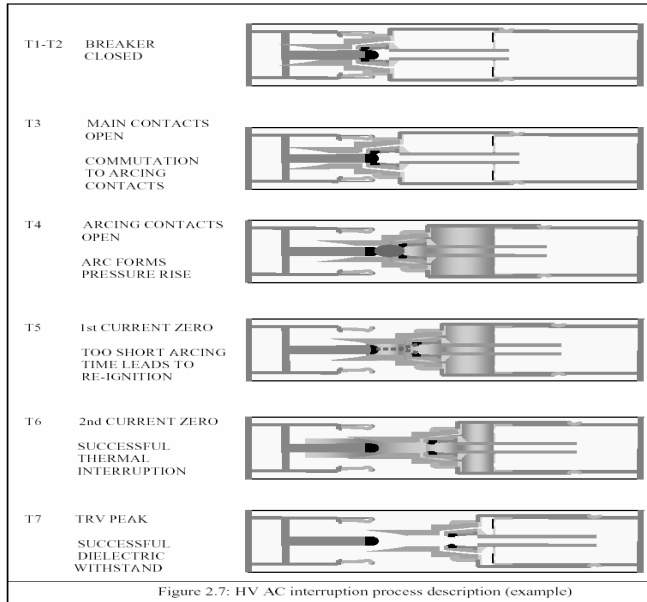


Figure II.4 shows the interruption process steps in regard to the physical processes occurring within the interrupter.

At time T1, the fault starts. The protection relay(s) detect the fault and initiate the trip signal to the circuit breaker at time T2. The disturbances on the current waveform between T1 and T2 are due to transient wave reflections on the power system arising from the fault. Some time is taken by the circuit breaker to accelerate its moving contact system in response to the trip command. At time T3 the main contacts of the circuit breaker separate, resulting in the current being commutated to the arcing contacts. Shortly after, at time T4, the arcing contacts separate and an arc is formed between these contacts. The arc is constricted within the interrupter nozzle (and by Lorenz forces), and blocks the outlet of the moving contact cylinder puffer volume. As the moving contact cylinder continues to move, the puffer volume is reduced and the pressure of the SF<sub>6</sub> gas within this volume increases.

At time T5 the current passes through its first current zero after arc formation and the breaker attempts to interrupt. In this example it is assumed the arcing time (T5-T4) has been too short and there is insufficient inflow of “cool” SF<sub>6</sub> to the arcing region to achieve thermal interruption. Consequently the current re-ignites and the current continues to flow to the next current zero crossing.

By the time of the second current zero after initial arc formation, T6, the puffer volume has been further compressed and as the arc diminishes there is sufficient “cool” SF<sub>6</sub> gas

flow to achieve thermal interruption. Now the transient recovery voltage (TRV) begins to develop rapidly between the contacts (at a rate in the order of  $\text{kV}/\mu\text{s}$ ). In this example the breaker achieves a sufficient contact gap in addition to sufficient inflow of “cool” SF<sub>6</sub> gas to maintain an adequate dielectric strength to withstand the TRV (T<sub>7</sub>). The breaker’s moving contact cylinder continues to move until the fully open position is reached.

It should be noted that the above description is based on a purely artificial example case. It is intended only to illustrate the general interruption process with a HV SF<sub>6</sub> puffer circuit breaker. It is important to recognize both the range of interruption cases a circuit breaker is required to manage, in addition to the statistical factors that arise in determining any particular circuit breaker’s performance.

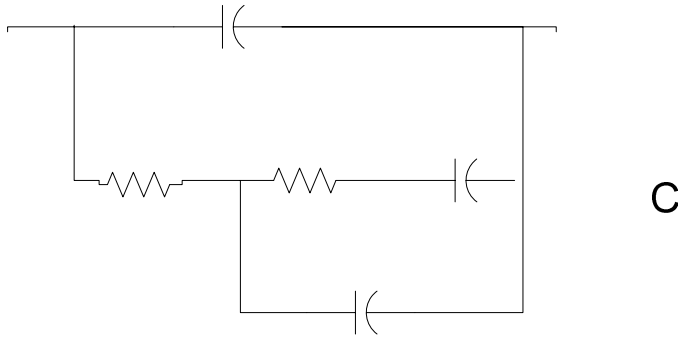
#### **II.4 .4 Typical ratings:**

SF<sub>6</sub> gas circuit breakers have been used since the early 1960s. They are used at voltages between 15.5 kV and 765 kV in two different major variations. The first variation is a two pressure system where SF<sub>6</sub> is stored at high pressure in a reservoir separate from the lower pressure main tank. During interruption, a valve is opened between the high pressure system and the lower main tank pressure allowing clean gas to flow across the contacts and nozzles. When the pressure in the high pressure becomes low, gas from the low pressure system is compressed into the high pressure system. An SF<sub>6</sub> gas compressor is used to move the gas back into the high pressure system. The second variation is a single pressure system. During interruption, the motion associated with the moving contact compresses gas between a cylinder and piston and forces the compressed gas across the main contacts and nozzles. Except during interruption, there is only one gas pressure in this type of circuit breaker. During closing the gas is not compressed. [46]

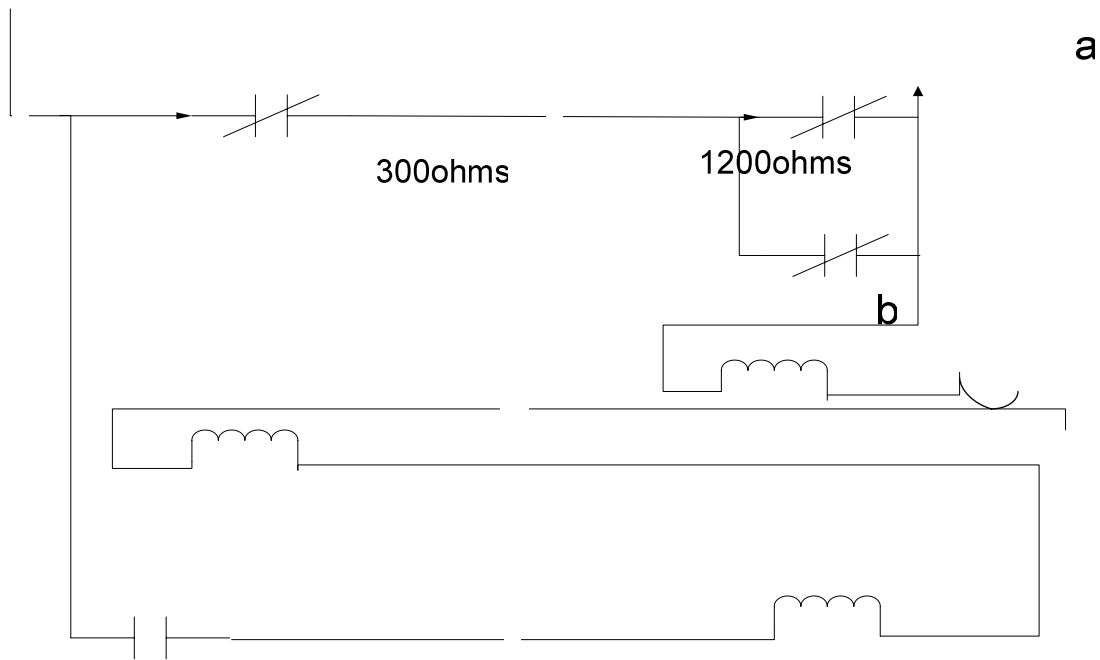
#### **II.4 .5 Typical applications:**

SF<sub>6</sub> insulated circuit breakers are used in both indoor metal-clad and in outdoor substations including gas insulated substations for practically all types of applications.

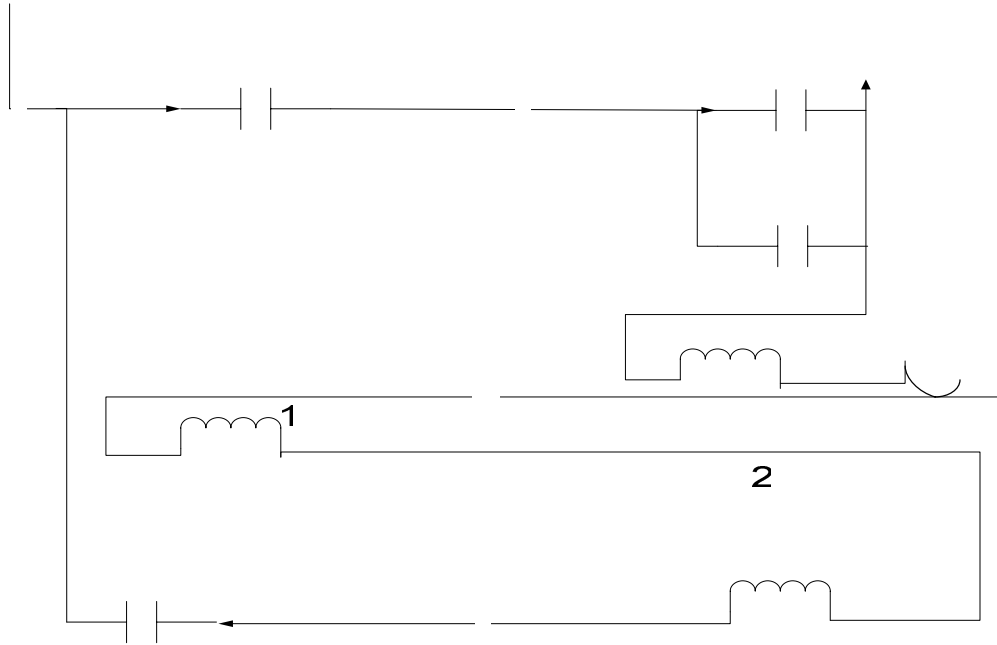




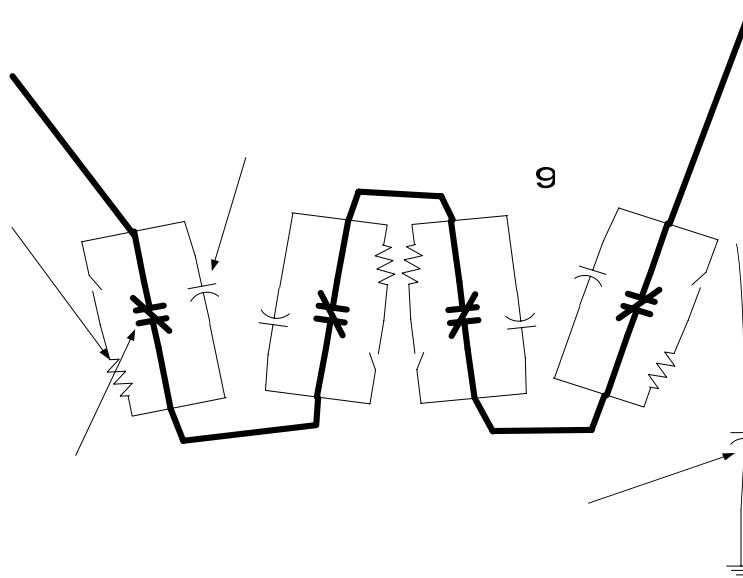
**Figure .II.5** Diagram illustrating closing sequence (a-b-c) for a two step resistor equipped breaker unit of an SF<sub>6</sub> double pressure interrupting unit for an EHV circuit breaker of the modular construction type [Westinghouse,[49]].



**Figure.II.6** Schematic diagram showing electric operation of interrupter in the closed position of a SF<sub>6</sub> single pressure interrupting unit for 1500MVA 34.5 kV vertically withdrawable circuit breaker using magnetically driven pistons[49] .



**Figure.II.7** Schematic diagram showing electric operation of interrupter in the open position of a SF<sub>6</sub> single pressure interrupting unit for 1500MVA 34.5 kV vertically withdrawable circuit breaker using magnetically driven pistons[49] .



**Figure.II.8** Typical 362kV Breaker schematic diagram[49] .

5

## II.5 Bulk oil circuit breakers:

### II.5.1 General Description:

This type of breaker uses a large oil volume for both interruption and dielectric withstand. Bushings typically are either solid or oil filled and the mechanism is typically powered by a low pressure (about ten atmospheres) air compressor and tank. Interruption is accomplished by the arc established between the contacts, causing decomposition of oil and the resulting gasses extinguishing the arc through a system of baffles which are immersed in a large tank of oil.

### **II.5.2 Typical ratings:**

Bulk oil breakers were the technology for most high voltage breakers of all ratings up to 362 kV transmission applications prior to the introduction of air blast and SF6 breakers, which gained momentum in the early 1960s. Although oil breaker maintenance was well understood, it had the disadvantages of high contact maintenance, potential oil fires from failures, relatively slow interruption, as well as sensitivity to an evolving fault. There are still many thousands of these breakers in service, although few new breakers of this type are now supplied, particularly for transmission voltages. [46]

### **II.5.3 Typical applications:**

Bulk oil circuit breakers are used in ails applications for high-voltage interruption within their limitations.

## **II.6 Vacuum circuit breakers:**

### **II.6.1 General Description:**

The internal components of a vacuum interrupter are shown in figure C.1. These include:

- A pair of butt contacts, one stationary and one moveable
- An insulating envelope made of ceramic or glass
- A metal shield for the condensation of metal vapour
- Metal end plates as stationary supports and seals for the envelope, and
- A metal bellows to transit motion to one contact and maintain a vacuum seal

The ambient gas pressure inside of the interrupter is approximately  $10^{-6}$  torr (0.133 mPa). To carry current, the contacts are butted together with several hundred pounds of force. To interrupt current, the contacts are rapidly separated to a gap of a fraction of an inch. An arc,

formed upon separating the contacts, is supported by metal vapour from the contacts. This metal vapour quickly expands from the contact gap region and condenses on relatively cooler surfaces, specifically the metal shield that surrounds the contact gap. The shield is located coaxial with and inside of the insulating envelope, and thereby prevents the metal vapour from condensing on the insulating envelope, which would decrease its dielectric strength. As the current approaches zero, the metal vapour dissipates within microseconds, which restores the vacuum between the contacts and their ability to withstand the open circuit voltage of the power system.

Vacuum circuit breakers are mostly provided with spring-operated mechanism.

The small gaps required by vacuum interrupters to meet their dielectric withstand and current interrupting requirements result in short stroke, low energy mechanisms.

### **II.6.2 Typical applications:**

Vacuum circuit breakers are typically applied in both indoor metal clad switchgear and in outdoor substations. The small size of the vacuum interrupter has enabled manufacturers to design compact circuit breakers and switchgear.

For indoor application, switchgear designs are available that stack two circuit breakers, one above the other, to minimize floor space. In addition, retrofit versions of vacuum circuit breakers are available that fit into older switchgear that was originally designed for air magnetic circuit breakers.

For outdoor application, vacuum interrupters are always contained in an outside enclosure, since the compact design of the interrupter and the need to use smooth sided ceramic or glass envelopes makes the interrupter itself unsuitable to deal with water and contamination, where a long insulation creep age distance is required.

In addition to general purpose applications, vacuum circuit breakers are especially useful in many definite purpose applications where the special properties of vacuum interruption provide outstanding performance. Such applications include

- Arc furnace switching, where the long life of the vacuum interrupter is essential,
- Capacitor switching, including general purpose and back-to-back applications, and motor switching.

Surge suppression is sometimes required in applications where the insulation strength of the connected equipment is less than the circuit breaker rating.

**II.6.3 Typical ratings:**

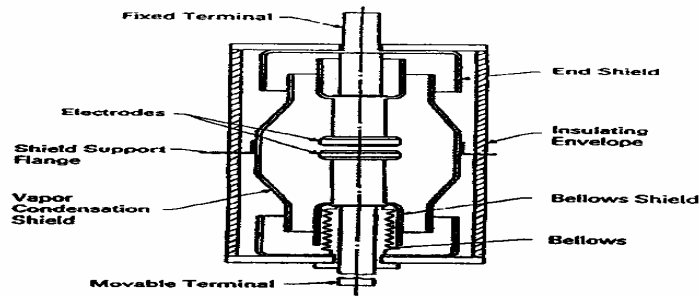
Vacuum circuit breakers are chiefly designed for medium voltages up to 38 kV and 200 kV BIL and up to 3000 A continuous current.

Higher system voltages are achievable by using two or more interrupters in series. At least one manufacturer has a retrofit design available that replaces the interrupters in an oil circuit breaker with 4 vacuum interrupters for a 145 kV rating. Higher currents are also achievable and available. Vacuum interrupters are also used in low voltage (600 V) contactors. [46]

**II.6.4 Typical maintenance checks:**

The manufacturer's instruction manual should be consulted for detailed checks and measurements to make acceptable values and suggestions on corrective actions. Typical checks are:

- a) Check for contact wear, especially if the circuit breaker operations counter shows a high number of operations. The location of a contact wear indicator or the measurement of contact position will provide a measure of the portion of contact life that remains. A small amount of contact material is eroded with each current interruption. While the interruption of many high fault currents will erode the interrupter contacts to the point where the interrupter can no longer operate properly, the interrupting life of vacuum interrupters is generally longer than other types of interrupters, and, moreover, the vacuum interrupter usually outlasts the mechanism.
- b) Check contact wear springs for proper compression.
- c) Check for loose or broken current transfer connections.
- d) Check for vacuum integrity.
- e) Check contact resistance.
- t) Check for proper opening and closing times.
- g) Check for proper closing over-travel and opening spacing. Mechanism wear in addition to contact wear can change these two dimensions that are of major importance. Contact wear indicators may be indicating mechanism change as well as contact erosion so it may not be the contact wear causing loss of over travel.



**Figure II.9-**A cross-section view of a typical vacuum interrupter [46]

## **II.7 Air magnetic circuit breakers**

### **II.7.1 General Description:**

This type of breaker uses stored energy spring mechanisms, to operate the main contacts. Interruption involves the use of an arc chute for breaking up and cooling arc products, in a similar manner to low voltage breakers, although blow

OF Out coils are frequently used to accelerate the movement of the arc into the arc chutes. The breakers for medium voltage were large and weighed more than 1000 lb (455 kg). This type of breaker was in wide use before the more modern vacuum breakers. Typically, closing energy is supplied by closing springs charged by a motor or by solenoid. Arc chutes may contain asbestos.

### **II.7.2 Typical ratings:**

This concept involves arc chutes and some means of controlling the arc so that it is established in the arc chutes. In that location, the arcing current is reduced by increased circuit resistance and splitting of the arc so that after a current zero, the breaker gaps will successfully resist reigniting. These concepts are presently applied in low voltage breakers and were applied in medium-voltage devices of the 4 kV, 7 kV, and 15 kV levels prior to the introduction of the more modern vacuum and SF<sub>6</sub> breakers in this class. The later technologies offer less maintenance, freedom from the large arc chutes, and a much more compact design.

### **II.7.3 Typical applications:**

Higher interrupting levels of low-voltage breakers, particularly those of continuous current exceeding 600 A and ac voltages of 440 and higher. Ratings in the medium voltage class covered all applications for interrupting levels.

## **II.8 Air blast circuit breakers:**

### **II.8.1 General Description:**

This type of breaker uses high pressure air, [typically 40 atmospheres (4000 kPa)], to operate a quick opening mechanism as well as to provide insulation between line and load after opening. Interruption takes place by rapid mechanism opening coincident with an air blast to remove arc products and prevent re-ignition after a current zero. Typically, the breaker includes a compressor and dryer system for providing a stored air supply at about 150 atmospheres (15 000 kPa). Bushings typically are gas insulated, often SF<sub>6</sub> at about 4 atmospheres (400 kPa), and the interrupter is of a live tank design.

### **II.8.2 Typical ratings:**

This technology had been applied for medium voltage and high interrupting currents in the 1940s and 1950s. In the early 1960s the voltages were increased into the transmission class and eventually covered all interrupting ratings from 155 kV through 765 kV. Their application started to decline with the advent of the SF<sub>6</sub> puffers, in the late 1970s, due mainly to the maintenance requirements for the high pressure (2000 psi) air systems and the complex gasketing, as well as their high noise levels during interruption.

### **II.8.3 Typical applications:**

During their high popularity, they were applied in all transmission applications, particularly where their strong capacitor switching was desired and where sound levels were not critical. They are still applied in many generator breakers where interrupting levels and continuous currents must be high.

## **II.9 Minimum oil circuit breakers**

### **II.9.1 General description**

This type of breaker, when applied below 170 kV, normally now has one interrupter per pole with the highest voltages having up to six breaks. Minimum oil circuit breakers built in the 1970s would likely have two interrupter breaks per pole up to 170 kV. The interrupter breaker units are mounted on post insulators, which constitute the insulation of the pole to earth. The breaking units consist of an arc control device usually of the cross-

blast type within an oil container. Units with more than one break are equipped with grading capacitors for voltage division across the breaks. The Closing energy is provided by a motor-charged spring or by an hydraulic or pneumatic stored energy closing device. The closing mechanism is connected to the breaking units via a pull-rod system, link gears, and rotating insulators. The opening springs are charged during a closing operation so the breaker can never be closed without sufficient energy for an opening operation. The breaker is opened by release of the trip latch.

### **II.9.2 Typical ratings:**

The design of this breaker has operated over a wide range of voltage classes up to 765 kV and interruption ratings of 40 kA. The use of this style of breaker has diminished due to the advent of SF6 breakers.

Closing energy is provided by a motor-charged spring or by an hydraulic or pneumatic stored energy closing device. The closing mechanism is connected to the breaking units via a pull-rod system, link gears, and rotating insulators. The opening springs are charged during a closing operation so the breaker can never be closed without sufficient energy for an opening operation. The breaker is opened by release of the trip latch.

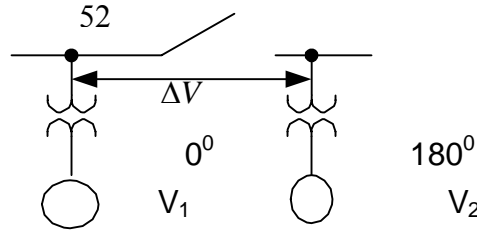
### **II.10 High voltage circuit breakers-flashover failures.**

Flashover can occur on any breaker in the network where an over voltage condition is present, but the probability is higher on breakers used to synchronize two isolated power systems or on generator breakers. During the synchronization process, the out-of-phase angle between breaker contacts changes from 0 to 360 degrees continuously. Voltage between breaker contacts reaches its maximum instantaneous value when the angle difference between the voltages is 180 degrees, with a magnitude equal to double the nominal phase-to-ground peak voltage (**Figure II.10**). One example is a breaker that synchronizes a generator on a 500 kV system: the voltage changes continuously between 0 and 577.3 kV rms or 0 and 816 kV peak instantaneous voltages.[7]

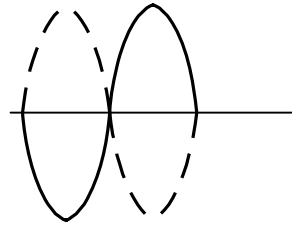


$$\Delta V_{rms} = \frac{500}{\sqrt{3}} \angle 0^\circ - \frac{500}{\sqrt{3}} \angle 180^\circ = 577.3kV$$

$$\Delta V_{peak} = 816.0kV$$



$$\Delta V = 2pu$$



**Figure II.10** Voltage Waves on Both Sides of an Open Breaker When the Angle Is 180 Degrees.

Another possible cause of flashover can occur when a long high-voltage line, without line reactors, is energized. When the local breaker is closed, the capacitive effect of the line will cause an over voltage at the remote end. This over voltage could cause the remote end breaker to develop a flashover. [7]

If the dielectric strength on any of the breaker phases is lower than normal, a flashover can occur when the voltage across the open breaker contacts increase. The highest probability that this will happen is when the voltage angle is near 180 degrees. Besides damaging the breaker, this out-of-phase and unbalanced condition affects system stability and can lead to abnormally high stresses on electric equipment near the breaker, such as a generator or transformer.

From the power system point of view, a flashover is a fault series. A flashover is not a ground or a phase-to-phase fault, but a condition that resembles one phase of a breaker closed, with a residual current much lower than a phase-to-ground fault. A flashover can lead to a power oscillation. Line, transformer, and generator protection are not effective in this situation because they either do not detect flashover failure or do not detect it quickly enough. Neither is traditional or standard breaker-failure protection effective to

detect flashover failure, because these require an external trip signal from another protection device to initiate the breaker failure.

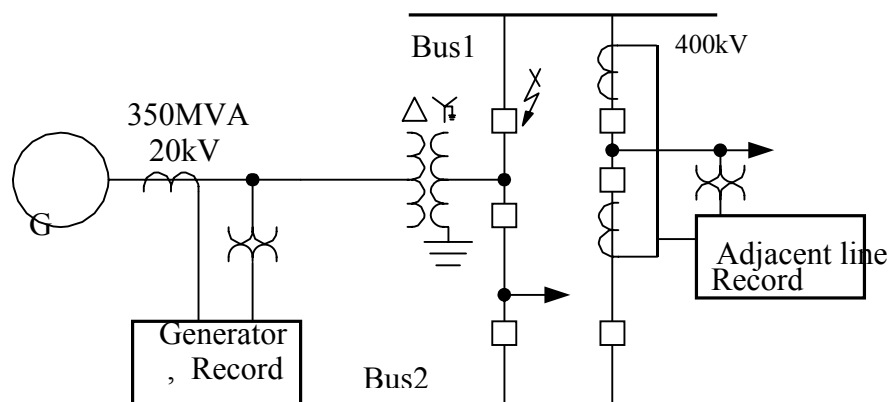
Relying on an external trip prolongs the failure until line, generator, or transformer protection trips. [7]

### II.10.1 EXAMPLE OF A REAL CASE ANALYSIS

The case study that has been chosen as an example is of a system where a real flashover happened during the synchronization process in a generator-transformer unit connected to a 400 kV power system. The unit consists of the following: [7]

- A generator rated at 350 MVA, with a rated voltage of 20 kV and rated current of 10.104 kA.
- A generator-transformer rated at 375 MVA nominal, with a 20 kV delta to 400 kV Grounded-wye

The flashover occurred in the main breaker. The half breaker was open. There were no oscillographic records for the 400 kV breakers where the flashover occurred, but there were oscillographic records for the generator and adjacent 400 kV line.

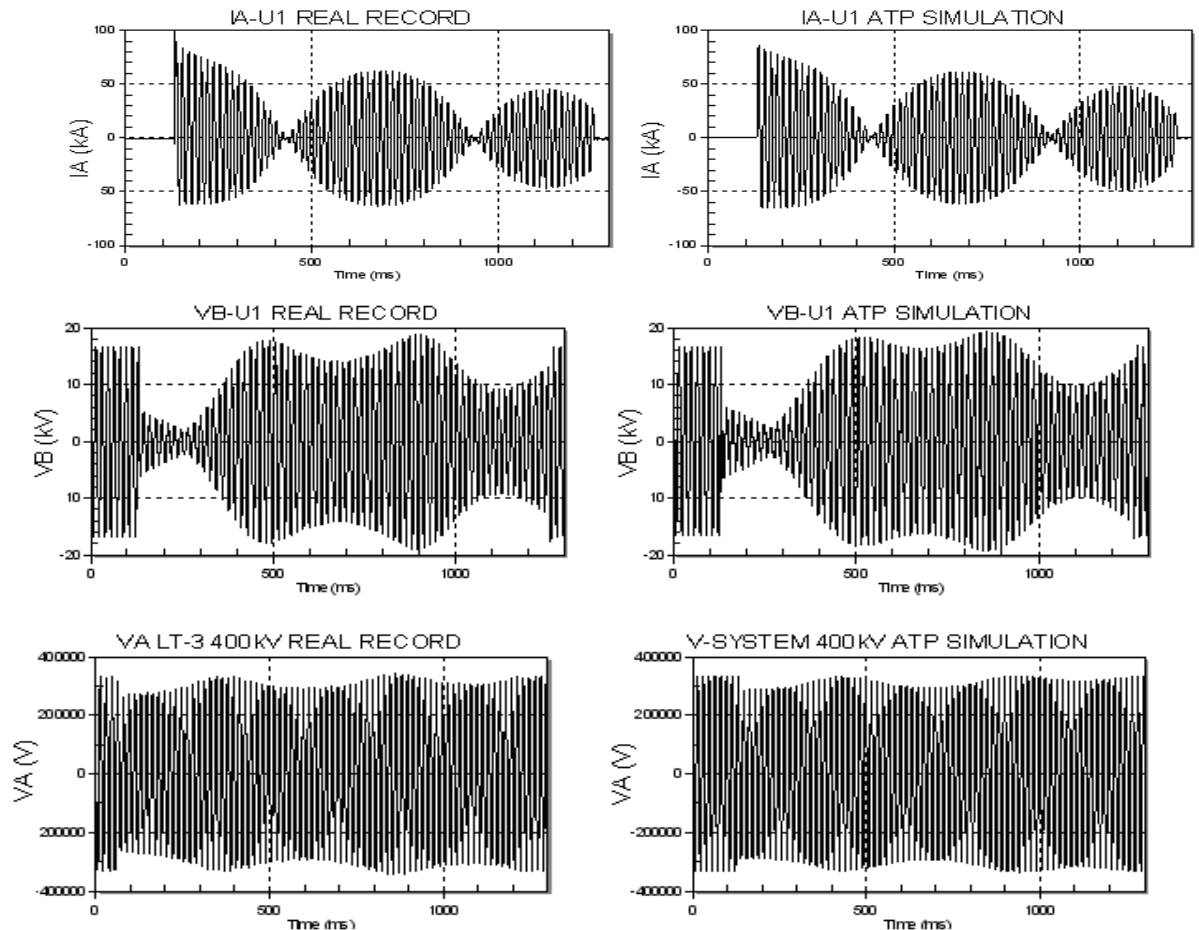


**Figure II.11** Case Study Data and Oscillographic Recorder Location [7]

### II.10.3 Comparisons between real and simulation results of different flashover conditions:

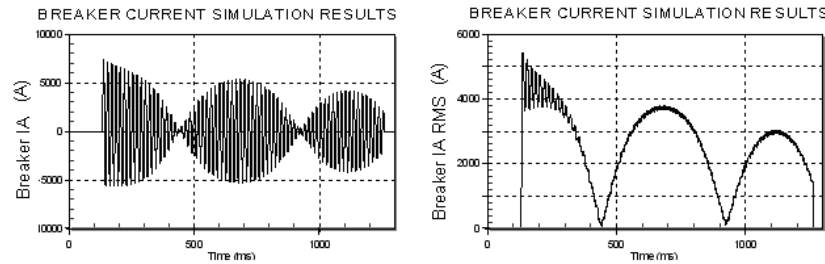
For a better understanding of different flashover conditions, a model of the actual power system has been implemented in ATP (EMTP) (Alternative Transients Program - Electromagnetic Transients Program). Comparisons of the simulation results using the modeled power system with the actual recorded results validated the power system model.

In Figure II.11 it can be seen that the actual and simulated results are match closely, which confirm the accuracy of the simulation model. This model will now be used to investigate different conditions that can lead to flashover failure. In the simulated model, flashover occurs when the voltage magnitude difference between the breaker contacts is approximately 2 p.u. At this point, the angular difference between the voltages is  $180^\circ$ . Note that the simulated model ignores the effect of the arc resistance.



**Figure II.12** Comparison of Actual Records and ATP Simulation Results for Generator Voltage, Generator Current and Adjacent Line Voltage [7]

One main variable is the current at the failed breaker for which there are no actual records available. Simulation results in **Figure II.13** show that current magnitude oscillates from a value of 3.3 p.u. during the first cycle of flashover to zero approximately 18 cycles later. When setting the pickup current threshold and time-delay pickup of an over current relay for flashover protection, consideration should be given to the magnitude and duration of the current oscillation. A dc offset of 900 A is also noticeable during the first few cycles after flashover; this effect can be ignored when setting a numerical digital protective relay.



**Figure II.13** Failed Breaker Current from ATP Simulation Results [7]

The effect of different flashover conditions can be evaluated using the simulated power system model; these different conditions are listed in Table II.2 [7].

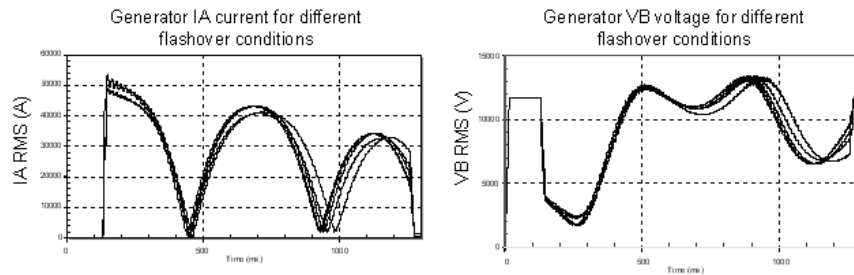
Case	Generator IA and IB	breaker IA	Generator VB (phase-to-ground)	400kV Bus VA (phase-to-ground)
Actual case	52.5 – 0 – 43 kA 5.1 – 0 – 4.2 p.u	4.5 – 0 – 3.7 kA 8.3 – 0 – 6.8 p.u.	3.6–1.68–13.4kV 0.31–0.14–1.16 p.u.	201-236 kV 0.87-1.02 p.u
Flashover at 360°kV,90°	53.3-0-43 kA 5.3-0 – 4.2 p.u	4.9 -0-6-3.7 kA 9-0-6.8 p.u	3.6-1.7-13.2 kA 0.31-0.15-1.14 p.u	200-236 kV 0.86-1.02 p.u
Without one of the parallel generators in the same bus	52.5-0-43 kA 5.2-0-4.2 p.u	4.4-0-3.8 kA 8.1-0-7 p.u	3.7- 1.67-13.3 kV 0.32-0.14-1.15 p.u	199-236 kV 0.86-1.02 p.u
with weak system( $Z_{thv} \times 2$ )	49.2-0-40.7 kA 4.9-0-4 p.u	4.0-0-3.6 kA 7.4-0-6.6 p.u	3.8-2.3-13.4 kV 0.33-0.2-1.16 p.u	177-239 kV 0.76-1.03 p.u
Without one of the generators in the same bus and weak system.	48.6-0-41.1 kA 4.8-0-4.1 p.u	4.1-0-3.6 kA 7.6-0-6.06 p.u	3.9-2.3-13.35 kV 0.34-0.2-1.16 p.u	170-239kV 0.73-1.03p.u

**Table II.2** Current and Voltage Variations for Different Flashover Conditions [7]

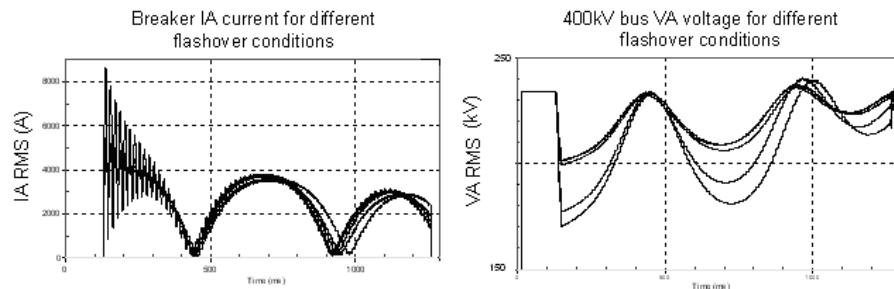
From **Table II.2** and **Figure II.14**, we can observe changes in currents and voltages during different flashover conditions. Failure behavior does not change too much with these variations in system short circuit or angle between open breaker contacts at flashover initiation. Two issues that should be considered are:

- Very high dc current level if the flashover occurred at a 90° angle difference between the voltages of the open breaker contacts. The level is about 4 kA, 1.81 asymmetry.
- Lower voltage at the high-voltage side (400 kV) of the transformer (breaker bus voltage)

if the system is weak, about 0.73 p.u.



**Figure II.14** Generator Current and Voltage for Different Flashover Conditions [7]



**Figure II.15** Breaker Current and Breaker/Bus Voltage for Different Flashover Conditions [7]

Using these data, we can suggest and validate settings for breaker-flashover protection schemes.

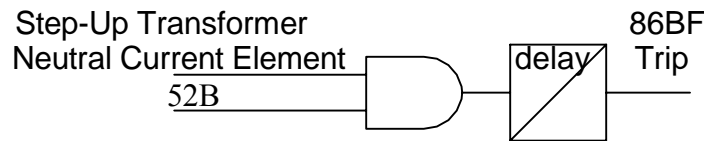
## II.11 METHODS FOR FLASHOVER PROTECTION [7]

There are several different schemes for breaker-flashover protection. These methods can use information from any of the following: phase currents, residual current, voltages from

one or both sides of the breaker, breaker position auxiliary contacts (52a or 52b), and close-signal monitoring or timers.

### II.11.1 Method A. Residual Over current and Breaker Auxiliary Contact.

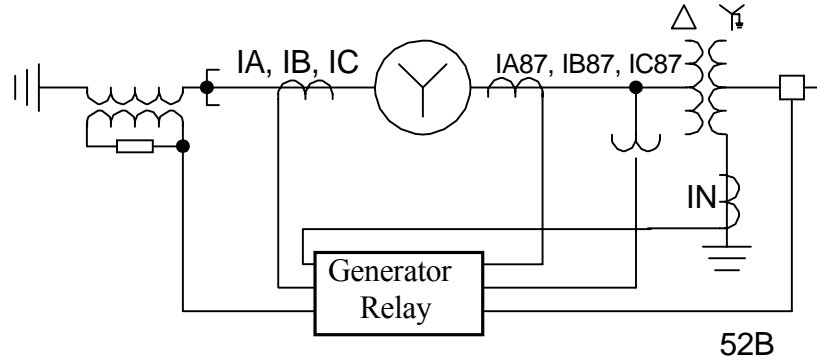
This is the simplest and easiest method. It is described in the IEEE C37.102 [5] standard and is based on breaker residual-current measurement and a breaker auxiliary contact (52a or 52b). Flashover is detected and the bus cleared if there is residual current and the breaker is open. This condition could also occur for a short period during normal close operations where phases do not close simultaneously and there is a delay in contact change. These cases require a timer to confirm that there is a flashover. The logic diagram for this scheme is shown in Figure II.16.



**Figure II.16** Logic Diagram of Breaker Flashover, Method A, Residual Current and Breaker Auxiliary Contact

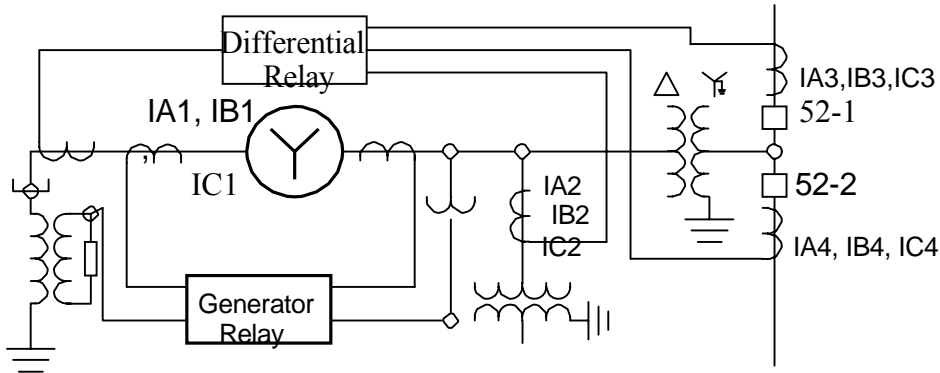
The residual current element should be set at a low level to detect small residual currents, thereby covering cases where flashover is not an out-of-phase condition and residual current is proportional to load. This element should also be set to cover cases where current decreases very rapidly to a value close to zero during an oscillation. The suggested value is above the normal residual current during load.

Residual current could be obtained directly from the breaker current transformer (CT), neutral connection, but is usually obtained from the neutral CT of a step-up transformer because any residual current at the breaker will pass through this point, as **Figure II.17** shows. It represents a typical connection to a multifunction generator relay with breaker-flashover protection included.



**Figure II.17** Flashover Protection Scheme with Multifunction Generator Relay

Step-up neutral transformer current is applicable where there is only one generator breaker. It should not be used where there are bus arrangements, such as breaker-and-a-half, ring bus, or double bus-double breaker, because it can detect flashover but cannot determine which breaker flashed over. For these cases, you need one breaker-flashover scheme per breaker that can be implemented in a multifunction relay at the substation (breaker-failure relay or line relay) or at the power plant protection panel in a multiwinding transformer relay, as Figure II.18 shows.



**Figure II.18** Flashover Protection Scheme with a Four-Winding, Multifunction Differential Relay

Another approach would be to use step-up transformer neutral protection and the logic in **Figure II.16** to detect flashover, and another relay with residual over current elements for each breaker to trip the right bus. The author of [7] didn't recommend this method because it adds points of failure without any advantage over using a separate scheme for each breaker.

The main disadvantage of Method A is lack of **security** and **dependability**. If the breaker auxiliary (52b) signal is not received; it will not trip for a flashover condition. If we use 52a instead of 52b, then it leads to a very insecure state where any external phase-to-ground failure with transformer-fed residual current will trip the bus. The breaker auxiliary signal could fail because the breaker mechanism fails, or the auxiliary relay fails, or the control circuit connections between breaker and relay fail. [7]

A further problem with these methods emerges at breaker-and-a-half arrangements where a generator and a line share the half breaker, or when the flashover scheme is for a line breaker. If the line has single-pole trip and reclose, residual current and one pole open is a normal condition. This method can be applied to single-pole operation breakers if we use 52b auxiliary contacts for phases A, B, and C in series, so that the scheme does not trip until there is an indication of the three phases of the breaker open. Here, too, dependability will drop because the probability that an open breaker will not be detected is multiplied by a factor of three.

This method also does not work for three-phase flashover, but the probability of this kind of failure is very low. Other methods are available that avoid an insecure condition without losing dependability. [7]

### **II.11.2 Method B. Current and Breaker Auxiliary Contact per Phase**

One possible variation of Method A is the use of current and breaker contact per phase, which has the advantages of directly targeting relay operation per phase and of applying to single-pole- operating breakers.

This method, which we call Method B, is not applied in practice because its security would be very low. During a normal close condition, if the breaker contact does not change, Method B would trip the bus incorrectly if the over current element were set as low as we recommend, so that the over current element remains asserted during current oscillations.

### **II.11.3 Method C. Time Limits and Close-Signal Monitoring to Detect Flashover.**

One way to increase the security of methods A and B is to limit the time period when the schemes can start [7]. The logic diagram in Figure II.10 allows scheme operation only if latch conditions occur in the first five cycles after current flows in the breaker. With this timer and logic combination, we solve the case where a breaker auxiliary signal is lost in

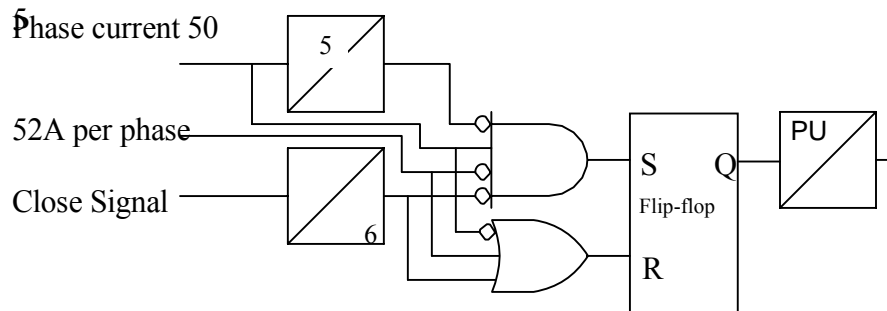


the scheme during normal operation with the breaker closed and residual or phase currents present. Methods A and B would trip for this condition, Method A with an external fault and Method B only with load.

Close-signal monitoring provides another security improvement to Method C. The logic shown in Figure II.10 blocks the start of the scheme if there is a close signal present and for six cycles afterward. With this we solve the case of a normal close with load, where the breaker contact does not change its state. Method B would trip in this situation. Then, in order to trip, Method C requires: [7]

- Phase current greater than the setting value, without any current five cycles before the start of the scheme
- Breaker auxiliary contact open (for 52a)
- No closing signals to breaker at least six cycles before the start

Once the scheme starts, it seals in and uses a timer to confirm the flashover condition. The timer could stop if current drops below the setting (near to zero), if 52a changes to indicate a closed breaker, or if there is a close signal.



**Figure II.19** Method C: Improvements with Close-Signal Monitoring and Time Limits to Start Method C could be applied to three-phase or single-phase breakers and improve security without loss of dependability.

Method C works well for three-phase flashover if used as shown in Figure II.19.

Method C could be modified to include residual or step-up transformer neutral current instead of phase current for generator breakers where there is no single-pole tripping, but then it would no longer work for three-phase flashovers. In this case, the 52a signal must be formed with A-, B- and C-phase 52a auxiliary contacts in parallel or with 52b auxiliary contacts in series.

#### II.11.4 Method D. Live-Bus Voltage Supervision [7]

Some flashover schemes use live-bus voltage relay supervision to initiate the scheme. The theory is that voltage should be at normal levels or higher before or during the flashover. But in many cases, such as the one in the case study, voltage is normal only before flashover, then drops to 0.8 p.u. at the beginning of the failure because of the out-of-phase synchronization. In this case, voltage drops to 0.8 p.u. because the bus has a very high short-circuit level (strong network). For buses in weak systems, voltage could drop to lower levels. The simulation results before indicated 0.73 p.u. for a weak system. The author advises us that, voltage supervision should be set to 0.6 p.u. or lower to ensure that the scheme starts. There is no increase in security because a voltage element set to 0.6 p.u. will be active all the time with load or for some external faults. Dependability is affected because two dependability-related failures are now possible: [7]

- Loss of secondary potentials from PTs
- One more setting, so more chance of human error.

We do not recommend the use of live-bus voltage supervision.

#### II.11.5 Method E. Voltage at Both Sides of the Breaker

Two characteristics of flashover events are [7]:

- There is no current before the flashover and there is high voltage between open breaker terminals.
- During flashover, current flows and voltage drops to near zero.

It is possible to detect flashover with a scheme that uses these conditions. These conditions also happen during a normal close of the breaker, so the scheme must be supervised by close-signal monitoring, similar to Method C. Logic for this scheme is shown in **FigureII.20**. Suggested setting for high voltage across open terminals before operation is 0.8 p.u. phase-to-ground voltage, to ensure operation when the breaker flashes with high voltage on one side and the other side dead. For The case study above, with a PT ratio of 3500/1, 400 kV nominal and 230 kV phase-to-ground, the recommended setting is 53 V secondary. To set the low-voltage detector for conditions after flashover, we need to consider possible voltage drop across the arc resistance. Based on the simulation results, the authors assume arc resistance was very low. They simulated zero ohms resistance and all the results matched oscillographic records. For the case

study, which does not have pre- insertion resistors, 10 percent of nominal phase-to-ground voltage could be used, about 6.8 V secondary. For breakers with pre-insertion resistors, the low-voltage detector should be set below voltage drop, with resistors inserted to increase security during close operations. Time limits need to be applied to ensure that voltage drop and current flow coincide.

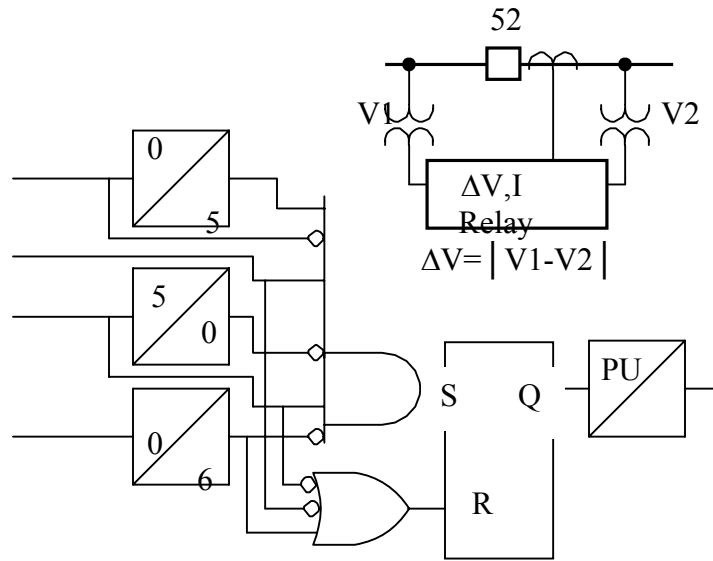
This method has the following advantages:

- Good dependability and security with supervision of voltage across the breaker
- Record of voltage that causes flashover, enabling users of digital relays with recording features to evaluate breaker performance.

Although it has these advantages, Method E has the following problems to solve:

- It requires three-phase PTs on both sides of the breaker, which are not available in most substations
- It cannot be used with PTs on the generator side and PTs on line side where there is a step-up transformer because:
  - The voltage drop in the transformer is proportional to current
  - The step-up transformer also introduces a phase-angle shift
  - A scheme to compensate for these issues could be used, but would be very complex and lack dependability
- There is security decrease compared to Methods A and C for two reasons:
  - Loss of secondary potential failure.
  - Two more settings increase risk of human error.

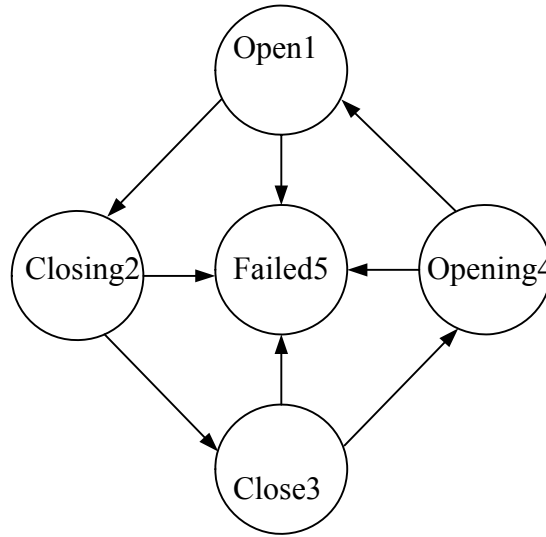
This method is not common in many electric companies; field engineers are not familiar with it. Training and information would be very important to applying it.



**Figure II.20** Flashover Protection Using Voltage at Both Sides of the Breaker and Close Monitor.

## II.12 BREAKER STATES AND FAILURE MODES [7]

We have described one of the possible failure modes for breakers, the flashover failure or failure while the breaker is open. Some utilities use standard, traditional breaker failure protection that covers the case of failure to trip when there is line, transformer, or generator failure, and primary protection trips. Breaker-flashover protection is more common everyday, but is not standard, and there are several questions about its application. There are other modes of breaker failure, for example, failure to trip with load current or without current, failure to close, or breaker failure while the breaker is closed, with pre-insertion resistors. Figure II.21 describes all the possible states and failure modes in a breaker. A comprehensive breaker-protection scheme should cover all these modes of failure and can be achieved in modern multifunction relays.



**Figure II.21** Breaker States and Failure Modes.

### II.13 CONCLUSION.

In this chapter we have been stated the design of different breakers types, then we have described one of the possible failure modes for breakers, the flashover failure or failure while the breaker is open. Results and theory have been referenced to [7] .The objective of the chapter is to present the electrical equipment, its failure modes and techniques to be used for protection .

### **Chapter III**

## **Dependability evaluation using static Fault Tree analysis.**

## Chapter III Dependability evaluation using static Fault Tree analysis

### III.1 Introduction

In multi-component systems such as power systems, chemical process plants or aerospace ships, it is important to analyze the possible mechanisms for failure and to perform probabilistic analyses for the expected rate of such failures. Typically, each system is unique in the sense that there are no other identical systems (same components interconnected in the same way and operating under the same conditions) for which failure data have been collected. Therefore, a statistical failure analysis is not possible. Furthermore, it is not only the probabilistic aspects of failure of the system which are of interest but also the initiating causes and the combination of events which can lead to a particular failure. [16]

The way to solve a problem of this nature, where many events interact to produce other events, is to relate these events using simple logical relationships (intersection, union, etc.) and to methodically build a logical structure which represents the system.

In this respect, *Fault tree analysis* is a systematic, deductive technique which allows developing the causal relations leading to a given undesired event. It is deductive in the sense that it starts from a defined system failure event and unfolds backward its causes down to the primary (basic) independent faults. The method focuses on a single system failure mode and can provide qualitative information on how a particular event can occur, to what consequences it leads, while at the same time allowing the identification of those components which play a major role in determining the defined system failure. Moreover, it can be solved in quantitative terms to provide the probability of events of interest starting from knowledge of the occurrence probability of the basic events which cause them. [11]

### III.2 The Fault Tree Approach

FTA can be simply described as an analytical technique, whereby an undesired state of the system is specified (usually a state that is critical from a safety or reliability standpoint), and the system is then analyzed in the context of its environment and operation to find all realistic ways in which the undesired event (top event) can occur. The fault tree itself is a graphic model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event. The faults

can be events that are associated with component hardware failures, human errors, software errors, or any other pertinent events which can lead to the undesired event. A fault tree thus depicts the logical interrelationships of basic events that lead to the undesired event, the top event of the fault tree.

It is important to understand that a fault tree is not a model of all possible system failures or all possible causes for system failure. A fault tree is tailored to its top event that corresponds to some particular system failure mode, and the fault tree thus includes only those faults that contribute to this top event. Moreover, these faults are not exhaustive. They cover only the faults that are assessed to be realistic by the analyst. [31]

It is also important to point out that a fault tree is not in itself a quantitative model. It is a qualitative model that can be evaluated quantitatively. This qualitative aspect, of course, is true of virtually all varieties of system models. The fact that a fault tree is a particularly convenient model to quantify does not change the qualitative nature of the model itself.

Intrinsic to a fault tree is the concept that an outcome is a binary event i.e., to either success or failure. A fault tree is composed of a complex of entities known as “gates” that serve to permit or inhibit the passage of fault logic up the tree. The gates show the relationships of events needed for the occurrence of a “higher” event. The “higher” event is the output of the gate; the “lower” events are the “inputs” to the gate. The gate symbol denotes the type of relationship of the input events required for the output event.[11]

### **III.3 Qualitative and Quantitative Evaluations of a Fault Tree.**

Both qualitative and quantitative evaluations can be performed on an FT. The FT itself is a qualitative assessment of the events and relationships that lead to the top event. In constructing the FT, significant insights and understanding are gained concerning the causes of the top event.

Additional evaluations serve to further refine the information that the FT provides. The qualitative evaluations basically transform the FT logic into logically equivalent forms that provide more focused information. The principal qualitative results that are obtained are the minimal cut sets (MCSs) of the top event. A cut set is a combination of basic events that can cause the top event. An MCS is the smallest combination of basic events that result in the top event. The basic events are the bottom events of the fault tree.



Hence, the minimal cut sets relate the top event directly to the basic event causes. The set of MCSs for the top event represent all the ways that the basic events can cause the top event. A more descriptive name for a minimal cut set may be “minimal failure set.” The set of MCSs can not only be obtained for the top event, but for any of the intermediate events (e.g., gate events) in the FT.

A significant amount of information can be obtained from the structure of MCSs. Any MCS with one basic event identifies a single failure or single event that alone can cause the top event to occur. These single failures are often weak links and are the focus of upgrade and prevention actions. Examples of such single failures are a single human error or single component failure that can cause a system failure. An MCS having events with identical characteristics indicates a susceptibility to implicit dependent failure, or common cause, which can negate a redundancy. An example is an MCS of failures of identical valves. A single manufacturing defect or single environmental sensitivity can cause all the valves to simultaneously fail.[16]

### III.3.1 QUALITATIVE EVALUATION:[7 ”]

#### Theorem1:

Let  $f$ ,  $f_1$  and  $f_0$  be three Boolean formulas and  $x$  is a variable such that :

$$f = (x \cdot f_1) \cdot (\neg x \cdot f_0),$$

$$PI(F) = PI_{1,0} \cup PI_1 \cup PI_0$$

$$PI_{1,0} \cdot PI(f_1 \cdot f_0)$$

$$PI_1 \cdot \{x\} \cup \sigma \text{ where } \sigma \in PI(f_1) \setminus PI_{1,0}$$

$$PI_0 \cdot \{\neg x\} \cup \sigma \text{ where } \sigma \in PI(f_0) \setminus PI_{1,0}, \quad \text{The symbol “} \setminus \text{” indicates sets difference}$$

In the case of coherent trees (Boolean formula is monotone) ,Then :

- First implicant (PI) • minimal cut sets(MC)

$$f_1 \cdot f_0 = f_0 ; PI_{1,0} = PI(f_0) = MC(f_0) ; PI_0 = \{\emptyset\}$$

- $MC(f) = MC_0 \cup MC_1,$

With

$$MC_0 = MC(f_0)$$

$$MC_1 = \{x\} \cup \sigma, \text{ where } \sigma \in MC(f_1) \setminus MC(f_0)$$

In the case of non-coherent trees, a general theorem can be applied

$$PI(f) = PI_{1,0} \cup PI_1 \cup PI_0$$

#### Theorem2 (search for minimal cut sets):

Let  $f$ ,  $f_0$ ,  $f_1$  three Boolean formulas and  $x$  is a variable such that :  $f = (x \cdot f_1) \cdot (\neg x \cdot f_0),$

Then,  $PC(f) = PC_0 \cup PC_1$  with  $PC_0 = PC(f_0)$

$$PC_1 = \{x\} \cup \sigma; \text{ where } \sigma \in PC(f_1 \cdot f_0) \setminus PC_0$$

### III.3.2 QUANTITATIVE EVALUATION: [10]

Known Basic events probabilities ( $e_i$ )  $\Rightarrow$  Dreaded event probability (top event probability) ( $D.E$ )

$$P(D.E) = f[p(e_i)];$$

- **Ascendant application of the two basic rules:**

$$p(e_i \bullet e_j) = p(e_i) \times p(e_j)$$

$$p(e_i \cup e_j) = p(e_i) + p(e_j) - p(e_i \bullet e_j)$$

It's an elementary method but rarely applicable in practice ( FT without repeated events )

- **Poincaré development :**

$$P(D.E) = \sum_{i=1}^n p(C_i) - \sum_{i=1}^{n-1} \sum_{j=i+1}^n p(C_i \cdot C_j) + \sum_{i=1}^{n-2} \sum_{j=i+1}^{n-1} \sum_{k=j+1}^n p(C_i \cdot C_j \cdot C_k) \dots$$

**n minimal cut sets  $C_i \Rightarrow (2^n - 1)$  terms to be calculated .**

- **Disjunction method :**

$$P(D.E) = p(C_i) + \sum_{j=2}^n p\left[\left(\prod_{i=1}^{j-1} \bar{C}_i\right) C_j\right]$$

**n minimal cut sets  $C_i \Rightarrow k(k \ll 2^n - 1)$  terms to be calculated .**

#### III.4 Role of FTA in Decision Making [16]:

A variety of information is provided by FTA to assist decision-making. An overview of the major uses of FTA is presented here to give the reader an appreciation of the breadth of applications of FTA in decision-making. Note that this section includes some information already provided in previous sections for the benefit of readers who want to focus on the FTA role in decision making.

1. Use of FTA to understand of the logic leading to the top event. FTA provides a visual, logic model of the basic causes and intermediate events leading to the top event. Typically, fault trees are not limited to a single system, but cross system boundaries. Because of this, they have shown great benefit in identifying system interactions that impact redundancy. The combination of failures and events that propagate through a system are clearly shown. The minimal cut sets can be organized and prioritized according to the number of events involved and their nature. For example, if there are minimal cut sets that contain only one component failure then this shows that single component failures can cause failure of the system. A failure path of only human errors shows that human errors alone can cause system failure.

2. Use of FTA to prioritize the contributors leading to the top event. One of the most important types of information from FTA is the prioritization of the contributors to the

top event. If a FT is quantified, the failures and basic events that are the causes of the top events can be prioritized according to their importance. In addition, the intermediate faults and events leading to the top event can also be prioritized.

Different prioritizations and different importance measures are produced for different applications. One of the valuable conclusions from FTAs is that generally only a few contributors are important to the top event. Often only 10% to 20% of the basic events contribute significantly to the top event probability. Moreover, the contributors often cluster in distinct groupings whose importances differ by orders of magnitude.

The prioritizations obtained from FTA can provide an important basis for prioritizing resources and costs. Significant reductions in resource expenditures can be achieved with no impact to the system failure probability. For a given resource expenditure, the system failure probability can be minimized by allocating resources to be consistent with contributor importance. The importance measures obtained from a FTA are as important as the top event probability or the ranked cut set lists obtained from the analysis.

3. Use of FTA as a proactive tool to prevent the top event. FTA is often used to identify vulnerable areas in a system. These vulnerable areas can be corrected or improved before the top event occurs. Upgrades to the system can be objectively evaluated for their benefits in reducing the probability of the top event. The evaluation of upgrades is an important use of the FTA. Advocates of different corrective measures and upgrades will often claim that what they are proposing provides the most benefit and they may be correct from their local perspective. However, FTA is a unique tool that provides a global perspective through a systematic and objective measure of the impact of a benefit on the top event. The probability of the top event can be used to determine the criticality of carrying out the upgrades. The probability of the top event can be compared to acceptability criteria or can be used in cost benefit evaluations. Advances in cost benefit methodology allow uncertainties and risk aversion to be incorporated as well as the probabilities. Furthermore, success paths provided from FTA can be used to identify specific measures that will prevent the top event. The proactive use of FTA has been shown to be one of its most beneficial uses.

4. Use of FTA to monitor the performance of the system. The use of the FT as a monitoring tool is a specific proactive use that has been identified because of its special

features. When monitoring performance with regard to the top event, FTA can account for updates in the basic event data as well as for trending and time dependent behaviors, including aging effects. Using systematic updating techniques, the fault tree can be re-evaluated with new information that can include information on defects and near failures. Actions can then be identified to maintain or replace necessary equipment to control the failure probability and risk. This use of FTA as a monitoring tool is common in the nuclear industry.

5. Use of FTA to minimize and optimize resources. This particular use of FTA is sometimes overlooked but it is one of the most important uses. Through its various importance measures, a FTA identifies not only what is important but also what is unimportant. For those contributors that are unimportant and have negligible impact on the top event, resources can be relaxed with negligible impact on the top event probability. In fact, using formal allocation approaches, resources can be re-allocated to result in the same system failure probability while reducing overall resource expenditures by significant amounts. In various applications, FTA has been used to reduce resource burdens by as much as 40% without impacting the occurrence probability of the top event. Software has been developed to help carry out these resource re-allocations for large systems.

6. Use of FTA to assist in designing a system. When designing a system, FTA can be used to evaluate design alternatives and to establish performance-based design requirements. In using FTA to establish design requirements, performance requirements are defined and the FTA is used to determine the design alternatives that satisfy the performance requirements. Even though system specific data are not available, generic or heritage data can be used to bracket performance. This use of FTA is often overlooked, but is important enough to be discussed further in a subsequent section.

7. Use of FTA as a diagnostic tool to identify and correct causes of the top event. This use of FTA as a diagnostic tool is different from the proactive and preventative uses described above. FTA can be used as a diagnostic tool when the top event or an intermediate event in the fault tree has occurred. When not obvious, the likely cause or causes of the top event can be determined more efficiently using the FTA power to prioritize contributors. The chain of events leading to the top event is identified in the

fault tree, providing valuable information on what may have failed and the areas in which improved mitigation could be incorporated. When alternative corrective measures are identified, FTA can be used to objectively evaluate their impacts on the top event re-occurrence. FTA can also be an important aid to contingency analysis by identifying the most effective actions to be taken to reduce the impact of a fault or failure. In this case, components are set to a failed condition in the fault tree and actions are identified to minimize the impact of the failures. This contingency analysis application is often used to identify how to reconfigure a system to minimize the impact of the component failures. Allowed downtimes and repair times can also be determined to control the risk incurred from a component failure.

As can be seen from the above, FTA has a wide variety of uses and roles it can play in decision-making. FTA can be used throughout the life cycle of the system from design through system implementation and improvement. As the system proceeds to the end of life, its performance can be monitored to identify trends before failure occurs. When consciously used to assist decision-making, the payoffs from FTA generally far outweigh the resources expended performing the analysis.

### **III.5 Fault tree construction**

A fault tree is a graphical representation of causal relations obtained when a system failure mode is traced backward to search for its possible causes. To complete the construction of a fault tree for a complicated system, it is necessary to first understand how the system functions. A system flow diagram (e.g. a Reliability Block Diagram) is used for this purpose, to depict the pathways by which materials are transmitted between components of the system.

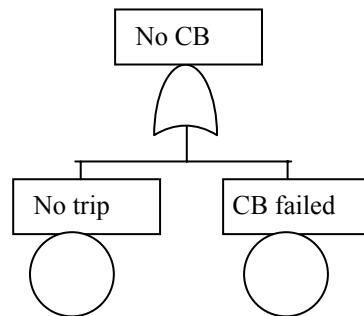
The first step in fault tree construction is then the selection of the system failure event of interest. This is called the top event and every following event will be considered in relation to its effect upon it.

The next step is to identify contributing events that may directly cause the top event to occur. At least four possibilities exist:

1. No input to the device.
2. Primary failure of the device (under operation in the design envelope, random, due to aging or fatigue).

3. Human error in actuating or installing the device.
4. Secondary failure of the device (due to present or past stresses caused by neighbouring components or the environments: e.g. common cause failure, excessive flow, external causes such as earthquakes).

If these events are considered to be indeed contributing to the system fault, then they are connected to the top event logically via an OR function and graphically through the OR gate.



**Figure III.1** Top and first level of a fault tree for a circuit breaker (CB) to trip

Once the first level of events directly contributing to the top has been established, each of them must be examined to decide whether it is to be further decomposed in more elementary events contributing to its occurrence. At this stage, the question to be answered is: is this event:

1. A primary failure?
2. Or is it to be broken down further in more primary failure causes?

In the first case, the corresponding branch of the tree is terminated and this primary event is symbolically represented by a circle. This also implies that the event is independent of the other terminating events (circles) which will be eventually identified and that a numerical value for the probability of its occurrence is available if a quantitative analysis of the tree is to be performed.

On the contrary, if a first level contributing event is not identified as a primary failure, it must be examined to identify the sub-events which contribute to its occurrence and their logical relationship.

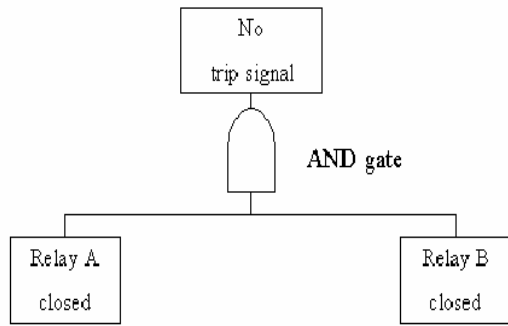


Figure III.2: AND function example for electrical system.

The procedure of analyzing every event is continued until all branches have been terminated in independent primary failures for which probability data are available. Sometimes, certain events which would require further breakdown can be temporarily classified as primary at the current state of the tree structure. These underdeveloped events are graphically represented by a diamond symbol rather than by a circle.

**Example: Failure of a mechanical holding latch.**

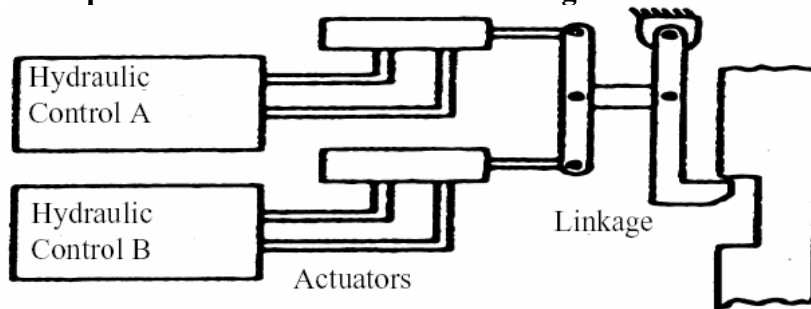


Figure III.3 schematic diagram of a mechanical holding latch.

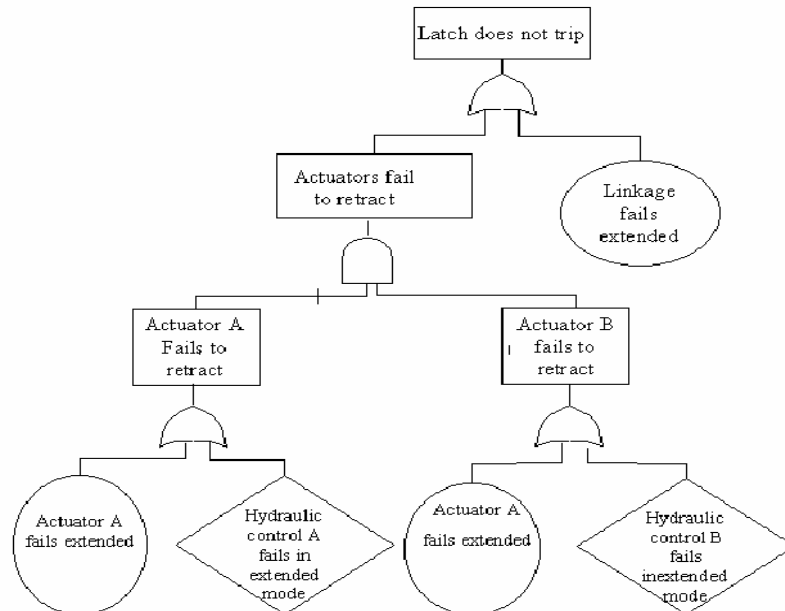


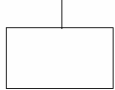
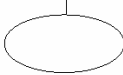

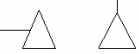








Figure III.4 fault tree for a mechanical holding latch.

Tables III.1 and III.2 report the symbols employed to represent the events and their Relationships in a fault tree. [10, 3]

	Event Symbol	Meaning of Symbols
1		Basic event with sufficient data
2		Undeveloped event
3		Event represented by a gate
4		Condition event used with inhibit gate
5		House event. Either occurring or not occurring
6		Transfer symbol

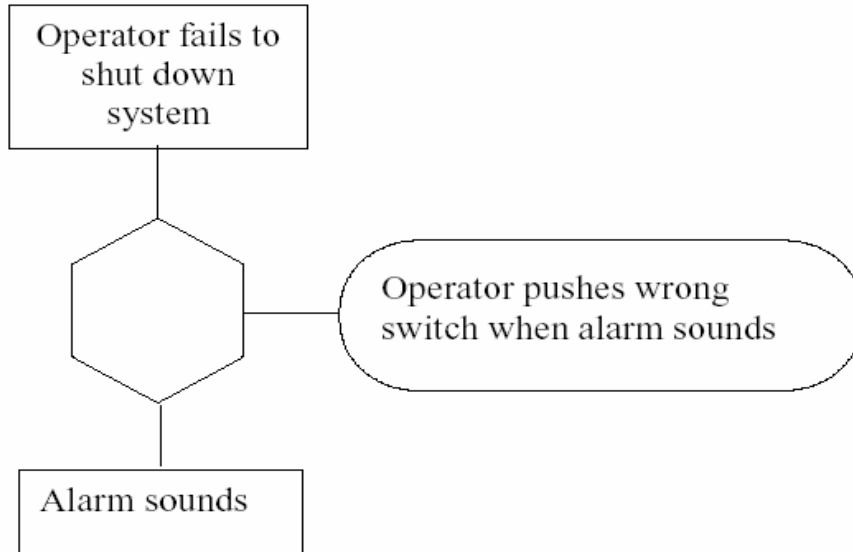
	Gate Symbol	Gate Name	Causal Relation
1		AND gate	Output event occurs if all input events occur simultaneously.
2		OR gate	Output event occurs if any one of the input events occurs.
3		Inhibit gate	Input produces output when conditional event occurs.
4		Priority AND Gate	Output event occurs if all input events occur in the order from left to right
5		Exclusive OR Gate	Output event occurs if one, but not both, of the input events occur.
6		m out of n gate (voting or sample gate)	Output event occurs if m out of n input events occur.

**Table III.1:** Event Symbols

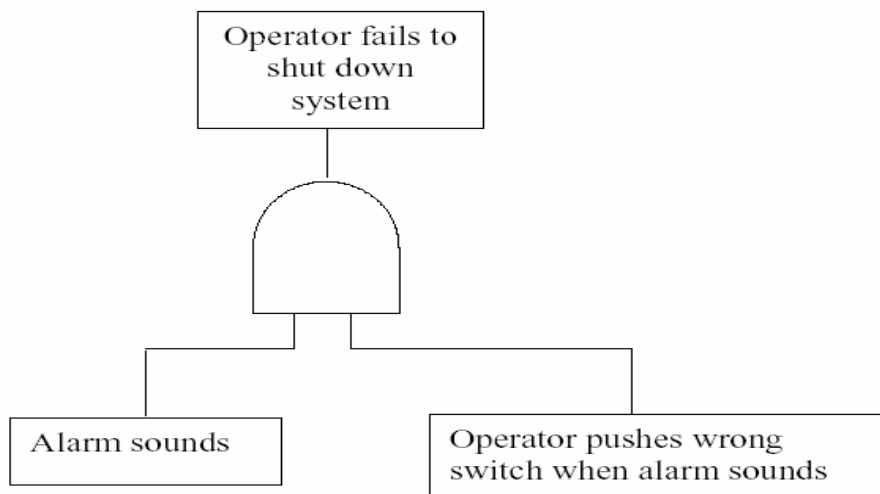
**Table III.2:** Gate Symbols

It is interesting to note that all the more complicated gate symbols can be constructed with the basic AND, OR and NOT symbols. Some examples follow.





**Figure III.5** Example of inhibit gate



**Figure III.6** Equivalent expressions to Fig. III.5

Actual construction of fault trees is an art as well as a science and comes only through experience. Below we report some useful guidelines [From H. E. Lambert, Systems Safety Analysis and Fault Tree Analysis. Lawrence Livermore Laboratory Rep. UCID-16238 (1973)]:

Rule I. State the fault event as a fault, including the description and timing of a fault condition at some particular time. Include:

- (a) What the fault state of that system or component is.
- (b) When that system or component is in the fault state.

Test the fault event by asking:

- (c) Is it a fault?

(d) Is the what-and-when portion included in the fault statement?

Rule2. There are two basic types of fault statements, state-of-system and state-of-component. To continue the tree:

(a) If the fault statement is a state-of-system statement, use

Rule3. (b) If the fault statement is a state-of-component statement, use Rule 4. Rule3. A state-of-system fault may use an AND, OR, or INHIBIT gate or no gate at all. To determine which gate to use. The faults must be the:

(a) Minimum necessary and sufficient fault events,

(b) Immediate fault events. To continue, state the fault events input into the appropriate gate.

Rule4. A state-of-component fault always uses an OR gate. To continue, look for the primary, secondary, and command failure fault events. Then state those fault events.

(a) Primary failure is failure of that component within the design envelope or environment.

(b) Secondary failures are failures of that component due to excessive environments exceeding the design environment.

(c) Command faults are inadvertent operation of the component because of a failure of a control element.

Rule5. No gate-to-gate relationships, i.e., put an event statement between any two gates.

Rule6. Expect no miracles; those things that would normally occur as the result of a fault will occur, and only those things. Also, normal system operation may be expected to occur when faults occur.

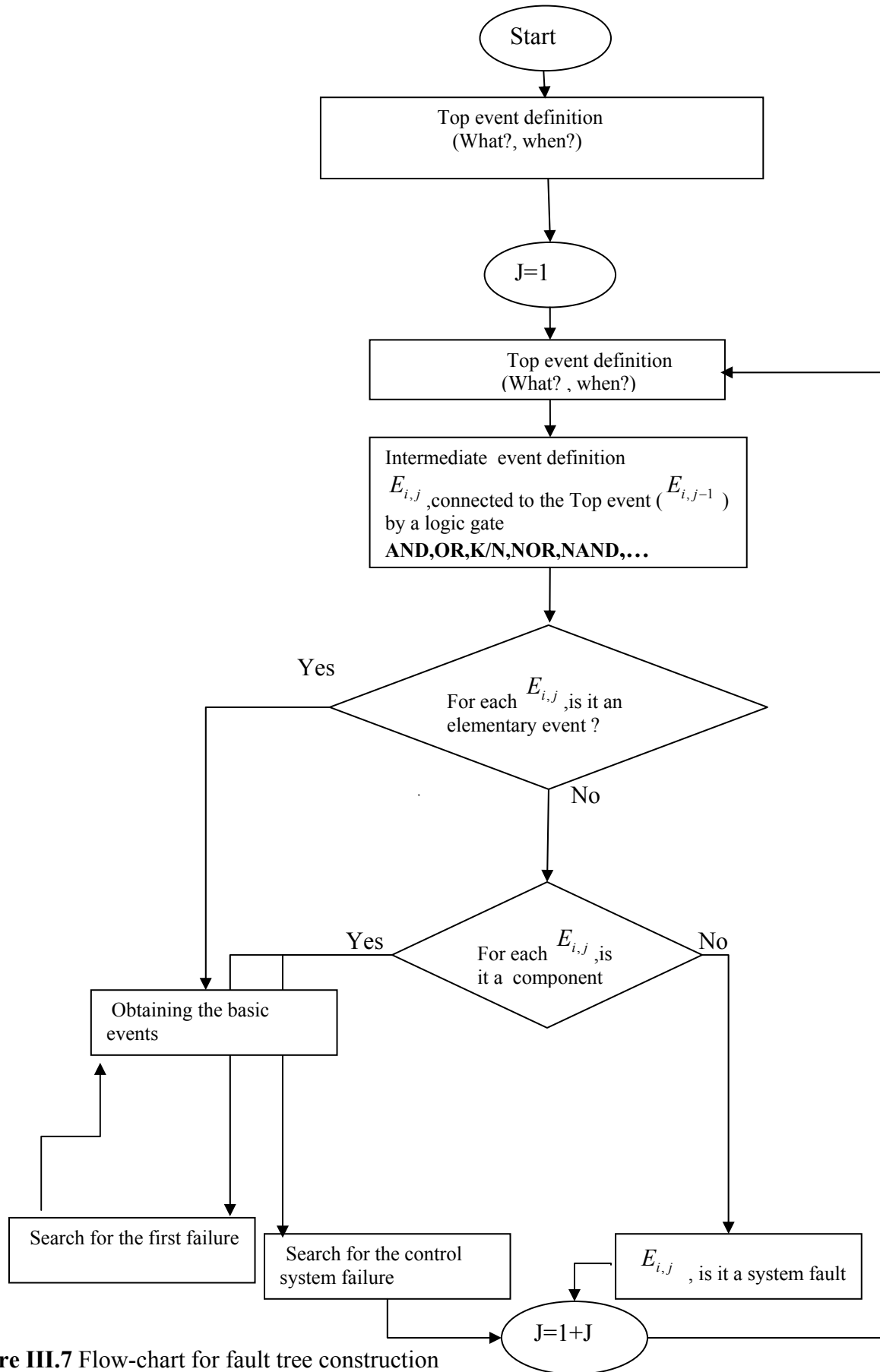
Rule7. In an OR gate, the input does not cause output. If any input exists, the output exists. Fault events under the gate may be a restatement of the output events.

Rule8. An AND gate defines a causal relationship. If the input events coexist, the output is produced.

Rule9. An INHIBIT gate describes a causal relationship between one fault and another, but the indicated condition must be present. The fault is the direct and sole cause of the output when that specified condition is present. Inhibit conditions may be faults or situations, which is why AND and INHIBIT gates differ.

Finally, the construction of a fault tree can be summarized according to the flow-chart shown in **Fig.III.7**; a Delphi software aided by a graphical interface is developed to model all the protection schemes for breaker-flashover and calculate their associated reliabilities. Using this software, the logical expression of each top event is represented graphically, moreover its associated probability is

calculated.

**Figure III.7** Flow-chart for fault tree construction

Using the presented Delphi-based software, a protective engineer could study and compare the relative reliability of various protective schemes for breaker-flashover failures. The fault-tree analysis method, reliability of different protective schemes against the flashover failures are analyzed and compared.

The fault tree is constructed for each protective design based on the elements of the studied protective scheme. The failure properties of these elements are lumped together by the fault tree to indicate the failure of the protective system.

Using the logical fault tree diagram, the unavailability of the protective system could be calculated. Different components of the system are either connected in series or parallel. When two components are in series, the correct operation of the system depends on availability of both of the components. Therefore, for a series system:

$$p(\text{System}) = p_i \times p_j$$

$$q(\text{System}) = 1 - p_i \times p_j = q_i + q_j$$

For a parallel combination of two components, it is sufficient that one of the components works properly so that the system would be available. Therefore,

$$p(\text{System}) = p_i + p_j$$

$$q(\text{System}) = 1 - p_i - p_j = q_i \times q_j$$

To calculate a system unavailability, we calculate the probability of occurrence of the top event for a fault tree logic diagram, series components are connected by OR gates and parallel components are connected by AND gates.

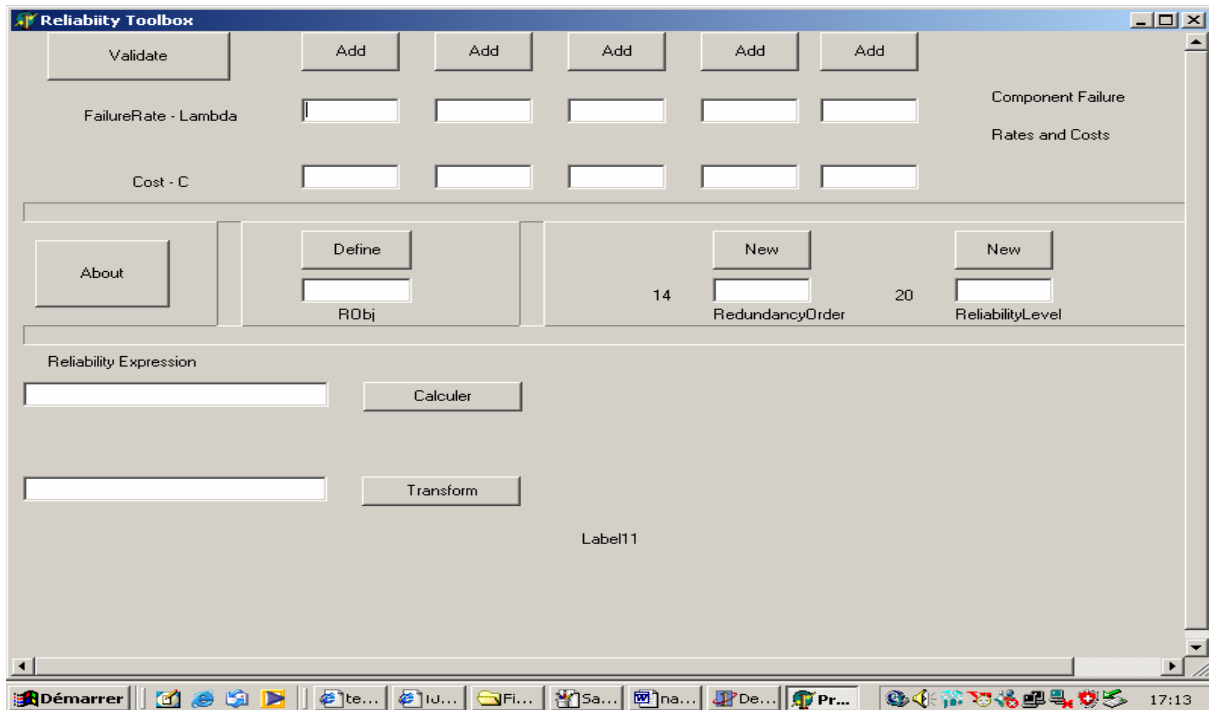
#### **Fault tree analysis software:**

Delphi-based software is developed to model different protection schemes and calculate their reliability. Using this software, different components and devices for each scheme are chosen and the unavailability of the scheme is calculated using fault tree method. The calculations are based on independent device failure rates. A failure in one device does not influence other components.

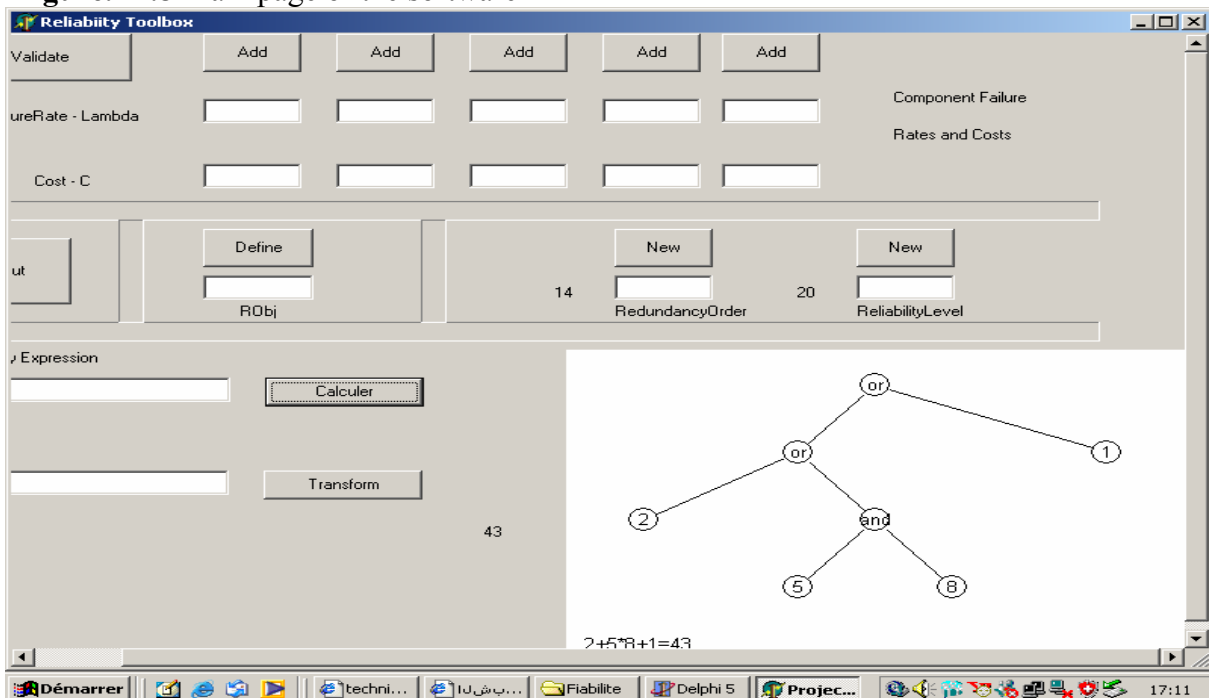
The main page of the software is shown in **FigIII.8** At the first step, input data failure rates should be entered by means of the Boolean expression.

Fault tree analysis (FTA) is an effective method through which reliability of a system could be calculated. The software provides a mathematical / graphical representation of combination of events which could lead to system operation failures. This method is used

for qualitative and quantitative analysis of the failures modes of critical systems. By means of Boolean logic, fault tree represents the relationship between causes, e.g. failures (basic event) and undesired hazardous event (top event). The Boolean logic is given in a graphical representation.



**Figure.III.8** Main page of the software



**figureIII.9** Fault tree construction and visualisation

### III.5.1 Qualitative analysis: coherent structure functions and minimal cut sets:

A fault tree can be described by a set of Boolean algebraic equations, one for each gate of the tree. For each gate, the input events are the independent variables and the output event is the dependent variable. Utilizing the rules for Boolean algebra it is then possible to solve these equations so that the top event is expressed in terms of sets which involve only the primary events.

When dealing with a Boolean event  $E_j$  we can introduce an indicator variable  $X_j$  which is equal to 1 if the event is true and 0 if it is false. If the system is considered from the point of view of reliability then  $X_j = 1$  indicates a system success and  $X_j = 0$  a failure; vice versa from the point of view of safety. A top event  $X_T$  is then a Boolean function of Boolean variables  $X_1, X_2, \dots, X_n$  describing the states of the various components of the system:

$$X_T = \Phi(X_1, X_2, \dots, X_n) \quad (3.1)$$

Such function is called a switching or structure function and it incorporates all the causal relations among the events which lead to the top. It maps an  $n$ -dimensional vector  $\underline{X} = (X_1, X_2, \dots, X_n)$  of 0's and 1's onto 0 or 1. For example, looking at a simple series system from the reliability viewpoint, we have that its success occurs when all its components are in a success state. From the rules of Boolean algebra, the corresponding structure function is:

$$X_T = \prod_{j=1}^n X_j \quad (3.2)$$

For a parallel system, at least one of the components must be in the success state for the system to be successful. Correspondingly, we have:

$$X_T = 1 - (1 - X_1)(1 - X_2) \cdots (1 - X_n) = \prod_{j=1}^n X_j \quad (3.3)$$

Obviously, for a given system there are various forms which can be used to write the structure function. The task that we wish to undergo is that of using the rules of Boolean algebra to reduce a structure function to its most simplified equivalent version. First of all we introduce the concept of fundamental product which is a product containing all of the  $n$  input variables, complemented or not. For  $n$  variables there are  $2^n$  such products; for example, for  $n = 3$ , we have:



$$X_1X_2X_3, X_1X_2\bar{X}_3, X_1\bar{X}_2X_3, \bar{X}_1X_2X_3, \bar{X}_1X_2\bar{X}_3, \bar{X}_1\bar{X}_2X_3, X_1\bar{X}_2\bar{X}_3, \bar{X}_1\bar{X}_2\bar{X}_3$$

Clearly a fundamental product is 1 if and only if all its variables are 1.

An important theorem states that a structure function can be written uniquely as the union of

the fundamental products which correspond to the combinations of the variables which render the function true (i.e.,  $\Phi=1$ ). This is called the canonical expansion or disjunctive normal form of  $\Phi$ .

Using the rules of Boolean algebra (see Table below), the canonical expansion can be simplified further to obtain an irreducible expression of the structure function in terms of minimal cut sets.

Table *Some Rules of Boolean Algebra for Events"*

Word description	Rules
1. Commutative Law	a. $XY = YX$ b. $X + Y = Y + X$
2. Associative Law	a. $X(YZ) = (XY)Z$ b. $X + (Y + Z) = (X + Y) + Z$
3. Idempotent Law	a. $XX = X$ b. $X + X = X$
4. Absorption Law	a. $X(X + Y) = X$ b. $X + XY = X$
5. Distributive Law	a. $X(Y + Z) = XY + XZ$ b. $(X + Y)(X + Z) = X + YZ$
6. Complementation*	a. $X\bar{X} = \phi$ b. $X + \bar{X} = \Omega$ c. $\bar{\bar{X}} = X$
7. De Morgan's Theorems	a. $\overline{XY} = \bar{X} + \bar{Y}$ b. $\overline{X + Y} = \bar{X}\bar{Y}$
8. Unnamed relationships but frequently useful	a. $X + \bar{X}Y = X + Y$ b. $\bar{X}(X + Y) = \bar{X}Y$

Table III.3 Boolean algebra rules.

\*The universal event  $\Omega$  is sometimes denoted by  $/$ , and the null event  $\phi$  is sometimes denoted by 0.

A physical system would be quite unusual (or perhaps poorly designed) if improving the performance of a component (that is, replacing a failed component by a functioning one) caused the system to deteriorate (that is to change from the success to the failed state). Thus, we restrict consideration to structure functions that are monotonically increasing in each input variable. These structure functions do not contain complemented variables; they are called coherent and can always be expressed as the union of fundamental products. The main properties of a coherent structure function are:

1.  $\Phi(1)=1$  if all the components are in their success state, the system is successful;
2.  $\Phi(0)=0$  if all the components are failed, the system is failed;
3.  $\Phi(X) \geq \Phi(Y)$  for  $X \geq Y$  if  $\Phi(1) = 1$  and a failed component in  $Y$  is repaired in  $X$ , this cannot cause the system to fail ( $\Phi(Y)=0$ ): if the system in  $Y$  was failed, in  $X$  it can either remain failed or repair; if the system in  $Y$  was successful, the additional repair can only make it maintain its safe status.

Coherent structure functions can be expressed in reduced expressions in terms of minimal path or cut sets. A path set is a set  $X$  such that  $\Phi(X) = 1$ ; a cut set is a set  $X$  such that  $\Phi(X) = 0$ . Physically, a path (cut) set is a set of components whose functioning (failure) insures the functioning (failure) of the system.

A minimal path (cut) set is a path (cut) set that does not have another path (cut) set as a subset.

Physically, a minimal path (cut) set is an irreducible path (cut) set: failing (repairing) one element of the set fails (repairs) the system. Therefore, removing one element from a path (cut) set makes the set thereby obtained no longer a path (cut) set.

Once the path (cut) sets are identified, the system structure function can be expressed as the union of the path (cut) sets: this constitutes a unique and irreducible form of the coherent structure function of the system.

From this analysis we see that any fault tree can be equivalently written in a form with an OR gate in the first level below the top combining all the minimal cut sets, each one represented by an AND gate intersecting all the elements comprising the given minimal cut set.

For trees of system with relatively few components, the minimal cut sets can be identified by inspection. Most often, however, such an approach is very inefficient, if possible at all, since the number of minimal cut sets increases very rapidly, as the complexity of the tree increases.

Therefore, a more systematic approach should be undertaken by which after writing the Boolean equations for each gate, Boolean algebra is used to solve the top event structure function in terms of the cut sets; using again Boolean algebra one can then eliminate all the redundancies in the events to obtain the minimal cut sets. Several computerized approaches exist to perform this task.

After the minimal cut sets have been obtained, the qualitative analysis is complete and the failure modes contributing to the top event have been identified. The analysis provides us with some indications on the criticality of the various components: those appearing in minimal cut sets of low order (number of primary events constituting the cut set) and those most frequently appearing in the various cut sets are good candidate to be critical for the system safe operation. Two general rules of thumb for judging the importance of a minimal cut set are:

1. The importance of a minimal cut set is inversely proportional to its order
2. Any one-event minimal cut set should be avoided by re-design if possible.

### **III.5.2 Quantitative analysis [10]**

Quantitative analysis of the fault tree consists of transforming its logical structure into an equivalent probability form and numerically calculating the probability of occurrence of the top event from the probabilities of occurrence of the basic events. The probability of the basic event is the failure probability of the component or subsystem during the mission time of interest.

From the definition of the structure function  $\Phi$  as a function of the indicator variables of the basic events  $X_1, X_2, \dots, X_n$ , we see that the structure function is itself an indicator variable which is equal to 1 when the top event is verified and 0 otherwise. Consequently we may write, for the probability of the top event:

$$(3.4) \quad P(\Phi(X)=1) = E[\Phi]$$

Where  $E[.]$  is the expectation operation. Given the expression of the structure function  $\Phi$  in terms of the indicator variables of the basic events, it is possible to write the probability (3.5) in terms of the probability values of the independent basic events,  $P(X_i=1) = E[X_i]$ .

Consistent with what previously said concerning the qualitative analysis of fault trees, there

exist two approaches for calculating the probability of the top event from the probabilities of the basic events.

If the fault tree is not solved for the minimal cut sets, then the probability of the top event can be calculated by hand, provided that the size and complexity of the tree are not too large.

This is done proceeding in an orderly fashion from the bottom to the top of the tree and computing at each gate the probability of the output from the probabilities of the input events, using the laws of probability corresponding to that gate structure (AND, OR, etc.). This can be “automatically” done through eq. (3.4). For example, the probability of the output  $Y$  of an AND gate with two input events  $X_1$ ,  $X_2$ , with probability  $P_1$  and  $P_2$  respectively, is

$$P(Y=1) = E[X_1 X_2] = E[X_1] E[X_2] = P_1 P_2 \quad (3.5)$$

While for the output of an OR gate,

$$\begin{aligned} P(Y=1) &= E[(1-(1-X_1)(1-X_2))] = E[X_1 + X_2 - X_1 X_2] \\ &= E[X_1] + E[X_2] - E[X_1 X_2] = P_1 + P_2 - P_{12} \end{aligned} \quad (3.6)$$

where  $P_{12}$  is the probability of the joint event  $X_1 X_2 = 1$ .

On the contrary, if a qualitative analysis has been performed to determine the system minimal cut sets  $M_1, M_2, \dots, M_{mcs}$ , by definition the probability of each of them is the probability of the intersection of the independent basic events comprising that minimal cut set, i.e.,

$$P(M_i) = P(M_1^i) \cdot P(M_2^i) \dots \quad i=1, 2, \dots, mcs \quad (3.7)$$

Where the product is extended to all the events comprising  $M_i$ . By definition, the system structure function is the intersection of the  $mcs$  minimal cut sets:

$$\Phi(X) = I - (I - M_1) \cdot (I - M_2) \cdot \dots \cdot (I - M_{mcs}) = \prod_{j=1}^{mcs} M_j \quad (3.8)$$

and the probability of the top event is

$$\begin{aligned} P[\Phi(X) = 1] &= E \left[ \sum_{j=1}^{mcs} M_j - \sum_{i=1}^{mcs-1} \sum_{j=i+1}^{mcs} M_i M_j + \dots + (-1)^{mcs+1} \prod_{j=1}^{mcs} M_j \right] \\ P[\Phi(X) = 1] &= E \left[ \left[ \sum_{j=1}^{mcs} M_j \right] - E \left[ \sum_{i=1}^{mcs-1} \sum_{j=i+1}^{mcs} M_i M_j \right] + \dots + (-1)^{mcs+1} E \left[ \prod_{j=1}^{mcs} M_j \right] \right] \\ P[\Phi(X) = 1] &= \sum_{j=1}^{mcs} P[M_j] - \sum_{i=1}^{mcs-1} \sum_{j=i+1}^{mcs} P[M_i M_j] + \dots + (-1)^{mcs+1} P \left[ \prod_{j=1}^{mcs} M_j \right] \end{aligned} \quad (3.9)$$

For two minimal cut sets, the formula gives the well-known result,

$$P[\Phi(X) = 1] = P[M_1] + P[M_2] - P[M_1 M_2] \quad (3.10)$$

It can be shown that the following upper and lower bounds to eq. (3.10) hold:

$$\begin{aligned} P[\Phi(X) = 1] &\leq \sum_{j=1}^{mcs} P[M_j] \\ P[\Phi(X) = 1] &\geq \sum_{j=1}^{mcs} P[M_j] - \sum_{i=1}^{mcs-1} \sum_{j=i+1}^{mcs} P[M_i M_j] \end{aligned} \quad (3.11)$$

In reliability calculations basic events are typically rare (low probability events), so that the

probability of high order events is very small: therefore, one can approximate using the first of the 3.12 (*rare-event approximation*):

$$P[\Phi(X) = 1] \approx \sum_{j=1}^{mcs} P[M_j] \quad (3.12)$$

### III.6 Dependability evaluation of methods for breaker-flashover protection.

#### III.6.1 Fault tree analysis of different flashover-protection methods. [7]

##### III.6.1.1 Fault Tree Methodology and Input Data

We use fault tree reliability analysis to numerically evaluate security and dependability, and quantitatively compare different flashover protection methods. This method is easy to apply, and its use for protection and automation reliability estimates has been previously documented [6] [8]. The scheme failure of concern is called the top event. The probability that the scheme fails for the top event is a combination of the failure

probabilities of the components in the scheme. We use AND and OR gates to represent combinations of failure probabilities. For an OR gate, any inputs to that OR gate can contribute to scheme failure. Total failure probability is the sum of the failure probabilities of input events. For an AND gate, any inputs to that gate must fail together to cause scheme failure. The upper level probability for scheme failure from an AND gate is the product of input probabilities.

We can use the device failure rate to estimate the failure probability for each device in the scheme. One industry practice is to provide failure rates as Mean Time Between Failures (MTBF). MTBF could be based on field failure data or on assumptions about complexity and exposure of equipment. If we have 50 auxiliary relays and only one such relay fails per year, we can assume a failure rate of 1/50 failure per year or an MTBF of 50 years from field experience. If we have 1000 units, we can expect  $1000 \cdot 1/50 = 20$  failures per year. Some communications equipment vendors, however, if they estimate failure rates based upon complexity, could publish an MTBF of 80 years.[1]

Failure rates are useful for predicting maintenance cost or the probability of security failure, but they do not tell us whether a device will be available when called upon to clear a fault. For dependability estimation, we should use unavailability, that is, the fraction of time a device cannot work when needed.

Unavailability, as calculated in the following equation, provides us with this information.

$$q = \lambda T = T / \text{MTBF} \quad (3.13)$$

Where:

$q$  is unavailability;

$\lambda$  is failure rate;

$T$  is average downtime per failure;

MTBF is mean time between failures;

Each failure causes downtime,  $T$ . Therefore, the system is unavailable for time  $T$  out of total time MTBF, and  $q$  indicates the fraction of time the system is not available. It is unitless. If a multifunction IED has self-tests and a monitored failure alarm, we could easily detect a failure on this device. Detection could take some seconds, but for total  $T$  we may consider two days for detection, analysis of the failure, and repair or replacement before the device is again in service and useful. Unavailability with this example:

T = 2 days with self-test and alarm

MTBF = 100 years

$q = 2 / (100 \cdot 365) = 0.0000548$  unavailability or 0.02 days/year

One weakness of several protection or control schemes is the dependency on breaker auxiliary relays. MTBF could work well for high-quality auxiliary relays, for example 200 years, but T is always large because of a lack of automatic supervision. Failure of an auxiliary relay could go unnoticed until the next maintenance period or until operation of that relay is required. If the maintenance or testing period is every two years, a failure could occur the day following a maintenance test or one day before the next period, an average time of one year. For this example:

T = 1 year without self-test and 2 years maintenance period

MTBF = 200 years

$q = 365 / (200 \cdot 365) = 0.005$  unavailability or 1.825 days/year

The result is 91 times worse than the example with the multifunction IED, even considering the much better MTBF.

Unavailability gives direct information about the probability that a device on the scheme will fail and contribute to scheme failure to trip when needed (dependability failures). From references [50] and [45], we obtain unavailability or MTBF estimations for several devices used in flashover schemes, and we make our own estimations for the rest of them. These numbers, although the approximations are subject to dispute, provide valuable information for checking the degree of magnitude improvements and the impact of automatic supervision and alarms, redundancy, or other changes on the scheme configuration. Some of them are based on field statistics and more precise models could be built using more field data. We would greatly appreciate any failure rate data that utilities could provide to us in order to refine these models.

Devices Basic Events	MTBF	T	Unavailability• 10 <sup>-6</sup>
Current Transformers	500 years	2 days	11
Potential transformers with loss of secondary Potentials supervision or PTs used for SCADA Measuring	125 years	2 days	44
52a breaker auxiliary relay false open	200 years	1 year	5000
52a breaker auxiliary relay false close	800 years	1 year	1250
52b breaker auxiliary relay false open	800 years	1 years	1250
52b breaker auxiliary relay false close	200 years	1 year	5000
Auxiliary relay with automatic supervision and alarm .(52a contradicts current or 52a and 52b coincidence or 52a contradicts voltage)	200 years	2 years	27
Control wiring connection point(like close signal or 52a).Tested at commission but without automatic supervision	5, 000 years	1 years	200
Monitored CD battery and charger	100 years	1 day	27
Multifunction relay (IED), dependability-related Failures	175 years	2 days	31
Multifunction relay (IED), security-related Failures	2000 years. Failure rate 0.0005 per relay per year		
Human error per setting , dependability-related failures		Indefinite	7.75
Human error per setting , security-related failures	4000 years. Failure rate 0.00025 per setting per year		

**Table III.4** Unavailability and MTBF Indices for Devices Used in breaker Flashover protection Schemes [7]



1 Reference [50] uses the same MTBF and  $q$  for CTs and PTs. Our own experience shows that secondary circuit PT failures are more common than CT failures because of some factors. CT failure consequences to personnel and equipment security are greater and field personnel have much more care with them. PT secondary is protected by fuses or molded case circuit breakers that mean an extra point of failure. We use a factor of 4 to reflect this experience.

2 Some panel factory statistics show that wiring points have 1 failure per about 500 connection points after the first point-to-point continuity check. After functional testing, this failure rate decreases 100 times. Then a 1/50,000 failure rate after testing when the scheme is new and tested is a good estimation. After years of service a control wiring could fail for some other reason; we increase by a 10 times factor to get 5000 MTBF per wiring point.

We use these numbers to analyze security and dependability for each breaker-flashover scheme described earlier. Our top event is “Protection Fails to Clear Breaker-Flashover Failure in Prescribed Time” for dependability analysis. We shorten this to “Failure to Trip During Flashover” in our fault trees and we use unavailability numbers.

Our top event is “Protection Trips 86BF and Bus Incorrectly” for security analysis and we use failure rate numbers. This is because unexpected operations or false trips typically occur at the instant a component fails or very soon afterwards.

For some data on multifunction relays, we separate failure rates and unavailability numbers for security-related failures and for dependability-related failures. CFE observed 57 damaged relays over a population of about 10,000 units with similar technology, resulting in 175 years MTBF(1998 data). Of these 57 damaged relays, only five trip incorrectly; all other failures disable the relay and alarm. For dependability-related failures, we use MTBF = 175 years and 2 days downtime. For security-related failures, relay failure rate is 5/10000, or MTBF = 2000 years. For dependability, human settings-error time to detect is indefinite. Our experience with multifunction programmable relays shows that unavailability is similar to IED hardware failures. We estimate that it is equal to relay hardware unavailability. If Method E has 4 settings and is the most complex one for breaker flashover, we can assign 1/4 of this unavailability per setting ( $7.75 \cdot 10^{-6}$ ), as a way to weight settings complexity for comparison purposes.

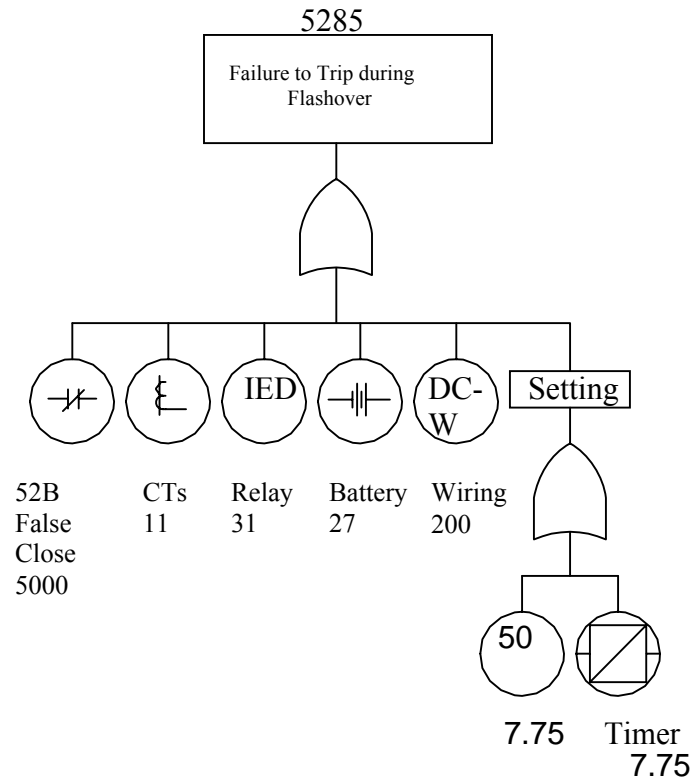
For security-related settings errors, the time to detect is much faster because load changes, close or trip operations, or external faults could cause incorrect trip and error detection very soon after relay commission. The experience shows that the security-related settings-error failure rate is higher than security-related relay hardware failures. We estimate a failure rate twice the failure rate of relay hardware per the Method E scheme, 1/4 per setting (0.00025 failure rate).

For breaker auxiliary relays, we can also separate the failure rate for open incorrect indication and for close incorrect indication. If we assume that 52a has a greater probability of false open breaker indication than of false close indication, and that 52b is the opposite, we can account for security and dependability changes with 52a to 52b change. We assume a factor of 4 times between these two opposite conditions.

### **III.6.1.2 Fault Tree for Method A. Residual Current and 52b.[7]**

#### **Dependability**

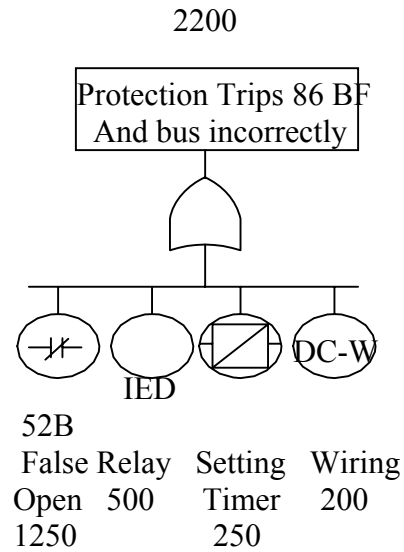
The fault tree shows components that may contribute to dependability failure of this method. For wiring unavailability, the authors consider only input signal 52b. They do not consider any trip circuit between the breaker flashover scheme and 86BF or between 86BF and breakers, because these will be common to all the schemes. Our failure to trip during flashover considers all the variables related to the scheme for comparison purposes, but does not consider 86BF or other breakers in the bus failing to clear the fault.



**Figure III.10** Unavailability  $\cdot 10^{-6}$  for Method A without Automatic 52a Supervision

#### Security

For security we consider only failure rates of the breaker auxiliary relay, dc wiring, multifunction relay, and timer setting. We consider that the CTs, PTs, battery, and 50-element setting cannot fail in a way that causes a false trip. An external ground failure must occur to cause scheme A to trip if 52b remains closed while the breaker is closed. If 52b does not have any kind of supervision, we assume that it could be closed enough time to coincide with ground failure. If we also assume a maintenance period of two years and downtime  $T = 1$  year, we can assume that it is almost certain that an external ground failure will occur and we can use directly the 52b failure rate.



**Figure III.11** security Failure Rate  $\cdot 10^{-6}$  for Method A Without Automatic 52a Supervision

#### Using Breaker Auxiliary 52a Instead of 52b in Method A

We evaluated changing to 52a instead of 52b for Method A. As we expected, dependability improves and security decreases. Using Method A with 52a instead of 52b, dependability is

$1,535 \cdot 10^{-6}$  and security is  $5950 \cdot 10^{-6}$ .

#### Adding Automatic Breaker Auxiliary Supervision to Method A

If we add any kind of automatic supervision to 52a or 52b and its dc wiring, for example, 52a contradicts 52b, or 52a contradicts current, a 52a failure will be quickly detected and fixed. If we assume downtime of two days, unavailability decreases from  $1250 \cdot 10^{-6}$  to  $27 \cdot 10^{-6}$ . The probability of dependability failure decreases from  $1535 \cdot 10^{-6}$  to  $312 \cdot 10^{-6}$ .

With this same assumption, we can estimate that the probability that an external ground fault will coincide with 52a false close indication is very low. If we use directly the 52a failure rate for the case without automatic supervision and with a one-year downtime, we can assume that with automatic supervision that probability is  $2/365$  times smaller. An external ground fault must occur in the two days following a 52a failure to cause a false

trip. The improvement in security is outstanding; the probability of a false trip decreases from  $5950 \cdot 10^{-6}$  to  $778 \cdot 10^{-6}$ .

### III.6.1.3 Fault Tree for Method B, Phase Current and 52a Per Phase

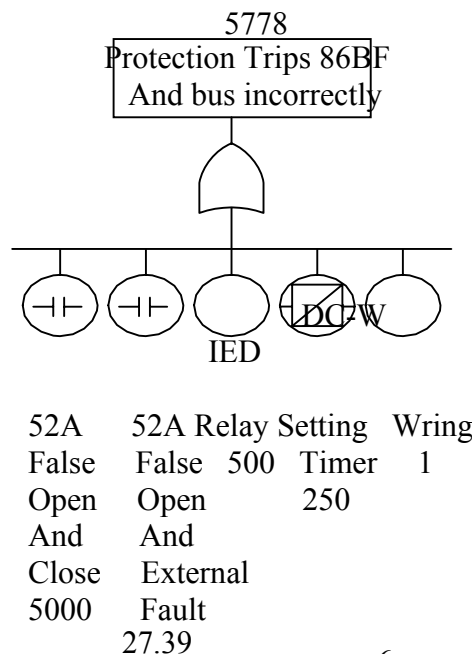
#### Dependability

Dependability for this method will be exactly the same as that of Method A with three advantages:

- Directly targets the failed phase
- Covers the rare case of three-phase flashover
- Could be applied to single-pole-trip breakers

#### Security

This method is not applied in practice because security is very low. We need to take into consideration the same conditions we use for Method A, plus the probability of a 52a false open indication or a normal breaker close with load. Although we use automatic supervision for the breaker auxiliary, if 52a fails during the breaker close, it will cause a false trip. We use the 52a failure rate directly to estimate the probability of security failure with this scheme.



**Figure III.12** Security Failure Rate  $\cdot 10^6$  for Method B with Automatic 52a Supervision

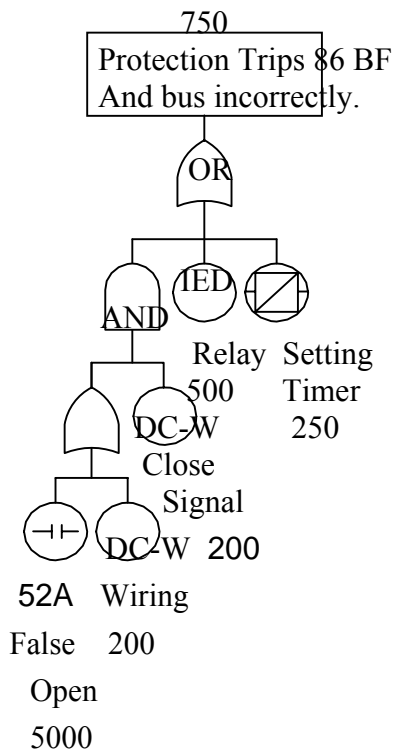
### III.6.1.4 Fault Tree for Method C, Close Monitoring and Coincidence Timers

## Dependability

Method C dependability is the same as that with Method A or B. We add close signal, coincidence timers, and some logic. Extra logic and timers (without more settings) do not increase unavailability because we are evaluating only multifunction digital relays and this extra component's unavailability is included in relay unavailability. Close signal could not fail in a way that causes a dependability failure. Our result is the same fault tree and  $1535 \cdot 10^{-6}$  unavailability without 52a automatic supervision or  $312 \cdot 10^{-6}$  unavailability with it.

## Security

Method C can be applied to single-pole-trip breakers, covers three-phase flashover, and is secure, because it will not fail and trip the bus incorrectly unless both 52a and the close signal fail simultaneously during a close operation. It will not trip if 52a fails later because of coincidence timers. Automatic 52a supervision becomes less important because 52a failure is no longer the most probable cause of security failure.



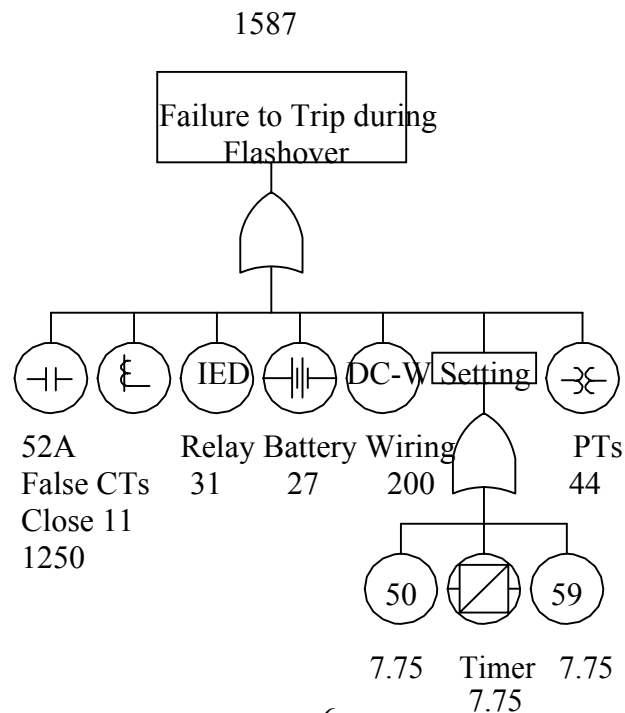
**Figure III.13** Security Failure Rate  $\bullet 10^6$  for Method C without Automatic Supervision

### III.6.1.5 Fault Tree for Method D, Close Monitoring, Coincidence Timers, and Live- Voltage Supervision

#### Dependability

Method D dependability is lower than other methods. The fault tree is similar to that for Method C, but we add two more unavailability components: PTs and one more setting. This is results in

$1587 \cdot 10^6$  unavailability without 52a automatic supervision or  $364 \cdot 10^{-6}$  with it.



**Figure III.14** Unavailability  $\cdot 10^6$  for Method D without Automatic 52a Supervision

#### Security

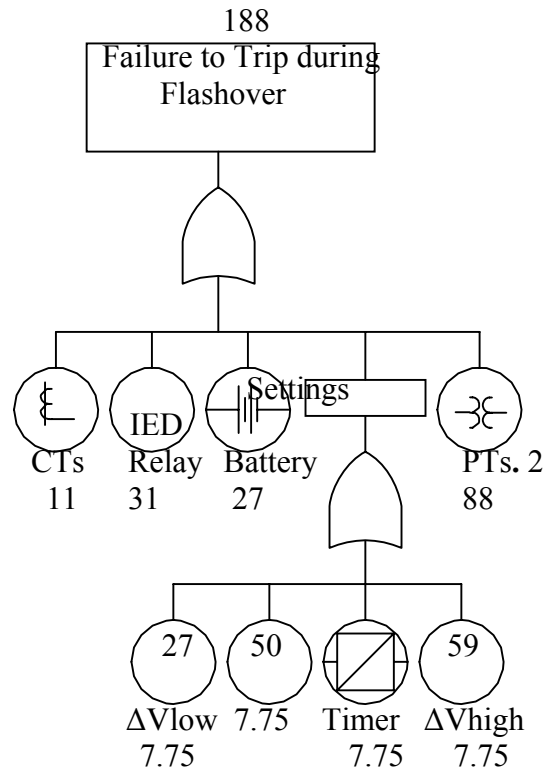
The Method D security failure rate fault tree is the same as that of Method C. Live voltage supervision does not add any security because settings must be too low and it will be active almost all the time, with normal load and with several fault conditions. On the other hand, there are no security related failures caused by this element.

### III.6.1.6 Fault Tree for Method E, Voltage at Both Sides of the Breaker

#### Dependability

This method adds the probability of failure caused by PT unavailability and by more settings, but eliminates breaker auxiliary and dc wiring related unavailability. The total

result is that this method shows the best dependability if we consider that both sets of three-phase PTs have some method of automatic supervision and a downtime of two days. This supervision could be in the form of alarms as 52a contradicts voltage difference, as current contradicts voltage difference, or from other methods based on changes of voltage or current-sequence components.

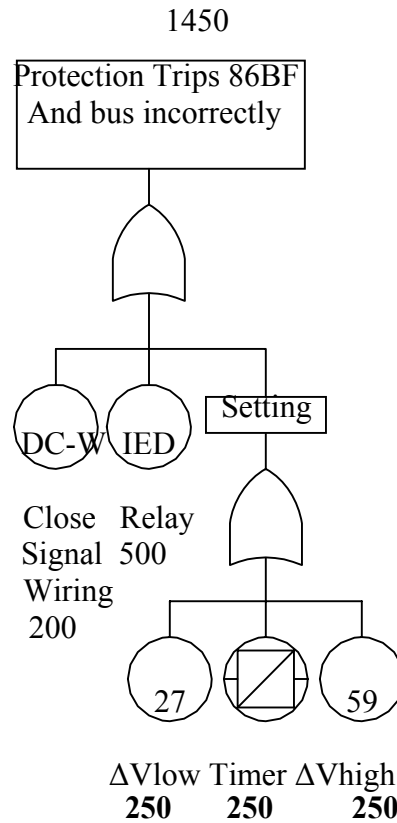


**Figure III.15** Unavailability  $\cdot 10^6$  for Method E

### Security

One source of failure rate in this method is a failure of the close signal. If this signal fails and there is a normal close, it will trip the bus incorrectly. Fortunately, this is a very simple component and we assume its failure rate to be equal to any other CD wiring point. This method also adds more settings.





**Figure III.16** Security Failure Rate  $\cdot 10^{-6}$  for Method E

**Table III.4** Results of Comparison between Breaker-Flashover Methods

Breaker-flashover Protection method	unavailability. $10^{-6}$ of (Pr. dependability F.	Security Failure Rate. $10^{-6}$	Observation
A, residual current and Breaker auxiliary contact 52b	5285 (worst)	2200	Do not apply 3 phase flashover or single pole trip and reclose breakers
A, residual current and Breaker auxiliary contact 52a	1535	5950(worst)	Do not apply 3 phase flashover or single pole trip and reclose breakers
A with automatic 52a Supervision and alarm	312	778	Do not apply 3 phase flashover or single pole trip and reclose breakers
B, phase current and Breaker auxiliary contact/phase	1535	5950(worst)	
B, with automatic 52a Supervision and alarm.	312	5778	

C, phase current , breaker Auxiliary; close Monitoring and coincidence timers	1535	750(best)	
C, with automatic 52a supervision and alarm	312	750(best)	Security does not depend on downtime of 52 a
D, same as C with live voltage supervision	1587	750(best)	
D, with automatic 52a supervision and alarm	364	750(best)	
E, phase current ,voltage difference, and close monitoring	188(best)	1450	Needs three-phase voltage on sides of the breaker

**Table III.4** Results of Comparison between Breaker-Flashover protection Methods

### III.6.2 MONITORING AND PREDICTIVE MAINTENANCE OF BREAKERS

Comprehensive breaker protection is needed in every breaker, and flashover-protection logic is a must in breakers used to synchronize generators or systems, or in long high-voltage lines. An important question is whether we can decrease the number of breaker failures or detect some problems before they cause a major failure. Present technology permits the same intelligent electronic device (IED) that is used as a multifunction protective relay to be used as a real-time monitoring and maintenance tool. [7].

As a performance monitor, this device could alarm for several abnormal conditions that can give us an early indication that there is a problem in the breaker or in the protection-associated scheme signals. Some of these important alarms are:

- Slow electrical trip or close alarm, per phase, measuring the time between the close or trip control signals and current interruption. This slow operation could mean mechanical or internal isolation problems.
- Slow mechanical trip or close alarm, per phase, measuring the time between the close or trip control signals and 52a or 52b breaker contacts. This slow operation could mean mechanical or control circuit problems.
- Current that contradicts breaker contact 52a indication (52a open and current flow).

This particular alarm increases the security of flashover methods A and C. It also

increases the security of standard breaker-failure schemes that use 52a instead of current, which is normal in generation applications.

- Voltage difference between the terminals of a closed breaker. This alarm increases the security and dependability of flashover Method E with six PTs, because it can indicate problems such as loss of secondary potential, as well as problems with the 52a signal for scheme A or C.
- Pole scatter during close or trip operations, alarming if the time between the 52a change in the first pole and the 52a in the last pole is longer than a threshold.
- Pole discrepancy, looking for conditions where 52a (or current) indicates one or two poles closed, with one or two poles open. IEEE 37.102 suggests pole discrepancy could protect against flashover because one phase has current and the other two do not. We do not recommend this approach because it requires a long delay, and current thresholds would be difficult to set. Some utilities use pole discrepancy with a one-to-two second timer and only trip the failed breaker, but this does not work for flashover protection.

Contact wear information, important from the maintenance point of view, is not just the number of operations. To provide good contact wear information, an IED needs to measure both the number of operations and the current per pole. Precise information helps to program maintenance as needed for the breaker to optimize maintenance resources, improve power system reliability, and increase circuit-breaker life expectancy.

### **III.7 Conclusion**

Although actual construction of fault trees is an art as well as a science and comes only through experience, fault tree analysis is a widely adopted tool for safety and risk analyses. Some of its recognized advantages are:

1. Straightforward modelling via few, simple logic operators;
2. Directing the analysis to ferret out failures;
3. Focus on one top event of interest at a time;
4. Pointing out the aspects of the system important to the failure of interest;
5. Providing a graphical communication tool whose analysis is transparent;
6. Providing an insight into system behaviour;
7. Minimal cut sets are a synthetic result which identifies the critical components.

## **Chapter.IV**

### **Dependability parameters modeling &Improvements.**

## **Chapter.IV Dependability parameters modeling &Improvements**

### **IV.1 INTRODUCTION**

The obtaining of dependability parameters of a system during its life cycle presents a certain interest for inventors and complex system operators. In most cases, studies are achieved using exponential distributions, failure rates and repairs being supposed constant: the behavior of these systems is generally described by Markovian equations. From a practical point of view, it was proven that transition rates of different entities of any system are time dependent (use of Erlang, Gamma or Weibull distributions) [6], the method of MARKOV is maladjusted because of its fundamental nature. The first part of this chapter presents a method that allows calculating the availability of a repairable system whatever the transition rate used is. The advantage of this method is to take into account the probability evolution of the system failure from initial state until the final value and we'll not be limited to asymptotic evaluation. The transient mode study allows to evaluate availability at all instants and thus, to consider an estimable evaluation of this parameter [4]. In the first section of this part, the different parameters of dependability are defined and the different methods those allow getting the availability are described. In the second section, the renewal theory applied to compute availability parameter was presented. Finally, a concrete example of the availability evaluation for a system consists of three repairable entities will be studied and their results are presented. The second part of this chapter deals with the design and implementation of algorithms to improve RAMS parameters.

Often, a complex system requires the choice of a compromise between its reliability and a constraint like cost, weight, consumption, time limits and performances to hold... etc. Each of these constraints can be considered like a resource to be liable to limitations that it is necessary to allocate different parts of the system considering a global value which is, either to limit or to optimize. It is the same thing for reliability. [5]

The allowance in dependability, presented under a form of an optimization problem, seems to be prior a simple optimization problem and therefore it would be sufficient to find an optimization algorithm to solve it.

Unfortunately, It exists several underlying difficulties that it's necessary to avoid, in order to achieve allowances in an optimal manner. For example, the survey of the main

existing allowance methods to this day in the literature allows to note clearly that models of allowance are, in general, very specific for a system architecture type (series, series-parallel in most cases). Otherwise, we also note the absence of models in which components are all 2 by 2 different. Indeed, the hypothesis according to which components have the same cost-function in each subsystem is often made, what is not realist. [5]

Our objective was to conceive a method permitting to achieve allowances of reliability, maintainability and availability on systems with any functional architecture, either via a functional modelling by reliability block diagrams(RBD's) or using a dysfunctional one by fault trees (FT's).

Therefore, we proposed algorithms for allowance in the case of cost's minimization under constraints of reliability, availability or maintainability (this is named the dual problem that is also solvable using these algorithms). This iterative algorithm allows allocating the redundancy as well as the reliability of subsystem components.

The originality of the proposed algorithms essentially rests in the act that one imposes no restriction on the system's architecture considered, and also on the possibility to increase the reliability of the system either by increasing the components reliabilities or by increasing their redundancies.

Besides, we consider that components don't have the same reliability within subsystems, and, it is possible to allocate the failure rates in interval of personalized values according to components.

The allowance method that we propose and, therefore, based on optimization heuristic permits:

- To achieve allowances for system with any architecture.
- To achieve the conjoined allowances of redundancy and reliability.
- To make vary the criteria of optimization (reliability. Availability, probability of dreaded event. Mean Down Time). [30]
- To use some discrete cost-functions.

In general, methods of redundancy allowance don't increase the elementary reliabilities, in the most often case, only by addition of redundancies, but don't propose any more

reliable components. We come in this chapter to the point, that the developed method can allocate a joined manner of an increase in reliability or redundancies.

When we replace a component by another one with a greater reliability, we say that we allocate Reliability.

The proposed algorithmic solution is original and inspires its approaches from dynamic optimization with discrete gradient. The idea is to initialize the algorithm with a solution that has the mediocre profitability (minimum cost and very low reliability for example) and to modify features of this solution progressively in order to improve its efficiency (the ratio reliability/cost), we proof the passage to the unoptimality of all solution's families. [41]

The developed heuristic permits also to dislocate the reliability of certain components in a dynamic manner in order to arrive to the solution respecting the initially fixed objectives and satisfying the best compromise cost / efficiency.

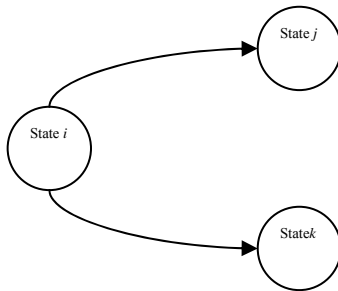
The second part of this chapter presents the principle of allowance algorithms for reliability and availability. The third section deals with an example of simple systems and for which the combinative exploration is possible, to study the solution gotten by the heuristic of the previous optimization.

## IV.2 METHODS FOR OBTAINING THE AVAILABILITY:

Several methods permit to evaluate the availability analytically.

### IV.2.1. Markov method; $\mu$ and $\lambda$ are constants: [8, 4]

Markov method [4] is used during the II<sup>nd</sup> phase of the bathtub curve when transition rates (repair and failure rate) are supposed constants,  $P_i(t)$  is the probability to find the system in state  $i$  at the moment  $t$  and  $a_{ij}$  is the transition rate of going from state  $i$  to the state  $j$  (figure IV.1).



**Figure IV.1 Markov Chain representation.**

The representative equations of such a system are given by:

$$\frac{dP_i(t)}{dt} = -\sum_{i \neq j} a_{ij} \cdot P_i(t) + \sum_{i \neq j} a_{ji} \cdot P_j(t) \quad (\text{IV.1})$$

In reliability, such systems are named stochastic systems and the unknown probabilities are determined by matrix algebra, For example, the calculation of the availability of a system with constant rates gives the following result for a system in operating condition at the initial state:

$$A(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} \cdot e^{-(\lambda + \mu)t} \quad (\text{IV.2})$$

#### IV.2.2 Analytical Description of Availability [4, 8, 23]:

Let  $A^k(t)$  the probability that a component is in an operational state at instant  $t$ , knowing that it already had  $k$  failures and that it was in the operating condition at  $t = 0$ :

$$A^k(t) = \int_0^t \int_{t_1}^t \int_{t_2}^t \dots \int_{t_{2k-1}}^t [f(t_1) \cdot g(t_2 - t_1) \cdot f(t_3 - t_2) \cdot g(t_4 - t_3) \dots f(t_{2k-1} - t_{2k-2}) \cdot g(t_{2k} - t_{2k-1})] \\ [1 - F(t_2 - t_{2k})] \cdot dt_1 \cdot dt_2 \dots dt_{2k} \quad (\text{IV.3})$$

The availability can be written as the sum of the probabilities whatever the values of  $k$ ,

$$\text{where; } A(t) = \sum_{k=0}^{\infty} A^k(t) \quad (\text{IV.4})$$

In general, the availability is given by a series of integrals. However, the practical applications of this formulation are rare for various distributions and more than 2 states.

#### IV.2.3 Monte-Carlo Simulation

Monte-Carlo simulation [32] allows estimating the availability by simulating the behavior of the system randomly. For each component constituting the system, the cycle's sequences of failures / repairs are simulated, and then superposed to find the availability of the system.



### IV.3. THE RENEWAL THEORY

The large majority of the RAMS studies, known as " traditional ", those applied to reparable systems don't take into account neither the number of the cycles failure / repair occurrences nor the transition rates depending on time [ 8],[62]. The mathematical bases of the renewal theory, resulting from sums of random variables those make it possible to calculate the dependability parameters (notably, availability), by integrating these various aspects.

#### A. The renewal Process:

The renewal theory was developed by COX [19], [62] permits to obtain transfer functions characterizing the replacement of a component by other one. The various transfer functions are summarized for each renewal process that exists (table IV.1).

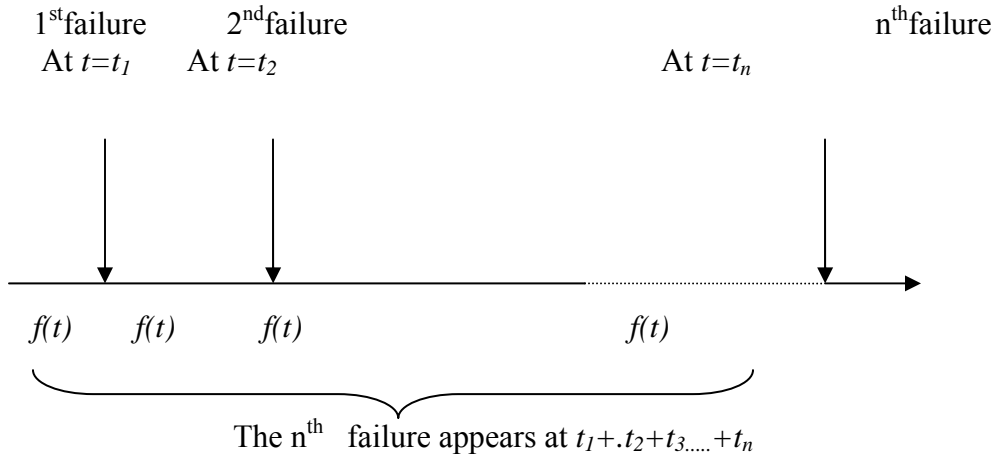
	<i>Renewal function</i>	<i>Renewal density</i>
Simple renewal	$H_s(p) = \frac{f(p)}{p \cdot [1 - f(p)]}$	$h_s(p) = \frac{f(p)}{1 - f(p)}$
Modified renewal	$H_M(p) = \frac{f_1(p)}{p \cdot [1 - f(p)]}$	$h_M(p) = \frac{f_1(p)}{1 - f(p)}$
Simple alternated renewal	$H_{AS} = \frac{f_1(p) \cdot f_2(p)}{p \cdot [1 - f_1(p) \cdot f_2(p)]}$	$h_{AS} = \frac{f_1(p) \cdot f_2(p)}{1 - f_1(p) \cdot f_2(p)}$
Modified alternated renewal	$H_{AM} = \frac{f_1(p)}{p \cdot [1 - f_1(p) \cdot f_2(p)]}$	$h_{AM} = \frac{f_1(p)}{1 - f_1(p) \cdot f_2(p)}$

**Table IV.1.Summary of transfer function for the renewal process [62, 4]**

#### IV.2.3.1 The simple renewal Process:

Let a population of components, having for life-time the random variable X with a probability density f (t). After a failure, the components are immediately replaced by components of the same probability density.

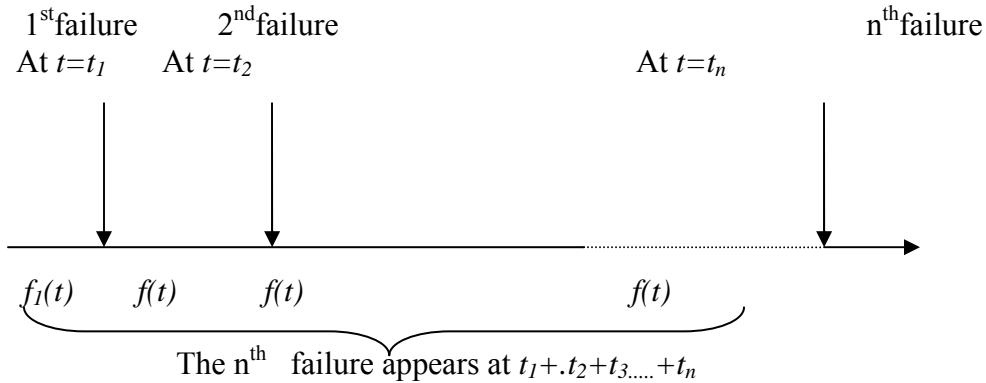
The transfer function characterizing this process is noted  $H_s(p)$ .



**Fig.IV.2 Representation of a simple renewal process**

#### IV .2.3.2 Modified renewal Process:

When the component used at  $t = 0$  s, is not a new component, the process of renewal is called modified renewal process. It is a simple renewal process, which starts with  $t = 0$  s with a probability density  $f_1(t)$  different from the others .



**Figure IV.3 Modified renewal Process representation**

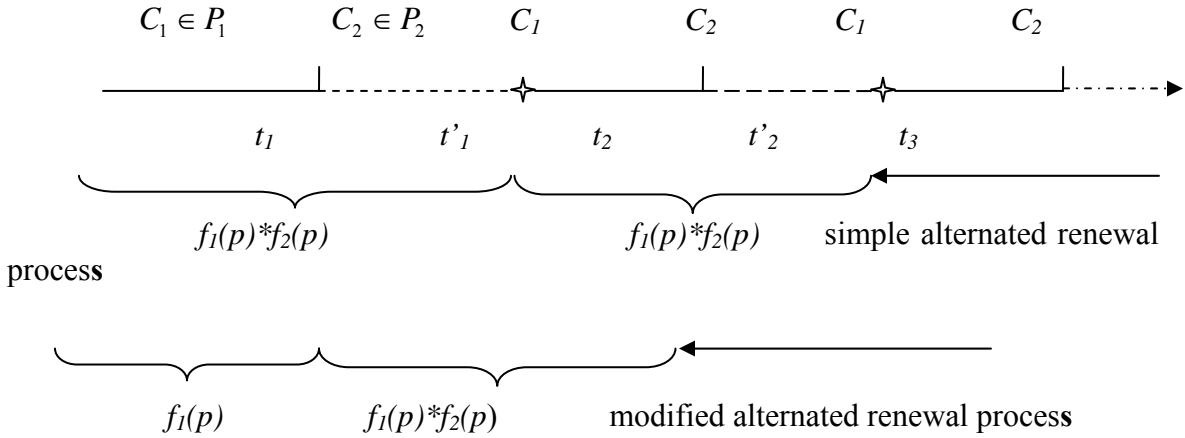
#### IV.2.3.3 Alternated simple & modified Renewal process:

Of alternate renewal is an alternate series of random variables. This type of process can be reduced to a simple or modified renewal processes.

Let 2 populations of components  $P_1$  and  $P_2$ , each one having a probability density  $f_1(t)$  and  $f_2(t)$ , respectively. After a failure, the damaged component is immediately replaced by a component of the other population. The life-time of each population is supposed statistically independent. The first component belongs to the population  $P_1$  and the others result alternatively from the 2 populations. This alternate renewal can be compared with

a simple renewal with a probability density  $f(t)$ , defined by  $f(t)=f_1(t)*f_2(t)$  ; the transfer function of such a system is noted  $H_{AS}(p)$ , if the first component results from the population  $P_2$  and just after the first failure, the components  $C_1$  and  $C_2$  resulting from the populations  $P_1$ , and  $P_2$ , respectively, are alternated, the alternate renewal is similar to a modified renewal process .  $f_1(t)$  is the first probability density and  $f_1(t)*f_2(t)$ , is the probability density of the life-time that follows. La function of transfer is noted

$H_{AM}(p)$ , table IV.1



**Fig.IV.4 Modified alternated renewal process representation.**

| : Failure of component  $C_1$  from population  $P_1$

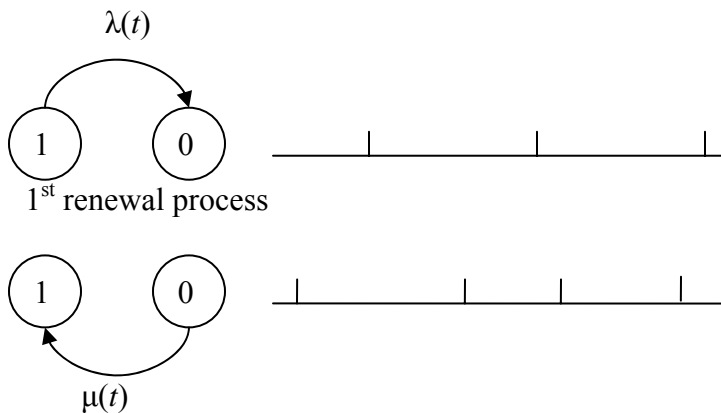
✦ : Failure of component  $C_2$  from population  $P_2$

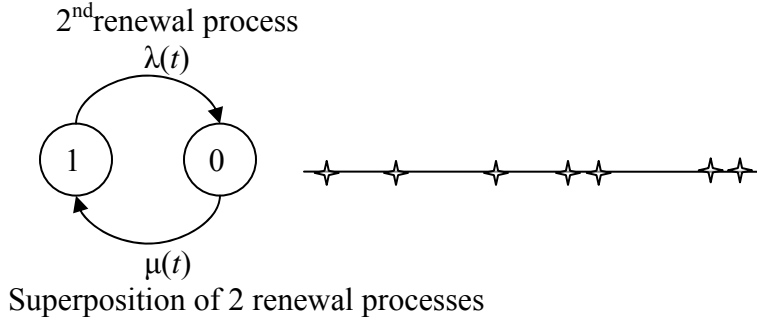
$C_i$ : component from population  $P_i$

$f_i$ : probability density of the life-time of  $C_i$

#### IV.4 CALCULATION OF AVAILABILITY FROM RENEWAL THEORY.

The availability is obtained by the superposition of several alternate renewal processes [9] (figure IV.5) and can be also characterized by a transfer function.





**Figure IV.5 Superposition of renewal processes**

Two cases occur:

-The system is available at initial state, and

The transfer function is written:

$$A_1(p) = \frac{1}{p} - [H_{AS}(p) - H_{AM}(p)] = \frac{1 - f_1(p)}{p \cdot [1 - f_1(p) \cdot f_2(p)]}$$

(IV.5)

The system is unavailable at the initial instant, and the transfer function is:

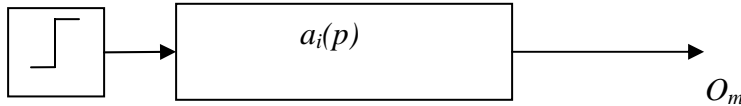
$$A_2(p) = H_{AM} - H_{AS} = \frac{f_1(p) \cdot [1 - f_2(p)]}{p \cdot [1 - f_1(p) \cdot f_2(p)]}$$

(IV.6)

These transfer functions are written only according to the densities of failure  $f_1(t)$  and the densities of repair  $f_2(t)$  and make it possible to obtain the availability by calculating the response to unit step functions (IV.5) and (IV.6):

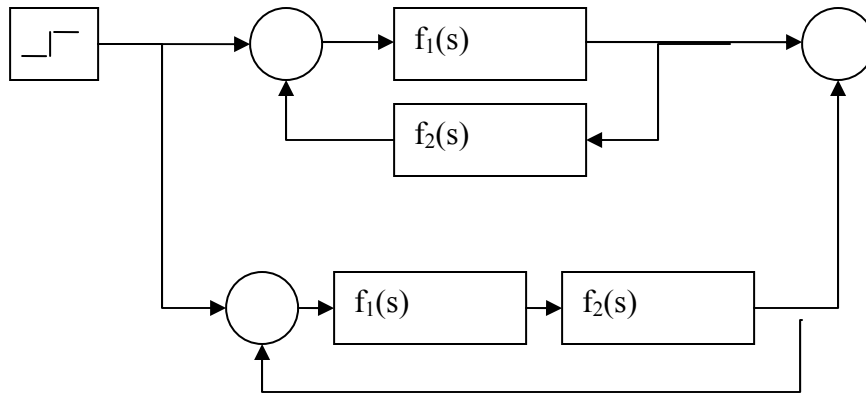
$$a_i(p) = p \cdot A_i(p) \text{ with } i=1,2.$$

$$a_i(p) = \frac{O_m(p)}{I_n(p)} ; \text{ Where } I_n(p) = 1/p \text{ is a unit-step.}$$

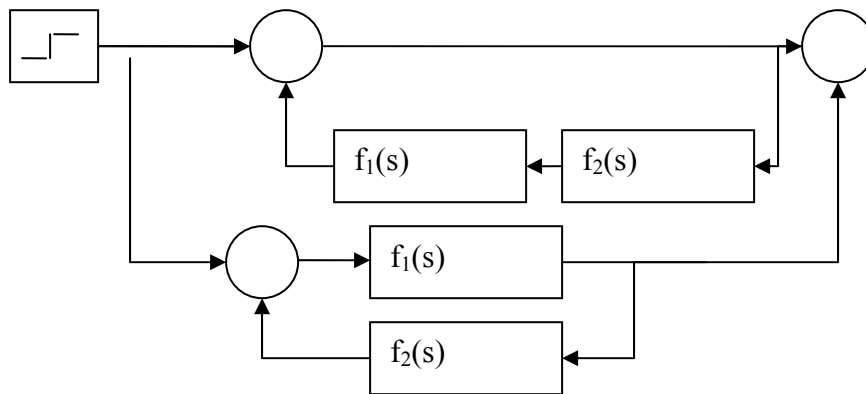


**Figure IV.6 Transfer function  $a_i(p)$**

For this type of study, the transfer function of figure IV.6 was represented by diagrams blocks under SIMULINK as figure IV.7 shows it:



### The system unavailable at $t = 0$



### The system available at $t = 0$

**Figure IV.7 Availability representation under SIMULINK.**

The final value theorem gives the asymptotic value of the availability  $A_{\infty}$ :

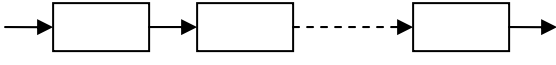
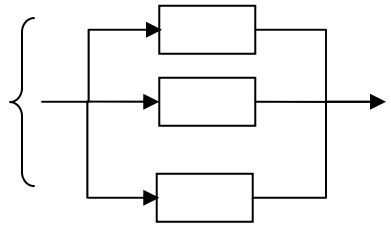
$$A_\infty = \lim_{t \rightarrow \infty} A(t) = \lim_{p \rightarrow 0} p \cdot A_i(p)$$

(IV.7)

This availability evaluation can be applied for any type of probability laws (Markovian-system or system with rate time dependent transition rates). This remark is of interest for systems in phase of design (phase I of the curve out of bath-tub). However, the results are valid for a component, knowing its failure and repair densities, or a system knowing the failure and repair densities of system it would be appreciable to calculate the availability of a system made up

of several components in series or parallel, knowing the transition rates from each component. Calculation is relatively simple in the Laplace space by using RBD method (Reliability Block Diagram).

RBD method [25] is used to calculate availability of a system made up of several entities in series or in parallel (table IV.2.), other associations of systems can be carried out starting from systems series and parallel.

System type	Availability
<p>Serial system</p>  <p><i>n serial entities</i></p>	$A_{system} = \prod_{i=1}^n A_i(t); \text{ where } A_i(t) \text{ is the availability of } i^{\text{th}} \text{ entity}$
<p>Parallel system</p> 	$A_{system} = 1 - \prod_{i=1}^n U_i(t) ; \text{ where } U_i(t) \text{ is the unavailability of the } i^{\text{th}} \text{ entity}$

**Table IV.2 series/parallel system availability**

#### 4.2.5. Transposition of the RDB method in the Laplace domain:

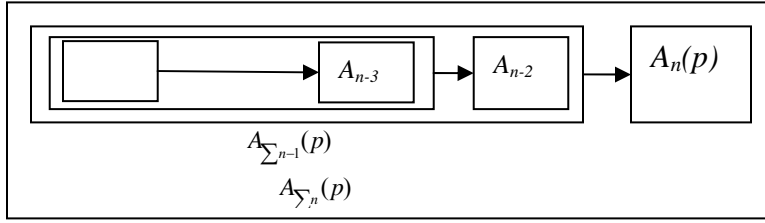
The Laplace transforms for the expressions of table IV.1 result from the Laplace transforms of a product:

$$L(f(t) \cdot g(t)) = L(f(t)) * L(g(t)) \quad (\text{IV.8})$$

In the case of traditional distributions (exponential laws, Gamma or normal)[8], the Laplace transforms are holomorphic functions. The convolution of the holomorphic functions is defined by HANUS [20] by an integral on a closed contour C materialized by the following expression:

$$F(p) * G(p) = \frac{1}{2 \cdot \pi \cdot j} \int_C F(q) \cdot G(p - q) \cdot dq \quad (\text{IV.9})$$

Since the functions used are causal, the residues method permits to calculate the transfer function of the resulting system,



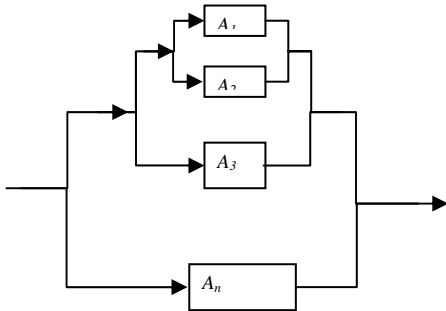
**Figure IV.8 series system representation using recursive sequences**

For a series system, the resulting transfer function will be given by the convolution of the transfer function of the system  $A_{\Sigma_{n-1}}(p)$  and the component  $A_n(p)$  (**Figure IV.8**). The final transfer function can be presented like a recursive sequence:

$$A_{\Sigma_n}(p) = \left( \sum_{poles(U_n(p))} residu[A_n(q) \cdot A_{\Sigma_{n-1}}(p-q)] \right) \quad (IV.10)$$

In the same way, the transfer function of a parallel system will be given by the relation where  $U_n$  indicates the unavailability of component  $n$ :

$$A_{\Sigma_n}(p) = 1 - \left( \sum_{poles(U_n(p))} residu[U_n(q) \cdot U_{\Sigma_{n-1}}(p-q)] \right) \quad (IV.11)$$

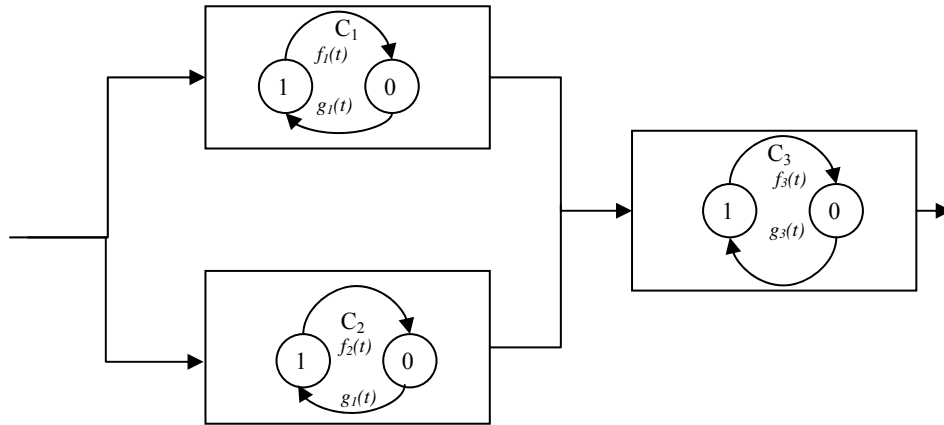


**Figure IV.9 Parallel system representation using recursive sequences**

This method, adapted to the systems series / parallel or the systems which can drive us ,to facilitate the availability calculation using transfer functions .

**Example: Case of mixed system constituted of 3 components**

Consider a system, constituted of 3 components  $C_i$ , represented on figure IV.10



**Figure IV.10 Mixed system**

Each component has a failure density  $f_i(t)$ , and a repair density  $g_i(t)$ , following Erlang laws (table IV.3), the availability of each component can be deduced by the equation (IV.10) or by equation (IV.10).

	$f_i(t)$	$g_i(t)$
$C_1$	$\left(\frac{1}{1+p}\right)^2$	$\left(\frac{4}{4+p}\right)^5$
$C_2$	$\left(\frac{2}{2+p}\right)^3$	$\left(\frac{10}{10+p}\right)^{20}$
$C_3$	$\left(\frac{5}{5+p}\right)^2$	$\left(\frac{100}{100+p}\right)$

**Table IV.3 Erlang distribution for  $C_1, C_2, C_3$**

The resulting system has  $2^3$  initial configurations, determined by the Boolean theory and has 8 states. **Table IV.4. Initial configurations**

$C_1$	$C_2$	$C_3$	System
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1



0: faulty state; 1: functioning state;

The transfer function will be obtained by the combination of the equations (IV.10) and (IV.11), formally applied to the system by MAPLE. Figure IV.12 gives for the eight transfer functions resulting from the eight initial configurations the availability of the system calculated by MATLAB. We proceed as follows through MAPLE to deduce the transfer function then we'll sketch the availability in function of time by MATLAB. So we gonna implement and evaluate the following expression in the case where  $C_1C_2C_3=111$ .

>

$$\sum_{q = \text{RootOf}\left(x^2 \left(1 - \left(\frac{5}{5+x}\right)^2 \frac{100}{100+x}\right), x\right)} \text{residue} \left( \left(1 - \left(\frac{5}{5+q}\right)^2\right) \left( \frac{1}{s-q} - \sum_{q = \text{RootOf}\left(x^2 \left(1 - \left(\frac{2}{2+x}\right)^3 \left(\frac{10}{10+x}\right)^{20}\right), x\right)} \text{residue} \left( \left( \frac{1}{q} - \frac{1 - \left(\frac{2}{q+2}\right)^3}{q \left(1 - \left(\frac{2}{2+q}\right)^3 \left(\frac{10}{10+q}\right)^{20}\right)} \right) \left( \frac{1}{s-2q} - \frac{1 - \left(\frac{1}{s-2q+1}\right)^2}{(s-2q) \left(1 - \left(\frac{4}{4+s-2q}\right)^5 \frac{1}{s-2q+1}\right)} \right) \right) \right) \right) \Bigg/ \left( q \left(1 - \left(\frac{5}{5+q}\right)^2 \frac{100}{100+q}\right), q = \text{RootOf}\left(x^2 \left(1 - \left(\frac{5}{5+x}\right)^2 \frac{100}{100+x}\right), x\right) \right)$$

```
> sum(residue((((1-((5)/(5+q))^2))/((q)*(1-
(((5)/(5+q))^2)*((100)/(100+q))))))*((1)/(s-q))-
sum(residue((((1/q)-((1-((2)/(q+2))^3))/((q)*(1-
(((2)/(2+q))^3)*((10)/(10+q))^20))))))*((1)/(s-((2)*q)))-((1-
((1)/(s-2*q+1))^2))/((s-2*q)*(1-(((4)/(4+s-2*q))^5)*(1)/(s-
2*q+1))))), q=RootOf((x^2)*(1-
((2)/(2+x))^3*((10)/(10+x))^20),x),q=RootOf((x^2)*(1-
((2)/(2+x))^3*((10)/(10+x))^20),x)), q=RootOf((x)*(1-
((5)/(5+x))^2*((100)/(100+x))),x),q=RootOf((x)*(1-
((5)/(5+x))^2*((100)/(100+x))),x));
```

```
> (1/q-(((1-(2/(q+2))^3))/((q)*(1-(((2)/(2+q))^3)*(10/(10+q))^20)))));
```

$$\frac{1}{q} - \frac{1 - \frac{8}{(q+2)^3}}{q \left(1 - \frac{8000000000000000000}{(q+2)^3 (10+q)^{20}}\right)}$$

```
> (((1/(s-q))-(((1-(1/(s-q+1))^2))/((s-q)*(1-(((1)/(1+s-q))^2)*(4/(4+s-
q))^5)))));
```

$$\frac{1}{s-q} - \frac{1 - \frac{1}{(s-q+1)^2}}{(s-q) \left(1 - \frac{1024}{(s-q+1)^2 (4+s-q)^5}\right)}$$

$$\left( \frac{1}{q} - \frac{1 - \frac{8}{(q+2)^3}}{q \left( 1 - \frac{80000000000000000000}{(q+2)^3 (10+q)^{20}} \right)} \right) \quad \left( \frac{1}{s-q} - \frac{1 - \frac{1}{(s-q+1)^2}}{(s-q) \left( 1 - \frac{1024}{(s-q+1)^2 (4+s-q)^5} \right)} \right)$$

```
> residue((1/q-((1-(2/(q+2))^3))/((q)*(1-
(((2)/(2+q))^3)*(10/(10+q))^20))))*((1/(s-q))-(((1-(1/(s-
q+1))^2))/((s-q)*(1-(((1)/(1+s-q))^2)*(4/(4+s-q))^5))))),q=0);
```

$$\begin{aligned} & \left( 1024000000000000000000 s + 320000000000000000000 s^3 \right. \\ & + 20480000000000000000000 s^2 \\ & + 1600000000000000000000 s^4) / (761600000000000000000 s^3 \\ & + 9318400000000000000000 s + 1182720000000000000000 s^2 \\ & + 5628000000000000000000 s^5 + 2744000000000000000000 s^4 \\ & \left. + 6160000000000000000000 s^6 + 280000000000000000000 s^7) \end{aligned}$$

```
> R1 := normal(
(1024000000000000000000000000*s+3200000000000000000000000*s^3+2048000000000
0000000000000+25600000000000000000000000*s^2+160000000000000000000000*s^4)/(7
6160000000000000000000000*s^3+9318400000000000000000000*s+11827200000000
000000000000*s^2+5628000000000000000000000*s^5+27440000000000000000000000
*s^4+61600000000000000000000000*s^6+28000000000000000000000*s^7) );
```

$$RI := \frac{4 (640 s + 20 s^3 + 1280 + 160 s^2 + s^4)}{7 s (2720 s^2 + 3328 + 4224 s + 201 s^4 + 980 s^3 + 22 s^5 + s^6)}$$

$$> ((1 - (5/(q+5))^2)) / ((q) * (1 - (((5)/(5+q))^2 * (100/(100+q)))));$$

$$\frac{1 - \frac{25}{(5 + q)^2}}{q \left( 1 - \frac{2500}{(5 + q)^2 (100 + q)} \right)}$$

```
> R17 := solve( {7*s*(3328+2720*s^2+4224*s+s^6+201*s^4+22*s^5+980*s^3)}  
) ;
```

$$R17 \quad := \quad \{ s = 0 \}, \{ s =$$
$$\text{RootOf} \left( 3328 + 2720 \_Z^2 + 4224 \_Z + \_Z^6 + 201 \_Z^4 + 22 \_Z^5 + 980 \_Z^3, \text{index} = 1 \right)$$
$$\}, \{s =$$
$$\text{RootOf} \left( 3328 + 2720 \_Z^2 + 4224 \_Z + \_Z^6 + 201 \_Z^4 + 22 \_Z^5 + 980 \_Z^3, \text{index} = 2 \right)$$
$$\}, \{s =$$
$$\text{RootOf} \left( 3328 + 2720 \_Z^2 + 4224 \_Z + \_Z^6 + 201 \_Z^4 + 22 \_Z^5 + 980 \_Z^3, \text{index} = 3 \right)$$
$$\}, \{s =$$
$$\text{RootOf} \left( 3328 + 2720 \_Z^2 + 4224 \_Z + \_Z^6 + 201 \_Z^4 + 22 \_Z^5 + 980 \_Z^3, \text{index} = 4 \right)$$

```

    }, { s =
RootOf ( 3328 + 2720 _Z ^2 + 4224 _Z + _Z ^6 + 201 _Z ^4 + 22 _Z ^5 + 980 _Z ^3, index = 5 )
    }, { s =
RootOf ( 3328 + 2720 _Z ^2 + 4224 _Z + _Z ^6 + 201 _Z ^4 + 22 _Z ^5 + 980 _Z ^3, index = 6 )
    }
}

> evalf(%);

{ s = 0. }, { s = -1.284956956 + 1.710920983 I }, { s = -3.902647370 + 2.358049774 I },
{ s = -5.812395674 + 1.085387026 I }, { s = -5.812395674 - 1.085387026 I },
{ s = -3.902647370 - 2.358049774 I }, { s = -1.284956956 - 1.710920983 I }

> residue((1/q-((1-(2/(q+2))^3))/(q)*(1-
(((2)/(2+q))^3)*(10/(10+q))^20))))*((1/(s-q))-((1-(1/(s-
q+1))^2))/(s-q)*(1-(((1)/(1+s-q))^2)*(4/(4+s-q))^5))))),q=-
1.284956956-1.710920983*I);

0

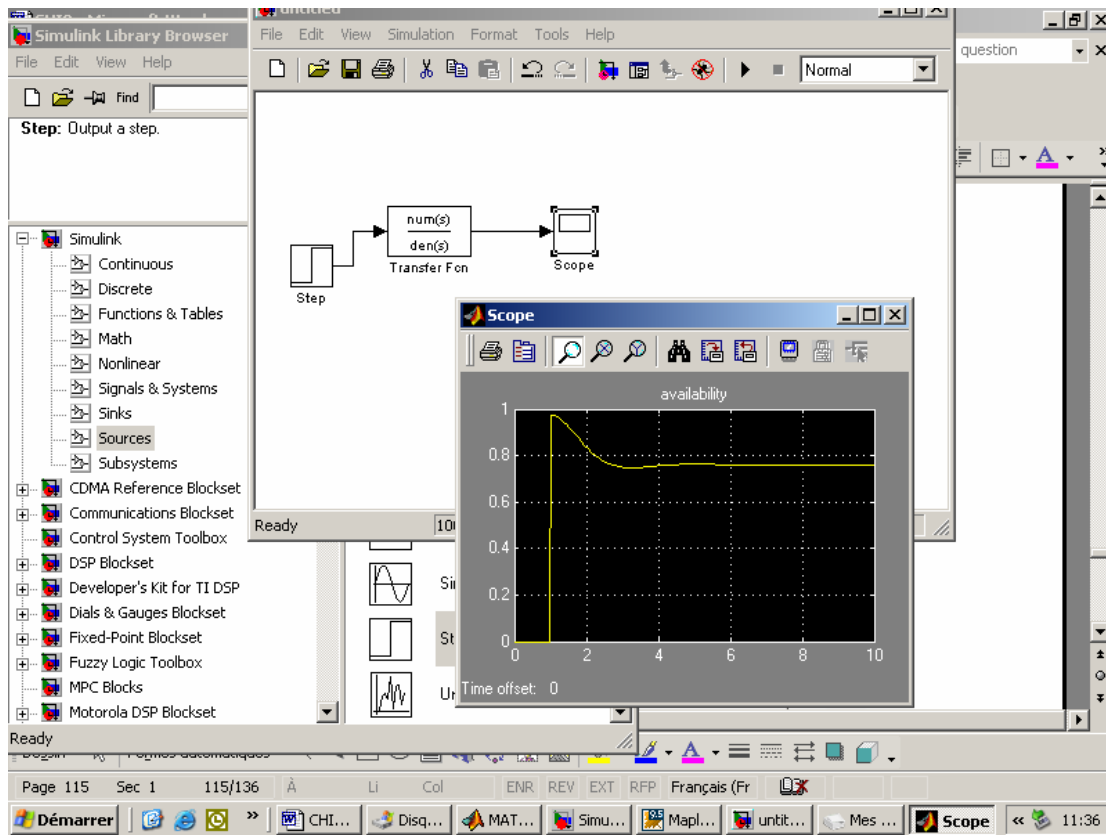
> ((1/(s-q))-4/7*(640*(s-q)+1280+20*(s-q)^3+(s-q)^4+160*(s-q)^2)/(s-
q)/((s-q)^6+3328+4224*(s-q)+980*(s-q)^3+201*(s-q)^4+22*(s-q)^5+2720*(s-
q)^2));


$$\frac{1}{s-q} - 4 \left( \frac{640}{s-q} - \frac{640}{q} + 1280 + 20(s-q)^3 + (s-q)^4 + 160(s-q)^2 \right) / (7(s-q) \left( (s-q)^6 + 3328 + 4224(s-q) + 980(s-q)^3 + 201(s-q)^4 + 22(s-q)^5 + 2720(s-q)^2 \right))$$

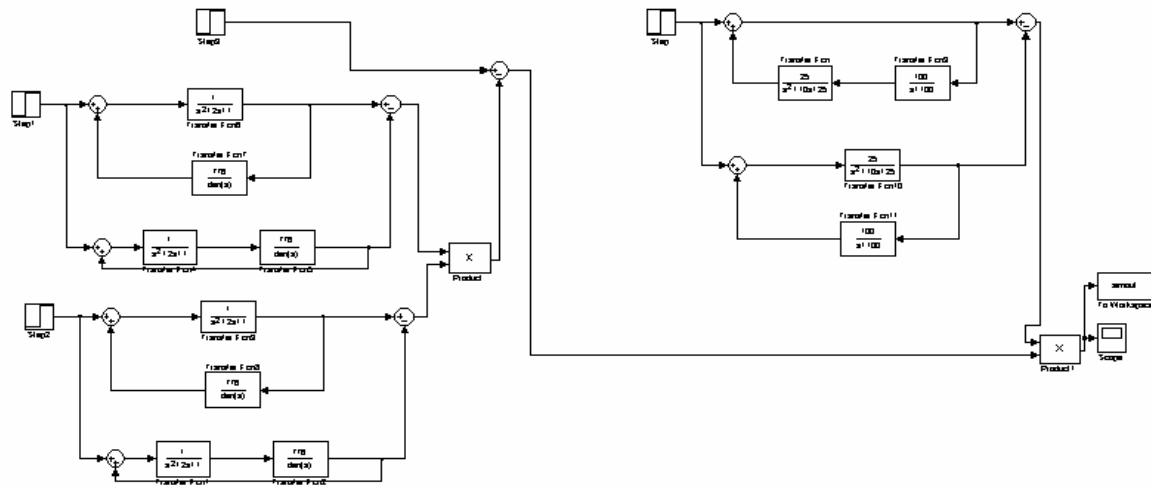

> residue((((1-(5/(q+5))^2))/(q)*(1-
(((5)/(5+q))^2)*(100/(100+q))))))*((1/(s-q))-4/7*(640*(s-
q)+1280+20*(s-q)^3+(s-q)^4+160*(s-q)^2)/(s-q)/((s-q)^6+3328+4224*(s-
q)+980*(s-q)^3+201*(s-q)^4+22*(s-q)^5+2720*(s-q)^2)),q=0);

(27008000 s + 18176000 + 6780000 s^3 + 1403000 s^4 + 18400000 s^2 + 7000 s^6 + 154000 s^5) / (1442175 s^5 + 7031500 s^4 + 7175 s^7 + 157850 s^6 + 30307200 s^2 + 19516000 s^3 + 23878400 s)

```

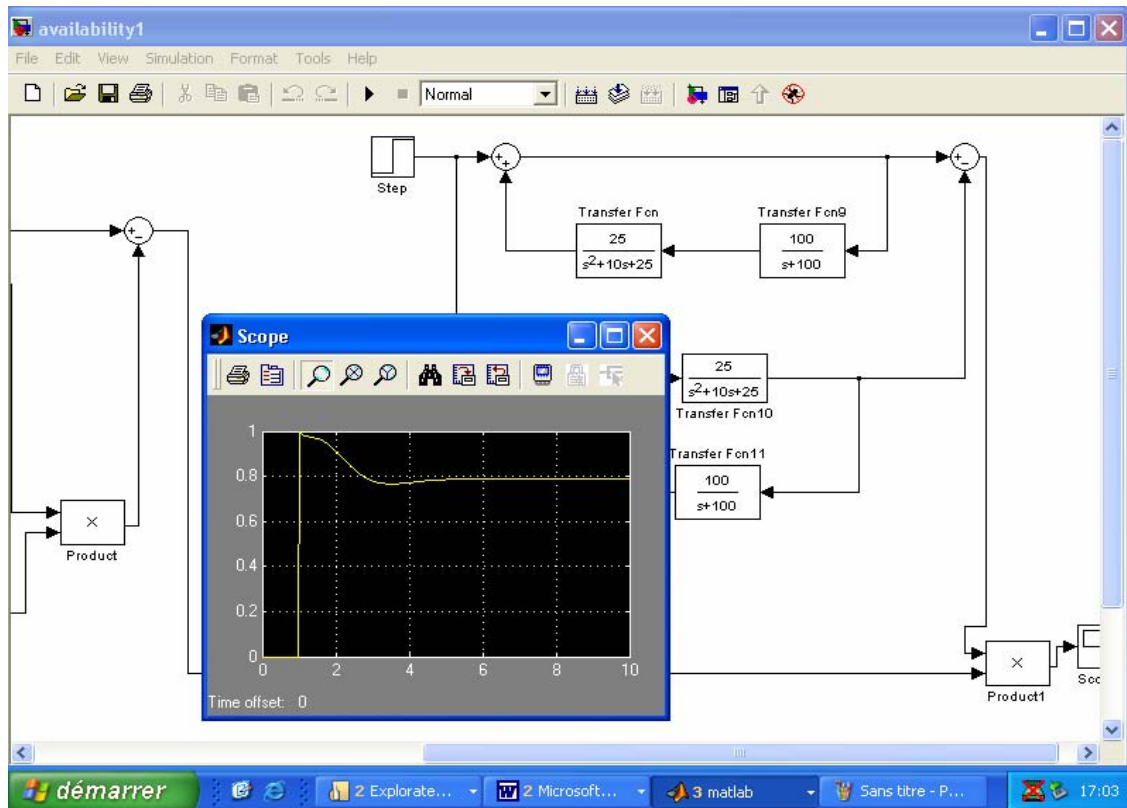


Let's now, implement directly the system in SIMULINK as shown in fig IV.11:



**Figure IV.11** Availability model implementation of the example under Simulink:

After visualisation of the results via the scope block we'll get the following availability graph:



**FigureIV.12 Availability model results:**

The asymptotic value obtained graphically, then, confirmed by the final value Theorem. From the two graphs above we can notice that the two implementation methods validate each other.

## IV.5 Part.II ALGORITHMS FOR ALLOCATION OF RAMS INDICATORS

### IV.5 .1 Optimization heuristic for reliability allowance:

We've to respect a reliability criterion at instant  $t$  ( $t$  being the mission system time).

In this paragraph, we limit the allowance problem to an allowance of reliability and availability.

The developed algorithms are iterative; they permit to drive allowances progressively in a recurrent manner, of any solution until the most economic solution among those respecting a fixed objective to the level of the system.

The algorithmic description concerns the indicator of a system reliability, whose assessment is based on a reliability block diagram modelling type.

We consider a system that consists of  $n$  components, disposed according to any architecture (series, parallel, redundancy  $k/n$ ...).

Let  $R$  the reliability of the system and  $r_i$ , the elementary reliability of the component  $i$ .

**At the first iteration**, we'll initialize all elementary reliabilities  $(r_1, r_2, r_3, \dots, r_i, \dots, r_n)$  to the worst values that the technology can provide:

$$r_i^0 = f_i(\lambda_{i_{\max}}) = r_{i_{\min}} \dots \forall i$$

(IV.12)

Let the initial point coordinates represented by the vector  $r^0$  of which, the components are elementary reliabilities  $r_i^0$  we calculate  $R^0 = f(r^0)$ .

We have:

$$R^0 = f(r^0) \langle R_{obj}$$

(IV.13)

#### IV.5.2 Taking into account the costs

Allowances must integrate in upstream the economic constraints of equipment's conception; it is why we will try to increase the reliability of the system by limiting the conception cost of the system. In this goal, it has been defined a criteria function  $C$  (function of elementary costs of the equipment's conception).

**IV.5.3 Optimization Heuristic:** At each iteration, we'll find the subsystem  $i$  that, by an increase  $\Delta r_i$  of its reliability maximizes the ratio  $\Delta R / \Delta C$ .

Thus; search for the subsystem  $i$  that maximizes the ratio  $\Delta R / \Delta C$  allows to take into account some economic aspects, when trying to respect a fixed reliability objectives, we note, to this stage, that the algorithm of allowance doesn't propose any structural modification of the system. The optimization of system architecture in an allowance problem of RAM can, however, be taken into account. The integration of this heuristic makes the object of the following part.

#### IV.5.4 Specifications on the input data:

The established optimizations Algorithms for allowances use the following decision variables:

- Failure Rates  $\lambda_i$  of the elementary components,
- Repair Rates  $\mu_i$ , of the elementary components.

In order to define variation domains of these decision variables; the user has to, for each component, to seize a possible variation interval of failure rates  $\lambda_i$  and of repair rates of it  $\mu_i$ .

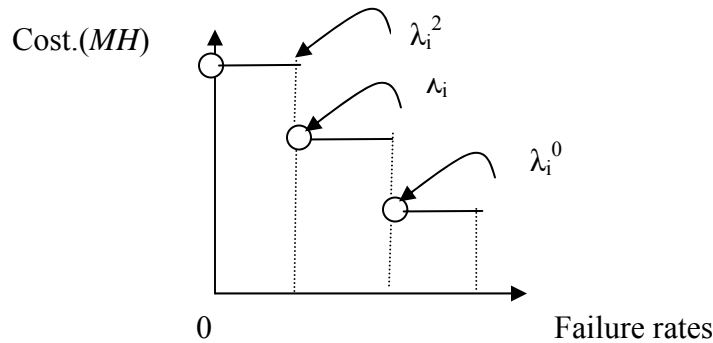
This foreclosure must be done taking into account the existing norms, but also of the user's possible knowledge on the components of the same type.

#### IV.5.5 Costs associated to failure rates:

To seize the failure rates of a component with associated acquisition costs, we didn't run toward the continuous cost models evoked in the literature (example: function Truelove[51]).

Indeed, it is little realist to consider that the acquisition costs vary in a continuous manner according to the component failure rates. In general, we will rather arrange several possible price ranges (with the different reliability levels) for components.

Therefore, the user of this method should seize the different possible values of failure rate for each component of the system. Then, the user must seize a corresponding cost for each failure rate seized,



**Figure IV.13**

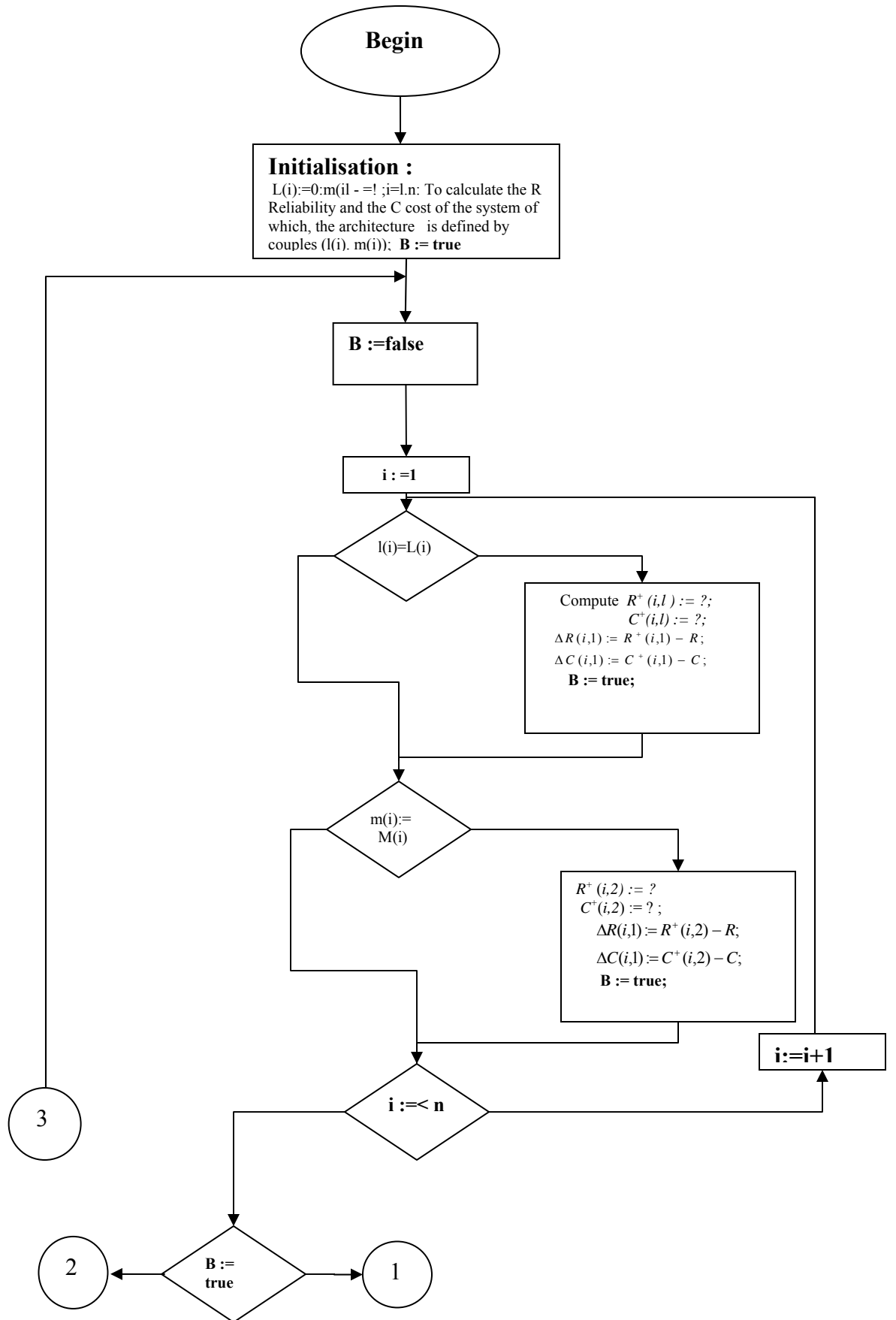
As we can note it on the diagram of the **figure. IV.13**, we dispose for each component of several points of coordinates  $(\lambda_i^j; C^j_i)$ .

The worst failure rate  $\lambda_i^0$  will be taken as the initial point for our algorithm.

The algorithm will propose, to improve the components failure rates by successive increase, according to the heuristic previously stated.

### IV.6. Principle of allowance algorithms

#### IV.6.1. Algorithm of associated allowance for reliability and redundancy:





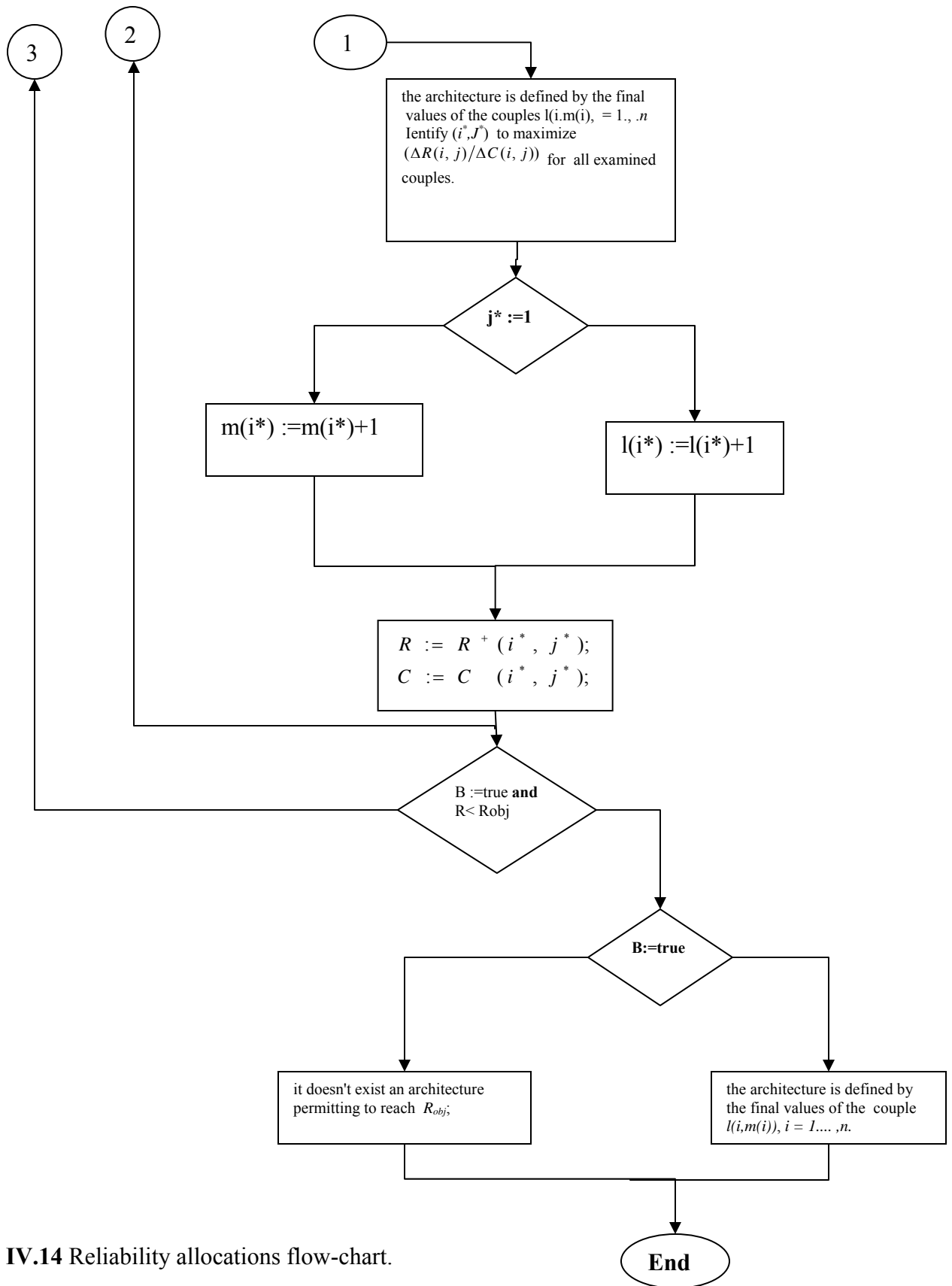


Figure IV.14 Reliability allocations flow-chart.

This paragraph details the different possibilities of the increase (or of redundancy) that the algorithm proposes at each iteration.

Concerning the allowance of redundancies, it is indispensable to know the expression of the failure rate of an identical equipments redundancy. We can demonstrate easily that for  $m$  identical components of index  $i$  in redundancy, the failure rate is as follows:

$$\lambda_i(t) = -(1/t) * \ln(1 - [1 - \exp(-\lambda_i^1 * t)]^m)$$

(IV.14)

We will use this formula for  $m = 2, 3, \dots$  components in redundancy, changing the power in the formula.

The algorithm of reliability allowance with propositions of redundancy is described below.

For the  $i$  components, it exists  $L(i+1)$  possible reliability levels noted  $0, 1, 2, \dots, L(i)$  and a redundancy of maximal order  $M(i)$ . We let:

$l(i)$  :integer characterizing the level of reliability of the  $i$  components:

$m(i)$ : redundancy order of the  $i$  components.

**BEGIN**

**Initialization:**

$l(i) := 0$  ;  $m(i) := 1$  ;  $i := 1, n$  ;

Compute the Reliability  $R$  and the cost  $C$  of the system in which the architecture is defined by the couples  $(l(i), m(i))$ ;

**B := true**

**End initialization**

**While** ( $B$  true **and**  $R < R_{obj}$ ) **do**

**B := false**

**For**  $i = 1, \dots, n$ , **do**

**If**  $l(i) < L(i)$  **then**

    Compute the reliability  $R^+(i, l)$  of the system when the components  $i$  are replaced by the components  $i$  of reliability level  $(l(i)+1)$ , as well as its cost

$C^+(i, l)$ ;

$\Delta R(i, l) := R^+(i, l) - R$ ;

$\Delta C(i, l) := C^+(i, l) - C$ ;

**B := true;**

**End If**

**If**  $m(i) < M(i)$  **then**

Compute reliability  $R^+(i,2)$  of the system when the redundancy order of the components  $i$  is increased by one unit,  
as well as , its cost  $C^+(i,2)$  ;

$$\Delta R(i,1) := R^+(i,2) - R;$$

$$\Delta C(i,1) := C^+(i,2) - C;$$

**B: = true;**

**End If**

**End For**

**If B is true, then**

the architecture is defined by the final values of the couples  $l(i,m(i))$  s .  $i = 1, \dots, n$

To identify the couple  $(i^*, j^*)$  to achieve the maximum

To identify the couple  $(i^*, j^*)$  to achieve the maximum of  $(\Delta R(i, j) / \Delta C(i, j))$

for all examined couples.

**if**  $j^* = 1$  **then**  $l(i^*) = l(i^*) + 1$  ;

**Otherwise**  $m(i^*) = m(i^*) + 1$  ;

**End If**

$$R := R^+(i^*, j^*);$$

$$C := C^+(i^*, j^*);$$

**End If**

**End While**

**If B is true ,then**

the architecture is defined by the final values of the couple

$l(i,m(i))$ ,  $i = 1, \dots, n$ .

**Otherwise** it doesn't exist an architecture permitting to reach  $R_{obj}$ ;

**End If**

**END**

**Remarks;**

*A) - comparisons to do at every iteration:*

At each step, and for each component, we have two propositions of reliability improvement: 'Either by a reduction of the failure rate, or by making in redundancy of the less reliable component.

In the case where the number of maximum redundancies of a component is achieved, it remains only one proposition to do in the next step (the reduction of component failure rates currently in redundancy).

Therefore, the maximum of 2 ratios  $\Delta R / \Delta C$  must be compared for each component, and at each step.

Knowing that, we've  $n$  components in the system, therefore; we will have the maximum  $2n$  ratios  $\Delta R/\Delta C$  to be compared at each step,

**B)-propositions on redundancies:**

- We only proposes one supplementary redundancy to each step,
- We don't decrease the number of redundancies with respect to the allocated number in the previous step.

#### IV.6.2. Availability allowance

For the availability allowance of, we use the same body of algorithm that for reliability, except that we take at a time in amount of rates of repair and failure rates. Indeed, the availability of the component  $i$  is the following:

$$a_i(t) = \frac{\mu_i}{\lambda_i + \mu_i} + \frac{\lambda_i}{\lambda_i + \mu_i} e^{-(\lambda_i + \mu_i)t} \quad (IV.15)$$

Therefore, the algorithm will propose more combinations at each step. Jumping from  $2n$  to  $3n$   $\Delta R/\Delta C$  ratio to be compared with respect to the reliability allowance,

#### IV.6.3 The heuristic Validation

The resolution of an allowance problem formulated under a discrete optimization problem form draws the processing a very big number of possible solutions to be examined.

For example, a system that contains 8 components, of which each can take 4 forms (with the different reliabilities) results to examine  $4^8=65536$  theoretical solutions.

The study of each of these solutions evidently requires a computer. Even though the study of these 65536 solutions doesn't represent an insurmountable task for a computer of PC type. It is necessary to know that one can assist, quickly to an explosion of combinative possible solution if the number of components increases. For example, if the number of components is doubled (16 components in the system), we'll have about 4 billion of solutions to examine.

Let's introduce the following variable:

$C_{ij}$ = cost of the solution for the subsystem  $i$ ,

$x_j$ =0 or 1 depending on whether the  $j$  solution is either chosen or not.

A possible politics can be described by the vector:

$$X = [(X_{11}, X_{12}, \dots, X_{1N1}), (X_{21}, X_{22}, \dots, X_{2N2}), (X_{n1}, X_{n2}, \dots, X_{nNn})].$$

Our reliability allowance problem is formulated as follows:

$$\left\{ \begin{array}{l} \min_{C_{ij}} \sum_i \sum_j C_{ij} \cdot x_{ij} \\ s.t R \geq R_{obj} \end{array} \right\} \quad (IV.16)$$

The total number of solutions has to examine is  $\prod_{i=1}^n N_i$ . This number is to have an exponential growth, therefore it is necessary to find some heuristic in order to reduce the combinative, as it has been presented in the previous paragraphs.

Which means; all solutions of discrete' optimization problem 'can be calculated when the number of components in the system is not too large (the following example)

#### IV.6.4 Calculation of all possible solutions on an example:

We'll calculate all existent solutions of a problem; it will be possible to know the position of the solution determined by the algorithm with respect to the whole possible solution. For this, it is necessary:

To calculate the reliability of the system for all possible combinations of component failure rates,

- Among the whole of these solutions. We preserve those superior or equal to  $R_{obj}$ , after this we study the solution gotten by the algorithm with respect to the retained solutions.

#### 4.1. Example of 3 components:

We consider the following reliability block diagram:

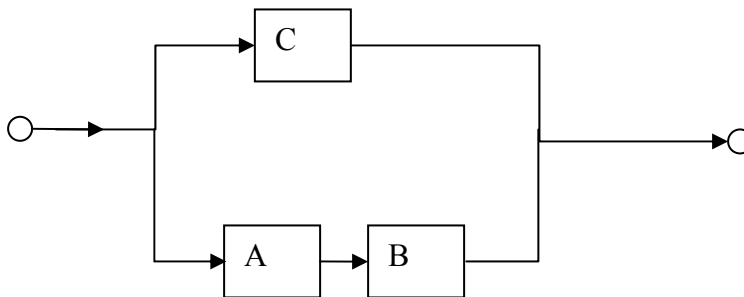


Figure: IV.15

The reliability of system is defined by:

$$R(t) = 1 - [1 - r_C(t)] \bullet [1 - r_A(t) \bullet r_B(t)]$$

(IV.17)

We'll be placed in the period of the useful life of the system (constant failure rate), ie, the elementary reliabilities follow an exponential law.

**Data for the component A:**

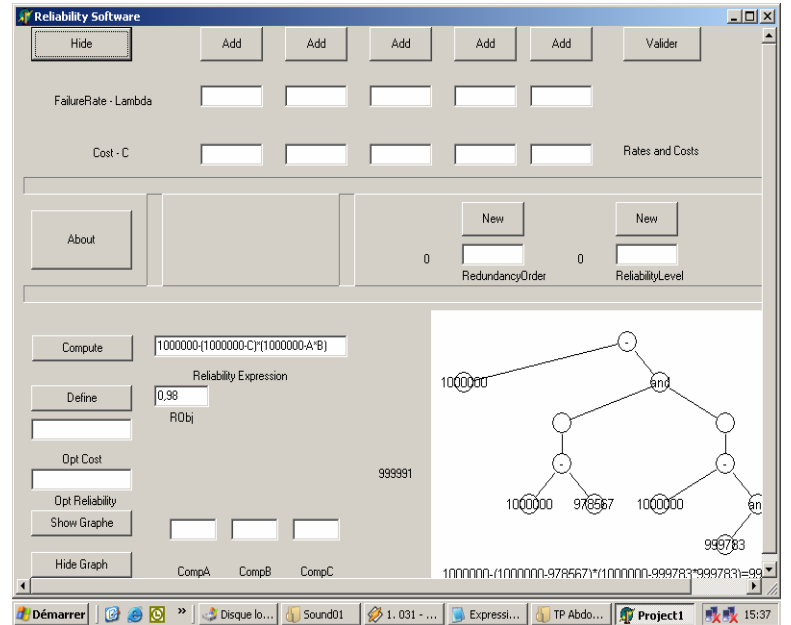
$\lambda_{A1} = 10^{-3} H^{-1} / \cos t C_{A1} = 1MH$
$\lambda_{A2} = 2 \bullet 10^{-6} H^{-1} / \cos t C_{A2} = 10MH$
$\lambda_{A3} = 10^{-6} H^{-1} / \cos t C_{A3} = 500MH$

**Data for the component B:**

$\lambda_{B1} = 10^{-3} H^{-1} / \cos t C_{B1} = 1MH$
$\lambda_{B2} = 2 \bullet 10^{-6} H^{-1} / \cos t C_{B2} = 10MH$
$\lambda_{B3} = 10^{-6} H^{-1} / \cos t C_{B3} = 500MH$

**Data for the component C:**

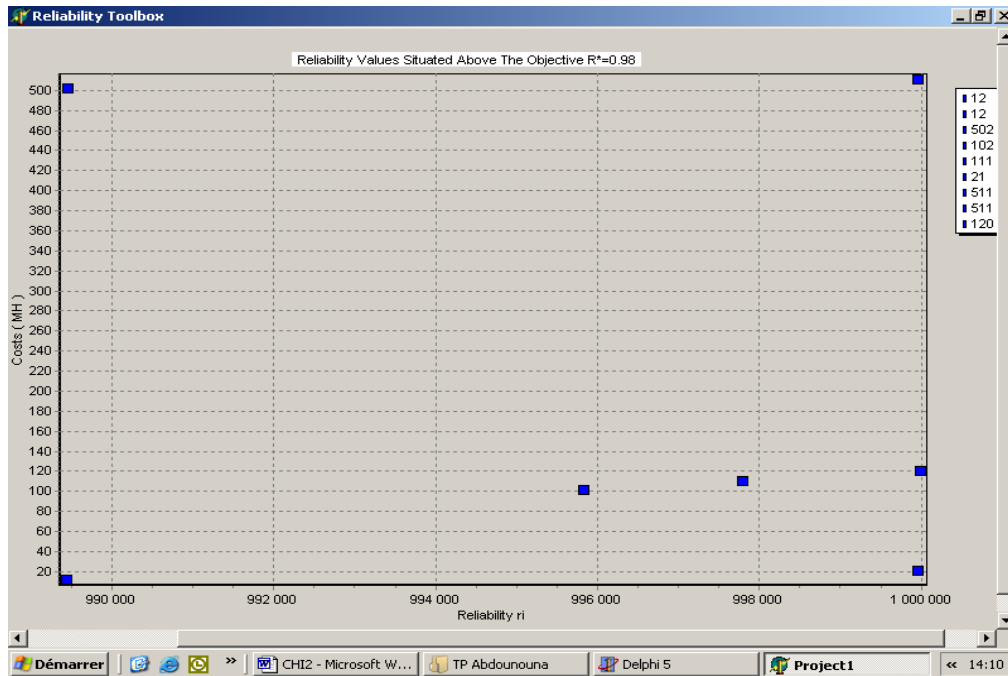
$\lambda_{C1} = 10^{-3} H^{-1} / \cos t C_{C1} = 1MH$
$\lambda_{C2} = 2 \bullet 10^{-6} H^{-1} / \cos t C_{C2} = 10MH$
$\lambda_{C3} = 10^{-6} H^{-1} / \cos t C_{C3} = 500MH$



The total number of possible solutions is 18.

**FigureIV.16a**

After calculation of the 18 solutions, we'll get a graph (figureIV.16) the one respecting  $s.t.R \geq R_{obj} = 0.98$ . Values of reliabilities situated above of the objective are shown in FigIV.16b.



FigureIV.16b

The solution determined by the algorithm is the following:  $R=0.99775$  for a cost of 111 MH (value shown in **FigIV.16b**).

#### IV.6. 5 Interpretations:

The study of this solution results in some algorithmic modifications which are necessary. Indeed, it would be interesting to be able to propose to the user all solutions situated between the objective  $R_{obj}$  and the solution proposed by the algorithm (example: to propose the solution with a cost of 100 MH on the graph).

For it, it is necessary to put in place a disallowance procedure (rein creasing of failure rates) in algorithms.

Indeed, the user will have the possibility, once upstart to the obtained solution by the described heuristic before, to reach the previous solutions.

#### IV.7 The disallowance procedure:

From the solution proposed by the previous heuristic, we look for the component  $i$ , by which a decrease of  $\Delta r_i$  in its reliability minimizes the ratio  $\Delta R / \Delta C$ , which means decrease as small as possible the system reliability  $R$ , but decreases more, the cost function  $C$ .

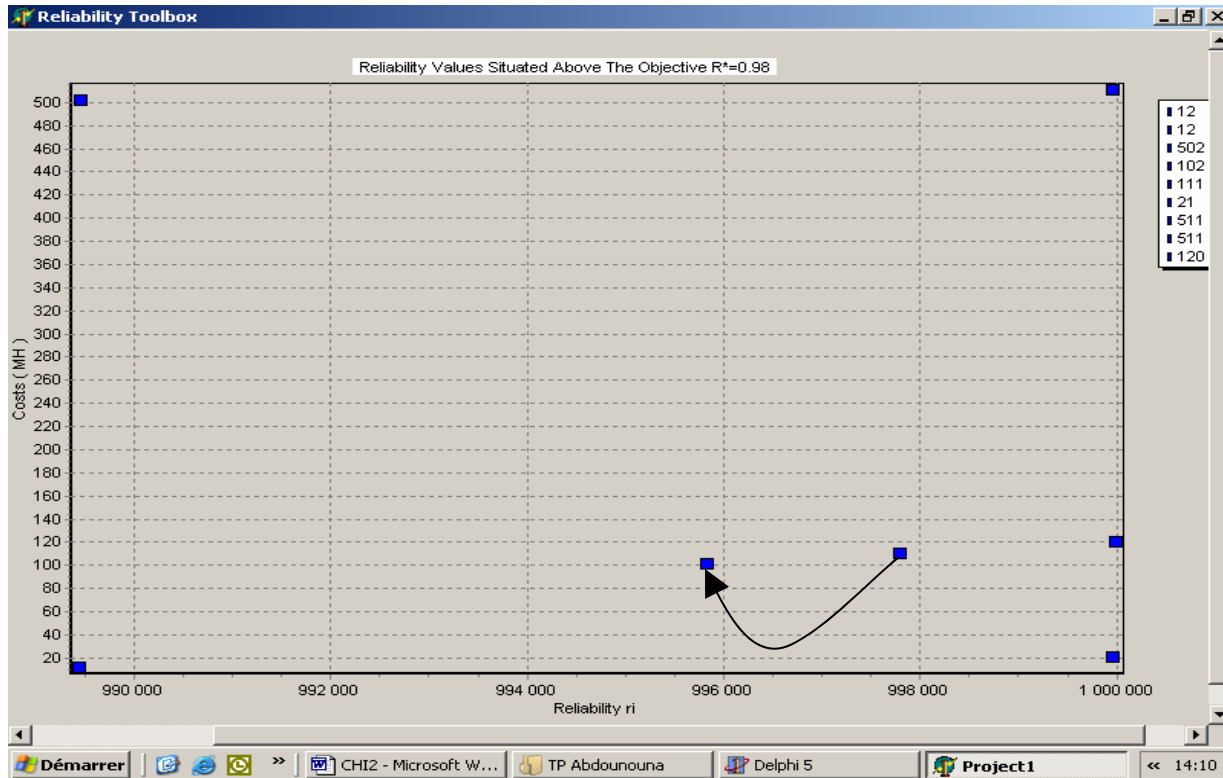
Evidently, this disallowance must only propose solutions greater or equal to the reliability objective  $R_{obj}$ .

In the previous example, the allowance results are without refinement, i.e., without disallowance procedure', are as follows  $R=0.99775$  for a cost of 111 MH.

With the disallowance procedure, the reliability of the system is  $R=0.99575$  for a cost de 100MH.

Therefore, the disallowance procedure is permitted, as we can note it in Figure IV.17, to reach the optimum, i.e. The nearest solution of  $R_{obj}=0.98$ , and with the least cost.

Reliabilities values situated above of the objective



**Figure IV.17 System reliability**

As we can note on figure IV.17, the dislocation procedure permits to avoid « to pass through » an optimum. In addition, we can note that the algorithm (with refinement) doesn't proposes the solution with a cost of 500MH, that certainly to the nearest reliability of  $R_{obj}=0.9775$ MH, but, presents a cost much greater with respect to other solutions (heuristic of disallowance).



## V CONCLUSIONS

A software program for dependability study have been developed .The advantage of the programs is that they are not constrained by any requirements pertaining to specific equipment or functional architecture. Architecture can be changed at will.

Furthermore the developed software program can describe any failure mode via its representative Boolean expression leading to its graphical representation .The software programs allow fault tree based

Dependability modelling and reliability analysis in the lights of which evaluation and improvements measures can be suggested; and this for various functional architectures with different components redundancies .

Renewal theory has been used to quantify the component availability using transfer functions. The transfer function approach leads to an adequate means for evaluating the availability of a complex multi system components and this whatever the law of distribution representing the failure/repair probability density function.

The second part of our work has addressed the problem of reliability requirements allocation for a system or subsystem.

In the published work in reliability requirements allocation indicate that the methods and techniques used are specific to a particular type of system architecture. Numerous existing allocation heuristic models deal with series-parallel architecture. We reviewed some different methods permitting to analyse this type of system, particularly, the weighted methods. we have noticed, on one hand, that these methods are not optimal, and on the other, that allocations suggested are often rather subjective because they depend directly on the user's judgment.

The series-parallel assumption used in various methods is already very restraining, we also note the absence of models in which components are all 2 by 2 different in cost. Generally, the assumption that components have identical cost functions in each subsystem is often made, something not necessarily true.

The objective being fundamentally to develop a method permitting to achieve reliability and availability requirements allocations, on systems of any type of architecture.

An algorithm of reliability and availability requirements allocation has been proposed to achieve the required level of reliability and availability with their appropriate allocations at a minimum cost. This is the dual problem which can be also solved using this algorithm. This iterative algorithm permits to allocate the redundancy level as well that the reliability of the subsystems.

The novelty of this algorithm stems for the fact that there is no constraint on the system architecture type, reliability and redundancy level allocation can be made concurrently.

Further more, we considered that components are quite different they do not have the same reliability and cost within subsystems, and it is possible to allocate the failure rates over interval of times adjusted according to components.

Application of the algorithm for several cases shows its quick convergence towards the most interesting solution of the allocation problem. It leads to the most economic solution at highest speed compared to other algorithms with similar objectives.

### **Suggestions for further work:**

Building on the present work the following points suggested as future studies:

- 1- The software program can be generalised for all dependability models state space models and non-state space models and increase its ability to draw large scale fault trees .and this can be done using more complex numerical techniques and algorithms .
- 2- The software program can be interfaced with an expert system or a Simulink model to allow comparison with on-line model in a survey communication protocol.

**Bibliography:**

- [1] M.Karakache, B.Nadji, A. Bourezg « application de la méthode de l'arbre des défaillances a la protection différentielles d'un turboalternateur » 3-rd international conférence on electrical engineering.
- [2] M.Karakache, B.Nadji, A. Bourezg « Application de l'analyse des modes de défaillance et leurs effets au disjoncteur haute tension » 3-rd international conférence on electrical and power engineering, Romania, octobre 2004.
- [3] M.Karakache, B.Nadji, A. Bourezg.FP4-1: "*Application of the FMEA and FTA for Analyzing Dependability of Generator Phase Fault Protection System*", IEEE Vehicle Power and Propulsion'04. Paris October 6-8 2004
- [4] Vincent Bernard.Laurent Caufriez,Dominique.Renaux « Modélisation des paramètres de la sûreté de fonctionnement par des fonctions de Transfert: Application à la disponibilité » .Conférence Internationale francophone d'automatique,Nantes 8-10 juillet 2002.
- [5] Raymond .Marie. Sébastien Pierron. « Algorithms for allocation of RAMS indicators"  $\lambda\mu$ 13-ESREL European Conference.2002.
- [6] A.Bourezg . B.Nadji Comparison between analytical methods for determining weibull parameters in reliability. Electrical engineering conference CGE'02 .Dec2002
- [7] Ramon Sandoval .Jean Leon Eternod. "Evaluation of methods for Breaker-flashover protection, Mexico ,2002
- [8] FRITZ A, BERTSCHE B, Analytic approach to the availability as a function of time, safety and reliability (1999).
- [9] E.Cabau,Cahier technique n°144 « Introduction à la conception de la sûreté »,Scheider , 1999
- [10] Zineb Simeu-Abazi, "Dependability of manufacturing systems", Ecole d'été d'automatique de Grenoble,1999
- [11] G.W. Scheer, "Answering Substation Automation Questions Through Fault Tree Analysis," Proceedings of the 4th Annual Texas A&M Substation Automation Conference, College Station, Texas, April 8–9, 1998.
- [12] COCOZZA THIVENT C, processus stochastiques et fiabilité des systèmes, SPRINGER(1997)
- [13] M.Bouissou and E.Bourgade. An availability evaluation and allocation at design stage for electric power plants: Methods and tools. Annual reliability and maintainability symposium,1997.
- [14] Ricardo Fricks, Mikilos Telek, Antonio Puliafito, and Kislior TrivRdi. Markov renewal

- theory applied to per formability evaluation. In KalloI Bagchi and George ZoLriat, editors, *State of the Art in Performance Modelling and Simulation of Advanced computer systems* : Applications and Systems, pages 193-238, Newark, NJ, EUA, Gordon and Breach Publishers, 1997
- [15] Sachin Garg Antonio Puliafito, Miklôs Telek and Kishor Trivedi. Analysis of preventive maintenance in transactions based software Systems. Submitted for publication, 1997.
  - [16] E.O. Schweitzer, III, B. Fleming, T.J. Lee, and P.M. Anderson, "Reliability Analysis of Transmission Protection Using Fault Tree Methods," Proceedings of the 24th Annual Western Protective Relay Conference, Spokane, Washington, October 21–23, 1997.
  - [17] Jogesh K. Muppala. Manish Malhotra, and Kishor S. Trivedi. Markov dependability models of complex Systems: Analysis techniques. In Süleyman Ozelaci, editor. Reliability and Maintenance of Complex System, pages 442-486, Berlim, Germany, 1996. Springer
  - [18] SOURISSE C, BOUDILLON L, la sécurité des machines automatisées, collections technique (1996).
  - [19] COX DR, théorie du renouvellement, DUNOD (1996).
  - [20] HANUS R, BOGAERTS P introduction a l'automatisme col,l de boeck université(1996)
  - [21] M-Bouissou and C.Brizec. Application of two generic availability allocation methods on a real life example. European conference on safety and reliability ,ESREL 96,1996.
  - [22] D.Kececioglu. Maintainability Availability), Operational Readiness Engineering. Prentice Hall PTR. 1995.
  - [23] R. A. Sahner, K- S. Trivedi, and A. Puliafito. "Performance and Reliability Analysis of Computer Systems: An Example- Based Approach. Using the SHARPE Software Package. Kluwer Academic Publishers, Dordrecht, Netherlands, 1995.
  - [24] DUBI A, GURVITZ N, A note on the analysis of systems with time dependent transition rates Ann.Nucl.Energy,vol 22 ,no3/4,pp.215-248(1995).
  - [25] PAGES A, GOURAN M, fiabilité des systèmes EYROLLES (1995)
  - [26] BON JL.Fiabilité des systèmes:méthodes mathématiques, technique stochastique (1995)
  - [27] G.Allain-Morin. I.M.Cloarec. L'allocation d'objectifs de sûreté de fonctionnement. en phase de spécification et de conception. European Safety and reliability conf.ESREL's 94,1994.
  - [28] IEEE C37.013-1993: IEEE Standard for AC High-Voltage Generator Circuit Breakers Rated on a Symmetrical Current. 1993
  - [29] K.K.Aggarwal. S.Guha. Reliability allocation in a general system with non-identical

- component's A practical approach. Microelectronics and reliability, vol33, N°8; 1993.
- [30] A-K.Dhingra. Optimal apportionment of reliability redundancy in serie is System under multiple objectives. IEEE Transactions on reliability, vol.R-41,N°4,pp576-582,1992.
- [31] J. B, Dugan, S. Bavuso, and M. Boyd. Dynamic fault-tree models for Fault-tolerant computer Systems. IEEE Transactions on Reliability, R- 4}SQ\.:SRS-377 Spn 1992.
- [32] BILLITON B, ALLAN RN, reliability evaluation of engineering systems, plenum press (1992)
- [33] D.Kececioglu. Reliability engineering handbook. vol.1. Prentice Hall PTR,1991
- [34] W.Kuo- H.H.Lin. Z.Xu. Optimization limits improving systems reliability .IEEE Transactions on Reliability N° 1 .pp51 -60, 1990.
- [35] U. Heimann, Ft. MittaJ, and K. S. Trivedi. Availability and reliability modelling of computer systems. In M. Yovits, editor, Advances in Computers, volume 31, pages 17S-233. Academic Press, San Diego, ÇA, 1990.
- [36] IEEE C84.1-1989: Voltage Ratings for Electric Power Systems and Equipment (60 Hz). 1989
- [37] G.H. Goiub and C- F. Van Loan. Matrix Computations. Mathematical Sciences. Johns Hopkms University Preas, Baltimore, MD, 2nd edition, 1989.
- [38] AFNOR ; french standards NF x60-500 Terminologies Relative à la fiabilité – maintenabilité disponibilité (1988).
- [39] VILLEMEUR A; sûreté de fonctionnement des systèmes industriels,EYROLLES(1988).
- [40] M. Baudot,Mme Dhoury,M Leray. Méthodologie d'allocation de fiabilité et de maintenabilité d'un système complexe.6<sup>eme</sup> colloque international de fiabilité et de maintenabilité. Strasbourg, 1988.
- [41] W.kuo. H.H.Lin. Z-Xu, and W.Zhang, reliability optimization with the Lagrange-multiplier and brunch and bound technique. IEEE Transactions on reliability N°5, pp624-630,1987.
- [42] R. A. Sahner and K, S, Trivedi. Performance and reliability analysis using directed acyclic graphs. IEEE Transactions on Software Engineering, SE- 13(10):1105-1114, Oct. 1987.
- [43] R. A. Sahner and K, S. Trivedi. Reliability modelling using SHARPE. IEEE Transactions on Reliability, R-36(2):186-193, June 1987.
- [44] IEEE C37.06-1987: AC High-Voltage Circuit Breakers Rated on a Symmetrical Current Basis—Preferred Ratings and Related Required Capabilities. 1987
- [45] IEEE C37.102-1987: IEEE Guide for AC Generator Protection. 1987

- [46] IEEE Std C37.10-1995:IEEE Guide for diagnostics and failure investigation of power power circuit breakers.1995
- [47] K.T.Fung. A philosophy for allocating component reliabilities in a network. IEEE transactions on reliability, vol R-34, N° 2, pp 151-153, 1985.
- [48] J. C, Laprie- dependable computing and fault-tolerance: Concepts and terminology. In Proceedings of the Fifteenth International Symposium os Fault- Tolerant Coputing, pages 2-7, Los Alamitos, ÇA, July 1985- IEEE Computer Society Press.1985
- [49] C.H. Flurscheim “Power circuit breaker theory and design “, IEE power engineering series , 1982.
- [50] IEEE C37.09-1979: IEEE Standard Test Procedure for AC High-Voltage Circuit Breakers Rated on a Symmetrical Current Basis. 1979
- [51] C.L.Hwang, F.A.Tillman, W.Kuo. Reliability optimization by generalized lagrangian functions and reduced Gradient methods. IEEE Transactions on reliability .N°4.pp316-319, 1979,
- [52] C. Singh, R. Billing ton, and S. Y- lee. The method of stages for non-Markovian models. IEEE Transactions on Reliability, 26(2); 135-137, June1977.
- [53] S.K Banerje. K-Rajamani. S.S.Deshpande. Optimal Redundancy Al location for non serie-parallel networks. IEEE transactions on reliability , vol. R-25,N°,pp115-118,1976,
- [55] B.M, Fussel, How to hand-calculate system reliability characteristics- IEEE transactions on reliability, N°3, 1975.
- [56] K.K.Aggarwal. J.S.Gupla. and K.B.Misra. A new heuristic criterion for solving a redundancy optimization problem- IEEE Transactions on reliability N° 1, pp 86-87, 1975.
- [57] M. Messinger. M.L.Shooman. Techniques for optimum spares allocation: a tutorial review. IEEE Transactions on Reliability. Vol R-19.N4pp 156-166.1970
- [58] M, L. Shooman. The equivalence of reliability diagram and fault-tree analysis, IEEE Transactions on Reliability, R-19 (5). 74-75. May 1970.
- [59] Z.W.birnbaum. on the importance of different components systems. Multivariable analysis11.1969.
- [60] C, Fröberg. Introduction to Numerical Analysis, 2nd. ed. Addision-Wesley, Reading, MA, USA, 1969-
- [61] S. Balaban and R.H. Jeffers. The allocation of system reliability: Development of procedures for reliability al local ion and testing. Technical report, directorate of operational support engineering .US air force, 1962.

- [62] D. R. Cox. The analysis of non-Markovian stochastic processes by the inclusion of supplementary variables. Proc. Camb. Philos. Soc. 51(3):433-441, 1955.