Introduction

Dependability: a generic term encompassing the concepts of reliability, availability, maintainability, security, etc. It is also simply designated by the term "reliability", which underlines its quantitative aspect.

The aim of reliability is the study of systems (sets of elements – hardware, software, human resources – that interact with a view to accomplishing a mission) that are subjected to physical processes such as the processes of failure, repair, and stresses.

The component is a part of a system which is non-resolvable within the framework of the study for which sufficient qualitative information (functioning, modes of failure, etc.) as well as quantitative information (failure rate, repair rate, etc.) has been provided in this study. The notion of component is relative and depends on the study. For example, an aircraft, within the framework of a study dealing with flight safety, represents the system, whereas for the airline company it represents a component.

The study of failures in components has led to very elaborate classifications. The failures that have been taken into account in this book are catastrophic failures, that is to say, they are sudden and complete.

As for reliability, the part that deals with the modeling of the components with a view to obtaining qualitative and quantitative information is called "component reliability" or "reliability statistics". Another part of reliability, called the "reliability of systems", is concerned with the modeling of systems with a view to studying their reliability according to the reliability of their components. The reliability of the systems and the component reliability can be complementary in that the results of the former form the data for the latter.

In this book, we will consider diverse classes of systems: in general, many criteria such as those regarding the number of system components with single- or multi-components, the system's structure function presenting a certain form of coherence or non-coherence, state spaces (system and components), binary systems or multi-performance systems, maintenance systems that are non-repairable, reliably repairable, repairable, the mission expressed by a structure function or not have been used.

Considerable diversity exists among reliability models. Excluding the diverse theories, prolongation and applications, we will be considering two large families, namely, models of minimal sets (cut sets and minimal paths) and models involving stochastic processes. The former, not possessing the accuracy and analytical comfort of the latter, have the advantage of considerably reducing the size of problems and of enabling, in most cases, their resolution.

From an algorithmic viewpoint, the complexity of systems in terms of reliability is generally determined by different elements such as a large number of components, a non-classical structure, the existence of certain forms of non-coherence, many levels of performance, extensive variables, non-constant hazard rates, stochastic dependences, and the coexistence of the three elements that is hardware-software-human factor. The problem of evaluating the reliability of a system is an NP-difficult problem ([ROS 75]), that is to say, there is no algorithm whose time execution is limited by a polynomial function of the problem's size (i.e., number of components), unless, for any class of problems considered as being difficult, there exists a polynomial algorithm.

The main problem of reliability is the construction of the structure function and the probabilistic risk assessment.

Fault trees: the fault tree (FT) forms part of the family of models called minimal sets, that is, the models using the minimal cut sets and/or the minimal paths for studying the reliability of systems. It was developed with the aim of making it possible to obtain the cut sets of complex systems. At present, the FT constitutes one of the most widely employed methods in the domain of the reliability of systems.

Designed by Watson 1962 in the laboratories of the "Bell Telephone Company" and within the framework of the project involving the "ICBM minuteman" missiles ordered by the US Air Force, it saw three stages of development. Initially, during the 1960s, it served as a tool for representing system failures but in the absence of the techniques and algorithms that are specific for its treatment. Subsequently, Haasl introduced the basic rules for the construction of the FTs in 1965, Vesely in 1970 [VES 70] supplied us with the "Kinetic Tree

Theory" called Kitt, where, through the underlying stochastic processes, the design of the FTs has become more complete; this theory remains the main tool for the quantitative evaluation of the FTs until now. At the same time, Fussell and Vesely [FUS 72] developed and perfected the MOCUS algorithm, which is distinct from the algorithms of combinatorial character. The third stage of development, in the 1980s, was marked by the extension of this theory to the non-coherent fault trees, multistate fault trees and fuzzy fault trees.

Recently, a new algorithm has considerably improved the calculation performances and has offered the possibility of large FTs; the algorithm described in this study is based, on the one hand, on recursive algorithms that do not require prior information of the minimal sets of the FT and, on the other hand, on the truncation algorithms of minimal cut sets.

The FT is a purely deductive technique. An FT represents a failure mode of a system according to the failure modes of its subsystems and components. The term "fault tree" is to a certain extent restrictive; for example, we will go on to discuss a dual FT which, in principle, represents the good functioning of a system (in the case of binary systems) is described in this study. Barlow and Proschan [BAR 75] make use of the term "event tree" and not "fault tree") for designating an FT; this term also adds to the ambiguity, for it also designates the inductive event trees [LIM 84]. For distinguishing it from the latter, we could use the term "deductive events tree". Nevertheless, in this book, we will be focusing on the use of the traditional term of "fault tree"; however, in a number of cases, it will not represent the failure but the good functioning of the systems.

Figure 1 shows the essential stages for the evaluation of the reliability of a system (1-4-5), that is, proceeding from the system, we obtain its structure function that we will introduce in a model of probabilities for evaluating its reliability. Obtaining the function of structure from the system is a difficult task and, except in the case of simple systems (in principle, systems of elementary structure), this cannot be done without special tools for the majority of complex systems. Thus, modeling of the system is obtained through standard graphs, of which FT is part, for obtaining in a systematic manner the structure function. As a result, the FT is employed right from the first stages of safety analysis for the functioning of the systems. The safety study of a system through FT includes three stages: the construction of the tree, qualitative analysis and quantitative analysis. This construction should be highly exhaustive, that is, representing all the (significant) causes for the failure of the system. The construction technique can be obtained quit quckly, which greatly facilitates the collaboration of specialists of diverse domains.

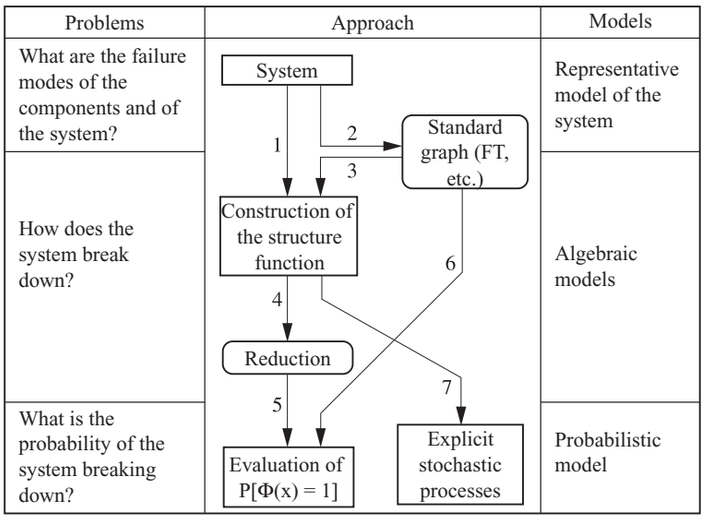

Figure 1 *Problems, approach and models for evaluating the reliability of systems*

The qualitative analysis deals with methods for obtaining the minimal sets: minimal cut sets and minimal paths. The quantitative analysis comprises on the one hand the evaluation of the probability of the top event (within the framework of the preliminary analysis of the risks, this event is called "undesirable") and on the other hand the study of influence concerning the sensitivity and the importance of the basic events vis-à-vis the top event. The evaluation of the probability of the top event can be carried out directly on the FT without passing through the minimal sets, when the FT does not contain repeated events. Another use for the FT, particularly for its minimal cut sets, is concerned with the division of the spaces of states into states of running and into states of breakdown of the systems modeled by the stochastic processes.

The undisputed efficacy of FTs for representing failures of complex systems encounters difficulties when probabilistic treatment is concerned. This is a limitation that is common to the methods based on minimal sets and is linked to the two following impossibilities: one representing the exact calculation of the reliability for the systems with repairable components and the other concerned with the calculation in case of certain dependences. In actual practice, we overcome this limitation by making an approximate calculation,

which in the case of the systems of a good reliability is having the correct accuracy.

The FT is used at first for analyzing the failures of the hardware and then for modelizing human failures or errors [DHI 86]. Its use is still very much limited in the software domain [LEV 83]. In principle, the FT can contain events concerning the software but is used very rarely for analyzing a software independent of its application.

Organization of the book: the FTs are at first presented for modeling the coherent binary systems, we refer to them as coherent FTs (c-FTs). Then, we face certain extensions such as the non-coherent FTs (nc-FTs) and the FTs with restrictions (FT-r), which represent a generalization of the nc-FT and the multistate FTs (m-FTs).

Before FTs are described, it is important to present in Chapters 1 and 2 the basic elements necessary for the study of FTs. In Chapters 3–9, FTs are discussed. In Chapter 10, the elements of stochastic simulation for FTs will be presented.

Chapter 1 deals with the basic relationships concerning the reliability of the binary component, wherein the notions of reliability, availability, maintainability, MTTF, etc., are introduced and expressed through their analytical expressions.

Chapter 2 presents the structure function, which will form the basis for the later development, the diverse classes of systems (systems with elementary structure, systems with complex structure, etc.), the reliability function and the general methods of evaluation.

Chapter 3 deals with the construction of FTs: the different graphic symbols and the stages of construction.

Chapter 4 covers qualitative treatment, that is, the search for minimal sets, and also the corresponding classical algorithms.

Chapter 5 deals with quantitative treatment: the diverse methods of evaluating the probability of the top event and the essential methods for the evaluation of large FTs.

Chapter 6 gives a study of influence: the uncertainty or the sensitivity and the importance, followed by the methods of calculating the uncertainty and the most well-known factors of importance.

Chapter 7 deals with the modularization of FTs, multi-phase FTs and the treatment of common failure modes.

Chapter 8 presents certain extensions: non-coherent FTs, delayed action FTs, FTs with restrictions and multistate FTs.

Chapter 9 presents new algorithms based on the binary decision diagrams (BDD).

Chapter 10 presents the stochastic simulation (or Monte Carlo method) for the evaluation of the probability of the top event and other quantities.

In this book, for designating the different parts of a system, apart from the notions of "system" and "component", the notion of the "sub-system" is used; it designates a part of a system containing at least one component and is endowed with a sub-mission within the framework of the overall aim. For designating without any special discrimination, a system, a subsystem or a component, we make use of the notion of "item".