NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
61165

Deuxième édition
Second edition
2006-05

Application des techniques de Markov

Application of Markov techniques

Numéro de référence
Reference number
CEI/IEC 61165:2006

Numérotation des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000. Ainsi, la CEI 34-1 devient la CEI 60034-1.

Editions consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

Informations supplémentaires sur les publications de la CEI

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique. Des renseignements relatifs à cette publication, y compris sa validité, sont disponibles dans le Catalogue des publications de la CEI (voir ci-dessous) en plus des nouvelles éditions, amendements et corrigenda. Des informations sur les sujets à l'étude et l'avancement des travaux entrepris par le comité d'études qui a élaboré cette publication, ainsi que la liste des publications parues, sont également disponibles par l'intermédiaire de:

- **Site web de la CEI (www.iec.ch)**
- **Catalogue des publications de la CEI**

  Le catalogue en ligne sur le site web de la CEI (www.iec.ch/searchpub) vous permet de faire des recherches en utilisant de nombreux critères, comprenant des recherches textuelles, par comité d'études ou date de publication. Des informations en ligne sont également disponibles sur les nouvelles publications, les publications remplacées ou retirées, ainsi que sur les corrigenda.
- **IEC Just Published**

  Ce résumé des dernières publications parues (www.iec.ch/online_news/justpub) est aussi disponible par courrier électronique. Veuillez prendre contact avec le Service client (voir ci-dessous) pour plus d'informations.
- **Service clients**

  Si vous avez des questions au sujet de cette publication ou avez besoin de renseignements supplémentaires, prenez contact avec le Service clients:

  Email: custserv@iec.ch
  Tél: +41 22 919 02 11
  Fax: +41 22 919 03 00

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site (www.iec.ch)**
- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (www.iec.ch/searchpub) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.
- **IEC Just Published**

  This summary of recently issued publications (www.iec.ch/online_news/justpub) is also available by email. Please contact the Customer Service Centre (see below) for further information.
- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

  Email: custserv@iec.ch
  Tel: +41 22 919 02 11
  Fax: +41 22 919 03 00

.

NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
61165

Deuxième édition
Second edition
2006-05

Application des techniques de Markov

Application of Markov techniques

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE V

Pour prix, voir catalogue en vigueur
For price, see current catalogue

SOMMAIRE

CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

APPLICATION DES TECHNIQUES DE MARKOV

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 61165 a été préparée par le Comité d'études 56 de la CEI: Sûreté de fonctionnement.

Cette seconde édition annule et remplace la première édition publiée en 1995. Elle constitue une révision technique. Cette révision était nécessaire pour faciliter l'application de cette norme pour les analyses de sécurité de même que pour l'importance accrue du solutions numérique comparativement aux solutions analytiques des techniques de Markov.

Les principaux changements par rapport à l'édition précédente sont les suivants:

- les annexes supplémentaires avec application d'exemples ont été retirées.
- la terminologie mathématique et les symboles ont été mis à jour.
- la terminologie a été harmonisée.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

APPLICATION OF MARKOV TECHNIQUES

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61165 has been prepared by IEC technical committee 56: Dependability.

This second edition cancels and replaces the first edition published in 1995, and constitutes a technical revision. The revision was necessary in order to facilitate the application of this standard for safety analysis as well as the increased importance of numerical solutions compared to analytical solutions of Markov techniques.

The main changes with respect to the previous edition are the following:

- additional annexes with application examples have been removed.
- the mathematical terminology and symbols have been updated.
- terminology has been harmonised.

Le texte de la présente norme est issu des documents suivants:

FDIS	Rapport de vote
56/1096/FDIS	56/1111/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette Norme.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 3.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous «http://webstore.iec.ch» dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite;
- supprimée;
- remplacée par une édition révisée, ou
- amendée.

The text of this standard is based on the following documents:

FDIS	Report on voting
56/1096/FDIS	56/1111/RVD

Full information on the voting for the approval of this standard can be found in the voting report indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

INTRODUCTION

Plusieurs méthodes analytiques différentes sont disponibles pour évaluer la fiabilité, la disponibilité, la maintenabilité et la sécurité. L'analyse de Markov est l'une de ces méthodes. La CEI 60300-3-1 donne une vue d'ensemble des méthodes disponibles et de leurs caractéristiques générales.

Cette norme définit la terminologie de base et les symboles pour l'application des techniques de Markov. Elle décrit des règles fondamentales pour le développement, la représentation et l'application des techniques de Markov de même que les hypothèses et les limitations de cette approche.

INTRODUCTION

Several distinct analytical methods for reliability, availability, maintainability and safety analysis are available of which the Markov technique is one. IEC 60300-3-1 gives an overview of available methods and their general characteristics.

This standard defines the basic terminology and symbols for the application of Markov techniques. It describes ground rules for the development, representation and application of Markov techniques as well as assumptions and limitations of this approach.

APPLICATION DES TECHNIQUES DE MARKOV

1 Domaine d'application

Cette Norme internationale fournit un guide sur l'application des techniques de Markov pour analyser et modéliser un système, et estimer la fiabilité, la disponibilité, la maintenabilité et les mesures de sécurité.

Cette norme est applicable à toutes les industries où les systèmes, qui présentent un comportement dépendant de leur état, doivent être analysés. Les techniques de Markov couvertes par cette norme supposent des fréquences de changement d'état constantes, indépendantes du temps. De telles techniques sont souvent appelées globalement «techniques de Markov».

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60050(191):1990, *Vocabulaire Electrotechnique International (VEI) – Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 60300-3-1, *Gestion de la sûreté de fonctionnement – Partie 3-1: Guide d'application – Techniques d'analyse de la sûreté de fonctionnement: Guide méthodologique*

CEI 61508-4:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de la CEI 60050(191):1990 ainsi que les suivants s'appliquent.

NOTE Pour faciliter l'application de cette norme pour les évaluations de la sécurité, la terminologie de la CEI 61508 est utilisée quand c'est approprié.

3.1
système
ensemble d'éléments interactifs ou reliés entre eux

[ISO 9000, 3.2.1]

NOTE 1 Dans le contexte de la sûreté de fonctionnement, un système aura un but précis exprimé en termes de fonctions prévues, de conditions établies d'exploitation/utilisation, et de limites définies.

NOTE 2 La structure d'un système peut être hiérarchique.

3.2
élément
composant ou ensemble de composants, qui fonctionne comme une entité individuelle

NOTE Un élément peut généralement prendre deux états: disponible ou indisponible (voir 3.4 et 3.5). Pour des raisons pratiques, le terme **état d'élément** sera utilisé pour désigner l'état d'un élément.

APPLICATION OF MARKOV TECHNIQUES

1 Scope

This International Standard provides guidance on the application of Markov techniques to model and analyze a system and estimate reliability, availability, maintainability and safety measures.

This standard is applicable to all industries where systems, which exhibit state-dependent behaviour, have to be analyzed. The Markov techniques covered by this standard assume constant time-independent state transition rates. Such techniques are often called homogeneous Markov techniques.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050(191):1990, *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

IEC 60300-3-1: *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability: Guide on methodology*

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050(191):1990 and the following apply.

NOTE To facilitate the application of this standard for safety evaluations, the terminology from IEC 61508 is used where appropriate.

3.1
system
set of interrelated or interacting elements

[ISO 9000, 3.2.1]

NOTE 1 In the context of dependability, a system will have a defined purpose expressed in terms of intended functions, stated conditions of operation/use, and defined boundaries.

NOTE 2 The structure of a system may be hierarchical.

3.2
element
component or set of components, which function as a single entity

NOTE An element can usually assume only two states: up or down (see 3.4 and 3.5). For convenience the term **element state** will be used to denote the state of an element.

3.3
état du système
X(t)
combinaison particulière des états d'élément

NOTE $X(t)$ est l'état du système au temps t. Il y a d'autres facteurs qui peuvent avoir un effet sur l'état du système (par exemple mode de fonctionnement).

3.4
état de disponibilité
état d'un système (ou élément) dans lequel le système (ou élément) est capable d'accomplir la fonction requise

NOTE Un système peut avoir plusieurs états de disponibilité distincts (par exemple états totalement opérationnels et états dégradés).

3.5
état d'indisponibilité
état d'un système (ou élément) dans lequel le système (ou élément) qui n'est pas capable d'accomplir la fonction requise

NOTE Un système peut avoir plusieurs états d'indisponibilité distincts.

3.6
danger
source potentielle de blessure corporelle ou de dommage pour la santé des personnes ou pour les biens

[CEI 61508-4, 3.1.2, modifiée]

3.7
défaillance dangereuse
défaillance mettant potentiellement le système relatif à la sécurité dans un état de danger ou dans l'impossibilité d'exécuter sa fonction

[CEI 61508-4, 3.6.7, modifiée]

NOTE 1 Le fait que cette potentialité se réalise ou pas peut dépendre de l'architecture du système.

NOTE 2 Le terme de défaillance à risque ou défaillance dangereuse est communément utilisé dans ce contexte.

3.8
défaillance sans risque
défaillance ne mettant pas potentiellement le système relatif à la sécurité dans un état de danger ou de défaillance fonctionnelle

[CEI 61058, modifiée]

3.9
transition
passage d'un état à un autre

NOTE La transition a lieu généralement suite à une défaillance ou un rétablissement. Une transition peut aussi être provoquée par d'autres événements tels que des erreurs humaines, des événements extérieurs, la reconfiguration de logiciel, etc.

3.10
probabilité de transition
$P_{ij}(t)$
probabilité conditionnelle de transition d'un état i à un état j dans un intervalle de temps donné (s, $s+t$), avec le système à l'état i au début de l'intervalle de temps

NOTE 1 De façon formelle $P_{ij}(s, s+t) = P(X(s+t) = j \mid X(s) = i)$. Lorsque le procédé de Markov est homogène dans le temps alors $P_{ij}(s, s+t)$ ne dépend pas de s et est désigné comme $P_{ij}(t)$.

NOTE 2 Pour qu'un procédé de Markov soit non réductible (par exemple si tous les états peuvent passer de l'un à l'autre) cela tient à $P_{ij}(\infty)=P_j$, où P_j est la probabilité d'état stationnaire et asymptotique de l'état j.

3.3
system state
X(t)
particular combination of element states

NOTE $X(t)$ is the state of the system at time t. There are other factors that may have an effect on the system state (e. g. mode of operation).

3.4
up state
system (or element) state in which the system (or element) is capable of performing the required function

NOTE A system can have several distinguishable up states (e.g. fully operational states and degraded states).

3.5
down state
system (or element) state in which the system (or element) is not capable of performing the required function

NOTE A system can have several distinguishable down states.

3.6
hazard
potential source of physical injury or damage to the health of people or property

[IEC 61508-4, 3.1.2, modified]

3.7
dangerous failure
failure which has the potential to put the safety-related system in a hazardous state or fail-to-function state

[IEC 61508-4, 3.6.7, modified]

NOTE 1 Whether or not the potential is realised may depend on the architecture of the system.

NOTE 2 The term unsafe failure or hazardous failure is also commonly used in this context.

3.8
safe failure
failure which does not have the potential to put the safety-related system in a hazardous state or fail-to-function state

[IEC 61508, modified]

3.9
transition
change from one state to another state

NOTE Transition takes place usually as a result of failure or restoration. A transition may also be caused by other events such as human errors, external events, reconfiguration of software, etc.

3.10
transition probability
$P_{ij}(t)$
conditional probability of transition from state i to state j in a given time interval (s, $s+t$) given that the system is in state i at the beginning of the time interval

NOTE 1 Formally $P_{ij}(s, s+t) = P(X(s+t) = j \mid X(s) = i)$. When the Markov process is time-homogeneous, then $P_{ij}(s, s+t)$ does not depend on s and is designated as $P_{ij}(t)$.

NOTE 2 For an irreducible Markov process (i.e. if every state can be reached from every other state) it holds that $P_{ij}(\infty)=P_j$, where P_j is the asymptotic and stationary or steady-state probability of state j.

3.11
taux de transition
q_{ij}
la limite, si elle existe, du rapport de la probabilité conditionnelle qu'une transition ait lieu de l'état *i* vers l'état *j* dans un intervalle de temps donné (t, $t+\Delta t$) et la longueur de l'intervalle Δt, quand Δt tend vers zéro, avec le système à l'état *i* à l'instant *t*

NOTE ρ_{ij} ou c_{ij} sont aussi utilisés dans ce contexte.

3.12
état initial
état du système à l'instant $t = 0$

NOTE Généralement, un système entre en exploitation à l'instant $t = 0$ dans un état de disponibilité où tous les éléments du système fonctionnent, puis il évolue vers un état final, qui est un état d'indisponibilité, en passant par d'autres états de disponibilité du système dans lesquels on trouve progressivement de moins en moins d'éléments fonctionnant.

3.13
état absorbant
état qui, dès lors qu'on y entre, ne peut être quitté (par exemple les transitions pour sortir de cet état ne sont pas possibles)

3.14
système apte au rétablissement
système composé d'éléments qui peuvent être défaillants puis être rétablis dans leur état de disponibilité sans nécessairement provoquer une défaillance du système

NOTE Le terme réparable est également utilisé dans ce contexte.

3.15
système non apte au rétablissement
système dont le graphe de Markov contient uniquement des transitions vers des états de défaillance du système

NOTE Le terme non réparable est également utilisé dans ce contexte.

4 Symboles et abréviations

4.1 Symboles utilisés dans les graphes de Markov

Les techniques de Markov sont représentées graphiquement par des graphes ou des diagrammes du taux de transition, les deux termes étant utilisés indifféremment dans cette norme.

Les symboles suivants sont utilisés dans ce document. D'autres symboles peuvent être appliqués suivant le cas.

4.1.1 Symbole d'état

Un état est représenté par un cercle ou un rectangle.

NOTE Pour faciliter la lecture, les états d'indisponibilité peuvent être mis en évidence, par exemple caractères en gras, en couleurs ou hachurés.

4.1.2 Description de l'état

La description de l'état est placée à l'intérieur du symbole d'état et peut se présenter sous la forme de mots ou de caractères alphanumériques définissant les combinaisons d'éléments fonctionnant ou défaillants qui caractérisent l'état.

3.11
transition rate
q_{ij}
limit, if it exists, of the ratio of the conditional probability that a transition takes place from state *i* to state *j* within a given time interval (t, $t+\Delta t$) and the length of the interval Δt, when Δt tends to zero, given that the system is in state *i* at time *t*

NOTE p_{ij} or c_{ij} are also used in this context.

3.12
initial state
system state at time $t = 0$

NOTE Generally, a system starts its operation at $t = 0$ from an up state in which all elements of the system are functioning and transits towards the final system state, which is a down state, via other system up states having progressively fewer functioning elements.

3.13
absorbing state
state which once entered, cannot be left (i. e. no transitions out of the state are possible)

3.14
restorable system
system containing elements which can fail and then be restored to their up state without necessarily causing system failure

NOTE Repairable is also used in this context.

3.15
non-restorable system
system the state transition diagram of which contains only transitions in the direction towards system failure states

NOTE Non-repairable is also used in this context.

4 Symbols and abbreviations

4.1 Symbols for state transition diagrams

Markov techniques are graphically represented by state transition diagrams or by transition rate diagrams, both terms being used as equivalents in this standard.

The following symbols are used throughout this document. Other symbols may be applied as appropriate.

4.1.1 State symbol

A state is represented by a circle or a rectangle.

NOTE In order to increase readability, down states can be highlighted, e. g. by bold lines, colouring or hatching.

4.1.2 State description

The state description is placed inside the state symbol and may take the form of words or alphanumeric characters defining those combinations of failed and functioning elements which characterise the state.

4.1.3 Repère d'état

Un repère d'état est un nombre ou une lettre dans un cercle, adjacent au symbole d'état, ou en l'absence de description d'état, à l'intérieur même du symbole d'état.

NOTE L'état peut souvent être représenté de façon adéquate par un cercle avec la lettre ou le nombre.

4.1.4 Flèche de transition

La flèche de transition indique le sens d'une transition (par exemple en conséquence d'une défaillance ou d'un rétablissement). Les taux de transition sont inscrits près de la flèche de transition.

4.2 Autres symboles et abréviations

Les symboles de mesures de fiabilité, disponibilité, maintenabilité et la sécurité sont ceux de la CEI 60050(191), lorsqu'ils s'y trouvent. Les références ci-dessous ayant un préfixe 191 sont issues de la CEI 60050(191). Dans cette norme, les symboles suivants sont utilisés:

Symbole/Abréviation	Terme	Référence
$R(t)$	fiabilité NOTE 191-12-01 utilise le symbole général $R(t_1,t_2)$	
DFR	taux de défaillance dangereux NOTE Dans un contexte de sécurité, le terme taux de danger (HR) est communément utilisé à la place de DFR.	CEI 61508
MTTF	durée moyenne de fonctionnement avant défaillance	191-12-07
MTTFF	durée moyenne de fonctionnement avant la première défaillance	191-12-06
MTTFH	durée moyenne de fonctionnement avant la première situation de danger	
PFD	probabilité de défaillance sur demande NOTE Le PFD à un temps donné *t* correspond à $\sum_j P_j(t)$ pour tous les états d'indisponibilité j.	CEI 61508
$\lambda(t)$	taux de défaillance (instantané)	191-12-02
$\mu(t)$	taux de rétablissement NOTE 191-13-02 utilise $\mu(t)$ pour le taux de réparation.	
$A(t)$	disponibilité instantanée	191-11-01
$U(t)$	indisponibilité instantanée	191-11-02
A	disponibilité de l'état stationnaire et asymptotique NOTE La disponibilité de l'état stationnaire a la même valeur numérique que la disponibilité asymptotique.	
MUT	durée moyenne de disponibilité	191-11-11
MDT	durée moyenne d'indisponibilité	191-11-12
$P_i(t)$	probabilité de trouver le système dans l'état *i* à l'instant *t*	
P_i	probabilité asymptotique et de l'état stationnaire de trouver le système dans l'état *i* à l'instant *t*	
Δt	petit intervalle de temps	
$P_{ij}(t)$	probabilité de transition de l'état *i* à l'état *j* à l'instant *t*,	
q_{ij}	taux de transition de l'état *i* à l'état *j*, $j \neq i$. NOTE q_i est défini de façon formelle comme $q_i = \sum_{j \neq i} q_{ij}$ C'est le taux initial de l'état *i*.	

4.1.3 State label

A state label is a number or a letter in a circle, placed adjacent to the state symbol, or in the absence of a state description, within the state symbol itself.

NOTE The state can often be adequately represented by a circle with the state number or letter.

4.1.4 Transition arrow

The transition arrow indicates the direction of a transition (e. g. as a result of failure or restoration). Transition rates are written near the transition arrow.

4.2 Other symbols and abbreviations

Symbols for reliability, availability, maintainability and safety measures follow those of IEC 60050(191), where available. The references below with a prefix 191 are from IEC 60050(191). In this standard the following symbols are used:

Symbol/ Abbreviation	Term	Reference
$R(t)$	reliability NOTE 191-12-01 uses the general symbol $R(t_1,t_2)$	
DFR	dangerous failure rate NOTE In a safety context, hazard rate (HR) is commonly used for DFR.	IEC 61508
MTTF	mean time to failure	191-12-07
MTTFF	mean time to first failure	191-12-06
MTTFH	mean time to first hazardous situation	
PFD	probability of failure on demand (unavailability) NOTE The PFD at a given time t corresponds to $\sum_j P_j(t)$ for all down states j.	IEC 61508
$\lambda(t)$	(instantaneous) failure rate	191-12-02
$\mu(t)$	restoration rate NOTE 191-13-02 uses $\mu(t)$ for repair rate	
$A(t)$	instantaneous availability	191-11-01
$U(t)$	instantaneous unavailability	191-11-02
A	asymptotic and steady-state availability NOTE Steady-state availability has the same numerical value as asymptotic availability.	
MUT	mean up time	191-11-11
MDT	mean down time	191-11-12
$P_i(t)$	probability of finding the system in state i at time t	
P_i	asymptotic and steady-state probability of finding the system in state i at time t	
Δt	a small time interval	
$P_{ij}(t)$	transition probability from state i to state j in time t	
q_{ij}	transition rate from state i to state j, $j \neq i$ NOTE q_i is formally defined as $q_i = \sum_{j \neq i} q_{ij}$. It is the departure rate from state i.	

4.3 Exemple

A titre d'exemple, la Figure 1 montre le diagramme des probabilités de transition en ($t,t+\Delta t$), avec t arbitraire et Δt petit, pour un élément non réparable ayant un taux de défaillance constant λ.

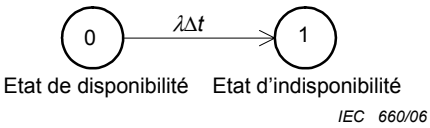


Figure 1 – Diagramme des probabilités de transition dans l'intervalle de (t, $t+\Delta t$), pour une valeur t arbitraire et Δt petit, pour un système à un élément non réparable ayant une défaillance constante λ

$\lambda\Delta t$ est la probabilité conditionnelle d'une transition de l'état 0 à l'état 1 dans un intervalle de temps réduit ($t,t+\Delta t$), avec le système étant à l'état 0 à l'instant t. Pour simplifier la notation, la quantité Δt est souvent omise et le diagramme des probabilités de transition de la Figure 1 devient le diagramme des taux de transition donné dans la Figure 2.

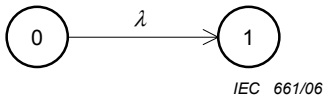


Figure 2 – Graphe de Markov d'un système à un élément non réparable

Dans la Figure 2 et ci-après, le terme de graphe de Markov est utilisé de façon équivalente au terme de diagramme des taux de transition.

5 Description générale

Les techniques de Markov utilisent un graphe qui est une représentation des comportements de la fiabilité, disponibilité, maintenabilité ou sécurité d'un système, à partir duquel les mesures de performance peuvent être calculées. Il modélise le comportement du système dans le temps. Dans cette norme, un système est considéré comme un nombre d'éléments, chacun de ceux-ci ne pouvant prendre qu'un des deux états: disponible ou indisponible. Le système dans sa globalité, toutefois, peut prendre plusieurs états différents, chacun étant déterminé par une combinaison particulière d'éléments fonctionnant et défaillants. Ainsi, lors d'une défaillance ou d'un rétablissement d'un élément, le système passe d'un état à un autre. Ce type de modèle est généralement désigné par les termes état discret, modèle temporel permanent.

Les techniques de Markov sont particulièrement adaptées à l'étude des systèmes incorporant des redondances, ou aux systèmes où la défaillance de système dépend d'événements séquentiels, ou pour des systèmes pour lesquels les stratégies de maintenance sont complexes, par exemple systèmes à rétablissements prioritaires ou temps de rétablissements multiples, problèmes de files d'attente et de ressources restreintes. Il convient que l'analyste s'assure que le modèle reflète de façon adéquate l'exploitation véritable du système en tenant compte des stratégies et politiques de maintenance. L'adaptabilité des distributions exponentielles pour la modélisation des temps de rétablissement doit plus particulièrement être revue. Il convient de noter que quand des systèmes redondants réparables sont modélisés avec des capacités de réparation restreintes, alors du fait de l'absence de mémorisation, le temps réel de réparation peut être surestimé, voir Figure B.9 pour exemple.

4.3 Example

As an example, Figure 1 shows the diagram of transition probabilities in ($t,t+\Delta t$), for t arbitrary and small Δt, for a non-restorable item with constant failure rate λ.

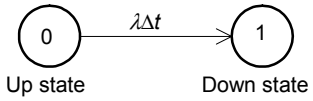


Figure 1 – Diagram of transition probabilities in time interval ($t,t+\Delta t$), for arbitrary value of t and small Δt, for a non-restorable one-element system with constant failure rate λ

$\lambda\Delta t$ is the conditional probability of a transition between state 0 and state 1 in the small time interval ($t,t+\Delta t$) given that the system was in state 0 at time t. To simplify the notation, the quantity Δt is often omitted and the transition probabilities diagram of Figure 1 becomes the transition rates diagram given in Figure 2.

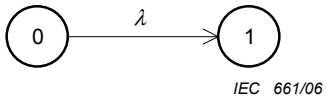


Figure 2 – State transition diagram of a non-restorable one-element system

In Figure 2 and in the following, the term state transition diagram will be used as equivalent to the term transition rates diagram.

5 General description

The Markov techniques make use of a state transition diagram which is a representation of the reliability, availability, maintainability or safety behaviours of a system, from which system performance measures can be calculated. It models the system's behaviour with respect to time. In this standard, a system is regarded as a number of elements, each of which can assume only one of two states: up or down. The system as a whole, however, can assume many different states, each being determined by the particular combination of functioning and failed elements. Thus as an element fails or is restored, the system "moves" from one state to another state. This kind of model is generally called a discrete-state, continuous time model.

Markov techniques are especially suited to the investigation of systems with redundancy, or to systems where system failure depends on sequential events, or to systems for which the maintenance strategies are complex, e.g. systems with restoration priorities or multiple restoration teams, queuing problems, and resource restrictions. The analyst should ensure that the model adequately reflects the operation of the real system with respect to maintenance strategies and policies. In particular the suitability of exponential distributions for the modelling of restoration times must be reviewed. It should be noted that when redundant repairable systems are modelled with limited repair capacity then due to the memory-less property of the model the actual repair time can be overrepresented, see Figure B.9 for an example.

Si les hypothèses et limitations décrites dans l'Article 6 (ci-dessus) sont acceptables, l'un des avantages majeurs des techniques de Markov est que les stratégies de maintenance, par exemple les priorités de rétablissement des éléments individuels, peuvent être modélisées. De plus, l'ordre dans lequel les défaillances multiples apparaissent peut être considéré dans le modèle. Il convient de noter que d'autres techniques d'analyse par exemple l'analyse par arbre de panne (AAP) et la méthode du diagramme de fiabilité (RBD) (telles que décrites dans la CEI 61025 et la CEI 61078 respectivement) ne permettent pas de prendre en compte des stratégies de maintenance complexes, bien qu'elles puissent avoir des barrières particulières représentées par des symboles particuliers (barrières dynamiques) pour indiquer la présence de ces cas. Cependant, l'effet de ces barrières doit être évalué séparément par les techniques de Markov ou autres, et les résultats inclus dans l'analyse de l'Arbre de Panne ou RBD, tout en observant les limitations possibles.

Bien que les techniques de Markov, d'un point de vue théorique, soient souples et polyvalentes, des précautions particulières sont nécessaires pour traiter les difficultés des applications pratiques. Le problème principal réside dans le fait que le nombre des états du système et de transitions possibles augmente rapidement en fonction du nombre d'éléments présents dans le système. Plus le nombre des états et des transitions est élevé, plus la probabilité d'erreurs et de représentations fausses est grande. Pour réduire ce risque, il est conseillé de suivre certaines règles lors de la conception d'un graphe de Markov (voir Article 8). Les techniques numériques utilisées pour le calcul du graphe peuvent également prendre du temps et nécessiter des programmes informatiques spéciaux.

Les techniques de Markov ne sont pas seulement adaptées à la modélisation de stratégies de maintenance mais elles conviennent à la modélisation sous forme de graphiques, ce qui est en soi une caractéristique précieuse. Le mécanisme de défaillance/rétablissement est représenté par des transitions d'un symbole d'état vers un autre symbole du graphe, l'ensemble constituant le graphe de Markov du système.

Le nombre d'états possibles étant limité, la somme de toutes les probabilités d'état est 1, c'est-à-dire que, à chaque instant, le système ne peut se trouver que en un, et un seul, des états du graphe. Si, pour des raisons pratiques, les états à très faible probabilité sont omis, alors la somme de toutes les probabilités d'état est seulement approximativement 1.

Les techniques de modélisation décrites peuvent également s'appliquer à des systèmes où certains ou tous les éléments ne sont pas rétablis. Il convient de noter qu'un système composé d'éléments non aptes au rétablissement peut être considéré comme un cas particulier d'un système composé d'éléments aptes au rétablissement, les taux de rétablissement étant égaux à zéro (ou bien les temps de rétablissement sont infinis).

6 Hypothèses et limitations

Les règles d'élaboration d'un graphe de Markov données en 8.2 s'appliquent en général (sauf pour la règle h). Cependant, la description de techniques numériques s'applique uniquement lorsque tous les taux de transition sont constants, ce qui implique que les taux de défaillance et de rétablissement de tous les éléments dans le système analysé soient constants dans le temps. L'hypothèse du taux de défaillance constant est raisonnablement acceptable pour les composants de nombreux systèmes avant la période d'usure (cependant il convient de les justifier), mais l'hypothèse d'un taux de rétablissement constant sauf si la durée moyenne de rétablissement des éléments est très faible en comparaison des durées moyennes de fonctionnement avant défaillance correspondantes. Le calcul du cas général où les taux de défaillance ou de rétablissement ne sont pas constants dans le temps, sort du domaine d'application de cette norme.

Une limitation particulière provient de l'hypothèse utilisée pour trouver les solutions mathématiques, à savoir le fait que le comportement futur du système dépend seulement de son état présent, et non de la façon dont le système est arrivé dans cet état. Il convient que l'analyste s'assure que cette propriété d'absence de mémorisation des modèles de Markov

Provided the assumptions and limitations described in Clause 6 can be accepted, one of the major advantages of Markov techniques is that maintenance strategies, for example restoration priorities of individual elements, can be modelled. Moreover, the order in which multiple failures occur can be considered in the model. It should be noted that other analysis techniques e.g. fault tree analysis (FTA) and reliability block diagram (RBD) methods (as described in IEC 61025 and IEC 61078 respectively) do not allow complex maintenance strategies to be taken into account, though they may have special gates represented by special symbols (dynamic gates) to indicate the presence of those cases. However, the effect of those gates has to be evaluated separately by Markov techniques or other techniques, and the results included in the analysis of the Fault Tree or RBD, whilst observing the possible limitations.

Although Markov techniques, from a theoretical viewpoint, are flexible and versatile, special precautions are necessary to deal with the difficulties of practical applications. The main problem is that the number of system states and possible transitions increases rapidly with the number of elements in the system. The larger the number of states and transitions, the more likely is it that there will be errors and misrepresentations. To reduce this risk, it is advisable that certain rules be followed in designing the state transition diagram (see clause 8). Also the numerical techniques used for the evaluation of the diagram can be time consuming and may require special computer programs.

Not only are Markov techniques suited to the modelling of maintenance strategies, but such methods enable the failure/restoration events to be modelled in a pictorial way, which is in itself a valuable feature. The process of failure/restoration is represented by transitions from one state symbol to another in the array of state symbols which together constitute the system state transition diagram.

As the number of possible states is finite, the sum of all the state probabilities is unity, i.e. at any instant in time the system can be in one – and only one – of the states in the state transition diagram. If, for practical reasons, states with very low probability are omitted, then the sum of all state probabilities is only approximately one.

The modelling techniques described can also be applied to systems where some or all of the elements are not restored. Note that a system with non-restorable elements can be regarded as a special case of a system with restorable elements where the restoration rates are zero (or restoration times are infinite).

6 Assumptions and limitations

The rules given in 8.2 of this standard, for generating the state transition diagram, apply generally (apart from rule h). However, the description of numerical techniques applies only when all transition rates are constant, which implies that failure and restoration rates of all elements in the analyzed system are constant with respect to time. The assumption of constant failure rate is reasonably acceptable for components in many systems before the wear-out period (however should also be justified) but the assumption of constant restoration rate should be justified unless the mean time to restoration of elements is very small by comparison with the corresponding mean times to failure. Evaluation for the general case where failure rates or restoration rates are not constant with time, is outside the scope of this standard.

One particular limitation arises because of the assumption used for mathematical solutions, namely, the future behaviour of the system depends only on the present state of the system, and not on the way the system arrived at this state. The analyst should ensure that this memory-less property of Markov models is a sufficient approximation of the real system

est une approximation suffisante pour le comportement du système réel (voir 8.1). Une attention particulière est nécessaire lors de la modélisation des effets des défaillances de cause commune qui peuvent avoir comme résultat l'omission d'états intermédiaires (voir Figure B.4).

Les hypothèses habituelles pour chaque élément dans le système considéré peuvent être résumées comme suit:

– le taux de défaillance, λ, et le taux de rétablissement, μ, sont constants (indépendants du temps),

– la probabilité de transition d'un état i à un état j dans un intervalle de temps court $(t,t+\Delta t)$ avec le système dans un état i à l'instant t est $q_{ij}\,\Delta t$, où q_{ij} est une somme des taux de défaillance et de rétablissement des éléments impliqués.

NOTE Théoriquement la limitation au regard des taux de rétablissement et de défaillance constants peut souvent être surmontée aux dépens de l'espace de l'état, une approximation des nombreuses distributions non-exponentielles de temps de défaillance ou de rétablissement pouvant être réalisée par une somme des distributions exponentielles. Chacune de ces distributions exponentielles doit passer par un état supplémentaire de modèle, qui agit comme une sorte de mémoire pour le temps écoulé avant défaillance ou le temps de rétablissement. Cependant ce concept, habituellement appelé phase (ou états supplémentaires), n'a pas été mis largement en pratique.

7 Relation avec d'autres techniques d'analyse

7.1 Généralités

Les techniques de Markov peuvent être utilisées pour modéliser des événements ou des états dans d'autres techniques de modélisation, en particulier lorsque ces autres techniques ne possèdent pas certaines des capacités des techniques de Markov, par exemple la capacité à exprimer un comportement dépendant de l'état ou du temps. Les modèles obtenus sont souvent appelés modèles hybrides.

Une discussion détaillée des techniques de modélisation est donnée dans la CEI 60300-3-1. Une discussion complète sur les modèles hybrides est laissée aux normes qui utilisent les graphes d'état de Markov dans cet objectif, par exemple la CEI 61078 ou la CEI 61025. L'objet de cet article est de donner des considérations d'ordre général pour les modèles hybrides.

7.2 Analyse par Arbre de Panne (AAP)

L'AAP peut être utilisée pour évaluer la probabilité de défaillance à un instant donné t dans le temps en utilisant la logique booléenne. Cette logique peut ne pas exprimer correctement les dépendances d'état ou de temps. Dans ces cas il est possible d'étendre l'AAP en créant de nouvelles barrières qui représentent des modèles de Markov particuliers qui sont évalués séparément et qui cachent le modèle de Markov réel à l'utilisateur. De telles barrières portent le nom de portes «dynamiques», par exemple PRIORITÉ ET, INTERDICTION SÉQUENTIELLE ou porte «DE RECHANGE». On peut remplacer ensuite ces barrières par un événement de base, avec la probabilité d'occurrence calculée par la technique de Markov. Le modèle obtenu est souvent appelé AAP hybride ou dynamique.

Les barrières dynamiques et les barrières statiques d'un arbre de panne peuvent être modélisées par les techniques de Markov. Cependant, une attention particulière doit être accordée aux propriétés d'indépendance entre les événements dans le modèle de Markov et les événements dans l'arbre de panne. Dans l'arbre de panne les parties évaluées par les techniques de Markov doivent être considérées comme des branches indépendantes.

behaviour (see 8.1). Special care is needed when modelling effects of common cause failures that may result in some potential intermediate states being by-passed (see Figure B.4).

The usual assumptions for each element in the system considered can be summarised as follows:

– the failure rate, λ, and the restoration rate, μ, are constant (time-independent);

– the transition probability from a state i to a state j within the small time interval $(t,t+\Delta t)$ given that the system is in state i at time t is $q_{ij}\ \Delta t$, where q_{ij} is a sum of failure and restoration rates of involved elements.

NOTE Theoretically the limitation with respect to the constant failure and restoration rates can often be overcome at the expense of expansion of the state space, as many non-exponential distribution of times to failure or to restore can be approximated by a sum of exponential distributions. Each of these exponential distributions has to be modelled as an additional state, which acts as a kind of memory for the elapsed time to failure or time to restore. However, this concept, usually called phase (or supplementary states) concept, has not been widely put into practice.

7 Relationship with other analysis techniques

7.1 General

Markov techniques can be used to model events or states in other modelling techniques, in particular, when these other techniques lack certain capabilities which Markov techniques have, e. g. the ability to express time or state dependent behaviour. The resulting models are often called hybrid models.

A comprehensive discussion of modelling techniques is given in IEC 60300-3-1. A full discussion on hybrid models is left to the standards which utilize Markov state transition diagrams for this purpose, e.g. IEC 61078 or IEC 61025. The purpose of this clause is to give some general considerations for hybrid models.

7.2 Fault Tree Analysis (FTA)

FTA can be used to evaluate the probability of a failure at a given instant t in time using Boolean logic. This logic may not express time or state dependencies properly. In these cases it is possible to extend FTA by creating new gates, which represent particular Markov models, which are separately evaluated and hide the actual Markov model from the user. Such gates bear the name of “Dynamic” gates, for example PRIORITY AND, SEQUENTIAL INHIBIT or SPARE gate. Each of such gates may be replaced by a basic event with the probability of occurrence as calculated from the Markov technique. The resulting model is often called hybrid or dynamic FTA.

Both static and dynamic gates of a fault tree can be modelled by Markov techniques. However, particular attention shall be paid to independence properties between the events in the Markov model and the events in the fault tree. In the fault tree, the parts evaluated by Markov techniques have to be assumed to be independent branches.

7.3 Diagramme de fiabilité (RBD)

Un RBD peut également être une technique qui utilise la logique booléenne et présente donc les mêmes limitations que l'AAP.

Dans le RBD il est possible de délimiter les parties du RBD (en encerclant les blocs), pour lesquelles on utilise le modèle Markov. Les blocs encerclés doivent former un réseau avec une seule entrée et une seule sortie, et ne doivent pas inclure de blocs répliqués par ailleurs. De plus amples informations sont données dans la CEI 61078.

7.4 Réseaux de Petri

Les réseaux de Petri sont une technique graphique pour la représentation et l'analyse d'interactions logiques complexes parmi les éléments d'un système.

Une classe particulière de réseaux de Petri, les «General Stochastic Petri Nets» (GSPN) a une capacité de modélisation similaire aux techniques de Markov. Les réseaux de Petri peuvent être considérés comme une expression implicite naturelle de la représentation explicite du modèle Markov. On peut convertir les réseaux de Petri en modèles Markov. Les modèles de «General Stochastic Petri Net» contenant des interactions complexes peuvent souvent être décrits plus facilement et par un schéma plus petit qu'avec les techniques de Markov. Pour les besoins de l'évaluation, le réseau de Petri est converti en son modèle Markov correspondant, qui est ensuite analysé. Dans la pratique ceci est automatisé par les outils informatiques.

8 Elaboration des graphes de Markov

8.1 Prérequis

Il convient que les tâches générales suivantes soient accomplies avant de commencer l'analyse d'un système:

a) déterminer le but de l'analyse: la première question cruciale à laquelle il s'agit de répondre est quel doit être l'objet de l'analyse. Cela peut être un ou plusieurs des points suivants:
   - la probabilité que le système tombe en panne avant l'instant *t*;
   - la fréquence d'événements dangereux;
   - la durée moyenne de fonctionnement avant la première défaillance du système;
   - la disponibilité de l'état stationnaire;
   - la probabilité de défaillance du système au moment d'une demande de fonctionnement (pour les systèmes partiellement en exploitation);
   - autre mesure, à spécifier.

   L'unité de mesure doit également être définie précisément.

b) Définir les caractéristiques du système et les conditions limites de l'analyse.

   Les questions suivantes doivent avoir une réponse:
   - quels sont les dispositifs importants du système qui doivent être modélisés ?
   - de quelle façon ces dispositifs peuvent-ils être évalués ou au moins vérifiés pour leur vraisemblance ?
   - le système sera-t-il ou non rétabli ?
   - est-il nécessaire de décrire le comportement dépendant du temps ?
   - quelle est l'incertitude exacte des données, par exemple taux de défaillance et de rétablissement ou facteurs de cause commune ?
   - quel est le niveau de précision requis du résultat ?

7.3 Reliability Block Diagram (RBD)

A RBD is also a technique that may use Boolean logic and therefore has similar limitations to those of FTA.

In the RBD, it is possible to delineate the portions of the RBD (by encircling the blocks), for which the Markov model is to be used. The encircled blocks have to form a network with a single input and a single output, and must not include blocks replicated elsewhere. Further guidance is given by IEC 61078.

7.4 Petri nets

Petri nets are a graphical technique for the representation and analysis of complex logical interactions among elements in a system.

A particular class of Petri nets, the General Stochastic Petri Nets (GSPN) have an equivalent modelling capability to Markov techniques. Petri nets may be regarded as a natural implicit expression of its explicit Markov model representation. Petri nets can be converted to Markov models. So General Stochastic Petri Net models containing complex interactions can often be described more easily and with a smaller diagram than using Markov techniques. For evaluation purposes, the Petri net is converted to its corresponding Markov model, which is then analyzed. In practice, this is automated by software tools.

8 Development of state transition diagrams

8.1 Prerequisites

Before starting to analyze a system, the following general tasks should be performed:

a) Set the goal of the analysis: The first crucial question which has to be answered is what should be the objective of the analysis. This could be any one or more of the following:
   - the probability that the system will fail before time *t*;
   - the frequency of hazardous events;
   - the mean time before the first system failure occurs;
   - the steady-state availability;
   - the probability that the system will fail when a request for its operation is issued (for systems not in continuous use);
   - other measure, to be specified.

   The unit of measurement also needs to be defined.

b) Define the characteristics of the system and the boundary conditions of the analysis.

   Here questions such as the following need to be answered:
   - what are the important features of the system which need to be modelled?
   - how can these features be validated or at least be checked for plausibility?
   - will the system be restored (after a failure) or not?
   - is it necessary to describe time-dependent behaviour?
   - what is the actual uncertainty of the data, e.g. failure and restoration rates, or common-cause factors?
   - what is the required accuracy and/or confidence level of the results?

Il convient de donner une explication détaillée de la raison pour laquelle certains dispositifs du système dans la réalité ne sont pas importants pour le modèle.

c) s'assurer que la technique de Markov est la technique d'analyse la mieux adaptée pour la tâche. Il convient de choisir la technique en fonction des objectifs de l'analyse et des caractéristiques du système et non pas le contraire, sinon certaines caractéristiques du système ne seront pas modélisées du tout. En particulier les hypothèses et limitations du modèle doivent être soigneusement vérifiées.

d) il convient de faire revoir le modèle et les données d'entrée par des experts du domaine d'application (ou utilisateurs expérimentés), car une erreur ou une imprécision dans le modèle ou les données a un fort impact sur le résultat de l'analyse.

La conception correcte du graphe est une tâche critique de l'analyse de Markov. Le paragraphe 8.2 donne quelques-unes des règles recommandées. Il convient d'établir les règles avant d'entreprendre l'analyse et d'identifier précisément chaque état. Ceci permettra la construction de modèles graphiques clairs.

8.2 Règles d'élaboration et de représentation

Les règles ci-dessous constituent un guide pour l'élaboration systématique des graphes de Markov. Les graphes de Markov respectant ces règles seront faciles à comprendre et comparer. D'autres symboles ou une autre présentation du graphe peuvent être mieux adaptés dans certains cas.

a) il convient d'indiquer par un cercle ou un rectangle l'état avec l'identification qui permet de rapporter uniquement la procédure numérique à cet état. L'identifiant est généralement une lettre ou un nombre;

b) lorsque cela est nécessaire pour la clarté du graphe de Markov, il convient que le symbole comporte une description détaillée de l'état, soit directement, soit en renvoyant à une liste explicative;

c) il est recommandé que les états soient disposés de telle sorte que l'état situé le plus à gauche corresponde à l'état de disponibilité et l'état le plus à droite corresponde à l'état d'indisponibilité du système. Il convient que les positions relatives des états intermédiaires soient telles qu'une transition de la gauche vers la droite soit le résultat d'une défaillance, et une transition de la droite vers la gauche soit la conséquence d'un rétablissement;

d) il convient d'aligner verticalement les états du système correspondant au même nombre d'éléments indisponibles;

e) il convient que les transitions entre états soient repérées par des lignes fléchées reliant les états particuliers. Une ligne dont la flèche est orientée vers la droite représente une défaillance alors qu'une ligne dont la flèche est dirigée vers la gauche représente un rétablissement. Si une transition entre deux états peut résulter soit d'une défaillance, soit d'un rétablissement, il convient que ces états particuliers soient alors reliés par une seule ligne comportant des flèches aux deux extrémités. Dans le cas d'un graphe de Markov simple, il est possible d'utiliser des lignes de transition distinctes pour indiquer les défaillances et les rétablissements;

f) il convient d'étiqueter les flèches sur les lignes représentant les transitions avec les taux de transition correspondants. Cela peut être fait en indiquant les taux soit directement, soit en référence à une liste explicative;

g) lorsque cela est possible, il convient que chaque transition relie uniquement les symboles d'états voisins. Si une défaillance de cause commune peut rendre invalides simultanément deux éléments ou plus, un état doit être oublié;

h) pour améliorer la lecture, les états d'indisponibilité au niveau du système peuvent être mis en évidence (par exemple caractères gras, en couleurs ou hachurés).

L'application de ces règles est illustrée en Annexe B.

If some features of the real world system are not important for the model this should be justified.

c) make sure that the Markov technique is the most appropriate analysis technique for the task. The choice of technique should be based on the objectives of the analysis and the characteristics of the system, not vice versa; otherwise certain characteristics of the system may not be modelled at all. In particular the assumptions and limitations of the model need to be carefully checked.

d) the model and the input data should be reviewed by experts (practitioners with field experience), because errors or inaccuracies in the model or the data could have a high impact on the result of the analysis.

A critical task in Markov analysis is the proper design of the state transition diagram. Subclause 8.2 gives some recommended rules. The rules should be established before the analysis is undertaken and hence should provide for a proper identification of the individual states. This will enable construction of clear graphical models**.**

8.2 Rules for development and representation

The rules below are given as a guide for the systematic development of state transition diagrams. State transition diagrams following these rules will allow easy comprehension and comparison. Other symbols or diagram arrangements may be more suitable in some instances.

a) the state should be depicted by a circle or rectangle with identification which allows the numerical procedure to refer uniquely to that state. The identifier is usually a letter or a number.

b) when necessary for clarity of the state transition diagram, the state symbol should include a clear description of the state, either directly or by reference to an explanatory list.

c) states should be arranged so that the leftmost state is an up state and the rightmost state is a down state of the system. The relative positions of intermediate states should be such that a transition from left to right is a result of a failure, and a transition from right to left is achieved by restoration.

d) system states corresponding to the same number of down elements should be aligned vertically.

e) transitions between states should be marked by lines with arrows interconnecting the particular states. A line with an arrow on the right represents a failure and a line with an arrow on the left represents a restoration. If a transition between two states can be achieved by either a failure or a restoration, then the particular states should be interconnected by a single line with arrows on both ends. On a simple state transition diagram, separate transition lines may be used to indicate failure and restoration.

f) the arrows on the lines representing transitions should be labelled with the corresponding transition rates. This may be done by indicating the rates either directly or by reference to an explanatory list.

g) where possible, each transition should link only neighbouring state symbols. If a common cause failure disables simultaneously two or more elements, a state needs to be by-passed.

h) to increase readability, down states at system level can be highlighted (e.g. by bold lines, colouring or hatching).

The application of these rules is illustrated in Annex B.

9 Evaluation

9.1 Généralités

Le but de l'évaluation du diagramme de transition est de déterminer la fiabilité, la disponibilité, la maintenabilité ou les mesures de sécurité du système concerné. L'évaluation utilise des techniques mathématiques bien connues (voir Annexes A à C). Il est à noter que la tâche qui consiste à obtenir des mesures transitoires (dépendant du temps), par exemple $R(t)$ et $A(t)$, nécessite des efforts d'informatisation beaucoup plus importants que l'obtention d'une mesure stationnaire A ou de valeurs moyennes, par exemple MTTF, MDT, MUT. Un exemple de calcul des mesures transitoires est donné en Annexe C.

Au début de l'analyse, il convient de décider si l'objectif principal du calcul du graphe de Markov est l'obtention de valeurs d'état stationnaire ou transitoire des probabilités d'état. Même si, pour les études de disponibilité, la dernière peut être obtenue à partir de la précédente (en laissant t tendre vers l'infini), une procédure mathématique relativement simple peut être utilisée si on sait dès le début que seulement la solution d'état stationnaire est nécessaire (voir Annexe A). En revanche, si une solution transitoire est exigée, alors une procédure beaucoup plus spécialisée impliquant, par exemple, les transformées de Laplace ou l'algèbre matricielle (voir Annexe C) peut être nécessaire. En général, on obtiendra des probabilités d'état des mesures d'ordre général, de fiabilité, de disponibilité, de maintenabilité ou de sécurité.

La distinction entre les mesures de fiabilité, de disponibilité, de maintenabilité et de sécurité tient surtout dans les points ciblés par les analyses et les interprétations des résultats. Pour expliquer ceci, on pourra considérer un élément de rétablissement dont les performances sont généralement définies par un taux de défaillance λ et un taux de rétablissement μ. Généralement après l'apparition d'une défaillance dans une entité, au moins deux choses doivent avoir lieu pour le retour à l'état de marche:

– la panne doit être détectée et isolée (parfois dit annulée: ce qui signifie qu'il convient d'entrer un état où une défaillance n'a pas de conséquence ultérieure);

– l'entité doit être rétablie et remise en service.

Le temps de rétablissement dans ce contexte comprend le temps logistique de rétablissement après la détection de la panne, le temps de rétablissement réel (détection de panne, rétablissement, échange, vérification) et le temps pour remettre les éléments ou le système lui-même en fonctionnement.

Dans le modèle de base commun les quatre intervalles de temps intéressants doivent être attribués à deux paramètres seulement (un taux de défaillance λ et un taux de rétablissement μ).

Dans le contexte de fiabilité, de maintenabilité ou de disponibilité, le temps de détection est pris en compte par le calcul du taux de défaillance et le temps entre la détection et le rétablissement par le calcul du taux de rétablissement. Les applications critiques de sécurité peuvent ne pas dépendre d'auto-tests ou de mesures similaires (qui sont courantes dans le contexte de disponibilité), mais la détection et l'isolation doivent être réalisées indépendamment de l'entité (voir CEI 61508 pour des exigences particulières et des exemples). La distinction entre la fiabilité, la maintenabilité et la disponibilité tient en définitive dans les mises au point sur les différentes mesures des objectifs, MTTF, MDT ou A(t).

Dans un contexte de sécurité, le temps de rétablissement exact est généralement négligé, si d'autres mesures de contrôle sont prises pendant cette période. Dans ce cas le calcul du taux de rétablissement des analyses de fiabilité compte pour le temps total d'isolation. Cependant, l'interprétation peut être différente suivant les applications, la Figure 3 montre uniquement un exemple d'interprétation.

9 Evaluation

9.1 General

The purpose in evaluating the state transition diagram is to determine the reliability, availability, maintainability or safety measures of the system. The evaluation uses well-known mathematical techniques (see annexes A to C). Note that the task of obtaining transient (time dependent) measures, e.g. $R(t)$ and $A(t)$, requires considerably more computational effort than that of obtaining a steady-state measure A or mean values, e.g. MTTF, MDT, MUT. An example for the calculation of transient measures is given in Annex C.

At the start of the analysis, one should decide whether the main objective in the state transition diagram evaluation is to obtain transient or steady state values of the state probabilities. Although for availability investigations the latter can be obtained from the former (by letting t tend to infinity), a relatively simple mathematical procedure can be used if, at the outset, it is known that only the steady-state solution is required (see Annex A). If on the other hand a transient solution is required, then a much more specialised procedure involving, for example, Laplace transforms or matrix algebra (see Annex C) may be needed. In general, reliability, availability, maintainability or safety measures can be derived from state probabilities.

The distinction between reliability, availability, maintainability and safety measures lies mainly in the focus of the analyzes and the interpretation of results. To explain this, a restorable element can be considered, whose performance is usually defined by a failure rate λ and a restoration rate μ. Usually, after a failure within an item has appeared, at least two things have to occur in order to get the item working again:

– the fault has to be detected and isolated (sometimes also called negated: this means that a state, where a failure has no further consequence, should be entered);
– the item has to be restored and put back into service.

The restoration time in this context includes the logistic time for restoration after fault detection, actual restoration time (fault finding, restoration, replacement, check) and time to put the elements or the system itself into operation.

In the common basic model, the four time intervals of interest need to be assigned to two parameters (a failure rate λ and a restoration rate μ) only.

In the context of reliability, maintainability or availability, the time to detection is taken into account by the failure rate calculation and the time from detection to restoration by the restoration rate calculation. Safety-critical applications may not rely on self-tests or similar measures (which are common in the availability context), but the detection and isolation has to be performed independently of the item (see IEC 61508 for particular requirements and examples). The distinction between reliability, maintainability and availability finally lies in the focus on different target measures, MTTF, MDT or A(t).

In a safety context, generally the actual restoration time is neglected, if other control measures are taken during this period. In this case, the restoration rate calculation from reliability analysis accounts for the complete time to isolation. However, the interpretation may differ also in several applications, Figure 3 shows an example interpretation only.

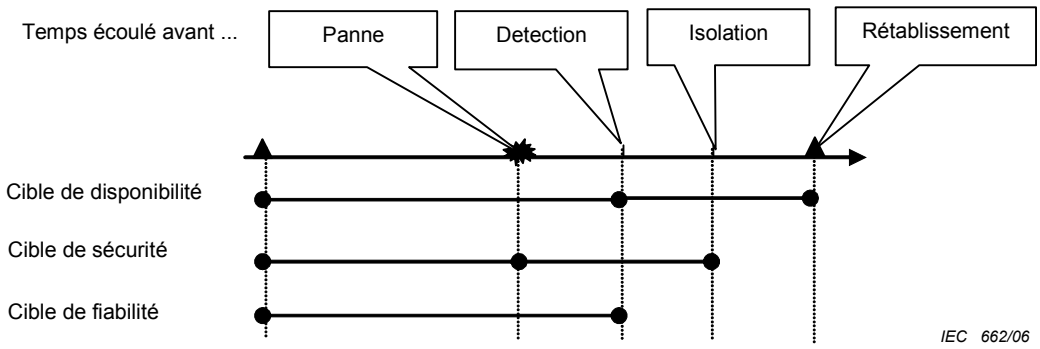


Figure 3 – Interprétation des temps de défaillance et de rétablissement dans différents contextes

Cependant, la principale observation est que, alors que le modèle et les formules mathématiques utilisés sont les mêmes, c'est l'interprétation des paramètres et des résultats qui fera la différence.

9.2 Evaluation des mesures de fiabilité

Pour les analyses de fiabilité, tous les états d'indisponibilité au niveau du système dans le graphe de Markov sont à l'état absorbant. La probabilité que le système soit dans un état donné à l'instant t est calculée en utilisant des techniques mathématiques spéciales (voir Annexes A à C). Alors que t tend vers l'infini, la probabilité associée à chaque état approche zéro, et la somme des probabilités des états absorbants approche un.

Une des mesures de fiabilité commune est le MTTFF. Lors de l'évaluation du graphe de Markov, le MTTFF pour le système complet est la moyenne du total des temps passés par le système en état de disponibilité avant transition dans un état absorbant. Le temps moyen dépend de l'état du système à t=0; $MTTF_{Si}$ est utilisé pour spécifier cette dépendance (voir Annexe A).

9.3 Evaluation des mesures de disponibilité et de maintenabilité

Pour les analyses de disponibilité, il faut vérifier que tous les états peuvent être atteints à partir de chaque autre, dans le diagramme de transition. La probabilité que le système soit dans un état donné à un instant t est déterminée par les techniques données en Annexe A à C. La disponibilité $A(t)$ est égale à la somme des probabilités d'état associée aux états de disponibilité. Alors que t tend vers l'infini, la probabilité associée à chaque état approche une valeur constante. La disponibilité du système approche également une valeur constante, A.

D'autres mesures utiles peuvent également être évaluées (voir Annexe A):

– intensité de défaillance au niveau du système,
– temps moyen écoulé dans un état donné *i,*
– fréquence d'entrée dans un état donné *i,*
– probabilité de sortie de l'état donné *i.*

Il est également possible d'obtenir des probabilités d'état le MUT (temps moyen de disponibilité) et le MDT (temps moyen d'indisponibilité) du système. MUT est le temps moyen passé dans les états de disponibilité et MDT le temps moyen passé dans les états d'indisponibilité.

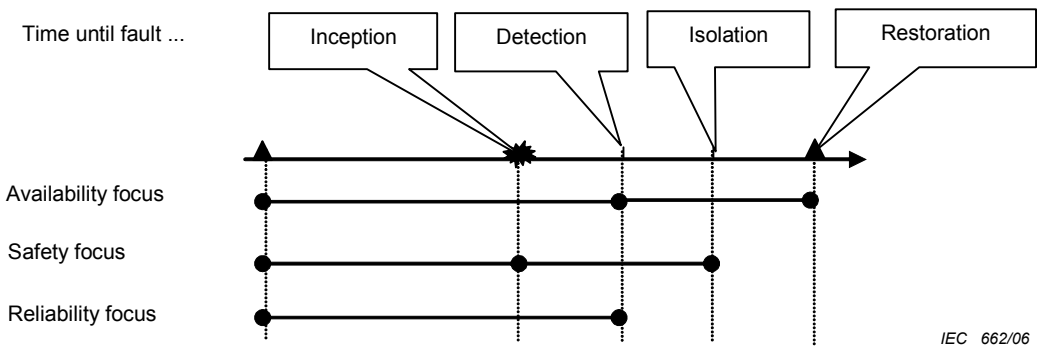


Figure 3 – Interpretation of failure and restoration times in different contexts

However, the major observation is that while the model and the mathematics used may be the same, it is the interpretation of the parameters and of the results that make a major difference.

9.2 Evaluation of reliability measures

For reliability analyzes, all down states at system level in the state transition diagram are made absorbing. The probability that the system is in a given state at time t is calculated using special mathematical techniques (see Annexes A to C). As t tends to infinity, the probability associated with each functioning state approaches zero, and the sum of the probabilities of absorbing states approaches unity.

One of the common reliability measures is MTTFF. When evaluating the state transition diagram, the MTTFF for the whole system is the mean of the total of the times spent by the system in up states before making a transition to an absorbing state. This mean time depends on the state of the system at t=0; $MTTF_{Si}$ is used to specify this dependence (see Annex A).

9.3 Evaluation of availability and maintainability measures

For availability analysis, it must be verified that in the state transition diagram every state can be reached from every other state. The probability that the system is in a given state at time t is determined by the techniques given in Annexes A to C. The availability $A(t)$ is equal to the sum of the state probabilities associated with the up states. As t tends to infinity, the probability associated with each state approaches a constant value. The availability of the system also approaches a constant value, A.

Other useful measures such as the following can also be evaluated (see Annex A):

– failure intensity at system level;
– mean time spent in a given state *i;*
– frequency of entering a given state *i;*
– frequency of leaving a given state *i.*

It is also possible to obtain from the state probabilities the MUT (mean up time) and MDT (mean down time) of the system. MUT is the mean time spent in the up states and MDT the mean time spent in the down states.

9.4 Evaluation des mesures de sécurité

L'évaluation des mesures de sécurité est en principe similaire à l'évaluation de la fiabilité ou aux mesures de disponibilité. Cependant, la terminologie est différente. Dans les applications de sécurité, les états d'indisponibilité sont sous-divisés en états d'indisponibilité certains (où le système n'est pas disponible ni potentiellement dangereux) et en états d'indisponibilité dangereux (où le système est potentiellement dangereux).

Le but est, par exemple, d'évaluer:

– le temps moyen avant l'apparition de la première défaillance dangereuse (MTTFH),
– le taux de défaillance dangereuse (DFR),
– la probabilité de défaillance sur demande (PFD).

Les calculs de MTTFH et DFR sont similaires à ceux de la MTTFF et du taux de défaillance, respectivement. Ils sont évalués comme la mesure de fiabilité correspondante mais seulement au regard des états d'indisponibilité dangereux. Le PFD à l'instant t est la probabilité que le système soit dans un état de danger à l'instant t et est évalué comme l'indisponibilité à l'instant t. Quelquefois le PFD moyen jusqu'à l'instant t est exigé, ce qui peut être obtenu par l'intégration suivante $PFD_{avg} = \frac{1}{t}\int_0^t PFD(s)ds$.

10 Documentation des résultats

Il convient que le rapport des résultats de l'analyse incorpore les éléments suivants:

a) spécification des mesures souhaitées (par exemple fiabilité, disponibilité, maintenabilité, sécurité),
b) les principales hypothèses utilisées, y compris leur justification (par exemple, taux de défaillance constant et taux de rétablissement),
c) justification de l'utilisation des techniques de Markov,
d) description du graphe de Markov comprenant un examen en profondeur des aspects suivants:
   – identification des états de disponibilité et des états d'indisponibilité,
   – lorsque cela est applicable, les raisons pour lesquelles certains états sont groupés et d'autres dont omis,
   – les transitions entre états,
   – le choix des valeurs numériques pour les taux de transition,
   – hypothèses sous-jacentes associées à la construction du diagramme,
e) description :
   – des méthodes de calcul,
   – des programmes informatiques, si utilisés,
f) résultats numériques :
   – résultats sous forme numérique et graphique,
   – influence des hypothèses utilisées dans la construction du graphe de Markov ou pour les calculs,
   – analyse de sensibilité.

   Voir aussi la CEI 60300-3-1.

9.4 Evaluation of safety measures

The evaluation of safety measures is basically similar to the evaluation of reliability or availability measures. The terminology is, however, different. In safety applications, the down states are further subdivided in safe down states (where the system is not up and not potentially hazardous) and dangerous down (or hazardous) states (where the system is potentially hazardous).

The purpose is, for example, to assess:

– the mean time to the first occurrence of a hazardous failure (MTTFH);
– the dangerous failure rate (DFR);
– the probability of failure on demand (PFD).

The MTTFH and DFR calculations are similar to those of the MTTFF and the failure rate calculations, respectively. They are evaluated like the corresponding reliability measure but only with respect to dangerous down states. The PFD at time t is the probability that the system is in a hazardous state at time t and is evaluated like the unavailability at time t. Sometimes the average PFD up to time t is required, which can be obtained by integration as

$$PFD_{avg} = \frac{1}{t}\int_0^t PFD(s)ds \ .$$

10 Documentation of results

The reporting of the results of the analysis should incorporate the following elements:

a) specification of the desired measures (e.g. reliability, availability, maintainability, safety);
b) the main assumptions used, including justification (for instance, constant failure and restoration rates);
c) justification, why Markov techniques are appropriate;
d) description of the state transition diagram including in-depth examination of the following aspects:
   – identification of the up states and down states;
   – where applicable, the reasons why some states are grouped and others are omitted;
   – transitions between states;
   – the choice of numerical values for the transition rates;
   – underlying assumptions associated with the construction of the diagram;
e) description of the
   – computation methods;
   – computer programs, if used;
f) numerical results
   – results in numerical and graphical form;
   – influence of the assumptions used in constructing the state transition diagram or in calculations;
   – sensitivity analysis.

Also see IEC 60300-3-1.

Annexe A
(informative)

Relations mathématiques de base pour les techniques de Markov

A.1 Généralités

Cette annexe traite des modèles basés sur les procédés de Markov homogènes dans le temps avec, de façon limitée, plusieurs états et un temps continu. A cause des propriétés sans mémorisation qui caractérisent de tels procédés, la durée de séjour dans chaque état donné suit une distribution exponentielle. Pour les modèles de fiabilité, ceci implique que les taux de défaillance et de rétablissement (λ et μ) de tous les éléments dans un système sont constants (indépendants du temps). Les taux de défaillance et de rétablissement peuvent changer uniquement dans un état de changement.

A.2 Matrice des taux de transition

A.2.1 Graphe de Markov

Un procédé de Markov homogène dans le temps est complètement caractérisé par la matrice des taux de transition $Q = \lfloor q_{ij} \rfloor$ et les conditions initiales à l'instant t = 0. Le graphe de Markov est une visualisation utile de la matrice des taux de transition. Pour la mise en place de ce graphe, un diagramme de fiabilité (s'il existe) et une FMEA peuvent être très utiles. Dans tous les cas, pour limiter le nombre d'états il est recommandé de rassembler tout groupe de n séries d'éléments (n=2,3, …) en un élément avec un taux de défaillance $\lambda_1 + \ldots + \lambda_n$ et un taux de rétablissement $(\lambda_1 + \ldots \lambda_n)/(\lambda_1/\mu_1 + \ldots + \lambda_n/\mu_n)$, en supposant $\lambda_i << \mu_i, i = 1,\ldots,n$.

Une fois le graphe de Markov dessiné et vérifié (en faisant attention aux modes de défaillances retenus, aux priorités de rétablissement prévues, et aux particularités spécifiques au système considéré), l'espace d'état est divisé en deux ensembles complémentaires D pour les états de disponibilité et I pour les états d'indisponibilité, où m est le nombre total d'états. L'ensemble des états d'indisponibilité peut varier en fonction de l'aspect du système évalué (fiabilité ou sécurité).

A.2.2 Relations de base utiles dans l'étude des modèles de fiabilité de Markov

A.2.2.1 Pour l'évaluation de la fiabilité, le temps moyen avant défaillance du système $MTTF_{S_i}$, en commençant avec le système dans un état i *à* t = 0, est obtenu en résolvant

$$MTTF_{S_i} = \frac{1}{q_i} + \sum_{\substack{j \in UP \\ j \neq i}} \frac{q_{ij}}{q_i} MTTF_{S_j}, \qquad i \in UP, \quad q_i = \sum_{\substack{j=0 \\ j \neq i}}^{m} q_{ij}$$

NOTE 1 Le système ci-dessus d' équations algébriques peut aussi être utilisé pour calculer le temps moyen avant une défaillance dangereuse (pour les études de sécurité) en définissant de façon adéquate l'ensemble *UP* des états de disponibilité.

NOTE 2 L'expression exacte pour la fonction de fiabilité $R_{S_i}(t)$, en commençant avec le système à l'état i à t = 0, est donné en résolvant (par exemple en utilisant les transformées de Laplace).

$$R_{S_i}(t) = e^{-q_i t} + \sum_{\substack{j \in UP \\ j \neq i}} \int_0^t q_{ij} e^{-q_i x} R_{S_j}(t - x) dx, \qquad i \in UP$$

Annex A
(informative)

Basic mathematical relationships for Markov techniques

A.1 General

This annex deals with models based on time-homogeneous Markov processes with finitely many states and continuous time. Because of the memory-less property that characterizes such processes, the time spent in any given state is exponentially distributed. For reliability models, this implies that failure and restoration rates (λ and μ) of all elements in a system are constant (time independent). Failure and or restoration rates can change only at a state change.

A.2 Transition rates matrix

A.2.1 State transition diagram

A time-homogeneous Markov process is completely characterized by the transition rates matrix $Q = \left[q_{ij} \right]$ and the initial probability vector at time t = 0. A useful visualization of the transition rates matrix is the state transition diagram. For setting up this diagram, a reliability block diagram (if it exists) and a FMEA for the system can be very useful. In any case, to reduce the number of states it is recommended to collect any group of n series elements (n = 2, 3, ...) in one element with failure rate $\lambda_1 + \ldots + \lambda_n$ and restoration rate $(\lambda_1 + \ldots \lambda_n)/(\lambda_1/\mu_1 + \ldots + \lambda_n/\mu_n)$, provided $\lambda_i << \mu_i, i = 1,\ldots,n$.

Having drawn and verified the state transition diagram (taking care of retained failure modes, assumed restoration priority, and particularities specific to the system considered), the state space $\{0,1,\ldots,m\}$ is divided into two complementary sets UP for the up states and D for the down states, where m is the total number of states. The set of down states can vary according to the system aspect being evaluated (reliability or safety).

A.2.2 Basic relations useful in evaluating Markov techniques

A.2.2.1 For reliability evaluation, the mean time to system failure $MTTF_{S_i}$ when starting with system in state i at t = 0, is obtained by solving

$$MTTF_{S_i} = \frac{1}{q_i} + \sum_{\substack{j \in UP \\ j \neq i}} \frac{q_{ij}}{q_i} MTTF_{S_j}, \qquad i \in UP, \quad q_i = \sum_{\substack{j=0 \\ j \neq i}}^{m} q_{ij}$$

NOTE 1 The above system of algebraic equations can also be used to compute the mean time to a dangerous failure (for safety investigations) by defining adequately the set *UP* of up states.

NOTE 2 The exact expression for the reliability function $R_{S_i}(t)$, when starting with system in state i at t = 0, is given by solving (e.g. using Laplace transforms).

$$R_{S_i}(t) = e^{-q_i t} + \sum_{\substack{j \in UP \\ j \neq i}} \int_0^t q_{ij} e^{-q_i x} R_{S_j}(t - x) dx, \qquad i \in UP$$

A.2.2.2 La disponibilité de l'état asymptotique et stationnaire A_s est donnée par:

$$A_S = \sum_{j \in UP} P_j$$

avec P_j comme solution de

$$P_j = \sum_{\substack{i=0 \\ i \neq j}}^{m} P_i \frac{q_{ij}}{q_j}, \qquad j = 0,...,m, \;\; P_j > 0, \;\; \sum_{j=0}^{m} P_j = 1, \;\; q_i = \sum_{\substack{j=0 \\ j \neq i}}^{m} q_{ij}$$

Ces équations n'étant pas indépendantes, une équation pour P_j (choisie arbitrairement) doit être abandonnée et remplacée par:

$$\sum_{j=0}^{m} P_j = 1$$

A.2.2.3 A cause du taux de défaillance constant, une bonne approximation de la fiabilité de l'intervalle IR_S à l'état stationnaire est:

$$IR_S(t, t+\theta) = \sum_{j \in UP} P_j R_{S_j}(\theta) \approx A_S e^{-\theta / MTTF_{S0}}$$

0 étant un état dans lequel tous les éléments fonctionnent (ou sont prêts à fonctionner).

A.2.2.4 L'intensité de défaillance de l'état asymptotique et stationnaire (fréquence de défaillance) au niveau du système z_S est donnée par:

$$z_S = \sum_{\substack{j \in UP \\ i \in D}} P_j q_{ji} = \sum_{j \in UP} P_j \left(\sum_{i \in D} q_{ji} \right)$$

NOTE 1 Dans l'équation ci-dessus, tous les taux de transition q_{ji} laissant l'état $j \in UP$ pour $i \in D$ doivent être pris en considération.

NOTE 2 Pour petit Δt, $z_s \Delta t$ donne la probabilité pour une transition d'un état dans l'ensemble des états de disponibilité dans l'ensemble des états d'indisponibilité, et vice-versa, dans $(t, t+\Delta t)$ quel que soit t arbitraire (état stationnaire).

A.2.2.5 Le MUT_S (temps moyen de disponibilité au niveau du système) et le MDT_S (temps moyen d'indisponibilité au niveau du système) sont donnés dans l'état stationnaire par:

$$MUT_S = \frac{A_S}{z_S} \quad \text{et} \quad MDT_S = \frac{1 - A_S}{z_s}$$

NOTE $\mathrm{MUT}_S + \mathrm{MDT}_S = 1/z_S$ où z_S est l'intensité de défaillance de l'état asymptotique et stationnaire (fréquence de défaillance) au niveau du système donnée en A.2.2.4.

A.2.2.6 Pour un état donné i, cela tient en particulier à

$\frac{1}{q_i}$ = temps moyen inconditionnel passé dans un état i

$P_i(t)q_i$ = fréquence d'une transition hors de l'état i

A.2.2.2 The asymptotic and steady-state availability A_S is given by

$$A_S = \sum_{j \in UP} P_j$$

with P_j as solution of

$$P_j = \sum_{\substack{i=0 \\ i \neq j}}^{m} P_i \frac{q_{ij}}{q_j}, \qquad j = 0,...,m, \;\; P_j > 0, \;\; \sum_{j=0}^{m} P_j = 1, \;\; q_i = \sum_{\substack{j=0 \\ j \neq i}}^{m} q_{ij}$$

Since these equations are not independent, one equation for P_j (arbitrarily chosen) must be dropped and replaced by

$$\sum_{j=0}^{m} P_j = 1$$

A.2.2.3 Since the failure rate is assumed constant, a good approximation for the interval reliability IR_S in steady-state is

$$IR_S(t, t+\theta) = \sum_{j \in UP} P_j R_{S_j}(\theta) \approx A_S e^{-\theta / MTTF_{S_0}}$$

Where 0 denotes the state in which all elements are operating (or ready to operate).

A.2.2.4 The asymptotic and steady-state failure intensity (failure frequency) at system level z_S is given by

$$z_S = \sum_{\substack{j \in UP \\ i \in D}} P_j q_{ji} = \sum_{j \in UP} P_j \left(\sum_{i \in D} q_{ji} \right)$$

NOTE 1 In the above equation, all transition rates q_{ji} leaving state $j \in UP$ toward $i \in D$ have to be considered.

NOTE 2 For small Δt, $z_S \Delta t$ gives the probability for a transition from a state in the set of up states to a state in the set of down states, and vice versa, within $(t, t+\Delta t)$ for any arbitrary time t (steady-state).

A.2.2.5 The MUT_S (mean up time at system level) and the MDT_S (mean down time at system level) are given in steady-state by

$$MUT_S = \frac{A_S}{z_S} \quad \text{and} \quad MDT_S = \frac{1 - A_S}{z_S}$$

NOTE $\mathrm{MUT}_S + \mathrm{MDT}_S = 1/z_S$, where z_S is the asymptotic and steady-state failure intensity (failure frequency) at system level given in A.2.2.4.

A.2.2.6 For a given state i, it holds in particular that

$\frac{1}{q_i}$ = unconditional mean time spent in state i

$P_i(t) q_i$ = frequency of a transition out of state i

$\sum_{\substack{j=0 \\ j \neq i}}^{m} P_j(t) q_{ji} \Delta t =$ probabilité inconditionnelle d'entrée dans un état *i* pendant $(t, t + \Delta t)$

pour Δt petit

Pour les séries importantes/structures parallèles, des expressions approximatives sont connues en littérature. Pour les systèmes très importants ou complexes, une simulation de Monte Carlo peut devenir nécessaire.

$\sum_{\substack{j=0 \\ j \neq i}}^{m} P_j(t) q_{ji} \Delta t$ = unconditional probability of entering state *i* within $(t, t + \Delta t)$ for Δt small

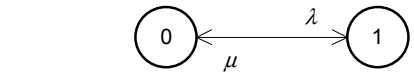
For large series/parallel structures, approximate expressions are known in the literature. For very large or complex systems, a Monte Carlo simulation can become necessary.

Annexe B
(informative)

Exemple: Elaboration des graphes de Markov

B.1 Système à un élément

La première étape dans l'application de la technique de Markov consiste à définir les états du système. Prenons comme exemple un système à un élément. Dans le cas le plus simple, le graphe de Markov correspondant comprend seulement deux états: un état de disponibilité 0, ayant un taux de transition λ, et un état d'indisponibilité 1, ayant un taux de transition μ, ainsi que l'indique la Figure B.1.



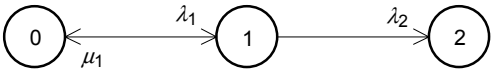
Etat de disponibilité: 0 Etat d'indisponibilité: 1

IEC 663/06

Figure B.1 – Graphe de Markov d'un système à un élément apte au rétablissement

La flèche de l'état 0 vers l'état 1 met en évidence l'apparition d'une défaillance avec la probabilité $\lambda\Delta t$ pendant le court intervalle de temps $(t,t+\Delta t)$ si l'élément était dans un état 0 à t. De façon similaire, la flèche d'un état 1 vers un état 0 indique la réalisation du rétablissement d'un système avec la probabilité $\mu\Delta t$.

Un système à un élément peut aussi être modélisé en utilisant plus que les deux états 0 (fonctionnel) et 1 (défaillant). Un état dégradé, qui reste disponible peut être inclus dans le graphe. Dans la Figure B.2, un tel état est indiqué par 1: l'état de défaillance du système étant indiqué par 2 (l'hypothèse étant faite qu'aucune réparation ne peut être faite à l'état 2).

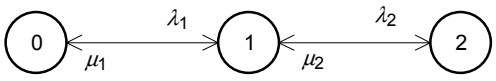


Etat total de disponibilité | Etat dégradé | Etat d'indisponibilité (état absorbant)

IEC 664/06

Figure B.2 – Graphe de Markov à trois états pour système à un élément

Si le rétablissement peut être obtenu à partir de l'état 2, le système peut être modélisé par le graphe de la Figure B.3 dans lequel le taux de rétablissement μ_2 représente la transition de l'état 2 vers l'état 1.



IEC 665/06

Figure B.3 – Graphe de Markov lorsque des rétablissements peuvent être réalisés à partir de l'état 2 pour système à un élément

Annex B
(informative)

Example: Development of state transition diagrams

B.1 One-element system

The first step, in applying the Markov technique, is to define the system states. As an example, consider a one-element system. For the simplest case, the corresponding state transition diagram comprises only two states: an up state 0, with transition rate λ, and a down state 1, with transition rate μ, as shown in Figure B.1.

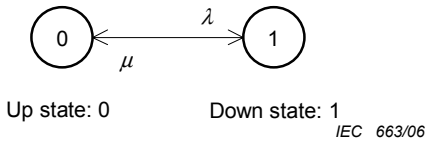


Figure B.1 – State transition diagram for a restorable one-element system

The arrow from state 0 to state 1 denotes a failure occurrence with the probability $\lambda\Delta t$ in the small time interval $(t,t+\Delta t)$ given that the element was in state 0 at t. Similarly, the arrow from state 1 to state 0 shows completion of a system restoration with the probability $\mu\Delta t$.

A one-element system can also be modelled using more than the two states 0 (functional) and 1 (failed). A degraded state which is still an up state may also be included. Such a state is state 1 in Figure B.2: the system failure state being state 2 (assuming no repair is possible in state 2).

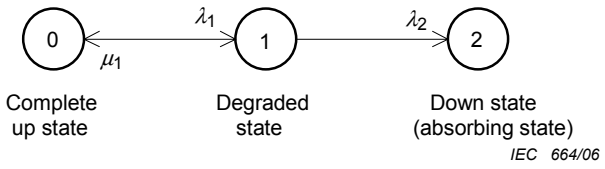


Figure B.2 – State transition diagram with three states for a one-element system

If restoration can be carried out from state 2, the system can be modelled by the diagram in Figure B.3 where the restoration rate μ_2 represents the transition from state 2 to state 1.

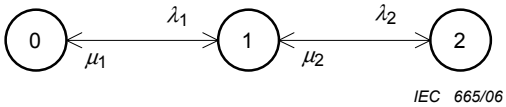


Figure B.3 – State transition diagram when restorations may be made from state 2 for a one-element system

Dans de nombreux cas, un chemin direct de défaillance catalectique de l'état 0 vers l'état 2 doit être considéré et une flèche λ_3, est ajoutée à la Figure B.2 pour donner la Figure B.4

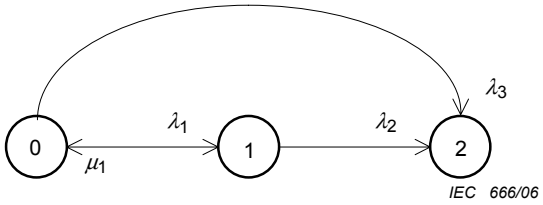


Figure B.4 – Graphe de Markov lorsque qu'une transition directe est considérée pour système à un élément

Le modèle décrit en Figure B.1 peut être utilisé pour obtenir la disponibilité instantanée $A(t)$ et la disponibilité de l'état stationnaire A. Si les calculs de la fiabilité $R(t)$ sont nécessaires, le graphe de Markov montré en Figure B.5 est applicable. Dans ce cas, uniquement le taux de défaillance λ est considéré et l'état 1 devient un état absorbant.

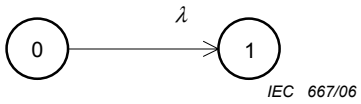
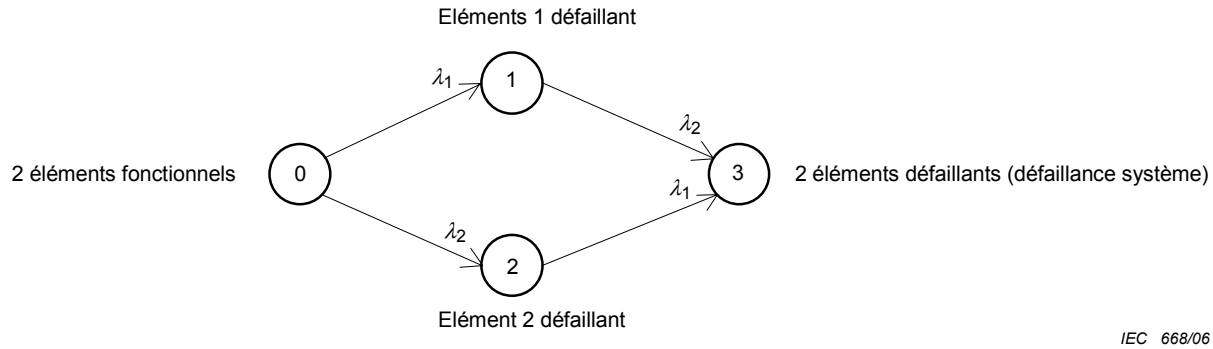


Figure B.5 – Graphe de Markov pour l'évaluation de la fiabilité d'un système à un élément

B.2 Système à deux éléments

En principe, puisqu'un élément peut être représenté par deux états 0 (fonctionnel) et 1 (défaillant) les états de système possibles pour un système ayant deux éléments indépendants sont (0 0), (0 1), (1 0) ,(1 1). Si le système à deux éléments est un système série, (0 0) représente le seul état de disponibilité et (0 1), (1 0), (1 1) représentent les états d'indisponibilité. Si le système contient une redondance active ou passive, (0 0), (0 1), (1 0) représentent les états de disponibilité. Dans ce qui suit, seuls les systèmes à redondance active 1 sur 2, sont considérés.

Le graphe pour système à redondance active «1 sur 2» sans élément apte au rétablissement est donné par la Figure B.6.



NOTE Les symboles d'état peuvent aussi être indiqués par (0 0), (0 1), (1 0), (1 1), correspondant respectivement aux états 0,1,2.3.

Figure B.6 – Graphe de Markov pour système à redondance active 1 sur 2 sans élément apte au rétablissement

In many cases a direct catastrophic failure path from state 0 to state 2 has to be considered and an arrow λ_3, is added to Figure B.2 to give Figure B.4.

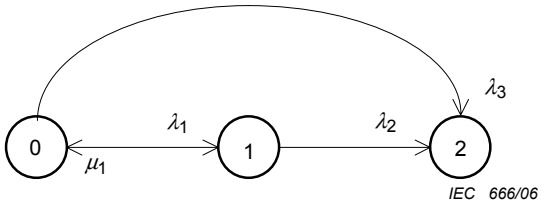


Figure B.4 – State transition diagram when direct transition is considered for a one-element system

The model depicted in Figure B.1 can be used to get the instantaneous availability $A(t)$ and the steady-state availability A. If calculation of reliability $R(t)$ is required, the state transition diagram shown in Figure B.5 is applicable. In this case, only the failure rate λ is considered and state 1 becomes an absorbing state.

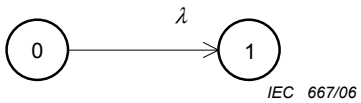
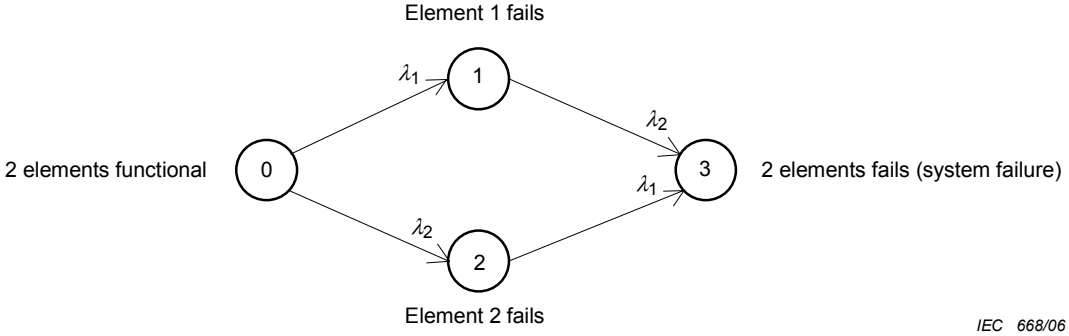


Figure B.5 – State transition diagram for the evaluation of reliability of a one-element system

B.2 Two-element system

Basically, since an element can be represented by two states 0 (up) and 1 (down), possible system states for a system with two independent elements are (0 0), (0 1), (1 0), (1 1). If the two-element system is a series system, (0 0) is the only up state and (0 1), (1 0), (1 1) are down states. If the system contains active or stand-by redundancy, (0 0), (0 1), (1 0) are all up states. In what follows, consideration will be given solely to a 1-out-of-2 active redundant system.

The state transition diagram for a 1-out-of-2 active redundant system with no restorable elements is given in Figure B.6.



NOTE The state symbols may also be marked (0 0), (0 1), (1 0), (1 1) corresponding to states 0,1,2,3 respectively.

Figure B.6 – State transition diagram for a 1-out-of-2 active redundant system with no restorable elements

Si le système est apte au rétablissement, des flèches sont ajoutées pour représenter le rétablissement avec des taux $\mu_{i\ i}$ (i=1,2) comme illustré en Figure B.7. On note qu'un rétablissement simultané est estimé dans ce cas (à partir de l'état 3).

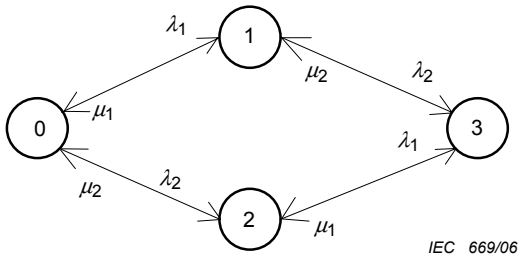


Figure B.7 – Graphe de Markov pour système à redondance active 1 sur 2 avec des éléments aptes au rétablissement,deux équipes de rétablissement et sans limitation de rétablissement

Si une défaillance de cause commune provoque une panne simultanée des deux éléments d'un système à redondance «1 sur 2» apte au rétablissement, il est probable que le temps nécessaire pour rétablir le système après une défaillance de cause commune (retour de l'état 3 à l'état 0) soit différent du temps requis pour remettre le système en état après des défaillances des éléments individuels. Ceci doit être pris en compte conformément à la Figure B.8, où λ_C et μ_C représentent respectivement les taux de défaillance de cause commune et de rétablissement.

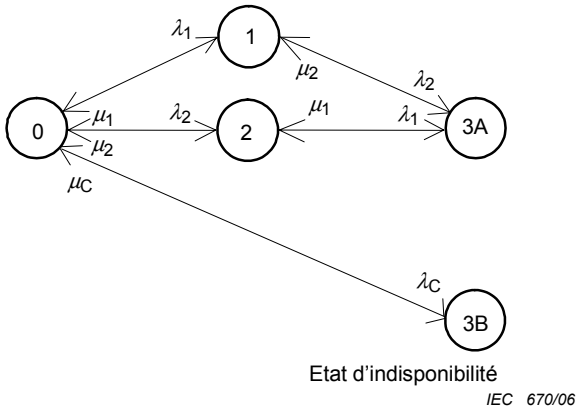


Figure B.8 – Graphe de Markov pour système à redondance active «1 sur 2» avec des éléments aptes au rétablissement, deux équipes de rétablissement et une cause commune de défaillance du système

A titre d'exemple, considérons un système à deux générateurs passifs qui ne démarrent pas dans des conditions de température ambiante basse. Lorsque le système atteint l'état «les deux générateurs ne démarrent pas», le temps de rétablissement dépendra du fait que, soit chaque générateur a été mis hors service par une défaillance mécanique indépendante, soit les deux générateurs ont été mis hors service par une défaillance de cause commune, telle qu'une température ambiante basse. Par conséquent, l'état «les deux générateurs ne démarrent pas à cause de pannes indépendantes» doit être considéré séparément de l'état «les deux générateurs ne démarrent pas suite à une cause commune». Cependant, pour l'utilisateur du système, seul importe que les «deux générateurs sont en panne», et non pas comment. Par conséquent, les deux états forment un état combiné pour lequel les mesures de fiabilité, de disponibilité, de maintenabilité et de sécurité peuvent être obtenues.

If the system is restorable, arrows are added representing restoration with rates μ_i (i=1,2) as illustrated in Figure B.7. Note that no resource limitation for restoration is assumed here (from state 3).

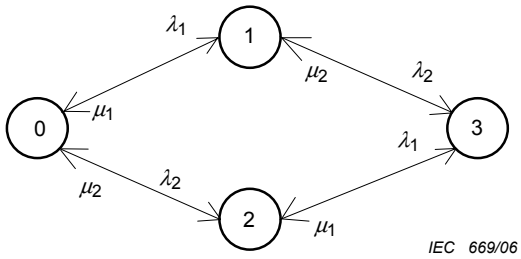


Figure B.7 – State transition diagram for a 1-out-of-2 active redundant system with restorable elements, two restoration teams and no restoration limitations

If a common cause failure disables simultaneously both elements in a restorable 1-out-of-2 redundant system, it is likely that the time needed to restore the system after a common cause failure (return from state 3 to state 0) differs from the time needed to restore the system after failures of the individual elements. This has to be taken into account as shown in Figure B.8, where λ_C and μ_C denote the common cause failure and restoration rates, respectively.

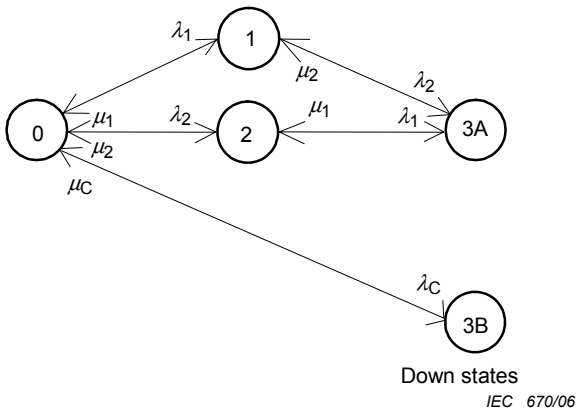


Figure B.8 – State transition diagram for a 1-out-of-2 active redundant system with restorable elements, two restoration teams and common cause for a system failure

As an example, consider a system with two stand-by generators which would not start at low ambient temperatures. When the system reaches the state "both generators failed to start", the restoration time will depend on whether each generator was disabled by an independent mechanical failure, or both generators were incapacitated by a common cause, such as low ambient temperature. Therefore, the state "both generators failed to start due to independent faults" has to be considered as separate from the state "both generators failed to start due to a common cause". However, for the user of the system it may only be important that "both generators failed", and not how. Therefore, both states form a combined state from which the reliability, availability, maintainability and safety measures can be obtained

L'analyse de Markov est apte à prendre en compte les stratégies de maintenance, mais une attention particulière doit être portée à la prise en compte des propriétés de non mémorisation. Supposons qu'il n'existe qu'une équipe chargée du rétablissement et que la stratégie de maintenance est la suivante: la priorité de rétablissement va au composant défaillant en premier. L'ordre des défaillances doit être pris en compte. Ceci est illustré par le graphe de la Figure B.9.

Dans la Figure B.9 les états 3 et 4 ont les significations suivantes:

– état 3: les deux composants sont défaillants, le composant 1 étant le premier défaillant,
– état 4: les deux composants sont défaillants, le composant 2 étant le premier défaillant.

Il faut noter que dans le diagramme de transition décrit en Figure B.9, le temps moyen de réparation d'un composant, par exemple le composant 1, est en fait plus long que le MTTR attendu $1/\mu_1$. Si dans l'état 1 une nouvelle panne se produit, le temps de réparation jusqu'à la seconde panne n'est pas pris en compte après la transition à l'état 3, où la réparation du composant 1 recommence à nouveau à cause des propriétés de non mémorisation. Afin de compenser cette surestimation du temps de réparation, il peut être possible d'augmenter les taux résiduels de réparation. Dans le cas particulier de la Figure B.9, les taux de réparation aux états 3 et 4 peuvent être doublés afin de compenser. Pour les autres niveaux de redondance et de réparation non instantanée, la compensation peut être différente et son application plus compliquée.

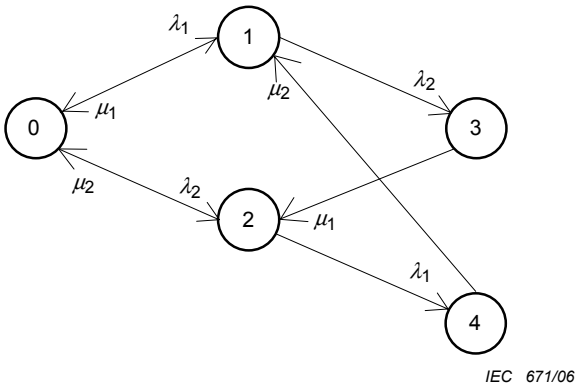


Figure B.9 – Graphe pour système à redondance active «1 sur 2» avec seulement une équipe chargée du rétablissement et une priorité de rétablissement premier entré/premier sorti

B.3 Regroupement des graphes de Markov

Pour faciliter le calcul, il convient de faire des tentatives pour construire les graphes de Markov en utilisant le moins possible d'états. Si des éléments dans une configuration redondante parallèle peuvent être estimés indépendants et λ avoir le même taux de défaillance et le même taux de rétablissement μ qu'indiqué en exemple dans la Figure B.10 pour un système à redondance active «2 sur 4», alors le diagramme d'état de transition peut être exprimé sous une forme de regroupement illustrée par la Figure B.11. Dans cette dernière, l'hypothèse est faite que des ressources illimitées de réparation sont disponibles. Il faut noter que si trois éléments sont défaillants, le système est défaillant et aucune autre défaillance n'est alors considérée.

State transition diagrams can take maintenance strategies into account, but particular care has to be taken with respect to the memory-less property. Assume that only one restoration team exists and that the maintenance strategy is as follows: the restoration priority is for the component which has failed first. The order of failure occurrences has to be taken into account. This is illustrated by the state transition diagram of Figure B.9.

In Figure B.9 states 3 and 4 have the following meanings:

– state 3: the two components have failed, the component number 1 has failed first;
– state 4: the two components have failed, the component number 2 has failed first.

Note that in the state transition diagram depicted in Figure B.9, the mean time to repair a component, e.g. component 1, actually takes longer than the intended MTTR $1/\mu_1$. If in state 1 a second failure occurs, the repair time up to the second failure is not taken into account after transition to state 3, where the repair of component 1 starts again, due to the memory-less property. In order to compensate for the overrepresentation of the repair time, it would be possible to increase the residual repair rates. In the particular case in Figure B.9, the repair rates in states 3 and 4 would have to be doubled as a compensation. For other levels of redundancy and non-instantaneous repair, the compensation would be different and more difficult to apply.

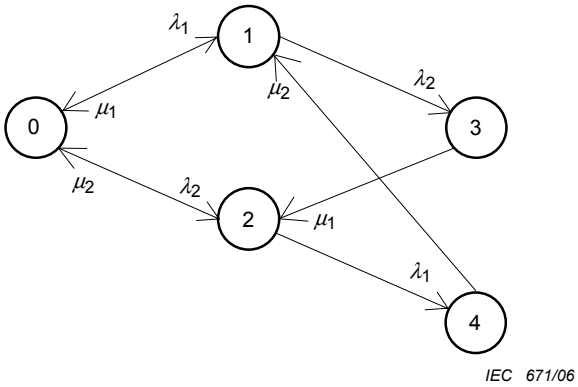


Figure B.9 – State transition diagram for a 1-out-of-2 active redundant system with only one restoration team and restoration priority as first-in/first-out

B.3 Aggregation of state transition diagram

For ease of computation, attempts should be made to construct state transition diagrams using a number of states as small as possible. If elements in a parallel redundant configuration are assumed to be independent and have the same failure rate λ, and the same restoration rate μ as shown in Figure B.10 for a 2-out-of-4 active redundant system, then the state transition diagram can be expressed in an aggregated form illustrated by Figure B.11. In Figure B.11, it is assumed that unlimited repair resources are available. Note that once three elements are failed, the system is failed and no further failure is considered.

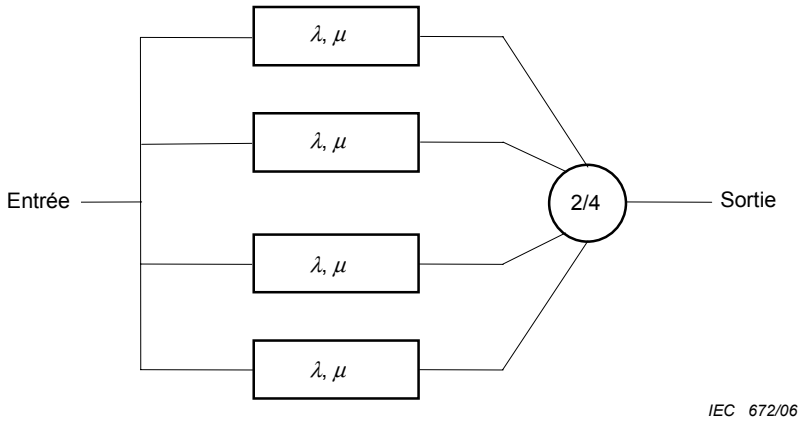


Figure B.10 – Diagramme de fiabilité pour système à redondance active «2 sur 4»

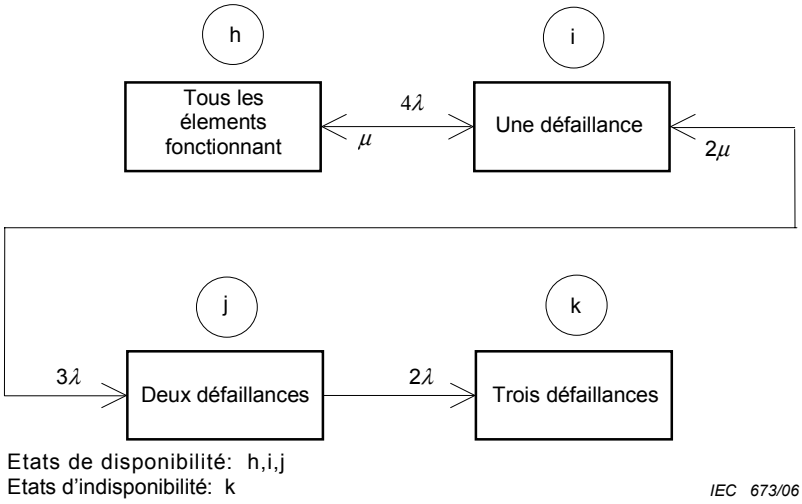


Figure B.11 – Graphe de Markov regroupé pour le calcul de la fiabilité du système dans la Figure B.10

A partir du diagramme ci-dessus, un ensemble d'équations algébriques peut être obtenu et résolu (voir Annexe A) pour donner l'expression suivante pour le temps moyen de fonctionnement du système avant défaillance en commençant à l'état 0 (les 4 éléments à l'état disponible) à t=0 ($MTTF_{S0}$):

$$MTTF_{S0} = \frac{1}{4\lambda}\left(\frac{\mu}{3\lambda}\cdot\frac{2\mu}{2\lambda}+\frac{\mu}{3\lambda}+1\right) + \frac{1}{3\lambda}\left(\frac{2\mu}{2\lambda}+1\right) + \frac{1}{2\lambda}$$

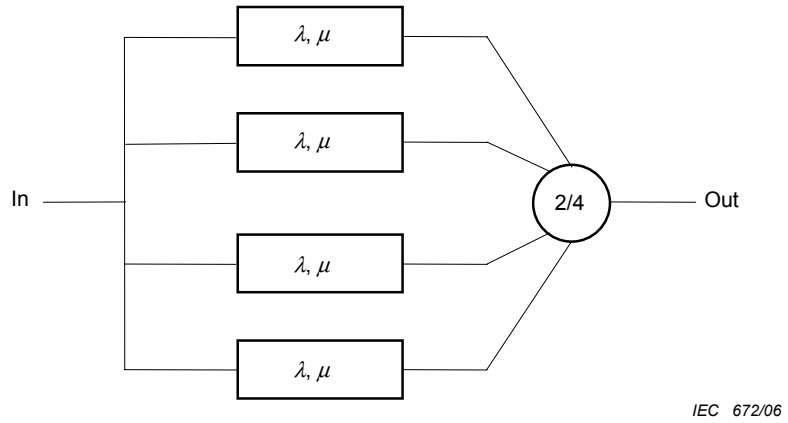


Figure B.10 – Reliability block diagram for a 2-out-of-4 active redundant system

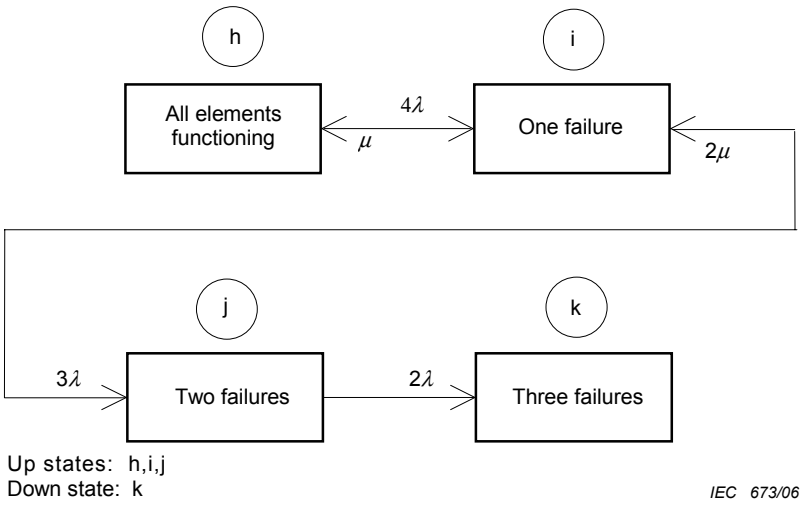


Figure B.11 – Aggregated state transition diagram for reliability computation of the system in Figure B.10

From the above diagram, a set of algebraic equations can be obtained and solved (see Annex A) to give the following expression for the system mean time to failure when starting in state 0 (all 4 elements up) at t=0 ($MTTF_{S0}$):

$$MTTF_{S0} = \frac{1}{4\lambda}\left(\frac{\mu}{3\lambda}\cdot\frac{2\mu}{2\lambda}+\frac{\mu}{3\lambda}+1\right) + \frac{1}{3\lambda}\left(\frac{2\mu}{2\lambda}+1\right) + \frac{1}{2\lambda}$$

Annexe C
(informative)

Exemple: Evaluation numérique de mesures de fiabilité, disponibilité, maintenabilité et de sécurité pour système en redondance active «1 sur 2»

C.1 Objectif

Dans cette annexe un système en redondance active «1 sur 2» apte au rétablissement sans contrainte de rétablissement est considéré. Les mesures à estimer sont celles de la disponibilité instantanée, de la disponibilité asymptotique, de la fiabilité et du MTTFF. Les méthodes mathématiques conventionnelles que l'on applique habituellement dans ce domaine sont utilisées.

C.2 Modélisation

Le graphe de Markov pour un système à redondance active «1 sur 2» est présenté à la Figure C.1 pour l'évaluation de la disponibilité. L'état 3 est l'état d'indisponibilité.

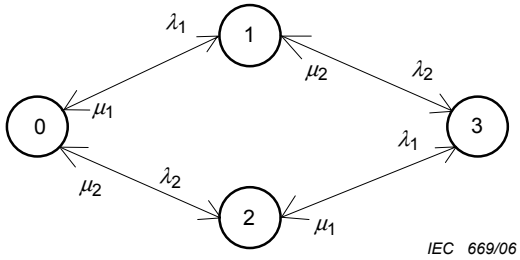


Figure C.1 – Graphe de Markov pour système à redondance active 1 sur 2 avec des éléments différents et deux équipes chargées du rétablissement

On remarque que le graphe de Markov pour évaluer la fiabilité R(t) est obtenu en éliminant les transitions de rétablissement de l'état 3 vers les états 1 et 2. Dans ces conditions, l'état 3 devient un état absorbant.

Si on suppose que les deux éléments du système sont identiques ou bien ont les mêmes taux de rétablissement et de défaillance, le graphe réduit se présente alors selon la Figure C.2.

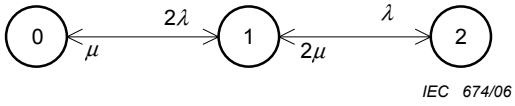


Figure C.2 – Graphe de Markov pour système à redondance active 1 sur 2 avec des éléments identiques, deux équipes chargées du rétablissement et avec des ressources illimitées de rétablissement

Il est à noter que le graphe de Markov pour évaluer la fiabilité R(t) est obtenu en éliminant la transition de rétablissement de l'état 2 vers l'état 1. Dans ces conditions, l'état 2 devient un état absorbant.

Annex C
(informative)

Example: Numerical evaluation of some reliability, availability, maintainability and safety measures for a 1-out-of-2 active redundant system

C.1 Objective

In this annex, a 1-out-of-2 restorable active redundant system with no restoration constraints considered. The measures to be assessed are instantaneous availability, asymptotic availability, reliability and MTTFF. Conventional mathematical methods commonly used in such evaluations are applied.

C.2 Modelling

The state transition diagram for the 1-out-of-2 active redundant system is given in Figure C.1 for the assessment of the availability. State 3 is the down state.

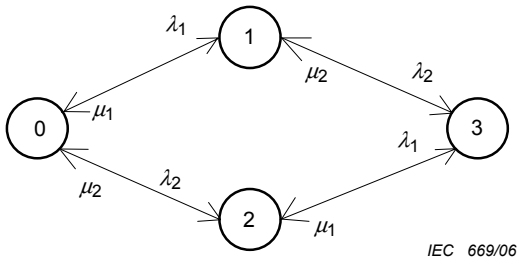


Figure C.1 – State transition diagram for 1-out-of-2 active redundant system with different elements and two restoration teams

Note that the state transition diagram to assess reliability $R(t)$ is obtained by eliminating the restoration transitions from state 3 to states 1 and 2. State 3 thus becomes an absorbing state.

Assuming that the two elements in the system are identical or have the same failure and restoration rates, the reduced diagram then becomes as Figure C.2.

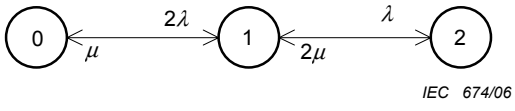


Figure C.2 – State transition diagram for a 1-out-of-2 active redundant system with identical elements, two restoration teams and unlimited restoration resources

Note also that the state transition diagram to assess reliability, $R(t)$, is obtained by eliminating the restoration transition from state 2 to state 1. State 2 thus becomes an absorbing state.

C.3 Méthode d'équation différentielle

C.3.1 Méthode pour déterminer la disponibilité

Soit $P_0(t), P_1(t), P_2(t)$ les probabilités du système d'être dans les états 0, 1 et 2 respectivement à l'instant t (Figure C.2). On obtient les équations différentielles suivantes à partir du graphe de Markov de la Figure C.2.

$$\frac{dP_0(t)}{dt} = -2\lambda P_0(t) + \mu P_1(t)$$
$$\frac{dP_1(t)}{dt} = 2\lambda P_0(t) - (\lambda + \mu) P_1(t) + 2\mu P_2(t)$$
$$\frac{dP_2(t)}{dt} = \lambda P_1(t) - 2\mu P_2(t)$$

Ainsi la matrice des taux de transition, qui peut être établie directement à partir du graphe, devient:

$$Q(\lambda,\mu) = \begin{bmatrix} -2\lambda & 2\lambda & 0 \\ \mu & -(\lambda+\mu) & \lambda \\ 0 & 2\mu & -2\mu \end{bmatrix}$$

et on peut exprimer de façon formelle l'équation différentielle $\frac{d}{dt}P(t) = Q(\lambda,\mu)^T \times P(t)$, où $P(t) = [P_0(t) \quad P_1(t) \quad P_2(t)]^T$.

Il devient nécessaire de trouver les valeurs propres $\varepsilon(\lambda,\mu)$ et les vecteurs propres $E(\lambda,\mu)$ de la matrice Q^T. Dans le cas de valeurs propres distinctes (qui dans la technique de Markov en temps continu tient pour la plupart des modèles d'intérêt pour presque toutes les valeurs de paramètres) le vecteur des probabilités d'état peut être exprimé directement par:

$$P(t) = E(\lambda,\mu) \times \begin{bmatrix} \exp(\varepsilon(\lambda,\mu)_0 t) & & \\ & \exp(\varepsilon(\lambda,\mu)_1 t) & \\ & & \exp(\varepsilon(\lambda,\mu)_2 t) \end{bmatrix} \times E(\lambda,\mu)^{-1} \times P(0)$$

Les probabilités $P_0(t), P_1(t), P_2(t)$ peuvent être calculées en évaluant l'équation de la matrice ci-dessus, en supposant, par exemple, que à l'instant t = 0 le système est dans un état 0, soit:

$$P(0) = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

La disponibilité instantanée, $A_{S0}(t)$ est alors calculée selon:

$$A_{S0}(t) = P_0(t) + P_1(t)$$

C.3 Differential equation method

C.3.1 Method for evaluating availability

Let $P_0(t), P_1(t), P_2(t)$ be the probabilities of the system being in states 0, 1 and 2 respectively at time t (Figure C.2). The following differential equations are obtained from the state transition diagram of Figure C.2:

$$\frac{dP_0(t)}{dt} = -2\lambda P_0(t) + \mu P_1(t)$$
$$\frac{dP_1(t)}{dt} = 2\lambda P_0(t) - (\lambda + \mu) P_1(t) + 2\mu P_2(t)$$
$$\frac{dP_2(t)}{dt} = \lambda P_1(t) - 2\mu P_2(t)$$

Thus the transition rates matrix, which can also be directly established from the state transition diagram, becomes

$$Q(\lambda,\mu) = \begin{bmatrix} -2\lambda & 2\lambda & 0 \\ \mu & -(\lambda+\mu) & \lambda \\ 0 & 2\mu & -2\mu \end{bmatrix}$$

and we can formally express the differential equation as $\frac{d}{dt}P(t) = Q(\lambda,\mu)^T \times P(t)$, where $P(t) = [P_0(t) \quad P_1(t) \quad P_2(t)]^T$.

It is now necessary to find the eigenvalues $\varepsilon(\lambda,\mu)$ and eigenvectors $E(\lambda,\mu)$ of the matrix Q^T. In the case of distinct eigenvalues (which in continuous-time Markov techniques holds for most models of interest for almost all parameter values) the vector of state probabilities can directly be expressed by

$$P(t) = E(\lambda,\mu) \times \begin{bmatrix} \exp(\varepsilon(\lambda,\mu)_0 t) & & \\ & \exp(\varepsilon(\lambda,\mu)_1 t) & \\ & & \exp(\varepsilon(\lambda,\mu)_2 t) \end{bmatrix} \times E(\lambda,\mu)^{-1} \times P(0)$$

By evaluating the above matrix equation, the probabilities $P_0(t), P_1(t), P_2(t)$ can be computed assuming, for instance, that at time t = 0 the system is in state 0, i.e.

$$P(0) = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

The instantaneous availability, $A_{S0}(t)$ is then computed as

$$A_{S0}(t) = P_0(t) + P_1(t)$$

Les indices *S0* dans $A_{S0}(t)$ montrent clairement qu'un des indices traite de la disponibilité au niveau du système pour le système commençant à l'état 0 à l'instant t = 0. Pour ce modèle simple, une expression explicite en λ et μ peut être calculée par exemple en utilisant les transformées de Laplace et est donnée par:

$$A_{S0}(t) = \frac{\mu^2 + 2\lambda\mu}{(\lambda+\mu)^2} + \left(\frac{\lambda}{\lambda+\mu}\right)^2 e^{-(\lambda+\mu)t}\left(2 - e^{-(\lambda+\mu)t}\right)$$

La Figure C.3 montre un exemple numérique pour l'indisponibilité $U_{S0}(t)=1 - A_{S0}(t)$.

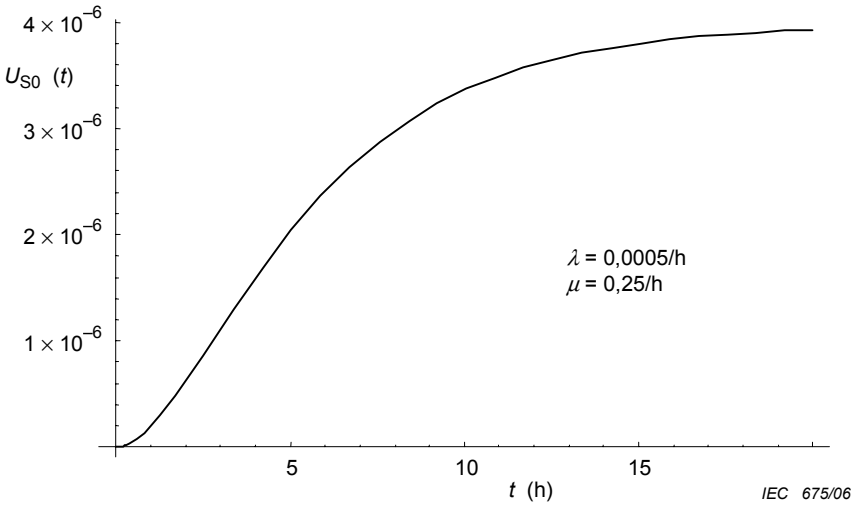


Figure C.3 – Exemple numérique pour l'Indisponibilité

Dans la généralité, il convient d'évaluer les équations différentielles par l'utilisation d'un programme informatique mathématique sous forme numérique ou symbolique.

Depuis $A_{S0}(t)$, la disponibilité d'état stationnaire et asymptotique $A_{S0}(\infty)=A_S$ suit immédiatement. Alternativement, en posant $P_i(\infty)=P_i$ (i=0,1,2) comme valeur asymptotique et stationnaire des probabilités d'état, A_S suit comme $A_S=P_0+P_1$ avec P_i comme solution des équations suivantes (voir Annexe A):

$$\begin{aligned} 0 &= -2\lambda P_0 + \mu P_1 \\ 0 &= 2\lambda P_0 - (\lambda+\mu)P_1 + 2\mu P_2 \\ 0 &= \lambda P_1 - 2\mu P_2 \end{aligned}$$

Dans l'ensemble ci-dessus d'équations algébriques, chacune d'entre elles peut être déduite des deux autres, de telle sorte qu'il n'y a vraiment que deux équations utiles et trois inconnues. Pour dépasser cette difficulté, on utilise le fait que $P_0 + P_1 + P_2 = 1$ est utilisé comme troisième équation. Il s'ensuit après quelques transformations mathématiques, que:

$$A_S = \frac{\mu^2 + 2\lambda\mu}{(\lambda+\mu)^2}$$

The indices *S0* in $A_{S0}(t)$ make clear that one deals with the availability at system level for the system starting in state 0 at t=0. For this simple model, an explicit expression in λ and μ can be calculated by e. g. using Laplace transforms and is given by

$$A_{S0}(t) = \frac{\mu^2 + 2\lambda\mu}{(\lambda+\mu)^2} + \left(\frac{\lambda}{\lambda+\mu}\right)^2 e^{-(\lambda+\mu)t}\left(2 - e^{-(\lambda+\mu)t}\right)$$

Figure C.3 shows a numerical example for the unavailability $U_{S0}(t) = 1 - A_{S0}(t)$.

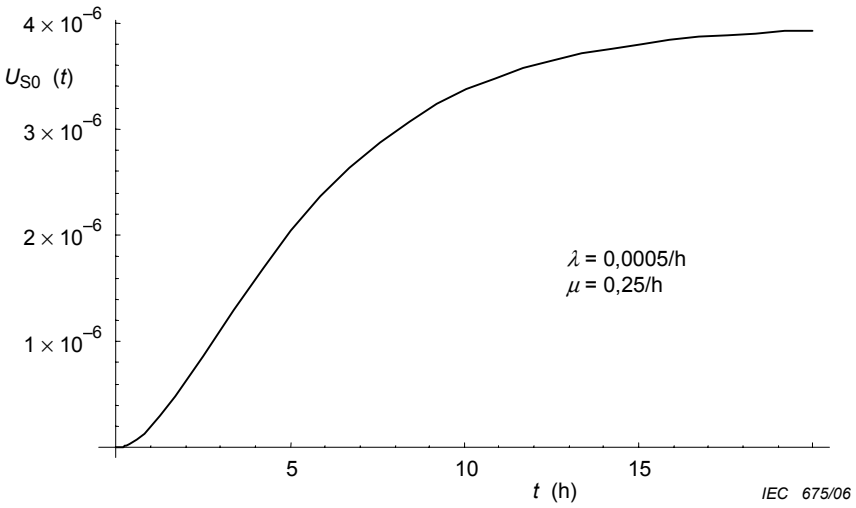


Figure C.3 – Numerical example for unavailability

In the general case, the differential equations would have to be evaluated by use of a mathematical computer program either numerically or in a symbolic form.

From $A_{S0}(t)$, the asymptotic and steady-state availability $A_{S0}(\infty) = A_S$ follows immediately. Alternatively, setting $P_i(\infty) = P_i$ (i = 0, 1, 2) for the asymptotic and steady-state value of the state probabilities, A_S follows as $A_S = P_0 + P_1$ with P_i as solution of the following equations (see Annex A)

$$\begin{aligned} 0 &= -2\lambda P_0 + \mu P_1 \\ 0 &= 2\lambda P_0 - (\lambda+\mu)P_1 + 2\mu P_2 \\ 0 &= \lambda P_1 - 2\mu P_2 \end{aligned}$$

In the above set of algebraic equations, any one can be obtained from the other two, so that there are really only two useful equations and three unknowns. To overcome this difficulty, the fact that $P_0 + P_1 + P_2 = 1$ is used as the third equation. Hence, after some mathematical manipulation, it can be shown that

$$A_S = \frac{\mu^2 + 2\lambda\mu}{(\lambda+\mu)^2}$$

On note à présent MUT_S et MDT_S peuvent être dérivés comme suit:

$$MUT_S = \frac{A_S}{z_S} = \frac{2\lambda + \mu}{2\lambda^2}$$

$$MDT_S = \frac{1 - A_S}{z_S} = \frac{1}{2\mu}$$

où

$$z_S = P_1\lambda = \frac{2\mu\lambda^2}{(\lambda + \mu)^2}$$

est l'intensité de défaillance d'état limité et stationnaire (fréquence de défaillance) au niveau du système (voir Annexe A).

C.3.2 Méthode pour déterminer la fiabilité

Afin d'évaluer la fiabilité et le MTTF d'un système à redondance active "1 sur 2" (indépendamment du nombre d'équipes chargées du rétablissement), l'état 2 (indisponibilité du système) est mis en état absorbant. Les équations différentielles suivantes sont déduites du diagramme de transition de la Figure C.2 en retirant la transition de rétablissement de l'état 2 vers l'état 1:

$$\frac{dP_0(t)}{dt} = -2\lambda P_0(t) + \mu P_1(t)$$
$$\frac{dP_1(t)}{dt} = 2\lambda P_0(t) - (\lambda + \mu) P_1(t)$$
$$\frac{dP_2(t)}{dt} = \lambda P_1(t)$$

Les probabilités $P_0(t), P_1(t), P_2(t)$ peuvent être calculées en résolvant ce système d'équation différentielle, en supposant que, à l'instant t = 0, le système est dans l'état 0:

$$P(0) = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

La fiabilité du système $R_{S0}(t)$ est alors calculée selon:

$$R_{S0}(t) = P_0(t) + P_1(t)$$

Une expression explicite en fonction de λ et μ peut être calculée en utilisant par exemple les transformées de Laplace. Elle est donnée par:

$$R_{S0}(t) = \frac{s_1 e^{s_2 t} - s_2 e^{s_1 t}}{s_1 - s_2}$$

où

$$s_1 s_2 = 2\lambda^2$$
$$s_1 + s_2 = -(\mu + 3\lambda)$$

Note that now MUT_S and MDT_S can be derived as

$$MUT_S = \frac{A_S}{z_S} = \frac{2\lambda + \mu}{2\lambda^2}$$

$$MDT_S = \frac{1 - A_S}{z_S} = \frac{1}{2\mu}$$

where

$$z_S = P_1\lambda = \frac{2\mu\lambda^2}{(\lambda + \mu)^2}$$

is the limiting and steady-state failure intensity (failure frequency) at system level (see Annex A).

C.3.2 Method for evaluating reliability

To assess the reliability and the MTTF of a 1-out-of-2 active redundant system (independently of the number of restoration teams), state 2 (system down state) is made the absorbing state. The following differential equations are obtained from the state transition diagram in Figure C.2 by removing the transition from state 2 to state 1:

$$\frac{dP_0(t)}{dt} = -2\lambda P_0(t) + \mu P_1(t)$$
$$\frac{dP_1(t)}{dt} = 2\lambda P_0(t) - (\lambda + \mu) P_1(t)$$
$$\frac{dP_2(t)}{dt} = \lambda P_1(t)$$

By solving this differential equation system, the probabilities $P_0(t), P_1(t), P_2(t)$ can be computed assuming that at time t = 0, the system is in state 0:

$$P(0) = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

The system reliability R_{S0}(t) is then computed as

$$R_{S0}(t) = P_0(t) + P_1(t)$$

An explicit expression in terms of λ and μ can be calculated, for example, by the use of Laplace transforms and is given by

$$R_{S0}(t) = \frac{s_1 e^{s_2 t} - s_2 e^{s_1 t}}{s_1 - s_2}$$

where

$$s_1 s_2 = 2\lambda^2$$
$$s_1 + s_2 = -(\mu + 3\lambda)$$

Le $MTTF_{S0}$ peut être calculé soit à partir de l'expression de $R_{S0}(t)$, auquel cas:

$$MTTF_{S0} = \int_0^\infty R_{S0}(t)dt = \frac{\mu + 3\lambda}{2\lambda^2}$$

ou bien à partir du système d'équations algébriques donné en A.2.2.1.

C.3.3 Méthode pour déterminer la sécurité

L'évaluation de la sécurité diffère uniquement par l'interprétation du modèle: l'état 2 peut être défini par un état dangereux et cet état est atteint quand les deux éléments sont défaillants ou si les deux éléments sont défaillants en même temps à cause d'une défaillance de cause commune (dans ce dernier cas, le diagramme des taux de transition doit être étendu comme montré dans la Figure B.8). Les temps de rétablissement doivent être interprétés comme temps d'inspection.

L'évaluation du PFD sera la même que l'évaluation de l'indisponibilité du système. Pour l'évaluation du MTTFH ou DFR, l'état 2 doit devenir un état absorbant et l'évaluation sera la même que pour des besoins de fiabilité.

La Figure C.4 montre une évaluation numérique du DFR, qui est dérivée de la relation de la fiabilité du système.

$$h_S(t) = \frac{-\frac{d}{dt}R_S(t)}{R_S(t)}$$

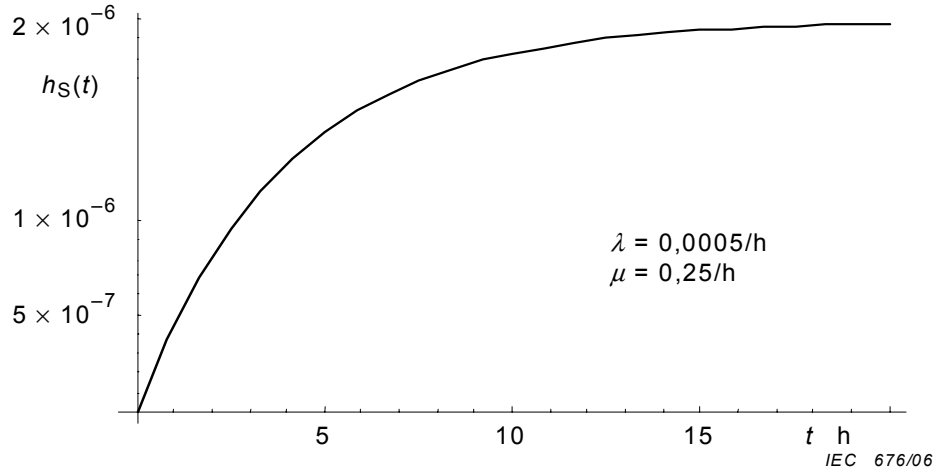


Figure C.4 – Exemple numérique pour le taux de défaillance dangereuse (DFR)

The $MTTF_{S0}$ can be calculated either from the expression for $R_{S0}(t)$, in which case

$$MTTF_{S0} = \int_0^\infty R_{S0}(t)dt = \frac{\mu + 3\lambda}{2\lambda^2}$$

or from the set of algebraic equations given in A.2.2.1.

C.3.3 Method for evaluating safety

The safety evaluation differs only by the interpretation of the model: state 2 could be defined as a hazardous state and this state is entered when both elements are failed or if both elements fail at the same time because of a common mode failure (in this last case, the transition rates diagram must be extended as shown in Figure B.8). The restoration times would then have to be interpreted as inspection times.

The evaluation of PFD would be the same as the evaluation of the unavailability of the system. For evaluation of MTTFH or DFR, state 2 would have to become an absorbing state and the evaluation would be the same as for reliability purposes.

Figure C.4 shows a numerical evaluation of the DFR, which was derived by the relation from the system reliability.

$$h_S(t) = \frac{-\frac{d}{dt}R_S(t)}{R_S(t)}$$

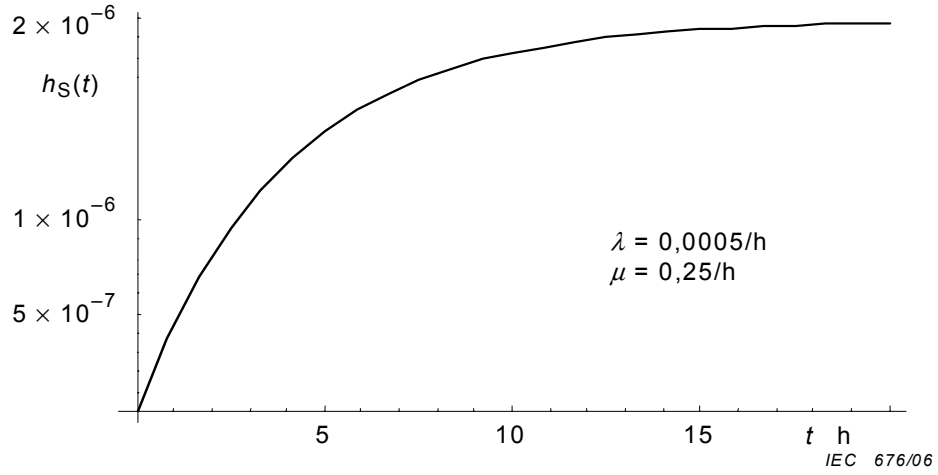


Figure C.4 – Numerical example for dangerous failure rate

Bibliographie

Cette bibliographie contient des normes relatives aux techniques citées et des références annotées pour une lecture plus détaillée.

CEI 60812, Techniques d'analyse de la fiabilité du système – *Procédure d'analyse des modes de défaillance et de leurs d'effets (AMDE)*

CEI 61025, *Analyse par arbre de pannes (AAP)*

CEI 61078, *Techniques d'analyse de la sûreté de fonctionnement – Méthode du diagramme de fiabilité et méthodes booléennes*

Ajmone Marsan, M. , Balbo, G. und Conte, G.: *Performance models of multi-processor systems*, 1986 (Application of Markov models and Petri nets to computer systems performance evaluation)

Billinton R., Allan R.N., *Reliability Evaluation of Engineering Systems. Concepts and Techniques*. Second Edition, New York, Plenum Press, 1992.
(Many examples of practical application of Markov models)

Birolini A., *Reliability Engineering: Theory and Practice*. 4th Edition, Berlin/Heidelberg/New York, Springer-Verlag, 2004.
(Theoretical basis of Markov models, with many applications, approximations)

Brémaud P., *Markov Chains: Gibbs Fields, Monte Carlo Simulation, and Queues*. Springer, New York, 1998.
(Theoretical basis of Markov models, with applications)

Bux, W., Herzog, U.: The Phase Concept: Approximation of Measured Data and Performance Analysis, in: Chandy, K. M., Reiser, M. (eds.): Computer Performance, North Holland, 1977, 23-38 (Explanation of the phase concept and algorithm for practical approximation)

Buzacott J.A., Markov approach to finding failure times of repairable systems. *IEEE Transactions on Reliability*, 1970, Vol.R-19, No.4, pp.128-134.
(Matrix algebra approach for MTTTF, MUT, MDT and etc.)

Çinlar E., *Introduction to Stochastic Processes*. Englewood Cliffs, Prentice Hall, 1975.
(Theoretical basis of Markov models, with applications)

Dhillon B.S., Singh C., *Engineering Reliability, New Techniques and Applications*. New York, Wiley, 1981.
(Many examples of practical application of Markov models)

Endrenyi J., *Reliability Modelling in Electric Power Systems*. New York, Wiley, 1978.
(Many examples of practical application of Markov models; changing weather conditions and etc.)

Gaede K.W., *Zuverlässigkeit, Mathematische Modelle*. München, Carl Hanser Verlag, 1977.
(Theoretical basis of Markov models, with applications)

Høyland A., Rausand M., *System Reliability Theory. Models and Statistical Methods*, New York, Wiley, 1994.
(Many examples of practical application of Markov models)

Bibliography

This bibliography contains standards for related techniques and annotated references for further reading.

IEC 60812 *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 61025 *Fault tree analysis (FTA)*

IEC 61078 *Analysis techniques for dependability – Reliability block diagram method and Boolean methods*

Ajmone Marsan, M. , Balbo, G.,Conte, G.: Performance models of multi-processor systems, MIT Press, Cambridge, 1986
(Application of Markov models and Petri nets to computer systems performance evaluation)

Billinton R., Allan, R.N.: *Reliability Evaluation of Engineering Systems. Concepts and Techniques*. Second Edition, New York, Plenum Press, 1992.
(Many examples of practical application of Markov models)

Birolini A.: *Reliability Engineering: Theory and Practice*. 4th Edition, Berlin/Heidelberg/New York, Springer-Verlag, 2004.
(Theoretical basis of Markov models, with many applications, approximations)

Brémaud P.: *Markov Chains: Gibbs Fields, Monte Carlo Simulation, and Queues*. Springer, New York, 1998.
(Theoretical basis of Markov models, with applications)

Bux, W., Herzog, U.: The Phase Concept: Approximation of Measured Data and Performance Analysis, in: Chandy, K. M., Reiser, M. (eds.): Computer Performance, North Holland, 1977, 23-38 (Explanation of the phase concept and algorithm for practical approximation)

Buzacott, J.A.: Markov approach to finding failure times of repairable systems. *IEEE Transactions on Reliability*, 1970, Vol.R-19, No.4, pp.128-134.
(Matrix algebra approach for MTTTF, MUT, MDT etc.)

Çinlar, E.: *Introduction to Stochastic Processes*. Englewood Cliffs, Prentice Hall, 1975.
(Theoretical basis of Markov models, with applications)

Dhillon, B.S., Singh C.: *Engineering Reliability, New Techniques and Applications*. New York, Wiley, 1981.
(Many examples of practical application of Markov models)

Endrenyi, J.: *Reliability Modelling in Electric Power Systems*. New York, Wiley, 1978.
(Many examples of practical application of Markov models; changing weather conditions etc.)

Gaede, K.W.: *Zuverlässigkeit, Mathematische Modelle*. München, Carl Hanser Verlag, 1977.
(Theoretical basis of Markov models, with applications)

Høyland, A.: Rausand M., *System Reliability Theory. Models and Statistical Methods*, New York, Wiley, 1994.
(Many examples of practical application of Markov models)

Keilson J., *Markov Chain Models: Rarity and Exponentiality*. Berlin, Springer Verlag, 1979.
(Theoretical basis of Markov models, with applications; uniformization method)

Kulkarni V., *Modeling and Analysis of Stochastic Systems*. London, Chapman & Hall, 1995.
(Theoretical basis of Markov models, with applications, uniformization method)

Kumar S., Grassmann W., Billinton R., A stable algorithm to calculate steady-state probability & frequency of a Markov system. *IEEE Transactions on Reliability*, 1987, Vol.R-36, No.1, pp.58-62.
(Very simple and efficient algorithms for the steady-state probabilities calculation)

Lisnianski A., Levitin G., *Multi-state System Reliability. Assessment, Optimization and Applications*. New Jersey, World Scientific, 2003.
(Application of Markov models for multistate systems, with examples)

Moorsel A.P.van, Sanders W.H., Transient solution of Markov models by combining adaptive and standard uniformization. *IEEE Transactions on Reliability*, 1997, Vol.46, No.3, pp.430-440.
(Recent paper on uniformization methods)

Murphy, K., Carter, C. und Brown, S.: The Exponential Distribution: the Good, the Bad and the Ugly. A practical Guide to its Implementation, Proc. RAMS2002 (Discussion of the constant failure rate property and its pitfalls)

Pagés A., Gondran A., *System Reliability. Evaluation and Prediction in Engineering*. 1986, Berlin, Springer Verlag.
(Theoretical basis of Markov models, with applications; approximations)

Pukite J., Pukite P., *Modeling for Reliability Analysis: Markov Modeling for Reliability, Maintainability, Safety, and Supportability Analyses of Complex Systems*. Wiley-IEEE Press, 1998.
(Many examples of practical application of Markov models)

Reinschke K., *Zuverlässigkeit von Systemen. Bd.1: Systeme mit endlich vielen Zuständen*. Berlin, VEB Verlag Technik, 1973.
(Theoretical basis of Markov models, with applications; matrix algebra methods)

Reinschke K., Ušakov I.A., *Zuverlässigkeitsstrukturen. Modellbildung, Modellauswertung*. Berlin, VEB Verlag Technik, Berlin, 1987.
(Theoretical basis of Markov models, with applications)

Ross S.M., *Stochastic processes*. Second edition. New York, Wiley, 1996.
(Theoretical basis of Markov models, with applications)

Ross S.M., *Introduction to Probability Models*. Seventh Edition. Boston, Academic Press, 2000.
(Theoretical basis of Markov models, with applications)

Schweitzer P., A survey of aggregation-disaggregation in large Markov chains, in W.J. Stewart, editor: *Numerical Solution of Markov Processes*, chapter 4, pp.63-88. New York, Marcel Dekker, 1991.
(Aggregation methods, including lumping)

Singh C., Billinton R., *System Reliability Modelling and Evaluation*. London, Hutchinson, 1977.
(Many examples of practical application of Markov models, basis of Markov techniques, lumping, duration and frequency methods)

Keilson, J.: *Markov Chain Models: Rarity and Exponentiality*. Berlin, Springer Verlag, 1979.
(Theoretical basis of Markov models, with applications; uniformization method)

Kulkarni, V.: *Modeling and Analysis of Stochastic Systems*. London, Chapman & Hall, 1995.
(Theoretical basis of Markov models, with applications, uniformization method)

Kumar, S., Grassmann, W., Billinton, R.: A stable algorithm to calculate steady-state probability & frequency of a Markov system. *IEEE Transactions on Reliability*, 1987, Vol.R-36, No.1, pp.58-62.
(Very simple and efficient algorithms for the steady-state probabilities calculation)

Lisnianski, A., Levitin, G.: *Multi-state System Reliability. Assessment, Optimization and Applications*. New Jersey, World Scientific, 2003.
(Application of Markov models for multistate systems, with examples)

Moorsel, A.P.van, Sanders, W.H.: Transient solution of Markov models by combining adaptive and standard uniformization. *IEEE Transactions on Reliability*, 1997, Vol.46, No.3, pp.430-440.
(Recent paper on uniformization methods)

Murphy, K., Carter, C., Brown, S.: The Exponential Distribution: the Good, the Bad and the Ugly. A practical Guide to its Implementation, Proc. RAMS2002, pp. 550-555 (Discussion of the constant failure rate property and its pitfalls)

Pagés, A., Gondran, A.: *System Reliability. Evaluation and Prediction in Engineering*. 1986, Berlin, Springer Verlag.
(Theoretical basis of Markov models, with applications; approximations)

Pukite, J., Pukite, P.: *Modeling for Reliability Analysis: Markov Modeling for Reliability, Maintainability, Safety, and Supportability Analyzes of Complex Systems*. Wiley-IEEE Press, 1998.
(Many examples of practical application of Markov models)

Reinschke, K.: *Zuverlässigkeit von Systemen. Bd.1: Systeme mit endlich vielen Zuständen*. Berlin, VEB Verlag Technik, 1973.
(Theoretical basis of Markov models, with applications; matrix algebra methods)

Reinschke, K., Ušakov, I.A.: *Zuverlässigkeitsstrukturen. Modellbildung, Modellauswertung*. Berlin, VEB Verlag Technik, Berlin, 1987.
(Theoretical basis of Markov models, with applications)

Ross, S.M.: *Stochastic processes*. Second edition. New York, Wiley, 1996.
(Theoretical basis of Markov models, with applications)

Ross, S.M.: *Introduction to Probability Models*. Seventh Edition. Boston, Academic Press, 2000.
(Theoretical basis of Markov models, with applications)

Schweitzer, P.: A survey of aggregation-disaggregation in large Markov chains, in W.J. Stewart, editor: *Numerical Solution of Markov Processes*, chapter 4, pp.63-88. New York, Marcel Dekker, 1991.
(Aggregation methods, including lumping)

Singh, C., Billinton, R.: *System Reliability Modelling and Evaluation*. London, Hutchinson, 1977.
(Many examples of practical application of Markov models, basis of Markov techniques, lumping, duration and frequency methods)

Stewart W.J., *Introduction to the Numerical Solution of Markov Chains*. Princeton, Princeton University Press, 1994.
(Numerical method for Markov techniques)

Tijms H.C., *Stochastic Models. An Algorithmic Approach*. New York, Wiley, 1994.
(Theoretical basis of Markov models, with applications; algorithms; passage times; uniformization method)

Villemeur A., *Reliability, Availability, Maintainability and Safety Assessment. Volume 1. Methods and Techniques*, Chichester, Wiley, 1992.
(Theoretical basis of Markov models, with many applications; approximation methods)

Yoshimura, I., Sato, Y., Suyama, K.: Safety Integrity Level Model for Safety-related Systems in Dynamic Demand State, *Proceedings of the 2004 Asian International Workshop on Advanced Reliability Modeling (AIWARM 2004)*, pp.577-584, Hiroshima, Japan
(Application of Markov techniques to programmable electronic safety systems)

Stewart, W.J.: *Introduction to the Numerical Solution of Markov Chains*. Princeton, Princeton University Press, 1994.
(Numerical method for Markov techniques)

Tijms, H.C.: *Stochastic Models. An Algorithmic Approach*. New York, Wiley, 1994.
(Theoretical basis of Markov models, with applications; algorithms; passage times; uniformization method)

Villemeur, A.: *Reliability, Availability, Maintainability and Safety Assessment. Volume 1. Methods and Techniques*, Chichester, Wiley, 1992.
(Theoretical basis of Markov models, with many applications; approximation methods)

Yoshimura, I., Sato, Y., Suyama, K.: Safety Integrity Level Model for Safety-related Systems in Dynamic Demand State, *Proceedings of the 2004 Asian International Workshop on Advanced Reliability Modeling (AIWARM 2004)*, pp.577-584, Hiroshima, Japan
(Application of Markov techniques to programmable electronic safety systems)

Standards Survey

The IEC would like to offer you the best quality standards possible. To make sure that we continue to meet your needs, your feedback is essential. Would you please take a minute to answer the questions overleaf and fax them to us at +41 22 919 03 00 or mail them to the address below. Thank you!

Customer Service Centre (CSC)

International Electrotechnical Commission
3, rue de Varembé
1211 Genève 20
Switzerland

or

Fax to: **IEC**/CSC at +41 22 919 03 00

Thank you for your contribution to the standards-making process.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Customer Service Centre (CSC)
International Electrotechnical Commission
3, rue de Varembé
1211 GENEVA 20
Switzerland

Q1 Please report on **ONE STANDARD** and **ONE STANDARD ONLY**. Enter the exact number of the standard: *(e.g. 60601-1-1)*

.....

Q2 Please tell us in what capacity(ies) you bought the standard *(tick all that apply).* I am the/a:

purchasing agent ❑
librarian ❑
researcher ❑
design engineer ❑
safety engineer ❑
testing engineer ❑
marketing specialist ❑
other.....

Q3 I work for/in/as a: *(tick all that apply)*

manufacturing ❑
consultant ❑
government ❑
test/certification facility ❑
public utility ❑
education ❑
military ❑
other.....

Q4 This standard will be used for: *(tick all that apply)*

general reference ❑
product research ❑
product design/development ❑
specifications ❑
tenders ❑
quality assessment ❑
certification ❑
technical documentation ❑
thesis ❑
manufacturing ❑
other.....

Q5 This standard meets my needs: *(tick one)*

not at all ❑
nearly ❑
fairly well ❑
exactly ❑

Q6 If you ticked NOT AT ALL in Question 5 the reason is: *(tick all that apply)*

standard is out of date ❑
standard is incomplete ❑
standard is too academic ❑
standard is too superficial ❑
title is misleading ❑
I made the wrong choice ❑
other .....

Q7 Please assess the standard in the following categories, using the numbers:
(1) unacceptable,
(2) below average,
(3) average,
(4) above average,
(5) exceptional,
(6) not applicable

timeliness.....
quality of writing.....
technical contents.....
logic of arrangement of contents .....
tables, charts, graphs, figures.....
other .....

Q8 I read/use the: *(tick one)*

French text only ❑
English text only ❑
both English and French texts ❑

Q9 Please share any comment on any aspect of the IEC that you would like us to know:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Enquête sur les normes

La CEI ambitionne de vous offrir les meilleures normes possibles. Pour nous assurer que nous continuons à répondre à votre attente, nous avons besoin de quelques renseignements de votre part. Nous vous demandons simplement de consacrer un instant pour répondre au questionnaire ci-après et de nous le retourner par fax au +41 22 919 03 00 ou par courrier à l'adresse ci-dessous. Merci !

Centre du Service Clientèle (CSC)

Commission Electrotechnique Internationale
3, rue de Varembé
1211 Genève 20
Suisse

ou

Télécopie: **CEI**/CSC +41 22 919 03 00

Nous vous remercions de la contribution que vous voudrez bien apporter ainsi à la Normalisation Internationale.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Centre du Service Clientèle (CSC)
Commission Electrotechnique Internationale
3, rue de Varembé
1211 GENÈVE 20
Suisse

Q1 Veuillez ne mentionner qu'**UNE SEULE NORME** et indiquer son numéro exact: (*ex. 60601-1-1)*

.....

Q2 En tant qu'acheteur de cette norme, quelle est votre fonction?
(cochez tout ce qui convient)
Je suis le/un:

agent d'un service d'achat ❑
bibliothécaire ❑
chercheur ❑
ingénieur concepteur ❑
ingénieur sécurité ❑
ingénieur d'essais ❑
spécialiste en marketing ❑
autre(s).....

Q3 Je travaille:
(cochez tout ce qui convient)

dans l'industrie ❑
comme consultant ❑
pour un gouvernement ❑
pour un organisme d'essais/ certification ❑
dans un service public ❑
dans l'enseignement ❑
comme militaire ❑
autre(s).....

Q4 Cette norme sera utilisée pour/comme
(cochez tout ce qui convient)

ouvrage de référence ❑
une recherche de produit ❑
une étude/développement de produit ❑
des spécifications ❑
des soumissions ❑
une évaluation de la qualité ❑
une certification ❑
une documentation technique ❑
une thèse ❑
la fabrication ❑
autre(s).....

Q5 Cette norme répond-elle à vos besoins:
(une seule réponse)

pas du tout ❑
à peu près ❑
assez bien ❑
parfaitement ❑

Q6 Si vous avez répondu PAS DU TOUT à Q5, c'est pour la/les raison(s) suivantes:
(cochez tout ce qui convient)

la norme a besoin d'être révisée ❑
la norme est incomplète ❑
la norme est trop théorique ❑
la norme est trop superficielle ❑
le titre est équivoque ❑
je n'ai pas fait le bon choix ❑
autre(s) .....

Q7 Veuillez évaluer chacun des critères ci-dessous en utilisant les chiffres
(1) inacceptable,
(2) au-dessous de la moyenne,
(3) moyen,
(4) au-dessus de la moyenne,
(5) exceptionnel,
(6) sans objet

publication en temps opportun .....
qualité de la rédaction.....
contenu technique .....
disposition logique du contenu .....
tableaux, diagrammes, graphiques, figures.....
autre(s) .....

Q8 Je lis/utilise: *(une seule réponse)*

uniquement le texte français ❑
uniquement le texte anglais ❑
les textes anglais et français ❑

Q9 Veuillez nous faire part de vos observations éventuelles sur la CEI:

.....
.....
.....
.....
.....
.....

ISBN 2-8318-8625-2

ICS 03.120.01; 03.120.30; 21.020

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND