

Analysis techniques for dependability — Reliability block diagram and boolean methods

The European Standard EN 61078:2006 has the status of a
British Standard

ICS 03.120.01; 03.120.99

National foreword

This British Standard is the official English language version of EN 61078:2006. It is identical with IEC 61078:2006. It supersedes BS EN 61078:1994 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee DS/1, Dependability and terotechnology, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the *BSI Catalogue* under the section entitled “International Standards Correspondence Index”, or by using the “Search” facility of the *BSI Electronic Catalogue* or of British Standards Online.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the EN title page, pages 2 to 37 and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2006

© BSI 2006

ISBN 0 580 48700 8

Amendments issued since publication

Amd. No.	Date	Comments

English version

**Analysis techniques for dependability -
Reliability block diagram and boolean methods
(IEC 61078:2006)**

Techniques d'analyse
pour la sûreté de fonctionnement -
Bloc-diagramme de fiabilité
et méthodes booléennes
(CEI 61078:2006)

Techniken für die Analyse
der Zuverlässigkeit -
Verfahren mit dem
Zuverlässigkeitsblockdiagramm
und Boole'sche Verfahren
(IEC 61078:2006)

This European Standard was approved by CENELEC on 2006-03-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

© 2006 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

Ref. No. EN 61078:2006 E



Documents

Document Sharing Hub

Foreword

The text of document 56/1071/FDIS, future edition 2 of IEC 61078, prepared by IEC TC 56, Dependability, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 61078 on 2006-03-01.

This European Standard supersedes EN 61078:1993.

The major change with respect to EN 61078:1993 is that an additional clause on Boolean disjointing methods (Annex B) has been added.

The following dates were fixed:

- | | | |
|--|-------|------------|
| – latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement | (dop) | 2006-12-01 |
| – latest date by which the national standards conflicting with the EN have to be withdrawn | (dow) | 2009-03-01 |

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 61078:2006 was approved by CENELEC as a European Standard without any modification.

CONTENTS

INTRODUCTION.....	5
1 Scope	6
2 Normative references	6
3 Terms and definitions	6
4 Symbols and abbreviated terms	7
5 Assumptions and limitations.....	8
5.1 Independence of events.....	8
5.2 Sequential events.....	8
5.3 Distribution of times to failure	8
6 Establishment of system success/failure definitions.....	8
6.1 General considerations	8
6.2 Detailed considerations	9
7 Elementary models	10
7.1 Developing the model	10
7.2 Evaluating the model	12
8 More complex models.....	15
8.1 General procedures	15
8.2 Models with common blocks.....	20
8.3 m out of n models (non-identical items)	22
8.4 Method of reduction	22
9 Extension of reliability block diagram methods to availability calculations.....	23
Annex A (informative) Summary of formulæ.....	25
Annex B (informative) Boolean disjointing methods.....	29
Annex ZA (normative) Normative references to international publications with their corresponding European publications.....	37
Bibliography	35
Figure 1 – Series reliability block diagram	10
Figure 2 – Duplicated (or parallel) series reliability block diagram	10
Figure 3 – Series duplicated (or parallel) reliability block diagram	11
Figure 4 – Mixed redundancy reliability block diagram	11
Figure 5 – Another type of mixed redundancy reliability block diagram	11
Figure 6 – 2/3 redundancy	11
Figure 7 – 2/4 redundancy	11
Figure 8 – Diagram not easily represented by series/parallel arrangement of blocks.....	12
Figure 9 – Parallel arrangement of blocks.....	13
Figure 10 – Standby redundancy.....	14
Figure 11 – Representation of Figure 8 when item A has failed	16
Figure 12 – Representation of Figure 8 when item A is working.....	16

Figure 13 – One-out-of-three parallel arrangement	17
Figure 14 – Reliability block diagram using an arrow to help define system success	20
Figure 15 – Alternative representation of Figure 14 using common blocks	20
Figure 16 – 2-out-of-5 non-identical system	22
Figure 17 – Illustrating grouping of blocks before reduction.....	23
Figure 18 – Reduced reliability block diagrams	23
Table 1 – Application of truth table to the example of Figure 13	18
Table 2 – Application of truth table to the example of Figure 8	19
Table 3 – Application of truth table to the examples of Figures 14 and 15.....	21

INTRODUCTION

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

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

ANALYSIS TECHNIQUES FOR DEPENDABILITY – RELIABILITY BLOCK DIAGRAM AND BOOLEAN METHODS

1 Scope

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

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

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

2 Normative references

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

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

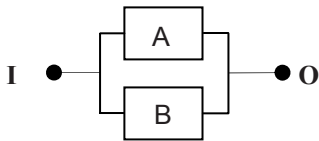
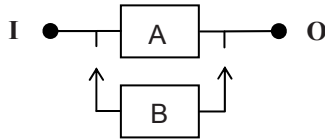
IEC 61025, *Fault tree analysis (FTA)*

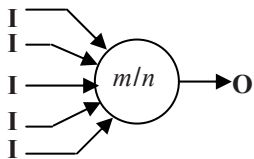
ISO 3534-1:1993, *Statistics – Vocabulary and symbols – Part 1: Probability and general statistical terms*

3 Terms and definitions

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

4 Symbols and abbreviated terms

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

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

5 Assumptions and limitations

5.1 Independence of events

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

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

5.2 Sequential events

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

5.3 Distribution of times to failure

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

6 Establishment of system success/failure definitions

6.1 General considerations

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

In addition, there should be clear statements concerning

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

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

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

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

6.2 Detailed considerations

6.2.1 System operation

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

6.2.2 Environmental conditions

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

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

6.2.3 Duty cycles

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

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

7 Elementary models

7.1 Developing the model

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

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

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

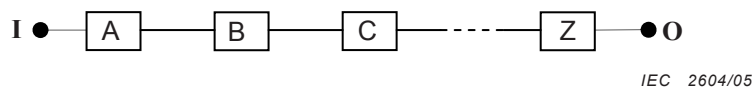


Figure 1 – Series reliability block diagram

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

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

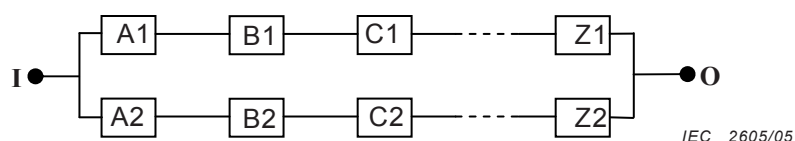


Figure 2 – Duplicated (or parallel) series reliability block diagram