

Application of Markov techniques

The European Standard EN 61165:2006 has the status of a British Standard

ICS 03.120.01; 03.120.30; 21.020; 29.020

National foreword

This British Standard is the UK implementation of EN 61165:2006, which is identical with IEC 61165:2006. This standard supersedes BS 5760-15:1995, which is withdrawn.

The UK participation in its preparation was entrusted by Technical Committee DS/1, Dependability and terotechnology, to Subcommittee DS/1/1, Dependability.

National Annex NA is informative and provides some simple approximation methods for evaluating state transition diagrams without the need for more complicated mathematical procedures or computer software programs. These methods were omitted from IEC 61165 during the latest revision.

The importance of care when using modelling techniques cannot be overemphasized, particularly in the case of safety applications. An inaccurate model is destined to yield inaccurate results. Furthermore, it is important to appreciate that there may be unpredictable divergences between the results obtained by mathematical calculation and those obtained by simulation methods.

A list of organizations represented on DS/1/1 can be obtained on request to its secretary.

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 cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 29 February 2008

© BSI 2008

ISBN 978 0 580 54072 1

Amendments/corrigenda issued since publication

Date	Comments

**Application of Markov techniques
(IEC 61165:2006)**

Application des techniques de Markov
(CEI 61165:2006)

Anwendung des Markoff-Verfahrens
(IEC 61165:2006)

This European Standard was approved by CENELEC on 2006-07-01. 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

Foreword

The text of document 56/1096/FDIS, future edition 2 of IEC 61165, prepared by IEC TC 56, Dependability, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 61165 on 2006-07-01.

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) 2007-04-01
- latest date by which the national standards conflicting
with the EN have to be withdrawn (dow) 2009-07-01

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC 61165:2006 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 abbreviations.....	8
4.1 Symbols for state transition diagrams.....	8
4.2 Other symbols and abbreviations.....	9
4.3 Example	10
5 General description	10
6 Assumptions and limitations	11
7 Relationship with other analysis techniques.....	12
7.1 General.....	12
7.2 Fault Tree Analysis (FTA).....	12
7.3 Reliability Block Diagram (RBD)	13
7.4 Petri nets.....	13
8 Development of state transition diagrams	13
8.1 Prerequisites	13
8.2 Rules for development and representation.....	14
9 Evaluation	15
9.1 General.....	15
9.2 Evaluation of reliability measures	16
9.3 Evaluation of availability and maintainability measures.....	16
9.4 Evaluation of safety measures.....	17
10 Documentation of results	17
Annex A (informative) Basic mathematical relationships for Markov techniques	18
Annex B (informative) Example: Development of state transition diagrams	21
Annex C (informative) Example: Numerical evaluation of some reliability, availability, maintainability and safety measures for a 1-out-of-2 active redundant system	26
Annex ZA (normative) Normative references to international publications with their corresponding European publications	34
Bibliography.....	31
Figure 1 – Diagram of transition probabilities in time interval $(t, t+\Delta t)$, for arbitrary value of t and small Δt , for a non-restorable one-element system with constant failure rate λ	10
Figure 2 – State transition diagram of a non-restorable one-element system.....	10
Figure 3 - Interpretation of failure and restoration times in different contexts	16
Figure B.1 – State transition diagram for a restorable one-element system	21
Figure B.2 – State transition diagram with three states for a one-element system	21
Figure B.3 – State transition diagram when restorations may be made from state 2 for a one-element system.....	21

Figure B.4 – State transition diagram when direct transition is considered for a one-element system.....	22
Figure B.5 – State transition diagram for the evaluation of reliability of a one-element system.....	22
Figure B.6 – State transition diagram for a 1-out-of-2 active redundant system with no restorable elements	22
Figure B.7 – State transition diagram for a 1-out-of-2 active redundant system with restorable elements, two restoration teams and no restoration limitations	23
Figure B.8 – State transition diagram for a 1-out-of-2 active redundant system with restorable elements, two restoration teams and common cause for a system failure	23
Figure B.9 – State transition diagram for a 1-out-of-2 active redundant system with only one restoration team and restoration priority as first-in/first-out	24
Figure B.10 – Reliability block diagram for a 2-out-of-4 active redundant system	25
Figure B.11 – Aggregated state transition diagram for reliability computation of the system in Figure B.10	25
Figure C.1 – State transition diagram for 1-out-of-2 active redundant system with different elements and two restoration teams	26
Figure C.2 – State transition diagram for a 1-out-of-2 active redundant system with identical elements, two restoration teams and unlimited restoration resources	26
Figure C.3 – Numerical example for unavailability	28
Figure C.4 – Numerical example for dangerous failure rate	30

INTRODUCTION

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

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

APPLICATION OF MARKOV TECHNIQUES

1 Scope

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

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

2 Normative references

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

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

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

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

3 Terms and definitions

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

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

3.1

system

set of interrelated or interacting elements

[ISO 9000, 3.2.1]

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

NOTE 2 The structure of a system may be hierarchical.

3.2

element

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

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

3.3 system state

$X(t)$

particular combination of element states

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

3.4 up state

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

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

3.5 down state

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

NOTE A system can have several distinguishable down states.

3.6 hazard

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

[IEC 61508-4, 3.1.2, modified]

3.7 dangerous failure

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

[IEC 61508-4, 3.6.7, modified]

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

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

3.8 safe failure

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

[IEC 61508, modified]

3.9 transition

change from one state to another state

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

3.10 transition probability

$P_{ij}(t)$

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

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

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

3.11**transition rate** **q_{ij}**

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

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

3.12**initial state**

system state at time $t = 0$

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

3.13**absorbing state**

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

3.14**restorable system**

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

NOTE Repairable is also used in this context.

3.15**non-restorable system**

system the state transition diagram of which contains only transitions in the direction towards system failure states

NOTE Non-repairable is also used in this context.

4 Symbols and abbreviations**4.1 Symbols for state transition diagrams**

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

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

4.1.1 State symbol

A state is represented by a circle or a rectangle.

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

4.1.2 State description

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

4.1.3 State label

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

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

4.1.4 Transition arrow

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

4.2 Other symbols and abbreviations

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

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

4.3 Example

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

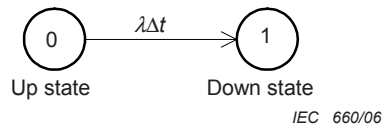


Figure 1 – Diagram of transition probabilities in time interval $(t, t+\Delta t)$, for arbitrary value of t and small Δt , for a non-restorable one-element system with constant failure rate λ

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

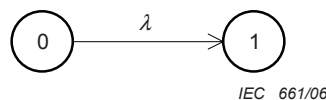


Figure 2 – State transition diagram of a non-restorable one-element system

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

5 General description

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

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