

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Reliability block diagrams

Diagrammes de fiabilité



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2016 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue

Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Reliability block diagrams

Diagrammes de fiabilité

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 03.120.01; 03.120.99

ISBN 978-2-8322-3561-4

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

FOREWORD.....	8
INTRODUCTION.....	10
1 Scope.....	11
2 Normative references.....	11
3 Terms and definitions	11
4 Symbols and abbreviated terms	18
5 Preliminary considerations, main assumptions, and limitations.....	22
5.1 General considerations.....	22
5.2 Pre-requisite/main assumptions.....	23
5.3 Limitations	23
6 Establishment of system success/failed states	24
6.1 General considerations.....	24
6.2 Detailed considerations	24
6.2.1 System operation	24
6.2.2 Environmental conditions	25
6.2.3 Duty cycles	25
7 Elementary models	25
7.1 Developing the model.....	25
7.2 Series structures.....	25
7.3 Parallel structures	26
7.4 Mix of series and parallel structures.....	26
7.5 Other structures	27
7.5.1 m out of n structures.....	27
7.5.2 Structures with common blocks	28
7.5.3 Composite blocks.....	29
7.6 Large RBDs and use of transfer gates	29
8 Qualitative analysis: minimal tie sets and minimal cut sets.....	30
8.1 Electrical analogy.....	30
8.2 Series-parallel representation with minimal success path and cut sets.....	32
8.3 Qualitative analysis from minimal cut sets.....	33
9 Quantitative analysis: blocks with constant probability of failure/success	33
9.1 Series structures.....	33
9.2 Parallel structures	34
9.3 Mix of series and parallel structures.....	34
9.4 m/n architectures (identical items).....	35
10 Quantitative analysis: blocks with time dependent probabilities of failure/success	35
10.1 General.....	35
10.2 Non-repaired blocks	36
10.2.1 General	36
10.2.2 Simple non-repaired block.....	36
10.2.3 Non-repaired composite blocks.....	36
10.2.4 RBDs with non-repaired blocks.....	37
10.3 Repaired blocks	37
10.3.1 Availability calculations	37
10.3.2 Average availability calculations	37

10.3.3	Reliability calculations.....	42
10.3.4	Frequency calculations.....	43
11	Boolean techniques for quantitative analysis of large models.....	43
11.1	General.....	43
11.2	Method of RBD reduction	44
11.3	Use of total probability theorem	45
11.4	Use of Boolean truth tables	46
11.5	Use of Karnaugh maps	47
11.6	Use of the Shannon decomposition and binary decision diagrams	49
11.7	Use of Sylvester-Poincaré formula.....	50
11.8	Examples of RBD application.....	51
11.8.1	Models with repeated blocks	51
11.8.2	m out of n models (non-identical items).....	54
12	Extension of reliability block diagram techniques	54
12.1	Non-coherent reliability block diagrams.....	54
12.2	Dynamic reliability block diagrams	57
12.2.1	General	57
12.2.2	Local interactions.....	58
12.2.3	Systemic dynamic interactions.....	59
12.2.4	Graphical representations of dynamic interactions	59
12.2.5	Probabilistic calculations	62
Annex A (informative)	Summary of formulae.....	63
Annex B (informative)	Boolean algebra methods.....	67
B.1	Introductory remarks	67
B.2	Notation.....	67
B.3	Tie sets (success paths) and cut sets (failure paths) analysis.....	68
B.3.1	Notion of cut and tie sets.....	68
B.3.2	Series-parallel representation using minimal tie and cut sets.....	69
B.3.3	Identification of minimal cuts and tie sets.....	70
B.4	Principles of calculations	71
B.4.1	Series structures	71
B.4.2	Parallel structures	71
B.4.3	Mix of series and parallel structures	73
B.4.4	m out of n architectures (identical items).....	73
B.5	Use of Sylvester Poincaré formula for large RBDs and repeated blocks.....	74
B.5.1	General	74
B.5.2	Sylvester Poincaré formula with tie sets.....	74
B.5.3	Sylvester Poincaré formula with cut sets.....	76
B.6	Method for disjointing Boolean expressions	77
B.6.1	General and background	77
B.6.2	Disjointing principle.....	78
B.6.3	Disjointing procedure	79
B.6.4	Example of application of disjointing procedure.....	79
B.6.5	Comments	81
B.7	Binary decision diagrams	82
B.7.1	Establishing a BDD	82
B.7.2	Minimal success paths and cut sets with BDDs.....	84
B.7.3	Probabilistic calculations with BDDs	86

B.7.4	Key remarks about the use of BDDs	87
Annex C (informative)	Time dependent probabilities and RBD driven Markov processes	88
C.1	General.....	88
C.2	Principle for calculation of time dependent availabilities	88
C.3	Non-repaired blocks	89
C.3.1	General	89
C.3.2	Simple non-repaired blocks	89
C.3.3	Composite block: example on a non-repaired standby system	89
C.4	RBD driven Markov processes	91
C.5	Average and asymptotic (steady state) availability calculations	92
C.6	Frequency calculations.....	93
C.7	Reliability calculations	94
Annex D (informative)	Importance factors	96
D.1	General.....	96
D.2	Vesely-Fussell importance factor	96
D.3	Birnbaum importance factor or marginal importance factor	96
D.4	Lambert importance factor or critical importance factor	97
D.5	Diagnostic importance factor	97
D.6	Risk achievement worth	98
D.7	Risk reduction worth.....	98
D.8	Differential importance measure	98
D.9	Remarks about importance factors.....	99
Annex E (informative)	RBD driven Petri nets	100
E.1	General.....	100
E.2	Example of sub-PN to be used within RBD driven PN models	100
E.3	Evaluation of the DRBD state	102
E.4	Availability, reliability, frequency and MTTF calculations	104
Annex F (informative)	Numerical examples and curves	105
F.1	General.....	105
F.2	Typical series RBD structure	105
F.2.1	Non-repaired blocks	105
F.2.2	Repaired blocks	106
F.3	Typical parallel RBD structure	107
F.3.1	Non-repaired blocks	107
F.3.2	Repaired blocks	108
F.4	Complex RBD structures	109
F.4.1	Non series-parallel RBD structure.....	109
F.4.2	Convergence to asymptotic values versus MTTR	110
F.4.3	System with periodically tested components	111
F.5	Dynamic RBD example.....	113
F.5.1	Comparison between analytical and Monte Carlo simulation results	113
F.5.2	Dynamic RBD example.....	113
Bibliography		116
Figure 1	– Shannon decomposition of a simple Boolean expression and resulting BDD	18
Figure 2	– Series reliability block diagram	25
Figure 3	– Parallel reliability block diagram	26

Figure 4 – Parallel structure made of duplicated series sub-RBD	26
Figure 5 – Series structure made of parallel reliability block diagram.....	27
Figure 6 – General series-parallel reliability block diagram	27
Figure 7 – Another type of general series-parallel reliability block diagram	27
Figure 8 – 2 out of 3 redundancy.....	28
Figure 9 – 3 out of 4 redundancy.....	28
Figure 10 – Diagram not easily represented by series/parallel arrangement of blocks	28
Figure 11 – Example of RBD implementing dependent blocks	29
Figure 12 – Example of a composite block.....	29
Figure 13 – Use of transfer gates and sub-RBDs	30
Figure 14 – Analogy between a block and an electrical switch.....	30
Figure 15 – Analogy with an electrical circuit	31
Figure 16 – Example of minimal success path (tie set).....	31
Figure 17 – Example of minimal failure path (cut set).....	31
Figure 18 – Equivalent RBDs with minimal success paths	32
Figure 19 – Equivalent RBDs with minimal cut sets.....	33
Figure 20 – Link between a basic series structure and probability calculations	33
Figure 21 – Link between a parallel structure and probability calculations	34
Figure 22 – "Availability" Markov graph for a simple repaired block	38
Figure 23 – Standby redundancy.....	38
Figure 24 – Typical availability of a periodically tested block.....	39
Figure 25 – Example of RBD reaching a steady state.....	41
Figure 26 – Example of RBD with recurring phases	41
Figure 27 – RBD and equivalent Markov graph for reliability calculations	42
Figure 28 – Illustrating grouping of blocks before reduction.....	44
Figure 29 – Reduced reliability block diagrams	44
Figure 30 – Representation of Figure 10 when item A has failed	45
Figure 31 – Representation of Figure 10 when item A is working.....	45
Figure 32 – RBD representing three redundant items.....	46
Figure 33 – Shannon decomposition equivalent to Table 5.....	49
Figure 34 – Binary decision diagram equivalent to Table 5.....	49
Figure 35 – RBD using an arrow to help define system success	51
Figure 36 – Alternative representation of Figure 35 using repeated blocks and success paths.....	51
Figure 37 – Other alternative representation of Figure 35 using repeated blocks and minimal cut sets.....	52
Figure 38 – Shannon decomposition related to Figure 35.....	53
Figure 39 – 2-out-of-5 non-identical items	54
Figure 40 – Direct and inverted block	55
Figure 41 – Example of electrical circuit with a commutator A	55
Figure 42 – Electrical circuit: failure paths	55
Figure 43 – Example RBD with blocks with inverted states.....	56
Figure 44 – BDD equivalent to Figure 43	57
Figure 45 – Symbol for external elements.....	58

Figure 46 – Dynamic interaction between a CCF and RBDs' blocks.....	60
Figure 47 – Various ways to indicate dynamic interaction between blocks	60
Figure 48 – Dynamic interaction between a single repair team and RBDs' blocks	60
Figure 49 – Implementation of a PAND gate	61
Figure 50 – Equivalent finite-state automaton and example of chronogram for a PAND gate	61
Figure 51 – Implementation of a SEQ gate	61
Figure 52 – Equivalent finite-state automaton and example of chronogram for a SEQ gate	62
Figure B.1 – Examples of minimal tie sets (success paths)	68
Figure B.2 – Examples of non-minimal tie sets (non minimal success paths)	68
Figure B.3 – Examples of minimal cut sets	69
Figure B.4 – Examples of non-minimal cut sets.....	69
Figure B.5 – Example of RBD with tie and cut sets of various order	70
Figure B.6 – Reminder of the RBD in Figure 35	82
Figure B.7 – Shannon decomposition of the Boolean function represented by Figure B.6.....	82
Figure B.8 – Identification of the parts which do not matter	83
Figure B.9 – Simplification of the Shannon decomposition	83
Figure B.10 – Binary decision diagram related to the RBD in Figure B.6.....	84
Figure B.11 – Obtaining success paths (tie sets) from an RBD.....	84
Figure B.12 – Obtaining failure paths (cut sets) from an RBD.....	85
Figure B.13 – Finding cut and tie sets from BDDs	85
Figure B.14 – Probabilistic calculations from a BDD.....	86
Figure B.15 – Calculation of conditional probabilities using BDDs	87
Figure C.1 – Principle of time dependent availability calculations	88
Figure C.2 – Principle of RBD driven Markov processes	91
Figure C.3 – Typical availability of RBD with quickly repaired failures	91
Figure C.4 – Example of simple multi-phase Markov process	92
Figure C.5 – Typical availability of RBD with periodically tested failures.....	92
Figure E.1 – Example of a sub-PN modelling a DRBD block.....	100
Figure E.2 – Example of a sub-PN modelling a common cause failure.....	101
Figure E.3 – Example of DRBD based on RBD driven PN	101
Figure E.4 – Logical calculation of classical RBD structures.....	102
Figure E.5 – Example of logical calculation for an n/m gate	102
Figure E.6 – Example of sub-PN modelling a PAND gate with 2 inputs	103
Figure E.7 – Example of the inhibition of the failure of a block	104
Figure E.8 – Sub-PN for availability, reliability and frequency calculations.....	104
Figure F.1 – Availability/reliability of a typical non-repaired series structure	105
Figure F.2 – Failure rate and failure frequency related to Figure F.1	106
Figure F.3 – Equivalence of a non-repaired series structure to a single block.....	106
Figure F.4 – Availability/reliability of a typical repaired series structure	106
Figure F.5 – Failure rate and failure frequency related to Figure F.4	107
Figure F.6 – Availability/reliability of a typical non-repaired parallel structure	107
Figure F.7 – Failure rate and failure frequency related to Figure F.6	108
Figure F.8 – Availability/reliability of a typical repaired parallel structure	108

Figure F.9 – Vesely failure rate and failure frequency related to Figure F.8	109
Figure F.10 – Example 1 from 7.5.2	109
Figure F.11 – Failure rate and failure frequency related to Figure F.10.....	110
Figure F.12 – Impact of the MTTR on the convergence quickness.....	111
Figure F.13 – System with periodically tested blocks	112
Figure F.14 – Failure rate and failure frequency related to Figure F.13.....	112
Figure F.15 – Analytical versus Monte Carlo simulation results	113
Figure F.16 – Impact of CCF and limited number of repair teams	114
Figure F.17 – Markov graphs modelling the impact of the number of repair teams	115
Figure F.18 – Approximation for two redundant blocks.....	115
Table 1 – Acronyms used in IEC 61078	18
Table 2 – Symbols used in IEC 61078.....	19
Table 3 – Graphical representation of RBDs: Boolean structures	21
Table 4 – Graphical representation of RBDs: non-Boolean structures/DRBD	22
Table 5 – Application of truth table to the example of Figure 32	46
Table 6 – Karnaugh map related to Figure 10 when A is in up state	48
Table 7 – Karnaugh map related to Figure 10 when A is in down state	48
Table 8 – Karnaugh map related to Figure 35.....	53
Table A.1 – Example of equations for calculating the probability of success of basic configurations.....	63
Table F.1 – Impact of functional dependencies	114

INTERNATIONAL ELECTROTECHNICAL COMMISSION

RELIABILITY BLOCK DIAGRAMS

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 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 third edition cancels and replaces the second edition published in 2006. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- a) the structure of the document has been entirely reconsidered, the title modified and the content extended and improved to provide more information about availability, reliability and failure frequency calculations;
- b) Clause 3 has been extended and clauses have been introduced to describe the electrical analogy, the "non-coherent" RBDs and the "dynamic" RBDs;
- c) Annex B about Boolean algebra methods has been extended;
- d) Annex C (Calculations of time dependent probabilities), Annex D (Importance factors), Annex E (RBD driven Petri net models) and Annex F (Numerical examples and curves) have been introduced.

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

FDIS	Report on voting
56/1685/FDIS	56/1694/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.

The committee has decided that the contents of this publication will remain unchanged until the stability 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

A reliability block diagram (RBD) is a pictorial representation of a system's successful functioning. It shows the logical connection of (functioning) components (represented by blocks) needed for successful operation of the system (hereafter referred to as "system success"). Therefore an RBD is equivalent to a logical equation of Boolean variables and the probabilistic calculations are primarily related to constant values of the block success/failure probabilities.

Many different analytical methods of dependability analysis are available, of which the RBD is one. Therefore, the purpose of each method and their individual or combined applicability in evaluating the availability, reliability, failure frequency and other dependability measures as may be applicable to a given system or component should be examined by the analyst prior to deciding to use 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.

Provided that the blocks in the RBD behave independently from each other and that the order in which failures occur does not matter then the probabilistic calculations can be extended to time dependent probabilistic calculations involving non-repaired as well as repaired blocks (e.g. blocks representing non-repaired or repaired components). In this case three dependability measures related to the system successful functioning have to be considered: the reliability itself, $R_S(t)$, but also the availability, $A_S(t)$ and the failure frequency, $w_S(t)$. While, for systems involving repaired components, the calculations of $A_S(t)$ or $w_S(t)$ can be done quite straightforwardly, the calculation of $R_S(t)$ implies systemic dependencies (see definition 3.34) which cannot be taken into account within the mathematical framework of RBDs. Nevertheless, in particular cases, approximations of $R_S(t)$ are available.

The RBD technique is linked to fault tree analysis [1]¹ and to Markov techniques [2]:

- The underlying mathematics is the same for RBDs and fault tree analysis (FTA): when an RBD is focused on system success, the FT is focused on system failure. It is always possible to transform an RBD into an FT and vice versa. From a mathematical point of view, RBD and FT models share dual logical expressions. Therefore, the mathematical developments and the limitations are similar in both cases.
- When the availability $A_i(t)$ of one block can be calculated by using an individual Markov process [2] independent of the other blocks, this availability, $A_i(t)$, can be used as input for the calculations related to an RBD including this block. This approach where an RBD provides the logic structure and Markov processes numerical values of the availabilities of the blocks is called "RBD driven Markov processes".

For systems where the order of failures is to be taken into account, or where the repaired blocks do not behave independently from each other or where the system reliability, $R_S(t)$, cannot be calculated by analytical methods, Monte Carlo simulation or other modelling techniques, such as dynamic RBDs, Markov [2] or Petri net techniques [3], may be more suitable.

¹ Numbers in square brackets refer to the Bibliography.

RELIABILITY BLOCK DIAGRAMS

1 Scope

This International Standard describes:

- the requirements to apply when reliability block diagrams (RBDs) are used in dependability analysis;
- the procedures for modelling the dependability of a system with reliability block diagrams;
- how to use RBDs for qualitative and quantitative analysis;
- the procedures for using the RBD model to calculate availability, failure frequency and reliability measures for different types of systems with constant (or time dependent) probabilities of blocks success/failure, and for non-repaired blocks or repaired blocks;
- some theoretical aspects and limitations in performing calculations for availability, failure frequency and reliability measures;
- the relationships with fault tree analysis (see IEC 61025 [1]) and Markov techniques (see IEC 61165 [2]).

2 Normative references

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

IEC 60050-192, *International Electrotechnical Vocabulary – Part 192: Dependability* (available at <http://www.electropedia.org>)

IEC 61703, *Mathematical expressions for reliability, availability, maintainability and maintenance support terms*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050-192 as well as the following apply.

NOTE Some terms have been taken from IEC 60050-192 and modified for the needs of this standard.

3.1

reliability block diagram

RBD

logical, graphical representation of a system showing how the success states of its sub-items (represented by blocks) and combinations thereof, affect system success state

Note 1 to entry: The RBD technique was developed a long time ago when the term “reliability” was used as an umbrella term for “successful functioning”. This umbrella term is now superseded by “dependability”. Nevertheless it is still in use in the vernacular language and terms like “reliability engineering”, “reliability studies” or “reliability block diagram”. Therefore the term “reliability” used in RBD does not mean that this technique allows to calculate the reliability of a complex system straightforwardly from reliabilities of its constituting blocks (see 10.3.1.4).

Note 2 to entry: An RBD is a directed acyclic graph (i.e. a graph without loops) representing the logical links between the success state of a system and the success states of its constituting blocks. This logical architecture is mainly represented by conventional series and parallel graphical structures (see Clause 4 and Clause 7).

Note 3 to entry: RBDs may be extended to represent multi-state (i.e. more than two states) systems but those extensions cannot be handled within the Boolean framework.

[SOURCE: IEC 60050-192:2015, 192-11-03, modified – Notes added]

3.2

Boolean related model

mathematical model where the state of a system is represented by a logical function of Boolean variables representing the states of its components

Note 1 to entry: A Boolean variable a only has two values and a logical function of several Boolean variables also has only two values. Those two values may be for example, {0, 1}, {up, down}, {true, false}, {working, failed}, etc. The underlying mathematics behind the logical functions is Boolean algebra.

3.3

RBD driven Markov process

Markov process modelled by an RBD made of blocks modelled by individual sub-Markov models behaving independently from each other

Note 1 to entry: The underlying logic of an RBD allows to combine the individual availabilities of the blocks to obtain the system availability. When the block are modelled by small individual Markov processes (e.g. with less than 10 states) the RBD is equivalent to the Markov process related to the system which may encompass millions of states. This is the basis for most of the probabilistic calculations achieved with RBDs. Such Markov process built through the use of the RBD as guideline is called "RBD driven Markov process".

Note 2 to entry: The independent Markov process is developed in [2].

3.4

dynamic RBD

DRBD

reliability block diagram where the assumption of independency between the blocks is not fulfilled

Note 1 to entry: The blocks of a DRBD can have interactions with elements external to the RBD itself.

3.5

non-coherent RBD

reliability block diagram modelling a non-monotonic logical function

Note 1 to entry: A non-coherent RBD is an RBD where the blocks may appear both in direct and inverted states (see Table 3). In this case, some of the minimal success path (see definition 3.15) may have some blocks in down state and some minimal failure paths, some blocks in up state. The concepts of minimal tie and cut sets are no longer valid and have to be replaced by the concept of prime implicants.

Note 2 to entry: In a non-coherent RBD, a minimal success path may become a failure path by the repair of a block in down state and a minimal failure path may become a success path by a further failure of one block in up state. This is why they are named "non-coherent".

3.6

item

subject being considered

Note 1 to entry: In this International Standard the word "item" covers mainly the system modelled by the RBD and the "blocks" in the RBD.

[SOURCE: IEC 60050-192:2015, 192-01-01, modified – Notes to entry have been deleted, Note 1 to entry has been added]

3.7

block

basic element used to build an RBD

Note 1 to entry: A block has only two states (up and down) and may represent any item with two states (e.g. components, functions, subsystems) repaired or not repaired. By analogy and to simplify the wording, a repaired/non-repaired block represents a repaired/non-repaired item, the failure/repair of a block represents the

failure/repair of the modelled item and the up/down state of a block represents the up/down state of the modelled item.

Note 2 to entry: The number of states may be extended to more than two states in order to represent multi-state (i.e. more than two states) systems but those extensions cannot be handled within the Boolean framework.

Note 3 to entry: For the purposes of this standard, the blocks are divided between "elementary blocks" – or more simply, "blocks" – and "composite blocks" comprising several "elementary blocks". This is illustrated in Table 3.

3.8

repeated block

block appearing more than once in an RBD

Note 1 to entry: Repeated blocks represent the same physical items. This should not be confused with duplicated blocks which represent different but similar physical items used to implement redundancy.

Note 2 to entry: Repeated blocks can appear in the direct or inverted state (i.e.; the block appears in up state in a part of the RBD and down state in another part, or vice versa). They are very useful to represent RBDs related to a complex system or for representing RBDs in the form of success or failure paths (see 8.2).

3.9

up state

available state

state of being able to perform as required

Note 1 to entry: The absence of necessary external resources may prevent operation, but do not affect the up state.

Note 2 to entry: Up state relates to availability of the item.

Note 3 to entry: An item may be considered to be in an up state for some functions and in a down state for others, concurrently.

Note 4 to entry: The adjectives "up" and "available" designate an item in an up state.

Note 5 to entry: Within the context of RBDs, the state of a block is identical to the state of the component modelled by this block. Therefore a block in up state refers to a component in up state. The same concept applies to the RBD and the corresponding system.

Note 6 to entry: Within an RBD and by analogy with an electrical circuit, a block in the up state can be considered as a virtual switch in closed position and a block in the down state as a virtual switch in open position.

[SOURCE: IEC 60050-192:2015, 192-02-01, modified – Note 5 to entry and Note 6 to entry have been added]

3.10

up time

time interval for which the item is in an up state

[SOURCE: IEC 60050-192:2015, 192-02-02]

3.11

mean up time

MUT

expectation of the up time

[SOURCE: IEC 60050-192:2015, 192-08-09]

3.12

down state

unavailable state

state of being unable to perform as required, due to internal fault, or preventive maintenance

Note 1 to entry: "Down" state relates to unavailability of the item.

Note 2 to entry: The adjectives "down" or "unavailable" designate an item in a down state

Note 3 to entry: Within the context of RBDs, the state of a block (respectively an RBD) is assimilated to the state of the component (respectively the system) modelled by this block (respectively this RBD). Therefore a block (respectively an RBD) in down state refers to a component (respectively a system) in down state.

Note 4 to entry: Within an RBD, a block in the down state may be interpreted as an open electrical switch.

[SOURCE: IEC 60050-192:2015, 192-02-20, modified – Note 3 and 4 to entry have been added]

3.13

down time

time interval for which the item is in a down state

[SOURCE: IEC 60050-192:2015, 192-02-21, modified – the figure and Note 1 to entry have been deleted]

3.14

mean down time

MDT

expectation of the down time

[SOURCE: IEC 60050-192:2015, 192-08-10]

3.15

success path

tie set

set of blocks, with each block in the set being in the up state thus resulting in the RBD to be in the up state

Note 1 to entry: The name tie set is given by analogy with an electrical circuit: the blocks in up states constitute a closed (tied) circuit between the RBD input and the RBD output.

3.16

minimal tie set

tie set such as that any failure of one of the blocks in up state also fails the whole RBD

Note 1 to entry: In a minimal tie set, every block in up state is necessary to retain the RBD in up state.

Note 2 to entry: The order of a minimal tie set is given by the number of blocks in the set in up state: order 1 comprises 1 block in up state, order 2 comprises 2 blocks in up state, etc.

3.17

failure path

cut set

set of blocks, with each block in the set being in the down state thus resulting in the RBD to be in the down state

Note 1 to entry: The name cut set is given by analogy with an electrical circuit: the blocks in down state constitute an open (cut) circuit between the RBD input and the RBD output.

3.18

minimal cut set

cut set such as that any restoration of one of the blocks in down state also restore the RBD to up state

Note 1 to entry: In a minimal cut set, every block in down state is necessary to retain the RBD in down state

Note 2 to entry: The order of a minimal cut set is given by the number of blocks in the down state: order 1 comprises 1 block in down state, order 2 comprises 2 blocks in down state, etc.

3.19

disjoint set of elements

set of Boolean elements whose intersections are empty

EXAMPLE If (C_i^d) is a set of disjoint cut sets then $C_i^d \cap C_j^d = \emptyset \quad \forall i \neq j$ and therefore, the probability $P(C_i^d \cap C_j^d) = 0 \quad \forall i \neq j$.

Note 1 to entry: The term "element" is used here in the general meaning used in the set theory, i.e. a member of a given collection of objects.

Note 2 to entry: Disjoint elements are incompatible: when one is true, the other is false and vice versa. This describes mutual exclusiveness and, therefore, complete dependency between the elements.

3.20

availability

<item> ability to be in up state

[SOURCE: IEC 60050-192:2015, 192-01-23, modified – notes have been deleted]

3.21

$A(t)$

instantaneous availability

point availability

<measure> probability of being in up state at a given instant

[SOURCE: IEC 60050-192:2015, 192-08-01, modified]

3.22

$U(t)$

instantaneous unavailability

point unavailability

<measure> probability of being in down state at a given instant

[SOURCE: IEC 60050-192:2015, 192-08-04, modified]

3.23

$A^{avg}(t_1, t_2)$

mean availability

average availability

<measure> average value of the instantaneous availability over a given time interval $[t_1, t_2]$

[SOURCE: IEC 60050-192:2015, 192-08-05, modified – Note 1 to entry has been deleted]

3.24

$U^{avg}(t_1, t_2)$

mean unavailability

average unavailability

<measure> average value of the instantaneous unavailability over a given time interval (t_1, t_2)

Note 1 to entry: The mean unavailability of a safety instrumented system (see IEC 61508 [5]) is also called "average probability of failure on demand" (Acronym: PFD_{avg}).

[SOURCE: IEC 60050-192:2015, 192-08-06, modified – Note 1 to entry has been replaced]

3.25

A^{st}

A^{as}

steady state availability

asymptotic availability

limit, if it exists, of the instantaneous availability, when the time tends to infinity

Note 1 to entry: Under certain conditions, the steady state availability may be expressed as the quotient $MUT/(MUT+MDT)$. See IEC 61703.

[SOURCE: IEC 60050-192:2015, 192-08-07, modified – Note 1 to entry modified]

3.26

reliability

<item> ability to perform as required, without failure, for a given time interval, under given conditions

[SOURCE: IEC 60050-192:2015, 192-01-24, modified – Notes to entry have been deleted]

3.27

$R(t_1, t_2)$

$R(t)$

reliability

<measure> probability of performing as required for time interval $[t_1, t_2]$, under given conditions

Note 1 to entry: The reliability $R(t)$ is the reliability for the time interval $[0, t]$.

[SOURCE: IEC 60050-192:2015, 192-01-24, modified – Notes to entry were replaced by new Note 1 to entry]

3.28

$F(t_1, t_2)$

$F(t)$

unreliability

<measure> probability of not performing as required for time interval $[t_1, t_2]$, under given conditions

Note 1 to entry: The unreliability $F(t)$ is the unreliability for the time interval $[0, t]$.

Note 2 to entry: The unreliability is the complement to 1 of the reliability: $F(t)=1-R(t)$.

3.29

$\lambda(t)$

instantaneous failure rate

failure rate

limit, if it exists, of the quotient of the conditional probability that an item goes from up state to down state within time interval $[t, t + \Delta t]$, and Δt , when Δt tends to zero, given that it has not been in down state within time interval $[0, t]$

Note 1 to entry: The definition has been adapted from IEC 60050-192 to also cover repairable items:

- if the item has no internal built-in redundancy, the failure rate is identical to what it would be if it was not repairable;
- if the item has built-in internal redundancy it can remain in up state when some redundant parts are failed. Therefore, those failures are repairable as long as the whole item has no transition to the down state due to a further part failure.

Note 2 to entry: The terms failure rate (3.29), conditional failure intensity (3.30) and unconditional failure intensity (3.31) seem similar but they differ by the conditional events used in their definitions. Even if these parameters can have close numerical values in particular cases, they behave in different ways and should not be confused with each other.

[SOURCE: IEC 60050-192:2015, 192-05-06, modified – Notes to entry have been replaced by new notes to entry]

3.30 $\lambda_v(t)$ **instantaneous conditional failure intensity****conditional failure intensity****Vesely failure rate**

limit, if it exists, of the quotient of the conditional probability that the failure of an item occurs within time interval $[t, t + \Delta t]$, and Δt , when Δt tends to zero, given that the item was in up state at time t and at time 0

Note 1 to entry: See Note 2 to entry of the failure rate definition (3.29).

3.31 $w(t)$ **instantaneous unconditional failure intensity****unconditional failure intensity****failure frequency**

limit, if it exists, of the quotient of the conditional probability that the failure of an item occurs within time interval $[t, t + \Delta t]$, and Δt , when Δt tends to zero, given that the item was in up state at time 0

Note 1 to entry: See Note 2 to entry of the failure rate definition (3.29).

Note 2 to entry: This parameter is equivalent to the failure intensity defined in IEC 60050-192:2015, 192-05-08. The name has been modified to distinguish it from the term, conditional failure intensity (3.30).

3.32 $w^{\text{avg}}(0, T)$ **average failure frequency**

number of failures per unit of time of an item averaged over a given period of time T

Note 1 to entry: If N is the number of failures of the item over $[0, T]$ then the average failure frequency over this period of time is calculated as $w^{\text{avg}}(0, T) = N/T$.

Note 2 to entry: If m is the mean time between failures (see IEC 60050-192) of an item then the average number of failures occurring over $[0, T]$ is $N \approx T/m$. Therefore $w^{\text{avg}}(0, T) = N/T \approx 1/m$.

Note 3 to entry: Mathematically speaking, $w^{\text{avg}}(0, T)$ is the average of $w(t)$ over $[0, T]$. Then

$$w^{\text{avg}}(0, T) = \frac{1}{T} \int_0^T w(\tau) d\tau.$$

3.33**mean operating time to failure****MTTF**

expectation of operating time to failure

Note 1 to entry: In the case of non-repairable items with an exponential distribution of times to failure (thus a constant failure rate) the MTTF is numerically equal to the reciprocal of the failure rate. This is also true for repairable items if, after restoration, they can be considered to be “as-good-as-new”.

Note 2 to entry: This note only applies to the French language.

[SOURCE IEC 60050-192, 192-05-11, modified – Note 2 to entry has been deleted]

3.34**systemic dependency****holistic dependency**

dependency between the parts of a system which are related to the system considered as a whole

EXAMPLE 1 A single repair team constitutes a systemic dependency between repairable items: when an item fails it can be repaired only if the repair team is not busy due to the repair of another item belonging to the system.

EXAMPLE 2 The reliability $R(t)$ of a system can be expressed as the probability for the system to be in up state at time t , provided it has never been in down state over the interval $[0, t]$. Therefore only the sequences of events

which do not lead to the down state over $[0, t]$ can be retained and the sequences of events which include a succession "up state"→"down state"→"up state" have to be excluded from the calculations. This implies that, with regards to the calculation of $R(t)$, an item going to the down state is repairable only if the system remains in up state during the repair of the item. Therefore, with regards to the calculation of $R(t)$, the items are repairable or not depending on the states of the other blocks and this constitutes systemic dependencies between all blocks of the RBD modelling the system.

Note 1 to entry: A systemic dependency cannot be described as a local property of the individual items of the system.

3.35

binary decision diagram

BDD

compact decision tree based on the Shannon decomposition of a Boolean expression

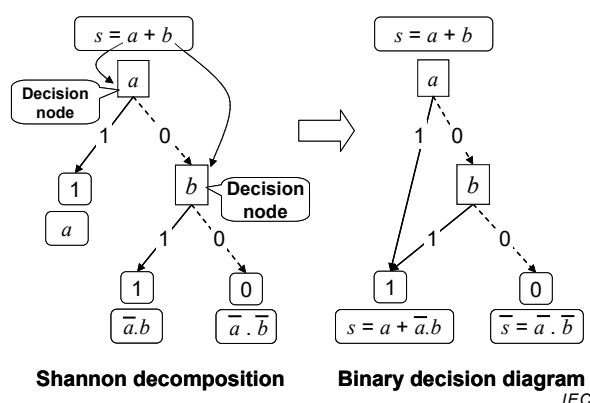


Figure 1 – Shannon decomposition of a simple Boolean expression and resulting BDD

Note 1 to entry: Figure 1 illustrates how the simple Boolean expression $s = a + b$ can be transformed into a decision tree by using the Shannon decomposition and then how the corresponding BDD is obtained by gathering the paths giving the same value (0 or 1) of the Boolean expression.

Note 2 to entry: Mathematically speaking, BDDs are rooted, directed acyclic graphs. This is a data structure expressing Boolean expressions as unions of disjointed terms. This, in turn, leads to exact probabilistic calculations. This is the state of the art with regards to probabilistic calculation on Boolean related models. More details about BDDs can be found in reference [33].

Note 3 to entry: This note only applies to the French language.

4 Symbols and abbreviated terms

Table 1 – Acronyms used in IEC 61078

Abbreviation/Acronym	Meaning
BDD	Binary decision diagram.
CCF	Common cause failure.
FMEA	Failure modes and effects analysis.
FT, FTA	Fault tree, fault tree analysis.
MTTF	Mean operating time to failure.
MTTR	Mean time to restoration.
DRBD	Dynamic reliability block diagram.
PFD_{avg}	Average of the probability of failure on demand (mean unavailability).
PAND	Priority AND gate.
PN	Petri net.
RBD	Reliability block diagram.
SEQ	Sequential gate.

Table 2 – Symbols used in IEC 61078

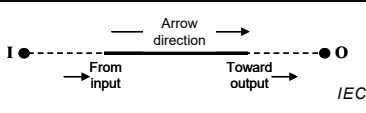
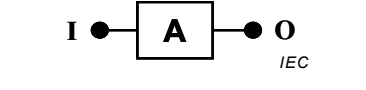
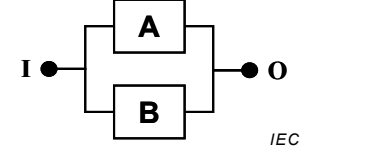
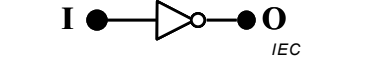
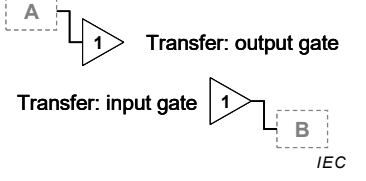
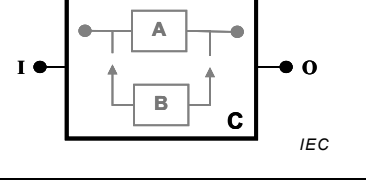
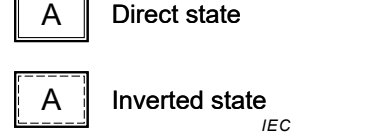
Symbol	Meaning
S	System modelled by an RBD.
$X \in (A, B, C, \dots), X \neq S$	Blocks used within an RBD. S is reserved for the system and the other letters for the blocks.
$s = S$ in "up" state	Boolean variable indicating that the system S is in the up state. This is also the event "S in up state".
$\bar{s} = S$ in "down" state	Boolean variable indicating that the system S is in the down state. This is also the event "S in down state".
$x = X$ in "up" state	Boolean variable indicating that block X is in the up state. This is also the event "X in up state".
$\bar{x} = X$ in "down" state	Boolean variable indicating that block X is in the down state. This is also the event "X in down state".
$(\Pi_i), (C_i)$	Minimal success paths (minimal tie sets), minimal failure paths (minimal cut sets).
$(\Pi_i^d), (C_i^d)$	Disjoint success paths (disjoint tie sets), disjoint failure paths (disjoint cut sets).
$P(\cdot)$	Probability function.
$P_s = P(S \text{ in "up" state})$	Constant probability that the system S is in the up state.
$P_{\bar{s}} = P(S \text{ in "down" state})$	Constant probability that the system S is in the down state.
$P_x = P(X \text{ in "up" state})$	Constant probability that block X is in the up state.
$P_{\bar{x}} = P(X \text{ in "down" state})$	Constant probability that block X is in the down state.
$P_{s x} = P(S \text{ in "up" state} \mid X \text{ in "up" state})$	Conditional probability that the system S is in the up state given that block X is in the up state.
$P_{s \bar{x}} = P(S \text{ in "up" state} \mid X \text{ in "down" state})$	Conditional probability that the system S is in the up state given that block X is in down state.
$P_s(t)$	Time dependent probabilities that the system S is in the up state.
$P_x(t)$	Time dependent probability that block X is in the up state.
$P_{\bar{s}}(t)$	Time dependent probabilities that the system S is in the down state.
$P_{\bar{x}}(t)$	Time dependent probability that block X is in the down state.
$P(OK, t)$	Probability of state OK at time t .
t, t_i	Current instant of time.
T, T_i	Time duration.
$[t_1, t_2], [0, T] \equiv [t_1 = 0, t_2 = 0 + T]$	Time interval, $t_1 < t_2$
$A_S(t) = P(S \text{ in "up" state at time } t)$	Availability of the system S at time t .
$A_S^{\text{avg}}(t_1, t_2), A_S^{\text{avg}}(0, T), A_S^{\text{avg}}(T)$	Average availability of the system S over the time interval $[t_1, t_2]$ or $[0, T]$.
$A_S^{\text{avg}}, A_S^{\text{st}}, A_S^{\text{as}}$	Average availability of the system S over $[0, \infty]$, steady state availability and asymptotic availability.
$A_X(t) = P(X \text{ in "up" state at time } t)$	Availability of block X at time t .
$A_i(t) = A_{X_i}(t) = P(X_i \text{ in "up" state at time } t)$	Availability of block X_i at time t .
$A_X^{\text{avg}}(t_1, t_2), A_X^{\text{avg}}(0, T), A_X^{\text{avg}}(T)$	Average availability of block X over the time interval $[t_1, t_2]$ or $[0, T]$.

Symbol	Meaning
$A_X^{\text{avg}}, A_X^{\text{st}}, A_X^{\text{as}}$	Average availability of block X over $[0, \infty]$, steady state availability and asymptotic availability.
$U_S(t) = P(\text{S in "down" state at time } t)$	Unavailability of the whole system S at time t .
$U_S^{\text{avg}}(t_1, t_2), U_S^{\text{avg}}(0, T), U_S^{\text{avg}}(T)$	Average unavailability of the system S over the time interval $[t_1, t_2]$ or $[0, T]$.
$U_S^{\text{avg}}, U_S^{\text{st}}, U_S^{\text{as}}$	Average unavailability of the system S over $[0, \infty]$, steady state unavailability and asymptotic unavailability.
$U_X(t) = P(\text{X in "down" state at time } t)$	Unavailability of block X at time t .
$U_i(t) = U_{X_i}(t) = P(X_i \text{ in "down" state at time } t)$	Unavailability of block X_i at time t .
$U_X^{\text{avg}}(t_1, t_2), U_X^{\text{avg}}(0, T), U_X^{\text{avg}}(T)$	Average unavailability of block X over the time interval $[t_1, t_2]$ or $[0, T]$.
$U_X^{\text{avg}}, U_X^{\text{st}}, U_X^{\text{as}}$	Average unavailability of block X over $[0, \infty]$, steady state unavailability and asymptotic unavailability.
$R_S(t) = P(\text{S in "up" state all over } [0, t])$	Reliability of the system S over $[0, t]$.
$F_S(t) = 1 - R_S(t)$	Unreliability of the overall system S over $[0, t]$ (failure distribution of the system S).
$f_S(t)$	Time to failure density functions of system S.
$R_X(t) = P(\text{X in "up" state all over } [0, t])$	Reliability of block X over $[0, t]$.
$F_X(t) = 1 - R_X(t)$	Unreliability of block X over $[0, t]$ (failure distribution of block X).
$f_X(t)$	Time to failure density functions of block X.
$\lambda_S, \lambda_S(t)$	Constant and time dependent failure rates of the system S.
$\lambda_{VS}, \lambda_{VS}(t)$	Conditional failure intensity (Vesely failure rate) of the overall system.
$w_S(t)$	Unconditional failure intensity (failure frequencies) of the system S, at time t .
$W_S(0, T), W_S(T)$	Expected number of failures of the system S over $[0, T]$.
$w_S^{\text{avg}}(0, T), w_S^{\text{avg}}(T)$	Average unconditional failure intensity (average failure frequency) of the system S over $[0, T]$.
$\lambda_X, \lambda_X(t)$	Constant and time dependent failure rates of block X.
$w_X(t)$	Unconditional failure intensity (failure frequencies) of block X, at time t .
$W_X(0, T), W_X(T)$	Expected number of failures of block X over $[0, T]$.
$w_X^{\text{avg}}(0, T), w_X^{\text{avg}}(T)$	Average unconditional failure intensity (average failure frequency) of block X over $[0, T]$.
λ_{Xd}	Dormant failure rate of block X.
$\mu_X, \mu_X(t)$	Constant or time-dependent repair rates of block X.
$\binom{n}{r}$	Number of ways of selecting r blocks from n blocks without order: $\binom{n}{r} = \frac{n!}{r!(n-r)!}$
"0", "1"	Symbols used in truth tables, Karnaugh map, Shannon decomposition and binary decision diagrams to denote down (failure) states and up (success) states of blocks or of systems.
$\cap, \bullet$	Boolean operators denoting AND logic, e.g. $a \cap b, a \bullet b$ (intersection).

Symbol	Meaning
$\cup, +$	Boolean operators denoting OR logic, e.g. $a \cup b, a + b$ (union).
Φ, Ω	"Impossible" event and "certain" events.

The use of the symbols in Table 3 is recommended when drafting a reliability block diagram (RBD).

Table 3 – Graphical representation of RBDs: Boolean structures

Graphical representation	Meaning
	Indicates input. Indicates output. Such indications are used for convenience. They are not mandatory, but may be useful where connections have a directional significance.
	An RBD is a directed graph. The direction of each link is from input to output (i.e., from left to right). When needed, arrows may be added to avoid confusion.
	(Elementary) block: grouping of equipment, components, units or other system elements.
	Series structure: the system is up if A and B are in up states. This represents the logic functions $s = a \cap b$. From a failure point of view it is equivalent to $\bar{s} = \bar{a} \cup \bar{b}$
	Parallel structure (full active redundancy): the system is up if A or B are in up state. This represents the logic functions $s = a \cup b$. From a failure point of view it is equivalent to $\bar{s} = \bar{a} \cap \bar{b}$
	NOT gate: the output of the gate is equal to 0 when its input is equal to 1 and vice-versa.
	Transfer gates: the output ι is linked to the input(s) with the same name. This is useful to: – split large RBDs into several smaller parts (sub-RBDs); – transfer the output at one place in an RBD to another place in the RBD.
	Composite block: grouping of elementary blocks. This may be useful to simplify the RBD drawing, to indicate parts needing further development or to gather non independent individual blocks into a structure independent of the rest of the RBD.
	Repeated blocks: the same block representing a given item appears in several places of the RBD either in the direct state or the inverted state i.e. when the block A in direct state is "up", the block in the inverted state is "down" and vice versa. These symbols are used for non-coherent RBDs.
	External element interacting with one or several blocks of the RBD. This symbol is used for dynamic RBDs.

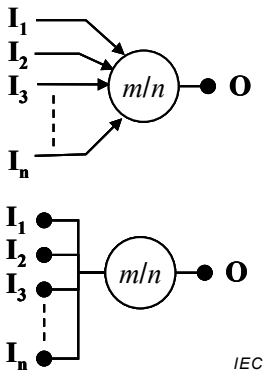
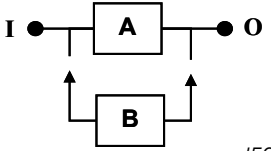
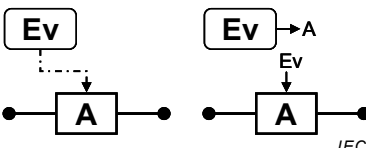
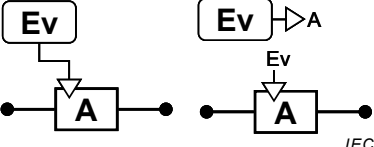
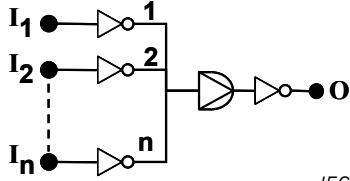
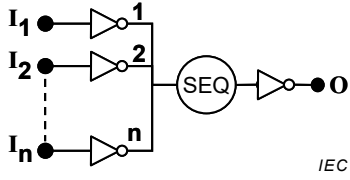
Graphical representation	Meaning
	Success majority vote logic (symbol m/n): at least m-out-of-n blocks are needed for system success in an active redundant configuration. NOTE It is important to make the difference between the "success" majority vote logics implemented in RBDs and the "failure" majority vote logics implemented in fault trees. Generally the context (RBD or fault tree) is sufficient to show the difference. The relationship is the following: $(m/n)_{\text{Suc}} \equiv ([n-m+1]/n)_{\text{Fail}}$.

Table 4 – Graphical representation of RBDs: non-Boolean structures/DRBD

Graphical representation	Meaning
	Standby redundancy: B takes over the function of A when A fails.
	Functional dependencies: the state of A depends on the event Ev. This event may be external or internal to the RBD. This symbol reminds that a dependency exists but the type of dependency may be diverse and has to be described somewhere else.
	Complete functional dependency: when the event Ev occurs, then block A goes to the down state. This event may be external or internal to the RBD. It plays the role of the trigger used in similar structures implemented in dynamic fault trees.
	PAND gate: the output goes to the down state when the inputs go to the down states in the order I_1, then I_2, then I_3, ... then I_n. The inputs I_1, I_2, I_3, ... I_n behave independently from each other. This gate has been introduced to be used in dynamic fault trees and this is why NOT gates are used to invert the inputs and the output in order to be consistent with the RBD logic.
	SEQ gate: the output goes to the down state when the inputs go to the down states in the order I_1, then I_2, then I_3, ... then I_n. The inputs don't behave independently as I_n cannot go to the down state if I_{n-1} is not already in the down state, I_{n-1} cannot go to the down state if I_{n-2} is not already in the down state, etc., I_2 cannot go to the down if I_1 is not already in the down state. This gate has been introduced to be used in dynamic fault trees and this is why NOT gates are used to invert the inputs and the output in order to be consistent with the RBD logic.

5 Preliminary considerations, main assumptions, and limitations

5.1 General considerations

An RBD models a system using the logical links existing between the success state (up state) of the system (i.e., the overall RBD) and the success states (up states) of its components.

(i.e., the blocks of the RBD). Therefore, an RBD embeds a logical formula and this is why an RBD is not necessarily similar to the physical architecture of the system (e.g. two redundant isolation valves in series on the same pipe are represented by two blocks in parallel into the corresponding RBD).

An RBD can be firstly used for qualitative analysis purposes by identifying the combinations of the blocks in the up state allowing the system to be in an up state (success paths or tie sets) or the combinations of the blocks being in down states leading to the system down state (failure paths or cut sets).

Secondly an RBD can be used for probabilistic calculations and, as this is a static representation (i.e., independent of the time), the probabilistic rules are basically related to blocks with constant probabilities of success or failure.

This can be extended to time dependent probabilistic calculations. This may be difficult for reliability calculations but, for availability and frequency calculations and provided that the blocks behave independently from each other, there is no restriction, other than mathematical tractability, on the distribution that may be used to describe the times to failure or repair of the blocks. This allows, for example, to model the (un)availabilities of each of the blocks by individual analytical formulae whose results are combined through the logic of the RBD to obtain the system (un)availability. When those analytical formulae are obtained through individual Markov processes, the RBD is equivalent to a global Markov process modelling the whole system. Such a model is called "RBD driven Markov process". This is the basis for most of the probabilistic calculations achieved with RBDs.

5.2 Pre-requisite/main assumptions

An RBD is an acyclic directed graph (i.e. no loops or retroactions are modelled in an RBD) which can be drawn by using the basic logical structures presented in Table 3. It is used to model the behaviour of a system on the basis of the following fundamental assumptions:

- a) the system has only two states: working ("success" state, "up" state) or failed ("down" state);
- b) the blocks of an RBD model the components of a system or parts (e.g. groups of components) of a system. Each of them has only two states: working ("success" state, "up" state) or failed ("down" state);
- c) the RBD represents the logic linking the success state of the system to the success states of its components (blocks);
- d) each block behaves independently from the others at all times.

The above assumptions have to be generally fulfilled to apply the analytical calculations (i.e. calculations with formulae) developed in this standard. When they are not fulfilled, the analytical calculations can be replaced by Monte Carlo simulation or other techniques like Markov analysis [2] or Petri nets [3] or the dynamic RBDs described in 12.2 and Annex E.

5.3 Limitations

The assumptions presented in 5.2 constitute some limitations but there are other limitations which are less obvious when dealing with time dependent probabilities. In particular, the users of this standard should be aware of the issues introduced by the independency requirements which shall be fulfilled at all times. For example:

- a) sequential events are outside the scope of the Boolean models. Therefore they cannot, in principle, be handled by RBDs. Nevertheless, in simple cases like standby redundancy, it is possible to overcome the problem by considering composite blocks (see Table 3 and 7.5.3) independently of the other blocks;
- b) availability or frequency calculations of repaired systems assume that the repairs of repaired blocks are independent from each other all the time, i.e. each block has its own repair team;

- c) reliability calculations of repaired systems imply that a failed block can be repaired only if the system is still operating when the block failure occurs. This introduces systemic dependencies between the blocks states, and between the blocks and the system states (see 10.3.1.4). This infringes the assumption described in 5.2 d) and so, except in particular cases and with approximations, analytical reliability calculations are generally not possible.

In short, provided that the assumptions in 5.2 are fulfilled, the RBD technique can be used straightforwardly for qualitative analysis and availability/frequency calculations but it can be used for reliability calculation only in particular cases.

It should be noted that, when dealing with probabilistic calculations, good approximations are available with low probabilities (e.g. failure of components/blocks) which cannot be used with high probabilities (e.g. probabilities of success of components/blocks). Therefore to overcome this limitation, it is often better to work with probabilities of failure (unavailability or unreliability) rather than probabilities of success (availability or reliability).

6 Establishment of system success/failed states

6.1 General considerations

A prerequisite for constructing system reliability models is a sound understanding of the ways in which the system and its components can operate. Systems often require more than one success/failure definition. These should be defined and listed. An RBD diagram can be made at 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.

In addition, there should be clear statements concerning

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

After establishing the system's success/failure definition the next step is to identify logical blocks in order to divide the system as appropriate for the purpose of the reliability analysis. Particular blocks may represent system substructures, which in turn may be represented by other RBDs (system reduction – see 11.2).

For the quantitative evaluation of an RBD, various methods are available. Depending on the type of structure, simple Boolean techniques (see 7) and/or path and cut set analyses (see 8) may be employed. Calculations may be made using analytical methods (e.g. basic component availability methods) or Monte Carlo simulation. An advantage with Monte Carlo simulation is that the probabilities of 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 12.2 and Clause F.5).

Since the RBD describes the logical relations needed for the system to function, the block diagram does not necessarily represent the way in which the hardware is physically connected, although an RBD should generally follow, 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. Therefore, when the same system is

used to perform all these functions, 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 shipboard, in an aircraft or on the ground. When this is so, reliability evaluations may be carried out using the same RBD each time but using the appropriate component/block 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 during non-use periods is negligible, then only the actual working time of the equipment needs to be considered.

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 non-use period than when in-service (e.g. due to moisture and corrosion). In complex cases where only parts of the system are switched on and off, modelling techniques other than RBDs (e.g. Markov analysis or Petri nets) 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 RBD 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. Attempt should be made to make the blocks as large as possible while ensuring that each block contains (preferably) no redundancy.

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" (see 3.15). As indicated in the diagrams that follow, the various success paths, between the input and output of the diagram, pass through those combinations of blocks that need to function in order that the system functions.

NOTE In practice, depending on the system configuration, it can be necessary to make repeated attempts at constructing the RBD (each time bearing in mind the steps referred to above) before a suitable block diagram is finalized.

7.2 Series structures

If all the blocks are required to function for the system to function, then the corresponding RBD will be one in which all the blocks are connected in series as illustrated in Figure 2.

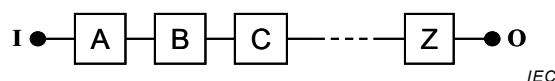


Figure 2 – Series reliability block diagram

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

This structure models the following logical function: $s = a \bullet b \bullet c \bullet \dots \bullet z$ (1)

where a , b , c and z represent the success states of the blocks A, B, C and Z (see Table 2) and s the success state of the corresponding system.

7.3 Parallel structures

A different type of RBD is needed when only one system component (i.e. one block) is required for system success. This is the case when redundant components are implemented.

This is modelled by parallel structures such as that presented in Figure 3 and which represent several redundant blocks. In this structure, the system is down if and only if all blocks are down.

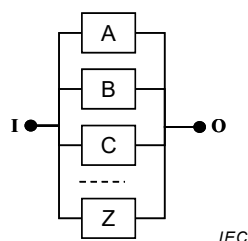


Figure 3 – Parallel reliability block diagram

This structure models the following logical function: $s = a + b + c + \dots + z$ (2)

7.4 Mix of series and parallel structures

The basic structure presented in Figure 2 and Figure 3 can be used to model more complex RBDs. For example, if the entire RBD presented in Figure 2 is duplicated (i.e. made redundant), then the RBD illustrated by Figure 4 is obtained. Alternatively, if each block within the RBD presented in Figure 2 is duplicated, the RBD illustrated by Figure 5 is obtained. Diagrams of this type are known as "series/parallel" RBDs or "series/parallel" models. Note that the terms "duplicated", "redundant" and "parallel" are very similar in meaning but should not be used interchangeably.

- 1) Duplicated is related to the way the RBD is built by repeating similar structures. For example, Figure 4 is the duplication of the structure presented in Figure 2 and Figure 5 is only the duplication of the components. In fact the parallel structures (B1,B2), (C1,C2) etc. are the duplication in series of the parallel structure (A1, A2).
- 2) Redundant is related to the fact that if one component fails, another one can perform its function. For example, A1 and A2 in Figure 5 are redundant.
- 3) Parallel is related to the logic of the architecture of the system and to the graphical representation. For example, A1 and A2 are drawn in parallel in Figure 5 because they are redundant.

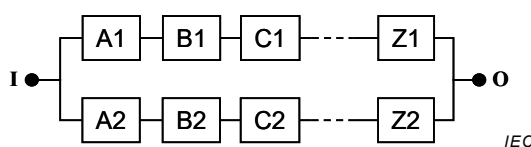


Figure 4 – Parallel structure made of duplicated series sub-RBD

This structure models the following logical function:

$$s = (a_1 \bullet b_1 \bullet \dots \bullet z_1) + (a_2 \bullet b_2 \bullet \dots \bullet z_2) \quad (3)$$

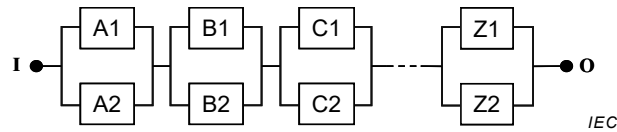


Figure 5 – Series structure made of parallel reliability block diagram

This structure models the following logical function:

$$s = (a_1 + a_2) \bullet (b_1 + b_2) \bullet \dots \bullet (z_1 + z_2) \quad (4)$$

RBDs used for modelling system reliability are often more complicated mixtures of series and parallel structures. For example, a duplicated communication link comprising three repeaters (A1, B1, C1 and A2, B2, C2), and a common power supply block (D) may take the form of, for example, Figure 6 or Figure 7.

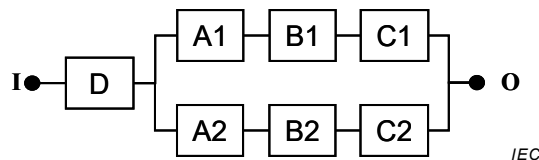


Figure 6 – General series-parallel reliability block diagram

This structure models the following logical function:

$$s = d \bullet [(a_1 \bullet b_1 \bullet c_1) + (a_2 \bullet b_2 \bullet c_2)] \quad (5)$$

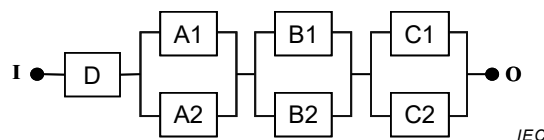


Figure 7 – Another type of general series-parallel reliability block diagram

This structure models the following logical function:

$$s = d \bullet (a_1 + a_2) \bullet (b_1 + b_2) \bullet (c_1 + c_2) \quad (6)$$

On account of the assumed statistical independence stated above, failure of any block does 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 does not affect system power supplies or signal sources.

7.5 Other structures

7.5.1 *m* out of *n* structures

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. Such logical structures are often called "majority vote" structures. For example see RBDs shown in Figure 8 or Figure 9.

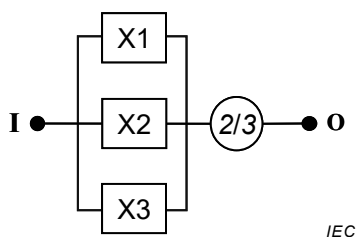


Figure 8 – 2 out of 3 redundancy

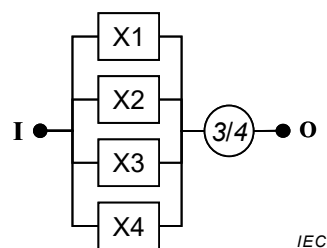


Figure 9 – 3 out of 4 redundancy

Thus, in Figure 8 at least 2 blocks are required for system success and in Figure 9, 3 blocks are required for system success. In both cases the failure of one item is tolerated but failure of two or more items is not.

These structures model the following logical functions:

– 2/3 redundancy: $s = x_1 \bullet x_2 + x_1 \bullet x_3 + x_2 \bullet x_3$; (7)

– 3/4 redundancy: $s = x_1 \bullet x_2 \bullet x_3 + x_1 \bullet x_2 \bullet x_4 + x_1 \bullet x_3 \bullet x_4 + x_2 \bullet x_3 \bullet x_4$. (8)

These logical functions cannot be represented by a simple combination of elementary series and parallel structure without the implementation of repeated blocks.

7.5.2 Structures with common blocks

Most RBDs are easily understood and the conditions for system success are evident. Not all RBDs, however, can be simplified to combinations of series or parallel structures with blocks appearing only once. The RBD in Figure 10 is an example with a block A being common to two paths.

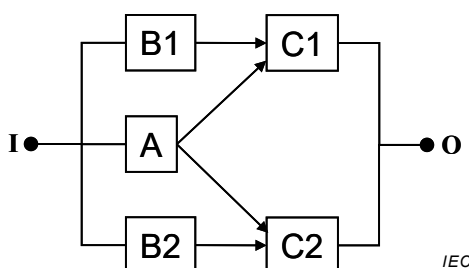


Figure 10 – Diagram not easily represented by series/parallel arrangement of blocks

This structure models the following logical function:

$$s = (b_1 \bullet c_1) + a \bullet (c_1 + c_2) + (b_2 \bullet c_2) \quad (9)$$

Again, the diagram is self-explanatory. System success is achieved if blocks B1 and C1 are both in up state, or blocks A and C1, or A and C2, or finally B2 and C2. Figure 10 could represent the fuel supply to engines of a light aircraft. B1 represents the supply to the port engine (C1), B2 represents the supply to the starboard engine (C2), and A represents a common backup supply to both engines. The system success definition is that at least one engine needs to be working for aircraft success, or alternatively, both engines need to fail for the aircraft to fail.

It should be noted that in all the above diagrams (Figure 2 to Figure 10), 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 8.2. Figure 18 and Figure 19 provide series-parallel RBDs equivalent to Figure 10 where repeated blocks are implemented.

7.5.3 Composite blocks

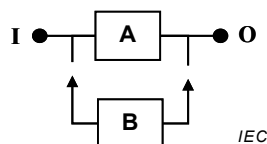


Figure 11 – Example of RBD implementing dependent blocks

Figure 11 models a system with cold standby redundancy where the item B starts when the item A fails and with a perfect switching from A to B. Then in the corresponding RBD, the blocks A and B are not independent and this structure infringes the fundamental assumption of independency between blocks which is the basis of this standard.

As blocks A and B cannot be considered independently from each other, it is necessary to consider them as a whole and this can be done by the use of a composite block like the block C presented in Figure 12.

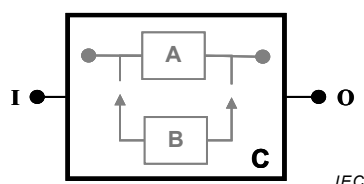


Figure 12 – Example of a composite block

The composite block C has two states, success/failure. Then if it is independent from the other blocks of the RBD, it can be handled as a single block. Of course its probability of failure/success has to be calculated by taking into account the blocks A and B and the dependency between them.

7.6 Large RBDs and use of transfer gates

RBDs related to industrial systems can be too large to be drawn as a whole on a single sheet of paper. In this case, they can be split in several smaller parts (sub-RBDs) linked together by using transfer gates.

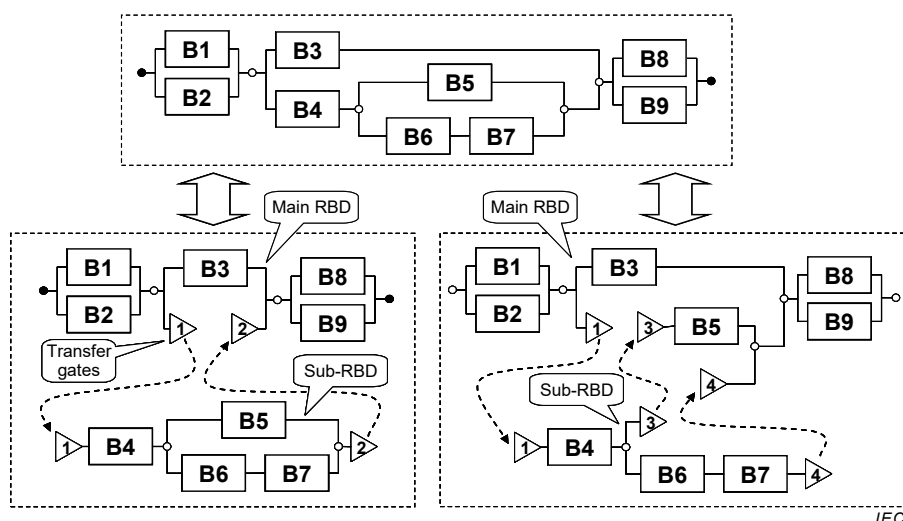


Figure 13 – Use of transfer gates and sub-RBDs

Figure 13 gives two examples of the use of transfer gates: each of the two RBDs at the bottom of the figure is equivalent to the RBD at the top. They are split in two parts: main RBDs and sub-RBDs. It should be noted that a sub-RBD does not necessarily need to have only one input and one output.

The overall underlying logical function is not affected by such a splitting but this allows the drawing of a large RBD on several separate pages. It is a matter for the analyst to choose a subdivision while keeping a good understanding of the whole RBD and of its sub-RBDs.

8 Qualitative analysis: minimal tie sets and minimal cut sets

8.1 Electrical analogy

The RBD can be used first for qualitative analysis purposes by identifying

- the combinations of the blocks in up states leading to the system being in the up state ("success" paths or "tie" sets),
- the combinations of the blocks in down states leading to the system being in the down state ("failure" paths or "cut" sets).

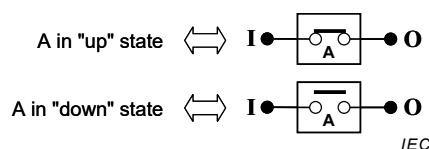


Figure 14 – Analogy between a block and an electrical switch

NOTE When building an RBD related to a physical electrical circuit, the position of a physical switch can be different from its representation by using the analogy described in Figure 14. For example, a physical switch stuck closed will be represented by a virtual switch open as it is in down state.

For doing that, the analogy with an electrical circuit shown in Figure 14 is very useful. This consists in considering that each block is equivalent to an electrical switch which is closed when the block is in up state and open when it is in down state. This has been done to represent Figure 10 by the equivalent Figure 15 where each block has been modelled by an electrical switch.

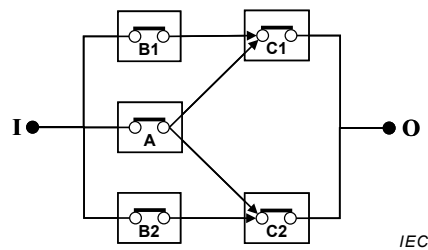


Figure 15 – Analogy with an electrical circuit

When this electrical circuit is closed ("tied"), an electrical signal sent from the input circulates throughout the RBD and reaches the output. Therefore, any combination ("set") of closed switches allowing a signal to circulate from the RBD input to the RBD output models an up state of the system. This is called a "success" path with regards to the state of the system or a "tie" set with regards to the closure of the electrical circuit.

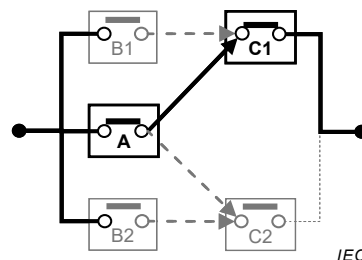


Figure 16 – Example of minimal success path (tie set)

Figure 16 illustrates one of the success paths, (a•c1), of the RBD shown in Figure 15. This success path is minimal as, if A fails or C1 fails, the overall system also fails, i.e. the successes of A and C1 are necessary and sufficient for the system to be in a success state.

B.3.1 gives other examples of minimal and non-minimal tie sets.

The Boolean algebra properties provide a general representation of the system up state, s , as the union of the minimal tie sets (Π_i) of the RBD. This leads to the following formula:

$$s = \bigcup_i \Pi_i \quad (10)$$

When this electrical circuit is broken ("cut"), an electrical signal sent from the input is not able to circulate throughout the RBD and does not reach the output. Therefore any combination ("set") of open switches preventing a signal to circulate from the RBD input to the RBD output models a down state of the system. This is called a "failure" path with regards to the state of the system or a "cut" set with regards to the closure of the electrical circuit.

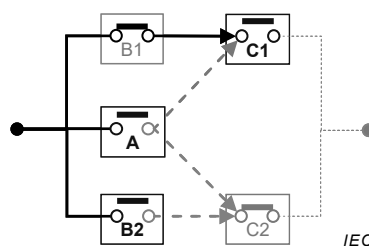


Figure 17 – Example of minimal failure path (cut set)

Figure 17 illustrates one of the failure paths, $(\bar{a} \bullet \bar{b}_2 \bullet \bar{c}_1)$, of the RBD shown in Figure 15. This failure path (cut set) is minimal as when any of A, B2 or C1 are repaired (switches closing), the system is also repaired, i.e. the failures of A, B2 and C1 are necessary and sufficient for the system being in failed state.

B.3.1 gives others examples of minimal and non-minimal cut sets.

The Boolean algebra properties provide a general representation of the down state, $\bar{s}$, as the union of the minimal cut sets (C_j) of the RBD:

$$\bar{s} = \bigcup_j C_j \quad (11)$$

Therefore, from Formulae (10) and (11) the identity: $s = \bigcup_i \Pi_i \equiv \overline{\bigcup_j C_j}$ (12)

is obtained.

The minimal cut sets and minimal tie sets can be obtained by expanding from the logical formulae corresponding to the RBD. Except in simple cases, this is not easy to do that by hand but powerful algorithms are available and implemented into RBD software packages.

8.2 Series-parallel representation with minimal success path and cut sets

The identity (12) provides two equivalent ways to represent an RBD from its minimal tie sets or its minimal cut sets.

Applied to the RBD presented in Figure 10, this leads to the two equivalent logical formulae (see detailed explanations in B.3.2):

$$s = \bigcup_i \Pi_i = b_1 \bullet c_1 + a \bullet c_1 + a \bullet c_2 + b_2 \bullet c_2 \quad (13)$$

$$s = \overline{\bigcup_j C_j} = (b_1 + a + b_2) \bullet (c_1 + c_2) \bullet (b_1 + a + c_2) \bullet (b_2 + a + c_1) \quad (14)$$

Then this RBD can be replaced by the equivalent representations presented in Figure 18 (made of tie sets) and in Figure 19 (made of cut sets) where it can be noticed that some blocks are repeated several times.

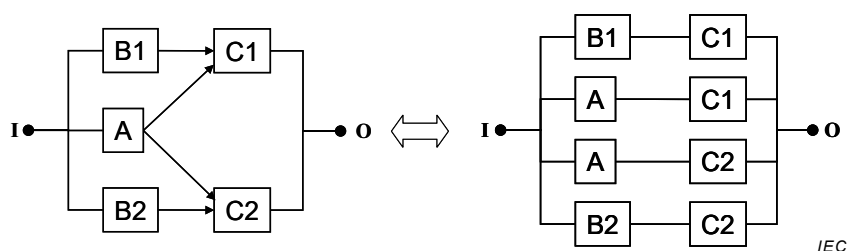


Figure 18 – Equivalent RBDs with minimal success paths

Figure 18 is made of four tie sets of order two (see 3.16, Note 2 to entry):

$(b_1 \bullet c_1), (a \bullet c_1), (a \bullet c_2)$ and $(b_2 \bullet c_2)$.

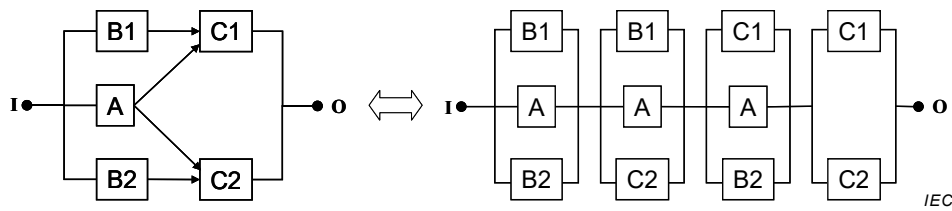


Figure 19 – Equivalent RBDs with minimal cut sets

Figure 19 is made of one cut set of order two $(\bar{c}_1 \bullet \bar{c}_2)$ and of three cut sets of order three: $(\bar{a} \bullet \bar{b}_1 \bullet \bar{b}_2)$, $(\bar{a} \bullet \bar{b}_1 \bullet \bar{c}_2)$ and $(\bar{a} \bullet \bar{b}_2 \bullet \bar{c}_1)$.

8.3 Qualitative analysis from minimal cut sets

For performing qualitative analysis it is more useful to consider the minimal cut sets rather than the minimal tie sets. This can be shown by using the above example: the cut set of order two $(\bar{c}_1 \bullet \bar{c}_2)$ is likely to be more probable than the cut sets of order three $(\bar{a} \bullet \bar{b}_1 \bullet \bar{b}_2)$, $(\bar{a} \bullet \bar{b}_1 \bullet \bar{c}_2)$ or $(\bar{a} \bullet \bar{b}_2 \bullet \bar{c}_1)$. Therefore, from a qualitative point of view, the minimal cut set $(\bar{c}_1 \bullet \bar{c}_2)$ is the weak point of the system and should be improved first.

Therefore, the qualitative analysis may be performed with the following steps:

- identify the minimal cut sets from the logical equation of the system failure;
- sort the minimal cut sets in their increasing orders;
- focus on the lowest order minimal cut sets to improve the system.

When failure probabilities are available for the blocks, the minimal cut sets can be more accurately sorted at step b) by calculating the probability of occurrence of each of them.

9 Quantitative analysis: blocks with constant probability of failure/success

9.1 Series structures

Figure 20 shows the link between the Boolean formulae of a basic series structure and the probabilistic calculations.

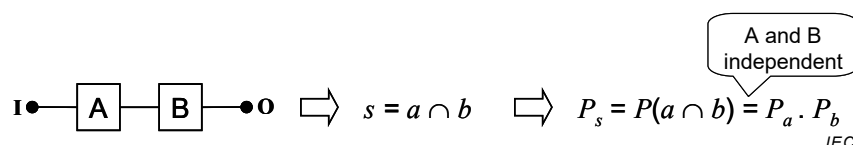


Figure 20 – Link between a basic series structure and probability calculations

This probabilistic formula is basically established for independent blocks with constant probabilities. It expresses the probability of success of the system P_s as a function of the individual probabilities of success of block A, P_A , and block B, P_B . Therefore, the RBD models can be primarily used for systems comprising independent blocks with constant probability of being in the up state.

At this step it would be irrelevant to talk about reliability, availability or failure frequency of the system as those probabilistic measures are only defined for systems with time dependent behaviour.

The formula established in Figure 20 can be easily extended to be used for systems such as those illustrated by Figure 2 (see B.4.1). When blocks A, B, ..., Z are independent, the probability of success of the system is given by the simple equation:

$$P_s = P_a \cdot P_b \cdot P_c \dots P_z \quad (15)$$

i.e. by multiplying together the probabilities of success of all the blocks constituting the RBD.

In general, with n blocks B_i in series, $P_s = \prod_{i=1}^n P_{b_i}$. (16)

9.2 Parallel structures

Figure 21 shows the link between the Boolean formulae of a basic parallel structure and the probabilistic calculations.

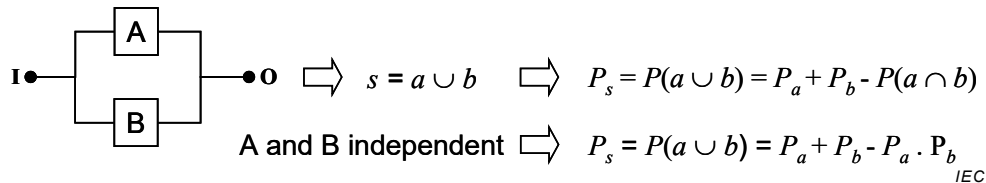


Figure 21 – Link between a parallel structure and probability calculations

As for the basic series structure, the formula for the basic parallel structure is established for constant probabilities and independent blocks in order to express P_s as a function of P_a and P_b .

As it is, the formula shown in Figure 21 is not easy to extend to more than two components (see the Sylvester-Poincaré formula in 11.7 and B.4.2). Fortunately, it can be observed that $P_s = (1 - P_f) = 1 - (P_a + P_b - P_a \cdot P_b) = (1 - P_a) \cdot (1 - P_b)$. This expresses simply that the system is failed when both A and B are failed.

Hence the probability of success of the system (P_s) is given by:

$$P_s = P_a + P_b - P_a \cdot P_b = 1 - (1 - P_a)(1 - P_b) \quad (17)$$

Formula (17) can be easily extended to n blocks B_i in parallel (see B.4.2), i.e.:

– Probability of failure: $P_f = \prod_{i=1}^n (1 - P_{b_i})$ (18)

– Probability of success: $P_s = (1 - P_f) = 1 - \prod_{i=1}^n (1 - P_{b_i})$ (19)

9.3 Mix of series and parallel structures

Formulae (15) and (17) can be combined and this can be done by hand in simple cases but the above calculations are generally not easily tractable by hand. Fortunately, powerful

algorithms are available and implemented into RBD software packages. They are based on the techniques described in Clauses B.5, B.6 or B.7.

9.4 m/n architectures (identical items)

The m/n architectures are analysed in B.4.4. When the blocks are identical (i.e. each with the same probability of success p), the probability of success of the system P_s is given by:

$$P_s = \sum_{r=0}^{n-m} \binom{n}{r} \cdot p^{n-r} \cdot (1-p)^r \quad (20)$$

and the probability of failure is given by:

$$P_{\bar{s}} = \sum_{r=0}^{m-1} \binom{n}{r} \cdot (1-p)^{n-r} \cdot p^r \quad (21)$$

When $n = 2m-1$ (e.g. 1/1, 2/3, 3/5, etc.), the system is up if m blocks are “up” and the system is down if m blocks are “down”. Those structures are symmetrical with regards to the success and failure events. Some of them, for example structure 2/3, are widely used for safety systems.

If the n items are not identical, use of a more general procedure is recommended (see 11.8.2).

10 Quantitative analysis: blocks with time dependent probabilities of failure/success

10.1 General

The calculations developed for constant probabilities in Clause 9 can be easily extended to the time dependent probability of the system $P_s(t)$ provided that the probabilities $P_{x_i}(t)$ of the blocks behave independently from each other. This means that the failure (or repair) of any block shall not affect the probability of failure or repair of any other block within the system being modelled. This implies that sufficient repair resources are available 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 and repairs of individual blocks are considered to be statistically independent events. The calculations for the time dependent probability of system success are detailed in Annex C.

As the probability for an item to be in the up state at a given instant is its instantaneous availability, $A_S(t) = P_s(t)$ and $A_{X_i}(t) = P_{x_i}(t)$. This result holds for complicated structures as well as large RBDs (see Clause 11 and Annex B): provided that the blocks behave independently from each other at all times, the formulae developed for the constant probability case are still valid for availability/unavailability calculations.

$$\text{– Series structures: } A_S(t) = \prod_{i=1}^n A_i(t) \text{ and } U_S(t) = 1 - \prod_{i=1}^n [1 - U_i(t)] \quad (22)$$

$$\text{– Parallel structures: } A_S(t) = 1 - \prod_{i=1}^n (1 - A_i(t)) \text{ and } U_S(t) = \prod_{i=1}^n (U_i(t)) \quad (23)$$

$$- \quad m/n \text{ structure: } A_S(t) = \sum_{r=0}^{n-m} \binom{n}{r} \cdot A(t)^{n-r} \cdot [1 - A(t)]^r \quad \text{and} \quad U_S(t) = \sum_{r=0}^{m-1} \binom{n}{r} \cdot U(t)^{n-r} \cdot [1 - U(t)]^r \quad (24)$$

The availability/unavailability calculations described above are not so simple but reliability/unreliability calculations are even more difficult. This is due to the definition of the reliability itself: $R_S(t) = P(\text{S in "up" state over } [0, t])$ which implies that the system remains in up state over the time interval $[0, t]$. That means that only the sequences of system events which do not go through to the system down state are relevant for calculating $R_S(t)$. Therefore the sequences of system events which include a succession "up state" → "down state" → "up state" have to be excluded from the calculations. This implies that a system part going to the down state is repairable only if the system remains in up state during the repair of this part. Thus, with regards to the calculation of $R_S(t)$, the system parts (e.g. components) are repairable or not depending on the system state (i.e. on the states of the other parts). This constitutes a systemic dependency between the system parts and therefore between the blocks modelling these parts within the RBD modelling the system. This happens in the case of redundancy of repairable items. This is the main difficulty in the understanding of this standard: except for RBDs made of blocks in series, the system reliability $R_S(t)$ cannot be calculated by combining the reliability $R_{Bi}(t)$ of its individual blocks. The formulae established above under the independency hypothesis are no longer valid. This is further discussed in 10.3.1.4.

10.2 Non-repaired blocks

10.2.1 General

When a block X is not repaired, its probability to be available at time t is equal to its probability to have had no failure over $[0, t]$. Therefore, its reliability $R_X(t)$ is equal to its availability $A_X(t)$.

When none of the blocks within a system are repaired, the system made of these blocks is not repaired either. Then its availability and reliability are identical and $R_S(t) = A_S(t)$

10.2.2 Simple non-repaired block

The reliability of any item X is linked to its failure rate $\lambda_X(t)$, with the following relationship:

$$A_X(t) = R_X(t) = \exp\left(-\int_0^t \lambda_X(u) du\right) \quad (25)$$

where $\lambda_X(u)$ denotes the failure rate of the block X at $t = u$, u being a dummy variable.

When λ_X is constant, Figure 25 is simplified to the classical formula:

$$A_X(t) = R_X(t) = \exp(-\lambda_X \cdot t) \quad (26)$$

$$\text{Therefore} \quad U_X(t) = F_X(t) = 1 - \exp(-\lambda_X \cdot t) \quad (27)$$

10.2.3 Non-repaired composite blocks

A non-repaired composite block C can be handled as a whole and as a simple non-repaired block provided its availability $A_C(t)$ is established. Note that in this case $A_C(t) = R_C(t)$.

This can be illustrated by the composite block presented in Figure 12. It corresponds to a cold standby system with the following parameters:

- λ_A is the constant failure rate of block A and $f_A(\tau)$ is the probability density function of its time to failure;
- λ_{Bd} is the constant failure rate of block B when in a passive (dormant) state, either cold or under low power;
- λ_B is the constant failure rate of block B when in an active state, after it has started due to the failure of block A.

NOTE In the following calculations, the switch is considered to be perfect but examples of modelling of the imperfect switching are given in 10.3.1.2 (Figure 23) and C.3.3.

This system is analysed in C.3.3 which provides the following results:

- if the dormant failure rate of item B is assumed to be equal to zero, then the availability of a standby redundant system is:

$$A_C(t) \equiv R_C(t) = e^{-\lambda_A \cdot t} + \frac{\lambda_A}{\lambda_A - \lambda_B} \cdot [e^{-\lambda_B \cdot t} - e^{-\lambda_A \cdot t}] \quad (28)$$

- if 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:

$$A_C(t) \equiv R_C(t) = e^{-\lambda \cdot t} \cdot (1 + \lambda \cdot t) \quad (29)$$

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

$$A_C(t) \equiv R_C(t) = e^{-\lambda \cdot t} \left(1 + \lambda \cdot t + \frac{(\lambda \cdot t)^2}{2!} + \frac{(\lambda \cdot t)^3}{3!} + \dots + \frac{(\lambda \cdot t)^n}{n!} \right) \quad (30)$$

Formulae (28), (29) or (30) can be used for the composite block C in exactly the same way as Formula (26) is used for ordinary blocks. Nevertheless, establishing those formulae is difficult and other procedures, such as Markov analysis, should be used to analyse standby systems (see 10.3.1.2).

10.2.4 RBDs with non-repaired blocks

- **Availability/reliability:** provided that the blocks behave independently from each other, the availability/reliability of the RBD can be calculated by combining availabilities/reliabilities of the blocks (see 10.2.2 and 10.2.3) according to the logic of the RBD and by using the formulae presented in 10.1.
- **Frequency:** a system made of non-repaired components can fail only once. The probability to observe this failure over $[0, T]$ is $F_S(T)$ and the average failure frequency $w_S^{\text{avg}}(T)$ is equal to $\frac{F_S(T)}{T}$. It decreases and tends to zero as time increases.

10.3 Repaired blocks

10.3.1 Availability calculations

10.3.1.1 Simple block

When a block i is repaired, its availability depends both on its failure rate and on the repair resources. Those resources are generally allocated at the system level and, when they are limited, this constitutes a systemic dependency between the blocks. Therefore, the blocks are independent only if the repair resources are unlimited. In this way the repair of one block can be done at any time even when one or several other blocks are already under repair. This

assumption implies, in particular, that there are as many repair teams as the number of blocks.

The block availabilities $[A_i(t)]$ can be expressed by any formula (simple or complex). In the simplest case, the repaired blocks are characterized by a constant failure rate λ_i and a constant repair rate μ_i and this leads to the classical formula:

$$A_i(t) = \frac{\mu_i}{\lambda_i + \mu_i} + \frac{\lambda_i}{\lambda_i + \mu_i} \exp[-(\lambda_i + \mu_i)t] \quad (31)$$

This analytical formula can be replaced by the equivalent Markov graph presented in Figure 22 where $A_i(t) = P(\text{OK}, t)$ where $P(\text{OK}, t)$ is the probability of the state OK at time t .

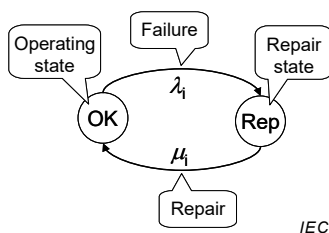


Figure 22 – "Availability" Markov graph for a simple repaired block

NOTE A Markov graph devoted to availability calculations is called "availability" Markov graph.

10.3.1.2 Repaired composite blocks

A repaired composite block, C, can be handled as a whole and as a simple repaired block provided its availability $A_C(t)$ is established. Note that in this case $A_C(t) \neq R_C(t)$.

This can be illustrated by the composite block presented in Figure 12. It has already been analysed in 10.2.3 in the non-repair case. If the components A and B are considered repairable, then the formula of the availability $A_C(t)$ of the composite block C can now be established by using the Markov graph in Figure 23.

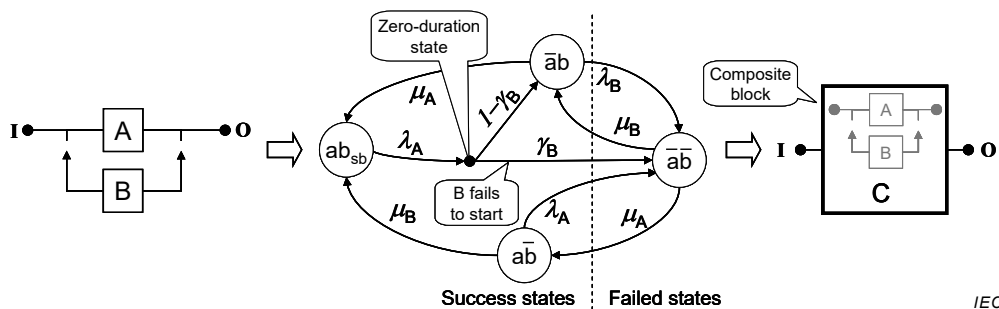


Figure 23 – Standby redundancy

In this graph, C is repaired after it has had a failure (see the transitions from the failed state to the success states): then, this is an "availability" Markov graph (see 10.3.3 to see the difference with a "reliability" Markov graph). This Markov graph can be used to establish availability $A_C(t)$ of the composite block C or even be used as an RBD input (see C.3).

In this Markov graph, the failure of the switching and sensing mechanism is modelled by using the probability γ_B that block B fails to start when A fails. As this occurs as soon as the component A fails, a zero-duration state has been introduced into the Markov graph. From this state, B immediately starts (probability $1-\gamma_B$) or not (probability γ_B).

The Markov graph shown in Figure 23 models the dependencies existing between the blocks A and B:

- B starts only after A has failed;
- B may fail when demanded by a failure of A;
- B comes back to a standby position as soon as A and B are in the up state.

Those dependencies between A and B cannot be taken into account by combining the individual availabilities of A and B and this is why C has to be considered as a whole. If blocks A and B were considered separately, a typical sequential structure outside the scope of the RBD would be obtained. Gathering A and B into a composite block C allows to manage this composite block as an individual block within the RBD framework.

The above principle is general and can be implemented when a few blocks are not independent. When the number of dependent blocks increases, other techniques like dynamic RBDs (see 12.2), Markov processes [2] or Petri nets [3] should be used.

10.3.1.3 Periodically tested blocks

With regards to the safety functions that they have to perform, the safety systems are only available or not available. Therefore, they are typical systems with only two states. Their main characteristic is that, in spite of the fact that they remain in the standby position most of the time, they have to react with a high availability when a safety demand occurs.

The components of such safety systems are then periodically tested in order to detect failures that may have occurred when the system is in the standby position. Therefore, the availability of a periodically tested component is maximal just after a test where the possible failures have been detected and repaired, and decreases afterwards until the next test is performed. The typical saw tooth curve shape of the availability $A_B(t)$ of such a block is illustrated in Figure 24. It can be modelled by a multi-phase Markov process (see Figure C.4). A whole RBD implementing periodically tested blocks is also illustrated in Figure C.5.

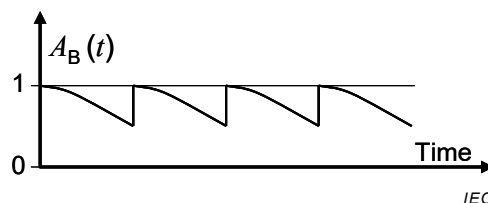


Figure 24 – Typical availability of a periodically tested block

The shape of the blocks availabilities does not change the principle of the calculation and they can be combined as described above in order to calculate the overall system availability $A_S(t)$ or unavailability $U_S(t)$. This is very useful to implement the average unavailability calculations (i.e. PFD_{avg}) required by functional safety standards (e.g. IEC 61508 [5] or IEC 61511 [6]) as explained at the end of 10.3.2.

10.3.1.4 Complex repaired blocks (RBD driven Markov processes)

Provided that the independency requirements are fulfilled, the idea developed in Figure 22 and Figure 23 to use small Markov graphs with few states to model the block availabilities can be easily extended to all the blocks of an RBD.

This allows the construction of large Markov models (comprising millions of states) made of small individual sub-Markov models (comprising a few states each) combined through the logic of an RBD. Therefore

- the Markov graphs provide the block availabilities,

- the RBD provides the logic used to combine the block availabilities.

Such models are called "RBD driven Markov processes".

See Clause C.4 for more details.

10.3.2 Average availability calculations

Another useful parameter to calculate from an RBD is the average availability $A_S^{avg}(0, T)$ of the system over a given period $[0, T]$. This can be done by the integration of the instantaneous system availability $A_S(t)$:

$$A_S^{avg}(0, T) = \frac{1}{T} \int_0^T A_S(t) dt \quad (32)$$

In the general case, such calculations are not really possible by hand but nowadays RBD software packages are available to make the needed numerical calculations.

Nevertheless, under certain conditions, a steady state is reached where the probability for B_i to leave the up state by a failure is equal to the probability for B_i to reach it by a repair. When a steady state exists, the availability $A_{B_i}(t)$ reaches an asymptotic value $A_{B_i}^{as}$.

This occurs when

- the failures are quickly detected and repaired (i.e. $1/\mu_i \ll 1/\lambda_i$),
- the failure and repair rates (λ_i, μ_i) are constant.

For example, in the case described in Figure 22, the steady state availability of the block is equal to $A_{B_i}^{as} = \mu_i / (\lambda_i + \mu_i)$.

When all the blocks reach such steady states, the system also reaches a steady state (see Figure 25 and Figure C.3) where $A_S(t) \rightarrow A_S^{as}$. Then, outside the transient period,

Equation (32) gives the long term average availability of the system: $A_S^{avg} = A_S^{as}$.

Therefore, when an RBD reaches a steady state, the steady state availabilities of the blocks become constant and the formulae established in Clause 9 can be used to carry out system steady-state availability predictions. This is accomplished by simply replacing the constant probabilities P_{b_i} by the constant values $A_{B_i}^{as}$.

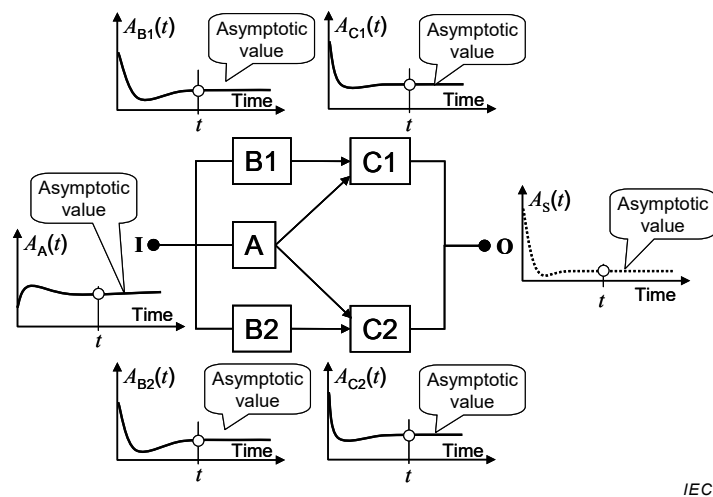


Figure 25 – Example of RBD reaching a steady state

Warning: the calculations given above are valid only with asymptotic block availabilities. They are not valid with ordinary average availabilities.

Then, when the RBD does not reach a steady state, the average availability has to be calculated by using the general Formula (32).

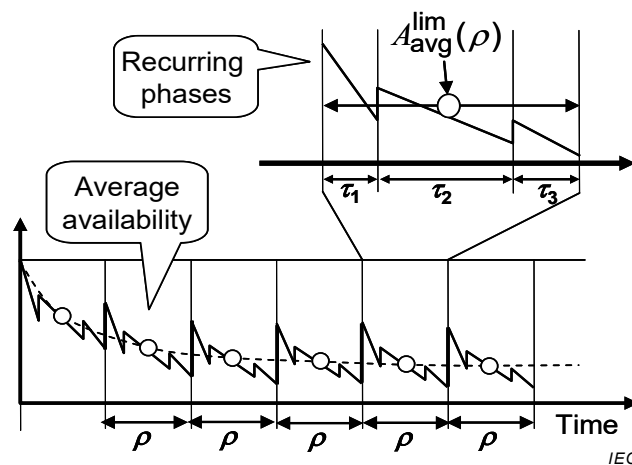


Figure 26 – Example of RBD with recurring phases

A special case occurs when the RBD is used through recurring phases such as:

- succession of seasons: winter, spring, summer and autumn;
- test intervals for periodically tested items.

Figure 26 illustrates a system with three recurring phases such that the same pattern of three phases is repeated with a time interval equal to $\rho = \tau_1 + \tau_2 + \tau_3$. The availability of such a system has no asymptotical value but the average availability $A_{\text{avg}}[n\rho, (n+1)\rho]$ generally reaches a limit value when n is large enough:

$$A_{\text{avg}}^{\text{Lim}}(\rho) = \xrightarrow{n \rightarrow \infty} A_{\text{avg}}[n\rho, (n+1)\rho] \quad (33)$$

As $A_{\text{avg}}[n\rho, (n+1)\rho]$ decreases when n increases, $A_{\text{avg}}^{\text{Lim}}(\rho)$ provides a good conservative approximation of the average availability over a time interval $[0, T]$ encompassing several sets of recurring phases.

Therefore, the techniques described in this standard can be used to calculate the average unavailability of safety systems and this makes the link with the functional safety standards (IEC 61508 or IEC 61511) which require such calculations for safety instrumented systems and where the average unavailability is called PFD_{avg} (average of the probability of failure on demand). This is described in Clauses C.4 and C.5.

10.3.3 Reliability calculations

When repaired blocks are considered, the calculation of the reliability $R_S(t)$ implies that the repairs of the blocks in the system (RBD) need to be considered only as long as the system remains in the up state (see in 10.1).

This can be illustrated by the simple redundant system modelled by the RBD on the left hand side of Figure 27. With regards to the calculation of $R_S(t)$, when the block B fails, it can be repaired only if S in the up state (i.e. if A is in the up state). In the same way when the block A fails, it can be repaired only if S in the up state (i.e. if B is in the up state). Therefore when one block fails, its repair depends on the state of the system S which, in turn, depends on the states of all the blocks. This systemic dependency between the blocks is modelled in the Markov graph presented on the right hand side of Figure 27. It is equivalent to the RBD presented on the left hand side.

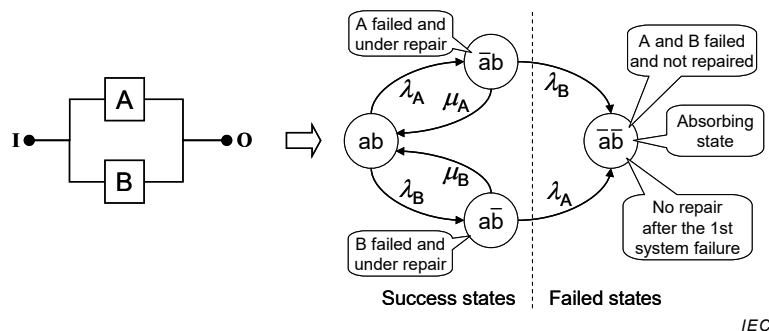


Figure 27 – RBD and equivalent Markov graph for reliability calculations

The simple redundant system is made of two redundant blocks A and B and it has 4 states. The success states are ab , $\bar{a}b$ and $a\bar{b}$ and the failed state is $\bar{a}\bar{b}$. The system is reliable over a given period $[0, t]$ only if it remains in the "success" states all the time. Therefore, the states ab , $\bar{a}b$ and $a\bar{b}$ are "reliable" states only if they come from transitions between each other. That means that, for reliability calculations at time t , the transition out of $\bar{a}\bar{b}$ is not allowed during $[0, t]$. The state $\bar{a}\bar{b}$ is an absorbing state and the presence of an absorbing state characterizes a reliability Markov graph.

In this graph, block A can be repaired in the state $\bar{a}b$ but not in the state $\bar{a}\bar{b}$ and block B can be repaired in the state $a\bar{b}$ but not in the state $\bar{a}\bar{b}$. Therefore, the repair of a failure of a block depends on the state of the whole system when it occurs: this is what is called a "systemic" dependency.

It is no longer possible to calculate the system reliability by combining the individual probabilities of success of the blocks.

- The block availabilities, $[A_i(t)]$, cannot be used as this would give the system availability and not the system reliability.

- The block reliabilities, $[R_i(t)]$, cannot be used as this would give the reliability of a system with non-repaired blocks (because the reliability of a repaired component is the same as the reliability of a non-repaired component with the same failure rate).

Therefore, except in the particular case developed hereafter, other techniques like Monte Carlo simulation (e.g. DRBDs, see 12.2 and Annex E), Markov [2] or Petri Nets [3] should be used instead.

The only case where reliability calculations are manageable occurs for quickly (i.e. $MTTR_i \ll MTTF_i$) and completely (i.e. every failure is repaired) repaired systems. That means that, when a block fails, the repair starts at once and lasts a short time. In this case the system reaches a steady state rather quickly and its availability $A_S(t)$ an asymptotic value A_S^{as} . In this steady state the conditional failure intensity, λ_{VS} (also called Vesely failure rate) is constant and provides a good approximation of the system failure rate, λ_S . Then the system reliability is obtained by using the classical formula $R_S(t) = e^{-\lambda_S t} \approx e^{-\lambda_{VS} t}$ and the system unreliability is given by $F_S(t) = 1 - e^{-\lambda_S t} \approx 1 - e^{-\lambda_{VS} t}$.

For example in Figure 27, when the steady state is reached, the properties of the Markov processes allow to obtain a good approximation of λ_{VS} and λ_S directly from the Markov process:

$$\lambda_S \approx \lambda_{VS} \approx \lambda_A \frac{\lambda_B}{\lambda_B + \mu_A} + \lambda_B \frac{\lambda_A}{\lambda_A + \mu_B} \quad (34)$$

This is not a simple formula even though the system is very simple. For larger RBDs, the Vesely failure rate, λ_{VS} , can be obtained from conditional probabilities which can be calculated by the algorithms currently in use in RBD software packages. The way to obtain the conditional and unconditional failure intensities from an RBD is detailed in Clause C.6 and more details are given about reliability calculations in Clause C.7.

10.3.4 Frequency calculations

When the blocks are repaired, another useful probabilistic measure is the average failure frequency of the system over a given time interval $[0, T]$ which is equal to n/T if n failures occur over T . This average failure frequency is obtained by calculating the average unconditional failure intensity of the system $w_S^{avg}(0, T) = n/T$.

The failure frequency can be calculated in any case but this is difficult by hand. Algorithms have been developed to do that and the principle is explained in Clause C.6.

11 Boolean techniques for quantitative analysis of large models

11.1 General

It is possible to evaluate the availability $A_S(t)$ of all the systems considered so far by the application of a suitable availability formula selected from Formulae (15) to (24). However, when the number of blocks increases, the corresponding RBDs may not conveniently be evaluated by any of the above formulae. Calculations are more difficult and so other mathematical approaches have to be employed.

Such approaches provide several ways to manipulate the Boolean equations in order to make the calculations possible. They can be generally employed manually on small RBDs but most of them can be used through a software package when the number of blocks is large. They are based on the following techniques:

- reduction of the RBD to simpler structures;
- use of the total probability theorem;
- use of Boolean truth tables;
- use of Karnaugh maps;
- use of Shannon decomposition and binary decision diagrams;
- use of general Sylvester-Poincaré formulae.

For the procedures that follow, the condition of independence, as stated in 5.2 d), applies and the formulae provided hereafter for constant probability calculations may be straightforwardly transformed for availability calculations by applying 10.1 and Annex C.

It should be noted that Monte Carlo simulation can also be used for complex RBDs. The use of such procedures is not dealt with in this standard but the dynamic RBDs are described in 12.2 and Annex E.

11.2 Method of RBD reduction

The RBDs modelling an industrial system may seem very complicated. By careful examination, however, the blocks in the diagram can often be grouped together such that the groups are statistically independent. In particular, this means that no two (or more) groups can contain the same block.

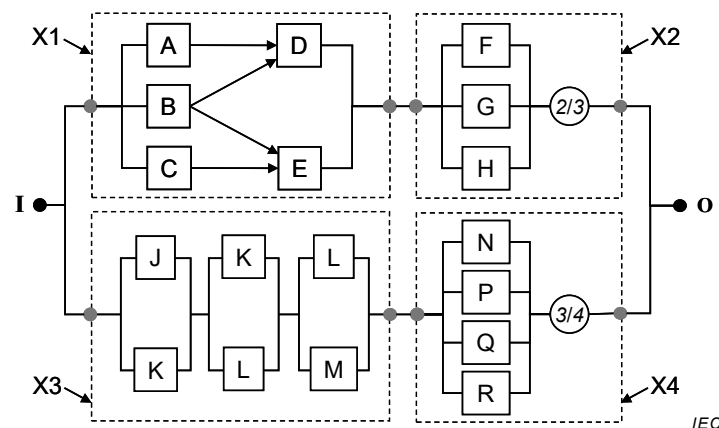


Figure 28 – Illustrating grouping of blocks before reduction

This can be illustrated by considering the RBD shown in Figure 28.

Figure 28 can be reduced to the diagram shown in Figure 29 which is made of the four dotted groups of blocks X1, X2, X3 and X4 as illustrated in Figure 10, Figure 8, Figure 37, and Figure 9 respectively.

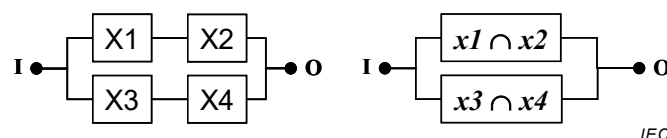


Figure 29 – Reduced reliability block diagrams

Hence the final system availability is given by

$$A_S(t) = A_{X1} \cdot A_{X2} + A_{X3} \cdot A_{X4} - A_{X1} \cdot A_{X2} \cdot A_{X3} \cdot A_{X4}$$

as explained in 9.2.

This technique of reduction is difficult to automate but very useful for calculations by hand.

11.3 Use of total probability theorem

When dealing with RBDs of the type illustrated by Figure 10 which implement a common block A, it is possible to implement an approach based on the total probability theorem.

Two mutually exclusive events x and $\bar{x}$ form a complete set of events (i.e. $x + \bar{x} = \Omega$) and the total probability theorem can be summarized as follows:

$$P_s = P_{s|x} \cdot P_x + P_{s|\bar{x}} \cdot P_{\bar{x}} = P_{s|x} \cdot P_x + P_{s|\bar{x}} \cdot (1 - P_x) \quad (36)$$

In Equation (36) P_s denotes the probability of success of a system, $P_{s|x}$ denotes the probability of success of the system given that a particular item X is working, and $P_{s|\bar{x}}$ denotes the probability success of the system given that the particular item X has failed.

Formula (36) can be applied to the block A of Figure 10 and this leads to:

$$P_s = P_{s|a} \cdot P_a + P_{s|\bar{a}} \cdot P_{\bar{a}} \quad (37)$$

For example, when the item A has failed, the RBD of Figure 10 becomes the RBD shown in Figure 30 so that $P_{s|\bar{a}} = P_{b1} \cdot P_{c1} + P_{b2} \cdot P_{c2} - P_{b1} \cdot P_{c1} \cdot P_{b2} \cdot P_{c2}$

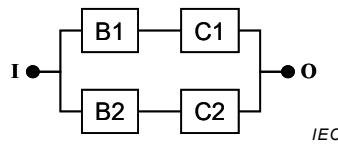


Figure 30 – Representation of Figure 10 when item A has failed

Similarly, when A is working, the RBD of Figure 10 becomes that given in Figure 31 so that $P_{s|a} = P_{c1} + P_{c2} - P_{c1} \cdot P_{c2}$.

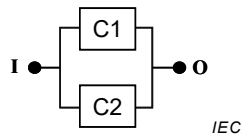


Figure 31 – Representation of Figure 10 when item A is working

$$\text{Hence } P_s = (P_{c1} + P_{c2} - P_{c1} \cdot P_{c2}) \cdot P_a + (P_{b1} \cdot P_{c1} + P_{b2} \cdot P_{c2} - P_{b1} \cdot P_{c1} \cdot P_{b2} \cdot P_{c2}) \cdot (1 - P_a) \quad (38)$$

If $P_{c1} = P_{c2} = P_c$ and $P_{b1} = P_{b2} = P_b$, the above Formula (38) simplifies to:

$$P_s = (2P_c - P_c^2) \cdot P_a + (2P_b \cdot P_c - P_b^2 \cdot P_c^2) \cdot (1 - P_a) \quad (39)$$

This procedure can be extended to n mutually exclusive events $a_1, \dots, a_n$, whose probabilities sum to unity (i.e., $a_1 + a_2 + \dots + a_n = \Omega$), then $P_s = P_s | a_1 \cdot P_{a_1} + \dots + P_s | a_n \cdot P_{a_n}$. It can be used to deal with an RBD with repeated blocks (see 11.8.1.2). When there are n repeated blocks, this leads to develop 2^n terms for the formula of P_s . Therefore, this technique is useful to deal with RBDs with a limited number of repeated blocks for example m/n structures.

11.4 Use of Boolean truth tables

The system success paths depicted by RBDs are the graphical description of an underlying Boolean expression. For example, three redundant items A, B and C (one out of three required for system success) can be represented by the parallel RBD configuration illustrated in Figure 32, or by the Boolean expression:

$$s = a + b + c \quad (40)$$

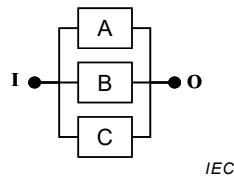


Figure 32 – RBD representing three redundant items

The Sylvester-Poincaré formula (see 11.7 and B.5) applied to three independent events leads to the following result:

$$P_s = P_a + P_b + P_c - (P_a \cdot P_b + P_a \cdot P_c + P_b \cdot P_c) + P_a \cdot P_b \cdot P_c \quad (41)$$

Formula (41) comprises seven terms when there are only three blocks (i.e. three events a , b and c). This number of terms increases exponentially when the number of involved events increases.

To prevent the increasing of terms, the idea is then to replace the events a , b and c by equivalent combinations of disjoint events (see 11.7) and this can be done by using the truth table of the system according to the states of blocks A, B and C.

Table 5 – Application of truth table to the example of Figure 32

State number	Block			System	Disjointed terms	Consensus	
	A	B	C				
1	0	0	0	0	$\bar{a} \bullet \bar{b} \bullet \bar{c}$		
2	0	0	1	1	$\bar{a} \bullet \bar{b} \bullet c$	$\bar{a} \bullet \bar{b} \bullet c$	$\bar{a} \bullet \bar{b} \bullet c$
3	0	1	0	1	$\bar{a} \bullet b \bullet \bar{c}$	$\bar{a} \bullet b$	$\bar{a} \bullet b$
4	0	1	1	1	$\bar{a} \bullet b \bullet c$		
5	1	0	0	1	$a \bullet \bar{b} \bullet \bar{c}$	$a \bullet \bar{b}$	a
6	1	0	1	1	$a \bullet \bar{b} \bullet c$		
7	1	1	0	1	$a \bullet b \bullet \bar{c}$	$a \bullet b$	
8	1	1	1	1	$a \bullet b \bullet c$		

NOTE 1= working, 0 = failed.

This truth table identifies 8 disjoint terms representing the 8 possible states of the system: the state number 1 corresponds to the failure of the system and the states 2 to 8 to the success states of the system.

Again there are seven terms to handle and therefore this raw decomposition in disjointed terms is not very effective to calculate P_s . Note that there is generally no link between the number of terms of the Sylvester-Poincaré formula and the number of the disjoint terms from the truth table.

Fortunately, some disjoint terms can be combined through "consensus" as this has been done on the right hand side of the table. In a first step, terms 7 and 8, 5 and 6 and 3 and 4 have been combined together to obtain 4 disjoint terms. In a second step, terms 5 to 7 have been merged into a single term and three disjoint terms are obtained:

$$s = (a + b + c) \equiv a + (\bar{a} \bullet b) + (\bar{a} \bullet \bar{b} \bullet c) \quad (42)$$

Finally, the probability of failure of the system can be calculated as:

$$P_s = P_a + (1 - P_a) \cdot P_b + (1 - P_a) \cdot (1 - P_b) P_c \quad (43)$$

Formula (43) can be directly used to evaluate the system availability:

$$A_S(t) = A_A(t) + [1 - A_A(t)] \cdot A_B(t) + [1 - A_A(t)] \cdot [1 - A_B(t)] \cdot A_C(t) \quad (44)$$

It has to be noted that Table 5 identifies only one term leading to the system down state $\bar{a} \bullet \bar{b} \bullet \bar{c}$. Therefore, the calculation of the probability of failure is simpler than the probability of success and:

$$P_s = 1 - P_{\bar{s}} = 1 - P_{\bar{a}} \cdot P_{\bar{b}} \cdot P_{\bar{c}} \quad (45)$$

and finally
$$A_S(t) = 1 - U_S(t) = 1 - U_A(t) \cdot U_B(t) \cdot U_C(t) \quad (46)$$

Formulae (44) and (46) are equivalent.

For a system with n blocks, the Boolean truth table has 2^n rows and therefore this approach can soon become unwieldy, although the principle involved is quite straightforward. This problem is overcome to some extent by using Karnaugh maps (see 11.5) but it is actually solved by using the Shannon decomposition and the binary decision diagrams explained hereafter (see 11.6). For a detailed description of a general application of Boolean methods, see Annex B.

11.5 Use of Karnaugh maps

The Karnaugh maps [8][9][10][11] technique has been developed to simplify the logical equation corresponding to a truth table. Therefore, it can be used for RBDs as well.

The principle of the use of such maps is illustrated hereafter with maps related to the RBD presented in Figure 10. This RBD comprises 5 blocks. As the Karnaugh maps are easier to manipulate with 4 variables, the whole map has been split into two disjoint cases:

- A is in up state (Table 6);
- A is in down state (Table 7).

Table 6 – Karnaugh map related to Figure 10 when A is in up state

B1 B2 \ C1 C2	00	01	11	10
00	0	0	0	0
01	1	1	1	1
11	1	1	1	1
10	1	1	1	1

Table 7 – Karnaugh map related to Figure 10 when A is in down state

B1 B2 \ C1 C2	00	01	11	10
00	0	0	0	0
01	0	1	1	0
11	0	1	1	1
10	0	0	1	1

In Table 6 and Table 7, the blocks have been split in two groups (B1 B2 and C1 C2) and the states of the components have been organized in such a way that only one state changes from a column to the next one and from a line to the next one. Therefore, the combinations which can be simplified are close together. For example, in Table 6, the combinations boxed in plain lines represent only C2 as the states of C1, B1 and B2 do not matter. In the same way, the combinations boxed in dotted lines represent only C1 as the states of C2, B1 and B2 do not matter. This leads to

$$s|a = c_1 + c_2 \quad (47)$$

where $s|a$ represents the system S being in up state given the block A is in the up state and c_1 and c_2 represent the state variables related to blocks C1 and C2.

With the Karnaugh map presented in Table 7 the following formula is obtained

$$s|\bar{a} = b_1 \cdot c_1 + b_2 \cdot c_2 \quad (48)$$

where $s|\bar{a}$ represents the system S being in up state given A is in the down state and b_1 , b_2 , c_1 and c_2 represent the state variables related to blocks B1, B2, C1 and C2.

Gathering the results gives:

$$s = a \cdot (c_1 + c_2) + \bar{a} \cdot (b_1 \cdot c_1 + b_2 \cdot c_2) \quad (49)$$

And finally, the system availability can be calculated with the following formula:

$$A_S(t) = A_A(t) \cdot \{1 - [1 - A_{C1}(t)] \cdot (1 - A_{C2})\} + [1 - A_A(t)] \cdot \{1 - [1 - A_{B1}(t) \cdot A_{C1}(t)] \cdot [1 - A_{B2}(t) \cdot A_{C2}(t)]\} \quad (50)$$