BRITISH STANDARD

BS 5760-15: 1995
IEC 1165:1995

Reliability of systems, equipment and components —

Part 15: Guide to the application of Markov techniques

Committees responsible for this British Standard

The preparation of this British Standard was entrusted to Technical Committee QMS/23, Reliability and maintainability of systems, upon which the following bodies were represented:

AEA Technology
Association of Consulting Engineers
Association of Project Managers
British Gas plc
British Railways Board
British Telecommunications plc
City University
Civil Aviation Authority
Consumers' Association
Cranfield Institute of Technology
Department of Trade and Industry (Standards Policy Unit)
Design Council
Electricity Association
Electronic Components Industry Federation
FEI (The Federation of the Electronics Industry)
Federation of Small Businesses
GAMBICA (BEAMA Ltd.)
Institute of Quality Assurance
Institute of Risk Management
Institution of Electrical Engineers
Institution of Mechanical Engineers
Institution of Plant Engineers
Mercury Communications Limited
Ministry of Defence
National Computing Centre Ltd.
Railway Industry Association of Great Britain
Royal Institution of Chartered Surveyors
Safety and Reliability Society
Society of British Aerospace Companies Limited
Society of Environmental Engineers
Society of Motor Manufacturers and Traders Limited
University of Technology, Loughborough

This British Standard, having been prepared under the direction of the Management Systems Sector Board, was published under the authority of the Standards Board and comes into effect on 15 July 1995

The following BSI references relate to the work on this standard:
Committee reference QMS/23
Draft for comment 90/97621 DC

ISBN 0 580 24164 5

Amendments issued since publication

Amd. No.	Date	Comments

Contents

National foreword

This Part of BS 5760 has been prepared by Technical Committee QMS/23. It is identical with IEC 1165:1995, *Application of Markov Techniques,* published by the International Electrotechnical Commission (IEC).

This Part provides guidance on the application of Markov techniques to dependability analysis. Further information, including advice on the application, benefits and limitations of Markov techniques, is given in BS 5760-2.11.

BS 5760 provides comprehensive guidance on many aspects of reliability management. Fifteen Parts of this standard have been published and these may be summarized as follows:

Part 0: Introductory guide to reliability. This Part provides guidance for senior management and non-specialists on the importance of reliability and explains how measures to achieve reliability should be integrated with other aspects of project management.

Part 1: Guide to reliability and maintainability programme management. This Part discusses the essential features of a comprehensive reliability and maintainability programme to produce reliable and maintainable products.

Part 2: Guide to the assessment of reliability. This Part explains the purpose and problems of assessing reliability. A range of available assessment techniques is reviewed and the principal advantages and limitations are outlined. Sections are included on the assessment of software reliability, human reliability and one-shot devices. The extension of these techniques to the assessment of availability and to the assessment of reliability of services is considered. This use of a range of statistical distributions to analyse reliability data is described.

Part 3: Guide to reliability practices: examples. This Part contains authentic practical examples illustrating the principles established in BS 5760-1 and 2.

Part 4: Guide to specification clauses relating to the achievement and development of reliability in new and existing items. This Part provides detailed guidance on the specification of reliability.

Part 5: Guide to failure modes, effects, and criticality analysis (FMEA and FMECA). This Part gives guidance on the application of these techniques.

Part 6: Guide to programmes for reliability growth. This Part describes procedures for exposing and removing weaknesses in hardware and software items in order to achieve acceptable reliability in a product. It explains basic concepts, management and test procedures and describes techniques for analysis and correction of failures.

Part 7: Guide to fault tree analysis. This Part gives guidance on the application of fault tree analysis. This technique may be used to identify factors affecting the reliability, performance and safety characteristics of a system.

Part 9: Guide to the block diagram technique. This Part describes the use of the block diagram technique for modelling and evaluating the reliability of both elementary and more complex systems. The extension of the method to calculate availability is also outlined.

Part 10: Guide to reliability of testing.

Section 10.1 General requirements. This Section provides guidance on general principles, procedures and considerations for reliability testing in the laboratory and in the field.

Section 10.2 Design of test cycles. This Section provides a general procedure for design of test cycles, where no applicable preferred test cycles can be found.

Section 10.3 Compliance test procedures for steady-state availability. This Section provides guidance on techniques for testing the availability performance of frequently maintained items under defined conditions.

Section 10.5 Compliance test plans for success ratio. This Section gives procedures for preparing and applying compliance test plans for success ratio or failure ratio. Plans are provided for three main types of test.

NOTE 1 Further Sections of Part 10 based on other Parts of IEC 605 and related IEC standards are planned.

Part 11: Guide to the collection of reliability, maintainability, availability and maintenance support data from the field. This Part provides guidance for the collection of data relating to reliability, maintainability, availability and maintenance support performance of items operating in the field. It deals in general terms with the practical aspects of data collection and presentation and briefly explores the related topics of data analysis and presentation of results.

Part 12: Guide to the presentation of reliability, maintainability and availability predictions. This Part gives guidance on the presentation of quantitative predictions of reliability, maintainability and availability. The items to be included when presenting prediction information are listed and explained with the object of facilitating comparisons between projects and reports.

Part 13: Guide to preferred test conditions for equipment reliability testing.

Section 13.1 Indoor portable equipment: low degree of simulation.

Section 13.2 Equipment for stationary use in weather protected locations: high degree of simulation.

Section 13.3 Equipment for stationary use in partially weather protected locations: low degree of simulation.

Section 13.4 Equipment for portable and non-stationary use: low degree of simulation.

Part 14: Guide to formal design review. This Part provides guidelines for planning and conducting design reviews. Much of the guidance given is widely applicable and relevant to the general conduct of design reviews but it also includes details of the specific contributions to be made by various specialists.

Part 15: Guide to the application of Markov techniques. This Part provides guidance on the application of Markov techniques to dependability analysis. Further information, including advice on the application, benefits and limitations of Markov techniques, is given in BS 5760-2.11.

Further Parts of BS 5760 are envisaged in order to provide guidance on other techniques of reliability management. At present one further Part is in the process of being drafted, and this is as follows:

Part 8: Guide to the assessment or reliability of systems containing software. This Part will provide guidance on the assessment of reliability of systems containing software. (This is currently published as DD 198:1991).

Whilst mainly addressing system and equipment level reliability, many of the techniques described in the Parts of BS 5760 may also be applied at the component level. Further guidance on component reliability is given in CECC 00804.

Guidance on specific aspects of maintainability is provided in the various Parts of BS 6548 *Maintainability of equipment.*

NOTE 2 This Part of BS 5760 makes reference to BS 4778 *Quality vocabulary*, and in particular to BS 4778-3.1, which contains definitions relating to reliability concepts applicable to this Part of BS 5760. It is essential that these definitions and concepts should be fully understood if this guide is to be interpreted correctly. For this reason it is recommended that BS 4778 should be read in conjunction with BS 5760.

NOTE 3 BS 4778-3.2 deprecates the use of the terms "failure modes and effects analysis" and "failure modes, effects and criticality analysis". It favours the use of "fault modes and effects analysis" and "fault modes, effects and criticality analysis", and these terms are used throughout BS 5760-2. However, the older terms have been retained in BS 5760-5 in order to align it with the current version of IEC 812.

Cross-references

Publication referred to	Corresponding British Standard
IEC 50(191):1990	BS 4778 *Quality vocabulary* Part 3. *Availability, reliability and maintainability terms.* Section 3.2:1991 *Glossary of international terms* (Identical)
IEC 1078:1991	BS 5760-9:1992 *Guide to the block diagram technique.* (Identical)

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their 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, pages i to vi, pages 1 to 14, an inside back cover and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

blank

Introduction

Several distinct analytical methods of dependability analysis are available, of which Markov analysis is one.

IEC 300-3-1 gives an overview of available methods and their general characteristics.

The relative merits of various methods and their individual or combined applicability in evaluating the dependability of a given system or component, should be examined by the analyst prior to deciding on the use of Markov analysis. For each method, consideration should also be given to the results produced, the data required to perform the analysis, the complexity of analysis, and other identified factors.

1 Scope

This International Standard provides guidance on the application of Markov techniques to dependability analysis.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 50(191):1990, *International Electrotechnical Vocabulary (IEV), chapter 191: Dependability and quality of service.*

IEC 1078:1991, *Analysis techniques for dependability — Reliability block diagram method.*

3 Definitions

For the purpose of this International Standard the terms and definitions of IEC (50)191 apply. In addition, the following terms and definitions are used:

3.1
unit

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

NOTE As such, the unit can exist in only two states: functional or failed (see **3.3** and **3.4**). For convenience, the term unit state will be used to denote the state of a unit.

3.2
system state

a system state is a particular combination of unit states

NOTE Several system states may be combined into one state.

3.3
functional state

a system (or unit) state in which the system (or unit) performs the required function

3.4
failed state

a system (or unit) state in which the system (or unit) does not perform the required function

NOTE A system can have several distinguishable failed states.

3.5
transition

a change from one state to another, usually as a result of failure or restoration

NOTE A transition may be also caused by other events such as human errors, external events, reconfiguration of software, etc.

3.6
transition probability

the probability of transition between one state and another state

3.7
initial state

the system state at time $t = 0$

NOTE Following a system failure, the system may be restored to the initial state. Generally, a system starts its operation at $t = 0$ from the complete functional state in which all units of the system are functioning and transits towards the final system state, which is a failed state, via other system functional states having progressively fewer functioning units.

3.8
absorbing state

a state from which, once entered, transitions are not possible

NOTE Once in an absorbing state, the system will stay there until in effect it is replaced, in its entirety, by a fully functional system.

3.9
restorable system

a system containing units which can fail and then be restored to their functional state, without necessarily causing system failure

NOTE 1 This corresponds to transitions in the state diagram in the direction towards the initial state. For this to be possible, the units concerned will invariably operate in redundant configurations.

NOTE 2 For a restorable system, dependability measures such as reliability, MTTFF, and availability are calculated.

3.10
non-restorable system

a system, the state transition diagram of which contains only transitions in the direction towards the final system failure state

NOTE For a non-restorable system, reliability measures such as reliability and MTTF are calculated.

4 Symbols and abbreviations

4.1 Symbols for state-transition diagrams

4.1.1 state symbol: A state is represented by a circle or a rectangle.

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 units which characterise the state.

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

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

4.1.4 transition arrow: The transition arrow indicates the direction of a transition (as a result of failure or restoration).

4.1.5 rates: Restoration rates and/or failure rates are written on the transition arrow.

4.2 Other symbols and abbreviations

Symbols for dependability measures follow those of IEC 50(191), where available. In this standard, the following symbols are used:

Symbol/ abbreviation	*Term*	*IEC 50(191) No*
$R(t)$	reliability NOTE 191-12-01 uses the general symbol $R(t_1, t_2)$	
MTTF	mean time to failure	191-12-07
MTTFF	mean time to first failure	191-12-06
MTBF	mean operating time between failures	191-12-09
MTTR	mean time to restoration	191-13-08
$\lambda(t)$	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
$A(\infty)$	asymptotic availability NOTE 191-11-05 uses A for 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	
Δt	a small time interval	

4.3 Example

An example of a state-transition diagram, applicable to a one-unit system, is shown in Figure 1.

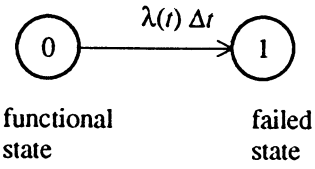


Figure 1 — State-transition diagram of a non-restorable one-unit system

$\lambda(t)\Delta t$ is the probability of a transition between states 0 and 1 in the small time interval Δt. Usually however, terms like $\lambda(t)\Delta t$ are replaced simply by λ. The reason for this is that in this standard $\lambda(t)$ is constant with respect to time (see clause **6**) and transition arrows are, by convention, labelled using transition rates rather than transition probabilities. Hence the diagram in Figure 1 is frequently drawn in the form shown in Figure 2.

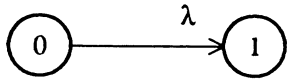


Figure 2 — State-transition diagram (simplified) of a non-restorable one-unit system

5 General

A Markov analysis makes use of a state-transition diagram which is a pictorial representation of the dependability performance of a system. It models the dependability aspects of the system's behaviour with time. In this standard, a system is regarded as a number of units, each of which can exist in only one of two states: failed or functional. The system as a whole, however, can exist in many different states, each being determined by the particular combination of failed and functioning units. Thus, as a unit fails or is repaired, the system "moves" from one state to the next. This kind of model is generally called a discrete-state, continuous time model. However, because of the way in which the model is presented, the associated methodology is also a special type of "state space" analysis.

State space analysis is especially suited to the dependability assessment of systems with redundancy, or to systems where system failure depends on sequential events, or to systems for which the maintenance strategies are complex, for example priority restoration, 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.

Provided the limitations described in clause **6** (below) can be accepted one of the major advantages of Markov analysis methods is that maintenance strategies, for example restoration priorities, can easily be modelled. Moreover, the order in which multiple failures occur can be represented in the model. It should be noted that other dependability analysis techniques, for example fault tree analysis and reliability block diagram methods, do not allow complex maintenance strategies to be taken into account.

Although state space analysis, from a theoretical viewpoint, is flexible and versatile, special precautions are necessary to deal with the difficulties of practical applications. The main problem is that the number of system states and possible transitions increases rapidly with the number of units in the system. The larger the number of states and transitions, the more likely is it that there will be errors and misrepresentations. To reduce this risk, it is advisable that certain rules be followed in designing the diagram. Also, the numerical techniques used for the evaluation of the diagram may be complex and may require special computer programs and/or assistance from experts in applied mathematics.

Not only are Markov analysis methods suited to the modelling of maintenance strategies, but such methods also enable the failure/restoration events to be modelled in a pictorial way, which is in itself a valuable feature. The process of failure/restoration is represented by transitions from one state symbol to another in the array of state symbols which together constitute the system state-transition diagram. The sum of all the state probabilities is unity, that is at any instant in time the system must be represented by one- and only one- of the states in the state-transition diagram. If, for practical reasons, states with low probability are omitted, the above condition is only approximately fulfilled.

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

6 Assumptions

The rules for generating the state-transition diagram stated in this standard apply generally. However, the description of numerical techniques apply only when the failure rates and restoration rates for all units in the analysed system are constant with respect to time. The assumption of constant failure rate is reasonably acceptable for components in many systems, but the assumption of constant restoration rate should be verified, unless the mean time to restoration of units is small by comparison with the corresponding mean-times-to-failure. Numerical evaluation for the general case, where failure rates or restoration rates are not constant with time, is outside the scope of this standard.

One particular difficulty is created by the assumption used for mathematical solutions: namely that the future behaviour of the system depends only on the present state of the system, and not on the way the system arrived at that state. The analyst shall ensure that the state-transition diagram is memoryless, even if the real system is not (see **7.3.2**).

The assumptions associated with transition probability can be summarised as follows:

— state transitions correspond to statistically independent events;

— the failure rate, λ, and the restoration rate, μ, are constant;

— the transition probabilities from one state to another in the time interval Δt, Δt being small, are given by $\lambda\Delta t$ and/or $\mu\Delta t$.

7 Development of state-transition diagrams

7.1 Precautions

A critical task in Markov analysis is the proper design of the state-transition diagram. Subclause **7.2** gives some recommended rules. They should be established before the analysis is undertaken and hence should provide for a proper identification of the individual states, thus enabling clear graphical models to be constructed.

7.2 Rules

The rules below are given as a guide. Other symbols or diagram arrangements may be more suitable in some instances, for example, for explaining various evaluation techniques, or for developing mathematical formulæ.

The following rules are recommended:

a) Each state should be identify by a symbol (circle or rectangle) with identification which allows the analytical procedure to refer uniquely to that state. The identifier is usually a letter or a number.

b) When necessary for clarity of the state-transition diagram, the symbol should include a clear description of the state, either directly, or by reference to an explanatory list. If a description is used the identifier for the state should be placed in a circle, or a small rectangle, adjacent to the state symbol.

c) States should be arranged so that the leftmost state is a fully functional state and the state(s) on the right is a failed state of the system. The relative positions of intermediate states should be such that a transition from left to right is a result of a failure, and a transition from right to left is achieved by a repair or restoration. For practical reasons, there may be a transition from the right margin to the left margin where this does not result in an increased number of transition line crossovers (see Figure 13 and Figure 14).

d) System states corresponding to the same number of failed units should be aligned vertically.

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

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

g) Transition lines associated with non-restorable units can have only one arrow, which in that case represents the failure transition. Systems where all units are restorable, and which are without maintenance constraints, that is the restoration starts immediately after failure of a unit, should be depicted by a diagram with transition line arrows from/to each unit. Partially restorable systems containing units, some of which are restorable and others which are not, or systems with restoration priorities, should be modelled using diagrams containing transition lines some of which have two arrows and others only one. To improve the readability of the diagram, two arrows between the same states should be combined into a single, doubleheaded arrow wherever possible.

h) Where possible, each transition should link only neighbouring state symbols. If a common cause failure disables simultaneously two or more units, a state may be bypassed (see Figure 6).

7.3 Examples

7.3.1 *One-unit system*

The first step in applying the Markov Analysis technique is to define the system states. As an example, consider a one-unit system. For the simplest case, the corresponding state-transition diagram comprises only two states: a functional state, with failure rate λ, and a failed state, with restoration rate μ, as shown in Figure 3.

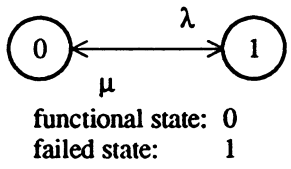


Figure 3 — State-transition diagram for a restorable one-unit system

The arrow from state 0 to state 1 denotes a failure occurrence with the probability $\lambda\Delta t$ during time Δt. The arrow from state 1 to state 0 shows completion of a system restoration with the probability $\mu\Delta t$ during time Δt.

A one-unit system can also be modelled using more than the two states 0 (functional) and 1 (failed). A degraded state which is still a functional state may also be included. Such a state is state 1 in Figure 4: the system failure state being state 2.

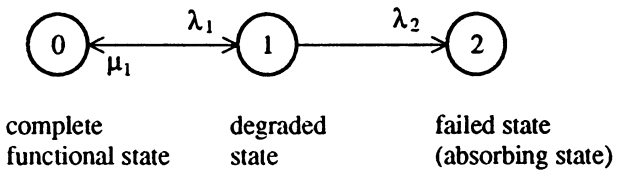


Figure 4 — State-transition diagram with three states for a one-unit system

If restoration can be carried out from state 2, the system can be modelled by the diagram in Figure 5, where the restoration rate μ_2 represents the transition from state 2 to state 1.

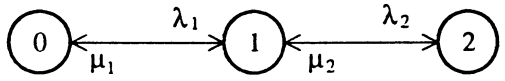


Figure 5 — State-transition diagram when repairs may be made from state 2

In many cases, a direct catastrophic failure path from state 0 to state 2 has to be considered, and an arrow λ_3 is added to Figure 4 to give Figure 6. This case may represent the life history of human beings, so that state 0 is a healthy state, state 1 is illness and state 2 is death.

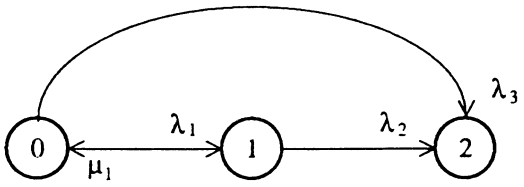


Figure 6 — State-transition diagram when direct path λ_3 is considered

The model depicted in Figure 3 can be used to obtain the instantaneous availability $A(t)$ and the steady-state (asymptotic) availability $A(\infty)$. If reliability $R(t)$ is required, the state-transition diagram shown in Figure 7 is applicable. Note that state 1 becomes an absorbing state.

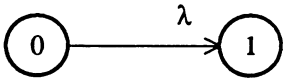


Figure 7 — State-transition diagram for the evaluation of reliability of a one-unit system

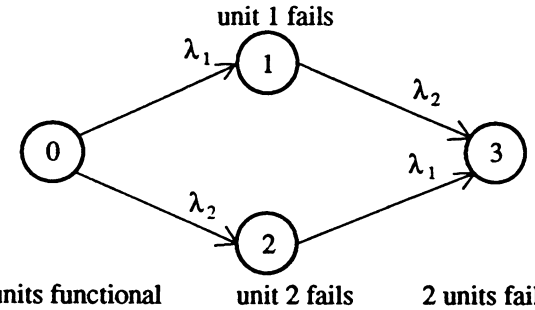
7.3.2 ***Two-unit system***

In general, since a unit can be represented by two states 0 (functional) and 1 (failed), possible system states for a two-unit
system are (0 0), (0 1), (1 0), (1 1). If the two-unit system is a series system, (0 0) is the only functional state and (0 1), (1 0), (1 1) axe failed states. If the two-unit system contains active or stand-by redundancy, (0 0), (0 1), (1 0) are all functional states. In what follows, consideration will be given solely to a two-unit active redundant system.

The state-transition diagram for a two-unit (series or parallel) system with no restorable units is illustrated in Figure 8.

If the system is restorable, arrows are added representing restoration with rates $\mu_1(i = 1, 2)$, as illustrated in Figure 9.

A common-cause failure can be introduced by considering a direct transition from state 0 to state 3, λ_3 representing the common cause failure rate (see Figure 10).



NOTE The state symbols may also be marked (0 0), (0 1), (1 0), (1 1).

Figure 8 — State-transition diagram for a two-unit system with no restorable units

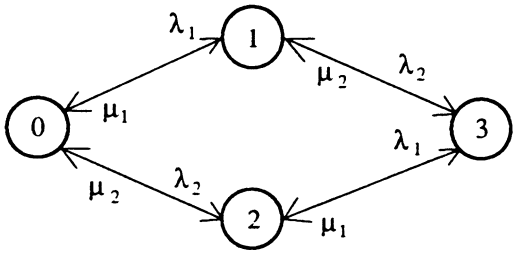


Figure 9 — State-transition diagram for a two-unit system with restorable units

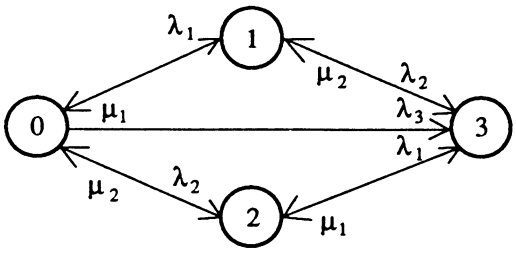


Figure 10 — State-transition diagram illustrating common cause failure

If a common-cause failure disables simultaneously two units in a restorable system, it is likely that the time needed to restore the system after a common cause failure (return from state 3 to state 0) differs from the time needed to restore the system after failures of the individual units. Thus, after reaching the failed state, the course of future action (type of restoration) depends on the past, which violates the requirement for the memoryless property of the model. In order to restore this property, it is necessary that the system restoration action shall be modelled as shown in Figure 11.

As an example, consider a system with two stand-by generators which does not start at low ambient temperatures. When the system reaches the state "both generators failed to start", the restoration time will depend on whether each generator was disabled by an independent mechanical failure, or both generators were incapacitated by a common cause, such as low ambient temperature. Therefore, it is necessary that the state "both generators failed to start due to independent faults" be considered as separate from the state "both generators failed to start due to a common cause". However, for the user of the system it may only be important that "both generators failed", and not how they failed. Therefore, it is necessary that both states form a combined state for which the dependability measures are obtained by combining (e.g. by adding the state probabilities) the measures of the included states.

State-transition diagrams can take maintenance strategies into account. Assume that only one restoration team exists and that the maintenance strategy is such that repair priority is always given to the component which has failed first. The order of failure occurrences has then to be taken into account. This is illustrated by the state diagram Figure 12.

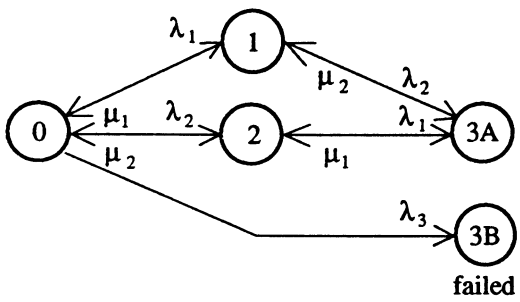


Figure 11 — State-transition diagram with common cause for a system failure

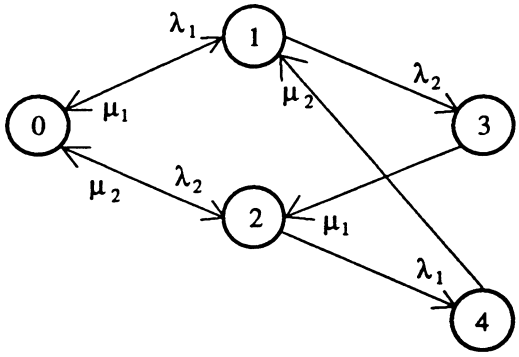


Figure 12 — State-transition diagram with only one restoration team

In Figure 12 the states 3 and 4 have the following meanings:

— state 3: the two components have failed, the component number 1 has failed first;

— state 4: the two components have failed, the component number 2 has failed first.

8 Evaluation of state-transition diagrams

8.1 General

The purpose of the evaluation of state-transition diagrams is to determine the dependability measures of the system concerned. The evaluation uses well known mathematical techniques. Note that the task of obtaining transient measures, for example $R(t)$ and $A(t)$, requires considerably more calculation than that of obtaining steady-state measures, for example MTTF, MDT, MUT and $A(\infty)$.

The first step consists of determining the probabilities of finding the system in individual states. Probabilities associated with individual states can be obtained by solving transition matrices, or by solving differential equations. See Annex A.

Other dependability measures can then be derived from such probabilities.

8.2 Evaluation of reliability measures

A state-transition diagram used for the evaluation of reliability [$R(t)$] contains at least one absorbing state. The probability that the system is in a given state at time t is calculated using special mathematical techniques. When t increases to infinity, the probability associated with each functioning state approaches zero, and that of absorbing states approaches unity.

A common dependability measure is MTTFF. When evaluating the state-transition diagram, the MTTFF is the mean of the total of the times spent by the system in functional states before making a transition to an absorbing state.

8.3 Evaluation of availability and maintainability measures

A state-transition diagram used for the evaluation of system availability [$A(t)$ or $A(\infty)$] contains no absorbing states.

The probability that the system is in a given state at time t is determined by the techniques given in Annex A. As t tends to infinity, the probability associated with each state approaches a constant value. The availability of the system also approaches a constant value, $A(\infty)$, being equal to the sum of the probabilities associated with the functioning states.

Two other useful measures can also be evaluated:

— mean time spent in a state, which is simply the reciprocal of the sum of the transition rates out of that state;

— frequency of entering a state, which is equal to the sum of terms such as $P_u\lambda_u + P_v\lambda_v + ...$ where P_u and λ_u denote the probability and failure rate respectively associated with state u, similarly for v and so on.

NOTE Each term of the type $P_u\lambda_u$ represents a transition into the state concerned and all such terms must be summed to obtain the frequency of entering the state. See the example in clause **9** below.

It is also possible to obtain from the state probabilities the MUT (mean up time) and MDT (mean down time) of the system. MUT is in fact the mean time spent in the functioning states and MDT the mean time spent in the failed states. It is also possible to derive the frequency of entering failed states. This is often equivalent to system failure rate. See the example in clause **9** below.

9 Simplifications and approximations

In many practical situations, it turns out that the mean time to restoration, MTTR, of a unit is very short in comparison with its MTTF, that is $\mu \gg \lambda$, for all the units involved. Under such circumstances, the use of a computer to solve sets of linear differential equations is rarely necessary. An approximate value for the asymptotic probability $P_i(\infty)$ of finding the system in the i-th state when t tends to infinity can easily be obtained. The approximation method is based on the fact that if a state "x" has one or more failure transitions into it given by $P_u(\infty)\lambda_u + P_v(\infty)\lambda_v + \ldots$ where $P_u(\infty)$ and λ_u and other similar terms are as indicated in **8.3** above, and transitions out of it (state "x") denoted by $\Sigma\mu_x$, then $P_x(\infty)$ is given approximately by

$$P_x(\infty) = \frac{\lambda_u P_u(\infty) + \lambda_v P_v(\infty) + \ldots}{\Sigma \mu_x}$$

where $P_x(\infty)$, $P_u(\infty)$, and $P_v(\infty)$ are steady state probabilities. If this procedure is repeated for each state, a set of equations for the individual state probabilities is generated. It should be noted, however, that if for some states there arc no repair transitions, then the approximation method as described will not be valid.

Using the above technique, an approximate value for the system MTTFF can be obtained by first of all calculating the (functional) state probabilities and using these to calculate the failure rate of the system. This is illustrated by the following example.

Example: Consider the state diagram of Figure 9 and omit the (∞) notation since, unless otherwise stated, all state probabilities are steady state probabilities. The quantities P_1 and P_2 are given by:

$$P_1 \approx \lambda_1 P_0/\mu_1$$

and

$$P_2 \approx \lambda_2 P_0/\mu_2$$

Thus the system failure rate λ_s being the frequency the system enters the "system failed" state (see above), is given by:

$$\lambda_s \approx \lambda_2 P_1 + \lambda_1 P_2$$

that is $\lambda_s \approx [\lambda_2\lambda_1/\mu_1 + \lambda_1\lambda_2/\mu_2]P_0$

that is $\lambda_s \approx \lambda_2\lambda_1/\mu_1 + \lambda_1\lambda_2/\mu_2$ since when $\mu >> \lambda, P_0 \approx 1$

This latter expression is a well known result and is often written in the form:

$$\lambda_s \approx \lambda_1\lambda_2[\tau_1 + \tau_2]$$

where $\tau_1 = 1/\mu_1$ and $\tau_2 = 1/\mu_2$ (τ denotes mean restoration time).

10 Collapsed state-transition diagram

For ease of computation, attempts should be made to construct state-transition diagrams using as few a number of states as possible. If units in a parallel redundant configuration can be assumed to all have the same failure rate, λ, and all have the same restoration rate, μ, as indicated, for example, by Figure 13, and if it is further assumed that there are as many repairmen as failures, then the state-transition diagram can be expressed in a collapsed form illustrated by Figure 14.

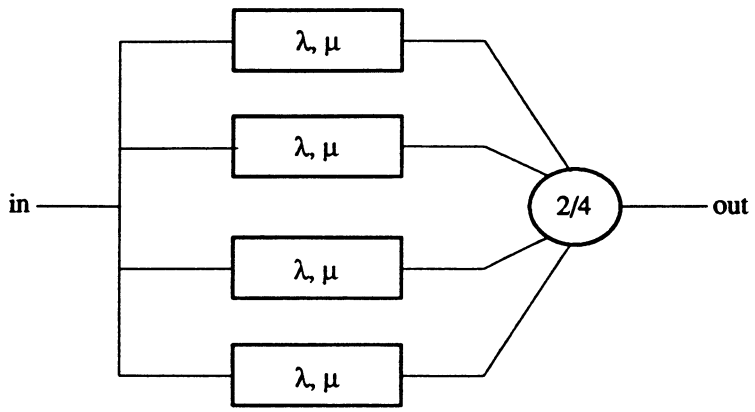


Figure 13 — Reliability block diagram for a 2-out-of-4 parallel system

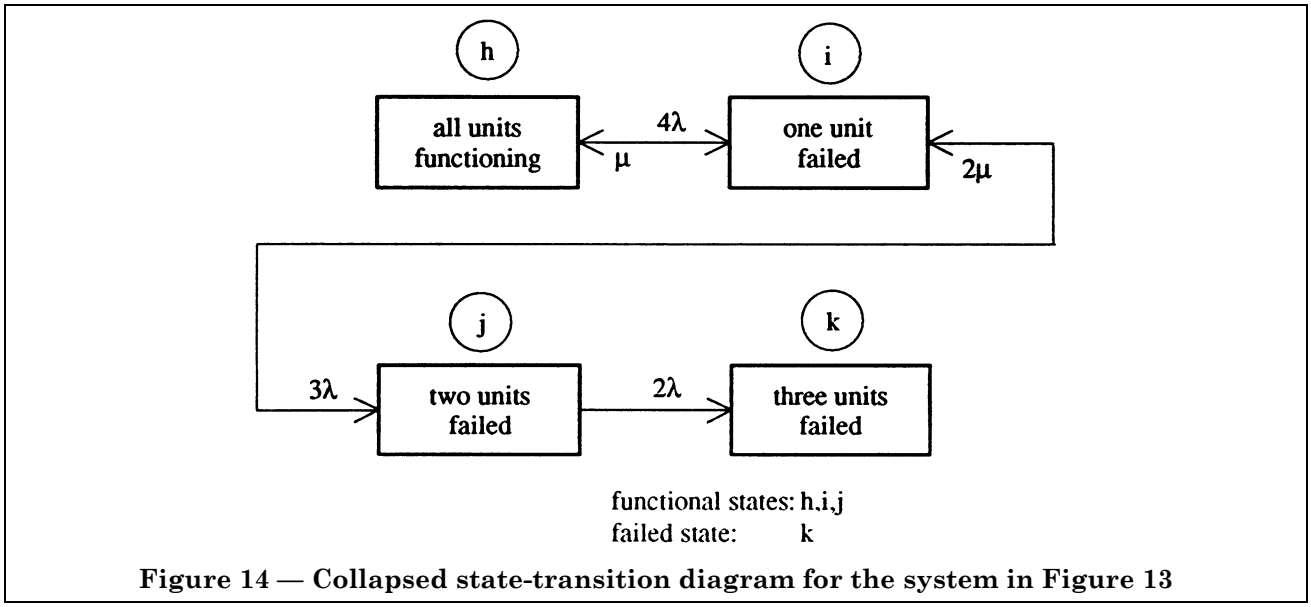


Figure 14 — Collapsed state-transition diagram for the system in Figure 13

From the above diagram, a set of linear differential equations can be obtained and solved (see Annex A) to give the following expression for the system mean time to first failure (MTTFF):

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

An exact expression for system MTTFF can thus be derived. The expression shows a distinct pattern which can be used to obtain a formula for collapsed chains of any length. As an example, for the configuration in Figure 15 it is possible to show that:

$$MTTFF = \frac{1}{\lambda_h}\left(\frac{\mu_i\mu_j\mu_k}{\lambda_i\lambda_j\lambda_k}+\frac{\mu_i\mu_j}{\lambda_i\lambda_j}+\frac{\mu_i}{\lambda_i}+1\right) + \frac{1}{\lambda_i}\left(\frac{\mu_j\mu_k}{\lambda_j\lambda_k}+\frac{\mu_j}{\lambda_j}+1\right) + \frac{1}{\lambda_j}\cdot\left(\frac{\mu_k}{\lambda_k}+1\right) + \frac{1}{\lambda_k}$$

11 Reliability and availability expressions for system configurations

Annex B contains two sets of tables, the first of which contains formulae for the dependability measures of non-restorable systems, while the second is concerned solely with restorable systems.

Further information can be found in standard textbooks.

12 Presentation of results

The presentation of the analysis should incorporate at least the following elements:

a) specification of the desired dependability measures (for example reliability, availability, maintainability, MTTF);

b) the main assumptions used (for instance, constant failure and restoration rates);

c) definition of method chosen, including justification;

d) description of the state-transition diagram including in-depth examination of the following aspects:

— the functioning and failed states described separately;

— where applicable, the reasons why some states are grouped and others are omitted;

— transitions between states described separately;

— the choice of numerical values for the transition rates;

— the way the graph is built including any assumptions;

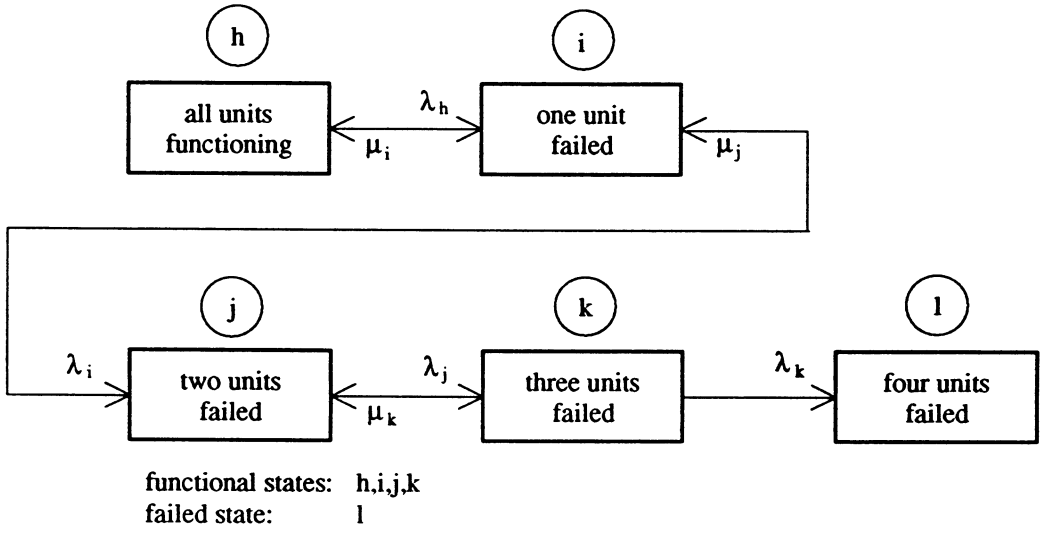


Figure 15 — Collapsed state-transition diagram for a parallel system (four units)

e) description of the computation:

— methods;

— computer programs, if used;

f) numerical results:

— results in numerical and other forms;

— influence of the assumptions used for constructing the state-transition diagram or for calculations;

— sensitivity analysis.

Annex A (informative) Example: Numerical evaluation of some dependability measures of a two-unit active redundant system

A.1 Objective

In this annex a system of two units in parallel is considered. The measures to be assessed are asymptotic availability, instantaneous availability, reliability and MTTFF. Conventional mathematical methods commonly used in this field, are applied.

A.2 Modelling

The state-transition diagram of a system of two parallel units (active redundancy) is given in Figure A.1 for the assessment of the availability. State 3 is the failed state.

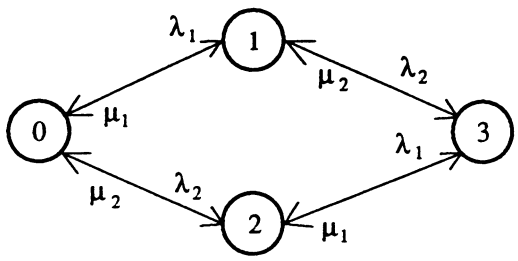


Figure A.1 — State-transition diagram for a two-unit system

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

Assume that the two units in the system are identical, or have the same failure/restoration rates. The reduced diagram then becomes as Figure A.2.

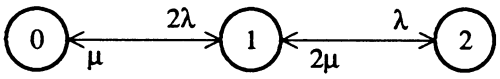


Figure A.2 — State-transition diagram of a system with two identical units

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

A.3 Differential equation method

A.3.1 *Method for availability*

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

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

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

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

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

$P_0(0) = 1$

$P_1(0) = 0$

$P_2(0) = 0$

The instantaneous availability, $A(t)$ is then computed as:

$A(t) = P_0(t) + P_1(t)$

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

$$A(t) = \frac{\mu^2 + 2\lambda\mu}{(\lambda+\mu)^2} + \left(\frac{\lambda}{\mu+\lambda}\right)^2 e^{-(\lambda+\mu)t}\left[2 - e^{-(\lambda+\mu)t}\right]$$

From the above expression, the asymptotic availability, $A(\infty)$, follows immediately. Alternatively, it can be calculated by noting that, at time t = ∞, the following equations are valid:

$$0 = -2\lambda P_0(\infty) + \mu P_1(\infty)$$

$$0 = 2\lambda P_0(\infty) - (\lambda+\mu) P_1(\infty) + 2\mu P_2(\infty)$$

$$0 = \lambda P_1(\infty) - 2\mu P_2(\infty)$$

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

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

A.3.2 *Method for reliability*

To assess the reliability and the MTTFF of such a system the following differential equations are obtained from the state diagram in Figure A.2 bearing in mind that state 2 must be considered as an absorbing state (the restoration transition from state 2 to state 1 is removed):

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

$$\frac{dP_1(t)}{dt} = 2\lambda P_0(t) - (\lambda + \mu) P_1(t) \qquad \text{Equation set A}$$

$$\frac{dP_2(t)}{dt} = \lambda P_1(t)$$

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

$P_0(0) = 1$

$P_1(0) = 0$

$P_2(0) = 0$

The system reliability $R_s(t)$ is then computed as:

$R_s(t) = P_0(t) + P_1(t)$

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

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

where

$s_1 s_2 = 2\lambda^2$

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

The MTTFF can be calculated either from the expression for $R_s(t)$, in which case

$$\text{MTTFF} = \int_0^\infty R(t)dt = \frac{\mu + 3\lambda}{2\lambda^2}$$

or from the set of equations obtained by integrating equations A above from $t = 0$ to $t = \infty$. Details of such methods can be found in the literature.

Annex B (informative)
Tables of reliability and availability expressions for basic system configurations

Table B.1 — Reliability, $R(t)$, and mean time to failure, MTTF, of non-restorable redundant structures

Type of structure	$R(t)$	MTTF
1-out-of-n (general formula)	$1-\prod_{k=1}^{n}\left(1-R_k(t)\right)$	$\left(\frac{1}{\lambda_1}+\ldots+\frac{1}{\lambda_n}\right)-\left(\frac{1}{\lambda_1+\lambda_2}+\ldots+\frac{1}{\lambda_i+\lambda_j}\right)+\left(\frac{1}{\lambda_1+\lambda_2+\lambda_3}+\ldots+\frac{1}{\lambda_i+\lambda_j+\lambda_k}\right)-\ldots+\frac{(-1)^{n+1}}{\sum_{i=1}^{n}\lambda_i}$
1-out-of-n	$1-(1-p)^n$	$\frac{1}{\lambda}\cdot\sum_{i=1}^{n}\frac{1}{i}$
(n-1)-out-of-n	$np^{n-1}-(n-1)p$	$\frac{1}{\lambda}\cdot\frac{2n-1}{n(n-1)}$
2-out-of-3	$3p^2-2p^3$	$\frac{1}{\lambda}\cdot\frac{5}{6}$
2-out-of-4	$6p^2-8p^3+3p^4$	$\frac{1}{\lambda}\cdot\frac{13}{12}$
3-out-of-5	$10p^3-15p^4+6p^5$	$\frac{1}{\lambda}\cdot\frac{47}{60}$
r-out-of-n	$\sum_{i=r}^{n}\binom{n}{i}p^i(1-p)^{n-1}$	$\frac{1}{\lambda}\cdot\sum_{i=r}^{n}\frac{1}{i},\quad 1\le r\le n$
1-out-of-n (n-1) units in standby, (ideal switch)	$e^{-\lambda t}\sum_{i=0}^{n-1}\frac{(\lambda t)^i}{i!}$	$\frac{1}{\lambda}\cdot$ n
r-out-of-n (n-r) units in standby, (ideal switch)	too complicated	$\frac{1}{\lambda}\cdot\frac{n-r+1}{r}$, $1\le r\le n$
NOTE $p=e^{-\lambda t}$		

Table B.2 — Approximate mean system failure rate of restorable parallel redundant structures

Type of structure	Type of redundancy	Mean system failure rate
1-out-of-n (general formula)	a	$\left(\prod_{k=1}^{n}\lambda_k\mu_k\right)\sum_{k=1}^{n}\frac{1}{\mu_k}$
1-out-of-n (identical units)	a	$n\lambda^n\mu^{n-1}$
(n-1)-out-of-n	a	$n(n-1)\lambda^2\mu$
1-out-of-2	a	$2\lambda^2\mu$
1-out-of-3	a	$3\lambda^3\mu^2$
2-out-of-3	a	$6\lambda^2\mu$
1-out-of-2	s	$\lambda^2\mu$
(n-1)-out-of-n	s	$(n-1)^2\lambda^2\mu$

NOTE 1 Types of redundancy:
a = active redundancy
s = passive redundancy

NOTE 2 Assumptions:
1) as many repairmen as faults
2) ideal switch
3) $\lambda\mu \ll 1$

Annex C (informative) Bibliography

IEC 300-3-1:1991, *Dependability management — Part 3: Application guide. — Section 1: Analysis techniques for dependability: Guide on methodology*.

List of references

See national foreword.

BS 5760-15: 1995
IEC 1165:1995

BSI — British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Tel: 020 8996 9000. Fax: 020 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: 020 8996 9001. Fax: 020 8996 7001.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: 020 8996 7111. Fax: 020 8996 7048.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: 020 8996 7002. Fax: 020 8996 7001.

Copyright

BSI
389 Chiswick High Road
London
W4 4AL