NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
61078

Deuxième édition
Second edition
2006-01

Techniques d'analyse pour la sûreté de fonctionnement – Bloc-diagramme de fiabilité et méthodes booléennes

Analysis techniques for dependability – Reliability block diagram and boolean methods

Numéro de référence
Reference number
CEI/IEC 61078:2006

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
61078

Deuxième édition
Second edition
2006-01

Techniques d'analyse pour la sûreté de fonctionnement – Bloc-diagramme de fiabilité et méthodes booléennes

Analysis techniques for dependability – Reliability block diagram and boolean methods

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 W

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

SOMMAIRE

CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

TECHNIQUES D'ANALYSE POUR LA SÛRETÉ DE FONCTIONNEMENT – BLOC-DIAGRAMME DE FIABILITÉ ET MÉTHODES BOOLÉENNES

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 61078 a été établie par le comité d'études 56 de la CEI: Sûreté de fonctionnement.

Cette seconde édition annule et remplace la première édition publiée en 1991. Elle constitue une révision technique complète. La principale modification par rapport à la précédente édition porte sur l'ajout d'un article concernant les méthodes disjointes booléennes (Annexe B).

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
56/1071/FDIS	56/1089/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 2.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ANALYSIS TECHNIQUES FOR DEPENDABILITY – RELIABILITY BLOCK DIAGRAM AND BOOLEAN METHODS

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardisation comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardisation 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 61078 has been prepared by IEC technical committee 56: Dependability.

This second edition cancels and replaces the first edition, published in 1991, and constitutes a full technical revision. The major change with respect to the previous edition is that an additional clause on Boolean disjointing methods (Annex B) has been added.

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

FDIS	Report on voting
56/1071/FDIS	56/1089/RVD

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

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

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 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

Différentes méthodes analytiques de sûreté de fonctionnement sont disponibles, dont le Bloc-diagramme de fiabilité (BDF) fait partie. Avant de commencer un travail sur le BDF, il convient que l'analyste examine l'objet de chaque méthode et de leur pertinence individuelle ou combinée dans l'évaluation de la fiabilité et de la disponibilité d'un système ou d'un composant donné. Il est recommandé que les résultats pouvant être obtenus par chaque méthode soient pris en considération, ainsi que les données exigées pour mener l'analyse, la complexité de celle-ci, et les autres facteurs identifiés dans cette norme.

Un Bloc-diagramme de fiabilité (BDF) est une représentation picturale de la performance de fiabilité d'un système. Il montre la connexion logique de composants nécessaires au fonctionnement réussi du système (ci-après appelé «état opérationnel du système»).

INTRODUCTION

Different analytical methods of dependability analysis are available, of which the reliability block diagram (RBD) is one. The purpose of each method and their individual or combined applicability in evaluating the reliability and availability of a given system or component should be examined by the analyst prior to starting work on the RBD. Consideration should also be given to the results obtainable from each method, data required to perform the analysis, complexity of analysis and other factors identified in this standard.

A reliability block diagram (RBD) is a pictorial representation of a system's reliability performance. It shows the logical connection of (functioning) components needed for successful operation of the system (hereafter referred to as “system success”).

TECHNIQUES D'ANALYSE POUR LA SÛRETÉ DE FONCTIONNEMENT – BLOC-DIAGRAMME DE FIABILITÉ ET MÉTHODES BOOLÉENNES

1 Domaine d'application

La présente Norme internationale décrit les procédures de modélisation de la sûreté de fonctionnement d'un système et l'utilisation du modèle pour calculer la fiabilité et la disponibilité.

La technique de modélisation BDF est destinée à être appliquée principalement aux systèmes sans réparation et où l'ordre d'apparition des défaillances n'a pas d'importance. Pour les systèmes où l'ordre des défaillances est à prendre en compte, ou lorsque des réparations sont effectuées, d'autres techniques de modélisation, telle que l'analyse de Markov conviennent mieux.

Il convient de noter que, bien que le mot «réparer» soit fréquemment utilisé dans cette norme, le mot «restaurer» est également applicable. Il est à noter également que les mots «entité/dispositif» et «bloc» sont beaucoup utilisés dans cette norme: le plus souvent de façon interchangeable.

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 61025, *Analyse par arbre de panne (AAP)*

ISO 3534-1:1993, *Statistiques – Vocabulaire et symboles – Partie 1: Probabilité et termes statistiques généraux*

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions fournis dans la CEI 60050-191 et l'ISO 3534-1 s'appliquent.

ANALYSIS TECHNIQUES FOR DEPENDABILITY – RELIABILITY BLOCK DIAGRAM AND BOOLEAN METHODS

1 Scope

This International Standard describes procedures for modelling the dependability of a system and for using the model in order to calculate reliability and availability measures.

The RBD modelling technique is intended to be applied primarily to systems without repair and where the order in which failures occur does not matter. For systems where the order of failures is to be taken into account or where repairs are to be carried out, other modelling techniques, such as Markov analysis, are more suitable.

It should be noted that although the word “repair” is frequently used in this standard, the word “restore” is equally applicable. Note also that the words “item” and “block” are used extensively throughout this standard: in most instances interchangeably.

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*

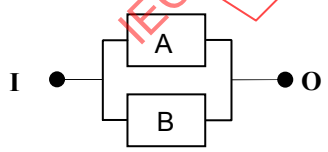
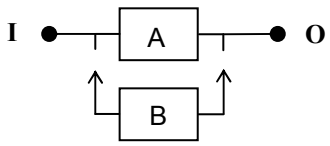
IEC 61025, *Fault tree analysis (FTA)*

ISO 3534-1:1993, *Statistics – Vocabulary and symbols – Part 1: Probability and general statistical terms*

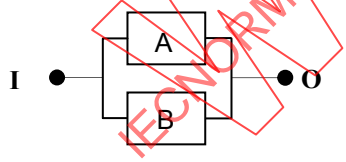
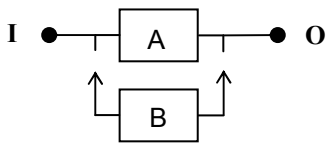
3 Terms and definitions

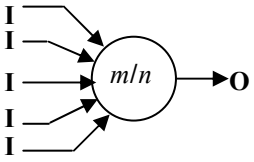
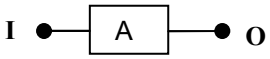
For the purposes of this document, the terms and definitions given in IEC 60050-191 and ISO 3534-1 apply.

4 Symboles et termes abrégés

Symbole/Abbréviation	Signification
$A, B, C, \ldots$	Lorsqu'ils sont utilisés dans des expressions booléennes, ces symboles indiquent que les entités/dispositifs $A, B, C, \ldots$ sont en état haut (fonctionnement)
$\overline{A}, \overline{B}, \overline{C}, \cdots$	Lorsqu'ils sont utilisés dans des expressions booléennes, ces symboles indiquent que les entités/dispositifs $A, B, C, \ldots$ sont en état bas (défaillance)
F_S	Probabilité de défaillance du système
$f_A(t)$	Fonction de densité de probabilité du bloc A. Le terme «bloc» est utilisé pour désigner un groupe de un ou plusieurs composants
Pr(SS|X en panne)	Probabilité conditionnelle de succès du système avec le dispositif/entité X en panne
R , $R(t)$, $R_S(t)$	Fiabilité [probabilité qu'un dispositif/entité puisse remplir une fonction exigée dans des conditions et durant un intervalle de temps donnés$(0,t)$]
R_A , R_B , ...	Fiabilité des blocs A, B, ...
R_S	Fiabilité du système
R_{SW}	Fiabilité des mécanismes de commutation et de détection
SF	Défaillance du système (utilisé dans les expressions booléennes)
SS	État opérationnel (utilisé dans les expressions booléennes)
t	Durée de la mission ou de la période d'intérêt
$\lambda_A, \lambda_B, \lambda_C$	Taux de défaillance (constant) des blocs A, B et C
λ_{Bd}	Taux de défaillance latent du bloc B
μ_A, μ_B, μ_C	Taux de réparation (constant) des blocs A, B et C
$\binom{n}{r}$	Nombre de possibilités de sélectionner les dispositifs/entités r des dispositifs/entités n
0, 1	Ces symboles sont utilisés dans les tables de vérité pour indiquer les états bas (défaillants) et les états hauts (fonctionnement) et s'appliquent au dispositif/entité, quel que soit l'en-tête de colonne
$\cap$	Les symboles booléens pour ET logique, ex. A $\cap$ B, A . B (intersection)
$\cup$	Les symboles booléens pour OU logique, ex. A $\cup$ B, A+B (union)
	Redondance (parallèle) active
	Redondance en attente

4 Symbols and abbreviated terms

Symbol/Abbreviation	Meaning
$A, B, C, \ldots$	When used in Boolean expressions, these symbols indicate that items $A, B, C, \ldots$ are in up states
$\overline{A}, \overline{B}, \overline{C}, \cdots$	When used in Boolean expressions, these symbols indicate that items $A, B, C, \ldots$ are in down states
F_S	Probability of system failure
$f_A(t)$	Probability density function of block A. The term "block" is used to denote a group of one or more components
Pr(SS|X failed)	Conditional probability of system success, given that item X is failed
R , $R(t)$, $R_S(t)$	Reliability [probability that an item can perform a required function under given conditions for a given time interval $(0,t)$]
R_A , R_B , ...	Reliability of blocks A, B, ...
R_S	System reliability
R_{SW}	Reliability of switching and sensing mechanism
SF	System failure (used in the Boolean expressions)
SS	System success (used in the Boolean expressions)
t	Mission time or time period of interest
$\lambda_A, \lambda_B, \lambda_C$	Failure rate (constant) of blocks A, B and C
λ_{Bd}	Dormant failure rate of block B
μ_A, μ_B, μ_C	Repair rates (constant) of blocks A, B and C
$\binom{n}{r}$	Number of ways of selecting r items from n items
0, 1	These symbols are used in truth tables to denote down and up states and apply to whichever item is the column heading
$\cap$	Boolean symbols denoting AND logic, e.g. A $\cap$ B, A.B (intersection)
$\cup$	Boolean symbols denoting OR logic, e.g. A $\cup$ B, A+B (union)
	Active (parallel) redundancy
	Standby redundancy

Symbole/Abbréviation	Signification
	*m*/*n* est un symbole utilisé pour montrer *m*- parmi -*n* dispositifs/entités dans une configuration redondante active
I O	indique une entrée indique une sortie Ces indications sont utilisées pour des raisons pratiques. Elles ne sont pas obligatoires, mais peuvent être utiles lorsque les connexions ont une signification directionnelle
	Groupement d'équipements, composants, dispositifs/entités ou éléments d'autres systèmes

5 Hypothèses et limitations

5.1 Indépendance des événements

Une des hypothèses les plus fondamentales sur laquelle les procédures décrites dans cette norme se basent, est que les composants (ou les blocs qui les représentent) ne peuvent exister que sous deux états: fonctionnement (état «haut») ou défaillant (état «bas»).

Une autre hypothèse importante est que la défaillance (ou réparation) d'un bloc ne doit affecter la probabilité de défaillance (ou réparation de) d'AUCUN bloc dans le système en modélisation. Cela implique qu'il convient, dans les faits, d'avoir suffisamment de ressources de réparation pour réparer ces blocs et lorsque deux personnes ou plus sont en train de réparer un bloc en même temps, aucune ne doit gêner l'autre. Ainsi, les défaillances et réparations des blocs individuels sont statistiquement considérées comme des événements indépendants.

5.2 Evénements séquentiels

Les BDFs ne conviennent pas pour les modélisations dépendant d'un ordre ou d'événements dépendant du temps. Dans de tels cas, il convient d'utiliser d'autres méthodes telles que l'analyse de Markov ou les réseaux de Petri.

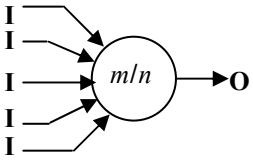
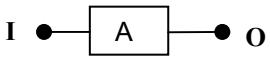
5.3 Distribution des temps avant défaillance

Tant que les hypothèses listées en 5.1 sont valables, la seule restriction est liée à la complexité mathématique de la distribution, qui peut être utilisée pour décrire les temps de défaillance ou de réparation.

6 Etablissement des définitions des états opérationnel/défaillant du système

6.1 Considérations générales

Une condition préalable à la construction des modèles de fiabilité d'un système est une bonne compréhension des manières dont le système peut fonctionner. Les systèmes nécessitent souvent plus d'une définition d'état opérationnel/défaillant. Il convient de les définir et de les lister. Un schéma BDF peut être établi à différents niveaux: niveau du système, niveau du sous-système (module) ou niveau de l'assemblage. Lorsqu'un BDF est réalisé pour d'autres analyses (par exemple des analyses AMDE), un niveau approprié à de telles analyses doit être choisi.

Symbol/Abbreviation	Meaning
	*m*/*n* is symbol used to show *m*-out-of-*n* items needed for system success in an active redundant configuration
I O	indicates input indicates output Such indications are used for convenience. They are not mandatory, but may be useful where connections have a directional significance
	Grouping of equipment, components, units or other system elements

5 Assumptions and limitations

5.1 Independence of events

One of the most fundamental assumptions on which the procedures described in this standard are based, is the assumption that components (or blocks representing them) can exist in only two states: working ("up" state) or failed ("down" state).

Another important assumption is that failure (or repair) of any block must not affect the probability of failure of (or repair to) ANY other block within the system being modelled. This implies that there should be available, in effect, sufficient repair resources to service those blocks needing repair and that when two or more persons are repairing a particular block at the same time, neither gets in the other's way. Thus failures of and repairs to individual blocks are considered to be statistically independent events.

5.2 Sequential events

RBDs are not suitable for modelling order-dependent or time-dependent events. In such instances, other methods such as Markov analysis or Petri nets should be used.

5.3 Distribution of times to failure

Provided the assumptions noted in 5.1 are valid, there is no restriction, other than mathematical tractability, on the distribution that may be used to describe the times to failure or repair.

6 Establishment of system success/failure definitions

6.1 General considerations

A prerequisite for constructing system reliability models is a sound understanding of the ways in which the system can operate. Systems often require more than one success/failure definition. These should be defined and listed. An RBD diagram can be made on different levels: system level, sub-system (module) level or assembly level. When an RBD is made for further analysis (for example for FMEA analysis), a level suitable for such analysis has to be chosen.

De plus, il convient de statuer clairement sur

– les fonctions à effectuer,
– les paramètres de performance et les limites autorisées pour de tels paramètres,
– les conditions d'environnement et de fonctionnement.

Des techniques d'analyse qualitatives diverses peuvent être employées dans la construction d'un BDF. En conséquence, les définitions du système opérationnel/défaillant doivent être établies. Pour chaque définition de système opérationnel/défaillant, l'étape suivante est la division du système en blocs logiques appropriés aux besoins de l'analyse de fiabilité. Des blocs particuliers peuvent représenter des sous-structures de système, qui à leur tour peuvent être représentées par d'autres BDF (réduction du système – voir 8.4).

Pour l'évaluation quantitative d'un BDF, diverses méthodes sont disponibles. Suivant le type de structure, des techniques booléennes simples (voir 8.1.3) et/ou des analyses par coupe et/ou par cheminement peuvent être utilisées. Pour une définition des coupes, voir la CEI 61025 (AAP (FTA en anglais)). Des calculs peuvent être effectués en utilisant des méthodes de fiabilité/disponibilité de composants et des méthodes analytiques ou des simulations Monte Carlo. Un avantage de la simulation Monte Carlo est que l'événement dans le BDF n'a pas besoin d'être combiné analytiquement puisque la simulation elle-même prend en compte la défaillance ou le fonctionnement de chaque bloc (voir 8.1).

Puisque le bloc-diagramme de fiabilité décrit les relations logiques nécessaires à la fonction du système, il ne représente pas nécessairement la façon dont le matériel est physiquement connecté bien qu'un RDB suive généralement, autant que possible, les liaisons physiques du système.

6.2 Considérations détaillées

6.2.1 Fonctionnement du système

Il est possible d'utiliser un système suivant plus d'un mode de fonctionnement. Si des systèmes séparés étaient utilisés pour chacun des modes de fonctionnement, il conviendrait de traiter chaque mode indépendamment des autres, et d'utiliser, en conséquence, des modèles de fiabilité séparés. Quand le même système est utilisé pour réaliser toutes ces fonctions, il convient d'utiliser des schémas séparés pour chaque type d'opération. Une formulation claire de ce qu'est l'état opérationnel pour chaque aspect du fonctionnement du système constitue une condition préalable.

6.2.2 Conditions d'environnement

Il convient de joindre aux spécifications de performance du système une description des conditions environnementales sous lesquelles le système conçu doit fonctionner. Il convient d'inclure également une description de toutes les conditions auxquelles le système sera soumis durant le transport, le stockage et l'utilisation.

Un élément d'équipement est souvent utilisé dans plus d'un environnement; par exemple, sur un bateau, dans un avion ou au sol. Le cas échéant, les évaluations de fiabilité peuvent être menées en utilisant le même bloc-diagramme de fiabilité à chaque fois mais en utilisant le taux de défaillance approprié à chaque environnement.

6.2.3 Cycles de utilisation

Il convient d'établir la relation entre le temps calendaire, la durée de fonctionnement et le nombre de cycles marche/arrêt. Si on peut supposer que le processus de commutation marche/arrêt ne favorise pas les défaillances, et que le taux de défaillance pour l'équipement stocké est négligeable, alors la durée réelle de travail peut être considérée isolément.

In addition, there should be clear statements concerning

– functions to be performed,
– performance parameters and permissible limits on such parameters,
– environmental and operating conditions.

Various qualitative analysis techniques may be employed in the construction of an RBD. Therefore the system's success/failure definition has to be established. For each system success/failure definition the next step is to divide the system into logical blocks appropriate to the purpose of the reliability analysis. Particular blocks may represent system substructures, which in turn may be represented by other RBDs (system reduction – see 8.4).

For the quantitative evaluation of an RBD, various methods are available. Depending on the type of structure, simple Boolean techniques (see 8.1.3) and/or path and cut set analyses may be employed. For a definition of cut set see IEC 61025 (FTA). Calculations may be made using basic component reliability/availability methods and analytical methods or Monte Carlo simulation. An advantage with Monte Carlo simulation is that the events in the RBD do not have to be combined analytically since the simulation itself takes into account whether each block is failed or functional (see 8.1).

Since the reliability block diagram describes the logical relations needed for system function, the block diagram does not necessarily represent the way the hardware is physically connected, although an RBD generally follows, as far as possible, the physical system connections.

6.2 Detailed considerations

6.2.1 System operation

It may be possible to use a system in more than one functional mode. If separate systems were used for each mode, such modes should be treated independently of other modes, and separate reliability models should be used accordingly. When the same system is used to perform all these functions, then separate diagrams should be used for each type of operation. Clear statements of what constitutes system success/failure for each aspect of system operation, is a prerequisite.

6.2.2 Environmental conditions

The system performance specifications should be accompanied by a description of the environmental conditions under which the system is designed to operate. Also included should be a description of all the conditions to which the system will be subjected during transportation, storage and use.

A particular piece of equipment is often used in more than one environment; for example, on board ship, in an aircraft or on the ground. When this is so, reliability evaluations may be carried out using the same reliability block diagram each time but using the appropriate failure rates for each environment.

6.2.3 Duty cycles

The relationship between calendar time, operating time and on/off cycles should be established. If it can be assumed that the process of switching equipment on and off does not in itself promote failures, and that the failure rate of equipment in storage is negligible, then only the actual working time of the equipment need be considered.

Cependant, dans certains cas, le processus de commutation marche/arrêt est la cause principale de défaillance de l'équipement, ou l'équipement peut avoir un taux de défaillance plus élevé en stockage qu'en fonctionnement (par exemple, humidité et corrosion). Dans les cas complexes où seulement certaines parties du système sont commutées marche/arrêt, les techniques de modélisation autres que les bloc-diagramme de fiabilité (par exemple analyse de Markov) peuvent être plus adaptées.

7 Modèles élémentaires

7.1 Développement du modèle

La première étape est la sélection d'une définition de l'état opérationnel/défaillant du système. Si plus d'une définition est impliquée, un bloc-diagramme de fiabilité peut être nécessaire pour chacune. L'étape suivante est la division du système en blocs pour refléter le comportement logique de façon que chaque bloc soit indépendant des autres, statistiquement, et aussi grand que possible. En même temps, il convient que chaque bloc ne contienne (de préférence) aucune redondance.

En pratique, il peut être nécessaire de réitérer les tentatives de construction d'un bloc-diagramme de fiabilité (en gardant toujours en mémoire les étapes ci-dessus) avant qu'un diagramme adapté soit au point.

L'étape suivante consiste à se référer à la définition du système opérationnel/défaillant et à construire un schéma qui connecte les blocs pour former un «cheminement réussi» Comme indiqué dans le schéma qui suit, les divers cheminements réussis, entre les points d'entrée et de sortie du schéma, traversent ces combinaisons de blocs qui doivent fonctionner pour que le système fonctionne. S'il faut que tous les blocs fonctionnent pour que le système fonctionne, alors le schéma bloc-diagramme de fiabilité correspondant sera un schéma dans lequel tous les blocs sont reliés en séries, tel qu'illustré à la Figure 1.

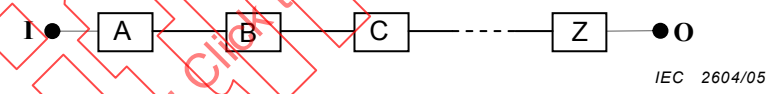


Figure 1 – Bloc-diagramme de fiabilité en série

Dans ce schéma «I» est le point d'entrée, «O» le point de sortie et A, B, C, … Z sont les blocs qui ensemble constituent le système. Les schémas de ce type sont connus comme bloc-diagramme de fiabilité «série» ou «modèles en série».

Un type différent de bloc-diagramme de fiabilité est nécessaire lorsque la défaillance de l'un des composants ou «bloc» seul n'affecte pas la performance du système dans le cadre de la définition succès/défaillance du système. Par exemple, dans le cas ci-dessous la liaison entière est dupliquée (redondante), ainsi le diagramme est tel qu'illustré à la Figure 2. En variante, si chaque bloc dans la liaison est dupliqué, le diagramme est tel qu'illustré par la Figure 3. Les schémas de ce type sont connus comme bloc-diagramme de fiabilité «parallèles» ou «modèle en parallèle». Noter que les termes «dupliqué», «redondant» et «parallèle» sont un sens très proche et sont souvent utilisés indifféremment.

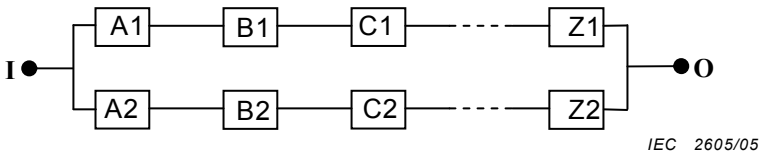


Figure 2 – Bloc-diagramme de fiabilité en séries dupliquées (ou parallèles)

However, in some instances, the process of switching on and off is in itself the prime cause of equipment failure, and equipment may have a higher failure rate in storage than when working (e.g. moisture and corrosion). In complex cases where only parts of the system are switched on and off, modelling techniques other than reliability block diagrams (e.g. Markov analysis) may be more suitable.

7 Elementary models

7.1 Developing the model

The first step is to select a system success/failure definition. If more than one definition is involved, a separate reliability block diagram may be required for each. The next step is to divide the system into blocks to reflect the logical behaviour so that each block is statistically independent of the others, and is as large as possible. At the same time each block should contain (preferably) no redundancy.

In practice it may be necessary to make repeated attempts at constructing the reliability block diagram (each time bearing in mind the steps referred to above) before a suitable block diagram is finalized.

The next step is to refer to the system success/failure definition and construct a diagram that connects the blocks to form a "success path". As indicated in the diagrams that follow, the various success paths, between the input and output ports of the diagram, pass through those combinations of blocks that need to function in order that the system functions. If all the blocks are required to function for the system to function, then the corresponding reliability block diagram will be one in which all the blocks are joined in series as illustrated in Figure 1.

Figure 1 – Series reliability block diagram

In this diagram "I" is the input port, "O" the output port and A, B, C, ... Z are the blocks which together constitute the system. Diagrams of this type are known as "series" reliability block diagrams or "series models".

A different type of reliability block diagram is needed when failure of one component or "block" alone, does not affect system performance as far as the system success/failure definition is concerned. For example, if in the above instance the entire link is duplicated (made redundant), then the block diagram is as illustrated by Figure 2. Alternatively, if each block within the link is duplicated, the block diagram is as illustrated by Figure 3. Diagrams of this type are known as "parallel" reliability block diagrams or "parallel models". Note that the terms "duplicated", "redundant" and "parallel" are very similar in meaning and are often used interchangeably.

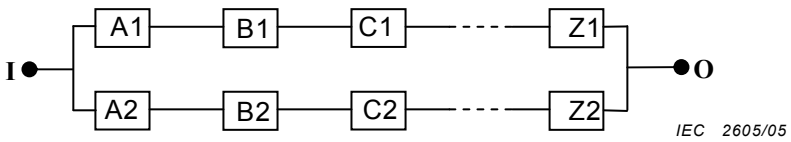


Figure 2 – Duplicated (or parallel) series reliability block diagram

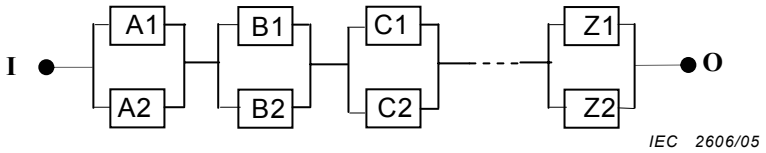


Figure 3 – Bloc-diagramme de fiabilité dupliqué (ou parallèle) en série

Les bloc-diagramme de fiabilité utilisés pour la modélisation de fiabilité du système sont souvent une combinaison de schémas séries et de schémas parallèles. Un tel schéma pourrait apparaître si l'on considérait un exemple consistant en une liaison de communication dupliquée comprenant trois répéteurs A, B, et C, et un bloc de puissance commun (D). Le schéma résultant deviendrait tel qu'illustré par les Figures 4 et 5.

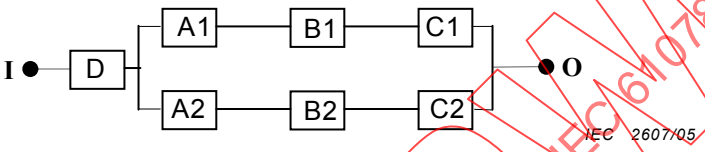


Figure 4 – Bloc-diagramme de fiabilité mixte avec redondance

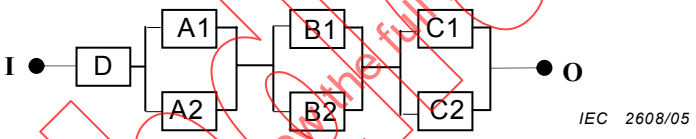


Figure 5 – Autre type de bloc-diagramme de fiabilité mixte avec redondance

Du fait de l'indépendance statistique indiquée précédemment, la défaillance de tout bloc ne doit pas conduire à une modification de la probabilité de défaillance de tout autre bloc dans le système. En particulier, la défaillance d'un bloc redondant ne doit pas affecter les alimentations du système ou les sources de signal.

Fréquemment, il faut modéliser des systèmes pour lesquels la définition de l'état opérationnel est telle qu'elle nécessite m éléments ou plus parmi n connectés en parallèle pour l'état opérationnel du système. Le bloc-diagramme de fiabilité prend alors la forme de la Figure 6 ou de la Figure 7.

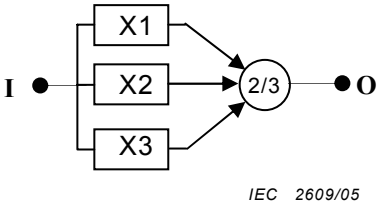


Figure 6 – Redondance 2/3

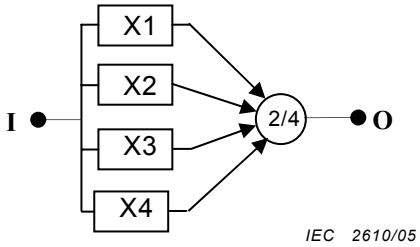


Figure 7 – Redondance 2/4

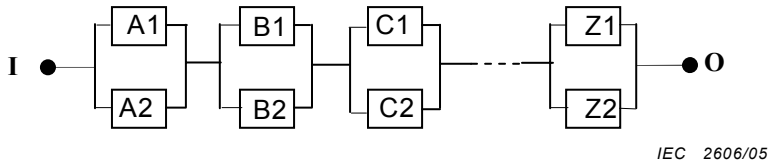


Figure 3 – Series duplicated (or parallel) reliability block diagram

Reliability block diagrams used for modelling system reliability are often more complicated mixtures of series and parallel diagrams. Such a diagram would arise if an example were to be considered consisting of a duplicated communication link comprising three repeaters A, B and C, and a common power supply block (D). The resulting diagram then takes the form of Figures 4 and 5.

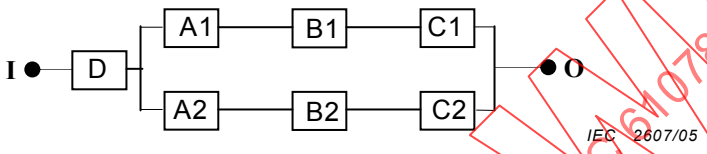


Figure 4 – Mixed redundancy reliability block diagram

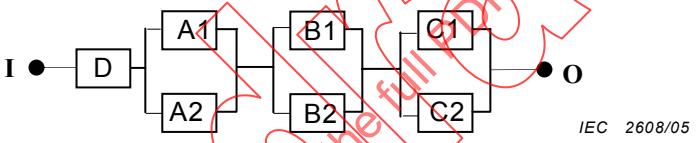


Figure 5 – Another type of mixed redundancy reliability block diagram

On account of the statistical independence stated above, failure of any block shall not give rise to a change in the probability of failure of any other block within the system. In particular, failure of a redundant block shall not affect system power supplies or signal sources.

The need frequently arises to model systems where the success definition is that m or more out of n items connected in parallel are required for system success. The reliability block diagram then takes the form of Figure 6 or Figure 7.

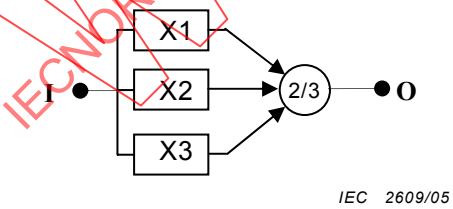


Figure 6 – 2/3 redundancy

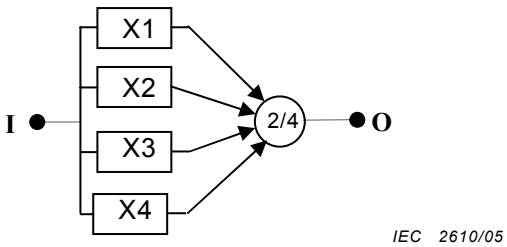


Figure 7 – 2/4 redundancy

Ainsi, dans la Figure 6, la défaillance d'un dispositif est tolérée mais la défaillance de deux ou plus ne l'est pas.

La plupart des bloc-diagramme de fiabilité sont facilement compris et les conditions pour l'état opérationnel du système sont évidents. Cependant, les diagrammes ne peuvent pas tous être simplifiés à des combinaisons de systèmes parallèles ou de série. Le schéma de la Figure 8 en est un exemple.

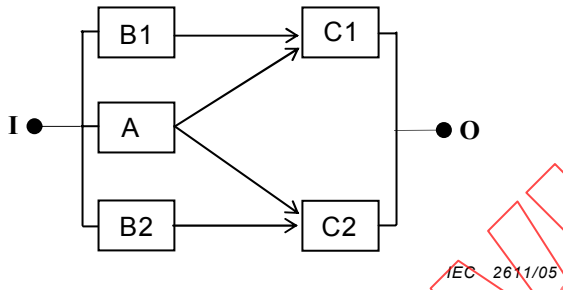


Figure 8 – Bloc diagramme non représenté facilement par un arrangement de blocs série/parallèle

Là encore, le schéma est évident. L'état opérationnel du système est atteint si les dispositifs B1 et C1 fonctionnent tous les deux, ou les dispositifs A et C1, ou A et C2, ou enfin B2 et C2. La Figure 8 pourrait représenter l'alimentation en carburant de moteurs d'un avion léger. Le dispositif B1 représente l'alimentation à l'accès du moteur (C1), le dispositif B2 représente l'alimentation du moteur à tribord (C2), et le dispositif A représente l'alimentation de secours des deux moteurs. La définition de système opérationnel/défaillant est que les deux moteurs doivent tomber en panne avant que l'avion lui-même soit défaillant.

A noter que dans tous les schémas ci-dessus, aucun bloc ne paraît plus d'une fois dans un schéma donné. Les procédures pour développer l'expression de fiabilité pour les schémas de ce type sont présentées à l'Article 8.

7.2 Evaluation du modèle

La fiabilité d'un système $R_S(t)$ est la probabilité qu'un système puisse réaliser une fonction requise sans défaillance sous des conditions spécifiées durant un intervalle de temps défini (0, t). En général, cela est défini par la relation:

$$R_S(t) = \exp\left(-\int_0^t \lambda(u)du\right)$$

où $\lambda(u)$ est le taux de défaillance du système à $t = u$, u étant une variable.

Dans ce qui suit, $R_S(t)$ sera écrit R_S pour simplifier. La probabilité de défaillance du système, F_S, est donnée par:

$$F_S = 1 - R_S$$

7.2.1 Modèles séries

Pour les systèmes tels qu'illustrés par la Figure 1, la fiabilité du système R_S est donnée par la simple équation:

$$R_S = R_A \cdot R_B \cdot R_C \cdots R_Z \qquad (1)$$

c'est-à-dire en multipliant entre elles les fiabilités de tous les blocs constituant le système.

Thus, in Figure 6, the failure of one item is tolerated but failure of two or more items is not.

Most reliability block diagrams are easily understood and the conditions for system success are evident. Not all block diagrams, however, can be simplified to combinations of series or parallel systems. The diagram in Figure 8 is an example.

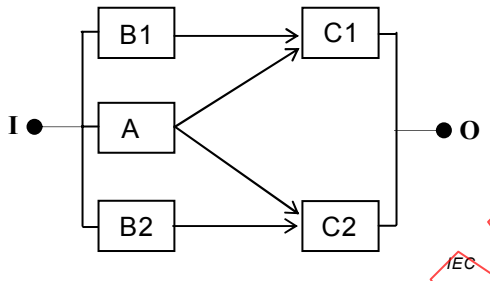


Figure 8 – Diagram not easily represented by series/parallel arrangement of blocks

Again, the diagram is self-explanatory. System success is achieved if items B1 and C1 are both working, or items A and C1, or A and C2, or finally B2 and C2. Figure 8 could represent the fuel supply to engines of a light aircraft. Item B1 represents the supply to the port engine (C1), item B2 represents the supply to the starboard engine (C2), and item A represents a backup supply to both engines. The system success/failure definition is that both engines have to fail before the aircraft fails.

It should be noted that in all the above diagrams, no block appears more than once in a given diagram. The procedures for developing the reliability expression for diagrams of this type are outlined in Clause 8.

7.2 Evaluating the model

The reliability of a system, $R_S(t)$, is the probability that a system can perform a required function without failure under stated conditions for a given time interval (0, t). In general, this is defined by the relationship:

$$R_S(t) = \exp\left(-\int_0^t \lambda(u)\,du\right)$$

where $\lambda(u)$ denotes the system failure rate at $t = u$, u being a dummy variable.

In what follows, $R_S(t)$ will be written for simplicity as R_S. The probability of system failure, F_S, is given by:

$$F_S = 1 - R_S$$

7.2.1 Series models

For systems such as those illustrated by Figure 1, the system reliability R_S is given by the simple equation:

$$R_S = R_A \cdot R_B \cdot R_C \cdots R_Z \qquad (1)$$

i.e. by multiplying together the reliabilities of all the blocks constituting the system.

7.2.2 Modèles parallèles

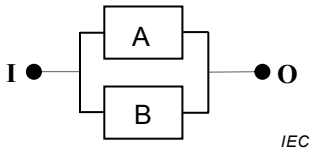


Figure 9 – Arrangement parallèle de blocs

Pour les systèmes du type illustré par la Figure 9, la probabilité de défaillance du système F_S est donné par:

$$F_S = F_A \cdot F_B$$

D'où la fiabilité du système (R_S) donnée par:

$$R_S = R_A + R_B - R_A \cdot R_B \quad (2)$$

On peut combiner les Formules (1) et (2). Ainsi, si on a un système tel que décrit par la Figure 2, mais avec seulement trois dispositifs dans chaque branche, la fiabilité du système est:

$$R_S = R_{A1} \cdot R_{B1} \cdot R_{C1} + R_{A2} \cdot R_{B2} \cdot R_{C2} - R_{A1} \cdot R_{B1} \cdot R_{C1} \cdot R_{A2} \cdot R_{B2} \cdot R_{C2} \quad (3)$$

De façon similaire, pour la Figure 3, on a:

$$R_S = (R_{A1} + R_{A2} - R_{A1} \cdot R_{A2}) \cdot (R_{B1} + R_{B2} - R_{B1} \cdot R_{B2}) \cdot (R_{C1} + R_{C2} - R_{C1} \cdot R_{C2}) \quad (4)$$

En général, $R_S = 1 - \prod_{i=1}^{n} (1 - R_i)$

Pour la Figure 4 et la Figure 5, les expressions de fiabilité du système sont obtenues simplement en multipliant les équations (3) et (4) par R_D.

7.2.3 *m* de *n* modèles (dispositifs identiques)

L'expression de fiabilité du système correspondant aux Figures 6 et 7 est un peu plus compliquée que les expressions ci-dessus. En général, si la fiabilité d'un système peut être représentée par n dispositifs identiques en parallèle où m dispositifs parmi n sont requis pour l'état opérationnel du système, alors la fiabilité du système R_S est donnée par:

$$R_S = \sum_{r=0}^{n-m} \binom{n}{r} \cdot R^{n-r} \cdot (1-R)^r \quad (5)$$

Ainsi la fiabilité du système illustré par la Figure 6 est donnée par:

$$R_S = R^3 + 3 \cdot R^2 \cdot (1-R) = 3 \cdot R^2 - 2 \cdot R^3 \quad (6)$$

où R est la fiabilité des dispositifs individuels.

De façon similaire pour la Figure 7:

$$R_S = R^4 + 4 \cdot R^3 \cdot (1-R) + 6 \cdot R^2 \cdot (1-R)^2 = 3 \cdot R^4 - 8 \cdot R^3 + 6 \cdot R^2 \quad (7)$$

7.2.2 Parallel models

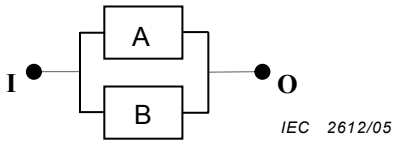


Figure 9 – Parallel arrangement of blocks

For systems of the type illustrated by Figure 9, the system probability of failure (F_S) is given by:

$$F_S = F_A \cdot F_B$$

Hence system reliability (R_S) is given by:

$$R_S = R_A + R_B - R_A \cdot R_B \quad (2)$$

Formulæ (1) and (2) can be combined. Thus, if a system exists as depicted by Figure 2, but with only three items in each branch, the system reliability is:

$$R_S = R_{A1} \cdot R_{B1} \cdot R_{C1} + R_{A2} \cdot R_{B2} \cdot R_{C2} - R_{A1} \cdot R_{B1} \cdot R_{C1} \cdot R_{A2} \cdot R_{B2} \cdot R_{C2} \quad (3)$$

Similarly, for Figure 3, the following applies:

$$R_S = (R_{A1} + R_{A2} - R_{A1} \cdot R_{A2}) \cdot (R_{B1} + R_{B2} - R_{B1} \cdot R_{B2}) \cdot (R_{C1} + R_{C2} - R_{C1} \cdot R_{C2}) \quad (4)$$

In general, $R_S = 1 - \prod_{i=1}^{n} (1 - R_i)$

For Figures 4 and 5, the system reliability equations are obtained simply by multiplying Equations (3) and (4) by R_D.

7.2.3 *m* out of *n* models (identical items)

The system reliability equation corresponding to Figures 6 and 7 is a little more complicated than those above. In general, if the reliability of a system can be represented by n identical items in parallel where m items out of n are required for system success, then the system reliability R_S is given by:

$$R_S = \sum_{r=0}^{n-m} \binom{n}{r} \cdot R^{n-r} \cdot (1 - R)^r \quad (5)$$

Thus the reliability of the system illustrated by Figure 6 is given by:

$$R_S = R^3 + 3 \cdot R^2 \cdot (1 - R) = 3 \cdot R^2 - 2 \cdot R^3 \quad (6)$$

where R is the reliability of the individual items.

Similarly for Figure 7:

$$R_S = R^4 + 4 \cdot R^3 \cdot (1 - R) + 6 \cdot R^2 \cdot (1 - R)^2 = 3 \cdot R^4 - 8 \cdot R^3 + 6 \cdot R^2 \quad (7)$$

Pour le cas particulier où $m = n - 1$, $R_S = n \cdot R^n - m \cdot R^n$

Si les n dispositifs ne sont pas identiques, l'utilisation d'une procédure plus générale est recommandée (voir 8.3)

7.2.4 Modèles de redondance en attente

Une autre forme fréquemment utilisée de redondance est la redondance en attente (voir premier alinéa de l'Annexe A). Sous sa forme la plus élémentaire, l'arrangement physique des dispositifs est représenté par le schéma de la Figure 10.

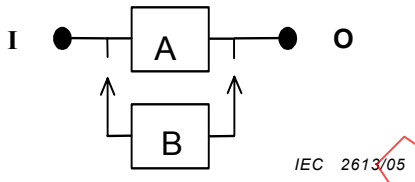


Figure 10 – Redondance en attente

Dans cette figure, le dispositif A est le dispositif actif en marche, et le dispositif B est en attente d'être connecté pour remplacer A lorsque ce dernier tombera en panne. Bien que pris en compte ci-dessous, le mécanisme de détection et de commutation n'est pas montré sur le schéma.

Une expression pour la fiabilité $R(t)$ d'un tel système peut être obtenue en considérant quels événements possibles sont susceptibles de survenir durant un temps de mission t. Ci-après sont les possibilités:

a) le dispositif A fonctionne pendant un temps t; ou

b) le dispositif A avec un taux de défaillance λ_A et une fonction de densité de probabilité $f_A(\tau)$ est initialement en fonction, mais tombe en panne au temps $\tau < t$ et

   – le dispositif B (taux de défaillance λ_{Bd}) est initialement à l'état passif (latent), (soit froid ou sous-tension) jusqu'à ce que A tombe en panne (temps τ) moment à partir duquel il est alimenté (taux de défaillance λ_B) et prend le relais avec A par le biais de la commutation S (fiabilité $R_{SW}(\tau)$) ou

   – le dispositif B «survit» au reste de la mission avec une probabilité $R_B(t-\tau)$.

Mathématiquement, on peut l'exprimer comme suit:

$$R_S(t) = R_A(t) + \int_0^t f_A(\tau) \cdot R_{Bd}(\tau) \cdot R_{SW}(\tau) \cdot R_B(t-\tau) \cdot d\tau$$

Si on suppose que tous les dispositifs ont un taux de défaillance latent ou actif constant, alors l'équation ci-dessus devient:

$$R_S(t) = e^{-\lambda_A t} + \int_0^t \lambda_A \cdot e^{-\lambda_A \tau} \cdot e^{-\lambda_{Bd} \cdot \tau} e^{-\lambda_{SW} \cdot t} e^{-\lambda_B \cdot (t-\tau)} \cdot d\tau$$

NOTE Si la fiabilité du commutateur n'est pas une fonction du temps mais une fonction de plusieurs autres variables (par exemple, nombre d'opérations, sollicitations, etc.) il est préférable de ne pas utiliser de notation fonctionnelle, mais plutôt d'utiliser R_{sw} pour la fiabilité du commutateur.

For the particular case where m = n -1, $R_S = n \cdot R^m - m \cdot R^n$

If the n items are not identical, use of a more general procedure is recommended (see 8.3).

7.2.4 Standby redundancy models

Another frequently used form of redundancy is what is known as standby redundancy (see first paragraph of Annex A). In its most elementary form, the physical arrangement of items is represented by the diagram in Figure 10.

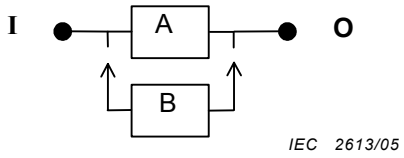


Figure 10 – Standby redundancy

In this figure, item A is the on-line active item, and item B is standing by waiting to be switched on to replace A when the latter fails. Although taken into account below, the switching and sensing mechanism is not shown on the diagram.

An equation for the reliability $R(t)$, of such a system can be obtained by considering what possible events may occur during a mission time t. The following are possibilities:

a) item A is working throughout time t; or

b) item A with a failure rate λ_A and probability density function $f_A(\tau)$ is initially working, but fails at some time $\tau < t$; and

- item B (failure rate λ_{Bd}) is initially in a passive state (dormant) state, (either cold or under low power) surviving until A fails (time τ) at which time it is energized (failure rate λ_B) then interchanged with A by means of switch S (reliability $R_{SW}(\tau)$); or
- item B survives the remainder of the mission with probability $R_B(t-\tau)$.

Mathematically, this can be expressed as follows:

$$R_S(t) = R_A(t) + \int_0^t f_A(\tau) \cdot R_{Bd}(\tau) \cdot R_{SW}(\tau) \cdot R_B(t-\tau) \cdot d\tau$$

If it is assumed that all items have a constant active or dormant failure rate, then the above equation becomes:

$$R_S(t) = e^{-\lambda_A t} + \int_0^t \lambda_A \cdot e^{-\lambda_A \tau} \cdot e^{-\lambda_{Bd} \cdot \tau} e^{-\lambda_{SW} \cdot \tau} e^{-\lambda_B \cdot (t-\tau)} \cdot d\tau$$

NOTE If the reliability of the switch is not a function of time but a function of some other variable (e.g. number of operations, demands, etc.) it would be preferable not to use functional notation at all, but to use instead R_{sw} to denote the switch reliability.

En évaluant la partie droite de l'équation ci-dessus:

$$R_S(t) = e^{-\lambda_A \cdot t} + \frac{\lambda_A}{\lambda_A + \lambda_{SW} + \lambda_{Bd} - \lambda_B} \cdot \left[e^{-\lambda_B \cdot t} - e^{-(\lambda_A + \lambda_{SW} + \lambda_{Bd}) \cdot t} \right]$$

Dans l'hypothèse d'une parfaite commutation, $\lambda_{SW} = 0$, l'équation devient:

$$R_S(t) = e^{-\lambda_A \cdot t} + \frac{\lambda_A}{\lambda_A + \lambda_{Bd} - \lambda_B} \cdot \left[e^{-\lambda_B \cdot t} - e^{-(\lambda_A + \lambda_{Bd}) \cdot t} \right]$$

Si le taux de défaillance latent du dispositif B est aussi supposé égal à zéro, alors la fiabilité d'un système redondant en attente est:

$$R_S(t) = e^{-\lambda_A \cdot t} + \frac{\lambda_A}{\lambda_A - \lambda_B} \cdot \left[e^{-\lambda_B \cdot t} - e^{-\lambda_A \cdot t} \right]$$

Si, en plus de ce qui est indiqué ci-dessus, les deux taux de défaillance sont égaux ($\lambda_A = \lambda$ et $\lambda_B = \lambda$), alors l'expression pour la fiabilité du système peut être montrée par:

$$R_S(t) = e^{-\lambda \cdot t} \cdot (1 + \lambda \cdot t)$$

Si sous de telles conditions idéales, il y a n (au lieu de un) dispositifs en attente, cette dernière expression devient:

$$R_S(t) = e^{-\lambda \cdot t} \left(1 + \lambda t + \frac{(\lambda \cdot t)^2}{2!} + \frac{(\lambda \cdot t)^3}{3!} + \ldots + \frac{(\lambda \cdot t)^n}{n!} \right)$$

A noter qu'il convient qu'un bloc-diagramme de fiabilité pratique comprenne des blocs pour représenter la fiabilité du système de détection et de commutation, qui est souvent le «maillon faible» dans les systèmes en attente.

A noter également que contrairement à tous les exemples considérés jusqu'à présent et dans le reste de cette norme, la probabilité de survie d'un dispositif (dispositif B) dépend du moment où l'autre dispositif (dispositif A) tombe en panne. En d'autres termes, les dispositifs A et B ne peuvent pas être regardés comme tombant en panne indépendamment. En conséquence, il convient d'utiliser d'autres procédures, telles que l'analyse de Markov, pour analyser les systèmes d'attente.

8 Modèles plus complexes

8.1 Procédures générales

8.1.1 Contexte

Il est possible d'évaluer la fiabilité $R_S(t)$ de tout système considéré jusqu'à présent par l'application d'une formule de fiabilité adaptée sélectionnée à partir des Equations (1) à (7). Cependant, pour certains systèmes le BDF correspondant peut ne pas être convenablement évalué par aucune des formules ci-dessus. Ces systèmes sont considérés comme plus complexes et d'autres techniques d'analyses de fiabilité doivent être utilisées. A noter que les BDF complexes peuvent habituellement être évalués par la simulation Monte Carlo. Cependant, l'utilisation de telles procédures n'est pas traité dans cette norme.

Pour la procédure suivante, la condition d'indépendance définie en 5.1 doit s'appliquer.

On evaluating the right-hand side of the above equation:

$$R_S(t) = e^{-\lambda_A \cdot t} + \frac{\lambda_A}{\lambda_A + \lambda_{SW} + \lambda_{Bd} - \lambda_B} \cdot \left[e^{-\lambda_B \cdot t} - e^{-(\lambda_A + \lambda_{SW} + \lambda_{Bd}) \cdot t} \right]$$

With an assumption of perfect switching, $\lambda_{SW} = 0$, the equation becomes:

$$R_S(t) = e^{-\lambda_A \cdot t} + \frac{\lambda_A}{\lambda_A + \lambda_{Bd} - \lambda_B} \cdot \left[e^{-\lambda_B \cdot t} - e^{-(\lambda_A + \lambda_{Bd}) \cdot t} \right]$$

If the dormant failure rate of item B is also assumed equal to zero, then reliability of a standby redundant system is:

$$R_S(t) = e^{-\lambda_A \cdot t} + \frac{\lambda_A}{\lambda_A - \lambda_B} \cdot \left[e^{-\lambda_B \cdot t} - e^{-\lambda_A \cdot t} \right]$$

If, in addition to the above, both failure rates are equal ($\lambda_A = \lambda$ and $\lambda_B = \lambda$), then the equation for system reliability can be shown to be given by:

$$R_S(t) = e^{-\lambda \cdot t} \cdot (1 + \lambda \cdot t)$$

If under such ideal conditions, there are n (instead of one) items on standby, this latter equation becomes:

$$R_S(t) = e^{-\lambda \cdot t} \left(1 + \lambda t + \frac{(\lambda \cdot t)^2}{2!} + \frac{(\lambda \cdot t)^3}{3!} + \ldots + \frac{(\lambda \cdot t)^n}{n!} \right)$$

It should be noted that a practical reliability block diagram should include blocks to represent the reliability of the switch plus sensing mechanism, which is often the "weak link" in standby systems.

It should also be noted that, unlike all the examples considered so far and in the remainder of this standard, the probability of survival of one item (item B) is dependent upon the time when the other item (item A) fails. In other words, items A and B cannot be regarded as failing independently. As a consequence, other procedures, such as Markov analysis, should be used to analyse standby systems.

8 More complex models

8.1 General procedures

8.1.1 Background

It is possible to evaluate the reliability $R_S(t)$ of all the systems considered so far by the application of a suitable reliability formula selected from Equations (1) to (7). However, for some systems the corresponding RBDs may not conveniently be evaluated by any of the above formulæ. These systems are considered to be more complex and so other reliability analysis techniques have to be employed. It should be noted that complex RBDs can usually be evaluated using Monte Carlo simulation. However, the use of such procedures is not dealt with in this standard.

For the procedures that follow, the condition of independence, as stated in 5.1, shall apply.

8.1.2 Utilisation du théorème de probabilité totale

Lorsque l'on traite des bloc-diagramme de fiabilité du type illustrés par la Figure 8, une approche différente est nécessaire. Une telle approche est basée sur le théorème de probabilité totale, qui peut être résumé comme suit:

Pour n événements mutuellement exclusifs $A_1 \ldots A_n$, dont la somme de probabilité est égale à l'unité, alors $P(B) = P(B \mid A_1) \cdot P(A_1) + \ldots + P(B \mid A_n) \cdot P(A_n)$ où B est un événement arbitraire, $P(A_i)$ est la probabilité d'occurrence de l'événement A_i et $P(B \mid A_i)$ est la probabilité conditionnelle de B étant donné A_i.

Une forme pratique de ce qui est indiqué ci-dessus, qui est adaptée à l'analyse des diagrammes de fiabilité, consiste à procéder à une utilisation répétée de la relation:

$$R_S = P_r(\text{SS} \mid \text{X working}) \cdot P_r(\text{X working}) + P_r(\text{SS} \mid \text{X failed}) \cdot P_r(\text{X failed})$$

Dans l'expression ci-dessus, R_S représente la fiabilité du système, P_r (SS | X opérationnel) représente la fiabilité du système (probabilité de succès du système) considérant qu'un bloc X particulier est en marche, et P_r (SS | X en panne) représente la fiabilité du système en considérant que le dispositif X particulier est tombé en panne. Par exemple, si dans la Figure 8 le dispositif A est tombé en panne, le bloc-diagramme de fiabilité devient simplement:

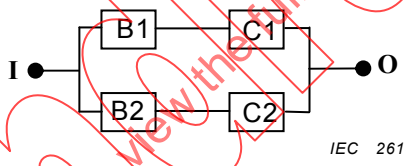


Figure 11 – Représentation de la Figure 8, quand l'entité A est défaillante

afin que

$$P_r \text{ (SS|A en panne)} = R_{B1} \cdot R_{C1} + R_{B2} \cdot R_{C2} - R_{B1} \cdot R_{C1} \cdot R_{B2} \cdot R_{C2}$$

De la même façon, quand A fonctionne, le diagramme est simplement celui donné à la Figure 12.

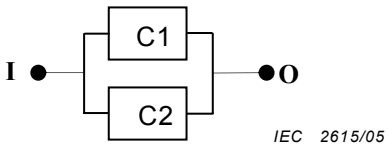


Figure 12 – Représentation de la Figure 8, quand l'entité A est opérationnelle

afin que

$$P_r \text{ (SS|A opérationnel)} = R_{C1} + R_{C2} - R_{C1} \cdot R_{C2}$$

d'où

$$R_S = (R_{C1} + R_{C2} - R_{C1} \cdot R_{C2}) \cdot R_A + (R_{B1} \cdot R_{C1} + R_{B2} \cdot R_{C2} - R_{B1} \cdot R_{C1} \cdot R_{B2} \cdot R_{C2}) \cdot (1 - R_A)$$

8.1.2 Use of the total probability theorem

When dealing with reliability block diagrams of the type illustrated by Figure 8, a different kind of approach is required. One such approach is based on the total probability theorem, which can be summarized as follows.

For n mutually exclusive events $A_1 \ldots A_n$, whose probabilities sum to unity, then $P(B) = P(B \mid A_1) \cdot P(A_1) + \ldots + P(B \mid A_n) \cdot P(A_n)$ where B is an arbitrary event, $P(A_i)$ is the probability of occurrence of event A_i and $P(B \mid A_i)$ is the conditional probability of B given A_i.

A convenient form of the above, which is appropriate for analysing reliability block diagrams, is to make repeated use of the relationship:

$$R_S = P_r(\text{SS} \mid \text{X working}) \cdot P_r(\text{X working}) + P_r(\text{SS} \mid \text{X failed}) \cdot P_r(\text{X failed})$$

In the above equation R_S denotes the reliability of the system, P_r (SS | X working) denotes the reliability of the system (probability of system success) given that a particular block X is working, and P_r (SS | X failed) denotes the reliability of the system given that the particular item X has failed. For example, if in Figure 8 the item A has failed, the reliability block diagram simply becomes:

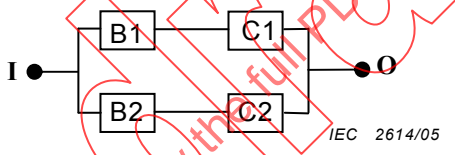


Figure 11 – Representation of Figure 8 when item A has failed

so that

P_r (SS|A failed) = $R_{B1} \cdot R_{C1} + R_{B2} \cdot R_{C2} - R_{B1} \cdot R_{C1} \cdot R_{B2} \cdot R_{C2}$

Similarly, when A is working, the reliability block diagram is simply that given in Figure 12.

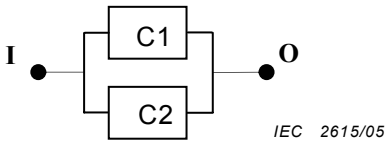


Figure 12 – Representation of Figure 8 when item A is working

so that

P_r (SS|A working) = $R_{C1} + R_{C2} - R_{C1} \cdot R_{C2}$

hence

$$R_S = (R_{C1} + R_{C2} - R_{C1} \cdot R_{C2}) \cdot R_A + (R_{B1} \cdot R_{C1} + R_{B2} \cdot R_{C2} - R_{B1} \cdot R_{C1} \cdot R_{B2} \cdot R_{C2}) \cdot (1 - R_A)$$

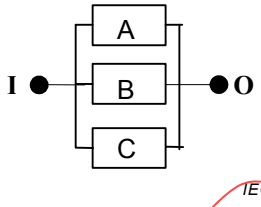
Si $R_{C1} = R_{C2} = R_C$ et $R_{B1} = R_{B2} = R_B$, l'expression ci-dessus se simplifie en:

$$R_S = \left(2R_C - R_C^2\right) \cdot R_A + \left(2R_B \cdot R_C - R_B^2 \cdot R_C^2\right) \cdot (1 - R_A) \quad (8)$$

La technique décrite en 8.1.2 peut être appliquée à la vérification des équations (6) et (7).

8.1.3 Utilisation des tables de vérités Booléennes

Les cheminements réussis du système décrit par BDF peuvent également être représentés par des expressions booléennes. Par exemple, trois dispositifs A, B et C, connectés en parallèle (un nécessaire à l'état opérationnel du système) peuvent être représentés par le BDF illustré dans la Figure 13, ou par



1/3 nécessaire

Figure 13 – Arrangement parallèle avec une entité opérationnelle nécessaire sur trois

l'expression Booléenne:

$$SS = A \cup B \cup C \quad (9)$$

où SS représente l'état opérationnel du système, A, B et C représentant les états opérationnels des blocs A, B et C.

Cependant, les termes Booléens A, B et C ne peuvent être directement remplacés par les probabilités correspondantes R_A, R_B, R_C pour obtenir une valeur pour la fiabilité du système. Cela parce que l'équation (9) est en effet un ensemble de termes «chevauchant». pas *disjoint* (voir l'Article B.3).

$$SS = \overline{A}\,\overline{B}C \cup \overline{A}B\overline{C} \cup \overline{A}BC \cup A\overline{B}\,\overline{C} \cup A\overline{B}C \cup AB\overline{C} \cup ABC \quad (10)$$

En termes purement Booléens, les Equations (9) et (10) sont équivalentes. Dans l' équation (10), chaque terme Littéral $\left(\text{tels que } A, \overline{A}, B, \overline{B}, C, \overline{C}\right)$ peut être remplacé par le terme de fiabilité/non-fiabilité correspondant:

$$R_A, (1 - R_A), R_B, (1 - R_B), R_C, (1 - R_C)$$

pour produire une expression de la fiabilité du système R_S, donné par:

$$\begin{aligned} R_S = {} & R_A(1-R_B)(1-R_C) + (1-R_A)R_B(1-R_C) + (1-R_A)(1-R_B)R_C + R_A(1-R_B)R_C \\ & + R_A R_B(1-R_C) + (1-R_A)R_B R_C + R_A R_B R_C \end{aligned} \quad (11)$$

Une façon encore plus simple d'écrire l'équation (9) en termes non chevauchant est:

$$SS = A \cup \overline{A} \cap B \cup \overline{B} \cup \overline{A} \cup C \quad (12)$$

afin que

$$R_S = R_A + (1 - R_A) \cdot R_B + (1 - R_B) \cdot (1 - R_A) \cdot R_C \quad (13)$$

If $R_{C1} = R_{C2} = R_C$ and $R_{B1} = R_{B2} = R_B$, the above equation simplifies to:

$$R_S = \left(2R_C - R_C^2\right) \cdot R_A + \left(2R_B \cdot R_C - R_B^2 \cdot R_C^2\right) \cdot (1 - R_A) \quad (8)$$

The technique described in 8.1.2 can be applied to verify Equations (6) and (7).

8.1.3 Use of Boolean truth tables

The system success paths depicted by RBDs can also be represented by Boolean expressions. For example, three items A, B and C which are connected in parallel (one required for system success) can be represented by the RBD illustrated in Figure 13, or by

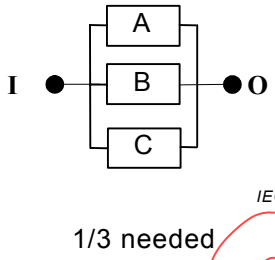


Figure 13 – One-out-of-three parallel arrangement

the Boolean expression:

$$\text{SS} = A \cup B \cup C \quad (9)$$

where SS denotes system success, while A, B and C denote success states of blocks A, B and C.

However, the Boolean terms A, B and C cannot be directly replaced by the corresponding probabilities R_A, R_B, R_C in order to obtain a value for system reliability. This is because Equation (9) is in effect a set of "overlapping" (not "disjoint") terms (see Clause B.3).

$$\text{SS} = \overline{A}\,\overline{B}C \cup \overline{A}B\overline{C} \cup \overline{A}BC \cup A\overline{B}\,\overline{C} \cup A\overline{B}C \cup AB\overline{C} \cup ABC \quad (10)$$

In purely Boolean terms, Equations (9) and (10) are equivalent. In Equation (10) each literal (terms like A, $\overline{A}$, B, $\overline{B}$, C, $\overline{C}$) can be replaced by the corresponding reliability/unreliability term:

$$R_A, (1 - R_A), R_B, (1 - R_B), R_C, (1 - R_C)$$

to yield an equation for system reliability R_S, given by:

$$\begin{aligned} R_S = {} & R_A(1-R_B)(1-R_C) + (1-R_A)R_B(1-R_C) + (1-R_A)(1-R_B)R_C + R_A(1-R_B)R_C \\ & + R_A R_B(1-R_C) + (1-R_A)R_B R_C + R_A R_B R_C \end{aligned} \quad (11)$$

An even simpler way of writing Equation (9) in non-overlapping terms is:

$$SS = A \cup \overline{A} \cap B \cup \overline{B} \cap \overline{A} \cap C \quad (12)$$

so that

$$R_S = R_A + (1 - R_A) \cdot R_B + (1 - R_B) \cdot (1 - R_A) \cdot R_C \quad (13)$$

On peut montrer qu'une fois simplifiées, les équations (11) et (13) sont identiques.

Le processus pour arriver à l'équation (11) peut être plus systématiquement mener en utilisant une table de vérité pour convertir l'équation (9) en Equation (10), comme montré dans le Tableau 1.

D'après le Tableau 1, les termes de l'état opérationnel sont (de haut en bas):

$$\overline{A} \cap \overline{B} \cap C,\ \overline{A} \cap B \cap \overline{C},\ \overline{A} \cap B \cap C,\ A \cap \overline{B} \cap \overline{C},\ A \cap \overline{B} \cap C,\ A \cap B \cap \overline{C},\ A \cap B \cap C$$

Ces termes sont combinés («OU-é») pour donner l'équation (10).

Tableau 1 – Application de la table de vérité à l'exemple de la Figure 13

Article			Système
A	**B**	**C**	
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1
NOTE 1= opérationnel, 0 =en panne.			

Si on considère l'exemple illustré par la Figure 8, et si toutes les combinaisons de dispositifs en marche et en panne sont listées telles qu'elles devraient exister (produisant 32 termes en tout), cela donne des résultats illustrés par le Tableau 2.

It can be shown that once simplified, Equations (11) and (13) are identical.

The process of arriving at Equation (11) can be more systematically carried out by using a truth table to convert Equation (9) to Equation (10), as shown in Table 1.

Referring to Table 1 the success terms are (from top to bottom):

$$\overline{A} \cap \overline{B} \cap C,\ \overline{A} \cap B \cap \overline{C},\ \overline{A} \cap B \cap C,\ A \cap \overline{B} \cap \overline{C},\ A \cap \overline{B} \cap C,\ A \cap B \cap \overline{C},\ A \cap B \cap C$$

These terms are combined ("OR-ed") to give Equation (10).

Table 1 – Application of truth table to the example of Figure 13

Item			System
A	**B**	**C**	
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1
NOTE 1= working, 0 = failed.			

The example illustrated by Figure 8 is next considered and all possible combinations (32 in all) of working and failed items are listed as illustrated in Table 2.

Tableau 2 – Application de la table de vérité à l'exemple de la Figure 8

Article					Système
B1	B2	C1	C2	A	
0	0	0	0	0	0
0	0	0	0	1	0
0	0	0	1	0	0
0	0	0	1	1	1
0	0	1	0	0	0
0	0	1	0	1	1
0	0	1	1	0	0
0	0	1	1	1	1
0	1	0	0	0	0
0	1	0	0	1	0
0	1	0	1	0	1
0	1	0	1	1	1
0	1	1	0	0	0
0	1	1	0	1	1
0	1	1	1	0	1
0	1	1	1	1	1
1	0	0	0	0	0
1	0	0	0	1	0
1	0	0	1	0	0
1	0	0	1	1	1
1	0	1	0	0	1
1	0	1	0	1	1
1	0	1	1	0	1
1	0	1	1	1	1
1	1	0	0	0	0
1	1	0	0	1	0
1	1	0	1	0	1
1	1	0	1	1	1
1	1	1	0	0	1
1	1	1	0	1	1
1	1	1	1	0	1
1	1	1	1	1	1
NOTE 1= opérationnel, 0 = en panne.					

Les combinaisons réussies des dispositifs peuvent être sélectionnées à partir du Tableau 2 et l'expression pour la fiabilité du système comme l'ensemble des termes mutuellement exclusifs peut s'écrire de la façon suivante:

$$SS = \overline{B1} \cap \overline{B2} \cap \overline{C1} \cap C2 \cap A \cup \overline{B1} \cap \overline{B2} \cap \overline{C1} \cap \overline{C2} \cap A \cup \cdots \cup B1 \cap B2 \cap C1 \cap C2 \cap A \qquad (14)$$

de laquelle

$$R_S = (1 - R_{B1}) \cdot (1 - R_{B2}) \cdot (1 - R_{C1}) \cdot R_{C2} \cdot R_A + (1 - R_{B1}) \cdot (1 - R_{B2}) \cdot R_{C1} \cdot (1 - R_{C2}) \cdot R_A + \ldots$$
$$+ R_{B1} \cdot R_{B2} \cdot R_{C1} \cdot R_{C2} \cdot R_A$$

Table 2 – Application of truth table to the example of Figure 8

Item					System
B1	B2	C1	C2	A	
0	0	0	0	0	0
0	0	0	0	1	0
0	0	0	1	0	0
0	0	0	1	1	1
0	0	1	0	0	0
0	0	1	0	1	1
0	0	1	1	0	0
0	0	1	1	1	1
0	1	0	0	0	0
0	1	0	0	1	0
0	1	0	1	0	1
0	1	0	1	1	1
0	1	1	0	0	0
0	1	1	0	1	1
0	1	1	1	0	1
0	1	1	1	1	1
1	0	0	0	0	0
1	0	0	0	1	0
1	0	0	1	0	0
1	0	0	1	1	1
1	0	1	0	0	1
1	0	1	0	1	1
1	0	1	1	0	1
1	0	1	1	1	1
1	1	0	0	0	0
1	1	0	0	1	0
1	1	0	1	0	1
1	1	0	1	1	1
1	1	1	0	0	1
1	1	1	0	1	1
1	1	1	1	0	1
1	1	1	1	1	1
NOTE 1= working, 0 = failed.					

The success combinations of items can be selected from Table 2 and the expression for system reliability is the set of mutually exclusive terms which can be written down as follows:

$$\mathrm{SS} = \overline{B1} \cap \overline{B2} \cap \overline{C1} \cap C2 \cap A \cup \overline{B1} \cap \overline{B2} \cap C1 \cap \overline{C2} \cap A \cup \cdots \cup B1 \cap B2 \cap C1 \cap C2 \cap A \qquad (14)$$

from which

$$R_{\mathrm{S}} = (1 - R_{\mathrm{B1}}) \cdot (1 - R_{\mathrm{B2}}) \cdot (1 - R_{\mathrm{C1}}) \cdot R_{\mathrm{C2}} \cdot R_{\mathrm{A}} + (1 - R_{\mathrm{B1}}) \cdot (1 - R_{\mathrm{B2}}) \cdot R_{\mathrm{C1}} \cdot (1 - R_{\mathrm{C2}}) \cdot R_{\mathrm{A}} + \cdots$$
$$+ R_{\mathrm{B1}} \cdot R_{\mathrm{B2}} \cdot R_{\mathrm{C1}} \cdot R_{\mathrm{C2}} \cdot R_{\mathrm{A}}$$

L'équation (14) contient 19 termes (un pour chaque combinaison qui aboutit à une réussite), devant tous être ajoutés pour obtenir le résultat souhaité. D'après ceci, on voit vite que l'approche de la table de vérité booléenne peut devenir compliquée, bien que le principe impliqué soit relativement simple. Pour une description détaillée d'une application générale des méthodes Booléennes, voir l'Annexe B.

8.2 Modèles avec blocs communs

A noter que, dans l'Article 7 aucun bloc n'apparaît plus d'une fois dans le BDF. Cependant, il peut parfois être avantageux d'utiliser des blocs-diagrammes du type illustré à la Figure 14. Par exemple, les dispositifs C et D pourraient être deux dispositifs fonctionnellement similaires agissant comme double l'un de l'autre, mais où le dispositif A ne peut alimenter que le dispositif C, alors que le dispositif B est capable d'alimenter à la fois C et D. Cela est illustré dans la Figure 14, qui représente non seulement les arrangements physiques des dispositifs, mais aussi le bloc-diagramme de fiabilité. L'introduction de flèches dans un tel diagramme est importante.

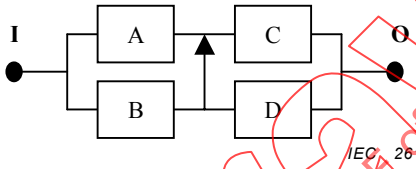


Figure 14 – Bloc-diagramme de fiabilité utilisant une flèche pour aider à définir l'état réussi du système

Les cheminements de l'état opérationnel du système dans l'exemple ci-dessus peuvent être représentés autrement, par un diagramme où des blocs apparaissent plus d'une fois, comme dans la Figure 15. Ce schéma a été déduit de la Figure 14 en étudiant cette dernière et constatant quelles paires de dispositifs, si elles tombent en panne en même temps, entraîneraient la défaillance du système. Ainsi, la Figure 15 est une combinaison des séries de telles paires.

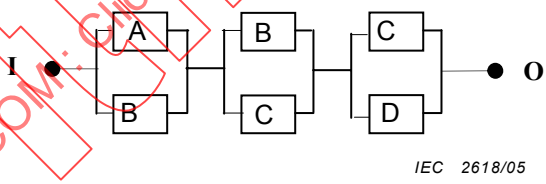


Figure 15 – Variante de la Figure 14 utilisant des blocs communs

S'agissant d'un bloc-diagramme de fiabilité du type ci-dessus, il serait incorrect de traiter les blocs comme paires indépendantes et donc de multiplier les fiabilités des paires ensemble. Il convient à la place d'utiliser l'une ou l'autre des méthodes données en 8.1.2 et 8.1.3. Pour exemple, l'utilisation de la méthode décrite en 8.1.2 donne:

$$R_S = P_r\,(\text{SS}\,|\,\text{B opérationnel}) \cdot P_r\,(\text{B opé.}) + P_r\,(\text{SS}\,|\,\text{B en panne}) \cdot P_r\,(\text{B en panne})$$

où P_r (SS|B opérationnel) est donné par le bloc-diagramme de fiabilité comprenant les blocs C et D en parallèle. Mais

$$P_r\,(\text{SS}\,|\,\text{B en panne}) = P_r\,(\text{SS}\,|\,\text{B en panne}\,|\,\text{C opérationnel}) \cdot P_r\,(\text{C opérationnel}) +$$
$$+ P_r\,(\text{SS}\,|\,\text{B en panne}\,|\,\text{C en panne}) \cdot P_r\,(\text{C en panne}) = R_A R_C + 0$$

D'où $R_S = (R_D + R_C - R_D \cdot R_C) \cdot R_B + R_A \cdot R_C \cdot (1 - R_B)$

c'est-à-dire $R_S = R_A \cdot R_C + R_B \cdot R_C + R_B \cdot R_D - R_A \cdot R_B \cdot R_C - R_D \cdot R_B \cdot R_C$

Equation (14) contains 19 terms (one for each combination that results in success), all of which have to be summed to give the desired result. From this it can be seen that the Boolean truth table approach can soon become unwieldy, although the principle involved is quite straightforward. For a detailed description of a general application of Boolean methods, see Annex B.

8.2 Models with common blocks

Note that in Clause 7 no block appeared more than once in the RBDs. It may sometimes, however, be advantageous to use block diagrams of the type illustrated by Figure 14. For example, items C and D might be two functionally similar items acting as duplicates for one another, but item A can power only item C, whereas item B is capable of supplying power to both C and D. This is illustrated by Figure 14, which represents not only the physical arrangements of the items, but also the reliability block diagram as well. It is important to include the arrows in such a diagram.

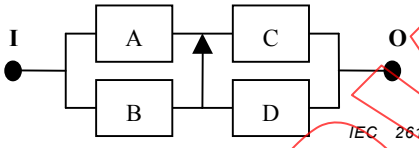


Figure 14 – Reliability block diagram using an arrow to help define system success

Alternatively the system success paths in the above example may be represented by a block diagram in which some blocks appear more than once, as in Figure 15. This diagram was derived from Figure 14 by examining the latter and noting which pairs of items, if failing together, would cause the system to fail. Figure 15 is thus a series combination of such pairs.

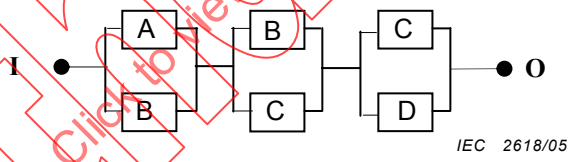


Figure 15 – Alternative representation of Figure 14 using common blocks

When dealing with a reliability block diagram of the above type, it would be incorrect to treat the blocks as independent pairs and then multiply the reliabilities of the pairs together. Instead, use should be made of either of the methods given in 8.1.2 and 8.1.3. As an example, using the method described in 8.1.2, gives:

$$R_S = P_r\,(\text{SS}\,|\,\text{B working}\,)\cdot P_r\,(\text{B working}) + P_r\,(\text{SS}\,|\,\text{B failed})\cdot P_r\,(\text{B failed})$$

where P_r(SS|B working) is given by the reliability block diagram comprising blocks C and D in parallel. But

$$P_r\,(\text{SS}\,|\,\text{B failed}) = P_r\,(\text{SS}\,|\,\text{B failed}\,|\,\text{C working})\cdot P_r\,(\text{C working}) + P_r\,(\text{SS}\,|\,\text{B failed}\,|\,\text{C failed})\cdot P_r\,(\text{C failed})$$
$$= R_A R_C + 0$$

Hence $R_S = (R_D + R_C - R_D \cdot R_C)\cdot R_B + R_A \cdot R_C \cdot (1 - R_B)$

i.e. $R_S = R_A \cdot R_C + R_B \cdot R_C + R_B \cdot R_D - R_A \cdot R_B \cdot R_C - R_D \cdot R_B \cdot R_C$

On remarque que les Figures 14 et 15 sont des manières différentes de modéliser la même définition de défaillance. A savoir, la défaillance du système survient lorsque les blocs A et B tombent en panne, ou B et C tombent en panne, ou C et D tombent en panne . En d'autres termes, les expressions booléennes pour l'état opérationnel du système (SS) ou pour la défaillance du système (SF) sont les mêmes pour les deux Figures 14 et 15, soit:

$$\text{SS} = A \cap C \cup B \cap C \cup B \cap D \qquad \text{SF} = \overline{A} \cap \overline{B} \cup \overline{B} \cap \overline{C} \cup \overline{C} \cap \overline{D}$$

Par l'application de la méthode décrite en 8.1.3, le Tableau 3 peut être développé.

Tableau 3 – Application de la table de vérité aux exemples des Figures 14 et 15

Article				Système
A	**B**	**C**	**D**	
1	1	1	1	1
1	1	1	0	1
1	1	0	1	1
1	1	0	0	0
1	0	1	1	1
1	0	1	0	1
1	0	0	1	0
1	0	0	0	0
0	1	1	1	1
0	1	1	0	1
0	1	0	1	1
0	1	0	0	0
0	0	1	1	0
0	0	1	0	0
0	0	0	1	0
0	0	0	0	0
NOTE 1 = opérationnel, 0 = en panne.				

D'après le Tableau 3, l'équation suivante peut s'exprimer.

$$\begin{aligned} R_S = {} & R_A \cdot R_B \cdot R_C \cdot R_D + R_A \cdot R_B \cdot R_C \cdot (1-R_D) + R_A \cdot R_B \cdot (1-R_C) \cdot R_D \\ & + R_A \cdot (1-R_B) \cdot R_C \cdot R_D + R_A.(1-R_B).R_C.(1-R_D) + (1-R_A).R_B.R_C.R_D \\ & + (1-R_A) \cdot R_B \cdot R_C \cdot (1-R_D) + (1-R_A) \cdot R_B \cdot (1-R_C) \cdot R_D \end{aligned}$$

Ce qui peut être simplifié en:

$$R_S = R_A \cdot R_C + R_B \cdot R_D + R_B \cdot R_C - R_A \cdot R_B \cdot R_C - R_D \cdot R_B \cdot R_C$$

Une autre méthode pour traiter des blocs communs est la suivante. D'abord, ignorer le fait que certains blocs apparaissent plus d'une fois puis écrire l'expression pour la fiabilité du système R_S de façon habituelle:

$$R_S = (R_A + R_B - R_A \cdot R_B) \cdot (R_B + R_C - R_B \cdot R_C) \cdot (R_C + R_D - R_C \cdot R_D)$$

Note that Figures 14 and 15 are different ways of modelling the same failure definition. Namely, system failure occurs when blocks A and B fail, or B and C fail or C and D fail. In other words, the Boolean expressions for system success (SS) or for system failure (SF) are the same for both Figures 14 and 15, i.e.

$$\text{SS} = A \cap C \cup B \cap C \cup B \cap D \qquad \text{SF} = \overline{A} \cap \overline{B} \cup \overline{B} \cap \overline{C} \cup \overline{C} \cap \overline{D}$$

By applying the method described in 8.1.3, Table 3 can be developed.

Table 3 – Application of truth table to the examples of Figures 14 and 15

Item				System
A	B	C	D	
1	1	1	1	1
1	1	1	0	1
1	1	0	1	1
1	1	0	0	0
1	0	1	1	1
1	0	1	0	1
1	0	0	1	0
1	0	0	0	0
0	1	1	1	1
0	1	1	0	1
0	1	0	1	1
0	1	0	0	0
0	0	1	1	0
0	0	1	0	0
0	0	0	1	0
0	0	0	0	0
NOTE 1 = working, 0 = failed.				

From Table 3, the following equation can be obtained.

$$\begin{aligned} R_S = {} & R_A \cdot R_B \cdot R_C \cdot R_D + R_A \cdot R_B \cdot R_C \cdot (1-R_D) + R_A \cdot R_B \cdot (1-R_C) \cdot R_D \\ & + R_A \cdot (1-R_B) \cdot R_C \cdot R_D + R_A . (1-R_B) . R_C . (1-R_D) + (1-R_A) . R_B . R_C . R_D \\ & + (1-R_A) \cdot R_B \cdot R_C \cdot (1-R_D) + (1-R_A) \cdot R_B \cdot (1-R_C) \cdot R_D \end{aligned}$$

This can be simplified to give:

$$R_S = R_A \cdot R_C + R_B \cdot R_D + R_B \cdot R_C - R_A \cdot R_B \cdot R_C - R_D \cdot R_B \cdot R_C$$

Yet another method of dealing with common blocks is as follows. First ignore the fact that some blocks appear more than once and write down the equation for system reliability R_S in the usual way:

$$R_S = (R_A + R_B - R_A \cdot R_B) \cdot (R_B + R_C - R_B \cdot R_C) \cdot (R_C + R_D - R_C \cdot R_D)$$

Si l 'expression est développée (produisant 27 termes en tout), et tous les termes tels que $R_A \cdot R_B \cdot R_C^2$ et $R_A \cdot R_B \cdot R_C^2$ remplacés respectivement par leurs équivalents booléens $R_A \cdot R_B \cdot R_C$ et $R_D \cdot R_B \cdot R_C$ et ainsi de suite, alors l'expression pour la fiabilité du système (R_S) se réduit à:

$$R_S = R_A \cdot R_C + R_B \cdot R_D + R_B \cdot R_C - R_A \cdot R_B \cdot R_C - R_D \cdot R_B \cdot R_C$$

8.3 *m* de *n* modèles (dispositifs non identiques)

La procédure décrite en 7.2.3 ne s'applique pas ici. Par exemple, considérons un système représenté par le bloc-diagramme de fiabilité de la Figure 16.

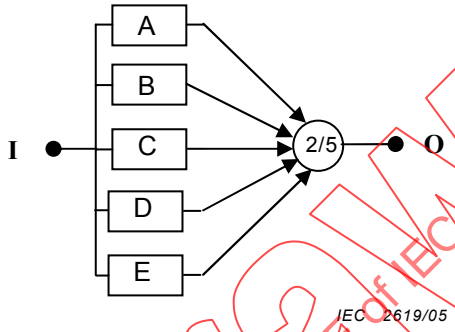


Figure 16 – 2 sur 5 système non identique

La fiabilité d'un tel système peut être évaluée par l'une ou l'autre des techniques décrites en 8.1.2 ou 8.1.3. La technique décrite en 8.1.3 nécessitera 32 entrées desquelles la probabilité de défaillance du système F_S peut être déduite:

$$F_S = (1-R_A)\cdot(1-R_B)\cdot(1-R_C)\cdot(1-R_D)\cdot(1-R_E) + (1-R_A)\cdot(1-R_B)\cdot(1-R_C)\cdot(1-R_D).R_E +$$
$$(1-R_A)\cdot(1-R_B)\cdot(1-R_C)\cdot R_D\cdot(1-R_E) + (1-R_A)\cdot(1-R_B)\cdot R_C\cdot(1-R_D)\cdot(1-R_E) +$$
$$(1-R_A)\cdot R_B\cdot(1-R_C)\cdot(1-R_D)\cdot(1-R_E) + R_A\cdot(1-R_B)\cdot(1-R_C)\cdot(1-R_D)\cdot(1-R_E)$$

et donc, obtenir $R_S = 1 - F_S$.

NOTE Une technique plus efficace est décrite dans l'Annexe B.

8.4 Méthode de réduction

Parfois les blocs-diagrammes de fiabilité paraissent très compliqués. Cependant, après examen attentif, les blocs dans le schéma peuvent souvent être groupés ensemble de telle sorte que les groupes sont statistiquement indépendants. Ce qui signifie que pas plus d'un groupe ne peut contenir un même bloc répertorié.

If these brackets are now multiplied out (producing 27 terms in all) and terms like $R_A \cdot R_B \cdot R_C^2$ and $R_D \cdot R_B \cdot R_C^2$ replaced by their Boolean equivalents $R_A \cdot R_B \cdot R_C$ and $R_D \cdot R_B \cdot R_C$ respectively and so on, then the equation for system reliability (R_S) will reduce to:

$$R_S = R_A \cdot R_C + R_B \cdot R_D + R_B \cdot R_C - R_A \cdot R_B \cdot R_C - R_D \cdot R_B \cdot R_C$$

8.3 *m* out of *n* models (non-identical items)

The procedure described in 7.2.3 is not applicable here. As an example, consider a system represented by the reliability block diagram in Figure 16.

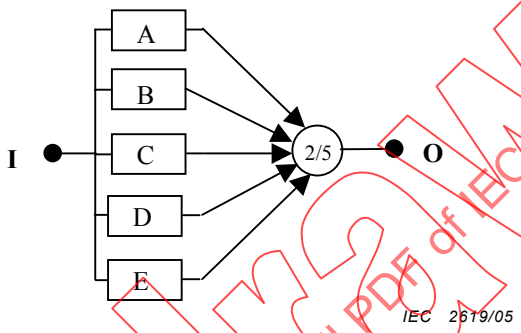


Figure 16 – 2-out-of-5 non-identical system

The reliability of such a system may be evaluated by either of the techniques described in 8.1.2 or 8.1.3. Of these, the technique described in 8.1.3 will require 32 entries from which the probability of system failure F_S can be derived as:

$$F_S = (1-R_A)\cdot(1-R_B)\cdot(1-R_C)\cdot(1-R_D)\cdot(1-R_E) + (1-R_A)\cdot(1-R_B)\cdot(1-R_C)\cdot(1-R_D).R_E +$$
$$(1-R_A)\cdot(1-R_B)\cdot(1-R_C)\cdot R_D\cdot(1-R_E) + (1-R_A)\cdot(1-R_B)\cdot R_C\cdot(1-R_D)\cdot(1-R_E) +$$
$$(1-R_A)\cdot R_B\cdot(1-R_C)\cdot(1-R_D)\cdot(1-R_E) + R_A\cdot(1-R_B)\cdot(1-R_C)\cdot(1-R_D)\cdot(1-R_E)$$

and so $R_S = 1 - F_S$ can be found.

NOTE A more efficient technique is described in Annex B.

8.4 Method of reduction

Occasionally reliability block diagrams seem very complicated. By careful examination, however, the blocks in the diagram can often be grouped together such that the groups are statistically independent. This means that no two (or more) groups can contain the same lettered block.

Par exemple, considérons le diagramme illustré par la Figure 17.

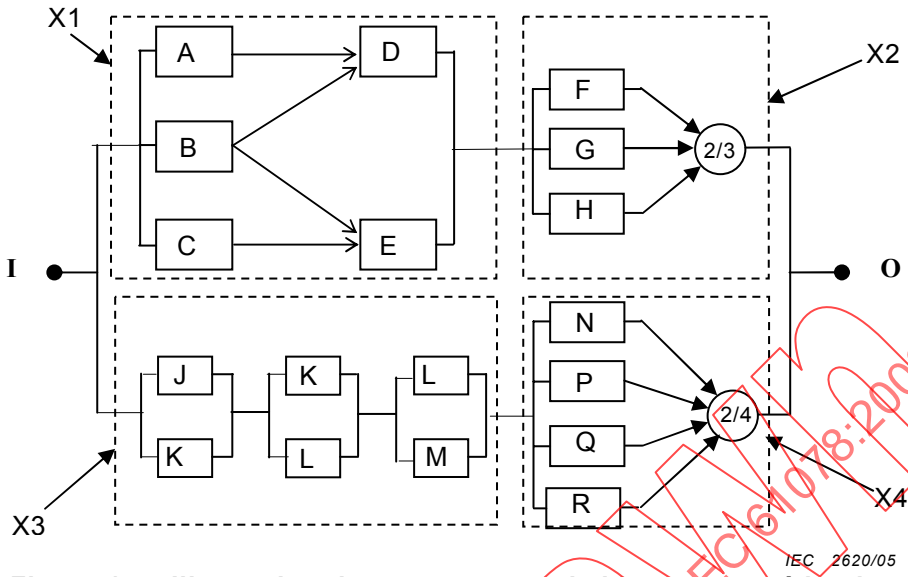


Figure 17 – Illustration de groupements de blocs avant réduction

La Figure 17 peut être réduite au bloc-diagramme montré dans la Figure 18a, en évaluant la fiabilité des quatre groupes de blocs en pointillés X1, X2, X3 et X4 tels qu'illustrés respectivement en 8.1, 7.2.3, 8.2 et 7.2.3 à nouveau. Le schéma de la Figure 18a peut être réduit à celui de la Figure 18b.

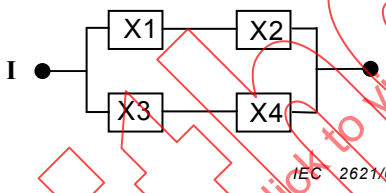


Figure 18a

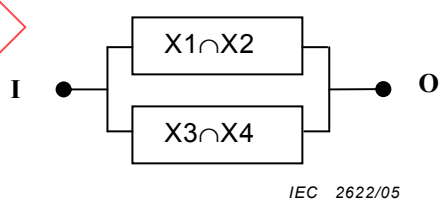


Figure 18b

Figure 18 – Bloc-diagramme bloc de fiabilité après réduction

D'où la fiabilité finale du système (suivant la Figure 18b) donnée par:

$$R_S = R_{X1} \cdot R_{X2} + R_{X3} \cdot R_{X4} - R_{X1} \cdot R_{X2} \cdot R_{X3} \cdot R_{X4}$$

comme expliqué en 7.2.2.

9 Extension des méthodes du bloc-diagramme de fiabilité aux calculs de la disponibilité

Sous certaines conditions, on pourra utiliser toutes les formules et procédures de cette norme, de façon à établir des prévisions de disponibilité d'un système en régime établi. Cela peut s'accomplir en remplaçant simplement les expressions de fiabilité, par les expressions correspondantes de disponibilité.

L'extension des méthodes ne sera valable que si les défaillances et réparations des dispositifs individuels sont indépendantes les unes des autres. Dans la pratique, cela signifie que la défaillance d'un dispositif ne doit en aucune façon affecter le début de défaillance d'un autre et il convient, en conséquence, qu'une «équipe illimitée» de réparateurs soit disponible.

For example, consider the reliability block diagram illustrated by Figure 17.

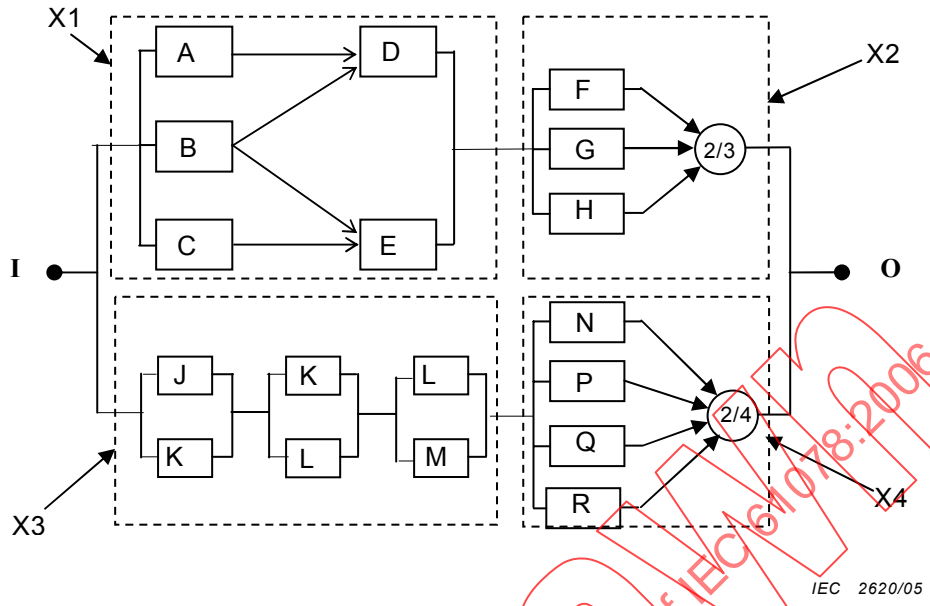


Figure 17 – Illustrating grouping of blocks before reduction

Figure 17 can be reduced to the diagram shown in Figure 18a, by evaluating the reliability of the four dotted groups of blocks X1, X2, X3 and X4 as illustrated in 8.1, 7.2.3, 8.2 and 7.2.3 again, respectively. The diagram in Figure 18a can be further reduced to the one in Figure 18b.

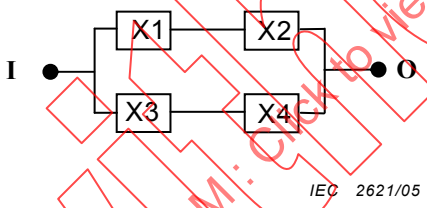


Figure 18a

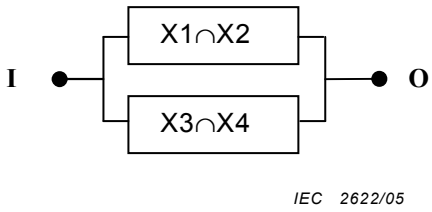


Figure 18b

Figure 18 – Reduced reliability block diagrams

Hence the final system reliability (referring to Figure 18b) is given by:

$$R_S = R_{X1} \cdot R_{X2} + R_{X3} \cdot R_{X4} - R_{X1} \cdot R_{X2} \cdot R_{X3} \cdot R_{X4}$$

as explained in 7.2.2.

9 Extension of reliability block diagram methods to availability calculations

Under certain conditions, one can use all the formulae and procedures in this standard in order to carry out system steady-state availability predictions. This is accomplished by simply replacing expressions for reliability, by corresponding expressions for availability.

The extension of the methods will be valid only if the failures and repairs of the individual items are independent of one another. In practice, this means that the failure of any item shall in no way affect the onset of failure of any other and that there should be available, in effect, an "infinite pool" of repair resources.

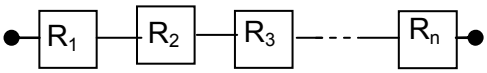
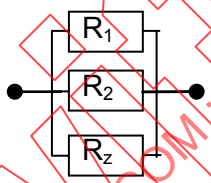
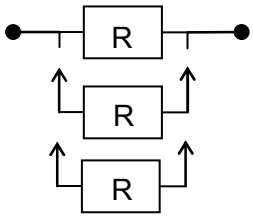
En d'autres termes, il convient que la moyenne du temps de panne de tout dispositif soit une mesure de ce dispositif seul et ne dépende pas du nombre d'autres dispositifs étant tombés en panne et nécessitant réparation. Cela signifie que dans la pratique, on doit prêter attention à la manière dont les dispositifs sont assemblés et tout particulièrement s'assurer que chaque dispositif est immédiatement accessible et non obstrué par un autre.

In other words, the mean down time of any item should be a measure of that item alone and should not depend upon how many other items have also failed and are in need of repair. The validity of the methods are more likely to be upheld if the way in which items are assembled is such that each item is readily accessible and not obstructed by any other.

Annexe A
(informative)

Récapitulatif des formules

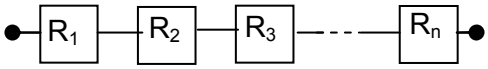
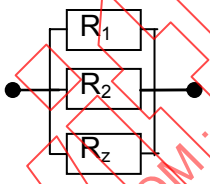
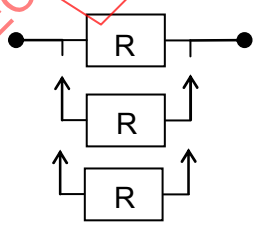
Dans les tableaux de cette annexe, un usage fréquent des termes «actif» et «en attente» est fait. Le premier terme est utilisé pour indiquer que les blocs concernés (chacun d'eux peut consister en un composant, un sous-système, un système, etc.) sont dans un état sous tension et ainsi être la cause d'une défaillance. Le second terme est utilisé pour indiquer que le ou les blocs concernés sont hors tension et ne peuvent être cause de défaillance.

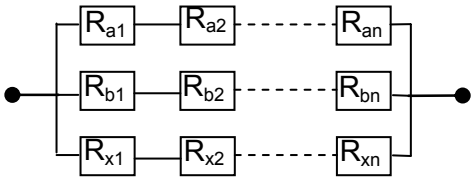
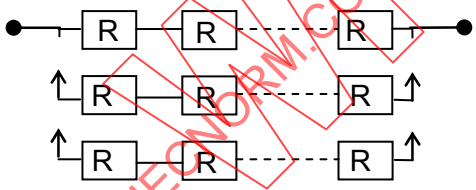
Configuration de base	Equation pour la fiabilité du système R_S
1 Séries  	A Cas général $R_s = R_1 . R_2 \ldots R_n$ --- B Avec $R_1 = R_2 = \ldots R_n = R$ $R_s = R^n$
2 Parallèle Actif  	A Cas général actif $R_s = 1 - (1 - R_1) \cdot (1 - R_2) \ldots (1 - R_z)$ B Actif avec $R_1 = R_2 \ldots = R_z$ $R_s = 1 - (1 - R_z)^z$
En attente  	C En attente avec $R = e^{-\lambda \cdot t}$ $R_S = e^{-\lambda \cdot t} + \lambda \cdot t . e^{-\lambda \cdot t} + \ldots + \frac{(\lambda \cdot t)^{z-1} e^{-\lambda \cdot t}}{(z-1)!}$

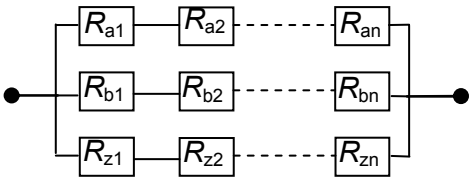
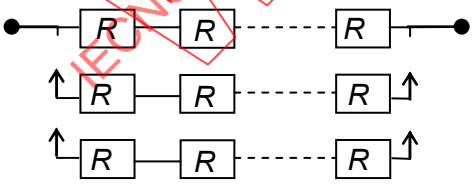
Annex A
(informative)

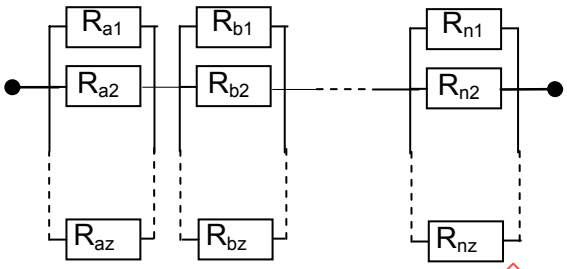
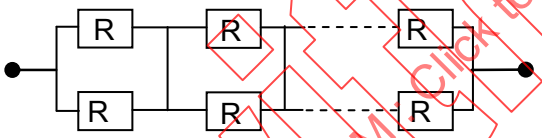
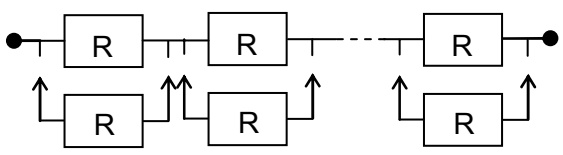
Summary of formulæ

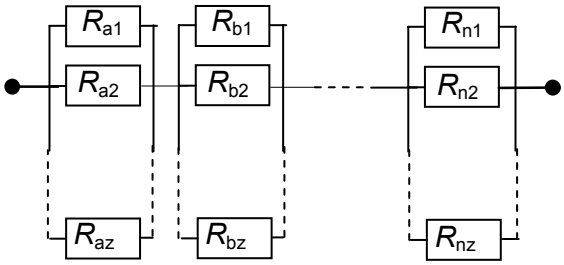
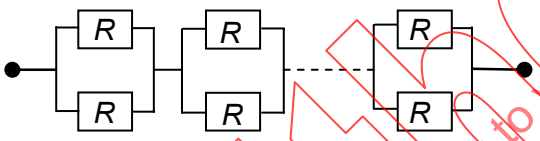
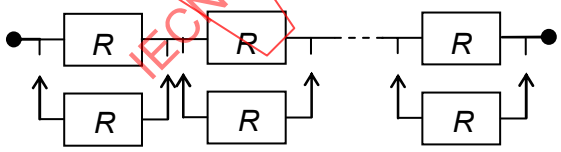
In the tables in this annex, frequent use is made of the terms “active” and “standby”. The former is used to indicate that the blocks concerned (each of which may consist of a component, sub-system, system, etc.) are energized (powered-up) and hence are liable to failure. The latter on the other hand is used to indicate that the block or blocks concerned are de-energized (powered-down) and not liable to failure.

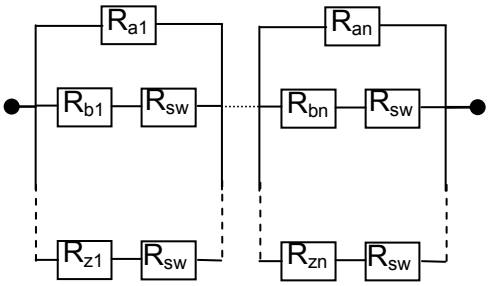
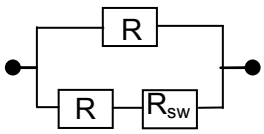
Basic configuration	Equation for system reliability R_S
1 Series 	A General case $R_s = R_1 \cdot R_2 \ldots R_n$
	B With $R_1 = R_2 = \ldots R_n = R$ $R_s = R^n$
2 Parallel Active 	A Active general case $R_s = 1-(1-R_1)\cdot(1-R_2)\ldots(1-R_z)$
	B Active with $R_1 = R_2 \ldots = R_z$ $R_s = 1-(1-R_z)^z$
Standby 	C Standby with $R = e^{-\lambda \cdot t}$ $R_S = e^{-\lambda \cdot t} + \lambda \cdot t . e^{-\lambda \cdot t} + \ldots + \frac{(\lambda \cdot t)^{z-1} e^{-\lambda \cdot t}}{(z-1)!}$

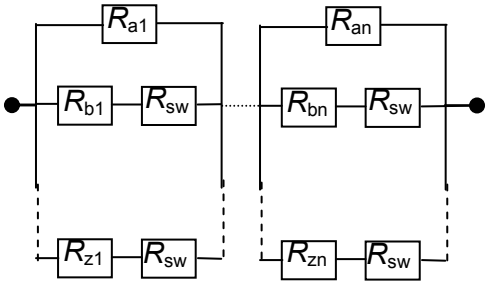
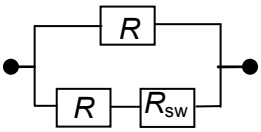
Configuration de base	Equation pour la fiabilité du système R_S
3 Séries / parallèles ou système redondant Actif  En attente  	A Cas général actif $$R_S = 1 - \prod_{j=a}^{z} (1 - R_{j1} \cdot R_{j2} \ldots R_{jn})$$ --- B Actif avec $$R_{a1} = R_{a2} = \cdots = R_a$$ $$R_{b1} = R_{b2} = \ldots = R_b$$ $$R_{z1} = R_{z2} = \cdots = R_z$$ $$R_S = 1 - \prod_{j=a}^{z} (1 - R_j{}^n)$$ --- C Actif avec $R_{aj} = R_{bj} = \cdots = R_{zj} = R$ pour j = 1 à n $$R_S = 1 - (1 - R^n)^z$$ --- D En attente avec $R = e^{-\lambda t}$ $$R_S = e^{-n\lambda t} + n\lambda t \cdot e^{-n \cdot \lambda \cdot t} + \ldots + \frac{(n\lambda t)^{z-1} e^{-n\lambda t}}{(x-1)!}$$

Basic configuration	Equation for system reliability R_S
3 Series parallel or system redundant Active  	A Active general case $$R_S = 1 - \prod_{j=a}^{z} (1 - R_{j1} \cdot R_{j2} \ldots R_{jn})$$
	B Active with $$R_{a1} = R_{a2} = \cdots = R_a$$ $$R_{b1} = R_{b2} = \cdots = R_b$$ $$R_{z1} = R_{z2} = \cdots = R_z$$ $$R_S = 1 - \prod_{j=a}^{z} (1 - R_j{}^n)$$
	C Active with $R_{aj} = R_{bj} = \cdots = R_{zj} = R$ for j = 1 to n $$R_S = 1 - (1 - R^n)^z$$
Standby  	D Standby with $R = e^{-\lambda t}$ $$R_S = e^{-n\lambda t} + n\lambda t \cdot e^{-n \cdot \lambda \cdot t} + \ldots + \frac{(n\lambda t)^{z-1} e^{-n\lambda t}}{(x-1)!}$$

Configuration de base	Equation pour la fiabilité du système R_S
4 Séries / parallèles ou élément redondant Actif   	A Cas général actif $R_S = \{1-(1-R_{a1})\cdot(1-R_{a2})\cdots(1-R_{az})\}\times$ $\{1-(1-R_{b1})\cdot(1-R_{b2})\cdots(1-R_{bz})\}\times$ $\ldots\{1-(1-R_{n1})\cdot(1-R_{n2})\cdots(1-R_{nz})\}$ --- B Actif avec -{}- $R_{a1} = R_{a2} = \cdots = R_a$ $R_{b1} = R_{b2} = \cdots = R_b$ $R_{n1} = R_{n2} = \cdots = R_n$ $R_S = \left(1-(1-R_a)^z\right)\cdot\left(1-(1-R_b)^z\right)\times$ $\ldots\left(1-(1-R_n)^z\right)$ --- C Actif avec tous les blocs ayant la même fiabilité «R» $R_{aj} = R_{bj} = \cdots = R_{nj} = R$ On assume $R = \mathrm{e}^{-\lambda\cdot t}$ $R_S = \left(2\cdot\mathrm{e}^{-\lambda\cdot t} - \mathrm{e}^{-2\cdot\lambda\cdot t}\right)^n$
En attente  	D En attente avec $R = \mathrm{e}^{-\lambda\cdot t}$ $R_S = \left(\mathrm{e}^{-\lambda\cdot t} + \lambda\cdot t\cdot\mathrm{e}^{-\lambda\cdot t}\right)^n$

Basic configuration	Equation for system reliability R_S
4 Parallel series or element redundant Active  	A Active general case $R_S = \{1-(1-R_{a1})\cdot(1-R_{a2})\cdots(1-R_{az})\}\times$ $\{1-(1-R_{b1})\cdot(1-R_{b2})\cdots(1-R_{bz})\}\times$ $\ldots\{1-(1-R_{n1})\cdot(1-R_{n2})\cdots(1-R_{nz})\}$
	B Active with $R_{a1} = R_{a2} = \cdots = R_a$ $R_{b1} = R_{b2} = \cdots = R_b$ $R_{n1} = R_{n2} = \cdots = R_n$ $R_S = \left(1-(1-R_a)^z\right)\cdot\left(1-(1-R_b)^z\right)\times$ $\ldots\left(1-(1-R_n)^z\right)$
	C Active with all blocks having the same reliability "R" $R_{aj} = R_{bj} = \cdots = R_{nj} = R$
 	Assuming $R = \mathrm{e}^{-\lambda\cdot t}$ $R_S = \left(2\cdot\mathrm{e}^{-\lambda\cdot t} - \mathrm{e}^{-2\cdot\lambda\cdot t}\right)^n$
Standby  	D Standby with $R = \mathrm{e}^{-\lambda\cdot t}$ $R_S = \left(\mathrm{e}^{-\lambda\cdot t} + \lambda\cdot t\cdot\mathrm{e}^{-\lambda\cdot t}\right)^n$

Configuration de base	Equation pour la fiabilité du système R_S
5 Séries / parallèles ou élément redondant  	A Actif en supposant que tous $R_{aj} = R_{bj} = \cdots = R_{zj} = R$ sauf R_{sw} $R_S = \left\{1 - (1 - R) \cdot (1 - R \cdot R_{sw})^{z-1}\right\}^n$
 	B Actif en supposant z = 2, n = 1 et tous $R_{aj} = R_{bj} = R_{zj} = R = e^{-\lambda t}$ sauf R_{sw} $R_S = e^{-\lambda t} + R_{sw} e^{-\lambda t} - R_{sw} e^{-2\lambda t}$
NOTE 1 Les formules pour les systèmes en attente sont basées sur l'hypothèse que la fiabilité des systèmes de commutation et de détection est de 100 % (R_{SW} = 1). NOTE 2 Pour des niveaux de défaillances constants, on peut remplacer $R(t)$ par $e^{-\lambda t}$.	

Basic configuration	Equation for system reliability R_S
5 Parallel series or element redundant   	A Active assuming all $R_{aj} = R_{bj} = \cdots = R_{zj} = R$ except R_{sw} $R_S = \left\{1 - (1 - R) \cdot (1 - R \cdot R_{sw})^{z-1}\right\}^n$ B Active assuming $z = 2$, $n = 1$ and all $R_{aj} = R_{bj} = R_{zj} = R = e^{-\lambda t}$ except R_{sw} $R_S = e^{-\lambda t} + R_{sw} e^{-\lambda t} - R_{sw} e^{-2\lambda t}$
NOTE 1 Formulæ for standby systems are based on the assumption that the reliability of switching and sensing mechanisms is 100 % ($R_{SW} = 1$). NOTE 2 For constant failure rates, $R(t)$ can be replaced by $e^{-\lambda t}$.	

Annexe B
(informative)

Méthodes booléennes disjointes

B.1 Remarques générales

Mis à part l'utilisation des tables de vérité booléennes données en 8.1.3, l'analyse du BDF telle que décrite jusqu'à présent, utilise principalement des formules mathématiques d'algèbre conventionnelle. Cependant, en général, l'algèbre booléenne peut également servir pour de telles analyses, et dans de nombreux cas est beaucoup plus efficace et simple. En particulier, l'utilisation de l'algèbre booléenne peut bien être l'approche la plus simple dès lors que:

a) BDF contient des blocs communs (voir Figure 15);

b) BDF contient des flèches directionnelles (voir Figures 8 et 14);

c) le système est particulièrement compliqué;

d) il est plus facile de construire une expression booléenne pour l'état opérationnel du système (ou défaillant) que de construire un BDF.

Le dispositif d) dans la liste ci-dessus est intéressant à remarquer. Pour de nombreux systèmes et réseaux la liste des combinaisons d'état opérationnel des équipements (ou défaillance) en termes booléens est souvent une tâche plus aisée que la construction du BDF correspondant. En utilisant au début l'approche booléenne pour analyser le système, le risque de faire des erreurs au cours de la construction du BDF est complètement éliminé.

B.2 Notation

Jusqu'ici les symboles $\cup$ et $\cap$ ont été utilisés pour désigner respectivement les «OU» et «ET» logiques. Cependant, dans ce qui suit, on trouvera plus pratique d'utiliser un symbole «+» pour indiquer le «OU» logique et un point pour indiquer le «ET». logique.[1] Un trait/une barre au dessus de la variable booléenne indiquera l'inverse ou le complément de la variable concernée: exemple $\bar{a}$ est interprété comme «non a». Par exemple $a \cdot b \cdot \bar{c} \cdot e + f \cdot g$ doit être interprété, «a ET b ET NON c ET e OU f ET g». Le contexte dans lequel les symboles sont utilisés peut clarifier la signification.

B.3 Principes – Variables booléennes et variables de probabilité

Considérons un système actif redondant à deux unités tel que décrit à la Figure 9. On peut voir que ce système en tant que tel survivra à condition que A ou B (ou les deux) survivent En d'autres termes, l'expression booléenne pour l'état opérationnel du système est donné par:

$$\mathrm{SS} = a + b \qquad (15)$$

où a et b sont des variables booléennes correspondant à la survie des blocs A et B respectivement. Il est tentant de substituer à R_a et R_b, a et b respectivement et de réécrire l'équation (15) sous la forme:

$$R_{\mathrm{S}} = R_a + R_b \qquad (16)$$

---

[1] L'avantage d'une telle notation se révèle dans l'Annexe B où des expressions du type

$\mathrm{SS1} = a \cdot b + \bar{a} \cdot e \cdot b + \bar{a} \cdot e \cdot d + a \cdot \bar{b} \cdot e \cdot d + \bar{a} \cdot c \cdot d + a \cdot \bar{b} \cdot c \cdot d$ se trouvent fréquemment. En prenant cette dernière expression comme exemple et en l'écrivant en utilisant les symboles théoriques, on obtient:

$\mathrm{SS1} = a \cap b \cup \bar{a} \cap e \cap b \cup \bar{a} \cap e \cap d \cup a \cap \bar{b} \cap e \cap d \cup \bar{a} \cap c \cap d \cup a \cap \bar{b} \cap c \cap d$ qui peut être difficile à interpréter ou à évaluer pour de nombreux lecteurs.