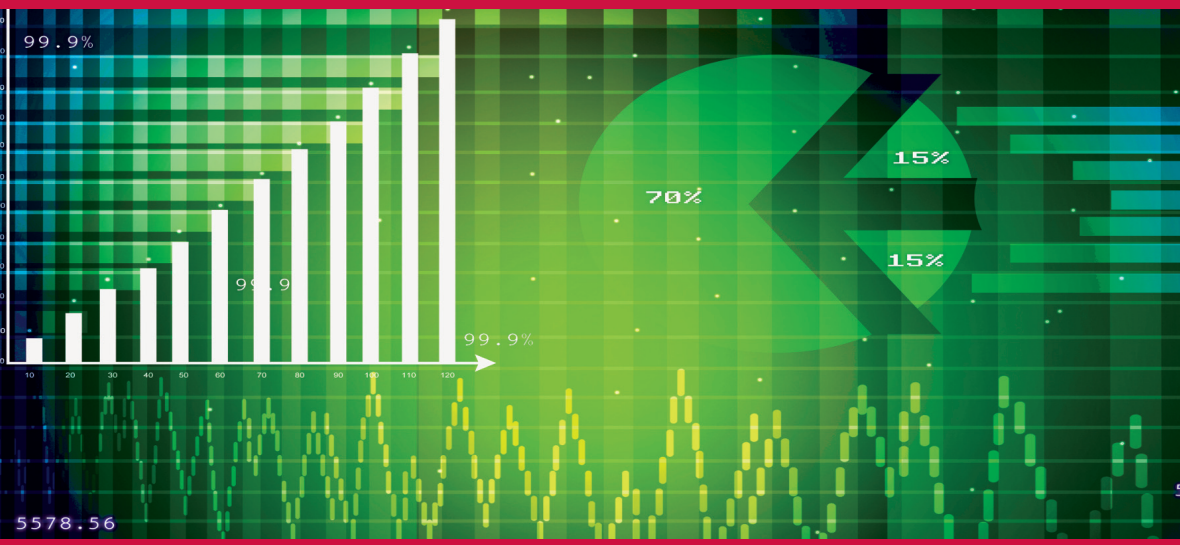
FOCUS

RISK MANAGEMENT AND DEPENDABILITY SERIES



Systems Dependability Assessment

Modeling with Graphs and Finite State Automata

Jean-François Aubry
Nicolae Brinzei

ISTE

WILEY

Systems Dependability Assessment

FOCUS SERIES

Series Editor Jean-François Aubry

Systems Dependability Assessment

Modeling with Graphs and Finite State Automata

Jean-François Aubry
Nicolae Brînzei

ISTE

WILEY

First published 2015 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.wiley.com

Library of Congress Control Number: 2014956809

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISSN 2051-2481 (Print)
ISSN 2051-249X (Online)
ISBN 978-1-84821-765-2

Contents

Preface

Systems dependability assessment

Systems dependability assessment! Many excellent books deal with this subject and describe its evolution from its beginning, at the end of World War II. We can recall the ability of the first computers that were occasionally in an operating state. From this time, a lot of robust methods and tools made the analysis and the assessment of their failures possible, in order for the potential users of these new technologies to rely on them. The word "reliability" was born. The safe development of electronics and then of computing, aerospace and nuclear technologies became possible. So it is logical to ask the question of the relevancy of a new book. In fact, it was found that the simplifying hypotheses commonly used to access the predictive measures of reliability are sometimes difficult to justify and that they can produce pessimistic values compared to the feedback experience or optimistic forecasting of rare dangerous events. This induced a lot of research in the specialized community, for example in the Automatic Control Research Center (*Centre de Recherche en Automatique de Nancy* – CRAN) of the University of Lorraine, France.

These are some of the works that we will modestly report in this book. They constituted significant contributions to recent approaches of predictive dependability due to resorting to concepts developed in automatic control but not yet turned to account of dependability. We

can cite, for example, graph theory, finite-state automata, Petri nets, Bayesian approach and fuzzy sets.

These developments spanned over approximately the last two decades and gave some original advances in the field, and it is difficult for us not to make a connection with the Nancy School of Art Nouveau one century ago. In fact, perhaps we could have called this book Systems Dependability Assessment; Beyond traditional approaches, the Nancy School!

Let us enter now into more technical and scientific considerations to give the clarifications that the title of this book deserves.

Dependability

The CEI 50 (191) standard [IEC 90] defines dependability as the ability of an entity to assume one or more requested functions in given conditions. This very general and non-quantitative notion may be further specified by its generally associated attributes which are [LAP 95]: hindering or barriers, achievement means, validation means and measures. Our contribution rightly takes a place within the latter, and especially in quantitative measures. Nevertheless, it is difficult to give a single value for this measure as the dependability is actually a concept including three components [IEC 90]: reliability, maintainability and availability. These three components, as well as their measures which are probabilities, are formally defined in the CEI 50 (191) standard. The lifetime (or time before failure) and the repair time of an entity are considered as random time variables whose distribution functions define, respectively, the reliability and the maintainability of the entity. The availability is the probability for the entity of being in operation at a given time instant, knowing that the entity could have been alternatively in operation or in repair states. Its asymptotic value is generally an interesting measure. In the Appendix, the basic mathematical definitions are recalled.

However, the CEI 50 (191) standard does not consider safety as a component of dependability. Safety is the ability of an entity to avoid the appearance of critical or catastrophic events that may affect

equipment or staff. The measure of the safety may be defined as a probability; however, it is also important to assess it with regard to the consequence of the occurrence of these critical or catastrophic events. This leads to the concept of risk, a risk being evaluated by the association of the occurrence frequency (or probability) of a dangerous event and the damage it induces on goods, people and environment. It is not the main purpose for this book to deal with risk management; nevertheless, it may be considered that a system may be in a dangerous state as well as in an availability state, both being sometimes compatible. As we will see later, it is possible to assess the probability for a system of being in any subset of its possible states and, for example, the subset of safe states. We can find in the CEI 61508 [IEC 98] a probabilistic approach of the functional safety that we can qualify as the reliability of systems responsible for safety loops in industrial plants. That is why it is difficult not to consider safety as a fourth element of dependability, especially when it is a matter of probabilistic assessment. Many authors and agencies prefer the RAMS acronym for reliability, availability, maintainability and safety instead of dependability. However, RAMS has a wider extension, covering all the attributes of dependability and safety: hindering, achievement means, validation means, and quantitative as well as qualitative measures.

System

By the term "system", we mean a set of components interacting together to perform one or more predefined functions. Components and system are included in the definitions of "dependability" under the generic term "entity"; however, their measures are issued from different approaches. For the components, they are based, for example, on known probabilistic laws whose parameters are adjusted from statistical data. For a system, the dependability measure is a prediction obtained by a dedicated model starting from the knowledge of the dependability measures of its components.

This definition of system does not evoke the complexity level of the system. The complexity may be expressed in terms of number of components, but it must be more particularly understood in terms of

interactions between them. As we will see, many types of models may be combined to describe these interactions and the solving method may be a matter of analytical calculus or simulation process. For large systems, it is usual to build hierarchical models with several levels of subentities, etc. It is not our purpose to discuss system engineering and we will only consider a sole decomposition level with the objective of finding a relationship model between one dependability measure of a system and that of its components.

Assessment

In the dependability or RAMS domain, two types of assessment are predominantly performed: qualitative and quantitative. Qualitative assessment is generally performed as a preliminary study to identify and qualify the components, events, interactions and limits of the system in order to eventually be able to start the quantitative assessment which must be understood as the set of means, methods and tools to give a quantitative measure of the systems dependability. As said previously, this measure is predictive and is based on models. These models are very large in number and more or less known for a long time, and it is not our goal to give an exhaustive description.

Jean-François AUBRY
December, 2014

Introduction

In this book, we are interested in the problem of characterizing the probabilistic indicators of the dependability of a complex system knowing *a priori* the dysfunctional characteristics of their components. These components may be material (machines, hardware, devices, structures, subsystems, etc.), immaterial (software, strategies, etc.) or people (designers, operators, repairers, etc.). It is supposed that the definition, the modeling and the assessment of the dysfunction of these components are well known as an issue of the application of probabilities and statistics theories. The reader may refer to so many books and publications on the subject that it is impossible to mention them all. We will only cite, for example, the following authors: Meeker [MEE 98], Modarres [MOD 93] and Cocozza [COC 97].

It may be thought that all, or almost all, has been written on the dependability of systems and that the electronics, aeronautic, space, chemical, transportation or nuclear industries practice this activity with expertise. Nevertheless, the interest developed in the past 20 years by many research experts on the so-called "dynamic reliability" shows that this is not exactly the case. A community of specialists is engaged in reconsidering a lot of simplifying hypotheses requested for the elaboration of analytical models but leading to the risk of impasses relative, for example, to insidious conditions, rare event sequences or complex interactions between functional and dysfunctional behaviors.

More extensively considering all the problems impacting a dependability assessment process today becomes possible due to the borrowing of concepts developed in other scientific domains and due to the power improvement of engineering tools (computers, network, languages, software, etc.).

From such a perspective, we propose in Part 1 to revisit the traditional approach of systems reliability modeling by the means of the monotone structure function concept and its representation by a graph, the concept that we will progressively transform in Part 2 into that of stochastic hybrid automaton. So, we will take advantages of concepts developed in the fields of graph and finite-state automata theories in which probabilistic aspects have been introduced.

We will present some simple examples and the associated tools to illustrate the pedagogical approach as well as results obtained with more complex case studies in the context of research programs. We thank Dr G.-A. Perez Castaneda and Dr G. Babykina for their important contribution to the research partially reported in the final part.

PART 1

Predicted Reliability of Static Systems; a Graph-Theory Based Approach

1

Static and Time Invariant Systems with Boolean Representation

A system whose outputs are only dependent at any time on its variables states is generally called a time invariant system or stationary system. Furthermore, a static system is a system whose outputs do not depend on the past of its inputs; it has no memory. Translated in the context of reliability, these definitions become: at any time, the same combination of components states induces the same state of the system and, at a given time, the knowledge of the reliability of each component is sufficient to access the reliability of the system. In addition, we will only consider in this section systems and components with Boolean behaviour ("ON or Operating" and "FAIL" states that will be represented by the Boolean variables "1" and "0").

1.1. Notations

Let us suppose that a system S with Boolean states is composed of r components c_i. The state of a component c_i is defined by the Boolean variable u_i. We will use the following notation:

– $C = \{c_1, c_2, ..., c_r\}$ the set of the r components,

– $\mathcal{U} = (u_1, u_2, ..., u_r)$ the Boolean word representing the states of the components with $u_i \in \mathbb{B} = \{0, 1\}$, so $\mathcal{U} \in \mathbb{B}^r$ can take at most 2^r different values (the system's state number is generally lower than

2^r because some degradation states are inaccessible, the system being stopped beforehand).

1.2. Order relation on $\mathcal{U}$

Let us recall that a relation R on a variable set is an order relation if it is reflexive (aRa), antisymmetric (aRb and $bRa \Longrightarrow a = b$) and transitive ($aRb$ and $bRc \Longrightarrow aRc$). A set provided with such a relation is an ordered set. In the Boolean set $\mathbb{B}$, two operations establish an order: the identity operation noted $\odot$ and the implication operations sometimes noted $\leqslant$ and $\geqslant$, (analog of the operations defined on the integers with the same symbols).

Let us now consider two distinct values of $\mathcal{U} \in \mathbb{B}^r : \mathcal{A} = (a_1, a_2, ..., a_r)$ and $\mathcal{B} = (b_1, b_2, ..., b_r)$. We will say that:

– $\mathcal{A} = \mathcal{B}$ if and only if $\forall i \in (0, 1, ..., r), a_i = b_i$;

– $\mathcal{A} \succcurlyeq \mathcal{B}$ (read $\mathcal{A}$ upper bounds $\mathcal{B}$) if and only if $\forall i \in (0, 1, ..., r), a_i \geqslant b_i$;

– $\mathcal{A} \preccurlyeq \mathcal{B}$ (read $\mathcal{A}$ lower bounds $\mathcal{B}$) if and only if $\forall i \in (0, 1, ..., r), a_i \leqslant b_i$.

It is really a matter of order relations on $\mathbb{B}^r$ because it is reflexive ($\mathcal{A} \preccurlyeq \mathcal{A}$ and $\mathcal{A} \succcurlyeq \mathcal{A}$), transitive ($\mathcal{A} \succcurlyeq \mathcal{B}, \mathcal{B} \succcurlyeq \mathcal{C} \Longrightarrow \mathcal{A} \succcurlyeq \mathcal{C}$ and $\mathcal{A} \preccurlyeq \mathcal{B}, \mathcal{B} \preccurlyeq \mathcal{C} \Longrightarrow \mathcal{A} \preccurlyeq \mathcal{C}$) and antisymmetric ($\mathcal{A} \succcurlyeq \mathcal{B}, \mathcal{B} \succcurlyeq \mathcal{A} \Longrightarrow \mathcal{A} = \mathcal{B}$ and $\mathcal{A} \preccurlyeq \mathcal{B}, \mathcal{B} \preccurlyeq \mathcal{A} \Longrightarrow \mathcal{A} = \mathcal{B}$).

For example we can write: $(1, 0, 0, 1, 0) \preccurlyeq (1, 1, 0, 1, 0) \preccurlyeq (1, 1, 0, 1, 1)$

But $(1, 0, 1, 1, 0)$ is not in relation with $(1, 1, 0, 1, 0)$.

A drawing of this order relation is given by its Hasse diagram [VEL 05], that is to say, a graph in which the nodes are the possible values of $\mathcal{U}$ and the arcs are the representations of the order relation. It is a subset of the sagittal diagram of the relation where the loops and the arcs representing respectively the reflexivity and the transitivity properties are removed. Such a structure is sometimes called r-cube [ARN 97].